JUNIPER NETWORKS | Engineering Simplicity

# Junos® OS

# Unified Threat Management User Guide

Published
2020-09-23

junos

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net



*Junos® OS Unified Threat Management User Guide*


The information in this document is current as of the date on the title page.

## YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

## END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

5

## Web Filtering

7

## Configuration Statements

8

## Operational Commands

# About the Documentation

IN THIS SECTION



Use this guide to configure, monitor, and manage the Unified Threat Management (UTM) features in Junos OS NFX Series and SRX Series devices to secure the network from viruses, malware, or malicious attachments and protect the users from security threats.

## Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at https://www.juniper.net/documentation/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at https://www.juniper.net/books.

## Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

### Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
       scripts {
           commit {
               file ex-script.xsl;
           }
       }
   }
   interfaces {
       fxp0 {
           disable;
           unit 0 {
               family inet {
                   address 10.0.0.1/24;
               }
           }
       }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

### Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

   ```
   [edit]
   user@host# edit system scripts
   [edit system scripts]
   ```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

   ```
   [edit system scripts]
   user@host# load merge relative /var/tmp/ex-script-snippet.conf
   load complete
   ```

For more information about the **load** command, see CLI Explorer.

## Documentation Conventions

Table 1 on page xxiii defines notice icons used in this guide.

**Table 1: Notice Icons**

| Icon | Meaning | Description |
|---|---|---|
|  | Informational note | Indicates important features or instructions. |
|  | Caution | Indicates a situation that might result in loss of data or hardware damage. |
|  | Warning | Alerts you to the risk of personal injury or death. |
|  | Laser warning | Alerts you to the risk of personal injury from a laser. |
|  | Tip | Indicates helpful information. |
|  | Best practice | Alerts you to a recommended use or implementation. |

Table 2 on page xxiii defines the text and syntax conventions used in this guide.

**Table 2: Text and Syntax Conventions**

| Convention | Description | Examples |
|---|---|---|
| **Bold text like this** | Represents text that you type. | To enter configuration mode, type the **configure** command:<br>user@host> **configure** |
| `Fixed-width text like this` | Represents output that appears on the terminal screen. | `user@host>` **show chassis alarms**<br>`No alarms currently active` |
| *Italic text like this* | • Introduces or emphasizes important new terms.<br>• Identifies guide names.<br>• Identifies RFC and Internet draft titles. | • A policy *term* is a named structure that defines match conditions and actions.<br>• *Junos OS CLI User Guide*<br>• RFC 1997, *BGP Communities Attribute* |

**Table 2: Text and Syntax Conventions *(continued)***

| Convention | Description | Examples |
|---|---|---|
| *Italic text like this* | Represents variables (options for which you substitute a value) in commands or configuration statements. | Configure the machine's domain name:<br>[edit]<br>root@# **set system domain-name** *domain-name* |
| **Text like this** | Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components. | • To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level.<br>• The console port is labeled **CONSOLE**. |
| < > (angle brackets) | Encloses optional keywords or variables. | **stub <default-metric *metric*>;** |
| \| (pipe symbol) | Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity. | **broadcast \| multicast**<br>**(*string1* \| *string2* \| *string3*)** |
| # (pound sign) | Indicates a comment specified on the same line as the configuration statement to which it applies. | **rsvp { # Required for dynamic MPLS only** |
| [ ] (square brackets) | Encloses a variable for which you can substitute one or more values. | **community name members [ *community-ids* ]** |
| Indention and braces ( { } ) | Identifies a level in the configuration hierarchy. | [edit]<br>routing-options {<br>  static {<br>  route default {<br>  nexthop *address*;<br>  retain;<br>  }<br>  }<br>} |
| ; (semicolon) | Identifies a leaf statement at a configuration hierarchy level. | |
| **GUI Conventions** | | |

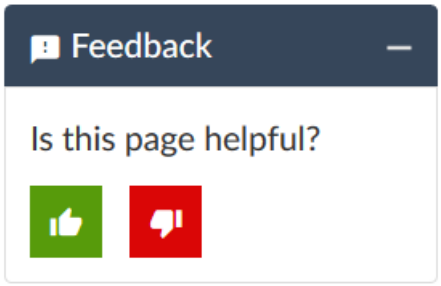
Table 2: Text and Syntax Conventions *(continued)*

| Convention | Description | Examples |
|---|---|---|
| **Bold text like this** | Represents graphical user interface (GUI) items you click or select. | • In the Logical Interfaces box, select **All Interfaces**.<br>• To cancel the configuration, click **Cancel**. |
| > (bold right angle bracket) | Separates levels in a hierarchy of menu selections. | In the configuration editor hierarchy, select **Protocols>Ospf**. |

## Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:




  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

### Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

### Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://myjuniper.juniper.net.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://support.juniper.net/support/requesting-support/.

1
CHAPTER

# Overview

# UTM Overview

IN THIS SECTION



Unified Threat Management (UTM) provides multiple security features and services in a single device or service on the network, protecting users from security threats in a simplified way. UTM includes functions such as antivirus, antispam, content filtering, and web filtering. UTM secures the network from viruses, malware, or malicious attachments by scanning the incoming data using Deep Packet Inspection and prevents access to unwanted websites by installing Enhanced Web filtering. For more information, see the following topics:

## Unified Threat Management Overview

Unified Threat Management (UTM) is a term used to describe the consolidation of several security features into one device, protecting against multiple threat types. The advantage of UTM is streamlined installation and management of these multiple security capabilities.

The security features provided as part of the UTM solution are:

- Antispam Filtering— E-mail spam consists of unwanted e-mail messages, usually sent by commercial, malicious, or fraudulent entities. The antispam feature examines transmitted e-mail messages to identify e-mail spam. When the device detects an e-mail message deemed to be spam, it either drops the message or tags the message header or subject field with a preprogrammed string. The antispam feature uses a constantly updated spam block list (SBL). Sophos updates and maintains the IP-based SBL. The antispam feature is a separately licensed subscription service.
- Content Filtering— Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, protocol command, and embedded object type. Content filtering does not require a separate license.
- Web Filtering— Web filtering lets you manage Internet usage by preventing access to inappropriate Web content. There are three types of Web filtering solutions. The integrated Web filtering solution, the decision-making for blocking or permitting Web access is done on the device after it identifies the category for a URL either from user-defined categories or from a category server (Websense provides the CPA Server). The integrated Web filtering feature is a separately licensed subscription service which is supported only on SRX Series devices. The redirect Web filtering solution intercepts HTTP requests

and forwards the server URL to an external URL filtering server provided by Websense to determine whether to block or permit the requested Web access. Redirect Web filtering does not require a separate license. With Juniper Local Web Filtering, the decision-making for blocking or permitting Web access is done on the device after it identifies the category for a URL from user-defined categories stored on the device. With Local filtering, there is no additional Juniper license or remote category server required.

- Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, on SRX1500 Services Gateways and vSRX instances, UTM policies, profiles, MIME patterns, filename extensions, and protocol-command numbers are increased to 500; custom URL patterns and custom URL categories are increased to 1000.

  Starting with Junos OS Release 15.1X49-D70 and Junos OS Release 17.3R1, SRX4100 and SRX4200 devices support up to 500 UTM policies, profiles, MIME patterns, filename extensions, and protocol commands, and up to 1000 custom URL patterns and custom URL categories.

  Starting with Junos OS Release 18.2R1, NFX150 devices support up to 500 UTM policies, profiles, MIME patterns, filename extensions, and protocol commands, and up to 1000 custom URL patterns and custom URL categories.

  Starting with Junos OS Release 18.2R1, the following commands under the **[edit security utm feature-profile]** hierarchy level are deprecated:
  - **set web-filtering type**
  - **set web-filtering url-blacklist**
  - **set web-filtering url-whitelist**
  - **set web-filtering http-persist**
  - **set web-filtering http-reassemble**
  - **set web-filtering traceoptions**
  - **set web-filtering juniper-enhanced cache**
  - **set web-filtering juniper-enhanced reputation**
  - **set web-filtering juniper-enhanced query-type**
  - **set anti-virus mime-whitelist**
  - **set anti-virus url-whitelist**
  - **set anti-virus type**
  - **set anti-virus traceoptions**
  - **set anti-virus sophos-engine**
  - **set anti-spam address-blacklist**
  - **set anti-spam address-whitelist**

- **set anti-spam traceoptions**
- **set content-filtering traceoptions**

Starting with Junos OS Release 18.4R3, on SRX1500, SRX4100, SRX4200, SRX4600, SRX4800, SRX5400, SRX5600, and SRX5800 devices, UTM policies, profiles, MIME patterns, filename extensions, protocol commands, and custom messages, are increased up to 1500. Custom URL patterns and custom URL categories are increased up to 3000.

This feature requires a license. To understand more about UTM Licensing, see, Understanding UTM Licensing. Please refer to the Juniper Licensing Guide for general information about License Management. Please refer to the product Data Sheets at SRX Series Services Gateways for details, or contact your Juniper Account Team or Juniper Partner.

- Antivirus— The Avira antivirus module in the unified threat management (UTM) solution consists of a virus pattern database, an application proxy, a scan manager, and a configurable scan engine. The antivirus module on the SRX Series device scans specific application layer traffic to protect the user from virus attacks and to prevent viruses from spreading.

### Understanding UTM Custom Objects

Before you can configure most UTM features, you must first configure the custom objects for the feature in question. Custom objects are global parameters for UTM features. This means that configured custom objects can be applied to all UTM policies where applicable, rather than only to individual policies.

The following UTM features make use of certain custom objects:

- Web Filtering (see “Example: Configuring Integrated Web Filtering” on page 340)
- Anti-Spam (see “Server-Based Antispam Filtering Configuration Overview” on page 111)
- Content Filtering (see “Content Filtering Configuration Overview” on page 135)

Starting in Junos OS Release 18.2R1, a new dynamic application policy match condition is added to SRX Series devices, allowing an administrator to more effectively control the behavior of Layer 7 applications. To accommodate Layer 7 application-based policies in UTM, the **[edit security utm default-configuration]** hierarchy level is introduced. If any parameter in a specific UTM feature profile configuration is not configured, then the corresponding parameter from the UTM default configuration is applied. Additionally, during the initial policy lookup phase which occurs prior to a dynamic application being identified, if there are multiple policies present in the potential policy list which contains different UTM profiles, the SRX Series device applies the default UTM profile until a more explicit match has occurred.

SEE ALSO

Understanding Unified Policies [Unified Threat Management (UTM)] | 46

**Release History Table**

| Release | Description |
| --- | --- |
| 18.4R3 | Starting with Junos OS Release 18.4R3, on SRX1500, SRX4100, SRX4200, SRX4600, SRX4800, SRX5400, SRX5600, and SRX5800 devices, UTM policies, profiles, MIME patterns, filename extensions, protocol commands, and custom messages, are increased up to 1500. Custom URL patterns and custom URL categories are increased up to 3000 |
| 18.2R1 | Starting with Junos OS Release 18.2R1, NFX150 devices support up to 500 UTM policies, profiles, MIME patterns, filename extensions, and protocol commands, and up to 1000 custom URL patterns and custom URL categories. |
| 18.2R1 | Starting with Junos OS Release 18.2R1, the following commands under the **[edit security utm feature-profile]** hierarchy level are deprecated:<br>• **set web-filtering type**<br>• **set web-filtering url-blacklist**<br>• **set web-filtering url-whitelist**<br>• **set web-filtering http-persist**<br>• **set web-filtering http-reassemble**<br>• **set web-filtering traceoptions**<br>• **set web-filtering juniper-enhanced cache**<br>• **set web-filtering juniper-enhanced reputation**<br>• **set web-filtering juniper-enhanced query-type**<br>• **set anti-virus mime-whitelist**<br>• **set anti-virus url-whitelist**<br>• **set anti-virus type**<br>• **set anti-virus traceoptions**<br>• **set anti-virus sophos-engine**<br>• **set anti-spam address-blacklist**<br>• **set anti-spam address-whitelist**<br>• **set anti-spam traceoptions**<br>• **set content-filtering traceoptions** |

| | |
|---|---|
| 18.2R1 | Starting in Junos OS Release 18.2R1, a new dynamic application policy match condition is added to SRX Series devices, allowing an administrator to more effectively control the behavior of Layer 7 applications. To accommodate Layer 7 application-based policies in UTM, the **[edit security utm default-configuration]** hierarchy level is introduced. If any parameter in a specific UTM feature profile configuration is not configured, then the corresponding parameter from the UTM default configuration is applied. Additionally, during the initial policy lookup phase which occurs prior to a dynamic application being identified, if there are multiple policies present in the potential policy list which contains different UTM profiles, the SRX Series device applies the default UTM profile until a more explicit match has occurred. |
| 15.1X49-D70 | Starting with Junos OS Release 15.1X49-D70 and Junos OS Release 17.3R1, SRX4100 and SRX4200 devices support up to 500 UTM policies, profiles, MIME patterns, filename extensions, and protocol commands, and up to 1000 custom URL patterns and custom URL categories. |
| 15.1X49-D60 | Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, on SRX1500 Services Gateways and vSRX instances, UTM policies, profiles, MIME patterns, filename extensions, and protocol-command numbers are increased to 500; custom URL patterns and custom URL categories are increased to 1000. |

RELATED DOCUMENTATION


- Web Filtering Overview | **147**
- Antispam Filtering Overview | **108**
- Express Antivirus Protection | **233**


# UTM Supported Features

**IN THIS SECTION**

# WELF Logging for UTM Features

IN THIS SECTION



## Understanding WELF Logging for UTM Features

UTM features support the WELF standard. The WELF Reference defines the WebTrends industry standard log file exchange format. Any system logging to this format is compatible with Firewall Suite 2.0 and later, Firewall Reporting Center 1.0 and later, and Security Reporting Center 2.0 and later.

A WELF log file is composed of records. Each record is a single line in the file. Records are always in chronological order. The earliest record is the first record in the file; the most recent record is the last record in the file. WELF places no restrictions on log filenames or log file rotation policies.

> **NOTE:** Each WELF record is composed of fields. The record identifier field (**id=**) must be the first field in a record. All other fields can appear in any order.

The following is a sample WELF record:

```
id=firewall time="2000-2-4 12:01:01" fw=192.168.0.238 pri=6 rule=3 proto=http
       src=192.168.0.23 dst=6.1.0.36 rg=www.example.com/index.html op=GET result=0
       rcvd=1426
```

The fields from the example WELF record include the following required elements (all other fields are optional):

- **id** (Record identifier)
- **time** (Date/time)
- **fw** (Firewall IP address or name)
- **pri** (Priority of the record)

## Example: Configuring WELF Logging for UTM Features

IN THIS SECTION



This example shows how to configure WELF logging for UTM features.

### *Requirements*

Before you begin, review the fields used to create a WELF log file and record. See "UTM Overview" on page 28.

### *Overview*

A WELF log file is composed of records. Each record is a single line in the file. Records are always in chronological order. The earliest record is the first record in the file; the most recent record is the last record in the file. WELF places no restrictions on log filenames or log file rotation policies. In this example, the severity level is emergency and the name of the security log stream is **utm-welf**.

### *Configuration*

#### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security log source-address 1.2.3.4 stream utm-welf
set security log source-address 1.2.3.4 stream utm-welf format welf
set security log source-address 1.2.3.4 stream utm-welf format welf category content-security
set security log source-address 1.2.3.4 stream utm-welf format welf category content-security severity emergency
set security log source-address 1.2.3.4 stream utm-welf format welf category content-security severity emergency
    host 5.6.7.8
```

#### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure WELF logging for UTM features:

1. Set the security log source IP address.

```
[edit security log]
user@host# set source-address 1.2.3.4
```

> **NOTE:** You must save the WELF logging messages to a dedicated WebTrends server.

2. Name the security log stream.

```
[edit security log]
user@host# set source-address 1.2.3.4 stream utm-welf
```

3. Set the format for the log messages.

```
[edit security log]
user@host# set source-address 1.2.3.4 stream utm-welf format welf
```

4. Set the category of log messages that are sent.

```
[edit security log]
user@host# set source-address 1.2.3.4 stream utm-welf format welf category content-security
```

5. Set the severity level of log messages that are sent.

```
[edit security log]
user@host# set source-address 1.2.3.4 stream utm-welf format welf category content-security severity
    emergency
```

6. Enter the host address of the dedicated WebTrends server to which the log messages are to be sent.

```
[edit security log]
```

```
user@host# set source-address 1.2.3.4 stream utm-welf format welf category content-security severity
  emergency host 5.6.7.8
```

**Results**

From configuration mode, confirm your configuration by entering the **show security log** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security log
stream utm-welf {
   severity emergency;
   format welf;
   category content—
security;
   host {
       5.6.7.8;
   }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

***Verification***

***Verifying the Security Log***

**Purpose**

Verify that the WELF log for UTM features is complete.

**Action**

From operational mode, enter the **show security utm status** command to verify if the UTM service is running or not.

SEE ALSO

Understanding UTM Support for Active/Backup Chassis Cluster | 49

*Understanding UTM Licensing*

# Explicit Proxy for UTM

IN THIS SECTION



UTM support the use of an explicit proxy for the cloud-based connectivity for Enhanced Web Filtering (EWF) and Sophos antivirus (SAV) on unified threat management (UTM). The explicit proxy hides the identity of the source device and establishes a connection with the destination device.

## Understanding Explicit Proxy

An explicit proxy hides the identity of source device, communicates directly with the Websense Threatseeker Cloud (TSC) server and establishes a connection with the destination device. The explicit proxy configuration consists of port address and direct IP address or hostname.

To use the explicit proxy, create one or more proxy profiles and refer to those profiles:

- In EWF, the explicit proxy is configured by referring to the created **proxy-profile** in **security utm default-configuration web-filtering juniper-enhanced server** hierarchy. The connection is established with the TSC server.
- In EWF predefined category upgrading and base filter, the explicit proxy is configured by referring to the created **proxy-profile** in **security utm custom-objects category-package proxy-profile** hierarchy. You can download and dynamically load new EWF categories without any software upgrade. The **proxy-profile** category file is installed and used for transfer of the traffic.

  SRX device sends *CONNECT* request to the proxy server, the SRX device and TSC server communicates through the HTTP connection. Then the proxy server is expected to identify the configured IP addresses, allowlist and allow SRX device to send traffic to the TSC server in cloud via proxy. After proxy filtering, it will create connection to real TSC server.

- In Sophos Antivirus (SAV), the explicit proxy is configured by referring to the created **proxy-profile** in **security utm default-configuration anti-virus sophos-engine pattern-update** hierarchy. The *utmd* process connects to the proxy host instead of the SAV pattern update server on the cloud.

On EWF, if the proxy profile is configured in UTM Web filtering configuration, the TSC server connection is established with the proxy host instead of the UTM server on the cloud.

On SAV, if the proxy profile is configured, the *utmd* process connects to the proxy host instead of the SAV pattern update server on the cloud.

> **NOTE:** The proxy server authentication is not supported if the **proxy-profile** is configured.

### Configuring the Explicit Proxy on Juniper Enhanced Server

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

Create a proxy profile with host and port information, and refer it in the Juniper enhanced server to establish a connection to the UTM cloud server.

The following configuration shows how to configure the explicit proxy on Juniper enhanced server.

1. Assigning host IP address for proxy profile.

```
[edit services proxy profile]
user@host# set proxy1 protocol http host 192.0.2.1
```

2. Assigning port address for proxy profile.

```
[edit services proxy profile]
user@host# set proxy1 protocol http port 3128
```

3. Assign the proxy profile to the Web filtering Juniper enhanced server.

```
[edit security utm default-configuration web-filtering juniper-enhanced server]
user@host# set proxy-profile proxy1
```

**Results**

From configuration mode, confirm your configuration by entering the **show security** and **show services** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security
    default-configuration {
        web-filtering {
            type juniper-enhanced;
            juniper-enhanced {
                server {
                    proxy-profile proxy1;
                }
            }
        }
    }
```

```
[edit]
user@host# show services
    proxy {
        profile proxy1 {
            protocol {
                http {
                    host 192.0.2.1;
                    port 3128;
                }
            }
        }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verifying the Explicit Proxy Configuration on Juniper Enhanced Server

**Purpose**

Display the status of explicit server on Juniper enhanced server.

**Action**

From operational mode, enter the **show security utm web-filtering status** command.

**user@host> show security utm web-filtering status**
**UTM web-filtering status:**
**Server status: Juniper Enhanced using Websense server UP**

**Meaning**

This command provides information on server status of Enhanced Web Filtering (EWF) using Websense Threatseeker Cloud (TSC).

## Configuring the Predefined Category Upgrading and Base Filter Configuration Using Explicit Proxy

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

Create a proxy profile with host and port information, and refer it in the predefined category upgrade and base filter to download and dynamically load new EWF categories without any software upgrade.

The following configuration shows how to configure the explicit proxy on predefined category upgrading and base filter.

1. Assigning host IP address for proxy profile.

```
[edit services proxy profile]
user@host# set proxy1 protocol http host 203.0.113.1
```

2. Assign port address for proxy profile.

```
[edit services proxy profile]
user@host# set proxy1 protocol http port 3128
```

3. Assign the proxy profile to the category packages in the custom objects.

```
[edit security utm custom-objects]
user@host# set category-package proxy-profile proxy1
```

**Results**

From configuration mode, confirm your configuration by entering the **show security** and **show services** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security
   custom-objects {
      category-package {
         proxy-profile proxy1;
      }
   }
```

```
[edit]
user@host# show services
   proxy {
      profile proxy1 {
         protocol {
            http {
               host 203.0.113.1;
               port 3128;
            }
         }
      }
   }
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verifying the Predefined Category Upgrading and Base Filter Configuration

**Purpose**

Display the Enhanced Web Filtering (EWF) predefined category package download, install, and update status.

**Action**

From operational mode, enter the **show security utm web-filtering category status** CLI command to see the web filtering category status.

**NOTE:** Before you execute the **show security utm web-filtering category status** CLI command, you must execute the **request security utm web-filtering category download-install** CLI command to get the results.

```
user@host> show security utm web-filtering category status
UTM category status:
    Installed version:  1
    Download version:   0
    Update status:      Done
```

**Meaning**

This command provides information on the number of installed and downloaded categories and the update status.

### Configuring the Sophos Antivirus Pattern Update

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

Create a proxy profile with host and port information, and refer it in the Sophos Antivirus (SAV) pattern update. The *utmd* process connects to the proxy host instead of the SAV pattern update server on the cloud.

The following configuration shows how to configure the explicit proxy on SAV pattern update.

1. Assigning host IP address for proxy profile.

   ```
   [edit services proxy profile ]
   user@host# set proxy1 protocol http host 203.0.113.1
   ```

2. Assign port address for proxy profile.

   ```
   [edit services proxy profile ]
   user@host# set proxy1 protocol http port 3128
   ```

3. Assign the proxy profile to the Sophos antivirus pattern update.

   ```
   [edit security utm default-configuration anti-virus sophos-engine pattern-update]
   ```

```
user@host# set proxy-profile proxy1
```

**Results**

From configuration mode, confirm your configuration by entering the **show security** and **show services** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security
   default-configuration {
      anti-virus {
         sophos-engine {
            pattern-update {
               proxy-profile proxy1;
            }
         }
      }
   }
```

```
[edit]
user@host# show services
   proxy {
      profile proxy1 {
         protocol {
            http {
               host 203.0.113.1;
               port 3128;
            }
         }
      }
   }
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verifying the Sophos Antivirus Pattern Update

**Purpose**

Display the Sophos Antivirus (SAV) update pattern status.

**Action**

From operational mode, enter the **show security utm anti-virus status** CLI command to see the UTM antivirus status.

```
user@host> show security utm anti-virus status
UTM anti-virus status:

   Anti-virus key expire date: 2018-08-02 00:00:00
   Update server: https://host2.example.com/SAV/
          Interval: 1000 minutes
          Pattern update status: next update in 979 minutes
          Pattern update via proxy server: 203.0.113.1:3128
          Last result: already have latest database
   Anti-virus signature version: 1.13 (1.02)
   Scan engine type: sophos-engine
   Scan engine information: last action result: No error
```

**Meaning**

This command provides information on the the Sophos Antivirus (SAV) pattern update server, update status, antivirus signature version, antivirus engine type and antivirus engine information.

## Unified Policies for UTM

**IN THIS SECTION**



### Understanding Unified Policies [Unified Threat Management (UTM)]

Unified policies are now supported on SRX Series devices, allowing granular control and enforcement of dynamic Layer 7 applications within the traditional security policy.

Unified policies are security policies in which you can use dynamic applications as match conditions along with existing 5-tuple or 6-tuple matching conditions (with user firewall) to detect application changes over time. The use of unified policies enable you to enforce a set of rules for the transit traffic. It uses the match criteria, namely, source zone, destination zone, source addresses, destination addresses, and application names. This results in potential match policies.

The unified policy configuration handles all Application Firewall (AppFW) functionalities and simplifies the task of configuring firewall policy to permit or block application traffic from the network. As part of the unified policy, a new dynamic application policy match condition is added to SRX Series devices, allowing an administrator to more effectively control the behavior of Layer 7 applications.

To accommodate Layer 7 application-based policies in UTM, the **[edit security utm default-configuration]** command is introduced. If any parameter in a specific UTM feature profile configuration is not configured, then the corresponding parameter from the UTM default configuration is applied.

Additionally, during the initial policy lookup phase which occurs prior to a dynamic application being identified, if there are multiple policies present in the potential policy list which contains different UTM profiles, the SRX Series device applies the default UTM profile until a more explicit match has occurred.

***Understanding Default UTM Policy***

A new predefined default UTM policy is available with the factory default configuration to provide a default UTM configuration. This predefined global UTM policy inherits the configuration from the default UTM configuration profile.

If there is an existing UTM policy defined, it will continue to be used to evaluate traffic based on the existing security policy configuration.

When a policy lookup is performed, existing UTM policies are evaluated prior to global policies. The predefined UTM default policy is leveraged if multiple UTM policies exist in the potential policy list during the UTM session creation process.

The predefined UTM default policy parameters are included under **[edit security utm default-configuration]** hierarchy level. These parameters are available for Web filtering, content filtering, antivirus, and antispam profile. If no UTM feature profile is configured (Web filtering, content filtering, antivirus, and antispam), the parameters in the predefined global UTM configuration are applied.

The predefined UTM default policy is available in **[edit groups junos-defaults security utm]**. You can modify certain parameters for Web filtering, content filtering, antivirus, and antispam. You can also modify default UTM profile parameters for Web filtering, content filtering, antivirus, and antispam features profiles at **[edit security utm default-configuration]**.

SEE ALSO

*Global Policy Overview*

utm default-configuration | **631**

feature-profile | **443**

# UTM Support for Chassis Cluster

IN THIS SECTION



UTM is supported for active/active chassis cluster and active/backup chassis cluster configuration. For more information, see the following topics:

## Understanding UTM Support for Active/Active Chassis Cluster

UTM requires a license for each device in the chassis cluster setup. For information about how to purchase a software license, contact your Juniper Networks sales representative at https://www.juniper.net/in/en/contact-us/ and for more information refer Licensing guide.

All the following UTM features are supported in active/active chassis cluster:

- Antispam Filtering
- Content Filtering
- Sophos Antivirus Scanning
- Enhanced Web Filtering
- Local Web Filtering
- Websense Redirect Web Filtering
- On-box/Avira AV

UTM supports active/active chassis cluster configuration from Junos OS Release 19.4R1 onwards. Active/Active cluster is a cluster where interfaces can be active on both cluster nodes simultaneously. This is the case when there are more than one data-plane redundancy-groups, that is redundancy-groups 1 and higher or when local (non-reth) interfaces are used on the cluster nodes.

Enhanced Web Filtering cloud connection does not support failover, it will create new connection automatically after the old connection is retired.

### Understanding UTM Support for Active/Backup Chassis Cluster

UTM requires a license for each device in the chassis cluster setup. For information about how to purchase a software license, contact your Juniper Networks sales representative at https://www.juniper.net/in/en/contact-us/.

The following UTM features are supported in chassis cluster:

- Content filtering
- URL (Web) filtering
- Antispam filtering
- Full file-based antivirus scanning
- Sophos antivirus scanning

Active/Active cluster is a cluster where interfaces can be active on both cluster nodes at the same time. This is the case when there are more than one data-plane redundancy-groups, i.e. redundancy-groups 1 and higher or when local (non-reth) interfaces are used on the cluster nodes.

If multiple data-plane redundancy-groups are configured, UTM works only if all the redundancy groups are active in the single node. In case one of the redundancy-group failed over automatically to another node, UTM won't work.

SEE ALSO

*Chassis Cluster Overview*

*Preparing Your Equipment for Chassis Cluster Formation*

*Understanding Chassis Cluster Redundancy Groups*

*Understanding Chassis Cluster Redundant Ethernet Interfaces*

Unified Threat Management Overview | **28**

RELATED DOCUMENTATION

Integrated Web Filtering | **337**

Local Web Filtering | **191**

Redirect Web Filtering | **207**

# Allowlist

IN THIS SECTION



A URL allowlist defines all the URLs listed for a specific category to always bypass the scanning process. The allowlist include hostnames that you want to exempt from undergoing SSL proxy processing. For more information, see the following topics:

## Understanding MIME Allowlist

The gateway device uses MIME (Multipurpose Internet Mail Extension) types to decide which traffic may bypass antivirus scanning. The MIME allowlist defines a list of MIME types and can contain one or many MIME entries.

A MIME entry is case-insensitive. An empty MIME is an invalid entry and should never appear in the MIME list. If the MIME entry ends with a / character, prefix matching takes place. Otherwise, exact matching occurs.

There are two types of MIME lists used to configure MIME type antivirus scan bypassing:

- mime-allowlist list—This is the comprehensive list for those MIME types that can bypass antivirus scanning.
- exception list—The exception list is a list for excluding some MIME types from the mime-allowlist list. This list is a subset of MIME types found in the mime-allowlist.

  For example, if the mime-allowlist includes the entry,**video/** and the exception list includes the entry **video/x-shockwave-flash**, by using these two lists, you can bypass objects with “video/” MIME type but not bypass “video/x-shockwave-flash” MIME type.

  You should note that there are limits for mime-allowlist entries as follows:

  - The maximum number of MIME items in a MIME list is 50.
  - The maximum length of each MIME entry is restricted to 40 bytes.
  - The maximum length of a MIME list name string is restricted to 40 bytes.

## Example: Configuring MIME Allowlist to Bypass Antivirus Scanning

IN THIS SECTION



This example shows how to configure MIME allowlists to bypass antivirus scanning.

### *Requirements*

Before you begin, decide the type of MIME lists used to configure MIME type antivirus scan bypassing. See "Understanding MIME Allowlist" on page 50.

### *Overview*

In this example, you create MIME lists called avmime2 and ex-avmime2 and add patterns to them.

### *Configuration*

#### Step-by-Step Procedure

To configure MIME allowlists to bypass antivirus scanning:

1. Create MIME lists and add patterns to the lists.

```
[edit]
user@host# set security utm custom-objects mime-pattern avmime2 value [video/quicktime
   image/x-portable-anymap x-world/x-vrml]
user@host# set security utm custom-objects mime-pattern ex-avmime2 value [video/quicktime-inappropriate]
```

2. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

### *Verification*

To verify the configuration is working properly, enter the **show security utm** command.

### Understanding URL Allowlist

A URL allowlist defines all the URLs listed for a specific category to always bypass the scanning process. The allowlist includes hostnames that you want to exempt from undergoing SSL proxy processing. There are also legal requirements to exempt financial and banking sites; such exemptions are achieved by configuring URL categories corresponding to those hostnames under the URL allowlists. If any URLs do not require scanning, corresponding categories can be added to this allowlisting.

Starting with Junos OS Release 15.1X49-D80 and Junos OS Release 17.3R1, the allowlisting feature is extended to include URL categories supported by UTM in the allowlist configuration of SSL forward proxy. For more information, see *Application Security User Guide for Security Devices*.

Starting with Junos OS Release 17.4R1, the allowlisting feature is extended to support custom URL categories supported by UTM in the allowlist configuration of SSL forward proxy.

### Configuring URL Allowlist to Bypass Antivirus Scanning (CLI Procedure)

To configure URL allowlists, use the following CLI configuration statements:

```
security utm custom-objects {
    custom-url-category { ; set of list
        name url-category-name; #mandatory
        value url-pattern-name;
    }
}
```

RELATED DOCUMENTATION

Full Antivirus File Scanning | 297

Full Antivirus Scan Results and Fallback Options | 313

2
CHAPTER

# Antivirus Protection

# On-Device Avira Antivirus

IN THIS SECTION



Read this topic to understand about how to use Avira Antivirus for scanning application traffic and preventing viruses from entering your network.

You can also watch the video Avira Antivirus Solution on SRX Series Devices to understand about installing and using Avira antivirus on your security device.

## Avira Antivirus Overview

Junos OS unified threat management (UTM) integrates with Avira's Antivirus functionality and provides full file-based scan engine. This antivirus protection secures your device by scanning the application layer traffic and blocks the harmful content such as infected files, trojans, worms, spyware, and other malicious data.

Avira Antivirus scans the network traffic by accessing the virus pattern database and identifies the virus. Avira Antivirus drops the infected file and notifies the user.

Table 3 on page 55 lists the components and license details for Avira Antivirus.

**Table 3: Components and License Details for Avira Antivirus**

| Components | Detailed Information |
|---|---|
| Virus pattern database | Avira Antivirus checks the virus signature database to identify and then remove signatures.<br><br>The virus pattern database is available at the following locations:<br><br>• Default: https://update.juniper-updates.net/avira<br>• For SRX4100, SRX4200, and SRX4600 Series devices: https://update.juniper-updates.net/AVIRA/SRXTVP<br>• For SRX5K-SPC3 devices: https://update.juniper-updates.net/AVIRA/SPC3<br>• For vSRX: https://update.juniper-updates.net/AVIRA/VSRX<br><br>By default, SRX Series devices downloads the updates for pattern database. See "Configure Avira Antivirus Scanning Options" on page 58 to schedule the automatic download option. |
| Avira Antivirus scan engine | Avira Antivirus provides the scan engine that examines a file for known viruses at real-time. You must install and activate Avira Antivirus scan engine on your SRX Series device. See "Example: Configure Avira Antivirus" on page 56 for steps to install and activate Avira Antivirus scan engine.<br><br>Avira Antivirus scan engine decompresses files before scanning for virus detection. For more information, see **decompress-layer-limit**.<br><br>In the following scenarios, Avira Antivirus scan engine on the SRX Series device does not scan the application traffic:<br><br>• The scan engine is not ready.<br>• There are too many scanning requests.<br>• The scanned file size is larger than a configured limit.<br>• The scanned file has too many nested layers of compression.<br>• The memory file system is full. |
| License details | Avira Antivirus scan engine is a licensed subscription service.<br><br>With this license, you can use a full file-based and real-time Avira Antivirus scanning function. The antivirus functionality uses the latest updated virus signature database.<br><br>When the license expires, you can continue to use the locally stored antivirus signatures without any updates. If you delete the local database, you cannot run antivirus scanning.<br><br>For more information about licenses, see *Licenses for SRX Series*. |

## Benefits

- Secures your device and protects your network from viruses, trojans, rootkits, and other types of malicious code.

- Provides improved scanning performance as the virus signature database and Avira Antivirus scan engine reside locally on the device.

SEE ALSO

Full Antivirus Scan Results and Fallback Options | 313

scan-options (Security Antivirus Avira Engine) | 563

## Example: Configure Avira Antivirus

### Requirements

Before you begin:

- Verify that you have a Avira antivirus license. For more information on how to verify licenses on your device, see Understanding Licenses for SRX Series Devices.
- SRX Series device with Junos OS Release 18.4R1 or later.

We've tested this example using an SRX1500 device with Junos OS Release 18.4R1.

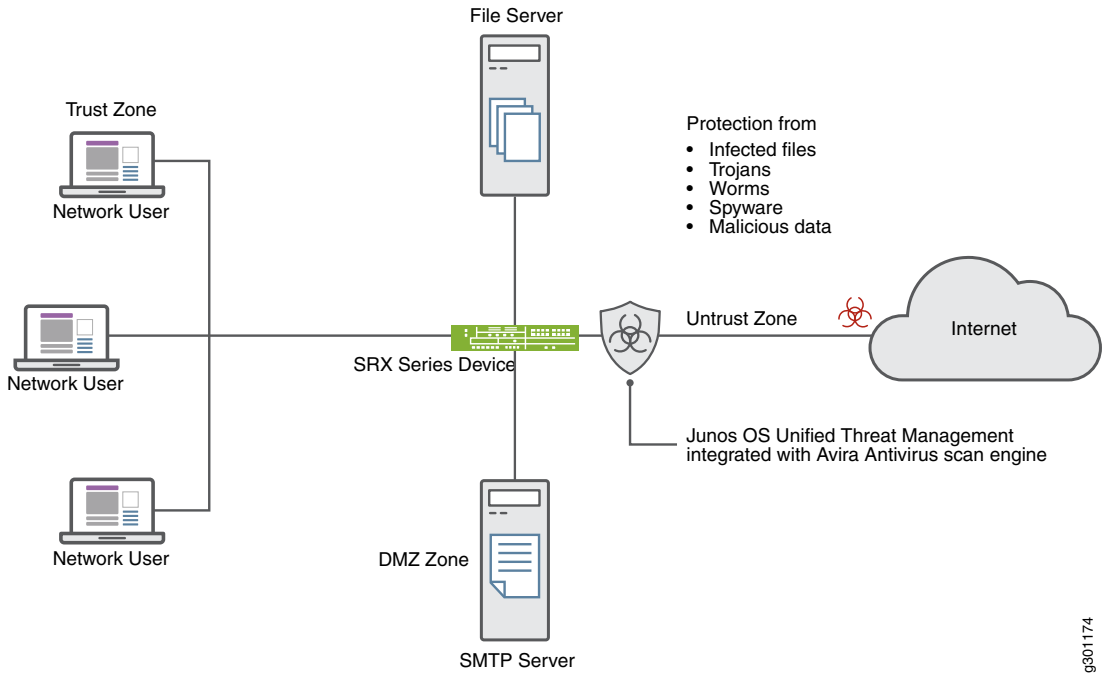
### Overview

Let's take a look at a typical enterprise network. An end user unknowingly visits a compromised Website and downloads a malicious content. This action results in compromise of the endpoint. The harmful content on the endpoint also becomes a threat to other hosts within the network. It is important to prevent the download of the malicious content.

You can use an SRX Series device with Avira antivirus to protect users from virus attacks and to prevent spreading of viruses in your system, Avira antivirus scans network traffic for viruses, trojans, rootkits, and other types of malicious code and blocks the malicious content immediately when detected.

Figure 1 on page 57 shows an example of Avira antivirus on SRX Series device usage.

**Figure 1: Avira Antivirus on SRX Series**




In this example, you'll learn how to configure Avira antivirus on your security device. You have the following options.

- To use default Avira antivirus options to get started, see Use Default Antivirus Profile to Start Antivirus Scanning
- To customize antivirus options as per your requirements, see Use Customized Avira Antivirus Options For Antivirus Scanning
- To set antivirus scanning options, see Enable Avira Antivirus Scanning

## Configuration

### *Use Default Antivirus Profile to Start Antivirus Scanning*

You can enable the Juniper Networks pre-configured antivirus profile. When you use the default antivirus feature profile option, you don't have to configure additional parameter. In this procedure, you create an UTM policy with default antivirus profiles for all protocols and apply the UTM policy in a security policy for the permitted traffic.

#### Step-by-Step Procedure

To use default antivirus profile, complete the following steps:

1. Enable Avira antivirus scan on your security device.

```
user@host# set security utm default-configuration anti-virus type avira-engine
```

After configuring Avira as the antivirus type, reboot the device for the new scan engine to take effect.

2. Select default antivirus profile for HTTP, FTP, SMTP, POP3, and IMAP protocols.

```
[edit]
user@host# set security utm default-configuration anti-virus type avira
user@host# set security utm utm-policy P1 anti-virus http-profile junos-av-defaults
user@host# set security utm utm-policy P1 anti-virus ftp upload-profile junos-av-defaults
user@host# set security utm utm-policy P1 anti-virus ftp download-profile junos-av-defaults
user@host# set security utm utm-policy P1 anti-virus smtp-profile junos-av-defaults
user@host# set security utm utm-policy P1 anti-virus pop3-profile junos-av-defaults
user@host# set security utm utm-policy P1 anti-virus imap-profile junos-av-defaults
```

3. Apply the UTM policy to the security policy.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy POLICY-1 match source-address
   any
user@host# set security policies from-zone trust to-zone untrust policy POLICY-1 match destination-address
   any
user@host# set security policies from-zone trust to-zone untrust policy POLICY-1 match application any
user@host# set security policies from-zone trust to-zone untrust policy POLICY-1 then permit
   application-services utm-policy P1
```

4. Commit the configuration.

```
[edit]
user@host# commit
```

You can also watch the video Avira Antivirus Solution on SRX Series Devices to understand about installing and using Avira antivirus on your security device.

***Configure Avira Antivirus Scanning Options***

**Step-by-Step Procedure**

In this procedure, you'll perform optional steps to prepare your security device to use Avira antivirus.

1. Manually update the virus signature database, specify the URL of the database server. If you do not specify a URL, a default URL is provided, https://update.juniper-updates.net/avira. By default, your security device downloads the pattern updates from https://update.juniper-updates.net/avira. The

location of virus pattern database depends on your SRX Series mode. See Table 3 on page 55 for more details.

```
[edit]
user@host# set security utm default-configuration anti-virus avira-engine pattern-update url
    http://www.example.net/
```

This step downloads the pattern and engine files from the specified URL.

2. Set an interval for regular download of antivirus pattern update.

```
[edit]
user@host# set security utm default-configuration anti-virus avira-engine pattern-update interval 2880
```

In this step, you are changing the default from every 24 hours to every 48 hours. The default antivirus pattern-update interval is 1440 minutes (every 24 hours).

3. Send an e-mail notification once pattern update completes.

```
[edit]
user@host# set security utm default-configuration anti-virus avira-engine pattern-update email-notify
    admin-email admin@email.net custom-message “Avira antivirus data file was updated”
    custom-message-subject “AV data file updated”
```

4. (Optional) Configure pattern update from an proxy profile.

```
[edit]
set security utm default-configuration anti-virus avira-engine pattern-update proxy-profile proxy-profile
    <proxy-profile>
```

Use this option in case your internal network device do not have direct access to the Internet and the device can reach the Internet only through a proxy server.

5. (Optional) Configure on-box antivirus to heavy mode.

```
[edit]
user@host# set chassis onbox-av-load-flavor heavy
```

This step allocates additional resources for improved performance.

To use the antivirus scan in light mode, use the **delete chassis onbox-av-load-flavor heavy** command. Reboot the device once you change the modes.

6. (Optional) Change the operating mode from the default continuous delivery function (CDF) to hold mode. When you change to hold mode, the system withhold all the packets until you get the final result.

```
[edit]
user@host# set security utm default-configuration anti-virus forwarding-mode hold
```

For more details on CDF mode and Inline Tap mode, see forwarding-mode.

***Configure Avira Antivirus Scanning with Custom Profile***

You must complete the steps as in Table 4 on page 60 to configure Avira antivirus with custom options on your security device.

**Table 4: Steps for Avira Antivirus Scanning Using Custom Profile**

| Step | Details |
|---|---|
| Step 1: Define custom objects | In this step, you will define antivirus scanning options:<br>• MIME allowlist—Include type of traffic that you want to bypass antivirus scanning<br>• MIME exception list—Specify excluding some MIME types from the MIME allowlist<br>• Custom URL categories—Define URLs that you want to bypass antivirus scanning.<br>Alternatively, you can use the default list junos-default-bypass-mime. |
| Step 2: Create antivirus feature profile | • Apply MIME list, exception list, and custom URL category created in step 1 to the antivirus feature profile.<br>• Configure antivirus scanning settings such as data file update interval, notification options for administrators, fallback options, and file size limits. |
| Step 3: Create UTM policy | Associate the antivirus profile created in Step 2 for FTP, HTTP, POP3, SMTP, and IMAP traffic. UTM policies control which protocol traffic is sent to the antivirus scanning engine. |
| Step 4: Apply UTM policy to a security policy | Specify UTM policy as application services in the security policy. The UTM antivirus settings are applied for the traffic that matches the security policy rules. |

See scan-options and trickling to understand about the scanning configuration parameters available for antivirus feature.

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm default-configuration anti-virus type avira-engine
set security utm custom-objects mime-pattern Mime_1 value video/
set security utm custom-objects mime-pattern Mime_exception value video/x-shockwave-flash
set security utm custom-objects url-pattern Pattern_List_1 value www.juniper.net
set security utm custom-objects custom-url-category Cust_URL_Cat value Pattern_List_1
set security utm feature-profile anti-virus profile Avira-AV-Profile fallback-options default log-and-permit
set security utm feature-profile anti-virus profile Avira-AV-Profile fallback-options content-size block
set security utm feature-profile anti-virus profile Avira-AV-Profile fallback-options engine-not-ready
    log-and-permit
set security utm feature-profile anti-virus profile Avira-AV-Profile fallback-options timeout log-and-permit
set security utm feature-profile anti-virus profile Avira-AV-Profile fallback-options out-of-resources
    log-and-permit
set security utm feature-profile anti-virus profile Avira-AV-Profile fallback-options too-many-requests
    log-and-permit
set security utm feature-profile anti-virus profile Avira-AV-Profile notification-options fallback-block type
    protocol-only
set security utm feature-profile anti-virus profile Avira-AV-Profile notification-options fallback-block
    notify-mail-sender
set security utm feature-profile anti-virus profile Avira-AV-Profile notification-options fallback-block
    custom-message " fallback block action occured “
set security utm feature-profile anti-virus profile Avira-AV-Profile notification-options fallback-block
    custom-message-subject " Antivirus Fallback Alert "
set security utm feature-profile anti-virus profile Avira-AV-Profile mime-whitelist list Mime_1
set security utm feature-profile anti-virus profile Avira-AV-Profile url-whitelist Cust_URL_Cat
set security utm feature-profile anti-virus profile Avira-AV-Profile mime-whitelist list Mime_exception
set security utm utm-policy UTM-AV-Policy anti-virus http-profile Avira-AV-Profile
set security utm utm-policy UTM-AV-Policy anti-virus ftp upload-profile Avira-AV-Profile
set security utm utm-policy UTM-AV-Policy anti-virus ftp download-profile Avira-AV-Profile
set security utm utm-policy UTM-AV-Policy anti-virus smtp-profile Avira-AV-Profile
set security utm utm-policy UTM-AV-Policy anti-virus pop3-profile Avira-AV-Profile
set security utm utm-policy UTM-AV-Policy anti-virus imap-profile Avira-AV-Profile
set security policies from-zone trust to-zone untrust policy POLICY-1 match source-address any
set security policies from-zone trust to-zone untrust policy POLICY-1 match destination-address any
set security policies from-zone trust to-zone untrust policy POLICY-1 match application any
set security policies from-zone trust to-zone untrust policy POLICY-1 then permit application-services utm-policy
    UTM-AV-Policy
```

**NOTE:** The **[edit security utm feature-profile]** hierarchy level is deprecated in Junos OS Release 18.2R1. For more information, see “UTM Overview” on page 28.

**Step-by-Step Procedure**

To configure the on-device antivirus feature profile using the CLI:

1. Enable Avira antivirus scan on your security device if you have not already enabled..

```
[edit]
user@host# set security utm default-configuration anti-virus type avira-engine
```

   After configuring Avira as the antivirus type, reboot the device for the new scan engine to take effect.

2. Create custom objects.

```
[edit]
user@host# set security utm custom-objects mime-pattern Mime_1 value video/
user@host# set security utm custom-objects mime-pattern Mime_exception value video/x-shockwave-flash
user@host# set security utm custom-objects url-pattern Pattern_List_1 value www.juniper.net
user@host# set security utm custom-objects custom-url-category Cust_URL_Cat value Pattern_List_1
```

3. Create the antivirus profile.

```
[edit]
user@host# set security utm feature-profile anti-virus profile Avira-AV-Profile
```

4. Configure a list of fallback options.

```
[edit]
user@host# set security utm feature-profile anti-virus profile Avira-AV-Profile fallback-options default
   log-and-permit
user@host# set security utm feature-profile anti-virus profile Avira-AV-Profile fallback-options content-size
   block
user@host# set security utm feature-profile anti-virus profile Avira-AV-Profile fallback-options
   engine-not-ready log-and-permit
user@host# set security utm feature-profile anti-virus profile Avira-AV-Profile fallback-options timeout
   log-and-permit
user@host# set security utm feature-profile anti-virus profile Avira-AV-Profile fallback-options
   out-of-resources log-and-permit
user@host# set security utm feature-profile anti-virus profile Avira-AV-Profile fallback-options
   too-many-requests log-and-permit
```

   Fallback options specify the actions to take when traffic cannot be scanned.

5. Configure notification options for fallback blocking actions.

```
[edit]
user@host# set security utm feature-profile anti-virus profile Avira-AV-Profile notification-options
   fallback-block type protocol-only
user@host# set security utm feature-profile anti-virus profile Avira-AV-Profile notification-options
   fallback-block notify-mail-sender
user@host# set security utm feature-profile anti-virus profile Avira-AV-Profile notification-options
   fallback-block custom-message " fallback block action occured “
user@host# set security utm feature-profile anti-virus profile Avira-AV-Profile notification-options
   fallback-block custom-message-subject " Antivirus Fallback Alert "
```

6. Configure the antivirus module to use MIME bypass lists and exception lists.

```
[edit]
user@host# set security utm feature-profile anti-virus profile Avira-AV-Profile mime-whitelist list
   Mime_exception
```

7. Configure the antivirus module to use URL bypass lists. URL allowlists are valid only for HTTP traffic. In this example you use the lists that you set up earlier.

```
[edit]
user@host# set security utm feature-profile anti-virus profile Avira-AV-Profile mime-whitelist list Mime_1
user@host# set security utm feature-profile anti-virus profile Avira-AV-Profile url-whitelist Cust_URL_Cat
```

8. Configure a UTM policy attach the antivirus feature profile Avira-AV-Profile.

```
[edit]
user@host# set security utm utm-policy UTM-AV-Policy anti-virus http-profile Avira-AV-Profile
user@host# set security utm utm-policy UTM-AV-Policy anti-virus ftp upload-profile Avira-AV-Profile
user@host# set security utm utm-policy UTM-AV-Policy anti-virus ftp download-profile Avira-AV-Profile
user@host# set security utm utm-policy UTM-AV-Policy anti-virus smtp-profile Avira-AV-Profile
user@host# set security utm utm-policy UTM-AV-Policy anti-virus pop3-profile Avira-AV-Profile
user@host# set security utm utm-policy UTM-AV-Policy anti-virus imap-profile Avira-AV-Profile
```

9. Configure a security policy and apply the UTM policy UTM-AV-Policy as application services for the permitted traffic.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy POLICY-1 match source-address
   any
```

```
user@host# set security policies from-zone trust to-zone untrust policy POLICY-1 match destination-address
    any
user@host# set security policies from-zone trust to-zone untrust policy POLICY-1 match application any
user@host# set security policies from-zone trust to-zone untrust policy POLICY-1 then permit
    application-services utm-policy UTM-AV-Policy
```

***Results***

From configuration mode, confirm your configuration by entering the **show security utm**, **show services**, and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show security utm
custom-objects {
    mime-pattern {
        Mime_1 {
            value video/;
        }
        Mime_exception {
            value video/x-shockwave-flash;
        }
    }
    url-pattern {
        Pattern_List_1 {
            value www.juniper.net;
        }
    }
    custom-url-category {
        Cust_URL_Cat {
            value Pattern_List_1;
        }
    }
}
feature-profile {
    anti-virus {
        profile Avira-AV-Profile {
            fallback-options {
                default log-and-permit;
                content-size block;
                engine-not-ready log-and-permit;
                timeout log-and-permit;
                out-of-resources log-and-permit;
                too-many-requests log-and-permit;
```

```
        }
        notification-options {
            fallback-block {
                type protocol-only;
                notify-mail-sender;
                custom-message " fallback block action occured ";
                custom-message-subject " Antivirus Fallback Alert ";
            }
        }
        mime-whitelist {
            list Mime_1;
        }
        url-whitelist Cust_URL_Cat;
    }
  }
}
utm-policy P1 {
  anti-virus {
    http-profile junos-av-defaults;
    ftp {
      upload-profile junos-av-defaults;
      download-profile junos-av-defaults;
    }
    smtp-profile junos-av-defaults;
    pop3-profile junos-av-defaults;
    imap-profile junos-av-defaults;
  }
}
utm-policy UTM-AV-Policy {
  anti-virus {
    http-profile Avira-AV-Profile;
    ftp {
      upload-profile Avira-AV-Profile;
      download-profile Avira-AV-Profile;
    }
    smtp-profile Avira-AV-Profile;
    pop3-profile Avira-AV-Profile;
    imap-profile Avira-AV-Profile;
  }
}
```

```
[edit]
user@host# show security policies
  from-zone untrust to-zone trust {
```

```
        policy POLICY-1 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit {
                    application-services {
                        utm-policy UTM-AV-Policy;
                    }
                }
            }
        }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

### Verification

**IN THIS SECTION**



To verify the configuration is working properly, use the following steps:

***Obtaining Information About the Current Antivirus Status***

**Action**

From operational mode, enter the **show security utm anti-virus status** command to view the antivirus status.

## Sample Output

**user@host>show security utm anti-virus status**

```
UTM anti-virus status:
  Update server: https://update.example-juniper.net/avira
           Interval: 360 minutes
           Pattern update status: next update in 236 minutes
           Last result: Downloading certs failed
    Scan engine type: avira-engine
    Scan engine information: 8.3.52.102
    Anti-virus signature version: 8.15.11.42
    Onbox AV load flavor: running heavy, configure heavy
```

**Meaning**

- Antivirus key expire date—The license key expiration date.
- Update server—URL for the data file update server.
  - Interval—The time period, in minutes, when the device will update the data file from the update server.
  - Pattern update status—When the data file will be updated next, displayed in minutes.
  - Last result—Result of the last update.
- Antivirus signature version—Version of the current data file.
- Scan engine type—The antivirus engine type that is currently running.
- Scan engine information—Version of the scan engine.

***Validate Avira Antivirus on Your Security Device***

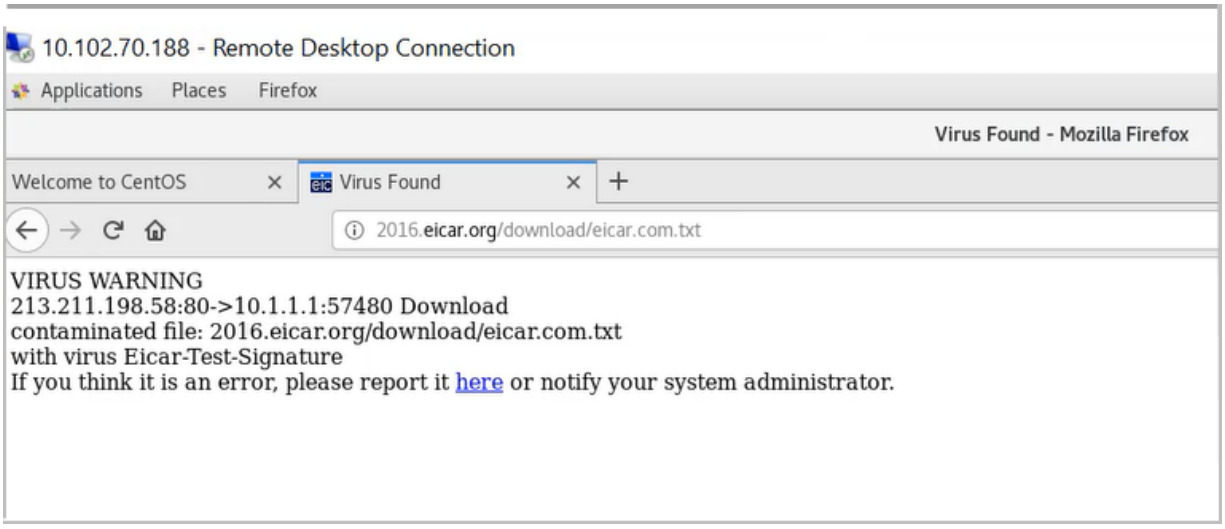
**Purpose**

Validate whether Avira Antivirus Solution is working on SRX Series Device

**Action**

Use the safe way of testing the antivirus capability using Eicar.org website. Your security device displays an error message as shown when you try to download an unsafe file.

Figure 2: Validating Antivirus Solution




**Meaning**

The message indicates that your security device has blocked a malicious content.

RELATED DOCUMENTATION

- Avira Antivirus Solution on SRX Series Devices
- Full Antivirus Scan Results and Fallback Options | 313
- Virus-Detected Notifications | 100
- HTTP Trickling to Prevent Timeouts | 105

# Sophos Antivirus Protection

IN THIS SECTION

The Sophos antivirus scanner uses a local internal cache to maintain query responses from the external list server to improve lookup performance. The Sophos antivirus scanning is offered as a less CPU-intensive alternative to the full file-based antivirus feature. For more information, see the following topics:

## Sophos Antivirus Protection Overview

Sophos antivirus is as an in-the-cloud antivirus solution. The virus pattern and malware database is located on external servers maintained by Sophos (Sophos Extensible List) servers, thus there is no need to download and maintain large pattern databases on the Juniper device. The Sophos antivirus scanner also uses a local internal cache to maintain query responses from the external list server to improve lookup performance.

Because a significant amount of traffic processed by Juniper Unified Threat Management (UTM) is HTTP based, Uniform Resource Identifier (URI) checking is used to effectively prevent malicious content from reaching the endpoint client or server. The following checks are performed for HTTP traffic: URI lookup, true file type detection, and file checksum lookup. The following application layer protocols are supported: HTTP, FTP, SMTP, POP3 and IMAP.

The full file-based antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, sophos antivirus scanning is offered as a less CPU-intensive alternative to the full file-based antivirus feature. Sophos supports the same protocols as full antivirus and functions in much the same manner; however, it has a smaller memory footprint and is compatible with lower end devices that have less memory.

Starting with Junos OS Release 15.1X49-D100, IPv6 pass-through traffic for HTTP, HTTPS, FTP, SMTP, POP3, IMAP protocols is supported for Sophos antivirus, Web filtering and Content filtering security features of UTM.

Starting with Junos OS Release 12.3X48-D35 and Junos OS Release 17.3R1, the UTM Sophos antivirus (SAV) single session throughput is increased for optimizing tcp-proxy forwarding.

Starting from Junos OS Release 19.4R1, the antivirus feature supports implicit and explicit SMTPS, IMAPS, and POP3S protocol, and supports only explicit passive mode FTPS.

*Implicit mode*—Connect to SSL/TLS encrypted port using secure channel.

*Explicit mode*—First connect to unsecured channel, then secure the communication by issuing STARTTLS command. For POP3S, use STLS command.

SEE ALSO

*Understanding TCP Proxy*

*Enabling TCP Proxy Session to Increase the Network Transmit Speed*

Understanding Full Antivirus Scan Mode Support | 299

## Sophos Antivirus Features

Sophos antivirus has the following main features:

- **Sophos antivirus expanded MIME decoding support**—Sophos antivirus offers decoding support for HTTP, POP3, SMTP, and IMAP. MIME decoding support includes the following for each supported protocol:
  - Multipart and nested header decoding
  - Base64 decoding, printed quote decoding, and encoded word decoding in the subject field
- **Sophos antivirus supports HTTPS traffic**—Starting with Junos OS Release 12.3X48-D25 and Junos OS Release 17.3R1, Sophos antivirus over SSL forward proxy supports HTTPS traffic. Sophos antivirus over SSL forward proxy does so by intercepting HTTPS traffic passing through the SRX Series device. The security channel from the SRX Series device is divided as one SSL channel between the client and the SRX Series device and another SSL channel between the SRX Series device and the HTTPS server. SSL forward proxy acts as the terminal for both channels and forwards the cleartext traffic to UTM. UTM extracts the URL and the file checksum information from cleartext traffic. The Sophos antivirus scanner determines whether to block or permit the requests.

  SSL forward proxy does not support client authentication. If client authentication is required by the server, UTM bypasses the traffic. UTM bypasses the HTTPS traffic under the following conditions:
  - If SSL proxy does not parse the first handshake packet from the client, SSL forward proxy bypasses the traffic.
  - If the SSL proxy handshake with the client and server is incomplete because of compatibility issues, connection drops.

  - If the system resource is low, SSL forward proxy cannot handle the new connection and Sophos antivirus bypasses the traffic.
  - If HTTPS traffic hits the allowlist of SSL forward proxy, SSL forward proxy and Sophos antivirus bypass the traffic.

- **Sophos antivirus scan result handling**—With Sophos antivirus, the TCP, traffic is closed gracefully when a virus is found and the data content is dropped.

  The following fail mode options are supported: content-size, default, engine-not-ready, out-of-resource, timeout, and too-many-requests. You can set the following actions: block, log-and-permit, and permit. Fail mode handling of supported options with Sophos is much the same as with full antivirus.

- **Sophos Uniform Resource Identifier checking**—Sophos provides Uniform Resource Identifier (URI) checking, which is similar to antispam realtime blackhole list (RBL) lookups. URI checking is a way of analyzing URI content in HTTP traffic against the Sophos database to identify malware or malicious content. Because malware is predominantly static, a checksum mechanism is used to identify malware to improve performance. Files that are capable of using a checksum include .exe, .zip, .rar, .swf, .pdf, and .ole2 (doc and xls).

  If you have a Juniper Networks device protecting an internal network that has no HTTP traffic, or has webservers that are not accessible to the outside world, you might want to turn off URI checking. If the webservers are not accessible to the outside world, it is unlikely that they contain URI information that is in the Sophos URI database. URI checking is on by default.

  Starting from Junos OS Release 18.4R1 onwards, the URI checking is off by default.

SEE ALSO

Understanding Full Antivirus Content Size Limits | 307
Understanding Full Antivirus Scanning Timeouts | 309

## Understanding Sophos Antivirus Data File Update

Sophos antivirus uses a small set of data files that need to be updated periodically. These data files only contain information on guiding scanning logic and do not contain the full pattern database. The main pattern database, which includes protection against critical viruses, URI checks, malware, worms, Trojans, and spyware, is located on remote Sophos Extensible List servers maintained by Sophos.

The Sophos data files are updated over HTTP or HTTPS and can be updated manually or scheduled to update automatically. With Sophos antivirus:

- The signature database auto-update interval is once a day by default. This interval can be changed.

- There is no interruption in virus scanning capability during the data file update. If the update fails, the existing data files will continue to be used.
- By default, the URL for Sophos antivirus data file update is http://update.juniper-updates.net/SAV/.

> **NOTE:** The Sophos antivirus scanning feature is a separately licensed subscription service. When your antivirus license key expires, functionality will no longer work because the pattern lookup database is located on remote Sophos servers. You have a 30-day grace period in which to update your license.

SEE ALSO

*Licenses Required for UTM Features*

Understanding Antivirus Scanning Fallback Options | 318

## Comparison of Sophos Antivirus to Kaspersky Antivirus

The Kaspersky and Express Antivirus feature is not supported from Junos OS Release 15.1x49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, Sophos Antivirus is much like Juniper Express Antivirus and also has similarities to the Full Antivirus feature:

- Unlike the Juniper Express and Full Antivirus solutions, the antivirus and malware database for Sophos is stored on a group of remote Sophos Extensible List servers. Queries are performed using the DNS protocol. Sophos maintains these servers, so there is no need to download and maintain large pattern databases on the Juniper device. Because the database is remote, and there is a quicker response to new virus outbreaks. The Antivirus database has no size limitation, but there is a limitation with the scan file size.

  > **NOTE:** Sophos antivirus uses a set of data files that need to be updated on a regular basis. These are not typical virus pattern files; they are a set of small files that help guide virus scanning logic. You can manually download the data files or set up automatic download.

- Sophos does not provide the same prescreening detection as Kaspersky Antivirus. Sophos does provide a similar solution that is part of the Sophos engine and cannot be turned on and off.

- The Sophos antivirus scanning feature is a separately licensed subscription service. Also, the pattern lookup database is located on remote servers maintained by Sophos, so when your antivirus license key expires, functionality will no longer work. You have a 30-day grace period in which to update your license.

SEE ALSO

Understanding Full Antivirus Intelligent Prescreening | 305

Example: Configuring Full Antivirus Intelligent Prescreening | 306

## Sophos Antivirus Configuration Overview

Sophos antivirus is part of the Unified Threat Management (UTM) feature set, so you first configure UTM options (custom objects), configure the Sophos Feature, then create a UTM policy and a security policy. The security policy controls all traffic that is forwarded by the device, and the UTM policy specifies which parameters to use to scan traffic. The UTM policy is also used to bind a set of protocols to one or more UTM feature profiles, including Sophos antivirus in this case.

You must complete the following tasks to configure Sophos antivirus:

1. Configure UTM custom objects and MIME lists. See “Example: Configuring Sophos Antivirus Custom Objects” on page 73,
2. Configure the Sophos antivirus feature profile. See “Example: Configuring Sophos Antivirus Feature Profile” on page 77.
3. Configure a UTM policy. See “Example: Configuring Sophos Antivirus UTM Policies” on page 85
4. Configure a security policy. See “Example: Configuring Sophos Antivirus Firewall Security Policies” on page 87.

## Example: Configuring Sophos Antivirus Custom Objects

IN THIS SECTION

This example shows you how to create UTM global custom objects to be used with Sophos antivirus.

## Requirements

Before you begin, read about UTM custom objects. See “UTM Overview” on page 28.

## Overview

Configure MIME lists. This includes creating a MIME allowlist and a MIME exception list for antivirus scanning. In this example, you bypass scanning of QuickTime videos, unless if they contain the MIME type quicktime-inappropriate.

## Configuration

### GUI Step-by-Step Procedure

To configure a MIME list:

1. Click the **Configure** tab from the taskbar, and then select **Security>UTM>Custom Objects**.
2. Click the **MIME Pattern List** tab and then click **Add**.
3. In the MIME Pattern Name box, type **avmime2**.
4. In the MIME Pattern Value box, type **video/quicktime**, and click **Add**.
5. In the MIME Pattern Value box, type **image/x-portable-anympa**, and click **Add**.
6. In the MIME Pattern Value box, type **x-world/x-vrml**, and click **Add**.

To configure a MIME exception list:

1. Click the **Configure** tab from the taskbar, and then select **Security>UTM>Custom Objects**.
2. Click the **MIME Pattern List** tab and then select **Add**.

3. In the MIME Pattern Name box, type **exception-avmime2**.

4. In the MIME Pattern Value box, type **video/quicktime-inappropriate** and click **Add**.

Configure a URL pattern list (allowlist) of URLs or addresses that will be bypassed by antivirus scanning. After you create the URL pattern list, you will create a custom URL category list and add the pattern list to it.

> **NOTE:** Because you use URL pattern lists to create custom URL category lists, you must configure URL pattern list custom objects before you configure custom URL category lists.

To configure a URL pattern allowlist:

1. Click the **Configure** tab from the taskbar, and then select **Security>UTM>Custom Objects**.

2. Click the **URL Pattern List** tab, and then click **Add**.

3. In the URL Pattern Name box, enter **urlist2**.

4. In the URL Pattern Value box, enter **http://example.net**. (You can also us the IP address of the server instead of the URL.)

Save your configuration:

1. Click **OK** to check your configuration and save it as a candidate configuration.

2. If you are done configuring the device, click **Actions>Commit**.

> **NOTE:** URL pattern wildcard support—The wildcard rule is as follows: ***\.[]\?*** and you must precede all wildcard URLs with **http://**. You can use "*****" only if it is at the beginning of the URL and is followed by a "**.**". You can only use "**?**" at the end of the URL.
>
> The following wildcard syntax is supported: **http://*.example.net**, **http://www.example.ne?**, **http://www.example.n??**. The following wildcard syntax is not supported: *.example.net , www.example.ne?, http://*example.net, http://*.

**Step-by-Step Procedure**

To configure antivirus protection using the CLI, you must create your custom objects in the following order:

1. Create the MIME allowlist.

```
[edit security utm]
user@host# set custom-objects mime-pattern avmime2 value [video/quicktime image/x-portable-anymap
   x-world/x-vrml]
```

   Create the MIME exception list.

```
[edit security utm]
user@host# set custom-objects mime-pattern exception-avmime2 value [video/quicktime-inappropriate]
```

2. Configure a URL pattern list (allowlist) of URLs or addresses that you want to bypass. After you create the URL pattern list, you create a custom URL category list and add the pattern list to it. Configure a URL pattern list custom object by creating the list name and adding values to it as follows. As you use URL pattern lists to create custom URL category lists, you must configure URL pattern list custom objects before you configure custom URL category lists.

```
[edit security utm]
user@host# set custom-objects url-pattern urllist2 value [http://www. example.net 192.168.1.5]
```

   **NOTE:** URL pattern wildcard support—The wildcard rule is as follows: ***\.[]\?*** and you must precede all wildcard URLs with **http://**. You can only use "*" if it is at the beginning of the URL and is followed by a "**.**". You can only use "**?**" at the end of the URL.

   The following wildcard syntax is supported: **http://*.example.net**, **http://www.example.ne?**, **http://www.example.n??**. The following wildcard syntax is not supported: *.example.net , www.example.ne?, http://*example.net, http://*.

3. Configure a custom URL category list custom object by using the URL pattern list urllist2 that you created earlier:

```
[edit security utm]
user@host# set custom-objects custom-url-category custurl2 value urllist2
```

### Verification

To verify the configuration, enter the **show security utm custom-objects** command.

SEE ALSO

Understanding URL Allowlist | 52

Configuring URL Allowlist to Bypass Antivirus Scanning (CLI Procedure) | 52

## Example: Configuring Sophos Antivirus Feature Profile

**IN THIS SECTION**



This example shows you how to configure a Sophos antivirus profile that defines the parameters that will be used for virus scanning.

### Requirements

Before you begin:

- Install a Sophos antivirus license. See Installation and Upgrade Guide.
- Configure custom objects for UTM. See "Example: Configuring Sophos Antivirus Custom Objects" on page 73.

### Overview

The following configuration defines Sophos as the antivirus engine and sets parameters, such as the data file update interval, notification options for administrators, fallback options, and file size limits.

NOTE: The **[edit security utm feature-profile]** hierarchy level is deprecated in Junos OS Release 18.2R1. For more information, see "UTM Overview" on page 28.

## Configuration

### GUI Step-by-Step Procedure

The following example shows you how to create a custom Sophos profile. If you want to use the Juniper Networks preconfigured profile, use the profile named junos-sophos-av-defaults in your UTM policy. See "Example: Configuring Sophos Antivirus UTM Policies" on page 85.

1. Select and configure the engine type. Because you are configuring Sophos antivirus, you configure sophos-engine:
   a. Click the **Configure** tab from the taskbar, and then select **Security>UTM>Anti-Virus**.
   b. Click the **Global Options** tab and then click **Sophos**.
   c. Click **OK** and commit your changes.
2. Return to the antivirus Global Options screen as you did in step 1, and set the following parameters:
   a. In the MIME allowlist list, select **exception-avmime2**.
   b. In the URL allowlist list, select **custurl2**.
   c. In the Pattern update interval (sec) box, type **2880**.
   d. In the box, type the e-mail address that will receive SophosAdmin e-mail data file update notifications. For example - admin@ example.net.
   e. In the Custom message subject box, type **Sophos Data File Updated**.
   f. Click **OK** to check your configuration and save it as a candidate configuration.
3. Configure a profile for the sophos-engine and set parameters.
   a. Click the **Configure** tab from the taskbar and then select **Security>UTM>Anti-Virus**. Click **Add**.
   b. In the Add profile box, click the **Main** tab.

c. In the Profile name box, type **sophos-prof1**.

d. In the Trickling timeout box, type **180**.

When enabling the trickling option, it is important to understand that trickling might send part of the file to the client during the antivirus scan. It is possible that some of the content could be received by the client and the client might become infected before the file is fully scanned.

e. URI checking is on by default. To turn it off, clear **yes** in the URI check box.

f. In the Content size Limit box, type **20000**.

g. In the Scan engine timeout box, type **1800**.

4. Configure fallback settings by clicking the **Fallback settings** tab. In this example, all fallback options are set to log and permit. Click **Log and permit** for the following items: Default action, Content size, Engine not ready, Timeout, Out of resource, Too many requests.

5. Configure notification options by clicking the **Notification options** tab. You can configure notifications for both fallback blocking and fallback nonblocking actions and for virus detection.

   To configure notifications for Fallback settings:

   a. For Notification type, click **Protocol**.

   b. For Notify mail sender, click **yes**.

   c. In the Custom message box, type **Fallback block action occurred**.

   d. In the Custom message subject box, type ***Antivirus fallback Alert***.

6. To configure notification options for virus detection, click the **Notification options cont...** tab.

   a. For the Notification type option button, select **Protocol**.

   b. For the Notify mail sender option button, select **yes**.

c. In the Custom message box, type **Virus has been detected**.

d. In the Custom message subject box, type ***Virus detected***.

7. Click **OK** to check your configuration and save it as a candidate configuration.

8. If you are done configuring the device, click **Actions>Commit**.

**Step-by-Step Procedure**

To configure the Sophos antivirus feature profile using the CLI:

The following example shows you how to create a custom Sophos profile. If you want to use the Juniper Networks preconfigured profile, use the profile named junos-sophos-av-defaults in your UTM policy. See "Example: Configuring Sophos Antivirus UTM Policies" on page 85.

1. Select and configure the engine type. Because you are configuring Sophos antivirus, you configure sophos-engine.

```
[edit]
user@host# set security utm default-configuration anti-virus type sophos-engine
```

2. Commit the configuration.

3. Select a time interval for updating the data files. The default antivirus pattern-update interval is 1440 minutes (every 24 hours). You can choose to leave this default, or you can change it. You can also force a manual update, if needed. To change the default from every 24 hours to every 48 hours:

```
[edit security utm default-configuration anti-virus]
user@host# set sophos-engine pattern-update interval 2880
```

4. Configure the network device with the proxy server details, to download the pattern update from a remote server:

```
[edit security utm default-configuration anti-virus]
user@host# set sophos-engine pattern-update proxy
```

5. In most circumstances, you will not need to change the URL to update the pattern database. If you do need to change this option, use the following command:

```
[edit security utm default-configuration anti-virus]
```

```
user@host# set sophos-engine pattern-update url http://www.example.net/test-download
```

6. You can configure the device to notify a specified administrator when data files are updated. This is an e-mail notification with a custom message and a custom subject line.

```
[edit security utm default-configuration anti-virus]
user@host# set sophos-engine pattern-update email-notify admin-email admin@example.net custom-message
    "Sophos antivirus data file was updated" custom-message-subject "AV data file updated"
```

7. Configure a list of fallback options as block, log and permit, or permit. The default setting is log-and-permit. You can use the default settings, or you can change them.

   Configure the content size action. In this example, if the content size is exceeded, the action taken is block.

   First create the profile named sophos-prof1.

```
[edit security utm feature-profile anti-virus]
user@host# set profile sophos-prof1
```

   Configure the content size fallback-option to block.

```
[edit security utm feature-profile anti-virus profile sophos-prof1]
user@host# set fallback-options content-size block
```

   Configure the default fallback option to log-and-permit.

```
[edit security utm feature-profile anti-virus profile sophos-prof1]
user@host# set fallback-options default log-and-permit
```

   Configure log-and-permit if the antivirus engine is not ready.

```
[edit security utm feature-profile anti-virus profile sophos-prof1]
user@host# set fallback-options engine-not-ready log-and-permit
```

   Configure log-and-permit if the device is out of resources.

```
[edit security utm feature-profile anti-virus profile sophos-prof1]
user@host# set fallback-options out-of-resources log-and-permit
```

   Configure log-and-permit if a virus scan timeout occurs.

```
[edit security utm feature-profile anti-virus profile sophos-prof1]
user@host# set fallback-options timeout log-and-permit
```

Configure log-and-permit if there are too many requests for the virus engine to handle.

```
[edit security utm feature-profile anti-virus profile sophos-prof1]
user@host# set fallback-options too-many-requests log-and-permit
```

8. Configure notification options. You can configure notifications for fallback blocking, fallback nonblocking actions, and virus detection.

   In this step, configure a custom message for the fallback blocking action and send a notification for protocol-only actions to the administrator and the sender.

```
[edit security utm feature-profile anti-virus profile sophos-prof1]
user@host# set notification-options fallback-block custom-message ***Fallback block action occurred***
   custom-message-subject Antivirus Fallback Alert notify-mail-sender type protocol-only allow email
   administrator-email admin@example.net
```

9. Configure a notification for protocol-only virus detection, and send a notification.

```
[edit security utm feature-profile anti-virus profile sophos-prof1]
user@host#set notification-options virus-detection type protocol-only notify-mail-sender
   custom-message-subject ***Virus detected*** custom-message Virus has been detected
```

10. Configure content size parameters.

    When you configure the content-size value, keep in mind that in certain cases, content size is available in the protocol headers, so the max-content-size fallback is applied before a scan request is sent. However, in many cases, content size is not provided in the protocol headers. In these cases, the TCP payload is sent to the antivirus scanner and accumulates until the end of the payload. If the accumulated payload exceeds the maximum content size value, then max-content-size fallback is applied. The default fallback action is log and permit, so you may want to change this option to block, in which case such a packet is dropped and a block message is sent to the client.

    In this example, if the content size exceeds 20 MB, the packet is dropped.

```
[edit security utm default-configuration anti-virus]
user@host# set scan-options content-size-limit 20000
```

11. URI checking is on by default. To turn off URI checking:

```
[edit security utm default-configuration anti-virus]
user@host# set scan-options no-uri-check
```

12. Configure the timeout setting for the scanning operation to 1800 seconds.

```
[edit security utm default-configuration anti-virus]
user@host# set scan-options timeout 1800
```

13. The Sophos Extensible List servers contain the virus and malware database for scanning operations. Set the response timeout for these servers to 3 seconds (the default is 2 seconds).

```
[edit security utm default-configuration anti-virus]
user@host# set scan-options sxl-timeout 3
```

14. Configure the Sophos Extensible List server retry option to 2 retries (the default is 1).

```
[edit security utm default-configuration anti-virus]
user@host# set scan-options sxl-retry 2
```

15. Configure the trickling setting to 180 seconds. If you use trickling, you can also set timeout parameters. Trickling applies only to HTTP. HTTP trickling is a mechanism used to prevent the HTTP client or server from timing out during a file transfer or during antivirus scanning.

    When you enable the trickling option, keep in mind that trickling might send part of a file to the client during its antivirus scan. It is therefore possible that some of the content could be received by the client before the file has been fully scanned.

```
[edit security utm default-configuration anti-virus]
user@host# set trickling timeout 180
```

16. Configure the antivirus module to use MIME bypass lists and exception lists. You can use your own custom object lists, or you can use the default list that ships with the device called junos-default-bypass-mime. In this example, you use the lists that you set up earlier.

```
[edit security utm default-configuration anti-virus]
user@host# set mime-whitelist list avmime2
[edit security utm feature-profile anti-virus]
user@host# set mime-whitelist list exception-avmime2
```

17. Configure the antivirus module to use URL bypass lists. If you are using a URL allowlist, this is a custom URL category you have previously configured as a custom object. URL allowlists are valid only for HTTP traffic. In this example you use the lists that you set up earlier.

```
[edit security utm default-configuration anti-virus]
user@host# set url-whitelist custurl2
```

## Verification

### *Obtaining Information About the Current Antivirus Status*

#### Action

From operational mode, enter the **show security utm anti-virus status** command to view the antivirus status.

```
user@host>show security utm anti-virus status
```

#### Meaning

- Antivirus key expire date—The license key expiration date.
- Update server—URL for the data file update server.
  - Interval—The time period, in minutes, when the device will update the data file from the update server.
  - Pattern update status—When the data file will be updated next, displayed in minutes.
  - Last result—Result of the last update. If you already have the latest version, this will display **already have latest database**.
- Antivirus signature version—Version of the current data file.
- Scan engine type—The antivirus engine type that is currently running.
- Scan engine information—Result of the last action that occurred with the current scan engine.

SEE ALSO

Understanding Protocol-Only Virus-Detected Notifications | 101

Example: Configuring Antivirus Scanning Fallback Options | 319

Understanding URL Allowlist | 52

# Example: Configuring Sophos Antivirus UTM Policies

IN THIS SECTION



This example shows how to create a UTM policy for Sophos antivirus.

## Requirements

Before you create the UTM policy, create custom objects and the Sophos feature profile.

1. Configure UTM custom objects and MIME lists. See “Example: Configuring Sophos Antivirus Custom Objects” on page 73.

2. Configure the Sophos antivirus feature profile. See “Example: Configuring Sophos Antivirus Feature Profile” on page 77.

## Overview

After you have created an antivirus feature profile, you configure a UTM policy for an antivirus scanning protocol and attach this policy to a feature profile. In this example, HTTP will be scanned for viruses, as indicated by the **http-profile** statement. You can scan other protocols as well by creating different profiles or adding other protocols to the profile, such as: imap-profile, pop3-profile, and smtp-profile.

## Configuration

### GUI Step-by-Step Procedure

To configure a UTM policy for Sophos antivirus:

1. Click the **Configure** tab from the taskbar, and then select **Security>Policy>UTM Policies**. Then click **Add**.

2. Click the **Main** tab. In the Policy name box, type **utmp3**.

3. Click the **Anti-Virus profiles** tab. In the HTTP profile list, select **sophos-prof1**.

4. Click **OK** to check your configuration and save it as a candidate configuration.

5. If you are done configuring the device, select **Actions>Commit**.

**Step-by-Step Procedure**

To configure a UTM policy for Sophos antivirus:

1. Go to the edit security utm hierarchy.

```
[edit]
user@host# edit security utm
```

2. Create the UTM policy utmp3 and attach it to the http-profile sophos-prof1. You can use the default Sophos feature profile settings by replacing sophos-prof1 in the above statement with junos-sophos-av-defaults.

```
[edit security utm]
user@host# set utm-policy utmp3 anti-virus http-profile sophos-prof1
```

## Verification

To verify the configuration, enter the **show security utm utm-policy utmp3** command.

SEE ALSO

Understanding Full Antivirus Application Protocol Scanning | 324

Understanding HTTP Scanning | 325

Understanding Protocol-Only Virus-Detected Notifications | 101

# Example: Configuring Sophos Antivirus Firewall Security Policies

IN THIS SECTION



This example shows how to create a security policy for Sophos antivirus.

## Requirements

Before you create the security policy, create custom objects, the Sophos feature profile, and the UTM policy.

1. Configure UTM custom objects and MIME lists. See "Example: Configuring Sophos Antivirus Custom Objects" on page 73.

2. Configure the Sophos antivirus feature profile. See "Example: Configuring Sophos Antivirus Feature Profile" on page 77.

3. Configure a UTM policy. See "Example: Configuring Sophos Antivirus UTM Policies" on page 85.

## Overview

Create a firewall security policy that will cause traffic from the untrust zone to the trust zone to be scanned by Sophos antivirus using the feature profile settings defined in "Example: Configuring Sophos Antivirus Feature Profile" on page 77. Because the match application configuration is set to any, all application types will be scanned.

## Configuration

### GUI Step-by-Step Procedure

To configure a security policy for Sophos antivirus:

1. Configure the untrust to trust policy to match any source address or destination address, and select the applications to be scanned to **any**.
   a. Click the **Configure** tab from the taskbar, and then select **Security>Policy>FW Policies**. Then select **Add**.
   b. In the Policy Name box, type **p3**.
   c. In the Policy Action box, select **permit**.
   d. In the From Zone list, select **untrust**.
   e. In the To Zone list, select **trust**.
   f. In the Source Address and Destination Address boxes, make sure that Matched is set to **any**.
   g. In the Applications boxes, select **any** from the Application/Sets list, and move it to the Matched list.
2. Attach the UTM policy named utmp3 to the firewall security policy. This will cause matched traffic to be scanned by the Sophos antivirus feature.
   a. From the Edit Policy box, click the **Application Services** tab.
   b. In the UTM Policy list, select **utmp3**.
3. Click **OK** to check your configuration and save it as a candidate configuration.
4. If you are done configuring the device, select **Actions>Commit**.

**Step-by-Step Procedure**

To configure a security policy for Sophos antivirus:

1. Configure the untrust to trust policy to match any source-address.

```
[edit security]
user@host# set policies from-zone untrust to-zone trust policy p3 match source-address any
```

2. Configure the untrust to trust policy to match any destination-address.

```
[edit security]
```

```
user@host# set policies from-zone untrust to-zone trust policy p3 match destination-address any
```

3. Configure the untrust to trust policy to match any application type.

```
[edit security]
user@host# set policies from-zone untrust to-zone trust policy p3 match application any
```

4. Attach the UTM policy named utmp3 to the firewall security policy. This will cause matched traffic to be scanned by the Sophos antivirus feature.

```
[edit security]
user@host# set policies from-zone untrust to-zone trust policy p3 then permit application-services utm-policy
  utmp3
```

### Verification

To verify the configuration, enter the **show security policies** command.

SEE ALSO

Example: Configuring MIME Allowlist to Bypass Antivirus Scanning | 51

## Example: Configuring Sophos Antivirus Scanner with SSL Forward Proxy

IN THIS SECTION

This example shows how to configure Sophos antivirus over SSL forward proxy to support HTTPS traffic passing through SRX Series devices.

> **NOTE:** Starting with Junos OS Release 12.3X48-D25 and Junos OS Release 17.3R1, Sophos antivirus over SSL forward proxy supports HTTPS traffic.

## Requirements

Before you begin, understand Sophos antivirus features. See "Sophos Antivirus Features" on page 70.

## Overview

In this example, you configure Sophos antivirus over SSL forward proxy to support HTTPS traffic. You load the PKI certificate, generate a self-signed CA certificate, configure a trusted CA list, configure an SSL proxy profile using the root certificate, and enable SSL forward proxy. To configure UTM over SSL forward proxy, first match the source/destination/application, set up the SSL proxy service, and perform scanning to determine whether to block or permit the requests.

> **NOTE:** The **[edit security utm feature-profile]** hierarchy level is deprecated in Junos OS Release 18.2R1. For more information, see "UTM Overview" on page 28.

## Configuration

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **edit** hierarchy level, and then enter **commit** from configuration mode.

```
request security pki generate-key-pair certificate-id ssl-inspect-ca size 2048 type rsa
request security pki local-certificate generate-self-signed certificate-id ssl-inspect-ca domain-name
    www.example.net subject "CN=www.example.net,OU=IT,O=example,L=Sunnyvale,ST=CA,C=US" email
    security-admin@example.net
set security pki ca-profile trusted-ca-example ca-identity trusted-ca-example
request security pki ca-certificate load ca-profile trusted-ca-example filename trusted-ca-example.crt
set services ssl proxy profile ssl-inspect-profile root-ca ssl-inspect-ca
set services ssl proxy profile ssl-inspect-profile trusted-ca trusted-ca-example
```

```
set security policies from-zone untrust to-zone trust policy 1 then permit application-services ssl-proxy
  profile-name ssl-inspect-profile
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Sophos Antivirus over SSL forward proxy:

1. Generate a self-signed CA certificate on the device.

```
user@host> request security pki generate-key-pair certificate-id ssl-inspect-ca size 2048 type rsa
user@host> request security pki local-certificate generate-self-signed certificate-id ssl-inspect-ca
  domain-name www.example.net subject
  "CN=www.example.net,OU=IT,O=example,L=Sunnyvale,ST=CA,C=US" email security-admin@example.net
```

2. Configure a trusted CA list.

```
[edit]
user@host# set security pki ca-profile trusted-ca-example ca-identity trusted-ca-example
```

```
user@host> request security pki ca-certificate load ca-profile trusted-ca-example filename
  trusted-ca-example.crt
```

3. Configure an SSL proxy profile using a root certificate.

```
[edit]
user@host# set services ssl proxy profile ssl-inspect-profile root-ca ssl-inspect-ca
user@host# set services ssl proxy profile ssl-inspect-profile trusted-ca trusted-ca-example
```

4. Enable SSL forward proxy.

```
[edit]
user@host# set security policies from-zone untrust to-zone trust policy 1 then permit application-services
  ssl-proxy profile-name ssl-inspect-profile
```

***Results***

From configuration mode, confirm your configuration by entering the **show security utm**, **show services**, and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security utm
    traceoptions {
        flag all;
    }
    application-proxy {
        traceoptions {
            flag sophos-anti-virus;
        }
    }
    default-configuration {
        anti-virus {
            type sophos-engine;
            scan-options {
                uri-check;
                sxl-timeout 4;
            }
            traceoptions {
                flag all;
            }
                profile profile1 {
                    fallback-options {
                        default log-and-permit;
                        content-size log-and-permit;
                        engine-not-ready log-and-permit;
                        timeout log-and-permit;
                        out-of-resources log-and-permit;
                        too-many-requests log-and-permit;
                    }
                    notification-options {
                        virus-detection {
                            type message;
                        }
                        fallback-block {
                            type message;
                        }
                    }
                }
            }
```

```
        }
    }
    utm-policy policy1 {
        anti-virus {
            http-profile profile1;
        }
    }
[edit]
user@host# show services
    ssl {
        traceoptions {
            file ssl_trace size 1g;
            flag all;
        }
        proxy {
            profile ssl-p {
                root-ca haojue;
                actions {
                    ignore-server-auth-failure;
                }
            }
        }
    }
[edit]
user@host# show security policies
    from-zone trust to-zone untrust {
        policy trust_2_untrust {
            match {
                source-address any;
                destination-address any;
                application [ junos-http junos-https ];
            }
            then {
                permit {
                    application-services {
                        ssl-proxy {
                            profile-name ssl-p;
                        }
                        utm-policy policy1;
                    }
                }
            }
        }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

IN THIS SECTION



To confirm that the configuration is working properly, perform these tasks:

### *Verifying the Security PKI Local Certificate*

**Purpose**

Verify the security PKI local certificate.

**Action**

From configurationl mode, enter the **show security pki local-certificate** command.

```
user@host# show security pki local-certificate
```

```
Certificate identifier: SELF-SIGNED
  Issued to: abc, Issued by: CN = abc
  Validity:
    Not before: 02-20-2015 00:49 UTC
    Not after: 02-19-2020 00:49 UTC
  Public key algorithm: rsaEncryption(2048 bits)

Certificate identifier: ssl-inspect-ca
  Issued to: www.example.net, Issued by: CN = www.example.net, OU = IT, O = example,
 L = Sunnyvale, ST = CA, C = US
  Validity:
    Not before: 01-28-2016 22:28 UTC
    Not after: 01-26-2021 22:28 UTC
  Public key algorithm: rsaEncryption(2048 bits)
```

**Meaning**

The sample output confirms that the PKI local ceritificate ssl-inspect-ca is configured.

***Verifying UTM Antivirus Statistics***

**Purpose**

Verify UTM antivirus statistics.

**Action**

From operational mode, enter the **show security utm anti-virus statistics** command.

```
user@host> show security utm anti-virus statistics
```

```
UTM Anti Virus statistics:

 Intelligent-prescreening passed:      0
 MIME-whitelist passed:                0
 URL-whitelist passed:                 0
 Session abort:                        0
 Scan Request:

  Total           Clean         Threat-found    Fallback
       0               0              0               0

 Fallback:
                             Log-and-Permit    Block             Permit
 Engine not ready:               0                 0                 0
 Out of resources:               0                 0                 0
 Timeout:                        0                 0                 0
 Maximum content size:           0                 0                 0
 Too many requests:              0                 0                 0
 Decompress error:               0                 0                 0
 Others:                         0                 0                 0
```

**Meaning**

The sample output shows the list of UTM antivirus statistics.

***Verifying UTM Antivirus Statistics Details***

**Purpose**

Verify UTM antivirus statistics details.

**Action**

From operational mode, enter the **show security utm anti-virus statistics detail** command.

```
user@host> show security utm anti-virus statistics detail
```

```
HTTP
        MIME-whitelist passed:              0
        URL-whitelist passed:               0

        URI request:
         Total   Clean     Threat-found      Need-further-inspection  Abort
           10          1             1                     8                 0

     File request:
         Total       Clean     Threat-found      Fallback      Abort
               8          6             1               1           0

        Fall back:                  log-and-permit      block      permit
            Engine not ready:             0               0          0
            Out of resources:             0               0          0
            Timeout:                      0               0          0
            Maxmium content size:         1               0          0
            Too many requests:            0               0          0
            Others                        0               0          0

    FTP
        Scan request:
         Total       Clean     Threat-found      Fallback      Abort
               10          8             1               1           0

        Fall back:                  log-and-permit      block      permit
            Engine not ready:             0               0          0
            Out of resources:             0               0          0
            Timeout:                      0               0          0
            Maxmium content size:         1               0          0
            Too many requests:            0               0          0
            Others                        0               0          0

    SMTP
        Scan request:
         Total       Clean     Threat-found      Fallback      Abort
               10          8             1               1           0

        Fall back:                  log-and-permit      block      permit
            Engine not ready:             0               0          0
            Out of resources:             0               0          0
            Timeout:                      0               0          0
            Maxmium content size:         1               0          0
            Too many requests:            0               0          0
```

```
        Others                        0              0          0

POP3
    Scan request:
     Total       Clean     Threat-found      Fallback      Abort
           10          8             1               1           0

    Fall back:                  log-and-permit      block      permit
        Engine not ready:             0               0          0
        Out of resources:             0               0          0
        Timeout:                      0               0          0
        Maxmium content size:         1               0          0
        Too many requests:            0               0          0
        Others                        0               0          0

IMAP
    Scan request:
     Total       Clean     Threat-found      Fallback      Abort
           10          8             1               1           0

    Fall back:                  log-and-permit      block      permit
        Engine not ready:             0               0          0
        Out of resources:             0               0          0
        Timeout:                      0               0          0
        Maxmium content size:         1               0          0
        Too many requests:            0               0          0
        Others                        0               0          0
```

**Meaning**

The sample output shows the list of antivirus statistics details.

***Verifying UTM Antivirus Status***

**Purpose**

Verify UTM antivirus status.

**Action**

From operational mode, enter the **show security utm anti-virus status** command to view the antivirus status.

```
user@host> show security utm anti-virus status
```

```
Anti-virus Key Expiry Date: 07/01/2010 00:00:00
       Update server: http://update.juniper-updates.net//
          Interval: 1440 minutes
          Auto update status: next update in 1440 minutes
          Last result: No error
       Anti-virus data file info:
          Version:
       Scan engine information:
          Last action result: No error(0x00000000)
          Engine type: sophos-engine
```

**Meaning**

- Antivirus key expire date—The license key expiration date.
- Update server—URL for the data file update server.
  - Interval—The time period, in minutes, when the device updates the data file from the update server.
  - Auto update status—Displays the next automatic update of the data file in minutes.
  - Last result—Result of the last database update.
- Antivirus signature version—Version of the current antivirus signature data file.
- Scan engine type—The antivirus scan engine type that is currently running.
- Scan engine information—Result of the last action that occurred with the current scan engine.

SEE ALSO

> *SSL Proxy Overview*

## Managing Sophos Antivirus Data Files

Before you begin:

- Install a Sophos antivirus license. See the *Installation and Upgrade Guide*.
- Configure Sophos as the antivirus feature for the device. See "Example: Configuring Sophos Antivirus Feature Profile" on page 77. To set the antivirus engine type, you run the **set security utm feature-profile anti-virus type sophos-engine** statement.

In this example, you configure the security device to update the data files automatically every 4320 minutes (every 3 days). The default data file update interval is 1440 minutes (every 24 hours).

To automatically update Sophos data files:

```
[edit security utm feature-profile anti-virus]
user@host# set sophos-engine pattern-update interval 4320
```

**NOTE:** The following commands are performed from CLI operational mode.

To manually update data files:

```
user@host> request security utm anti-virus sophos-engine pattern-update
```

To manually reload data files:

```
user@host> request security utm anti-virus sophos-engine pattern-reload
```

To manually delete data files:

```
user@host> request security utm anti-virus sophos-engine pattern-delete
```

To check the status of antivirus, which also shows the data files version:

```
user@host> show security utm anti-virus status
```

To check the status of the proxy server:

```
user@host> show security utm anti-virus status
```

SEE ALSO

*Understanding UTM Licensing*

**Release History Table**

| Release | Description |
|---|---|
| 15.1X49-D100 | Starting with Junos OS Release 15.1X49-D100, IPv6 pass-through traffic for HTTP, HTTPS, FTP, SMTP, POP3, IMAP protocols is supported for Sophos antivirus, Web filtering and Content filtering security features of UTM. |
| 15.1X49-D10 | The full file-based antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Kaspersky and Express Antivirus feature is not supported from Junos OS Release 15.1x49-D10 and Junos OS Release 17.3R1 onwards. |
| 12.3X48-D35 | Starting with Junos OS Release 12.3X48-D35 and Junos OS Release 17.3R1, the UTM Sophos antivirus (SAV) single session throughput is increased for optimizing tcp-proxy forwarding. |
| 12.3X48-D25 | Starting with Junos OS Release 12.3X48-D25 and Junos OS Release 17.3R1, Sophos antivirus over SSL forward proxy supports HTTPS traffic. |
| 12.3X48-D25 | Starting with Junos OS Release 12.3X48-D25 and Junos OS Release 17.3R1, Sophos antivirus over SSL forward proxy supports HTTPS traffic. |

RELATED DOCUMENTATION

Virus-Detected Notifications | **100**

Full Antivirus Protection | **262**

*Licenses Required for UTM Features*

*Enabling TCP Proxy Session to Increase the Network Transmit Speed*

# Virus-Detected Notifications

**IN THIS SECTION**

Virus-Detected notification is used to notify the sender or the recipient about the detected viruses or the scanning errors. For more information, see the following topics:

## Understanding Protocol-Only Virus-Detected Notifications

The Protocol-Only Virus-Detected Notifications are not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, when content is blocked because a virus is found or a scan error occurs, the client generally still receives a successful response code but with modified content (file replacement) containing a warning message. But with protocol-only notifications, a protocol-specific error code may be returned to the client. This way, the client determines that a virus was detected rather than interpreting that a file transfer succeeded.

## Configuring Protocol-Only Virus-Detected Notifications (CLI Procedure)

The Protocol-Only Virus-Detected Notifications are not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, to configure protocol-only virus-detected notifications, use the following CLI configuration statements:

```
security utm feature-profile anti-virus kaspersky-lab-engine profile name {
   notification-options {
      virus-detection {
         type { protocol-only | message }
      }
      fallback-block {
         type { protocol-only | message }
            }
         }
      }
   }
```

**NOTE:** The **[edit security utm feature-profile]** hierarchy level is deprecated in Junos OS Release 18.2R1. For more information, see "UTM Overview" on page 28.

## Understanding E-Mail Virus-Detected Notifications

The E-Mail Virus-Detected Notifications are not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, for mail protocols (SMTP, POP3, IMAP), e-mail notification is used to notify the sender or the recipient about the detected viruses or the scanning errors. There are three settings for e-mail notifications:

- virus-detection/notify-mail-sender — This setting is used when a virus is detected. If it is enabled, an e-mail is sent to the sender upon virus detection.
- fallback-block/notify-mail-sender — This setting is used when other scan codes or scanning errors are returned and the message is dropped. If it is enabled, an e-mail is sent to the sender when an error code is returned.
- fallback-non-block/notify-mail-recipient — This setting is used when other scan codes or scanning errors are returned and the message is passed. If it is enabled, the e-mail sent to the recipient is tagged when an error code is returned.

## Configuring E-Mail Virus-Detected Notifications (CLI Procedure)

The E-Mail Virus-Detected Notifications are not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, to configure the system to send e-mail notifications when viruses are detected, use the following CLI configuration statements:

```
security utm feature-profile anti-virus kaspersky-lab-engine profile name {
    notification-options {
        virus-detection {
            notify-mail-sender
            }
    fallback-block {
        notify-mail-sender
        }
    fallback-non-block {
    notify-mail-recipient
```

```
    }
    }
}
}
```

**NOTE:** The **[edit security utm feature-profile]** hierarchy level is deprecated in Junos OS Release 18.2R1. For more information, see "UTM Overview" on page 28.

## Understanding Custom Message Virus-Detected Notifications

The Custom Message Virus-Detected Notifications are not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file. When using custom messages, you can provide a customized message in the message content you can define customized subject tags.

**NOTE:** Custom-message in fallback-nonblock is used only by mail protocols.

## Configuring Custom Message Virus-Detected Notifications (CLI Procedure)

The Custom Message Virus-Detected Notifications are not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, to configure the system to send custom messages when viruses are detected, use the following CLI configuration statements:

```
security utm feature-profile anti-virus kaspersky-lab-engine profile name {
    notification-options {
        virus-detection {
            custom-message msg
            custom-message-subject subject-msg
        }
    fallback-block {
        custom-message msg
```

```
        custom-message-subject subject-msg
    }
    fallback-non-block {
        custom-message msg
        custom-message-subject subject-msg
        }
        }
    }
}
```

**NOTE:** The **[edit security utm feature-profile]** hierarchy level is deprecated in Junos OS Release 18.2R1. For more information, see "UTM Overview" on page 28.

**Release History Table**

| Release | Description |
|---|---|
| 15.1X49-D10 | The Protocol-Only Virus-Detected Notifications are not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Protocol-Only Virus-Detected Notifications are not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The E-Mail Virus-Detected Notifications are not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The E-Mail Virus-Detected Notifications are not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Custom Message Virus-Detected Notifications are not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Custom Message Virus-Detected Notifications are not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |

RELATED DOCUMENTATION

Full Antivirus Application Protocol Scanning | 323

Full Antivirus Scan Results and Fallback Options | 313

# HTTP Trickling to Prevent Timeouts

IN THIS SECTION



HTTP trickling is a mechanism used to prevent the HTTP client or server from timing-out during a file transfer or during antivirus scanning. For more information, see the following topics:

## Understanding HTTP Trickling

HTTP trickling is a mechanism used to prevent the HTTP client or server from timing-out during a file transfer or during antivirus scanning. On some slow link transferring, a large file could timeout if too much time is taken for the antivirus scanner to scan a complex file.

For Sophos Antivirus, the HTTP trickling is supported from Junos OS Release 10.1R1. Starting from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1, Kaspersky Anitvirus support is discontinued. For Avira Antivirus, the HTTP Trickling is supported from Junos OS Release 18.4R1.

HTTP trickling is the forwarding of specified amounts of unscanned HTTP traffic to the requesting HTTP client to prevent the browser window from timing out while the scan manager examines downloaded HTTP files. (The security device forwards small amounts of data in advance of transferring an entire scanned file.)

HTTP Trickling is time-based and there is only one parameter, the time-out interval, to configure for this feature. By default, trickling is disabled.

The timeout based trickling is packet driven. This means, if no packet is received within a certain time frame, HTTP trickling is discontinued. This setting is only supported for HTTP connections.

## Configuring HTTP Trickling to Prevent Timeouts During Antivirus Scanning (CLI Procedure)

To configure HTTP trickling, use the following CLI configuration statements:

```
security utm feature-profile anti-virus kaspersky-lab-engine {
    profile name {
        trickling timeout seconds;
    }
}
```

**Release History Table**

| Release | Description |
|---|---|
| 18.4R1 | For Avira Antivirus, the HTTP Trickling is supported from Junos OS Release 18.4R1. |
| 15.1X49-D10 | Starting from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1, Kaspersky Anitvirus support is discontinued. |

RELATED DOCUMENTATION

Full Antivirus Application Protocol Scanning | 323

Full Antivirus File Scanning | 297

3
CHAPTER

# Antispam Filtering

# Antispam Filtering Overview

IN THIS SECTION



Antispam filtering allows you to tag or block unwanted e-mail traffic by scanning inbound and outbound SMTP e-mail traffic. Antispam filtering allows you to use both a third-party server-based spam block list (SBL) and to optionally create your own local allowlists and blocklists for filtering against e-mail messages. For more information, see the following topics:

## Antispam Filtering Overview

Spam consists of unwanted e-mail messages, usually sent by commercial, malicious, or fraudulent entities. The antispam feature examines transmitted e-mail messages to identify spam. When the device detects a message deemed to be spam, it blocks the e-mail message or tags the e-mail message header or subject with a preprogrammed string.

Antispam filtering allows you to use both a third-party server-based spam block list (SBL) and to optionally create your own local allowlists (benign) and blocklists (malicious) for filtering against e-mail messages. The antispam feature is not meant to replace your antispam server, but to complement it.

Starting in Junos OS Release 18.2R1, the antispam filtering supports IPv6 traffic.

Starting in Junos OS Release 19.4R1, the antispam filtering supports implicit and explicit SMTPS protocol.

*Implicit mode*—Connect to SSL/TLS encrypted port using secure channel.

*Explicit mode*—First connect to unsecured channel, then secure the communication by issuing STARTTLS command.

### Handling Spam Messages

#### *Blocking Detected Spam*

The device can block and drop detected spam at either the connection level or the e-mail level:

- Blocking spam at the connection level

When the SMTP sender is identified as a spam sender based on its IP address, the SMTP connection is rejected and dropped. An error message with a proper error code from the firewall is sent out on behalf of the SMTP server. An example of such an error message is:

```
554 Transaction failed due to anti spam setting
```

- Blocking spam at the e-mail level

  When a particular e-mail sender is identified as spam sender based on its sender address, the e-mail is rejected and dropped. An error message with a proper error code from the firewall is sent back to the sender on behalf of the server. An example of such an error message is:

```
550 Requested action not taken: mailbox unavailable
```

***Tagging Detected Spam***

The device can allow and tag the e-mail if the message sender is detected as a spammer. This tagging can occur at the connection level so that all the e-mails for the connection in question are tagged. Otherwise, you can tag only an individual e-mail. Two tagging methods are supported:

- Tag the subject: A user-defined string is added at the beginning of the subject of the e-mail.
- Tag the header: A user-defined string is added to the e-mail header.

SEE ALSO

Understanding Server-Based Antispam Filtering | 110

Understanding Local List Antispam Filtering | 120

RELATED DOCUMENTATION

Full Antivirus Application Protocol Scanning | 323

Virus-Detected Notifications | 100

# Server-Based Antispam Filtering

IN THIS SECTION



Server-based spam filtering supports only IP-based spam blocklist lookup. Server-based antispam filtering requires Internet connectivity with the spam block list (SBL) server. For more information, see the following topics:

## Understanding Server-Based Antispam Filtering

Server-based antispam filtering requires Internet connectivity with the spam block list (SBL) server. Domain Name Service (DNS) is required to access the SBL server. The firewall performs SBL lookups through the DNS protocol. The lookups are against the IP address of the sender (or relaying agent) of the e-mail, adding the name of the SBL server as the authoritative domain. The DNS server then forwards each request to the SBL server, which returns a DNS response to the device. The device then interprets the DNS response to determine if the e-mail sender is a spammer.

IP addresses that are included in the block lists are generally considered to be invalid addresses for mail servers or easily compromised addresses. Criteria for listing an IP address as a spammer on the SBL can include:

- Running an SMTP open relay service
- Running open proxy servers (of various kinds)
- Being a zombie host possibly compromised by a virus, worm, Trojan, or spyware
- Using a dynamic IP range
- Being a confirmed spam source with a known IP address

By default, the device first checks incoming e-mail against local allowlists and blocklists. If there are no local lists, or if the sender is not found on local lists, the device proceeds to query the SBL server over the Internet. When both server-based spam filtering and local list spam filtering are enabled, checks are done in the following order:

1. The local allowlist is checked. If there is a match, no further checking is done. If there is no match...
2. The local blocklist is checked. If there is a match, no further checking is done. If there is no match...
3. The SBL server list is checked.

**NOTE:**

- SBL server matching stops when the antispam license key is expired.
- Server-based spam filtering supports only IP-based spam blocklist lookup. Sophos updates and maintains the IP-based spam block list. Server-based antispam filtering is a separately licensed subscription service. When your antispam license key expires, you can continue to use locally defined blocklists and allowlists.

  When you delete or deactivate a feature profile created for server based antispam filtering for SBL server, the default SBL server configuration is applied automatically. When a default SBL server configuration is applied, the default SBL server lookup is enabled. If you want to disable the default SBL server lookup, that is, you want to configure the **no-sbl-default-server** option as a default value, then you must use the **set security utm default-configuration anti-spam sbl no-sbl-default-server** command.

SEE ALSO

Antispam Filtering Overview | 108
Understanding Local List Antispam Filtering | 120

## Server-Based Antispam Filtering Configuration Overview

For each UTM feature, configure feature parameters in the following order:

1. Configure UTM custom objects for the feature:

```
user@host# set security utm custom-objects
```

2. Configure the main feature parameters, using feature profiles.

```
user@host# set security utm feature-profile anti-spam
```

3. Configure a UTM policy for each protocol, and attach this policy to a profile.

```
user@host# set security utm utm-policy utmp1 anti-spam smtp-profile smtp1
```

> **NOTE:** Antispam filtering is only supported for the SMTP protocol.

4. Attach the UTM policy to a security policy.

```
user@host# set security policies from-zone trust to-zone untrust policy p1 then permit application-services
    utm-policy utmp1
```

## Example: Configuring Server-Based Antispam Filtering

**IN THIS SECTION**



This example shows how to configure server-based antispam filtering.

### Requirements

Before you begin, review how to configure the feature parameters for each UTM feature. See “Server-Based Antispam Filtering Configuration Overview” on page 111.

## Overview

Server-based antispam filtering requires Internet connectivity with the spam block list (SBL) server. Domain Name Service (DNS) is required to access the SBL server.

## Configuration

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm feature-profile anti-spam sbl profile sblprofile1 sbl-default-server
set security utm feature-profile anti-spam sbl profile sblprofile1 sbl-default-server spam-action block
set security utm feature-profile anti-spam sbl profile sblprofile1 sbl-default-server custom-tag-string ***spam***
set security utm utm-policy spampolicy1 anti-spam smtp-profile sblprofile1
set security policies from-zone trust to-zone untrust policy utmsecuritypolicy1 match source-address any
set security policies from-zone trust to-zone untrust policy utmsecuritypolicy1 match destination-address any
set security policies from-zone trust to-zone untrust policy utmsecuritypolicy1 match application junos-smtp
set security policies from-zone trust to-zone untrust policy utmsecuritypolicy1 then permit application-services
    utm-policy spampolicy1
```

### GUI Step-by-Step Procedure

To configure server-based antispam filtering:

1. Configure a profile and enable/disable the SBL server lookup. Select **Configure>Security>UTM>Anti-Spam**.

   a. In the Anti-Spam profiles configuration window, click **Add** to configure a profile for the SBL server, or click **Edit** to modify an existing item.

   b. In the Profile name box, enter a unique name for the antispam profile that you are creating.

   c. If you are using the default server, select **Yes** next to Default SBL server. If you are not using the default server, select **No**.

      The SBL server is predefined on the device. The device comes preconfigured with the name and address of the SBL server. If you do not select Yes, you are disabling server-based spam filtering. You should disable it only if you are using only local lists or if you do not have a license for server-based spam filtering.

d. In the Custom tag string box, enter a custom string for identifying a message as spam. By default, the devices uses ***SPAM***.

e. From the antispam action list, select the action that the device should take when it detects spam. Options include Tag subject, Block email, and Tag header.

2. Configure a UTM policy for SMTP to which you attach the antispam profile.

a. Select **Configure>Security>Policy>UTM Policies**.

b. In the UTM policy configuration window, click **Add**.

c. In the policy configuration window, select the **Main** tab.

d. In the Policy name box, type a unique name for the UTM policy.

e. In the Session per client limit box, type a session per client limit. Valid values range from 0 to 2000.

f. From the Session per client over limit list, select the action that the device should take when the session per client limit for this UTM policy is exceeded. Options include Log and permit and Block.

g. Select the **Anti-Spam profiles** tab in the pop-up window.

h. From the SMTP profile list, select an antispam profile to attach to this UTM policy.

3. Attach the UTM policy to a security policy.

a. Select **Configure>Security>Policy>FW Policies**.

b. In the Security Policy window, click **Add** to configure a security policy with UTM or click **Edit** to modify an existing policy.

c. In the Policy tab, type a name in the **Policy Name** box.

d. Next to From Zone, select a zone from the list.

e. Next to To Zone, select a zone from the list.

f. Choose a source address.

g. Choose a destination address.

h. Choose an application by selecting **junos-smtp** (for antispam) in the Application Sets box and move it to the Matched box.

i. Next to Policy Action, select one of the following: **Permit**, **Deny**, or **Reject**.

When you select Permit for Policy Action, several additional fields become available in the Applications Services tab, including UTM Policy.

j. Select the **Application Services** tab.

k. Next to UTM Policy, select the appropriate policy from the list. This attaches your UTM policy to the security policy.

l. Click **OK** to check your configuration and save it as a candidate configuration.

m. If the policy is saved successfully, you receive a confirmation, and you must click **OK** again. If the profile is not saved successfully, click **Details** in the pop-up window to discover why.

> **NOTE:**
> - You must activate your new policy to apply it.
> - In SRX Series devices the confirmation window that notifies you that the policy is saved successfully disappears automatically.

n. If you are done configuring the device, click **Commit Options>Commit**.

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure server-based antispam filtering:

1. Create a profile.

```
[edit security]
user@host# set utm feature-profile anti-spam sbl profile sblprofile1
```

2. Enable or disable the default SBL server lookup.

```
[edit security]
```

```
user@host# set utm feature-profile anti-spam sbl profile sblprofile1 sbl-default-server
```

If you are using server-based antispam filtering, you should type **sbl-default-server** to enable the default SBL server. (The SBL server is predefined on the device. The device comes preconfigured with the name and address of the SBL server.) You should disable server-based antispam filtering using the **no-sbl-default-server** option only if you are using only local lists or if you do not have a license for server-based spam filtering.

3. Configure the action to be taken by the device when spam is detected (block, tag-header, or tag-subject).

```
[edit security]
user@host# set utm feature-profile anti-spam sbl profile sblprofile1sbl-default-server spam-action block
```

4. Configure a custom string for identifying a message as spam.

```
[edit security]
user@host# set utm feature-profile anti-spam sbl profile sblprofile1 sbl-default-server custom-tag-string
   ***spam***
```

5. Attach the spam feature profile to the UTM policy.

```
[edit security]
user@host# set utm utm-policy spampolicy1 anti-spam smtp-profile sblprofile1
```

6. Configure a security policy for UTM to which to attach the UTM policy.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy utmsecuritypolicy1 match
   source-address any
user@host# set security policies from-zone trust to-zone untrust policy utmsecuritypolicy1 match
   destination-address any
user@host# set security policies from-zone trust to-zone untrust policy utmsecuritypolicy1 match application
   junos-smtp
user@host# set security policies from-zone trust to-zone untrust policy utmsecuritypolicy1 then permit
   application-services utm-policy spampolicy1
```

**NOTE:** The device comes preconfigured with a default antispam policy. The policy is called junos-as-defaults. It contains the following configuration parameters:

```
anti-spam {
    sbl {
    profile junos-as-defaults {
        sbl-default-server;
        spam-action block;
    custom-tag-string "***SPAM***";
        }
    }
}
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm** and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security utm
feature-profile {
    anti-spam {
        sbl {
            profile sblprofile1 {
                sbl-default-server;
                spam-action block;
                custom-tag-string ***spam***;
            }
        }
    }
utm-policy spampolicy1 {
    anti-spam {
        smtp-profile sblprofile1;
    }
}
```

```
[edit]
user@host# show security policies
from-zone trust to-zone untrust {
```

```
    policy utmsecuritypolicy1 {
        match {
            source-address any;
            destination-address any;
            application junos-smtp;
        }
        then {
            permit {
                application-services {
                    utm-policy spampolicy1;
                }
            }
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### *Verifying Antispam Statistics*

#### Purpose

Verify the antispam statistics.

#### Action

From operational mode, enter the **show security utm anti-spam status** and **show security utm anti-spam statistics** commands.

The following information appears:

```
SBL Whitelist Server:
SBL Blacklist Server:
msgsecurity.example.net
DNS Server:
Primary : 1.2.3.4, Src Interface: ge-0/0/0
Secondary: 2.3.4.5, Src Interface: ge-0/0/1
Ternary : 0.0.0.0, Src Interface: fe-0/0/2
```

```
Total connections: #
Denied connections: #
Total greetings: #
Denied greetings: #
```

```
Total e-mail scanned: #
White list hit: #
Black list hit: #
Spam total: #
Spam tagged: #
Spam dropped: #
DNS errors: #
Timeout errors: #
Return errors: #
Invalid parameter errors: #
Statistics start time:
Statistics for the last 10 days.
```

SEE ALSO

Understanding Local List Antispam Filtering | 120

spam-action | 577

RELATED DOCUMENTATION

Allowlist | 50

Content Filtering | 131

# Local-List Antispam Filtering

**IN THIS SECTION**



Antispam filtering allows you to use both a third-party server-based spam block list (SBL) and to optionally create your own local allowlists (benign) and blocklists (malicious) for filtering against e-mail messages.

The antispam feature is not meant to replace your antispam server, but to complement it. For more information, see the following topics:

## Understanding Local List Antispam Filtering

When creating your own local allowlist and blocklist for antispam filtering, you can filter against domain names, e-mail addresses, and/or IP addresses. Pattern matching works a bit differently depending upon the type of matching in question. For example, pattern matching for domain names uses a longest suffix match algorithm. If the sender e-mail address has a domain name of aaa.bbb.ccc, the device tries to match "aaa.bbb.ccc" in the list. If no match is found, it tries to match "bbb.ccc", and then "ccc". IP address matching, however, does not allow for partial matches.

Antispam filtering uses local lists for matching in the following manner:

1. Sender IP: The sender IP is checked against the local allowlist, then the local blocklist, and then the SBL IP-based server (if enabled).

2. Sender Domain: The domain name is checked against the local allowlist and then against the local blocklist.

3. Sender E-mail Address: The sender e-mail address is checked against the local allowlist and then against the local blocklist.

By default, the device first checks incoming e-mail against the local allowlist and blocklist. If the sender is not found on either list, the device proceeds to query the SBL server over the Internet. When both server-based antispam filtering and local list antispam filtering are enabled, checks are done in the following order:

1. The local allowlist is checked. If there is a match, no further checking is done. If there is no match...

   Local blocklist and allowlist matching continues after the antispam license key is expired.

2. The local blocklist is checked. If there is a match, no further checking is done. If there is no match...

3. The SBL server list is checked.

SEE ALSO

Antispam Filtering Overview | 108

Understanding Server-Based Antispam Filtering | 110

Server-Based Antispam Filtering Configuration Overview | 111

## Local List Antispam Filtering Configuration Overview

For each UTM feature, configure feature parameters in the following order:

1. Configure UTM custom objects for the feature:

```
user@host# set security utm custom-objects url-pattern url-pattern-name
```

2. Configure the main feature parameters, using feature profiles.

```
user@host# set security utm feature-profile anti-spam as-profile-name
```

3. Configure a UTM policy for each protocol, and attach this policy to a profile.

```
user@host# set security utm utm-policy utmp1 anti-spam smtp-profile smtp1
```

4. Attach the UTM policy to a security policy.

```
user@host# set security policies from-zone trust to-zone untrust policy p1 then permit application-services
    utm-policy utmp1
```

## Example: Configuring Local List Antispam Filtering

IN THIS SECTION

This example shows how to configure local list antispam filtering.

### Requirements

Before you begin, review how to configure the feature parameters for each UTM feature. See “Local List Antispam Filtering Configuration Overview” on page 121.

### Overview

Antispam filtering uses local lists for matching. When creating your own local allowlist and blocklist for antispam filtering, you can filter against domain names, e-mail addresses, and/or IP addresses.

### Configuration

#### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm custom-objects url-pattern as-black value [150.61.8.134]
set security utm custom-objects url-pattern as-white value [150.1.2.3]
set security utm feature-profile anti-spam address-whitelist as-white
set security utm feature-profile anti-spam sbl profile localprofile1
set security utm feature-profile anti-spam sbl profile localprofile1 spam-action block
set security utm feature-profile anti-spam sbl profile localprofile1 custom-tag-string ***spam***
set security utm utm-policy spampolicy2 anti-spam smtp-profile localprofile1
set security policies from-zone trust to-zone untrust policy utmsecuritypolicy2 match source-address any
set security policies from-zone trust to-zone untrust policy utmsecuritypolicy2 match destination-address any
set security policies from-zone trust to-zone untrust policy utmsecuritypolicy2 match application junos-smtp
set security policies from-zone trust to-zone untrust policy utmsecuritypolicy2 then permit application-services
    utm-policy spampolicy2
```

#### GUI Step-by-Step Procedure

To configure local list antispam filtering:

1. Create local allowlist and blocklist custom objects by configuring a URL pattern list.
   a. Select **Configure>Security>UTM>Custom Objects**.
   b. In the UTM custom objects configuration window, select the **URL Pattern List** tab.
   c. Click **Add** to create URL pattern lists.

d. Next to URL Pattern Name, type a unique name.

> **NOTE:** If you are creating a allowlist, it is helpful to indicate this in the list name. The same applies to a blocklist. The name you enter here becomes available in the Address Allowlist and Address Blocklist fields when you are configuring your antispam profiles.

e. Next to URL Pattern Value, type the URL pattern for allowlist or blocklist antispam filtering.

2. Configure antispam filtering to use the allowlist and blocklist custom objects.
   a. Select **Configure>Security>UTM>Global options**.
   b. In the right pane, select the **Anti-Spam** tab.
   c. Under Anti-Spam, select an Address Allowlist and/or an Address Blocklist from the list for local lists for spam filtering. (These lists are configured as custom objects.)
   d. Click **OK**.
   e. If the configuration item is saved successfully, you receive a confirmation, and you must click **OK** again. If it is not saved successfully, click **Details** in the pop-up window to discover why.
   f. In the left pane under Security, select the **Anti-Spam** tab.
   g. Click **Add** to configure an anti-spam profile. The profile configuration pop-up window appears.
   h. In the Profile name box, enter a unique name.
   i. If you are using the default server, select **Yes** beside Default SBL server. If you are not using the default server, select **No**.

      If you select No, you are disabling server-based spam filtering. You disable it only if you are using local lists or if you do not have a license for server-based spam filtering.

j. In the Custom tag string box, type a custom string for identifying a message as spam. By default, the device uses ***SPAM***.

k. In the Actions list, select the action that the device should take when it detects spam. Options include Tag subject, Block email, and Tag header.

3. Configure a UTM policy for SMTP to which you attach the antispam profile.

a. Select **Configure>Security>Policy>UTM Policies**.

b. In the UTM policy configuration window, click **Add** to configure a UTM policy. The policy configuration pop-up window appears.

c. Select the **Main** tab.

d. In the Policy name box, type a unique name.

e. In the Session per client limit box, type a session per client limit. Valid values range from 0 through 2000.

f. From the Session per client over limit list, select the action that the device should take when the session per client limit for this UTM policy is exceeded. Options include Log and permit and Block.

g. Select the **Anti-Spam profiles** tab.

h. From the SMTP profile list, select the antispam profile that you are attaching to this UTM policy.

4. Attach the UTM policy to a security policy.

a. Select **Configure>Security>Policy>FW Policies**.

b. In the Security Policy window, click **Add** to configure a security policy with UTM. The policy configuration pop-up window appears.

c. In the Policy tab, type a name in the Policy Name box.

d. Next to From Zone, select a zone from the list.

e. Next to To Zone, select a zone from the list.

f. Choose a source address.

g. Choose a destination address.

h. Choose an application by selecting **junos-smtp** (for antispam) in the Application Sets box and move it to the Matched box.

i. Next to Policy Action, select one of the following: **Permit**, **Deny**, or **Reject**.

When you select Permit for policy action, several additional fields become available in the Applications Services tab, including UTM Policy.

j. Select the **Application Services** tab.

k. Next to UTM Policy, select the appropriate policy from the list. This attaches your UTM policy to the security policy.

l. Click **OK** to check your configuration and save it as a candidate configuration.

m. If the policy is saved successfully, you receive a confirmation, and you must click **OK** again. If the profile is not saved successfully, click **Details** in the pop-up window to discover why.

> **NOTE:** You must activate your new policy to apply it.

n. If you are done configuring the device, click **Commit Options>Commit**.

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure local list antispam filtering:

1. Configure the local list spam blocking by first creating your global local spam lists.

```
[edit security]
user@host# set utm custom-objects url-pattern as-black value [150.61.8.134]
user@host# set utm custom-objects url-pattern as-white value [150.1.2.3]
```

2. Configure the local list antispam feature profile by first attaching your custom-object blocklist or allowlist or both.

When both the allowlist and the blocklist are in use, the allowlist is checked first. If there is no match, then the blocklist is checked.

```
[edit security]
user@host# set utm feature-profile anti-spam address-whitelist as-white
```

3. Configure a profile for your local list spam blocking.

   Although you are not using the SBL for local list spam blocking, you configure your profile from within that command similar to the server-based spam blocking procedure.

```
[edit security]
user@host# set utm feature-profile anti-spam sbl profile localprofile1
```

4. Configure the action to be taken by the device when spam is detected (block, tag-header, tag-subject).

```
[edit security]
user@host# set utm feature-profile anti-spam sbl profile localprofile1 spam-action block
```

5. Configure a custom string for identifying a message as spam.

```
[edit security]
user@host# set utm feature-profile anti-spam sbl profile localprofile1 custom-tag-string ***spam***
```

6. Attach the spam feature profile to the UTM policy.

```
[edit security]
user@host# set utm utm-policy spampolicy2 anti-spam smtp-profile localprofile1
```

7. Configure a security policy for UTM, and attach the UTM policy to the security policy.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy utmsecuritypolicy2 match
   source-address any
user@host# set security policies from-zone trust to-zone untrust policy utmsecuritypolicy2 match
   destination-address any
user@host# set security policies from-zone trust to-zone untrust policy utmsecuritypolicy2 match application
   junos-smtp
user@host# set security policies from-zone trust to-zone untrust policy utmsecuritypolicy2 then permit
   application-services utm-policy spampolicy2
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm** and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security utm
custom-objects {
    anti-spam {
        url-pattern patternwhite;
        address-whitelist as-white;
        sbl {
            profile localprofile1 {
                spam-action block;
                custom-tag-string ***spam***;
            }
        }
    }
utm-policy spampolicy2 {
    anti-spam {
        smtp-profile localprofile1;
    }
}
```

```
[edit]
user@host# show security policies
from-zone trust to-zone untrust {
    policy utmsecuritypolicy2 {
        match {
            source-address any;
            destination-address any;
            application junos-smtp;
        }
        then {
            permit {
                application-services {
                    utm-policy spampolicy2;
                }
            }
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### *Verifying Antispam Statistics*

#### Purpose

Verify the antispam statistics.

#### Action

From operational mode, enter the **show security utm anti-spam status** and **show security utm anti-spam statistics** commands.

The following information appears:

```
SBL Whitelist Server:
SBL Blacklist Server:
msgsecurity.example.net
DNS Server:
Primary : 1.2.3.4, Src Interface: ge-0/0/0
Secondary: 2.3.4.5, Src Interface: ge-0/0/1
Ternary : 0.0.0.0, Src Interface: fe-0/0/2
```

```
Total connections: #
Denied connections: #
Total greetings: #
Denied greetings: #
Total e-mail scanned: #
White list hit: #
Black list hit: #
Spam total: #
Spam tagged: #
Spam dropped: #
DNS errors: #
Timeout errors: #
Return errors: #
Invalid parameter errors: #
Statistics start time:
Statistics for the last 10 days.
```

SEE ALSO

spam-action | 577

Antispam Filtering Overview | 108

RELATED DOCUMENTATION

Allowlist | 50

4

CHAPTER

# Content Filtering

# Content Filtering

IN THIS SECTION



Content Filtering provides basic data loss prevention functionality. Content filtering filters traffic is based on MIME type, file extension, and protocol commands. You can also use the content filter module to block ActiveX, Java Applets, and other types of content. Content filtering does not require a separate license. For more information, see the following topics:

## Content Filtering Overview

Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, and protocol command. The content filter controls file transfers across the gateway by checking traffic against configured filter lists.

The content filter module evaluates traffic before all other UTM modules, except Web Filtering. Therefore, if traffic meets criteria configured in the content-filter, the content-filter acts first upon this traffic.

You can configure the following types of content filters:

- MIME Pattern Filter — MIME patterns are used to identify the type of traffic in HTTP and MAIL protocols. There are two lists of MIME patterns that are used by the content filter to determine the action to be taken. The block MIME list contains a list of MIME type traffic that is to be blocked by the content filter. The MIME exception list contains MIME patterns that are not to be blocked by the content filter and are generally subsets of items on the block list. Note that the exception list has a higher priority than the block list. If you have MIME entries that appear on both lists, those MIME types are not blocked by

the content filter because the exception list takes priority. Therefore, when adding items to the exception list, it is to your advantage to be specific.

- Block Extension List — Because the name of a file is available during file transfers, using file extensions is a highly practical way to block or allow file transfers. The content filter list contains a list of file extensions to be blocked. All protocols support the use of the block extension list.
- Protocol Command Block and Permit Lists — Different protocols use different commands to communicate between servers and clients. By blocking or allowing certain commands, traffic can be controlled on the protocol command level.

  The block and permit command lists are intended to be used in combination, with the permit list acting as an exception list to the block list.

  If a protocol command appears on the both the permit list and the block list, that command is permitted.

  Starting with Junos OS Release 15.1X49-D100, IPv6 pass-through traffic for HTTP, FTP, SMTP, POP3, IMAP protocols is supported for Web filtering and Content filtering security features of UTM.

Because not all harmful files or components can be controlled by the MIME type or by the file extension, you can also use the content filter module to block ActiveX, Java Applets, and other types of content. The following types of content blocking are supported only for HTTP:

- Block ActiveX
- Block Java applets
- Block cookies
- Block EXE files
- Block ZIP files

SEE ALSO

Understanding MIME Allowlist | 50

## Understanding Content Filtering Protocol Support

**IN THIS SECTION**

Each supported protocol may implement available content filters differently. Not all filtering capabilities are supported for each protocol. This topic contains the following sections:

### HTTP Support

The HTTP protocol supports all content filtering features. With HTTP, the content filter remains in the gateway, checking every request and response between the HTTP client and server.

If an HTTP request is dropped due to content filtering, the client receives a response such as:

```
<custom drop message/user-configured drop message>.<src_port><dst_ip>:<dst_port>Download request was dropped due to <reason>
```

Therefore, a message may appear as follows:

```
Juniper Networks Firewall Content Filtering blocked request. 5.5.5.1:80->4.4.4.1:55247 Download request was dropped due to file extension block list
```

### FTP Support

The FTP protocol does not support all content filtering features. It supports only the following: Block Extension List and Protocol Command Block List.

When content filtering blocks an FTP request, the following response is sent through the control channel:

```
550 <src_ip>:<src_port>-<dst_ip>:<dst_port><custom drop message/user-configured drop message> for Content Filtering file extension block list.>
```

Therefore, a message may appear as follows:

```
550 5.5.5.1:21->4.4.4.1:45237 Requested action not taken and the request is dropped for Content Filtering file extension block list
```

### E-Mail Support

E-mail protocols (SMTP, IMAP, POP3) have limited content filtering support for the following features: Block Extension List, Protocol Command Block List, and MIME Pattern Filtering. Support is limited for e-mail protocols for the following reasons:

- The content filter scans only one level of an e-mail header. Therefore recursive e-mail headers and encrypted attachments are not scanned.

- If an entire e-mail is MIME encoded, the content filter can only scan for the MIME type.
- If any part of an e-mail is blocked due to content filtering, the original e-mail is dropped and replaced by a text file with an explanation for why the e-mail was blocked.

Starting from Junos OS Release 19.4R1, the antivirus and content filtering feature supports implicit and explicit SMTPS, IMAPS, and POP3S protocol, and supports only explicit passive mode FTPS.

*Implicit mode*—Connect to SSL/TLS encrypted port using secure channel.

*Explicit mode*—First connect to unsecured channel, then secure the communication by issuing STARTTLS command. For POP3S, use STLS command.

SEE ALSO

Unified Threat Management Overview | 28

Understanding HTTP Scanning | 325

## Specifying Content Filtering Protocols (CLI Procedure)

To configure content filtering protocols, use the following CLI configuration statements:

```
content-filtering {
    profile name {
        permit-command cmd-list
            block-command cmd-list
        block-extension file-ext-list
            block-mime {
                list mime-list
                exception ex-mime-list
            }
    block-content-type {
        activex
            java-applet
            exe
            zip
        http-cookie
    }
    notification-options {
        type { message }
            notify-mail-sender
        custom-message msg
```

```
    }
  }
  traceoptions {
    flag {
      all
        basic
        detail
      }
    }
  }
```

## Content Filtering Configuration Overview

A content security filter blocks or allows certain type of traffic base on the mime type, file extension, protocol commands and embedded object type. The content filter controls file transfers across the gateway by checking traffic against configured filter lists. The content filtering module evaluates traffic before all other UTM modules, if traffic meets the criteria configured in the content filter, the content filter acts first upon this traffic. The following procedure lists the recommended order in which you should configure content filters:

1. Configure UTM custom objects for the feature. See “Example: Configuring Content Filtering Custom Objects” on page 136.

2. Configure the main feature parameters using feature profiles. See *Example: Configuring Content Filtering Feature Profiles* .

3. Configure a UTM policy for each protocol and attach this policy to a profile. See “Example: Configuring Content Filtering UTM Policies” on page 139.

4. Attach the UTM policy to a security policy. See “Example: Attaching Content Filtering UTM Policies to Security Policies” on page 141.

# Example: Configuring Content Filtering Custom Objects

IN THIS SECTION



This example shows how to configure content filtering custom objects.

## Requirements

Before you begin:

1. Decide on the type of content filter you require. See “Content Filtering Overview” on page 131.

2. Understand the order in which content filtering parameters are configured. See “Content Filtering Configuration Overview” on page 135.

## Overview

In this example, you define custom objects that are used to create content filtering profiles. You perform the following tasks to define custom objects:

1. Create two protocol command lists called ftpprotocom1 and ftpprotocom2, and add user, pass, port, and type commands to it.

2. Create a filename extension list called extlist2, and add the .zip, .js, and .vbs extensions to it.

3. Define block-mime list call cfmime1 and add patterns to the list.

## Configuration

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm custom-objects protocol-command ftpprotocom1 value [user pass port type]
set security utm custom-objects protocol-command ftpprotocom2 value [user pass port type]
set security utm custom-objects filename-extension extlist2 value [zip js vbs]
set security utm custom-objects mime-pattern cfmime1 value [video/quicktime image/x-portable-anymap
    x-world/x-vrml]
set security utm custom-objects mime-pattern ex-cfmime1 value [video/quicktime-inappropriate]
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure content filtering custom objects:

1. Create two protocol command lists.

```
[edit security utm]
user@host# set custom-objects protocol-command ftpprotocom1
[edit security utm]
user@host# set custom-objects protocol-command ftpprotocom2
```

2. Add protocol commands to the list.

```
[edit security utm]
user@host# set custom-objects protocol-command ftpprotocom1 value [user pass port type]
[edit security utm]
user@host# set custom-objects protocol-command ftpprotocom2 value [user pass port type]
```

3. Create a filename extension list.

```
[edit security utm]
user@host# set custom-objects filename-extension extlist2
```

4. Add extensions to the list.

```
[edit security utm]
user@host# set custom-objects filename-extension extlist2 value [zip js vbs]
```

5. Create antivirus scanning lists.

```
[edit security utm]
user@host# set custom-objects mime-pattern cfmime1
user@host# set custom-objects mime-pattern ex-cfmime1
```

6. Add patterns to the lists.

```
[edit security utm]
user@host# set custom-objects mime-pattern cfmime1 value [video/quicktime image/x-portable-anymap
   x-world/x-vrml]
user@host# set custom-objects mime-pattern ex-cfmime1 value [video/quicktime-inappropriate]
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
userhost#show security utm
      custom-objects {
         mime-pattern {
            cfmime1 {
               value [ video/quicktime image/x-portable-anymap x-world/x-vrml ];
            }
            ex-cfmime1 {
               value video/quicktime-inappropriate;
            }
         }
         filename-extension {
            extlist2 {
               value [ zip js vbs ];
            }
         }
         protocol-command {
            ftpprotocom1 {
               value [ user pass port type ];
            }
            }
            protocol-command {
            ftpprotocom2 {
               value [ user pass port type ];
```

```
        }
      }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

### Verification

#### *Verifying Content Filtering Custom Objects*

**Purpose**

Verify the content filtering custom objects.

**Action**

From operational mode, enter the **show configuration security utm** command.

SEE ALSO

Understanding MIME Allowlist | 50

## Example: Configuring Content Filtering UTM Policies

**IN THIS SECTION**



This example describes how to create a content filtering UTM policy to attach to your feature profile.

### Requirements

Before you begin:

1. Decide on the type of content filter you require. See “Content Filtering Overview” on page 131.

2. Configure UTM custom objects for each feature and define the content-filtering profile. See “Content Filtering Configuration Overview” on page 135.

## Overview

You configure UTM policies to selectively enforce various UTM solutions on network traffic passing through a UTM-enabled device. Through feature profiles you associate custom objects to these policies and specify blocking or permitting certain types of traffic.

In this example, you configure a UTM policy called utmp4, and then assign the preconfigured feature profile confilter1 to this policy.

## Configuration

### Step-by-Step Procedure

To configure a content filtering UTM policy:

You can configure different protocol applications in the UTM policy. The example only shows HTTP and not other protocols. Earlier you configured custom objects for FTP (ftpprotocom1 and ftpprotocom2). Next you should add a content filter policy for FTP, for example:

**set security utm utm-policy utmp4 content-filtering ftp upload-profile confilter1**

**set security utm utm-policy utmp4 content-filtering ftp download-profile confilter1**

1. Create a UTM policy.

```
[edit security utm]
user@host# set utm-policy utmp4
```

2. Attach the UTM policy to the profile.

```
[edit security utm]
user@host# set utm-policy utmp4 content-filtering http-profile contentfilter1
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

### Verification

To verify the configuration is working properly, enter the **show security utm** command.

SEE ALSO

Unified Threat Management Overview | 28

## Example: Attaching Content Filtering UTM Policies to Security Policies

IN THIS SECTION



This example shows how to create a security policy and attach the UTM policy to the security policy.

### Requirements

Before you begin:

1. Configure UTM custom objects, define the content filtering profile, and create a UTM policy. See "Content Filtering Configuration Overview" on page 135.

2. Enable and configure a security policy. See *Example: Configuring a Security Policy to Permit or Deny All Traffic*.

### Overview

By attaching content filtering UTM policies to security policies, you can filter traffic transiting from one security zone to another.

In this example, you create a security policy called p4 and specify that traffic from any source address to any destination address with an HTTP application matches the criteria. You then assign a UTM policy

called utmp4 to the security policy p4. This UTM policy applies to any traffic that matches the criteria specified in the security policy p4.

## Configuration

### CLI Quick Configuration

To quickly attach a content filtering UTM policy to a security policy, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
[edit]
set security policies from-zone trust to-zone untrust policy p4 match source-address any
set security policies from-zone trust to-zone untrust policy p4 match destination-address any
set security policies from-zone trust to-zone untrust policy p4 match application junos-htttp
set security from-zone trust to-zone untrust policy p4 then permit application-services utm-policy utmp4
```

### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To attach a UTM policy to a security policy:

1. Create a security policy.

```
[edit]
user@host# edit security policies from-zone trust to-zone untrust policy p4
```

2. Specify the match conditions for the policy.

```
[edit security policies from-zone trust to-zone untrust policy p4]
user@host# set match source-address any
user@host# set match destination-address any
user@host# set match application junos-http
```

3. Attach the UTM policy to the security policy.

```
[edit security policies from-zone trust to-zone untrust policy p4]
user@host# set then permit application-services utm-policy utmp4
```

### Results

From configuration mode, confirm your configuration by entering the **show security policies** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
    from-zone trust to-zone untrust {
        policy p4 {
            match {
                source-address any;
                destination-address any;
                application junos-http;
            }
            then {
                permit {
                    application-services {
                        utm-policy utmp4;
                    }
                }
            }
        }
    }
        default-policy {
            permit-all;
        }
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### *Verifying Attaching Content Filtering UTM Policies to Security Policies*

#### Purpose

Verify the attachment of the content filtering UTM policy to the security policy.

#### Action

From operational mode, enter the **show security policy** command.

SEE ALSO

Unified Threat Management Overview | 28

## Monitoring Content Filtering Configurations

**Purpose**

View content filtering statistics.

**Action**

To view content filtering statistics in the CLI, enter the **user@host > show security utm content-filtering statistics** command.

The content filtering **show statistics** command displays the following information:

```
Base on command list: # Blocked
Base on mime list: # Blocked
Base on extension list: # Blocked
ActiveX plugin: # Blocked
Java applet: # Blocked
EXE files: # Blocked
ZIP files: # Blocked
HTTP cookie: # Blocked
```

To view content filtering statistics using J-Web:

1. Select **Clear Content filtering statisticsMonitor>Security>UTM>Content FilteringMonitor>Security>UTM>Content Filtering**.

   The following statistics become viewable in the right pane.

   ```
   Base on command list: # Passed # Blocked
   Base on mime list: # Passed # Blocked
   Base on extension list: # Passed # Blocked
   ActiveX plugin: # Passed # Blocked
   Java applet: # Passed # Blocked
   EXE files: # Passed # Blocked
   ZIP files: # Passed # Blocked
   HTTP cookie: # Passed # Blocked
   ```

2. You can click **Clear Content filtering statistics** to clear all current viewable statistics and begin collecting new statistics.

**Release History Table**

| Release | Description |
| --- | --- |
| 15.1X49-D100 | Starting with Junos OS Release 15.1X49-D100, IPv6 pass-through traffic for HTTP, FTP, SMTP, POP3, IMAP protocols is supported for Web filtering and Content filtering security features of UTM. |

## RELATED DOCUMENTATION


- Enhanced Web Filtering | **149**
- Full Antivirus Protection | **262**
- Full Antivirus Application Protocol Scanning | **323**

5
CHAPTER

# Web Filtering

# Web Filtering Overview

The Web filtering lets you to manage Internet usage by preventing access to inappropriate Web content. There are four types of Web filtering solutions:

- Redirect Web filtering—The redirect Web filtering solution intercepts HTTP and HTTPS requests and sends them to an external URL filtering server, provided by Websense, to determine whether to block the requests.

  Redirect Web filtering does not require a license.

- Local Web filtering—The local Web filtering solution intercepts every HTTP request and the HTTPS request in a TCP connection. In this case, the decision making is done on the device after it looks up a URL to determine if it is in the allowlist or blocklist based on its user-defined category.

  Local Web filtering does not require a license or a remote category server.

- Enhanced Web filtering—The enhanced Web filtering solution intercepts the HTTP and the HTTPS requests and sends the HTTP URL or the HTTPS source IP to the Websense ThreatSeeker Cloud (TSC). The TSC categorizes the URL into one of the 151 or more categories that are predefined and also provides site reputation information. The TSC further returns the URL category and the site reputation information to the device. The device determines if it can permit or block the request based on the information provided by the TSC.

  Starting in Junos OS Release 17.4R1, Websense redirect support IPv6 traffic.

You can bind either Web filtering profiles or antivirus profiles, or both, to a firewall policy. When both are bound to a firewall policy, Web filtering is applied first, then antivirus is applied. If a URL is blocked by Web filtering, the TCP connection is closed and no antivirus scanning is necessary. If a URL is permitted, the content of the transaction is then passed to the antivirus scanning process.

Web filtering is applied by TCP port number.

Web filtering supports HTTPS protocol. Web filtering solution uses the IP address of the HTTPS packet to make blocklist, allowlist, permit, or block decisions.

During a block decision, the Web filtering solution does not generate a block page because the clear text is not available for a HTTPS session. However, the solution terminates the session and sends resets to the client and the server for the blocked HTTPS sessions.

Web filtering configuration for HTTP is also applicable for the HTTPS sessions.

The **sessions-per-client limit** CLI command, which imposes a session throttle to prevent a malicious user from generating large amounts of traffic simultaneously, does not support Web filtering.

Starting with Junos OS Release 15.1X49-D100, IPv6 pass-through traffic for HTTP, HTTPS, FTP, SMTP, POP3, IMAP protocols is supported for Web filtering and Content filtering security features of UTM.

## Server Name Indication (SNI) Support

SNI is an extension of SSL/TLS protocol to indicate what server name the client is contacting over an HTTPS connection. SNI inserts the actual hostname of the destination server in "Client Hello" message in clear text format before the SSL handshake is complete. Web filtering includes SNI information in the query. In this implementation, the SNI includes only the server name, and not the full URL of the server. Support of SNI enhances the Web filtering feature as using only destination IP address in the query might lead to inaccurate results, because multiple HTTP servers might share the same host IP address.

With SNI support, Web filtering analyzes the first packet of the HTTPS traffic as a "Client Hello" message and extracts the server name from the SNI extension, and uses server name along with the destination IP address to maintain/run the query. If this packet has no SNI extension or if an error is encountered during parsing, Web filtering reverts to using only destination IP address.

In Web Filtering (EWF), if HTTPS session with SSL forward proxy is enabled, then the Server Name Indication (SNI) is obtained before Web filtering and used for pre-check query, site-reputation and category in response. If the cache is enabled, then these responses populates the cache without any action. EWF extracts the full path and checks if there is a cache. If the full path in the cache is not matched, then the EWF sends a query.

The SNI functionality is enabled by default for all types of Web filtering, and therefore, no additional configuration using the CLI is required.

**Release History Table**

| Release | Description |
|---|---|
| 15.1X49-D100 | Starting with Junos OS Release 15.1X49-D100, IPv6 pass-through traffic for HTTP, HTTPS, FTP, SMTP, POP3, IMAP protocols is supported for Web filtering and Content filtering security features of UTM. |

RELATED DOCUMENTATION


- Understanding Integrated Web Filtering | 337
- Understanding Redirect Web Filtering | 208
- Understanding the Enhanced Web Filtering Process | 151
- Understanding Local Web Filtering | 192
- Monitoring Web Filtering Configurations | 230

# Enhanced Web Filtering

IN THIS SECTION



Web Filtering provides URL filtering capability by using either a local Websense server or Internet-based SurfControl server. For more information, see the following topics:

# Enhanced Web Filtering Overview

Enhanced Web Filtering (EWF) with Websense is an integrated URL filtering solution. When you enable the solution on the device, it intercepts the HTTP and the HTTPS requests and sends the HTTP URL or the HTTPS source IP to the Websense ThreatSeeker Cloud (TSC). The TSC categorizes the URL into one of the 95 or more categories that are predefined and also provides site reputation information. The TSC further returns the URL category and the site reputation information to the device. The device determines if it can permit or block the request based on the information provided by the TSC.

Starting in Junos OS Release 15.1X49-D40 and Junos OS Release 17.3R1, EWF supports HTTPS traffic by intercepting HTTPS traffic passing through the SRX Series device. The security channel from the device is divided as one SSL channel between the client and the device and another SSL channel between the device and the HTTPS server. SSL forward proxy acts as the terminal for both channels and forwards the cleartext traffic to the UTM. UTM extracts the URL from the HTTP request message.

You can consider the EWF solution as the next-generation URL filtering solution, building upon the existing Surf-Control solution.

Enhanced Web Filtering supports the following HTTP methods:

- GET
- POST
- OPTIONS
- HEAD
- PUT
- DELETE
- TRACE
- CONNECT

## User Messages and Redirect URLs for Enhanced Web Filtering (EWF)

Starting with Junos OS Release 15.1X49-D110, a new option, **custom-message**, is added for the **custom-objects** command that enables you to configure user messages and redirect URLs to notify users when a URL is blocked or quarantined for each EWF category. The **custom-message** option has the following mandatory attributes:

- **Name**: Name of the custom message; maximum length is 59 bytes.
- **Type**: Type of custom message: **user-message** or **redirect-url**.
- **Content**: Content of the custom message; maximum length is 1024 bytes.

You configure a user message or redirect URL as a custom object and assign the custom object to an EWF category.

- User messages indicate that website access has been blocked by an organization's access policy. To configure a user message, include the **type user-message content *message-text*** statement at the **[edit security utm custom-objects custom-message *message*]** hierarchy level.
- Redirect URLs redirect a blocked or quarantined URL to a user-defined URL. To configure a redirect URL, include the **type redirect-url content redirect-url** statement at the **[edit security utm custom-objects custom-message *message*]** hierarchy level.

The **custom-message** option provides the following benefits:

- You can configure a separate custom message or redirect URL for each EWF category.
- The **custom-message** option allows you to fine-tune messages to support your polices to know which URL is blocked or quarantined.

  Only one **custom-message** configuration option is applied for each category. The **custom-message** configuration is supported only on Enhanced Web Filtering (EWF). Therefore, only the Juniper EWF engine type is supported.

Starting with Junos OS Release 17.4R1, support for custom category configuration is available for local and Websense redirect profiles.

SEE ALSO

Understanding Integrated Web Filtering | 337

Understanding Local Web Filtering | 192

Understanding Redirect Web Filtering | 208

## Understanding the Enhanced Web Filtering Process

Web filtering enables you to manage Internet access, preventing access to inappropriate Web content. The Enhanced Web Filtering (EWF) feature intercepts, scans, and acts upon HTTP or HTTPS traffic in the following way:

1. The device creates TCP socket connections to the Websense ThreatSeeker Cloud (TSC).
2. The device intercepts an HTTP or an HTTPS connection and extracts URL or hostname or IP address to perform Web filtering. For an HTTPS connection, EWF is supported through SSL forward proxy.

   Starting with Junos OS Release 12.3X48-D25 and Junos OS Release 17.3R1, Enhanced Web Filtering (EWF) over SSL forward proxy supports HTTPS traffic.

3. The device looks for the URL in the user-configured blocklist or allowlist.

   A blocklist or a allowlist action type is a user-defined category in which all the URLs or IP addresses are always blocked or permitted and optionally logged.

   - If the URL is in the user-configured blocklist, the device blocks the URL.
   - If the URL is in the user-configured allowlist, the device permits the URL.

4. The device checks the user-defined categories and blocks or permits the URL based on the user-specified action for the category.
5. The device looks for predefiend category in local cache or from cloud service.
   - If the URL is not available in the URL filtering cache, the device sends the URL in HTTP format to the TSC with a request for categorization. The device uses one of the connections made available to the TSC to send the request.
   - The TSC responds to the device with the categorization and a reputation score.
6. The device performs the following actions based on the identified category:
   - If the URL is permitted, the device forwards the HTTP request to the HTTP server.
   - If the URL is blocked, the device sends a deny page to the HTTP client and also sends a reset message to the HTTP server to close the connection
   - If the URL is quarantined, the device sends a quarantine page with set-cookie to the HTTP client. If the client decided to continue, the device permits new request with cookie.
   - If the category is configured and the category action is available, the device permits or blocks the URL based on the category action.
   - If the category is not configured, the device permits or blocks the URL based on the global reputation action.
   - If the global reputation is not configured, the device permits or blocks the URL based on the default action configured in the Web filtering profile.

   By default, the EWF processes a URL in the order of blocklist, allowlist, custom category, and then predefined category.

### Functional Requirements for Enhanced Web Filtering

The following items are required to use Enhanced Web Filtering (EWF):

- **License key**— You need to install a new license to upgrade to the EWF solution.

  You can ignore the warning message "requires 'wf_key_websense_ewf' license" because it is generated by routine EWF license validation check.

  A grace period of 30 days, consistent with other UTM features, is provided for the EWF feature after the license key expires.

  This feature requires a license. To understand more about UTM Licensing, see, Understanding UTM Licensing. Please refer to the Licensing Guide for general information about License Management. Please refer to the product Data Sheets at SRX Series Services Gateways for details, or contact your Juniper Account Team or Juniper Partner.

  When the grace period for the EWF feature has passed (or if the feature has not been installed), Web filtering is disabled, all HTTP requests bypass Web filtering, and any connections to the TSC are disabled. When you install a valid license, the connections to the server are established again.

- The **debug** command provides the following information to each TCP connection available on the device:

  - Number of processed requests
  - Number of pending requests
  - Number of errors (dropped or timed-out requests)

- **TCP connection between a Web client and a webserver**—An application identification (APPID) module is used to identify an HTTP connection. The EWF solution identifies an HTTP connection after the device receives the first SYN packet. If an HTTP request has to be blocked, EWF sends a block message from the device to the Web client. EWF further sends a TCP FIN request to the client and a TCP reset (RST) to the server to disable the connection. The device sends all the messages through the flow session. The messages follow the entire service chain.

- **HTTP request interception**—EWF intercepts the first HTTP request on the device and performs URL filtering on all methods defined in HTTP 1.0 and HTTP 1.1. The device holds the original request while waiting for a response from the TSC. If the first packet in the HTTP URL is fragmented or if the device cannot extract the URL for some reason, then the destination IP address is used for the categorization. If you turn on **http-reassemble**, EWF can recover the whole request from fragment and get URL.

  For HTTP 1.1 persistent connections, the subsequent requests on that session are ignored by the EWF module.

  If the device holds the original request for a long time, then the client will retransmit the request. The URL filtering code will detect the retransmitted packets. If the original HTTP request has already been forwarded, then EWF forwards the retransmitted packet to the server. However, if EWF is in the middle of first-packet processing or makes the calculation to block the session, then the solution drops the retransmitted packet. A counter tracks the number of retransmitted packets received by the device.

  If the TSC does not respond in time to the categorization request from the device, then the original client request is blocked or permitted according to the timeout fallback setting.

- **HTTPS request interception**—Starting with Junos OS 15.1X49-D40 and Junos OS Release 17.3R1, EWF intercepts HTTPS traffic passing through the SRX Series device. The security channel from the device is divided as one SSL channel between the client and the device and another SSL channel between the device and the HTTPS server. SSL forward proxy acts as the terminal for both channels and forwards the cleartext traffic to the UTM. UTM extracts the URL from the HTTP request message.
- **Blocking message**—The blocking message sent to the Web client is user-configurable and is of the following types:
  - The Juniper Networks blocking message is the default message defined in the device that can be modified by the user. The default blocking message contains the reason why the request is blocked and the category name (if it is blocked because of a category).
  - Syslog message.

  For example, if you have set the action for Enhanced_Search_Engines_and_Portals to block, and you try to access www.example.com, the blocking message is of the following form: **Juniper Web Filtering:Juniper Web Filtering has been set to block this site. CATEGORY: Enhanced_Search_Engines_and_Portals REASON: BY_PRE_DEFINED** . However, the corresponding syslog message on the device under test (DUT) is: **WEBFILTER_URL_BLOCKED: WebFilter: ACTION="URL Blocked" 56.56.56.2(59418)->74.125.224.48(80) CATEGORY="Enhanced_Search_Engines_and_Portals" REASON="by predefined category" PROFILE="web-ewf" URL=www.example.com OBJ=/** .
- **Monitoring the Websense server**—The URL filtering module uses two methods to determine if the TSC is active: socket connections and heartbeat. EWF maintains persistent TCP sockets to the TSC. The server responds with a TCP ACK if it is enabled. EWF sends an application layer NOOP keepalive to the TSC. If the device does not receive responses to three consecutive NOOP keepalives in a specific period, it determines the socket to be inactive. The EWF module attempts to open a new connection to the TSC. If all sockets are inactive, the TSC is considered to be inactive. Therefore an error occurs. The error is displayed and logged. Subsequent requests and pending requests are either blocked or passed according to the server connectivity fallback setting until new connections to the TSC are opened again.
- **HTTP protocol communication with the TSC**—EWF uses the HTTP 1.1 protocol to communicate with the TSC. This ensures a persistent connection and transmission of multiple HTTP requests through the same connection. A single HTTP request or response is used for client or server communication. The TSC can handle queued requests; for optimal performance, an asynchronous request or response mechanism is used. The requests are sent over TCP, so TCP retransmission is used to ensure request or response delivery. TCP also ensures that valid in-order, non-retransmitted HTTP stream data is sent to the HTTP client on the device.
- **Responses**—The responses adhere to the basic HTTP conventions. Successful responses include a 20x response code (typically 200). An error response includes a 4xx or 5xx code. Error responses in the 4xx series indicate issues in the custom code. Error responses in the 5xx series indicate issues with the service.

Error codes and meanings are as follows:

- 400–Bad request
- 403–Forbidden
- 404–Not found
- 408–Request canceled or null response
- 500–Internal server error

Errors in the 400 series indicate issues with the request. Errors in the 500 series indicate issues with the TSC service. Websense is notified of these errors automatically and responds accordingly.

You can configure the default fallback setting to determine whether to pass or block the request: **set security utm feature-profile web-filtering juniper-enhanced profile juniper-enhanced fallback-settings default ?**

The response also contains the site categorization and site reputation information.

- **Categories**—A category list is available on the device. This list consists of categories, each containing a category code, a name, and a parent ID. Categories can also be user-defined. Each category consists of a list of URLs or IP addresses. Categories are not updated dynamically and are tied to the Junos OS release because they have to be compiled into the Junos OS image. Any update in categories needs to be synchronized with the Junos OS release cycle.

  Starting with Junos OS Release 17.4R1, you can download and dynamically load new EWF categories. The downloading and dynamic loading of the new EWF categories do not require a software upgrade. Websense occasionally releases new EWF categories. EWF classifies websites into categories according to host, URL, or IP address and performs filtering based on the categories.

  If the category file transfer fails between the primary and secondary devices, then the file transfer results in an upgrading error and an error log is generated.

  During new category file installation, if the category filename is changed, then the new category file overwrites the old category file in the internal system and all related output information is replaced with the new category name.

  Starting with Junos OS Release 17.4R1, predefined base filters, defined in a category file, are supported for individual EWF categories. Each EWF category has a default action in a base filter, which is attached to the user profile to act as a backup filter. If the categories are not configured in the user profile, then the base filter takes the action.

  A base filter is an object that contains a category-action pair for all categories defined in the category file. A base filter is a structured object, and is defined with the help of a filter name and an array of category-action pairs.

  The following is an example of a base filter with an array of category-action pairs. For the Enhanced_Adult_Material category, the action is block; for the Enhanced_Blog_Posting category, the action is permit; and so on.

```
{
"predefined-filter": [
        {
            "filter-name": "ewf-default-filter",
            "cat-action-table": [
                {"name":"Enhanced_Adult_Material","action":"block"},

{"name":"Enhanced_Blog_Posting","action":"permit"},
                {"name":"Enhanced_Blog_Commenting","action":"permit"}
            ]
        }
    ]
}
```

EWF supports up to 16 base filters. Junos OS Release 17.4R1 also supports online upgradation of base filters.

If the user profile has the same name as the base filter, then the Web filter uses the wrong profile.

- **Caching**—Successfully categorized responses are cached on the device. Uncategorized URLs are not cached. The size of the cache can be configured by the user.
- **Safe search (HTTP support only, not HTTPS)**—A safe-search solution is used to ensure that the embedded objects, such as images on the URLs received from the search engines, are safe and that no undesirable content is returned to the client.

  A URL is provided to the TSC to provide categorization information. If it is a search URL, the TSC also returns a safe-search string. For instance, the safe-search string is **safe=active**. This safe-search string is appended to the URL, and a redirect response for redirecting the client's query with safe search is turned on. This ensures that no unsafe content is returned to the client. If the TSC indicates that it needs to be safe-searched, then you can perform the safe-search redirect.

  For example, the client makes a request to the URL https://www.google.com/search?q=test, which is permitted by EWF profile. On packet mode, the EWF on the DUT will generate a HTTP 302 response, with the redirect URL: https://www.google.com/search?q=test&safe=active. This response returns to the client. The client now sends out a safe redirect request to this URL. On stream mode, the EWF on the DUT rewrites the URL to https://www.google.com/search?q=test&safe=active and forwards it.

  **NOTE:** Safe-search redirect supports HTTP only. You cannot extract the URL for HTTPS. Therefore it is not possible to generate a redirect response for HTTPS search URLs. Safe-search redirects can be disabled by using the CLI option **no-safe-search**.

- **Site reputation**—The TSC provides site reputation information. Based on these reputations, you can choose a block or a permit action. If the URL is not handled by a allowlist or a blocklist and does not fall in a user or predefined category, then the reputation can be used to perform a URL filtering decision.

  Starting with Junos OS Release 17.4R1, the reputation base scores are configurable. Users can apply global reputation values, provided by the Websense ThreatSeeker Cloud (TSC). For the non-category URLs, the global reputation value is used to perform filtering,

  The reputation scores are as follows:

  - 100-90–Site is considered very safe.
  - 80-89–Site is considered moderately safe.
  - 70-79–Site is considered fairly safe.
  - 60-69–Site is considered suspicious.
  - 0-59–Site is considered harmful.

  The device maintains a log for URLs that are blocked or permitted based on site reputation scores.

- **Profiles**—A URL filtering profile is defined as a list of categories, with each profile having an action type (permit, log-and-permit, block, quarantine) associated with it. A predefined profile, *junos-wf-enhanced-default*, is provided to users if they choose not to define their own profile.

  You can also define an action based on site reputations in a profile to specify the action when the incoming URL does not belong to any of the categories defined in the profile. If you do not configure the site reputation handling information, then you can define a default action. All URLs that do not have a defined category or defined reputation action in their profile will be blocked, permitted, logged-and-permitted, or quarantined depending on the block or permit handling for the default action explicitly defined in the profile. If you do not specify a default action, then the URLs will be permitted. For search engine requests, if there is no explicit user-defined configuration, and the URL request is without the safe-search option, then EWF generates a redirect response and sends it to the client. The client will generate a new search request with the safe-search option enabled.

  A URL filtering profile can contain the following items:

  - Multiple user-defined and predefined categories, each with a permit or block action
  - Multiple site reputation handling categories, each with a permit or block action
  - One default action with a permit or block action

  The order of search is blocklist, allowlist, user-defined category, predefined category, safe-search, site reputation, and default action.

### User Messages and Redirect URLs for Enhanced Web Filtering (EWF)

Starting with Junos OS Release 15.1X49-D110, a new option, **custom-message**, is added for the **custom-objects** statement that enables you to configure user messages and redirect URLs to notify users

when a URL is blocked or quarantined for each EWF category. The **custom-message** option has the following mandatory attributes:

- **Name**: Name of the custom message; maximum length is 59 ASCII characters.
- **Type**: Type of custom message: **user-message** or **redirect-url**.
- **Content**: Content of the custom message; maximum length is 1024 ASCII characters.

You configure a user message or redirect URL as a custom object and assign the custom object to an EWF category.

- User messages indicate that website access has been blocked by an organization's access policy. To configure a user message, include the **type user-message content *message-text*** statement at the **[edit security utm custom-objects custom-message *message*]** hierarchy level.
- Redirect URLs redirect a blocked or quarantined URL to a user-defined URL. To configure a redirect URL, include the **type redirect-url content redirect-url** statement at the **[edit security utm custom-objects custom-message *message*]** hierarchy level.

The **custom-message** option provides the following benefits:

- You can configure a separate custom message or redirect URL for each EWF category.
- The **custom-message** option allows you to fine-tune messages to support your polices to know which URL is blocked or quarantined.

  Only one **custom-message** configuration option is applied for each category. The **custom-message** configuration is supported only on Enhanced Web Filtering (EWF). Therefore, only the Juniper EWF engine type is supported.

Starting with Junos OS Release 17.4R1, support for custom category configuration is available for local and Websense redirect profiles.

SEE ALSO

Web Filtering Overview | 147

## Predefined Category Upgrading and Base Filter Configuration Overview

You can download and dynamically load new Enhanced Web Filtering (EWF) categories without any software upgrade. The predefined base filters defined in a category file are supported for individual EWF categories.

To configure a predefined category upgrade without any software upgrade:

1. Configure UTM custom objects for the UTM features. Set the interval, set the start time, and enter the URL of category package download:

```
user@host# set security utm custom-objects
user@host# set security utm custom-objects category-package
user@host# set security utm custom-objects category-package automatic
user@host# set security utm custom-objects category-package automatic interval 60
user@host# set security utm custom-objects category-package automatic interval 60 enable
user@host# set security utm custom-objects category-package automatic interval 60 enable start-time
   2017-09-05.08.08.08
user@host# set security utm custom-objects category-package automatic route-instance VRF
user@host# set security utm custom-objects category-package automatic route-instance VRF url
   https://update.juniper-updates.net/EWF
```

2. Configure the predefined base filters. Each EWF category has a default action in a base filter, which is attached to the user profile to act as a backup filter. If the categories are not configured in the user profile, then the base filter takes the action. You can also upgrade the base filters online.

```
user@host# set security utm feature-profile web-filtering juniper-enhanced juniper-enhanced-profile
user@host# set security utm feature-profile web-filtering juniper-enhanced juniper-enhanced-profile
   base-filter [base-filter]
user@host# set security utm feature-profile web-filtering juniper-enhanced juniper-enhanced-profile
   base-filter [base-filter] category <category-action >
user@host# set security utm feature-profile web-filtering juniper-enhanced juniper-enhanced-profile
   base-filter [base-filter] category category-action default <default-action>
user@host# set security utm feature-profile web-filtering juniper-enhanced juniper-enhanced-profile
   base-filter [base-filter] category category-action default <default-action>site-reputation-action
   <reputation-action>
```

**show security utm custom-objects**

```
category-package{
automatic{
 interval 60;
```

```
 enable;
 start-time "2017-09-05.08.08.08";
 }
route-instance VRF;
url https://update.juniper-updates.net/EWF;
}
```

**show security utm feature-profile web-filtering juniper-enhanced**

```
server {
    host rp.cloud.threatseeker.com;
}
sockets 8;
profile ewf_p1 {
+ base-filter gov-filter;
default log-and-permit;
    timeout 15;
}
+reputation {
 reputation-very-safe 90;
 reputation-moderately-safe 80;
 reputation-fairly-safe 70;
 reputation-suspicious 60;
}
```

SEE ALSO

- show security utm web-filtering category status | **732**
- category (Security Web Filtering) | **388**
- request security utm web-filtering category install | **675**
- show security utm web-filtering category base-filter | **727**

# Example: Configuring Enhanced Web Filtering

IN THIS SECTION



This example shows how to configure Enhanced Web filtering (EWF) for managing website access. This feature is supported on all SRX Series devices. The EWF solution intercepts HTTP and the HTTPS requests and sends the HTTP URL or the HTTPS source IP to the Websense ThreatSeeker Cloud (TSC). The TSC categorizes the URL into one of the 151 or more predefined categories and also provides site reputation information. The TSC further returns the URL category and the site reputation information to the device. The SRX Series device determines whether it can permit or block the request based on the information provided by the TSC.

## Requirements

This example uses the following hardware and software components:

- SRX5600 device
- Junos OS Release 12.1X46-D10 or later

Before you begin, you should be familiar with Web filtering and Enhanced Web filtering (EWF). See "Web Filtering Overview" on page 147 and "Understanding the Enhanced Web Filtering Process" on page 151.

## Overview

Web filtering is used to monitor and control how users access the website over HTTP and HTTPS. In this example, you configure a URL pattern list (allowlist) of URLs or addresses that you want to bypass. After you create the URL pattern list, define the custom objects. After defining the custom objects, you apply them to feature profiles to define the activity on each profile, apply the feature profile to the UTM policy, and finally attach the Web filtering UTM policies to the security policies. Table 5 on page 162 shows information about EWF configuration type, steps, and parameters used in this example.

**Table 5: Enhanced Web filtering (EWF) Configuration Type, Steps, and Parameters**

| Configuration Type | Configuration Steps | Configuration Parameters |
|---|---|---|
| **URL pattern and custom objects** | Configure a URL pattern list (allowlist) of URLs or addresses that you want to bypass.<br><br>Create a custom object called urllist3 that contains the pattern http://www.example.net 1.2.3.4 | • [http://www.example.net 1.2.3.4]<br>• value urllist3<br>• http://www.untrusted.com<br>• http://www.trusted.com |
| | Add the urllist3 custom object to the custom URL category custurl3. | • **urllistblack**<br>• **urllistwhite** |

**Table 5: Enhanced Web filtering (EWF) Configuration Type, Steps, and Parameters *(continued)***

| Configuration Type | Configuration Steps | Configuration Parameters |
|---|---|---|
| **Feature profiles** | Configure the Web filtering feature profile: | |
| | • Set the URL blocklist filtering category to **custblacklist**, set the allowlist filtering category to **custwhitelist**, and set the type of Web filtering engine to **juniper-enhanced**. Then you set the cache size and cache timeout parameters. | • **custwhitelist**<br>• **custblacklist**<br>• **type juniper-enhanced**<br>• **cache size 500**<br>• **cache timeout 1800** |
| | • Name the EWF server and enter the port number for communicating with it. (Default port is 80.) Then you create an EWF profile name. | • **rp.cloud.threatseeker.com**<br>• **port 80**<br>• **http-profile my_ewfprofile01** |
| | • Select a category from the included allowlist and blocklist categories or select a custom URL category list you created for filtering against. | • **http-reassemble**<br>• **http-persist**<br>• **Action: log-and-permit**<br>• **site-reputation-action:**<br>  ◦ **very-safe permit** |
| | • Enter a custom message to be sent when HTTP requests are blocked. Finally, enter a timeout value in seconds. | • **ewf_my_profile-default block**<br>• **custom-block-message "***access denied ***"**<br>• **fallback-settings:**<br>  ◦ **server-connectivity block**<br>  ◦ **timeout block**<br>  ◦ **too-many-requests block**<br>• **quarantine-custom-message “**The requested webpage is blocked by your organization's access policy**”.**<br>• **quarantine-message type custom-redirect-url**<br>• **quarantine-message url besgas.spglab.example.net**<br>• **ewf_my_profile-default:**<br>  ◦ **timeout 10**<br>  ◦ **no-safe-search** |

## Configuration

IN THIS SECTION



This example shows how to configure custom URL patterns, custom objects, feature profiles, and security policies.

***Configuring Enhanced Web Filtering Custom Objects and URL Patterns***

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm custom-objects url-pattern urllist3 value http://www.example.net
set security utm custom-objects url-pattern urllist3 value 1.2.3.4
set security utm custom-objects url-pattern urllistblack value http://www.untrusted.com
set security utm custom-objects url-pattern urllistblack value 13.13.13.13
set security utm custom-objects url-pattern urllistwhite value http://www.trusted.com
set security utm custom-objects url-pattern urllistwhite value 11.11.11.11
set security utm custom-objects custom-url-category custurl3 value urllist3
set security utm custom-objects custom-url-category custblacklist value urllistblack
set security utm custom-objects custom-url-category custwhiltelist value urllistwhite
```

Starting with Junos OS Release 15.1X49-D110, the "* " in a wildcard syntax, required to create URL pattern for Web filtering profile, matches all subdomains.  For example, *.example.net matches:

- http://a.example.net
- http://example.net
- a.b.example.net

A custom category does not take precedence over a predefined category when it has the same name as one of the predefined categories. Do not use the same name for a custom category that you have used for a predefined category.

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure custom objects and URL patterns in Enhanced Web Filtering:

1. Configure a URL pattern list (allowlist) of URLs or addresses that you want to bypass. After you create the URL pattern list, you create a custom URL category list and add the pattern list to it. Configure a URL pattern list custom object by creating the list name and adding values to it as follows:

   **NOTE:** Because you use URL pattern lists to create custom URL category lists, you must configure URL pattern list custom objects before you configure custom URL category lists.

   ```
   [edit security utm]
   user@host# set custom-objects url-pattern urllist3 value [http://www. example.net 1.2.3.4]
   ```

   **NOTE:** The guideline to use a URL pattern wildcard is as follows: Use ***\.[]\?*** and precede all wildcard URLs with **http://**. You can use "*" only if it is at the beginning of the URL and is followed by "**.**". You can use "**?**" only at the end of the URL.

   The following wildcard syntaxes are supported: **http://*.example.net**, **http://www.example.ne?**, **http://www.example.n??**. The following wildcard syntaxes are not supported: *.example.???, http://*example.net, http://?.

2. Create a custom object called urllist3 that contains the pattern http://www.example.net and then add the urllist3 custom object to the custom URL category custurl3.

   ```
   [edit security utm]
   user@host# set custom-objects custom-url-category custurl3 value urllist3
   ```

3. Create a list of untrusted and trusted sites.

   ```
   [edit security utm]
   user@host# set custom-objects url-pattern urllistblack value [http://www.untrusted.com 13.13.13.13]
   user@host# set custom-objects url-pattern urllistwhite value [http://www.trusted.com 11.11.11.11]
   ```

4. Configure the custom URL category list custom object by using the URL pattern list of untrusted and trusted sites.

```
[edit security utm]
user@host# set custom-objects custom-url-category custblacklist value urllistblack
user@host# set custom-objects custom-url-category custwhitelist value urllistwhite
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm custom-objects** command. If the output does not display the intended configuration, repeat the instructions in this example to correct.

```
[edit]
userhost#show security utm custom-objects
   url-pattern {
      urllist3 {
         value [ 1.2.3.4 http://www.example.net ];
      }
      urllistblack {
         value [ 13.13.13.13 http://www.untrusted.com ];
      }
      urllistwhite {
         value [ 11.11.11.11 http://www.trusted.com ];
      }
   }
      custom-url-category {
         custurl3 {
            value urllist3;
         }
         custblacklist {
            value urllistblack;
         }
         custwhiltelist {
            value urllistwhite;
         }
      }
```

If you are done configuring the device, enter **commit** from configuration mode.

***Configuring Enhanced Web Filtering Feature Profiles***

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and

paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

Starting in Junos OS Release 12.3X48-D25, new CLI options are available. The **http-reassemble** and **http-persist** options are added in the **show security utm feature-profile web-filtering** command.

```
[edit security utm]
set security utm feature-profile web-filtering url-whitelist custwhitelist value
set security utm feature-profile web-filtering url-blacklist custblacklist value
set security utm feature-profile web-filtering type juniper-enhanced
set security utm feature-profile web-filtering juniper-enhanced cache size 500
set security utm feature-profile web-filtering juniper-enhanced cache timeout 1800
set security utm feature-profile web-filtering juniper-enhanced server host rp.cloud.threatseeker.com
set security utm feature-profile web-filtering juniper-enhanced server port 80
set security utm feature-profile web-filtering http-reassemble
set security utm feature-profile web-filtering http-persist
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile category
    Enhanced_Hacking action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile category
    Enhanced_Government action quarantine
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile site-reputation-action
    very-safe permit
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile custom-block-message
    "***access denied ***"
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile block-message type
    custom-redirect-url
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile block-message url
    http://10.10.121.18
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile default block
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile fallback-settings
    server-connectivity block
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile fallback-settings timeout
    block
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile fallback-settings
    too-many-requests block
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile timeout 10
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile no-safe-search
set security utm utm-policy mypolicy web-filtering http-profile ewf_my_profile
set security policies from-zone utm_clients to-zone mgmt policy 1 then permit application-services utm-policy
    mypolicy
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
    quarantine-custom-message “**The requested webpage is blocked by your organization's access policy**”.
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile quarantine-message
    type custom-redirect-url
```

```
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile quarantine-message url
    besgas.spglab.example.net
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the EWF feature profiles:

1. Configure the Web filtering URL blocklist, URL allowlist, and the Web filtering engine.

```
[edit security utm feature-profile web-filtering]
user@host# set url-blacklist custblacklist
user@host# set url-whitelist custwhitelist
user@host# set type juniper-enhanced
```

2. Set the cache size and cache timeout parameters for the configured EWF engine.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced cache size 500
user@host# set juniper-enhanced cache timeout 1800
```

3. Set the server name or IP address and the port number for communicating with the server. The default host value in the system is rp.cloud.threatseeker.com.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced server host rp.cloud.threatseeker.com
user@host# set juniper-enhanced server port 80
```

4. Set the **http-reassemble** statement to reassemble the requested packet and the **http-persist** statement to check every HTTP request packet in the same session. If the **http-reassemble** statement is not configured for cleartext HTTP traffic, then EWF does not reassemble the fragmented HTTP request to avoid incomplete parsing in the packet-based inspection. If the **http-persist** statement is not configured for cleartext HTTP traffic, then EWF does not check every HTTP request packet in the same session.

```
[edit security utm feature-profile web-filtering]
user@host# set http-reassemble
user@host# set http-persist
```

5. Create a profile name, and select a category from the included allowlist and blocklist categories.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf_my_profile category Enhanced_Hacking action log-and-permit
user@host# set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile category
   Enhanced_Government action quarantine
```

6. Specify the action to be taken depending on the site reputation returned for the URL if there is no category match found.

```
[edit security utm feature-profile web-filtering]
user@host#set juniper-enhanced profile ewf_my_profile site-reputation-action very-safe permit
```

7. Enter a custom message to be sent when HTTP requests are blocked.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf_my_profile custom-block-message "***access denied ***"
```

8. Define a redirect URL server so that instead of the device sending a block page with plain text HTML, the device will send an HTTP 302 redirect to this redirect server with some special variables embedded in the HTTP redirect location field. These special variables can be parsed by the redirect server and serve a special block page to the client with rich images and formatting.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf_my_profile block-message type custom-redirect-url
   http://10.10.1.1
user@host# set juniper-enhanced profile ewf_my_profile block-message url http://10.10.121.18
```

   If you configure the **security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile block-message** statement, then the default block message configuration takes precedence over the **security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile custom-block-message** configuration.

9. Specify a default action (permit, log and permit, block, or quarantine) for the profile, when no other explicitly configured action (blocklist, allowlist, custom category, predefined category actions, or site reputation actions) is matched .

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf_my_profile default block
```

10. Configure the fallback settings (block or log and permit) for this profile.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf_my_profile fallback-settings default block
user@host# set juniper-enhanced profile ewf_my_profile fallback-settings server-connectivity block
user@host# set juniper-enhanced profile ewf_my_profile fallback-settings timeout block
user@host# set juniper-enhanced profile ewf_my_profile fallback-settings too-many-requests block
```

11. Enter a timeout value in seconds. When this limit is reached, fallback settings are applied. This example sets the timeout value to 10. You can also disable the safe-search functionality. By default, search requests have safe-search strings attached to them, and a redirect response is sent to ensure that all search requests are safe or strict.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf_my_profile timeout 10
user@host# set juniper-enhanced profile ewf_my_profile no-safe-search
```

> **NOTE:** The timeout value range for SRX210, SRX220, SRX240, SRX300, SRX320, SRX345, SRX380, SRX550, SRX1500, SRX4100, and SRX4200 is 0 through 1800 seconds and the default value is 15 seconds. The timeout value range for SRX3400 and SRX3600 is 1 through 120 seconds and the default value is 3 seconds.

12. Configure a UTM policy (mypolicy) for the Web-filtering HTTP protocol, associating ewf_my_profile to the UTM policy, and attach this policy to a security profile to implement it.

```
[edit security utm]
user@host# set utm-policy mypolicy web-filtering http-profile ewf_my_profile
user@host# set security policies from-zone utm_clients to-zone mgmt policy 1 then permit application-services
    utm-policy mypolicy
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm feature-profile** command. If the output does not display the intended configuration, repeat the instructions in this example to correct.

```
[edit]
user@host# show security utm
feature-profile{
web-filtering {
   url-whitelist custwhitelist{
```

```
url-blacklist custblacklist;
http-reassemble;
http-persist;
type juniper-enhanced;
juniper-enhanced {
    cache {
        timeout 1800;
        size 500;
    }
    server {
        host rp.cloud.threatseeker.com;
        port 80;
    }
    profile ewf_my_profile {
        category {
            Enhanced_Hacking {
                action log-and-permit;
                }
                Enhanced_Government {
                action quarantine;
            }
        }
        site-reputation-action {
            very-safe permit;
            moderately-safe log-and-permit;
            fairly-safe log-and-permit;
            harmful block;
            suspicious block;
        }
        default block;
        custom-block-message "***access denied ***";
        fallback-settings {
            default block;
            server-connectivity block;
            timeout block;
            too-many-requests block;
        }
        timeout 10;
        no-safe-search;
    }
    utm-policy mypolicy {
        web-filtering {
    http-profile ewf_my_profile;
}
```

```
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

***Attaching Web Filtering UTM Policies to Security Policies***

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security policies from-zone trust to-zone untrust policy sec_policy match source-address any
set security policies from-zone trust to-zone untrust policy sec_policy match destination-address any
set security policies from-zone trust to-zone untrust policy sec_policy match application any
set security policies from-zone trust to-zone untrust policy sec_policy then permit application-services utm-policy
    mypolicy
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To attach a UTM policy to a security policy:

1. Create the security policy sec_policy.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy sec_policy
```

2. Specify the match conditions for sec-policy.

```
[edit security policies from-zone trust to-zone untrust policy sec_policy]
user@host# set match source-address any
user@host# set match destination-address any
user@host# set match application any
```

3. Attach the UTM policy mypolicy to the security policy sec_policy.

```
[edit security policies from-zone trust to-zone untrust policy sec_policy]
user@host#  set then permit application-services utm-policy mypolicy
```

### Results

From configuration mode, confirm your configuration by entering the **show security policies** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
    from-zone trust to-zone untrust {
        sec_policy {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit {
                    application-services {
                        utm-policy mypolicy;
                    }
                }
            }
        }
    }
        default-policy {
            permit-all;
        }
```

After you are done configuring the device, enter **commit** from configuration mode.

## Verification

**IN THIS SECTION**



To confirm that the configuration is working properly, perform these tasks:

*Verifying the Status of the Web Filtering Server*

**Purpose**

Verify the Web filtering server status.

**Action**

From the top of the configuration in operational mode, enter the **show security utm web-filtering status** command.

```
user@host> show security utm web-filtering status
```

```
UTM web-filtering status:
   Server status: Juniper Enhanced using Websense server UP
```

**Meaning**

The command output shows that the Web filtering server connection is up.

*Verifying that Web Filtering Statistics Have Increased*

**Purpose**

Verify the increase in Web filtering statistics. The initial counter value is 0; if there is an HTTP request URL hit, then there is a increase in the Web filtering statistics.

**Action**

From the top of the configuration in operational mode, enter the **show security utm web-filtering statistics** command.

```
user@host> show security utm web-filtering statistics
```

```
UTM web-filtering statistics:
   Total requests:                   0
   white list hit:                   0
   Black list hit:                   0
   Queries to server:                0
   Server reply permit:              0
   Server reply block:               0
   Server reply quarantine:          0
   Server reply quarantine block:    0
   Server reply quarantine permit:   0
   Custom category permit:           0
   Custom category block:            0
   Custom category quarantine:       0
   Custom category qurantine block:  0
```

```
    Custom category quarantine permit:  0
    Site reputation permit:             0
    Site reputation block:              0
    Site reputation quarantine:         0
    Site reputation quarantine block:   0
    Site reputation quarantine permit:  0
    Site reputation by Category         0
    Site reputation by Global           0
    Cache hit permit:                   0
    Cache hit block:                    0
    Cache hit quarantine:               0
    Cache hit quarantine block:         0
    Cache hit quarantine permit:        0
    Safe-search redirect:               0
   SNI pre-check queries to server:    1
    SNI pre-check server responses:     1
    Web-filtering sessions in total:    128000
    Web-filtering sessions in use:      0
    Fallback:                       log-and-permit           block
          Default                                   0               0
          Timeout                                   0               0
     Connectivity                                   0               0
Too-many-requests                                   0               0
```

**Meaning**

The output displays Web filtering statistics for connections including allowlist and blocklist hits and custom category hits. If there is an HTTP request URL hit, then there is a increase in the Web filtering statistics from an earlier value.

***Verifying That the Web Filtering UTM Policy Is Attached to the Security Policy***

**Purpose**

Verify that the Web filtering UTM policy mypolicy is attached to the security policy sec_policy.

**Action**

From operational mode, enter the **show security policy** command.

`user@host>` **show security policies global policy-name mypolicy detail**

```
node0:
-
   Global policies:
```

```
Policy: mypolicy, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 1
From zones: zone1, zone2
To zones: zone3, zone4
Source addresses: any
Destination addresses: any
Applications: any
Action: permit
Unified Threat Management: enabled
```

**Meaning**

The output displays a summary of all security policies configured on the device. If a particular policy is specified, it displays information specific to that policy. If UTM is enabled, then mypolicy is attached to sec_policy.

SEE ALSO

Web Filtering Overview | 147

Monitoring Web Filtering Configurations | 230

## Understanding the Quarantine Action for Enhanced Web Filtering

UTM Enhanced Web Filtering supports block, log-and-permit, and permit actions for HTTP/HTTPS requests. In addition to this, UTM Enhanced Web Filtering now supports the quarantine action which allows or denies access to the blocked site based on the user's response to the message.

The following sequence explains how the HTTP or HTTPs request is intercepted, redirected, and acted upon by the quarantine action:

- The HTTP client requests URL access.
- The device intercepts the HTTP request and sends the extracted URL to the Websense Thread Seeker Cloud (TSC).
- The TSC returns the URL category and the site reputation information to the device.
- If the action configured for the category is quarantine, the device logs the quarantine action and sends a redirect response to HTTP client.
- The URL is sent to the HTTP server for redirecting.

- The device shows a warning message stating that the access to the URL is blocked according to the organization's security policies and prompts the user to respond.
- If the user response is "No," the session is terminated. If the user response is "Yes," the user is allowed access to the site and such access is logged and reported to the administrator.

> **NOTE:** The quarantine action is supported only for UTM Enhanced Web Filtering or Juniper enhanced type of Web filtering.

**Quarantine Message**

The quarantine message sent to the HTTP client is user-configurable and is of the following types:

- Default message

  The default quarantine message is displayed when a user attempts to access a quarantined website and it contains the following information:

  - URL name
  - Quarantine reason
  - Category (if available)
  - Site-reputation (if available)

  For example, if you have set the action for Enhanced_Search_Engines_and_Portals to quarantine, and you try to access www.search.example.com, the quarantine message is as follows:

  ***The requested webpage is blocked by your organization's access policy***.**

- Syslog message.

  The syslog message will be logged by the system when the user access the web page that has already been quarantined and marked as block or permit.

  The corresponding syslog message on the device under test is:

  **Jan 25 15:10:40 rodian utmd[3871]: WEBFILTER_URL_BLOCKED: WebFilter: ACTION="URL Blocked" 99.99.99.4(60525)->74.125.224.114(80) CATEGORY="Enhanced_Search_Engines_and_Portals" REASON="by predefined category(quarantine)" PROFILE="ewf-test-profile" URL=www.search.example.com OBJ=/**

  Starting in Junos OS 12.1X47-D40 and Junos OS Release 17.3R1, the structured log fields have changed. The structured log field changes in the UTM Web filter logs WEBFILTER_URL_BLOCKED, WEBFILTER_URL_REDIRECTED, and WEBFILTER_URL_PERMITTED are as follows:

  - **name -> category**
  - **error-message -> reason**

- **profile-name -> profile**
- **object-name -> url**
- **pathname -> obj**

### User Messages and Redirect URLs for Enhanced Web Filtering (EWF)

Starting with Junos OS Release 15.1X49-D110, a new option, **custom-message**, is added for the **custom-objects** statement that enables you to configure user messages and redirect URLs to notify users when a URL is blocked or quarantined for each EWF category. The **custom-message** option has the following mandatory attributes:

- **Name**: Name of the custom message; maximum length is 59 ASCII characters.
- **Type**: Type of custom message: **user-message** or **redirect-url**.
- **Content**: Content of the custom message; maximum length is 1024 ASCII characters.

You configure a user message or redirect URL as a custom object and assign the custom object to an EWF category.

- User messages indicate that website access has been blocked by an organization's access policy. To configure a user message, include the **type user-message content *message-text*** statement at the **[edit security utm custom-objects custom-message *message*]** hierarchy level.
- Redirect URLs redirect a blocked or quarantined URL to a user-defined URL. To configure a redirect URL, include the **type redirect-url content redirect-url** statement at the **[edit security utm custom-objects custom-message *message*]** hierarchy level.

The **custom-message** option provides the following benefits:

- You can configure a separate custom message or redirect URL for each EWF category.
- The **custom-message** option enables you to fine-tune messages to support your polices to know which URL is blocked or quarantined.
- Only one custom-message configuration option is applied for each category. The custom-message configuration is supported only on Enhanced Web Filtering (EWF). Therefore, only the Juniper EWF engine type is supported.

Starting with Junos OS Release 17.4R1, support for custom category configuration is available for local and Websense redirect profiles.

SEE ALSO

Understanding Integrated Web Filtering | 337

# Example: Configuring Site Reputation Action for Enhanced Web Filtering

IN THIS SECTION



This example shows how to configure the site reputation action for both categorized and uncategorized URLs.

## Requirements

Before you begin, you should be familiar with Web Filtering and Enhanced Web Filtering. See "Web Filtering Overview" on page 147 and "Understanding the Enhanced Web Filtering Process" on page 151.

## Overview

In this example, you configure Web Filtering profiles to URLs according to defined categories using the site reputation action. You set the URL allowlist filtering category to **url-cat-white** and the type of Web Filtering engine to **juniper-enhanced**. Then you set the cache size parameters for Web Filtering and the cache timeout parameters to 1.

Then you create a **juniper-enhanced** profile called profile **ewf-test-profile**, set the URL allowlist category to **cust-cat-quarantine**, and set the reputation action to quarantine.

You enter a custom message to be sent when HTTP requests are quarantined. In this example, the following message is sent: **The requested webpage is blocked by your organization's access policy**.

You block URLs in the Enhanced_News_and_Media category and permit URLs in the Enhanced_Education category. Then you quarantine the URLs in the Enhanced_Streaming_Media category and configure the device to send the following message: **The requested webpage is blocked by your organization's access policy**.

In this example, you set the default action to permit. You select fallback settings (block or log-and-permit) for this profile in case errors occur in each configured category. Finally, you set the fallback settings to block.

## Configuration

### *Configuring Site Reputation Action*

#### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm feature-profile web-filtering set url-whitelist url-cat-white
set security utm feature-profile web-filtering juniper-enhanced cache size
set security utm feature-profile web-filtering juniper-enhanced reputation reputation-very-safe 85
set security utm feature-profile web-filtering juniper-enhanced reputation reputation-moderately-safe 75
set security utm feature-profile web-filtering juniper-enhanced reputation reputation-fairly-safe 65
set security utm feature-profile web-filtering juniper-enhanced reputation reputation-suspicious 55
set security utm feature-profile web-filtering juniper-enhanced cache timeout 1
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile category
    cust-cat-quarantine action quarantine
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile category
    Enhanced_News_and_Media action block
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile category
    Enhanced_Education action permit
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile category
    Enhanced_Education reputation-action harmful block
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile category
    Enhanced_Streaming_Media action quarantine
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile default permit
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile default quarantine-message
    “*** The requested webpage is blocked by your organization’s access policy***”.
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile fallback-settings
    server-connectivity block
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile fallback-settings timeout
    block
```

#### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the site reputation action:

1. Configure the Web Filtering URL allowlist.

```
[edit security utm feature-profile web-filtering]
user@host# set url-whitelist custwhitelist
```

2. Specify the Enhanced Web Filtering engine, and set the cache size parameters.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced cache size
```

3. Configure the base reputation scores.

```
[edit security utm feature-profile web-filtering]
set juniper-enhanced reputation reputation-very-safe 85
set juniper-enhanced reputation reputation-moderately-safe 75
set juniper-enhanced reputation reputation-fairly-safe 65
set juniper-enhanced reputation reputation-suspicious 55
```

**NOTE:** The base reputation value must be ordered.

4. Set the cache timeout parameters.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced cache timeout 1
```

5. Create a profile name, and select a category from the allowlist categories.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile category cust-cat-quarantine action quarantine
```

6. Create a profile name, and select a category from the allowlist categories.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile category Enhanced_News_and_Media action block
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile category Enhanced_Education action permit
user@host# set juniper-enhanced profile ewf-test-profile category Enhanced_Education action harmful
    block
```

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile category Enhanced_Streaming_Media action
    quarantine
```

7. Enter a warning message to be sent when HTTP requests are quarantined.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile quarantine-custom-message "***The requested
    webpage is blocked by your organization's access policy ***"
```

8. Select a default action (permit, log-and-permit, block, or quarantine) for the profile, when no other explicitly configured action (blocklist, allowlist, custom category, predefined category or site reputation ) is matched .

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile default permit
```

9. Select fallback settings (block or log-and-permit) for this profile.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile fallback-settings server-connectivity block
user@host# set juniper-enhanced profile ewf-test-profile fallback-settings timeout block
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm** command. If the output does not display the intended configuration, repeat the instructions in this example to correct.

```
[edit]
user@host# show security utm
feature-profile{
web-filtering {
    url-whitelist url-cat-white;
    type juniper-enhanced;
    traceoptions;
    flag all;
}
    juniper-enhanced {
        reputation {
            reputation-very-safe 85
```

```
    reputation-moderately-safe 75
    reputation-fairly-safe 65
  reputation-suspicious 55
  cache {
    timeout 1
  }
  profile ewf-test-profile {
    category {
      cust-cat-quarantine {
        action quarantine;
        }
        Enhanced_News_and_Media {
          action block;
          reputation-action;
        }
        Enhanced_Education {
        action permit;
        reputation-action;
        {
        harmful block;
        }
        }
        Enhanced_Streaming_Media {
        action quarantine;
        }
      }
    default permit;
  quarantine-custom-message "***The requested webpage is blocked by your organization's access policy***".
    fallback-settings {
      server-connectivity block;
      timeout block;
      }
      }
      }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

IN THIS SECTION



Confirm that the configuration is working properly.

***Verifying the Status of UTM Service***

**Purpose**

Verify the UTM service status.

**Action**

From operational mode, enter the **show security utm status** command.

## Sample Output

`user@host>`**show security utm status**

```
UTM service status: Running
```

***Verifying the Status of UTM Session***

**Purpose**

Verify the UTM session status.

**Action**

From operational mode, enter the **show security utm session** command.

## Sample Output

user@host>**show security utm session**

```
UTM session info:
 Maximum sessions:                4000
 Total allocated sessions:        0
 Total freed sessions:            0
 Active sessions:                 0
```

***Verifying the Status of UTM Web Filtering***

**Purpose**

Verify the UTM Web filtering status.

**Action**

From operational mode, enter the **show security utm web-filtering status** command.

## Sample Output

user@host>**show security utm web-filtering status**

```
UTM web-filtering status:
    Server status: Juniper Enhanced using Websense server UP
```

***Verifying the Statistics of UTM Web Filtering***

**Purpose**

Verify the Web filtering statistics for connections including allowlist and blocklist hits and custom category hits.

**Action**

From operational mode, enter the **show security utm web-filtering statistics** command.

## Sample Output

user@host>**show security utm web-filtering statistics**

```
UTM web-filtering statistics:
    Total requests:                     2594
    white list hit:                     0
    Black list hit:                     0
    Queries to server:                  2407
    Server reply permit:                1829
    Server reply block:                 0
    Server reply quarantine:            517
    Server reply quarantine block:      0
    Server reply quarantine permit:     8
    Custom category permit:             0
    Custom category block:              0
    Custom category quarantine:         0
    Custom category qurantine block:    0
    Custom category quarantine permit:  0
    Site reputation permit:             0
    Site reputation block:              0
    Site reputation quarantine:         0
    Site reputation quarantine block:   0
    Site reputation quarantine permit:  0
    Site reputation by Category         0
    Site reputation by Global           0
    Cache hit permit:                   41
    Cache hit block:                    0
    Cache hit quarantine:               144
    Cache hit quarantine block:         0
    Cache hit quarantine permit:        1
    Safe-search redirect:               0
    Web-filtering sessions in total:    16000
    Web-filtering sessions in use:      0
    Fallback:                       log-and-permit          block
          Default                                0              0
          Timeout                                0              0
     Connectivity                                0              1
Too-many-requests                                0              0
```

***Verifying the URL status using Log file***

**Purpose**

Verify the blocked and allowed URL status using log file.

**Action**

To see blocked and allowed URLs, send the utm logs to a syslog server using stream mode. For more information see: Configuring Off-Box Binary Security Log Files.

From operational mode, enter the **show log messages | match RT_UTM** command.

## Sample Output

user@host>**show log messages | match RT_UTM**

```
RT_UTM: WEBFILTER_URL_BLOCKED: WebFilter: ACTION="URL Blocked" source-zone="trust"
 destination-zone="untrust" 4.0.0.3(59466)->5.0.0.3(80) SESSION_ID=268436912
APPLICATION="UNKNOWN" NESTED-APPLICATION="UNKNOWN" CATEGORY="URL_Blacklist"
REASON="BY_BLACK_LIST" PROFILE="ewf" URL=www.example1.com OBJ=/ username N/A roles
 N/A application-sub-category N/A urlcategory-risk 0
```

SEE ALSO

Understanding URL Allowlist | 52

## TAP Mode Support Overview for UTM

In TAP mode, an SRX Series device will be connected to a mirror port of the switch, which provides a copy of the traffic traversing the switch. An SRX Series device in TAP mode processes the incoming traffic from TAP interface and generates security log to display the information on threats detected, application usage, and user details.

Starting in Junos OS Release 19.1R1 you can enable TAP mode on UTM module. When you enable TAP mode on UTM module, the SRX Series device inspects the incoming and outgoing traffic that matches a firewall policy or policies with the enabled UTM service. TAP mode can't block traffic but generates security logs, reports, and statistics to show the number of threats detected, application usage, and user details. If some packet gets lost in the TAP interface, the UTM terminates the connection, and the TAP mode do not generate any security logs, reports, and statistics for this connection. The UTM configuration remains the same as non-TAP mode.

UTM functionality configured on an SRX Series device continues to work and exchange information from the server. To use UTM functionality when the SRX Series device is configured in TAP mode, you must configure the DNS server to resolve the cloud server's IP addresses.

To use TAP mode, the SRX device will be connected to a mirror port of the switch, which provides a copy of the traffic traversing the switch. SRX Series device process the incoming traffic from TAP interface and

generates security log information to display the information on threats detected, application usage, and user details.

When operating in TAP mode, the SRX Series device performs:

- Enhanced Web filtering (EWF) for mirrored HTTP traffic.
- Sophos antivirus (SAV) for mirrored HTTP/FTP/SMTP/POP3/IMAP traffic.
- Antispam (AS) for mirrored SMTP traffic.

SEE ALSO

Antispam Filtering Overview.

**Release History Table**

| Release | Description |
| --- | --- |
| 17.4R1 | Starting with Junos OS Release 17.4R1, support for custom category configuration is available for local and Websense redirect profiles. |
| 17.4R1 | Starting with Junos OS Release 17.4R1, you can download and dynamically load new EWF categories. The downloading and dynamic loading of the new EWF categories do not require a software upgrade. Websense occasionally releases new EWF categories. EWF classifies websites into categories according to host, URL, or IP address and performs filtering based on the categories. |
| 17.4R1 | Starting with Junos OS Release 17.4R1, predefined base filters, defined in a category file, are supported for individual EWF categories. Each EWF category has a default action in a base filter, which is attached to the user profile to act as a backup filter. If the categories are not configured in the user profile, then the base filter takes the action. |
| 17.4R1 | Starting with Junos OS Release 17.4R1, the reputation base scores are configurable. Users can apply global reputation values, provided by the Websense ThreatSeeker Cloud (TSC). For the non-category URLs, the global reputation value is used to perform filtering, |
| 17.4R1 | Starting with Junos OS Release 17.4R1, support for custom category configuration is available for local and Websense redirect profiles. |
| 17.4R1 | Starting with Junos OS Release 17.4R1, support for custom category configuration is available for local and Websense redirect profiles. |
| 15.1X49-D40 | Starting in Junos OS Release 15.1X49-D40 and Junos OS Release 17.3R1, EWF supports HTTPS traffic by intercepting HTTPS traffic passing through the SRX Series device. |
| 15.1X49-D40 | Starting with Junos OS 15.1X49-D40 and Junos OS Release 17.3R1, EWF intercepts HTTPS traffic passing through the SRX Series device. The security channel from the device is divided as one SSL channel between the client and the device and another SSL channel between the device and the HTTPS server. SSL forward proxy acts as the terminal for both channels and forwards the cleartext traffic to the UTM. UTM extracts the URL from the HTTP request message. |
| 15.1X49-D110 | Starting with Junos OS Release 15.1X49-D110, a new option, **custom-message**, is added for the **custom-objects** command that enables you to configure user messages and redirect URLs to notify users when a URL is blocked or quarantined for each EWF category. |
| 15.1X49-D110 | Starting with Junos OS Release 15.1X49-D110, a new option, **custom-message**, is added for the **custom-objects** statement that enables you to configure user messages and redirect URLs to notify users when a URL is blocked or quarantined for each EWF category. |

| | |
|---|---|
| 15.1X49-D110 | Starting with Junos OS Release 15.1X49-D110, the “* “ in a wildcard syntax, required to create URL pattern for Web filtering profile, matches all subdomains. |
| 15.1X49-D110 | Starting with Junos OS Release 15.1X49-D110, a new option, **custom-message**, is added for the **custom-objects** statement that enables you to configure user messages and redirect URLs to notify users when a URL is blocked or quarantined for each EWF category. |
| 12.3X48-D25 | Starting with Junos OS Release 12.3X48-D25 and Junos OS Release 17.3R1, Enhanced Web Filtering (EWF) over SSL forward proxy supports HTTPS traffic. |
| 12.1X47-D40 | Starting in Junos OS 12.1X47-D40 and Junos OS Release 17.3R1, the structured log fields have changed. |

RELATED DOCUMENTATION

Displaying Global SurfControl URL Categories | 351
Monitoring Web Filtering Configurations | 230
Redirect Web Filtering | 207

# Local Web Filtering

**IN THIS SECTION**



The Web filtering lets you to manage Internet usage by preventing access to inappropriate Web content. There are four types of Web filtering solutions. For more information, see the following topics:

# Understanding Local Web Filtering

IN THIS SECTION



Local web filtering allows you to define custom URL categories, which can be included in blocklists and allowlists that are evaluated on the SRX Series device. All URLs for each category in a blocklist are denied, while all URLs for each category in a allowlist are permitted.

With local Web filtering, a firewall intercepts every HTTP request in a TCP connection and extracts the URL. A decision is made by the device after it looks up a URL to determine whether it is in the allowlist or blocklist based on its user-defined category. A URL is first compared to the blocklist URLs. If a match is found, the request is blocked. If no match is found, the URL is compared to the allowlist. If a match is found, the request is permitted. If the URL is not in either list, the custom category is taken (block, log-and-permit, or permit). If the URL is not in custom category, the defined default action is taken (block, log-and-permit, or permit). You can permit or block access to a requested site by binding a Web filtering profile to a firewall policy. Local Web filtering provides basic Web filtering without requiring an additional license or external category server.

This topic contains the following sections:

## Local Web Filtering Process

The following section describes on how Web traffic is intercepted and acted upon by the Web filtering module.

1. The device intercepts a TCP connection.

2. The device intercepts each HTTP request in the TCP connection.

3. The device extracts each URL in the HTTP request and checks its URL against the user-defined allowlist and blocklist.

4. If the URL is found in the blocklist, the request is not permitted and a deny page is sent to the http client. If the URL is found in the allowlist, the request is permitted.

5. If the URL is not found in the allowlist or blocklist, the configured default fallback action is applied. If no fallback action is defined, then the request is permitted.

### User-Defined Custom URL Categories

To perform local Web filtering, you must define a blocklist and allowlist content that can be applied to the profile.

When defining your own URL categories, you can group URLs and create categories specific to your needs. Each category can have a maximum of 20 URLs. When you create a category, you can add either the URL or the IP address of a site. When you add a URL to a user-defined category, the device performs DNS lookup, resolves the hostname into IP addresses, and caches this information. When a user tries to access a site with the IP address of the site, the device checks the cached list of IP addresses and tries to resolve the hostname. Many sites have dynamic IP addresses, meaning that their IP addresses change periodically. A user attempting to access a site can type an IP address that is not in the cached list on the device. Therefore, if you know the IP addresses of sites you are adding to a category, enter both the URL and the IP address(es) of the site.

You define your own categories using URL pattern list and custom URL category list custom objects. Once defined, you assign your categories to the global user-defined url-blocklist (block) or url-allowlist (permit) categories.

Web filtering is performed on all the methods defined in HTTP 1.0 and HTTP 1.1.

### Local Web Filtering Profiles

You configure Web filtering profiles that permit or block URLs according to defined custom categories. A Web filtering profile consists of a group of URL categories assigned one of the following actions:

- Blocklist — The device always blocks access to the websites in this list. Only user-defined categories are used with local Web filtering.
- Allowlist — The device always allows access to the websites in this list. Only user-defined categories are used with local Web filtering.

A Web filtering profile can contain one blocklist or one allowlist with multiple user-defined categories each with a permit or block action. You can define a default fallback action when the incoming URL does not belong to any of the categories defined in the profile. If the action for the default category is block, the incoming URL is blocked if it does not match any of the categories explicitly defined in the profile. If an action for the default action is not specified, the default action of permit is applied to the incoming URL not matching any category.

Starting with Junos OS Release 17.4R1, custom category configuration is supported for local Web filtering. The **custom-message** option is also supported in a category for local Web filtering and Websense redirect profiles. Users can create multiple URL lists (custom categories) and apply them to a UTM Web filtering profile with actions such as permit, permit and log, block, and quarantine. To create a global allowlist or blocklist, apply a local Web filtering profile to a UTM policy and attach it to a global rule.

### User Messages and Redirect URLs for Web Filtering

Starting with Junos OS Release 17.4R1, a new option, **custom-message**, is added for the **custom-objects** statement that enables you to configure user messages and redirect URLs to notify users when a URL is blocked or quarantined for each EWF category. The **custom-message** option has the following mandatory attributes:

- **Name**: Name of the custom message; maximum length is 59 ASCII characters.
- **Type**: Type of custom message: **user-message** or **redirect-url**.
- **Content**: Content of the custom message; maximum length is 1024 ASCII characters.

You configure a user message or redirect URL as a custom object and assign the custom object to an EWF category.

- User messages indicate that website access has been blocked by an organization's access policy. To configure a user message, include the **type user-message content *message-text*** statement at the **[edit security utm custom-objects custom-message *message*]** hierarchy level.
- Redirect URLs redirect a blocked or quarantined URL to a user-defined URL. To configure a redirect URL, include the **type redirect-url content redirect-url** statement at the **[edit security utm custom-objects custom-message *message*]** hierarchy level.

The **custom-message** option provides the following benefits:

- You can configure a separate custom message or redirect URL for each EWF category.
- The **custom-message** option enables you to fine-tune messages to support your polices to know which URL is blocked or quarantined.

### Profile Matching Precedence

When a profile employs several categories for URL matching, those categories are checked for matches in the following order:

1. If present, the global blocklist is checked first. If a match is made, the URL is blocked. If no match is found...

2. The global allowlist is checked next. If a match is made, the URL is permitted. If no match is found...

3. User-defined categories are checked next. If a match is made, the URL is blocked or permitted as specified.

SEE ALSO

Web Filtering Overview | 147
Understanding Redirect Web Filtering | 208
Example: Configuring Local Web Filtering | 195

# Example: Configuring Local Web Filtering

IN THIS SECTION



This example shows how to configure local Web filtering for managing website access.

## Requirements

This example uses the following hardware and software components:

- SRX1500 device
- Junos OS Release 12.1X46-D10 or later

Before you begin, learn more about Web filtering. See "Web Filtering Overview" on page 147.

## Overview

In this example you configure local Web filtering custom objects, local Web filtering feature profiles, and local Web filtering UTM policies. You also attach local Web filtering UTM policies to security policies. Table 5 on page 162 shows information about local Web filtering configuration type, steps, and parameters used in this example.

**Table 6: Local Web filtering Configuration Type, Steps, and Parameters**

| Configuration Type | Configuration Steps | Configuration Parameters |
|---|---|---|
| **URL pattern and custom objects** | Configure a URL pattern list of URLs or addresses that you want to bypass.<br><br>Create a custom object called urllis1 that contains the pattern [http://www.example1.net 192.0.2.0]<br><br>Create a custom object called urllist2 that contains the pattern [http://www.example2.net 192.0.2.3]<br><br>Create a custom object called urllist3 that contains the pattern [http://www.example3.net 192.0.2.9]<br><br>Create a custom object called urllist4 that contains the pattern [http://www.example4.net 192.0.2.8] | • [http://www.example1.net 192.0.2.0]<br>• [http://www.example2.net 192.0.2.3]<br>• [http://www.example3.net 192.0.2.9]<br>• [http://www.example4.net 192.0.2.8]<br>• **value urllist3**<br>• **value urllist4** |
| | The urllist1 and urllist2 custom objects are then added to the custom URL categories cust-blocklist, and cust-permit-list respectively. | • **value urllist1**<br>• **value urllist2** |

**Table 6: Local Web filtering Configuration Type, Steps, and Parameters *(continued)***

| Configuration Type | Configuration Steps | Configuration Parameters |
|---|---|---|
| **Feature profiles** | Configure the Web filtering feature profile: | |
| | • Set the URL blocklist filtering category to custurl4 and the URL allowlist filtering category to custurl3. Set the type of Web filtering engine to juniper-local. | • **custurl3**<br>• **custurl4**<br>• **type juniper-local** |
| | • Create a juniper-local profile name called localprofile1. Select a default action (permit, log-and-permit, block) for this profile for requests that experience errors. This example sets the default action to permit. Add category cust-permit-list with log-and-permit action and cus-blocklist with block action. | • **localprofile1**<br>• **Action: block**<br>• **Action: log-and-permit**<br>• **cust-black-list**<br>• **cust-permit-list** |
| | • Define redirect url. Enter a custom message to be sent when HTTP requests are blocked.<br>• Select fallback settings (block or log-and-permit) for this profile, in case errors occur in each configured category. This example sets fallback settings to block. | • **block-message type custom-redirect-url**<br>• **block-message url 192.0.2.10**<br>• **custom-block-message "**Access to this site is not permitted**".**<br>• **fallback-settings:**<br>  ◦ **block**<br>  ◦ **log-and-permit** |
| **UTM policies** | Create the UTM policy utmp5 and attach it to the profile localprofile1. In the final configuration example, attach the UTM policy utmp5 to the security policy p5. | • **utm policy utmp5**<br>• **policy p5** |

## Configuration

IN THIS SECTION



### *Configuring Local Web Filtering Custom Objects and URL Patterns*

#### CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm custom-objects url-pattern urllist1 value http://www.example1.net
set security utm custom-objects url-pattern urllist1 value 192.0.2.0
set security utm custom-objects url-pattern urllist2 value http://www.example2.net
set security utm custom-objects url-pattern urllist2 value 192.0.2.3
set security utm custom-objects url-pattern urllist3 value http://www.example3.net
set security utm custom-objects url-pattern urllist3 value 192.0.2.9
set security utm custom-objects url-pattern urllist4 value http://www.example4.net
set security utm custom-objects url-pattern urllist4 value 192.0.2.8
set security utm custom-objects custom-url-category cust-black-list value urllist1
set security utm custom-objects custom-url-category cust-permit-list value urllist2
set security utm custom-objects custom-url-category custurl3 value urllist3
set security utm custom-objects custom-url-category custurl4 value urllist4
```

Starting in Junos OS Release 15.1X49-D110, the “* “ in a wildcard syntax, used for URL pattern Web filtering profile, matches all subdomains.  For example, *.example.net matches:

- http://a.example.net
- http://example.net
- aaa.example.net

#### Step-by-Step Procedure

To configure local Web filtering using the CLI:

1. Configure a URL pattern list custom object by creating the list name and adding values to it as follows:

   **NOTE:** Because you use URL pattern lists to create custom URL category lists, you must configure URL pattern list custom objects before you configure custom URL category lists.

```
[edit]
user@host# set security utm custom-objects url-pattern urllist1 value [http://www.example1.net 192.0.2.0]
user@host# set security utm custom-objects url-pattern urllist2 value [http://www.example2.net 192.0.2.3]
user@host# set security utm custom-objects url-pattern urllist3 value [http://www.example3.net 192.0.2.9]
user@host# set security utm custom-objects url-pattern urllist4 value [http://www.example4.net 192.0.2.8]
```

   **NOTE:**
   - The guideline to use a URL pattern wildcard is as follows: Use *\.[]\?* and precede all wildcard URLs with **http://**. You can use "*" only if it is at the beginning of the URL and is followed by ".". You can use "**?**" only at the end of the URL.
   - The following wildcard syntaxes are supported: **http://*.example.net**, **http://www.example.ne?**, **http://www.example.n??**. The following wildcard syntaxes are not supported: *.example.???, http://*example.net, http://?.

2. Applying the URL pattern to a custom URL category.

```
[edit]
user@host# set security utm custom-objects custom-url-category cust-black-list value urllist1
user@host# set security utm custom-objects custom-url-category cust-permit-list value urllist2
user@host# set security utm custom-objects custom-url-category custurl3 value urllist3
user@host# set security utm custom-objects custom-url-category custurl4 value urllist4
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm custom-objects** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
userhost#show security utm custom-objects
    url-pattern {
```

```
        urllist1 {
            value [ http://www.example1.net 192.0.2.0 ];
        }
        urllist2 {
            value [ http://www.example2.net 192.0.2.3 ];
        }
        urllist3 {
            value [ http://www.example3.net 192.0.2.9 ];
        }
        urllist4 {
            value [ http://www.example4.net 192.0.2.8 ];
        }
    }
        custom-url-category {
            cust-black-list {
                value urllist1;
            }
            cust-permit-list {
                value urllist2;
            }
            custurl3 {
                value urllist3;
            }
            custurl4 {
                value urllist4;
            }
        }
```

If you are done configuring the device, enter **commit** from configuration mode.

***Apply Custom Objects to the Feature Profiles***

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm feature-profile web-filtering url-whitelist custurl3
set security utm feature-profile web-filtering url-blacklist custurl4
set security utm feature-profile web-filtering type juniper-local
set security utm feature-profile web-filtering juniper-local profile localprofile1 category cust-black-list action
    block
```

```
set security utm feature-profile web-filtering juniper-local profile localprofile1 category cust-permit-list action
    log-and-permit
set security utm feature-profile web-filtering juniper-local profile localprofile1 block-message type
    custom-redirect-url
set security utm feature-profile web-filtering juniper-local profile localprofile1 block-message url http://192.0.2.10
set security utm feature-profile web-filtering juniper-local profile localprofile1 custom-block-message "Access
    to this site is not permitted."
set security utm feature-profile web-filtering juniper-local profile localprofile1 default log-and-permit
set security utm feature-profile web-filtering juniper-local profile localprofile1 fallback-settings default block
set security utm feature-profile web-filtering juniper-local profile localprofile1 fallback-settings too-many-requests
    block
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure local Web filtering feature profiles:

1. Configure the Web filtering URL blocklist, URL allowlist, and the Web filtering engine.

   ```
   [edit security utm feature-profile web-filtering]
   user@host# set url-whitelist custurl3
   user@host# set url-blacklist custurl4
   user@host# set type juniper-local
   ```

2. Create a profile name, and select a category from the included permit and blocklist categories. The custom category action could be block, permit, log-and-permit, and quarantine.

   ```
   [edit security utm feature-profile web-filtering]
   user@host# set juniper-local profile localprofile1 category cust-black-list action block
   user@host# set juniper-local profile localprofile1 category cust-permit-list action log-and-permit
   ```

3. Define a redirect URL server so that instead of the device sending a block page with plain text HTML, the device send an HTTP 302 redirect to this redirect server with special variables embedded in the HTTP redirect location field. These special variables are parsed by the redirect server and serve as a special block page to the client with images and a clear text format.

   ```
   [edit security utm feature-profile web-filtering]
   user@host# set security utm feature-profile web-filtering juniper-local profile localprofile1 block-message
       type custom-redirect-url
   ```

```
user@host# set security utm feature-profile web-filtering juniper-local profile localprofile1 block-message
  url http://192.0.2.10
```

4. Enter a custom message to be sent when HTTP requests are blocked.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-local profile localprofile1 custom-block-message “Access to this site is not permitted”
```

5. Specify a default action (permit, log and permit, block, or quarantine) for the profile, when no other explicitly configured action (blocklist, allowlist, custom category, predefined category actions, or site reputation actions) is matched .

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-local profile localprofile1 default log-and-permit
```

6. Configure fallback settings (block or log and permit) for this profile.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper–local profile localprofile1 fallback-settings default block
user@host# set juniper–local profile localprofile1 fallback-settings too-many-requests block
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm feature-profile** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
userhost#show security utm feature-profile
web-filtering {
   url-whitelist custurl3;
   url-blacklist custurl4;
   type juniper-local;
   juniper-local {
      profile localprofile1 {
         default log-and-permit;
         category {
         cust-black-list {
         action block;
         }
```

```
            cust-permit-list {
            action log-and-permit;
            }
            }
            custom-block-message "Access to this site is not permitted.";
            block-message {
            type custom-redirect-url;
            url http://192.0.2.10;
            }
            fallback-settings {
               default block;
               too-many-requests block;
            }
            }
            }
         }
      }
   }
```

If you are done configuring the device, enter **commit** from configuration mode.

***Attaching Web Filtering UTM Policies to Security Policies***

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm utm-policy utmp5 web-filtering http-profile localprofile1
```

**Step-by-Step Procedure**

To configure a UTM policy:

1. Create the UTM policy referencing a profile. Apply the Web filtering profile to the UTM policy.

```
[edit]
user@host# set security utm utm-policy utmp5 web-filtering http-profile localprofile1
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this show command output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]
userhost# show security utm
utm-policy utmp5 {
    web-filtering {
        http-profile localprofile1;
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

***Attaching Local Web Filtering UTM Policies to Security Policies***

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security policies from-zone trust to-zone untrust policy p5 match source-address any
set security policies from-zone trust to-zone untrust policy p5 match destination-address any
set security policies from-zone trust to-zone untrust policy p5 match application junos-http
set security policies from-zone trust to-zone untrust policy p5 then permit application-services utm-policy
    utmp5
```

**Step-by-Step Procedure**

To attach a UTM policy to a security policy:

1. Create and configure the security policy.

```
[edit security policies from-zone trust to-zone untrust policy p5]
user@host# set match source-address any
user@host# set match destination-address any
user@host# set match application junos-http
```

2. Apply the UTM policy to the security policy.

```
[edit security policies from-zone trust to-zone untrust policy p5]
user@host# set then permit application-services utm-policy utmp5
```

**Results**

From configuration mode, confirm your configuration by entering the **show security policies** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
userhost# show security policies
   from-zone trust to-zone untrust {
      policy p5 {
         match {
            source-address any;
            destination-address any;
            application junos-http;
         }
         then {
            permit {
               application-services {
                  utm-policy utmp5;
               }
            }
         }
      }
   }
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

**IN THIS SECTION**



To confirm that the configuration is working properly, perform the following task:

***Verifying the Statistics of UTM Web Filtering***

**Purpose**

Verify the Web filtering statistics for connections including allowlist and blocklist hits and custom category hits.

**Action**

From operational mode, enter the **show security utm web-filtering statistics** command.

## Sample Output

user@host>**show security utm web-filtering statistics**

```
UTM web-filtering statistics:
    Total requests:                    0
    white list hit:                    0
    Black list hit:                    0
    Custom category permit:            0
    Custom category block:             0
    Custom category quarantine:        0
    Custom category qurantine block:   0
    Custom category quarantine permit: 0
    Web-filtering sessions in total:   0
    Web-filtering sessions in use:     0
    Fallback:                      log-and-permit          block
          Default                                0              0
          Timeout                                0              0
     Connectivity                                0              0
Too-many-requests                                0              0
```

SEE ALSO

Example: Enhancing Security by Configuring Redirect Web Filtering Using Custom Objects | 210

Monitoring Web Filtering Configurations | 230

**Release History Table**

| Release | Description |
|---|---|
| 17.4R1 | Starting with Junos OS Release 17.4R1, custom category configuration is supported for local Web filtering. The **custom-message** option is also supported in a category for local Web filtering and Websense redirect profiles. Users can create multiple URL lists (custom categories) and apply them to a UTM Web filtering profile with actions such as permit, permit and log, block, and quarantine. To create a global allowlist or blocklist, apply a local Web filtering profile to a UTM policy and attach it to a global rule. |
| 17.4R1 | Starting with Junos OS Release 17.4R1, a new option, **custom-message**, is added for the **custom-objects** statement that enables you to configure user messages and redirect URLs to notify users when a URL is blocked or quarantined for each EWF category. |
| 15.1X49-D110 | Starting in Junos OS Release 15.1X49-D110, the "* " in a wildcard syntax, used for URL pattern Web filtering profile, matches all subdomains. |

RELATED DOCUMENTATION

Enhanced Web Filtering | **149**

Allowlist | **50**

# Redirect Web Filtering

**IN THIS SECTION**



The redirect Web filtering solution intercepts HTTP requests and sends them to an external URL filtering server, provided by Websense, to determine whether to block the requests. For more information, see the following topics:

## Understanding Redirect Web Filtering

With redirect Web filtering, the Web filtering module intercepts an HTTP request. The URL in the request is then sent to the external Websense server, which makes a permit or a deny decision. If access is permitted to the URL in question, the original HTTP request and all the subsequent requests are sent to the intended HTTP server. But if access is denied to the URL in question, a blocking message is sent to the client.

This is a general description of how Web traffic is intercepted, redirected, and acted upon by the Web filtering module:

1. A Web client establishes a TCP connection with the webserver.

2. The Web client then sends an HTTP request.

3. The device intercepts the requests and extracts the URL. The URL is checked against global Web filtering allowlists and blocklists. If no match is made, the Websense server configuration parameters are utilized. Otherwise the process continues with step 6.

4. The URL is sent to the Websense server for checking,

5. The Websense server returns a response indicating whether or not the URL is to be permitted or blocked.

6. If access is allowed, the original HTTP request is sent to the webserver. If access is denied, the device sends a blocking message to the client and tears down the TCP connection.

   Web filtering is performed on all the methods defined in HTTP 1.0 and HTTP 1.1. However, redirect Web filtering uses destination IP as URL when it is checking HTTPS traffic.

   Decision making from real-time options provides a higher level of accuracy, therefore caching for redirect Web filtering is not supported.

   Redirect Web filtering does not require a subscription license.

### User Messages and Redirect URLs for Web Filtering

Starting with Junos OS Release 17.4R1, a new option, **custom-message**, is added for the **custom-objects** statement that enables you to configure user messages and redirect URLs to notify users when a URL is blocked or quarantined for each EWF category. The **custom-message** option has the following mandatory attributes:

- **Name**: Name of the custom message; maximum length is 59 ASCII characters.
- **Type**: Type of custom message: **user-message** or **redirect-url**.

- **Content**: Content of the custom message; maximum length is 1024 ASCII characters.

You configure a user message or redirect URL as a custom object and assign the custom object to an EWF category.

- User messages indicate that website access has been blocked by an organization's access policy. To configure a user message, include the **type user-message content *message-text*** statement at the **[edit security utm custom-objects custom-message *message*]** hierarchy level.
- Redirect URLs redirect a blocked or quarantined URL to a user-defined URL. To configure a redirect URL, include the **type redirect-url content redirect-url** statement at the **[edit security utm custom-objects custom-message *message*]** hierarchy level.

The **custom-message** option provides the following benefits:

- You can configure a separate custom message or redirect URL for each EWF category.
- The **custom-message** option enables you to fine-tune messages to support your polices to know which URL is blocked or quarantined.

### Dynamic Support for New Websense EWF Categories

Starting with Junos OS Release 17.4R1, you can download and dynamically load new Enhanced Web Filtering (EWF) categories. The downloading and dynamic loading of the new EWF categories do not require a software upgrade. Websense occasionally releases new EWF categories. EWF classifies websites into categories according to host, URL, or IP address and performs filtering based on the categories. Users can leverage new categories as soon as they are available rather than waiting for a patch release.

> **NOTE:** Existing configurations are not affected by the new categories but can be modified to make use of the new categories.

SEE ALSO

Web Filtering Overview | 147

Understanding Local Web Filtering | 192

# Example: Enhancing Security by Configuring Redirect Web Filtering Using Custom Objects

IN THIS SECTION



This example shows how to manage Internet usage by configuring redirect Web filtering using custom objects and preventing access to inappropriate Web content.

## Requirements

Before you begin, learn more about Web filtering. See "Web Filtering Overview" on page 147.

## Overview

The benefit of using Web filtering is that it extracts the URLs from HTTP request messages and performs filtering according to the requirements. The advantage of configuring redirect Web filtering is that it extracts the URLs from the HTTP requests and sends them to an external URL filtering server to determine whether to allow or deny access.

In this example you configure redirect Web filtering custom objects, redirect Web filtering feature profiles, and redirect Web filtering UTM policies. You also attach redirect Web filtering UTM policies to security policies.

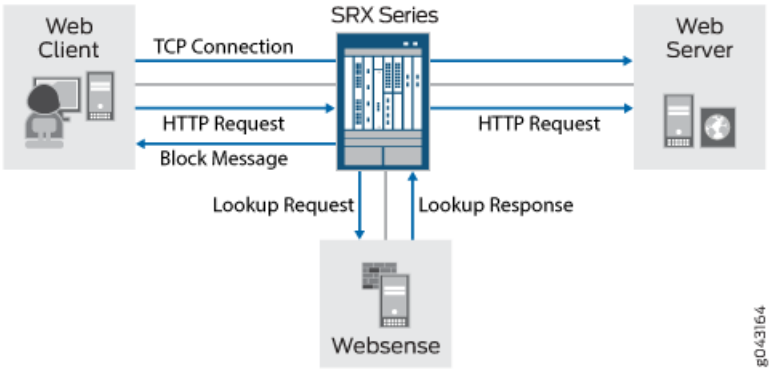
The default websense-redirect server port number is 15868.

You select fallback settings (block or log-and-permit) for this profile, in case errors occur in each configured category. This example sets fallback settings to block the profile. You enter the number of sockets used for communicating between the client and the server. The default is 32 for SRX Series devices.

Finally, you enter a timeout value in seconds. Once this limit is reached, fail mode settings are applied. The default is 15 seconds, and you can enter a value from 1 to 1800 seconds. This example sets the timeout value to 10.

Figure 3 on page 211 shows the overall architecture for the Websense redirect feature.

Figure 3: Websense Redirect Architecture




## Configuration

**IN THIS SECTION**



### *Configuring Redirect Web Filtering Custom Objects*

#### CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm custom-objects url-pattern urllist4 value 1.2.3.4
set security utm custom-objects url-pattern urllistblack value http://www.untrusted.com
set security utm custom-objects url-pattern urllistblack value 13.13.13.13
set security utm custom-objects url-pattern urllistwhite value http://www.trusted.com
set security utm custom-objects url-pattern urllistwhite value 7.7.7.7
set security utm custom-objects custom-url-category custurl4 value urllist4
set security utm custom-objects custom-url-category custblacklist value urllistblack
set security utm custom-objects custom-url-category custwhitelist value urllistwhite
```

**Step-by-Step Procedure**

To configure redirect Web filtering custom objects:

1. Create custom objects and create the URL pattern list.

```
[edit security utm]
user@host# set custom-objects url-pattern urllist4 value [http://www.example.net 1.2.3.4]
```

2. Configure the custom URL category list custom object using the URL pattern list.

```
[edit security utm]
user@host# set custom-objects custom-url-category custurl4 value urllist4
```

3. Create a list of untrusted sites

```
[edit security utm]
user@host# set custom-objects url-pattern urllistblack value [http://www.untrusted.com 13.13.13.13]
```

4. Configure the custom URL category list custom object using the URL pattern list of untrusted sites.

```
[edit security utm]
user@host# set custom-objects custom-url-category custblacklist value urllistblack
```

5. Create a list of trusted sites.

```
[edit security utm]
user@host# set custom-objects url-pattern urllistwhite value [http://www.trusted.com 7.7.7.7]
```

6. Configure the custom URL category list custom object using the URL pattern list of trusted sites.

```
[edit security utm]
user@host# set custom-objects custom-url-category custwhitelist value urllistwhite
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm custom-objects** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
userhost# show security utm custom-objects
url-pattern {
    urllist4 {
        value [ http://www.example.net 1.2.3.4 ];
    }
    urllistblack {
        value [ http://www.untrusted.com 13.13.13.13 ];
    }
    urllistwhite {
        value [ http://www.trusted.com 7.7.7.7 ];
    }
}
    custom-url-category {
        custurl4 {
            value urllist4;
        }
        custblacklist {
            value urllistblack;
        }
        custwhitelist {
            value urllistwhite;
        }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

***Configuring the Redirect Web Filtering Feature Profiles***

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm feature-profile web-filtering url-whitelist custwhitelist
set security utm feature-profile web-filtering url-blacklist custblacklist
set security utm feature-profile web-filtering type websense-redirect
set security utm feature-profile web-filtering websense-redirect profile websenseprofile1 server host
    Websenseserver
set security utm feature-profile web-filtering websense-redirect profile p1 category cust-white-list action
    log-and-permit
set security utm feature-profile web-filtering websense-redirect profile p1 category cust-list2 action permit
set security utm feature-profile web-filtering websense-redirect profile websenseprofile1 server port 15868
```

```
set security utm feature-profile web-filtering websense-redirect profile websenseprofile1 fallback-settings
    server-connectivity block
set security utm feature-profile web-filtering websense-redirect profile websenseprofile1 fallback-settings
    timeout block
set security utm feature-profile web-filtering websense-redirect profile websenseprofile1 fallback-settings
    too-many-requests block
set security utm feature-profile web-filtering websense-redirect profile websenseprofile1 timeout 10
set security utm feature-profile web-filtering websense-redirect profile websenseprofile1 sockets 1
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure redirect Web filtering feature profiles:

1. Configure the Web filtering URL blocklist.

   ```
   [edit security utm feature-profile web-filtering]
   user@host# set url-blacklist custblacklist
   ```

2. Configure the Web filtering URL allowlist.

   ```
   [edit security utm feature-profile web-filtering]
   user@host# set url-whitelist custwhitelist
   ```

3. Specify the Web filtering type, create a profile name, and set the server name or IP address.

   ```
   [edit security utm feature-profile web-filtering]
   user@host# set websense-redirect profile websenseprofile1 server host Websenseserver
   ```

4. Configure the custom category action **log-and-permit** and **permit** for the URL allowlist and cust-list2, respectively.

   ```
   [edit security utm feature-profile web-filtering]
   user@host# set websense-redirect profile websenseprofile1 category cust-white-list action log-and-permit
   user@host# set websense-redirect profile websenseprofile1 category cust-list2 action permit
   ```

5. Enter the port number for communicating with the server.

```
[edit security utm feature-profile web-filtering]
user@host# set websense-redirect profile websenseprofile1 server port 15868
```

6. Configure the fallback settings action **block**for this profile.

```
[edit security utm feature-profile web-filtering]
user@host# set websense-redirect profile websenseprofile1 fallback-settings default block
```

```
user@host# set websense-redirect profile websenseprofile1 fallback-settings server-connectivity block
user@host# set websense-redirect profile websenseprofile1 fallback-settings timeout block
user@host# set websense-redirect profile websenseprofile1 fallback-settings too-many-requests block
```

7. Enter the number of sockets used for communicating between the client and the server.

```
[edit security utm feature-profile web-filtering]
user@host# set websense-redirect profile websenseprofile1 sockets 1
```

8. Enter a timeout value, in seconds.

```
[edit security utm feature-profile web-filtering]
user@host# set .websense-redirect profile websenseprofile1 timeout 10
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm feature-profile** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
userhost# show security utm feature-profile
   web-filtering {
      url-whitelist custwhitelist;
      url-blacklist custblacklist;
      type websense-redirect {
         profile websenseprofile1 {
            server {
               host Websenseserver;
               port 15868;
               }
```

```
            category {
            cust-white-list {
            action log-and-permit ;
            cust-list2 {
            action permit;
            }
            }
          }
          fallback-settings {
            server-connectivity block;
            timeout block;
            too-many-requests block;
          }
          timeout 10;
          sockets 1;
        }
      }
    }
      content-filtering {
        profile contentfilter1;
      }
```

If you are done configuring the device, enter **commit** from configuration mode.

***Configuring Redirect Web Filtering UTM Policies and Attaching the Redirect Web Filtering UTM Policies to Security Policies***

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm utm-policy utmp6 web-filtering http-profile websenseprofile1
set security policies from-zone trust to-zone untrust policy p6 match source-address any
set security policies from-zone trust to-zone untrust policy p6 match destination-address any
set security policies from-zone trust to-zone untrust policy p6 match application junos-http
set security policies from-zone trust to-zone untrust policy p6 then permit application-services utm-policy
  utmp6
```

**Step-by-Step Procedure**

To configure a UTM policy and attach it to a security policy:

1. Create the UTM policy referencing a profile.

```
[edit security utm]
user@host# set utm-policy utmp6 web-filtering http-profile websenseprofile1
```

2. Create and configure the security policy.

```
[edit security policies from-zone trust to-zone untrust policy p6]
user@host# set match source-address any
user@host#  set match destination-address any
user@host# set match application junos-http
```

3. Attach the UTM policy to the security policy.

```
[edit security policies from-zone trust to-zone untrust policy p6]
user@host# set then permit application-services utm-policy utmp6
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
userhost# show security utm
utm-policy utmp6 {
   web-filtering {
      http-profile websenseprofile1;
   }
}
```

From configuration mode, confirm your configuration by entering the **show security policies** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
userhost# show security policies
   from-zone trust to-zone untrust {
      policy p6 {
         match {
            source-address any;
            destination-address any;
            application junos-http;
```

```
        }
        then {
            permit {
                application-services {
                    utm-policy utmp6;
                }
            }
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

**IN THIS SECTION**



To confirm that the configuration is working properly, perform these tasks:

### *Verifying the Configuration of Redirect Web Filtering Custom Objects*

#### Purpose

Verify the configuration of redirect Web filtering custom objects.

#### Action

From the top of the configuration in configuration mode, enter the **show security utm custom-objects** command.

```
[edit]
userhost# show security utm custom-objects
url-pattern {
    urllist4 {
        value [ http://www.example.net 1.2.3.4 ];
    }
    urllistblack {
```

```
            value [ http://www.untrusted.com 13.13.13.13 ];
        }
        urllistwhite {
            value [ http://www.trusted.com 7.7.7.7 ];
        }
    }
        custom-url-category {
            custurl4 {
                value urllist4;
            }
            custblacklist {
                value urllistblack;
            }
            custwhitelist {
                value urllistwhite;
            }
        }
```

**Meaning**

The sample output shows the list of custom objects created.

***Verifying the Configuration of Redirect Web Filtering Feature Profiles***

**Purpose**

Verify the configuration of redirect Web filtering feature profiles.

**Action**

From the top of the configuration in configuration mode, enter the **show security utm feature-profile** command.

```
[edit]
userhost# show security utm feature-profile
    web-filtering {
        url-whitelist custwhitelist;
        url-blacklist custblacklist;
        type websense-redirect {
            profile websenseprofile1 {
                server {
                    host Websenseserver;
                    port 15868;
                }
                fallback-settings {
                    server-connectivity block;
                    timeout block;
```

```
            too-many-requests block;
          }
          timeout 10;
          sockets 1;
        }
      }
    }
      content-filtering {
        profile contentfilter1;
      }
```

**Meaning**

The sample output shows the feature profile configured for a Websense redirect server.

***Verifying the Attachment of Redirect Web Filtering UTM Policies to Security Policies***

**Purpose**

Verify the attachment of the newly created redirect Web filtering UTM policies to the security policies.

**Action**

From the top of the configuration in configuration mode, enter the **show security utm** and **show security policies** commands.

```
[edit]
userhost# show security utm
utm-policy utmp6 {
  web-filtering {
    http-profile websenseprofile1;
  }
}
```

```
[edit]
userhost# show security policies
  from-zone trust to-zone untrust {
    policy p6 {
      match {
        source-address any;
        destination-address any;
        application junos-http;
      }
      then {
        permit {
          application-services {
```

```
                utm-policy utmp6;
            }
        }
    }
}
}
```

**Meaning**

The sample output shows the security policies to which the newly created redirect Web filtering UTM policies are attached.

SEE ALSO

- Example: Configuring Enhanced Web Filtering | **161**

**Release History Table**

| Release | Description |
|---|---|
| 17.4R1 | Starting with Junos OS Release 17.4R1, a new option, **custom-message**, is added for the **custom-objects** statement that enables you to configure user messages and redirect URLs to notify users when a URL is blocked or quarantined for each EWF category. |
| 17.4R1 | Starting with Junos OS Release 17.4R1, you can download and dynamically load new Enhanced Web Filtering (EWF) categories. |

RELATED DOCUMENTATION

- Enhanced Web Filtering | **149**
- Monitoring Web Filtering Configurations | **230**

# Safe Search Enhancement for Web Filtering


**SUMMARY**

Learn about our safe search enhancement for Unified Threat Management (UTM) Web filtering solutions to enforce the safest Web browsing mode available, by default.


**IN THIS SECTION**



## Safe Search Enhancement for Web Filtering Overview

**IN THIS SECTION**



### Benefits of Safe Search Enhancement for Web Filtering

- Provides the safest Web browsing mode available, by default.
- Protects the HTTPS-based search engine cache. This protection is a key security feature requirement for organizations with multiple Web users in educational, financial, health-care, banking, and corporate segments. In a campus or branch, enabling a default safe search solution for all users and blocking the search engine cache provides secure and comfortable Web browsing.

### Features of Safe Search Enhancement for Web Filtering

You use UTM Web filtering to manage Web browsing by preventing access to inappropriate Web content. To do this, you use the following Web filtering solutions:

- Redirect Web filtering

- Local Web filtering
- Enhanced Web Filtering (EWF)

We've enhanced the safe search functionality for these UTM Web filtering solutions to provide an extremely safe search environment for the Web user. Table 7 on page 223 describes the features of the safe search enhancement.

**Table 7: Safe Search Enhancement Features**

| Safe Search Feature | Description |
|---|---|
| Default safe search | By enabling the safe search enhancement feature, you enforce the safest Web browsing mode available by default on the well-known search engines. Doing so helps those users that are not using the strictest safe search settings.<br><br>If you enable the safe search feature on your security device, it enforces the search service to the strictest mode by URL query rewriting, which is transparent to you. For example, when you do a search request on the search engines Google, Bing, Yahoo, or Yandex, the safe search feature rewrites the requested URLs to the safest search URLs.<br><br>Here're a few examples of requested and converted URLs:<br><br>• Google search engine:<br>  ◦ Requested URL: https://www.google.com/search?q=test<br>  ◦ Converted URL: https://www.google.com/search?q=test&safe=active<br>• Bing search engine:<br>  ◦ Requested URL: https://www.bing.com/search?q=test<br>  ◦ Converted URL: https://www.bing.com/search?q=test&adlt=strict<br>• Yahoo search engine:<br>  ◦ Requested URL: https://search.yahoo.com/search?q=test<br>  ◦ Converted URL: https://search.yahoo.com/search?q=test&vm=r<br>• Yandex search engine:<br>  ◦ Requested URL: https://yandex.com/search/?text=test&lr=10619<br>  ◦ Converted URL: https://yandex.com/search/?text=test&lr=10619&filter=strict |
| Blocking search engine cache | By blocking the search engine cache on the well-known search engines, you can hide your Web-browsing activities from other users if you are a part of an organization that has multiple Web users in educational, financial, health-care, banking, and corporate segments.<br><br>To block the search engine cache, you configure a general URL block pattern and category for the search engine cache service. |

You can disable the safe search option at the Web filtering-level and profile-level configurations. See juniper-local, websense-redirect, and juniper-enhanced.

### Limitations of Safe Search Enhancement for Web Filtering

- For HTTP safe search enhancement, you must enable stream mode by enabling the **http-reassemble** option at the **[edit security utm default-configuration web-filtering]** hierarchy level. If you don't enable stream mode, you can't use the safe search feature. As a result, the system sends an HTTP 302 redirect message to the user.
- For HTTPS safe search enhancement, you must enable the SSL proxy service on the security policy. If SSL proxy bypasses the HTTPS traffic, then the safe search feature also bypasses the HTTPS traffic.

## Configure Web Filtering with Safe Search

**SUMMARY**

Use this example to configure UTM Web filtering solutions and verify the safe search enhancement for UTM Web filtering.

**IN THIS SECTION**



### Requirements

This example uses the following hardware and software components:

- An SRX Series device
- Junos OS Release 20.2R1

Before you begin:

- Make sure you understand how to use Web filtering to manage Web browsing. See Web Filtering Overview.
- Configure a Root CA Certificate. See Configuring a Root CA Certificate.

## Overview

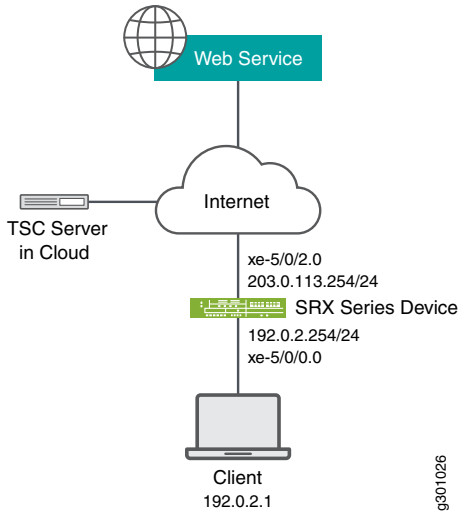
In this example, you configure the following policies and Web filtering profiles on your security device:

- UTM policies
- Security policies
- Web filtering profiles
- SSL proxy

After you've configured the policies and profiles, you generate the Web filtering statistics and verify the performance of the safe search enhancement.

Figure 4 on page 225 shows the basic UTM Web filtering topology. When you enable your security device with the safe search feature, the device rewrites the search requests from the user to the safest search mode of the search engines. The cloud engine or the local engine performs Web filtering on the search requests before forwarding to the Internet or external webserver.

**Figure 4: Topology for Web Filtering Basic Function**




## Configuration

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm default-configuration web-filtering type juniper-enhanced
```

```
set security utm default-configuration web-filtering http-reassemble
set security utm default-configuration web-filtering juniper-enhanced default log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile1 category
   Enhanced_Search_Engines_and_Portals action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile1 default log-and-permit
set security utm utm-policy utmpolicy1 web-filtering http-profile ewf_my_profile1
set security policies from-zone trust to-zone internet policy sec_policy match source-address any
set security policies from-zone trust to-zone internet policy sec_policy match destination-address any
set security policies from-zone trust to-zone internet policy sec_policy match application junos-ping
set security policies from-zone trust to-zone internet policy sec_policy match application junos-http
set security policies from-zone trust to-zone internet policy sec_policy then permit application-services utm-policy
   utmpolicy1
set security policies default-policy deny-all
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces xe-5/0/0.0
set security zones security-zone internet host-inbound-traffic system-services all
set security zones security-zone internet host-inbound-traffic protocols all
set security zones security-zone internet interfaces xe-5/0/2.0
set interfaces xe-5/0/0 unit 0 family inet address 192.0.2.254/24
set interfaces xe-5/0/2 unit 0 family inet address 203.0.113.254/24
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *Junos OS CLI User Guide*.

To configure UTM Web filtering:

1. Configure UTM Web filetring solution.

```
[edit security utm]
user@host# default-configuration web-filtering type juniper-enhanced
user@host# default-configuration web-filtering http-reassemble
user@host# default-configuration web-filtering juniper-enhanced default log-and-permit
user@host# feature-profile web-filtering juniper-enhanced profile ewf_my_profile1 category
   Enhanced_Search_Engines_and_Portals action log-and-permit
user@host# feature-profile web-filtering juniper-enhanced profile ewf_my_profile1 default log-and-permit
user@host# utm-policy utmpolicy1 web-filtering http-profile ewf_my_profile1
```

2. Configure the security policies to control HTTP or HTTPS traffic from the trust zone to the Internet zone.

```
[edit security policies]
```

```
user@host# from-zone trust to-zone internet policy sec_policy match source-address any
user@host# from-zone trust to-zone internet policy sec_policy match destination-address any
user@host# from-zone trust to-zone internet policy sec_policy match application junos-ping
user@host# from-zone trust to-zone internet policy sec_policy match application junos-http
user@host# from-zone trust to-zone internet policy sec_policy then permit application-services utm-policy
  utmpolicy1
user@host# default-policy deny-all
```

3. Configure security zones.

```
[edit security zones security-zone]
user@host# trust host-inbound-traffic system-services all
user@host# trust host-inbound-traffic protocols all
user@host# trust interfaces xe-5/0/0.0
user@host# internet host-inbound-traffic system-services all
user@host# internet host-inbound-traffic protocols all
user@host# internet interfaces xe-5/0/2.0
```

4. Configure interfaces.

```
[edit interfaces]
user@host# xe-5/0/0 unit 0 family inet address 192.0.2.254/24
user@host# xe-5/0/2 unit 0 family inet address 203.0.113.254/24
```

**Results**

From configuration mode, confirm your configuration by entering the **show security policies**, **show security utm**, and **show interfaces** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show security policies
from-zone trust to-zone internet {
   policy sec_policy {
      match {
         source-address any;
         destination-address any;
         application [ junos-ping junos-http ];
      }
      then {
         permit {
            application-services {
```

```
            utm-policy utmpolicy1;
          }
        }
      }
    }
}
default-policy {
    deny-all;
}
```

```
user@host# show security utm
default-configuration {
    web-filtering {
        http-reassemble;
        type juniper-enhanced;
        juniper-enhanced {
            default log-and-permit;
        }
    }
}
feature-profile {
    web-filtering {
        juniper-enhanced {
            profile ewf_my_profile1 {
                category {
                    Enhanced_Search_Engines_and_Portals {
                        action log-and-permit;
                    }
                }
                default log-and-permit;
            }
        }
    }
}
utm-policy utmpolicy1 {
    web-filtering {
        http-profile ewf_my_profile1;
    }
}
```

```
user@host# show interfaces
xe-5/0/0 {
    unit 0 {
```

```
        family inet {
            address 192.0.2.254/24;
        }
    }
}
xe-5/0/2 {
    unit 0 {
        family inet {
            address 203.0.113.254/24;
        }
    }
}
```

If you are done configuring the feature on your device, enter **commit** from configuration mode.

## Verification

### *Verify Safe Search Function*

#### Purpose

Verify that the safe search feature is enabled for UTM Web filtering solutions.

#### Action

From operational mode, enter the **show security utm web-filtering statistics** command to view the Web filtering statistics. In the output, the **Safe-search redirect** and **Safe-search rewrite** fields display the enhanced safe search redirect and rewrite statistics.

```
user@host> show security utm web-filtering statistics
```

```
UTM web-filtering statistics:
    Total requests:                   0
    white list hit:                   0
    Black list hit:                   0
    No license permit:                0
    Queries to server:                0
    Server reply permit:              0
    Server reply block:               0
    Server reply quarantine:          0
    Server reply quarantine block:    0
    Server reply quarantine permit:   0
    Custom category permit:           0
    Custom category block:            0
```

```
    Custom category quarantine:         0
    Custom category qurantine block:    0
    Custom category quarantine permit:  0
    Site reputation permit:             0
    Site reputation block:              0
    Site reputation quarantine:         0
    Site reputation quarantine block:   0
    Site reputation quarantine permit:  0
    Site reputation by Category         0
    Site reputation by Global           0
    Cache hit permit:                   0
    Cache hit block:                    0
    Cache hit quarantine:               0
    Cache hit quarantine block:         0
    Cache hit quarantine permit:        0
Safe-search redirect:               0
+Safe-search rewrite:               0
    SNI pre-check queries to server:    0
    SNI pre-check server responses:     0
    Web-filtering sessions in total:    64000
    Web-filtering sessions in use:      0
    Fallback:                       log-and-permit          block
          Default                                   0              0
          Timeout                                   0              0
     Connectivity                                   0              0
Too-many-requests                                   0              0
```

**Meaning**

The output displays that the safe search feature is enabled and there are no safe search redirects and safe search rewrites.

WHAT'S NEXT

> Now that you've learned about safe search enhancement for Web filtering, you'll be interested to know how to disable the safe search function. Check out juniper-local, websense-redirect, and juniper-enhanced for more information.

# Monitoring Web Filtering Configurations

**Purpose**

View Web-filtering statistics.

**Action**

To view Web-filtering statistics using the CLI, enter the following commands:

```
user@host> show security utm web-filtering status
user@host> show security utm web-filtering statistics
```

To view Web-filtering statistics using J-Web:

1. Select **Clear Web Filtering Statistics**.

   The following information is displayed in the right pane.

   ```
   Total Requests: #
   White List Hit: #
   Black List Hit: #
   Queries to Server: #
   Server Reply Permit: #
   Server Reply Block: #
   Custom Category Permit: #
   Custom Category Block: #
   Cache Hit Permit: #
   Cache Hit Block: #
   Web Filtering Session Total: #
   Web Ffiltering Session Inuse: #
   Fall Back: Log-and-Permit Block
   Default # #
   Timeout # #
   Server-Connectivity # #
   Too-Many-Requests # #
   ```

2. You can click the **Clear Web Filtering Statistics** button to clear all current viewable statistics and begin collecting new statistics.

## RELATED DOCUMENTATION

Web Filtering Overview | 147

Example: Configuring Enhanced Web Filtering | 161

CHAPTER 6

# UTM Support for SRX100, SRX110, SRX210, SRX240, SRX550, SRX650, and SRX1400 Devices

# Express Antivirus Protection

IN THIS SECTION



Express antivirus scanning is offered as a less CPU intensive alternative to the full file-based antivirus feature. Express antivirus supports the same protocols as full antivirus and functions in much the same manner. For more information, see the following topics:

## Express Antivirus Protection Overview

IN THIS SECTION

The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, Express antivirus scanning is offered as a less CPU intensive alternative to the full file-based antivirus feature. Express antivirus supports the same protocols as full antivirus and functions in much the same manner, however, it has a smaller memory footprint, compatible with the smaller system memory present on lower end devices. The express antivirus feature, like the full antivirus feature, scans specific Application Layer traffic for viruses against a virus signature database. However, unlike full antivirus, express antivirus does not reconstruct the original application content. Rather, it just sends (streams) the received data packets, as is, to the scan engine. With express antivirus, the virus scanning is executed by a hardware pattern matching engine. This improves performance while scanning is occurring, but the level of security provided is lessened. Juniper Networks provides the scan engine. The express antivirus scanning feature is a separately licensed subscription service.

This topic includes the following sections:

### Express Antivirus Packet-Based Scanning Versus File-Based Scanning

Express antivirus uses a different antivirus scan engine than the full file-based antivirus feature and a different back-end hardware engine to accelerate pattern matching for higher data throughput.

The packet-based scanning done by express antivirus provides virus scanning data buffers without waiting for entire file to be received by the firewall, whereas the file-based scanning done by full antivirus can only start virus scanning when entire file is received.

### Express Antivirus Expanded MIME Decoding Support

Express antivirus offers MIME decoding support for HTTP, POP3, SMTP, and IMAP. MIME decoding support includes the following for each supported protocol:

- Multi-part and nested header decoding
- Base64 decoding, printed quote decoding, and encoded word decoding (in the subject field)

### Express Antivirus Scan Result Handling

With express antivirus, the TCP traffic is closed gracefully when a virus is found and the data content is dropped.

Express antivirus supports the following fail mode options: default, engine-not-ready, out-of-resource, and too-many-requests. Fail mode handling of supported options with express antivirus is much the same as with full antivirus.

### Express Antivirus Intelligent Prescreening

Intelligent prescreening functionality is identical in both express antivirus and full antivirus.

### Express Antivirus Limitations

Express antivirus has the following limitations when compared to full antivirus functionality:

- Express antivirus provides limited support for the scanning of file archives and compressed file formats. Express antivirus can only support gzip, deflate and compressed compressing formats.
- Express antivirus provides limited support for decompression. Decompression is only supported with HTTP (supports only gzip, deflate, and compress for HTTP and only supports one layer of compression) and POP3 (supports only gzip for POP3 and only supports one layer of compression).
- Express antivirus does not support scanning by extension.
- Express antivirus scanning is interrupted when the scanning database is loading.
- Express antivirus may truncate a warning message if a virus has been detected and the replacement warning message that is sent is longer than the original content it is replacing.
- If you switch from express antivirus protection to full file-based antivirus protection, you must reboot the device in order for full file-based antivirus to begin working.
- Because express antivirus does only packet-based string matching, if you use the standard EICAR file to test express antivirus, you will see false positives. To avoid these false positives, Juniper Networks has disabled scanning on the standard EICAR file to create a modified EICAR file for testing express antivirus. You can download this modified EICAR file from the following links:

  https://www.juniper.net/security/avtest/ss-eicar.txt

  https://www.juniper.net/security/avtest/ss-eicar.com

  https://www.juniper.net/security/avtest/ss-eicar.zip
- The modified EICAR file must be tested with express antivirus only. The Kaspersky antivirus and Sophos antivirus do not detect this file.
- The express antivirus feature provides better performance but lower security. If you switch from full file-based antivirus protection to express antivirus protection, you must reboot the device in order for express antivirus to begin working.

SEE ALSO

Understanding Express Antivirus Scanner Pattern Updates | 258

Example: Automatically Updating Express Antivirus Patterns | 259

Understanding the Full Antivirus Scan Engine | 298

## Express Antivirus Configuration Overview

The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, for each UTM feature, you should configure feature parameters in the following order:

1. Configure UTM custom objects for the UTM features. The following example enables the mime-pattern, url-pattern, and custom-url-category custom objects:

```
user@host# set security utm custom-objects mime-pattern
user@host# set security utm custom-objects url-pattern
user@host# set security utm custom-objects custom-url-category
```

2. Configure main feature parameters using feature profiles. The following examples enables the anti-virus feature profile:

```
user@host# set security utm feature-profile anti-virus juniper-exress-engine
```

3. Configure a UTM policy for each protocol and attach this policy to a profile. The following example creates the utmp3 UTM policy for the HTTP protocol:

```
user@host# set security utm utm-policy utmp3 anti-virus http-profile http1
```

4. Attach the UTM policy to a security policy. The following example attaches the utmp3 UTM policy to the p3 security policy:

```
user@host# set security policies from-zone trust to-zone untrust policy p3 then permit application-services
    utm-policy utmp3
```

## Example: Configuring Express Antivirus Custom Objects

**IN THIS SECTION**

The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, this example shows how to configure express antivirus custom objects.

## Requirements

Before you begin:

- Decide the type of express antivirus protection you require. See "Express Antivirus Protection Overview" on page 233.
- Understand the order in which express antivirus parameters are configured. See "Express Antivirus Configuration Overview" on page 236.

## Overview

In this example, you define custom objects that are used to create express antivirus feature profiles. You perform the following tasks to define custom objects:

- Create two MIME lists called avmime2 and ex-avmime2, and add patterns to the list.
- Configure a URL pattern list called urllist2.

  When entering the URL pattern, note the following wildcard character support:

  - The *\.[]\?* wildcard characters are supported.
  - You must precede all wildcard URLs with http://.
  - You can use the asterisk * wildcard character only if it is at the beginning of the URL and is followed by a period.
  - You can use the question mark ? wildcard character only at the end of the URL.
  - The following wildcard syntax is supported: http://*.example.net, http://www.example.ne?, http://www.example.n??.
  - The following wildcard syntax is not supported: *.example.net , www.example.ne?, http://*example.net, http://* .
  - Configure a custom URL category list called custurl2, using the urllist2 URL pattern list.

## Configuration

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm custom-objects mime-pattern avmime2 value [video/quicktime image/x-portable-anymap
    x-world/x-vrml]
set security utm custom-objects mime-pattern ex-avmime2 value [video/quicktime-inappropriate]
set security utm custom-objects url-pattern urllist2 value [http://www.example.net 1.2.3.4]
set security utm custom-objects custom-url-category custurl2 value urllist2
```

### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure express antivirus filtering custom objects:

1. Create MIME lists, and add MIME patterns to the lists. As you use URL pattern lists to create custom URL category lists, you must configure URL pattern list custom objects before you configure custom URL category list.

   ```
   [edit security utm]
   user@host# set custom-objects mime-pattern avmime2 value [video/quicktime image/x-portable-anymap
       x-world/x-vrml]
   user@host# set custom-objects mime-pattern ex-avmime2 value [video/quicktime-inappropriate]
   ```

2. Configure a URL pattern list custom object.

   ```
   [edit security utm]
   user@host# set custom-objects url-pattern urllist2 value [http://www.example.net 1.2.3.4]
   ```

3. Configure a custom URL category list.

   ```
   [edit security utm]
   user@host# set custom-objects custom-url-category custurl2 value urllist2
   ```

### Results

From configuration mode, confirm your configuration by entering the **show security utm** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security utm
custom-objects {
    mime-pattern {
        avmime2 {
            value [ video/quicktime image/x-portable-anymap x-world/x-vrml ];
        }
        ex-avmime2 {
            value video/quicktime-inappropriate;
        }
    }
    url-pattern {
        urllist2 {
            value [ http://www.example.net 1.2.3.4 ];
        }
    }
    custom-url-category {
        custurl2 {
            value urllist2;
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### *Verifying Express Antivirus Custom Objects*

#### Purpose

Verify the express antivirus custom objects.

#### Action

From operational mode, enter the **show configuration security utm** command.

## Configuring Express Antivirus Custom Objects (J-Web Procedure)

The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, to configure express antivirus protection using the J-Web configuration editor, you must first create your custom objects (MIME pattern list, URL pattern list, and custom URL category list).

Configure a MIME pattern list custom object as follows:

1. Select **Configure>Security>UTM Custom Objects**.

2. From the MIME Pattern List tab, click **Add** to create MIME pattern lists.

3. In the Add MIME Pattern pop-up window, next to **MIME Pattern Name**, enter a unique name.

   Keep in mind that you are creating a MIME allowlist and a MIME exception list (if necessary). Both MIME lists appear in the MIME Allowlist and Exception MIME Allowlist fields when you configure antivirus. Therefore, the MIME list names you create should be as descriptive as possible.

4. Next to MIME Pattern Value, enter the MIME pattern.

5. Click **Add** to add your MIME pattern to the Values list box. Within this box, you can also select an entry and use the Delete button to delete it from the list. Continue to add MIME patterns in this manner.

6. Optionally, create a new MIME list to act as an exception list. The exception list is generally a subset of the main MIME list.

7. Click **OK** to check your configuration and save the selected values as part of the MIME list, then click **Commit Options**>**Commit**.

8. If the configuration item is saved successfully, you receive a confirmation and you must click **OK** again. If it is not saved successfully, you can click **Details** in the pop-up window that appears to discover why.

Configure a URL pattern list custom object as follows:

> **NOTE:** Because you use URL pattern lists to create custom URL category lists, you must configure URL pattern list custom objects before you configure a custom URL category list.

1. Select **Configure>Security>UTM>Custom Objects**.

2. From the URL Pattern List tab, click **Add** to create URL pattern lists.

3. Next to URL Pattern Name, enter a unique name. This name appears in the Custom URL Category List Custom Object page for selection.

4. Next to URL Pattern Value, enter the URL or IP address you want added to list for bypassing scanning.

   When entering the URL pattern, note the following wildcard character support:

   - The ***\.[]\?*** wildcard characters are supported.
   - You must precede all wildcard URLs with **http://**.
   - You can only use the asterisk * wildcard character if it is at the beginning of the URL and is followed by a period.
   - You can only use the question mark **?** wildcard character at the end of the URL.
   - The following wildcard syntax IS supported: **http://*.example.net**, **http://www.example.ne?**, **http://www.example.n??**.
   - The following wildcard syntax is NOT supported: ***.example.net** , **www.example.ne?**, **http://*example.net, http://***.

5. Click **Add** to add your URL pattern to the Values list box. The list can contain up to 8192 items. You can also select an entry and use the Delete button to delete it from the list. Continue to add URLs or IP addresses in this manner.

6. Click **OK** to check your configuration and save the selected values as part of the URL pattern list, then click **Commit Options**>**Commit**.

7. If the configuration item is saved successfully, you receive a confirmation and you must click **OK** again. If it is not saved successfully, you can click **Details** in the pop-up window that appears to discover why.

Configure a custom URL category list custom object using the URL pattern list that you created:

1. Select **Configure>Security>UTM>Custom Objects**.

2. From the URL Category List tab, click **Add** to create URL category lists.

3. Next to URL Category Name, enter a unique name. This name appears in the URL Allowlist list when you configure antivirus global options.

4. In the Available Values box, select a **URL Pattern List** name from the list for bypassing scanning and click the right arrow button to move it to the Selected Values box.

5. Click **OK** to check your configuration and save the selected values as part of the URL list, then click **Commit Options**>**Commit**.

6. If the configuration item is saved successfully, you receive a confirmation and you must click **OK** again. If it is not saved successfully, you can click **Details** in the pop-up window that appears to discover why.

SEE ALSO

Understanding MIME Allowlist | 50

Example: Configuring MIME Allowlist to Bypass Antivirus Scanning | 51

## Example: Configuring Express Antivirus Feature Profiles

IN THIS SECTION



The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, this example shows how to configure an express antivirus feature profile.

### Requirements

Before you begin:

- Decide the type of express antivirus protection you require. See “Express Antivirus Protection Overview” on page 233.
- Understand the order in which express antivirus parameters are configured. See “Express Antivirus Configuration Overview” on page 236.
- MIME patterns must be defined for lists and exception lists. See “Example: Configuring MIME Allowlist to Bypass Antivirus Scanning” on page 51.
- Custom objects must be defined. See “Example: Configuring Express Antivirus Custom Objects” on page 236
- SMTP must be configured on the device. See “Understanding SMTP Antivirus Scanning” on page 328

### Overview

In this example, you configure a feature profile called junexprof1 and specify custom objects to be used for filtering content.

- Select and configure the Juniper Express Engine as the engine type.
- Select 120 as the time interval for updating the pattern database. The default antivirus pattern-update interval is once a day.

> **NOTE:** The command for changing the URL for the pattern database is:
>
> ```
> [edit]
> user@host# set security utm feature-profile anti-virus juniper-express-engine pattern-update url
>    http://...
> ```
>
> Under most circumstances, you should not need to change the default URL.

- Enable an e-mail notification with a custom message as pattern file was updated and a custom subject line as AV pattern file updated.
- Configure a list of fallback options as block.
- Configure the notification options for fallback blocking for virus detection. Configure a custom message for the fallback blocking action, and send a notification.
- Configure a notification for protocol-only virus detection, and send a notification as Antivirus Alert.

- Configure content size parameters as 20000. For SRX100, SRX110, SRX210, SRX220, and SRX240 devices, the maximum value for content size is 20,000. For SRX650 devices, the maximum value for content size is 40,000. Platform support depends on the Junos OS release in your installation.
- Enable intelligent prescreening and set its timeout setting to 1800 seconds and trickling setting (applicable only to HTTP) to 600 seconds. This means that if the device receives a packet within a 600-second period during a file transfer or while performing an antivirus scan, it should not time out.

  Intelligent prescreening is intended only for use with non-encoded traffic. It is not applicable to mail protocols (SMTP, POP3, IMAP) or HTTP POST.
- Configure the antivirus scanner to use MIME bypass lists and exception lists. You can use your own custom object lists, or you can use the default list, called junos-default-bypass-mime, which ships with the device. The following example enables the avmime2 and ex-avmime2 lists.
- Configure the antivirus module to use URL bypass lists. If you are using a URL allowlist (valid only for HTTP traffic), this is a custom URL category that you previously configured as a custom object. For this example, you enable the custurl1 bypass list.

## Configuration

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm feature-profile anti-virus juniper-express-engine pattern-update interval 120
set security utm feature-profile anti-virus juniper-express-engine pattern-update email-notify admin-email
    administrator@example.net custom-message “pattern file was updated” custom-message-subject “AV pattern
    file updated”
set security utm feature-profile anti-virus juniper-express-engine profile junexprof1 fallback-options content-size
    block
set security utm feature-profile anti-virus juniper-express-engine profile junexprof1 fallback-options default
    block
set security utm feature-profile anti-virus juniper-express-engine profile junexprof1 fallback-options
    engine-not-ready block
set security utm feature-profile anti-virus juniper-express-engine profile junexprof1 fallback-options
    out-of-resources block
set security utm feature-profile anti-virus juniper-express-engine profile junexprof1 fallback-options timeout
    block
set security utm feature-profile anti-virus juniper-express-engine profile junexprof1 fallback-options
    too-many-requests block
set security utm feature-profile anti-virus juniper-express-engine profile junexprof1 notification-options
    fallback-block custom-message “Dropped due to fallback condition”
```

```
set security utm feature-profile anti-virus juniper-express-engine profile junexprof1 notification-options
    virus-detection type protocol-only
set security utm feature-profile anti-virus juniper-express-engine profile junexprof1 notification-options
    virus-detection custom-message ***virus-found***
set security utm feature-profile anti-virus juniper-express-engine profile junexprof1 scan-options
    content-size-limit 20000
set security utm feature-profile anti-virus juniper-express-engine profile junexprof1 scan-options
    intelligent-prescreening
set security utm feature-profile anti-virus juniper-express-engine profile junexprof1 scan-options timeout 1800
set security utm feature-profile anti-virus juniper-express-engine profile junexprof1 trickling timeout 600
set security utm feature-profile anti-virus mime-whitelist list avmime2
set security utm feature-profile anti-virus mime-whitelist list avmime2 exception ex-avmime2
set security utm feature-profile anti-virus url-whitelist custurl2
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure express antivirus feature profiles:

1. Select and configure the engine type.

   ```
   [edit]
   user@host# set security utm feature-profile anti-virus type juniper-express-engine
   ```

2. Select a time interval for updating the pattern database.

   ```
   [edit security utm feature-profile anti-virus juniper-express-engine]
   user@host# set pattern-update interval 120
   ```

3. Configure the device to notify a specified administrator when patterns are updated.

   ```
   [edit security utm feature-profile anti-virus juniper-express-engine]
   user@host# set pattern-update email-notify admin-email administrator@example.net custom-message
       “pattern file was updated” custom-message-subject “AV pattern file updated”
   ```

4. Create a profile for the Juniper Express Engine, and configure fallback options as block.

   ```
   [edit security utm feature-profile anti-virus juniper-express-engine]
   user@host# set profile junexprof1 fallback-options content-size block
   user@host# set profile junexprof1 fallback-options default block
   ```

```
user@host# set profile junexprof1 fallback-options engine-not-ready block
user@host# set profile junexprof1 fallback-options out-of-resources block
user@host# set profile junexprof1 fallback-options timeout block
user@host# set profile junexprof1 fallback-options too-many-requests block
```

5. Configure a custom notification for the fallback blocking action, and send a notification.

```
[edit security utm feature-profile anti-virus juniper-express-engine]
user@host# set profile junexprof1 notification-options fallback-block custom-message “Dropped due to
   fallback condition”
```

6. Configure a notification for protocol-only virus detection, and send a notification.

```
[edit security utm feature-profile anti-virus juniper-express-engine]
user@host# set profile junexprof1 notification-options virus-detection type protocol-only
```

7. Configure a custom notification for virus detection.

```
[edit security utm feature-profile anti-virus juniper-express-engine]
set profile junexprof1 notification-options virus-detection custom-message ***virus-found***
```

8. Configure content size parameter.

```
[edit security utm feature-profile anti-virus juniper-express-engine]
user@host# set profile junexprof1 scan-options content-size-limit 20000
```

9. Configure intelligent prescreening.

```
[edit security utm feature-profile anti-virus juniper-express-engine]
user@host# set profile junexprof1 scan-options intelligent-prescreening
```

10. Configure the timeout setting.

```
[edit security utm feature-profile anti-virus juniper-express-engine]
user@host# set profile junexprof1 scan-options timeout 1800
```

11. Configure trickling setting.

```
[edit security utm feature-profile anti-virus juniper-express-engine]
user@host# set profile junexprof1 trickling timeout 600
```

12. Configure the antivirus scanner to use MIME bypass lists and exception lists.

```
[edit security utm feature-profile anti-virus]
user@host# set mime-whitelist list avmime2
user@host# set mime-whitelist list avmime2 exception ex-avmime2
```

13. Configure the antivirus module to use URL bypass lists.

```
[edit security utm feature-profile anti-virus]
user@host# set url-whitelist custurl2
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm feature-profile anti-virus** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security utm feature-profile anti-virus
mime-whitelist {
    list avmime2;
    exception ex-avmime2;
}
url-whitelist custurl2;
juniper-express-engine {
    pattern-update {
        email-notify {
            admin-email "administrator@example.net";
            custom-message "pattern file was updated";
            custom-message-subject "AV pattern file updated";
        }
        interval 120;
    }
    profile junexprof1 {
        fallback-options {
            default block;
            content-size block;
            engine-not-ready block;
```

```
            timeout block;
            out-of-resources block;
            too-many-requests block;
        }
        scan-options {
            intelligent-prescreening;
            content-size-limit 20000;
            timeout 1800;
        }
        trickling timeout 600;
        notification-options {
            virus-detection {
                type protocol-only;
                custom-message ***virus-found***;
            }
            fallback-block {
                custom-message “Dropped due to fallback condition”;
            }
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### *Verifying the Configuration of Express Antivirus Feature Profile*

#### Purpose

Verify the express antivirus feature profile.

#### Action

From operational mode, enter any of the following commands:

- **show configuration security utm**
- **show security utm anti-virus status**
- **show security utm anti-virus statistics**

SEE ALSO

Understanding Full Antivirus Application Protocol Scanning | 324

Understanding Express Antivirus Scanner Pattern Updates | 258

## Configuring Express Antivirus Feature Profiles (J-Web Procedure)

The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, after you create your custom objects, configure the antivirus feature profile:

1. Select Configure>Security>UTM>Global options.
2. In the Anti-Virus tab, next to MIME allowlist, select the custom object you created from the list.
3. Next to Exception MIME allowlist, select the custom object you created from the list.
4. Next to URL Allowlist, select the custom object you created from the list.
5. In the Engine Type section, select the type of engine you are using. For express antivirus protection, you should select Juniper Express.
6. Next to Pattern update URL, enter the URL for the pattern database in the box. Note that the URL is http://update.juniper-updates.net/EAV/<device version> and you should not change it.
7. Next to Pattern update interval, enter the time interval for automatically updating the pattern database in the box. The default for express antivirus checking is once per day.
8. Select whether you want the pattern file to update automatically (Auto update) or not (No Auto update).
9. Click OK to save the selected values.
10. If the configuration item is saved successfully, you receive a confirmation and you must click OK again. If it is not saved successfully, you can click Details in the pop-up window that appears to discover why.
11. Under Security, in the left pane, select Anti-Virus.
12. Click Add in the right window to create a profile for the antivirus Juniper Express Engine. To edit an existing item, select it and click **Edit**.
13. In the Main tab, next to Profile name, enter a unique name for this antivirus profile.
14. Select the Profile Type. In this case, select Juniper Express.
15. Next to Trickling timeout, enter timeout parameters.

Trickling applies only to HTTP. HTTP trickling is a mechanism used to prevent the HTTP client or server from timing out during a file transfer or during antivirus scanning.

16. Next to Intelligent prescreening, select Yes or No.

    Intelligent prescreening is only intended for use with non-encoded traffic. It is not applicable for mail protocols (SMTP, POP3, IMAP, and HTTP POST).

17. Next to Content Size Limit, enter content size parameters. The content size check occurs before the scan request is sent. The content size refers to accumulated TCP payload size.

18. Next to Scan engine timeout, enter scanning timeout parameters.

19. Select the Fallback settings tab.

20. Next to Default (fallback option), select Log and permit or Block from the list. In most cases, Block is the default fallback option.

21. Next to Decompress Layer (fallback option), select Log and permit or Block from the list.

22. Next to Content Size (fallback option), select Log and permit or Block from the list.

23. Next to Engine Not Ready (fallback option), select Log and permit or Block from the list.

24. Next to Timeout (fallback option), select Log and permit or Block from the list.

25. Next to Out of Resource (fallback option), select Log and permit or Block from the list.

26. Next to Too Many Requests (fallback option), select Log and permit or Block from the list.

27. Select the Notification options tab.

28. In the Fallback block section, next to Notification type, select Protocol Only or Message to select the type of notification that is sent when a fallback option of block is triggered.

29. Next to Notify mail sender, select Yes or No.

30. If you selected Yes, next to Custom Message, enter text for the message body of your custom message for this notification (if you are using a custom message).

31. Next to Custom message subject, enter text to appear in the subject line of your custom message for this notification (if you are using a custom message).

32. In the Fallback non block section, next to Notify mail recipient, select Yes or No.

33. If you selected Yes, next to Custom Message, enter text for the message body of your custom message for this notification (if you are using a custom message).

34. Next to Custom message subject, enter text to appear in the subject line of your custom message for this notification (if you are using a custom message).

35. Select the Notification options cont tab.

36. In the Virus detection section, next to Notification type, select Protocol Only or Message to select the type of notification that is sent when a fallback option of block is triggered.

37. Next to Notify mail sender, select Yes or No.

38. If you selected Yes, next to Custom Message, enter text for the message body of your custom message for this notification (if you are using a custom message).

39. Next to Custom message subject, enter text to appear in the subject line of your custom message for this notification (if you are using a custom message). The limit is 255 characters.

40. Click OK to check your configuration and save it as a candidate configuration, then click Commit Options>Commit.

41. If the configuration item is saved successfully, you receive a confirmation and you must click OK again. If it is not saved successfully, you can click Details in the pop-up that appears window to discover why.

    You create a separate antivirus profile for each antivirus protocol. These profiles may basically contain the same configuration information, but when you are creating your UTM policy for antivirus, the UTM policy configuration page provides separate antivirus profile selection fields for each supported protocol.

SEE ALSO

Understanding HTTP Trickling | **105**

# Example: Configuring Express Antivirus UTM Policies

IN THIS SECTION



The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, this example shows how to create an express antivirus UTM policy to attach to your feature profile.

## Requirements

Before you begin, create an antivirus feature profile. See "Example: Configuring Express Antivirus Feature Profiles" on page 242.

## Overview

In this example, you configure an express antivirus UTM policy called utmp3 and attach the policy to the antivirus profile called junexprof1.

## Configuration

### Step-by-Step Procedure

To configure an express antivirus UTM policy:

1. Create a UTM policy for HTTP antivirus scanning and attach the policy to the profile.

```
[edit]
user@host# set security utm utm-policy utmp3 anti-virus http-profile junexprof1
```

2. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

### Verification

To verify the configuration is working properly, enter the **show security utm** command.

## Configuring Express Antivirus UTM Policies (J-Web Procedure)

The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, after you have created an antivirus feature profile, configure a UTM policy to which you can attach the feature profile:

1. Select **Configure>Security>Policy>UTM Policies**.
2. From the UTM policy configuration window, click **Add** to configure a UTM policy. The policy configuration pop-up window appears.
3. Select the **Main** tab.
4. In the **Policy name** box, enter a unique name.
5. In the **Session per client limit** box, enter a session per client limit from 0 to 20000 for this UTM policy.
6. In the Session per client over limit list, select the action that the device should take when the session per client limit for this UTM policy is exceeded. Options include **Log and permit** and **Block**.
7. Select the **Anti-Virus profiles** tab.
8. Select the appropriate profile you have configured from the list for the corresponding protocol listed.
9. Click **OK**.
10. If the policy is saved successfully, you receive a confirmation and you must click **OK** again. If the profile is not saved successfully, you can click **Details** in the pop-up window that appears to discover why.

# Example: Attaching Express Antivirus UTM Policies to Security Policies

IN THIS SECTION



The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, this example shows how to attach an express antivirus UTM policy to a security policy.

## Requirements

Before you begin, create a UTM policy. See "Example: Configuring Express Antivirus UTM Policies" on page 252.

## Overview

In this example, you attach the express antivirus UTM policy called utmp3 to the security policy called p3.

## Configuration

### Step-by-Step Procedure

To attach an express antivirus UTM policy to a security policy:

1. Enable and configure the security policy.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy p3 match source-address any
user@host# set security policies from-zone trust to-zone untrust policy p3 match destination-address any
user@host# set security policies from-zone trust to-zone untrust policy p3 match application junos-http
```

2. Attach the UTM policy to the security policy.

```
[edit]
```

```
user@host# set security policies from-zone trust to-zone untrust policy p3 then permit application-services
  utm-policy utmp3
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

### Verification

To verify the configuration is working properly, enter **show security policies detail** from operational mode.

## Attaching Express Antivirus UTM Policies to Security Policies (J-Web Procedure)

The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, after you create a UTM policy, create a security policy and attach the UTM policy to the security policy:

1. Select **Configure>Security>Policy>FW Policies**.
2. From the Security Policy window, click **Add** to configure a security policy with UTM. The policy configuration pop-up window appears.
3. In the Policy tab, enter a name in the **Policy Name** box.
4. Next to Default Policy Action, select one of the following: **Deny-All** or **Permit-All**.
5. Next to **From Zone**, select a zone from the list.
6. Next to **To Zone**, select a zone from the list.
7. Under Zone Direction, click **Add a Policy**.
8. Choose a **Source Address**.
9. Choose a **Destination Address**.

10. Choose an application by selecting **junos-*protocol*** (for all protocols that support antivirus scanning) in the Application Sets box and clicking the —> button to move it to the Matched box.

11. Next to Policy Action, select **Permit**.

    When you select Permit for Policy Action, several additional fields become available in the Applications Services tab, including UTM Policy.

12. Select the **Application Services** tab.

13. Next to **UTM Policy**, select the appropriate policy from the list. This action attaches your UTM policy to the security policy.

14. Click **OK**.

15. Click **OK** to check your configuration and save it as a candidate configuration, then click **Commit Options**>**Commit**.

16. If the policy is saved successfully, you receive a confirmation and you must click **OK** again. If the profile is not saved successfully, you can click **Details** in the pop-up window that appears to discover why.

    You must activate your new policy to apply it.

**Release History Table**

| Release | Description |
|---|---|
| 15.1X49-D10 | The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |

## RELATED DOCUMENTATION


Full Antivirus Scan Results and Fallback Options | 313

HTTP Trickling to Prevent Timeouts | 105

Full Antivirus Protection | 262

# Express Antivirus Pattern Updates

IN THIS SECTION



The express antivirus pattern database is updated over HTTP or HTTPS and can occur automatically or manually. For more information, see the following topics:

## Understanding Express Antivirus Scanner Pattern Updates

The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, Express antivirus uses a different signature database than the full antivirus signature database. The express antivirus signature database is called Juniper Express antivirus database and it is compatible with the hardware engine. The express signature database targets only critical viruses and malware, including worms, Trojans, and spyware. This is a smaller sized database, providing less coverage than the full antivirus signature database.

The express antivirus pattern database is updated over HTTP or HTTPS and can occur automatically or manually. This is similar functionality to that found in full antivirus with some minor differences:

- With express antivirus, the signature database auto-update interval, is once a day.
- With express antivirus, there is no support for the downloading of multiple database types.
- With express antivirus, during database loading, all scan operations are interrupted. Scan operations for existing traffic flows are stopped and no new scan operations are initiated for newly established traffic flows. You can specify the desired action for this interruption period using the fall-back parameter for engine-busy-loading-database. The available actions are block or log-and-permit.
- By default, the URL for express antivirus is *http://update.juniper-updates.net/EAV/SRX-platform-name* where *SRX-platform-name* is the name of your device. If your device is an SRX210, then the URL for express antivirus would be http://update.juniper-updates.net/EAV/SRX210. The *SRX-platform-name* part of the URL is different and platform-specific. (Other than the platform name, you should not change

this URL unless you are experiencing problems with it and have called for support. Platform support depends on the Junos OS release in your installation.)

Once your subscription expires, you have a 30 day grace period during which you can continue to update the antivirus pattern file. Once that grace period expires, the update server no longer permits antivirus pattern file updates.

The express Antivirus scanning feature is a separately licensed subscription service. When your antivirus license key expires, you can continue to use locally stored antivirus signatures. But in that case, if the local database is deleted, antivirus scanning is disabled.

SEE ALSO

Understanding the Full Antivirus Scan Engine | 298

## Example: Automatically Updating Express Antivirus Patterns

**IN THIS SECTION**



The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, this example shows how to update the pattern file automatically on a security device.

### Requirements

Before you begin:

- Obtain a valid antivirus scanner license. See "Full Antivirus Protection Overview" on page 262.
- Get network connectivity and access to the pattern database server. See "Understanding Full Antivirus Pattern Updates" on page 288.
- Configure your DNS settings and port settings (port 80) correctly. See *DNS Overview*.

### Overview

In this example, you configure the security device to update the pattern file automatically every 120 minutes. (The default antivirus pattern-update interval is once a day.)

### Configuration

#### Step-by-Step Procedure

To configure the security device to update the pattern file automatically:

1. Set the interval.

```
[edit]
user@host# set security utm feature-profile anti-virus juniper-express-engine pattern-update interval 120
```

2. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

### Verification

To verify the configuration is working properly, enter the **show security utm** command.

## Example: Automatically Updating Express Antivirus Patterns (J-Web Procedure)

The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, in this example, you configure the security device to update the pattern file automatically every 120 minutes. (The default antivirus pattern-update interval is once a day.)

To automatically update antivirus patterns:

1. Select **Configure>Security>UTM>Anti-Virus**.
2. Next to Interval, in the Juniper Express Engine section, enter **120** in the box.
3. Click **OK** to check your configuration and save it as a candidate configuration, then click **Commit Options>Commit**.

## Manually Updating, Reloading, and Deleting Express Antivirus Patterns (CLI Procedure)

The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, to manually update antivirus patterns, enter the following CLI statement:

```
user@host> request security utm anti-virus juniper-express-engine pattern-update
```

To manually reload antivirus patterns, enter the following CLI statement:

```
user@host> request security utm anti-virus juniper-express-engine pattern-reload
```

To manually delete antivirus patterns, enter the following CLI statement:

```
user@host> request security utm anti-virus juniper-express-engine pattern-delete
```

SEE ALSO

Understanding MIME Allowlist | 50

Example: Configuring MIME Allowlist to Bypass Antivirus Scanning | 51

**Release History Table**

| Release | Description |
|---|---|
| 15.1X49-D10 | The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |

RELATED DOCUMENTATION

Full Antivirus Pattern Updates | 288

HTTP Trickling to Prevent Timeouts | 105

# Full Antivirus Protection

IN THIS SECTION



The full file-based antivirus feature provides file-based scanning on specific Application Layer traffic checking for viruses against a virus signature database. It collects the received data packets until it has reconstructed the original application content, such as an e-mail file attachment, and then scans this content. For more information, see the following topics:

## Full Antivirus Protection Overview

A virus is executable code that infects or attaches itself to other executable code in order to reproduce itself. Some malicious viruses erase files or lock up systems, while other viruses merely infect files and can overwhelm the target host or network with bogus data. The full file-based antivirus feature provides file-based scanning on specific Application Layer traffic checking for viruses against a virus signature database. It collects the received data packets until it has reconstructed the original application content, such as an e-mail file attachment, and then scans this content.

The full file-based antivirus scanning feature is a separately licensed subscription service. Kaspersky Lab provides the scan engine for full file-based antivirus. When your antivirus license key expires, you can continue to use locally stored antivirus signatures without any updates. But in that case, if the local database is deleted, antivirus scanning is disabled.

The express antivirus feature provides better performance but lower security. Note that if you switch from full file-based antivirus protection to express antivirus protection, you must reboot the device in order for express antivirus to begin working.

The Kaspersky and Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, the Kaspersky scan engine is provided as a downloadable UTM module. To download the Kaspersky scan engine, your SRX Series device must have an active UTM license. When you install the KAV license, the system automatically downloads the Kaspersky module from the Juniper Networks server and runs it.

When you set the antivirus type to KAV, and if the SRX Series device had a preinstalled Kaspersky engine, then the downloaded module replaces the original module on the device. Regardless of the UTM license status, when the KAV license is deleted from the device, the Kaspersky engine and all files associated with KAV are removed from the system immediately.

Use the **set security utm feature-profile anti-virus type kaspersky-lab-engine** command to set the antivirus type to KAV. If Kaspersky engine is not available on the device, and if the Kaspersky engine cannot be downloaded from the predefined URL, then use the **set security utm feature-profile anti-virus kaspersky-lab-engine pattern-update url *url*** command to configure the downloading application URL.

SEE ALSO


- Understanding Full Antivirus Pattern Updates | **288**
- Understanding Full Antivirus Scan Level Settings | **302**
- Understanding the Full Antivirus Scan Engine | **298**


## Full Antivirus Configuration Overview

The Kaspersky and Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, when configuring antivirus protection, you must first create the antivirus custom objects you are using. Those custom objects may include the MIME pattern list, MIME exception list, and the filename extension list. Once you have created your custom objects, you can configure full antivirus protection, including intelligent prescreening, and content size limits.

To configure full file-based antivirus protection:

1. Configure UTM custom objects for the UTM feature. The following example enables the mime-pattern, filename-extension, url-pattern, and custom-url-category custom-objects:

```
user@host# set security utm custom-objects mime-pattern
```

```
user@host# set security utm custom-objects filename-extension
user@host# set security utm custom-objects url-pattern
user@host# set security utm custom-objects custom-url-category
```

2. Configure the main feature parameters using feature profiles. The following example enables options using the anti virus feature profile:

```
user@host# set security utm feature-profile anti-virus kaspersky-lab-engine pattern-update
user@host# set security utm feature-profile anti-virus kaspersky-lab-engine profile
user@host# set security utm feature-profile anti-virus kaspersky-lab-engine profile fallback-options
user@host# set security utm feature-profile anti-virus kaspersky-lab-engine profile notification-options
user@host# set security utm feature-profile anti-virus kaspersky-lab-engine profile scan-options
user@host# set security utm feature-profile anti-virus kaspersky-lab-engine profile trickling
user@host# set security utm feature-profile anti-virus mime-whitelist
user@host# set security utm feature-profile anti-virus url-whitelist
```

3. Configure a UTM policy for each protocol and attach this policy to a profile. The following example configure the utmp2 UTM policy for the HTTP protocol:

```
user@host# set security utm utm-policy utmp2 anti-virus http-profile http1
```

4. Attach the UTM policy to a security policy. The following example attaches the utmp2 UTM policy to the p2 security policy:

```
user@host# set security policies from-zone trust to-zone untrust policy p2 then permit application-services
    utm-policy utmp2
```

SEE ALSO

Understanding Full Antivirus Content Size Limits | 307

Example: Configuring the Full Antivirus Pattern Update Server | 289

Understanding Full Antivirus Intelligent Prescreening | 305

# Example: Configuring Full Antivirus Custom Objects

IN THIS SECTION



The Kaspersky and Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, this example shows how to configure full antivirus custom objects.

## Requirements

Before you begin:

- Decide the type of full antivirus protection you require. See "Full Antivirus Protection Overview" on page 262.
- Understand the order in which full antivirus parameters are configured. See "Full Antivirus Pattern Update Configuration Overview" on page 291.

## Overview

In this example, you define custom objects that are used to create full antivirus feature profiles. You perform the following tasks to define custom objects:

1. Configure a filename extension list called extlist1 and add extensions such as .zip, .js, and .vbs to the list.
2. Create two MIME lists called avmime1 and ex-avmime1 and add patterns to the list.
3. Configure a URL pattern list called urllist1.
4. Configure a custom URL category list called custurl1 using the urllist1 URL pattern list.

## Configuration

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm custom-objects filename-extension extlist1 value [zip js vbs]
set security utm custom-objects mime-pattern avmime1 value [video/quicktime image/x-portable-anymap
  x-world/x-vrml]
set security utm custom-objects mime-pattern ex-avmime1 value [video/quicktime-inappropriate]
set security utm custom-objects url-pattern urllist1 value [http://www.url.com 5.6.7.8]
set security utm custom-objects custom-url-category custurl1 value urllist1
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure full antivirus filtering custom objects:

1. Configure the filename extension list and add extensions to it.

   ```
   [edit security utm]
   user@host# set custom-objects filename-extension extlist1 value [zip js vbs]
   ```

   **NOTE:** The Kaspersky scan engine ships with a read-only default extension list that you can use.

2. Create MIME lists and add MIME patterns to the lists.

   ```
   [edit security utm]
   user@host# set custom-objects mime-pattern avmime1 value [video/quicktime image/x-portable-anymap
     x-world/x-vrml]
   user@host# set custom-objects mime-pattern ex-avmime1 value [video/quicktime-inappropriate]
   ```

3. Configure a URL pattern list.

   ```
   [edit security utm]
   user@host# set custom-objects url-pattern urllist1 value [http://www.url.com 5.6.7.8]
   ```

   When entering the URL pattern, note the following wildcard character support:

- The *\.[]\?* wildcard characters are supported.
- You must precede all wildcard URLs with http://.
- You can only use the asterisk * wildcard character if it is at the beginning of the URL and is followed by a period.
- You can only use the question mark ? wildcard character at the end of the URL.
- The following wildcard syntax is supported: http://*.example.net, http://www.example.ne?, http://www.example.n??.
- The following wildcard syntax is not supported: *.example.net , www.example.ne?, http://*example.net, http://*.

> **NOTE:** Because you use URL pattern lists to create custom URL category lists, you must configure URL pattern list custom objects before you configure custom URL category lists.

4. Configure a custom URL category list.

```
[edit security utm]
user@host# set custom-objects custom-url-category custurl1 value urllist1
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
userhost# show security utm
custom-objects {
   mime-pattern {
      avmime1 {
         value [ video/quicktime image/x-portable-anymap x-world/x-vrml ];
      }
      ex-avmime1 {
         value video/quicktime-inappropriate;
      }
   }
   filename-extension {
      extlist1 {
         value [ zip js vbs ];
      }
```

```
    }
    url-pattern {
        urllist1 {
            value [ http://www.url.com 5.6.7.8 ];
        }
    }
    custom-url-category {
        custurl1 {
            value urllist1;
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

### Verification

#### *Verifying Full Antivirus Custom Objects*

**Purpose**

Verify the full antivirus custom objects.

**Action**

From operational mode, enter the **show configuration security utm** command.

SEE ALSO

Understanding MIME Allowlist | 50

Example: Configuring MIME Allowlist to Bypass Antivirus Scanning | 51

## Configuring Full Antivirus Custom Objects (J-Web Procedure)

The Kaspersky and Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, to configure antivirus protection, you must first create your custom objects (MIME Pattern List, Filename Extension List, URL Pattern List, and Custom URL Category List).

Configure a MIME pattern list custom object:

1. Select **Configure>Security>UTM>Custom Objects**.

2. From the MIME Pattern List tab, click the **Add** button to create MIME pattern lists.

3. In the Add MIME Pattern pop-up window, next to **MIME Pattern Name**, enter a unique name.

   Keep in mind that you are creating a MIME allowlist and a MIME exception list (if necessary). Both MIME lists appear in the MIME Allowlist and Exception MIME Allowlist fields when you configure antivirus. Therefore, the MIME list names you create should be as descriptive as possible.

4. Next to **MIME Pattern Value**, enter the MIME pattern.

5. Click **Add** to add your MIME pattern to the Values list box. Within this box, you can also select an entry and use the Delete button to delete it from the list. Continue to add MIME patterns in this manner.

6. Optionally, create a new MIME list to act as an exception list. The exception list is generally a subset of the main MIME list.

7. Click **OK** to check your configuration and save the selected values as part of the MIME list, then click **Commit Options**>**Commit**.

8. If the configuration item is saved successfully, you receive a confirmation and you must click **OK** again. If it is not saved successfully, you can click **Details** in the pop-up window that appears to discover why.

Configure a filename extension list custom object:

1. Select **Configure>Security>UTM>Custom Objects**.

2. From the Filename Extension List tab, click the **Add** button to create filename extension lists.

3. Next to **File Extension Name**, enter a unique name. This name appears in the Scan Option By Extension list when you configure an antivirus profile.

4. In the **Available Values** box, select one or more default values (press Shift to select multiple concurrent items or press Ctrl to select multiple separate items) and click the right arrow button to move the value or values to the Selected Values box.

5. Click **OK** to check your configuration and save it as a candidate configuration, then click **Commit Options>Commit**.

6. If the configuration item is saved successfully, you receive a confirmation and you must click **OK** again. If the profile is not saved successfully, you can click **Details** in the pop-up window that appears to discover why.

Configure a URL pattern list custom object:

> **NOTE:** Because you use URL pattern lists to create custom URL category lists, you must configure URL pattern list custom objects before you configure a custom URL category list.

1. Select **Configure>Security>UTM>Custom Objects**.

2. From the URL Pattern List tab, click the **Add** button to create URL pattern lists.

3. Next to URL Pattern Name, enter a unique name. This name appears in the Custom URL Category List Custom Object page for selection.

4. Next to **URL Pattern Value**, enter the URL or IP address you want added to the list for bypassing scanning.

   When entering the URL pattern, note the following wildcard character support:

   - The *\.[]\?* wildcard characters are supported.
   - You must precede all wildcard URLs with **http://**.
   - You can only use the asterisk * wildcard character if it is at the beginning of the URL and is followed by a period.
   - You can only use the question mark **?** wildcard character at the end of the URL.
   - The following wildcard syntax IS supported: **http://*.example.net**, **http://www.example.ne?**, **http://www.example.n??**.
   - The following wildcard syntax is NOT supported: ***.example.net** , **www.example.ne?**, **http://*example.net, http://***.

5. Click **Add** to add your URL pattern to the Values list box. The list can contain up to 8192 items. You can also select an entry and use the Delete button to delete it from the list. Continue to add URLs or IP addresses in this manner.

6. Click **OK** to check your configuration and save the selected values as part of the URL pattern list you have created, then click **Commit Options**>**Commit**.

7. If the configuration item is saved successfully, you receive a confirmation and you must click **OK** again. If it is not saved successfully, you can click **Details** in the pop-up window that appears to discover why.

Configure a custom URL category list custom object:

> **NOTE:** Because you use URL Pattern Lists to create custom URL category lists, you must configure URL pattern list custom objects before you configure a custom URL category list.

1. Select **Configure>Security>UTM>Custom Objects**.

2. In the URL Category List tab, click **Add** to create URL category lists.

3. Next to **URL Category Name**, enter a unique name. This name appears in the URL Allowlist list when you configure antivirus global options.

4. In the **Available Values** box, select a URL Pattern List name from the list for bypassing scanning and click the right arrow button to move it to the Selected Values box.

5. Click **OK** to check your configuration and save the selected values as part of the URL list that you have created, then click **Commit Options**>**Commit**.

   Click **OK** to save the selected values as part of the custom URL list you have created.

6. If the configuration item is saved successfully, you receive a confirmation and you must click **OK** again. If it is not saved successfully, you can click **Details** in the pop-up window that appears to discover why.

SEE ALSO

Understanding MIME Allowlist | **50**

Example: Configuring MIME Allowlist to Bypass Antivirus Scanning | **51**

# Example: Configuring Full Antivirus Feature Profiles

IN THIS SECTION



The full antivirus feature profile is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, this example shows how to configure a full antivirus feature profile.

## Requirements

Before you begin:

- Decide the type of full antivirus protection you require. See "Full Antivirus Protection Overview" on page 262.
- Understand the order in which full antivirus parameters are configured. See "Full Antivirus Configuration Overview" on page 263.
- MIME patterns must be defined for lists and exception lists. See "Example: Configuring MIME Allowlist to Bypass Antivirus Scanning" on page 51.

## Overview

In this example, you configure a feature profile called kasprof1 and specify custom objects to be used for filtering content:

- Select and configure the engine type as Kaspersky Lab Engine.
- Select 120 as the time interval for updating the pattern database. The default full file-based antivirus pattern-update interval is 60 minutes.

  The command for changing the URL for the pattern database is:

```
[edit]
user@host# edit security utm feature-profile anti-virus kaspersky-lab-engine
```

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
user@host# set pattern-update url http://..
```

- Enable an e-mail notification with a custom message as pattern file was updated and a custom subject line as AV pattern file updated.
- Configure a list of fallback options as block.
- Configure the notification options for fallback blocking for virus detection. Configure a custom message for the fallback blocking action.
- Configure a notification for protocol-only virus detection.
- Configure scan options. For this example, configure the device to perform a TCP payload content size check before the scan request is sent.
- Configure the decompression layer limit. For this example configure the device to decompress three layers of nested compressed files before it executes the virus scan.
- Configure content size parameters as 20000.

  For SRX100, SRX110, SRX210, SRX220, and SRX240 devices the content size is 20000. For SRX650 devices the content size is 40,000. Platform support depends on the Junos OS release in your installation.
- Configure scan extension settings. The default list is junos-default-extension. For this example, you select extlist1, which you created as a custom object.
- Configure the scan mode setting to configure the device to use a custom extension list. Although you can choose to scan all files, for this example you select only files with the extensions that you specify.
- Enable intelligent prescreening and set its timeout setting to 1800 seconds and trickling setting (applicable only to HTTP) to 600 seconds. This means that if the device receives a packet within a 600-second period during a file transfer or while performing an antivirus scan, it should not time out.

  Intelligent prescreening is only intended for use with non-encoded traffic. It is not applicable for mail protocols (SMTP, POP3, IMAP) and HTTP POST.

  The following example disables intelligent prescreening for the kasprof1 profile:

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
user@host# set profile kasprof1 scan-options no-intelligent-prescreening
```

- Configure the antivirus scanner to use MIME bypass lists and exception lists. You can use your own custom object lists, or you can use the default list that ships with the device called junos-default-bypass-mime. For this example, you use the avmime1 and ex-avmime1 lists.
- Configure the antivirus module to use URL bypass lists. If you are using a URL allowlist (valid only for HTTP traffic), this is a custom URL category that you have previously configured as a custom object. For this example, you enable the custurl1 bypass list.

## Configuration

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm feature-profile anti-virus type kaspersky-lab-engine
set security utm feature-profile anti-virus kaspersky-lab-engine pattern-update interval 120
set security utm feature-profile anti-virus kaspersky-lab-engine pattern-update email-notify admin-email
    administrator@example.net custom-message patternfilewasupdated custom-message-subject
    AVpatternfileupdated
set security utm feature-profile anti-virus type kaspersky-lab-engine
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options content-size
    block
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options corrupt-file
    block
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options decompress-layer
    block
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options default block
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options engine-not-ready
    block
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options out-of-resources
    block
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options password-file
    block
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options timeout block
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options
    too-many-requests block
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 notification-options fallback-block
    custom-message “Dropped due to fallback settings”
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 notification-options
    virus-detection type protocol-only
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 scan-options content-size-limit
    20000
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 scan-options
    decompress-layer-limit 3
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 scan-options
    intelligent-prescreening
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 scan-options scan-extension
    extlist1
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 scan-options scan-mode
    by-extension
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 scan-options timeout 1800
```

```
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 trickling timeout 600
set security utm feature-profile anti-virus mime-whitelist list avmime1
set security utm feature-profile anti-virus mime-whitelist list avmime1 exception ex-avmime1
set security utm feature-profile anti-virus url-whitelist custurl1
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure full antivirus feature profiles:

1. Select and configure the engine type.

```
[edit]
user@host# set security utm feature-profile anti-virus type kaspersky-lab-engine
user@host#set security utm feature-profile anti-virus kaspersky-lab-engine pattern-update interval 120
```

2. Configure the device to notify a specified administrator when patterns are updated.

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
user@host# set pattern-update email-notify admin-email administrator@example.net custom-message
   patternfilewasupdated custom-message-subject AVpatternfileupdated
```

3. Create a profile for the Kaspersky Lab engine and configure fallback options as block.

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
user@host# set profile kasprof1 fallback-options content-size block
user@host# set profile kasprof1 fallback-options corrupt-file block
user@host# set profile kasprof1 fallback-options decompress-layer block
user@host# set profile kasprof1 fallback-options default block
user@host# set profile kasprof1 fallback-options engine-not-ready block
user@host# set profile kasprof1 fallback-options out-of-resources block
user@host# set profile kasprof1 fallback-options password-file block
user@host# set profile kasprof1 fallback-options timeout block
user@host# set profile kasprof1 fallback-options too-many-requests block
```

4. Configure a custom notification for the fallback blocking action and send a notification.

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
user@host# set profile kasprof1 notification-options fallback-block custom-message “Dropped due to
   fallback settings”
```

5. Configure a notification for protocol-only virus detection.

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
user@host# set profile kasprof1 notification-options virus-detection type protocol-only
```

6. Configure content size parameter.

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
user@host# set profile kasprof1 scan-options content-size-limit 20000
```

7. Configure the decompression layer limit.

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
user@host# set profile kasprof1 scan-options decompress-layer-limit 3
```

8. Configure intelligent prescreening.

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
user@host# set profile kasprof1 scan-options intelligent-prescreening
```

9. Configure scan extension setting.

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
user@host# set profile kasprof1 scan-options scan-extension extlist1
```

10. Configure the scan mode setting.

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
user@host# set profile kasprof1 scan-options scan-mode by-extension
```

11. Configure the timeout setting.

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
user@host# set profile kasprof1 scan-options timeout 1800
```

12. Configure trickling setting.

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
user@host# set profile kasprof1 trickling timeout 600
```

13. Configure the antivirus scanner to use MIME bypass lists and exception lists.

```
[edit security utm feature-profile anti-virus]
user@host# set mime-whitelist list avmime1
user@host# set mime-whitelist list avmime1 exception ex-avmime1
```

14. Configure the antivirus module to use URL bypass lists.

```
[edit security utm feature-profile anti-virus]
user@host# set url-whitelist custurl1
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm feature-profile anti-virus** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security utm feature-profile anti-virus
mime-whitelist {
    list avmime1;
    exception ex-avmime1;
}
url-whitelist custurl1;
kaspersky-lab-engine {
    pattern-update {
        email-notify {
            admin-email "administrator@example.net";
            custom-message patternfilewasupdated;
            custom-message-subject AVpatternfileupdated;
        }
        interval 120;
    }
    profile kasprof1 {
        fallback-options {
            default block;
            corrupt-file block;
            password-file block;
```

```
            decompress-layer block;
            content-size block;
            engine-not-ready block;
            timeout block;
            out-of-resources block;
            too-many-requests block;
        }
        scan-options {
            intelligent-prescreening;
            scan-mode by-extension;
            scan-extension extlist1;
            content-size-limit 20000;
            timeout 1800;
            decompress-layer-limit 3;
        }
        trickling timeout 600;
        notification-options {
            virus-detection {
                type protocol-only;
                custom-message ***virus-found***;
            }
            fallback-block {
                custom-message “Dropped due to fallback settings”;
            }
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### *Verifying the Configuration of Full Antivirus Feature Profile*

#### Purpose

Verify the full antivirus feature profile.

#### Action

From operational mode, enter the **show configuration security utm** command.

SEE ALSO

Understanding HTTP Trickling | 105

Understanding Protocol-Only Virus-Detected Notifications | 101
Understanding Full Antivirus Decompression Layer Limits | 308

## Configuring Full Antivirus Feature Profiles (J-Web Procedure)

The full antivirus feature profile is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, after you have created your custom object, configure an antivirus feature profile:

1. Select **Configure>Security>UTM>Global options**.
2. In the Anti-Virus tab, next to **MIME whitelist**, select the custom object you created from the list.
3. Next to **Exception MIME whitelist**, select the custom object you created from the list.
4. Next to **URL Whitelist**, select the custom object you created from the list.
5. In the **Engine Type** section, select the type of engine you are using. For full antivirus protection, you should select **Kaspersky Lab**.
6. In the Kaspersky Lab Engine Option section, in the **Pattern update URL** box, enter the URL for the pattern database.

   The URL is http://update.juniper-updates.net/AV/<device version> and you should not change it.
7. Next to **Pattern update interval**, enter the time interval, in seconds, for automatically updating the pattern database in the box. The default interval is 60.
8. Select whether you want the pattern file to update automatically (**Auto update**) or not (**No Auto update**).
9. Click **OK** to save the selected values.
10. If the configuration item is saved successfully, you receive a confirmation and you must click **OK** again. If it is not saved successfully, you can click **Details** in a pop-up window that appears to discover why.
11. Under Security, in the left pane, select **Anti-Virus**.
12. In the right window, click **Add** to create a profile for the antivirus Kaspersky Lab Engine. (To edit an existing item, select it and click the **Edit** button.)

13. Next to **Profile name**, enter a unique name for this antivirus profile.

14. Select the **Profile Type**. In this case, select **Kaspersky**.

15. Next to **Trickling timeout**, enter timeout parameters.

> **NOTE:** Trickling applies only to HTTP. HTTP trickling is a mechanism used to prevent the HTTP client or server from timing out during a file transfer or during antivirus scanning.

16. Next to Intelligent prescreening, select **Yes** or **No**.

    Intelligent prescreening is only intended for use with non-encoded traffic. It is not applicable for mail protocols (SMTP, POP3, IMAP, and HTTP POST).

17. In the Scan Options section, next to Intelligent prescreening, select **Yes** if you are using it.

    Intelligent prescreening is only intended for use with non-encoded traffic. It is not applicable for mail protocols (SMTP, POP3, IMAP, and HTTP POST).

18. Next to **Content Size Limit**, enter content size parameters. The content size check occurs before the scan request is sent. The content size refers to accumulated TCP payload size.

19. Next to **Scan engine timeout**, enter scanning timeout parameters.

20. Next to **Decompress Layer Limit**, enter decompression layer limit parameters.

21. In the Scan mode section, select either **Scan all files**, if you are scanning all content, or **Scan files with specified extension**, if you are scanning by file extensions.

    If you select Scan files with specified extension, you must select a filename extension list custom object from the Scan engine filename extention list that appears.

22. Select the **Fallback settings** tab.

23. Next to Default (fallback option), select **Log and permit** or **Block** from the list. In most cases, Block is the default fallback option.

24. Next to Corrupt File (fallback option), select **Log and permit** or **Block** from the list.

25. Next to Password File (fallback option), select **Log and permit** or **Block** from the list.

26. Next to Decompress Layer (fallback option), select **Log and permit** or **Block** from the list.

27. Next to Content Size (fallback option), select **Log and permit** or **Block** from the list.

28. Next to Engine Not Ready (fallback option), select **Log and permit** or **Block** from the list.

29. Next to Timeout (fallback option), select **Log and permit** or **Block** from the list.

30. Next to Out Of Resources (fallback option), select **Log and permit** or **Block** from the list.

31. Next to Too Many Request (fallback option), select **Log and permit** or **Block** from the list.

32. Select the **Notification options** tab.

33. In the Fallback block section, next to Notification type, select **Protocol Only** or **Message** to select the type of notification that is sent when a fallback option of block is triggered.

34. Next to Notify mail sender, select **Yes** or **No**.

35. If you selected Yes, next to **Custom Message**, enter text for the message body of your custom message for this notification (if you are using a custom message).

36. Next to **Custom message subject**, enter text to appear in the subject line of your custom message for this notification (if you are using a custom message).

37. In the Fallback non block section, next to Notify mail recipient, select **Yes** or **No**.

38. If you selected Yes, next to **Custom Message**, enter text for the message body of your custom message for this notification (if you are using a custom message).

39. Next to **Custom message subject**, enter text to appear in the subject line of your custom message for this notification (if you are using a custom message).

40. Select the **Notification options cont** tab.

41. In the Virus detection section, next to Notification type, select **Protocol Only** or **Message** to select the type of notification that is sent when a fallback option of block is triggered.

42. Next to Notify mail sender, select **Yes** or **No**.

43. If you selected Yes, next to **Custom Message**, enter text for the message body of your custom message for this notification (if you are using a custom message).

44. Next to **Custom message subject**, enter text to appear in the subject line of your custom message for this notification (if you are using a custom message). The limit is 255 characters.

45. Click **OK** to check your configuration and save it as a candidate configuration, then click **Commit Options>Commit**.

46. If the configuration item is saved successfully, you receive a confirmation and you must click **OK** again. If it is not saved successfully, you can click **Details** in the pop-up window that appears to discover why.

    You create a separate antivirus profile for each antivirus protocol. These profiles may basically contain the same configuration information, but when you are creating your UTM policy for an antivirus profile, the UTM policy configuration page provides separate antivirus profile selection fields for each supported protocol.

SEE ALSO


- Understanding Protocol-Only Virus-Detected Notifications | **101**
- Understanding HTTP Trickling | **105**
- Configuring HTTP Trickling to Prevent Timeouts During Antivirus Scanning (CLI Procedure) | **106**


## Example: Configuring Full Antivirus UTM Policies

**IN THIS SECTION**



The full antivirus feature profile is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, this example shows how to create a UTM policy to attach to a feature profile.

### Requirements

Before you begin, create an antivirus feature profile. See “Example: Configuring Full Antivirus Feature Profiles” on page 272.

### Overview

In this example, you configure a full antivirus UTM policy called utmp2 and attach the policy to an HTTP profile called kasprofile1 HTTP.

### Configuration

#### Step-by-Step Procedure

To configure a full antivirus UTM policy:

1. Create a UTM policy for HTTP antivirus scanning and attach the policy to the profile.

```
[edit]
user@host# set security utm utm-policy utmp2 anti-virus http-profile kasprofile1
```

2. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

### Verification

To verify the configuration is working properly, enter the **show security utm** command.

SEE ALSO

Understanding Antivirus Scanning Fallback Options | 318

## Configuring Full Antivirus UTM Policies (J-Web Procedure)

The full antivirus UTM policies is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, after you have created an antivirus feature profile, configure a UTM policy to which you can attach the feature profile:

1. Select **Configure>Security>Policy>UTM Policies**.
2. From the UTM policy configuration window, click **Add** to configure a UTM policy. This action takes you to the policy configuration pop-up window.
3. Select the **Main** tab in pop-up window.
4. In the **Policy name** box, enter a unique name for the UTM policy.
5. In the **Session per client limit** box, enter a session per client limit from 0 to 20000 for this UTM policy.
6. In the **Session per client over limit** list, select the action that the device should take when the session per client limit for this UTM policy is exceeded. Options include **Log and permit** and **Block**.
7. Select the **Anti-Virus profiles** tab in the pop-up window.
8. Select the appropriate profile you have configured from the list for the corresponding protocol listed.
9. Click **OK** to check your configuration and save it as a candidate configuration, then click **Commit Options>Commit**.
10. If the policy is saved successfully, you receive a confirmation and you must click **OK** again. If the profile is not saved successfully, you can click **Details** in the pop-up window that appears to discover why.

## Example: Attaching Full Antivirus UTM Policies to Security Policies

**IN THIS SECTION**

The full antivirus UTM policies is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, this example shows how to attach a UTM policy to a security policy.

## Requirements

Before you begin, create a UTM policy. See "Example: Configuring Full Antivirus UTM Policies" on page 282.

## Overview

In this example, you attach the UTM policy called utmp2 to the security policy called p2.

## Configuration

### Step-by-Step Procedure

To attach a full antivirus UTM policy to a security policy:

1. Enable and configure the security policy.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy p2 match source-address any
user@host# set security policies from-zone trust to-zone untrust policy p2 match destination-address any
user@host# set security policies from-zone trust to-zone untrust policy p2 match application junos-http
```

2. Attach the UTM policy to the security policy.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy p2 then permit application-services
    utm-policy utmp2
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

### Verification

To verify the configuration is working properly, enter the **show security policies** command.

## Attaching Full Antivirus UTM Policies to Security Policies (J-Web Procedure)

The full antivirus UTM policies is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, after you create a UTM policy, create a security policy and attach the UTM policy to the security policy:

1. Select **Configure>Security>Policy>FW Policies**.
2. From the Security Policy window, click **Add** to configure a security policy with UTM. This action takes you to the policy configuration pop-up window.
3. In the Policy tab, enter a name in the **Policy Name** box.
4. Next to **From Zone**, select a zone from the list.
5. Next to **To Zone**, select a zone from the list.
6. Choose a **Source Address**.
7. Choose a **Destination Address**.
8. Choose an application by selecting **junos-*protocol*** (for all protocols that support antivirus scanning) in the Application Sets box and clicking the —> button to move it to the Matched box.
9. Next to Policy Action, select **Permit**.

   When you select Permit for Policy Action, several additional fields become available in the Applications Services tab, including UTM Policy.
10. Select the **Application Services** tab in the pop-up window.
11. Next to **UTM Policy**, select the appropriate policy from the list. This action attaches your UTM policy to the security policy.

12. Click **OK** to check your configuration and save it as a candidate configuration, then click **Commit Options>Commit**.

13. If the policy is saved successfully, you receive a confirmation and you must click **OK** again. If the profile is not saved successfully, you can click **Details** in the pop-up window that appears to discover why.

    You must activate your new policy to apply it.

**Release History Table**

| Release | Description |
|---|---|
| 15.1X49-D10 | The Kaspersky and Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Kaspersky and Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Kaspersky and Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Kaspersky and Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The full antivirus feature profile is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The full antivirus feature profile is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The full antivirus feature profile is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The full antivirus UTM policies is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The full antivirus UTM policies is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The full antivirus UTM policies is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |

RELATED DOCUMENTATION

Full Antivirus Application Protocol Scanning | 323

Antispam Filtering Overview | 108

Full Antivirus File Scanning | 297

# Full Antivirus Pattern Updates

IN THIS SECTION



The full file-based antivirus protection signature database is called the Juniper Full antivirus database, it detects all destructive malicious code, including viruses (polymorphic and other advanced virus types), worms, Trojans, and malware. For more information, see the following topics:

## Understanding Full Antivirus Pattern Updates

The full antivirus Pattern Updates is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, the full file-based antivirus protection signature database is called the Juniper Full antivirus database (downloaded by the pattern-update command). This database is different from the database used by express antivirus. It detects all destructive malicious code, including viruses (polymorphic and other advanced virus types), worms, Trojans, and malware.

Updates to the pattern file are added as new viruses are discovered. When Kaspersky Lab updates the signatures in its pattern database, the security device downloads these updates so that the antivirus scanner is using the latest, most up-to-date signatures when scanning traffic. The security device can perform these updates automatically (the default), or you can perform pattern update downloads manually.

The database pattern server is accessible through HTTP or HTTPS. By default, the antivirus module checks for database updates automatically every 60 minutes. You can change this interval and you can trigger updates manually, as well. The number of files that are downloaded during an update and the duration of the download process can vary.

A local copy of the pattern database is saved in persistent data storage (that is, the flash disk). If the device is rebooted, the local copy remains available for the antivirus scan engine to use during the antivirus scan engine initialization time, without the need for network access to the pattern database server.

If the auto-update fails, the updater automatically retries to update three more times. If the database download continues to fail, the updater stops trying and waits for the next periodic update before trying again.

Once your subscription expires, you have a 30 day grace period during which you can continue to update the antivirus pattern file. Once that grace period expires, the update server no longer permits antivirus pattern file updates.

SEE ALSO

Full Antivirus Protection Overview | 262

## Example: Configuring the Full Antivirus Pattern Update Server

IN THIS SECTION



The full antivirus Pattern Updates is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, this example shows how to configure the pattern-update server on the security device.

### Requirements

Before you begin:

- Obtain a valid antivirus scanner license. See "Full Antivirus Protection Overview" on page 262.
- Get network connectivity and access to the pattern database server. See "Understanding Full Antivirus Pattern Updates" on page 288.
- Configure your DNS settings and port settings (port 80) correctly. See *DNS Overview*.

## Overview

To configure the pattern-update server on the security device, enter the URL address of the pattern-update server.

By default, the Juniper-Kaspersky URL for full antivirus protection is http://update.juniper-updates.net/AV/*device-name*, where *device-name* is the name of your device.

## Configuration

### Step-by-Step Procedure

To configure the pattern-update server on a security device:

1. Specify the URL of the pattern-update server.

```
[edit]
user@host# set security utm feature-profile anti-virus kaspersky-lab-engine pattern-update url
    http://update.juniper-updates.net/AV/device-name
```

> **NOTE:** Other than the platform name, you should not change this URL unless you are experiencing problems with it and have called for support.

2. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

## Verification

To verify the configuration is working properly, enter the **show security utm** command.

## Full Antivirus Pattern Update Configuration Overview

The Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, Before you begin, there are several prerequisites that must be met in order to perform a successful pattern database update:

- You must have a valid antivirus scanner license.
- You must have network connectivity and access to the pattern database server.
- Your DNS settings and port settings (port 80) must be correct.

To update the patterns for the antivirus signature database:

1. On the security device, specify the URL address of the pattern-update server.

2. (Optional) Specify how often the device should automatically check for pattern-server updates.

After the security device downloads the server-initialization file, the device checks that the pattern file is valid. The device then parses the file to obtain information about it, including the file version, size, and location of the pattern file server.

If the pattern file on the security device is out-of-date (or nonexistent because this is the first time you are loading it), and, if the antivirus pattern-update service subscription is still valid, the device automatically retrieves an updated pattern file from the pattern file server.

The following is an example of the CLI for configuring the database update feature:

```
utm {
    feature-profile {
        anti-virus {
            type
                kaspersky-lab-engine {
                    pattern-update
                        url url
                    interval minutes
                }
            }
        }
    }
```

# Example: Automatically Updating Full Antivirus Patterns

IN THIS SECTION



The full antivirus Pattern Updates is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, this example shows how to update the pattern file automatically on a security device.

## Requirements

Before you begin:

- Obtain a valid antivirus scanner license. See "Full Antivirus Protection Overview" on page 262.
- Get network connectivity and access to the pattern database server. See "Understanding Full Antivirus Pattern Updates" on page 288.
- Configure your DNS settings and port settings (port 80) correctly. See *DNS Overview*.

## Overview

In this example, you configure the security device to update the pattern file automatically every 120 minutes. (The default antivirus pattern-update interval is 60 minutes.)

## Configuration

### Step-by-Step Procedure

To configure the security device to update the pattern file automatically:

1. Set the interval.

```
[edit]
user@host# set security utm feature-profile anti-virus kaspersky-lab-engine pattern-update interval 120
```

2. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

### Verification

To verify the configuration is working properly, enter the **show security utm** command.

## Example: Automatically Updating Full Antivirus Patterns (J-Web Procedure)

The full antivirus Pattern Updates is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, in this example, you configure the security device to update the pattern file automatically every 120 minutes. (The default antivirus pattern-update interval is 60 minutes.)

To automatically update antivirus patterns:

1. Select **Configure>UTM>Anti-Virus**.

2. Next to Interval, in the Kaspersky Lab Engine section, enter **120** in the box.

3. Click **OK** to check your configuration and save it as a candidate configuration, then click **Commit Options>Commit**.

## Manually Updating, Reloading, and Deleting Full Antivirus Patterns (CLI Procedure)

The Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, to manually update antivirus patterns, enter the following CLI command:

```
user@host> request security utm anti-virus kaspersky-lab-engine pattern-update
```

To manually reload antivirus patterns, enter the following CLI command:

```
user@host> request security utm anti-virus kaspersky-lab-engine pattern-reload
```

To manually delete antivirus patterns, enter the following CLI command:

```
user@host> request security utm anti-virus kaspersky-lab-engine pattern-delete
```

You can update the Kaspersky antivirus signature database offline without using a direct Internet connection. This is required in some security installations and for sites that access the Internet through a proxy server.

To update the Kaspersky antivirus signature database offline, you must configure a local webserver.

To configure a webserver, use the following CLI statement.

**user@host# set security utm feature-profile anti-virus kaspersky-lab-engine pattern-update url <*http_server*>**

**user@host# commit**

To update the Kaspersky antivirus signature database, perform the following tasks:

1. Based on your hardware platform, enter the following URLs in your computer browser.

2. Copy all the files to a directory on your local webserver. You might want to use a download manager for your browser to get all the files more quickly.

3. Download the Kaspersky Lab engine from http://update.juniper-updates.net/KAV_engine/.
   - For JSR, the URL is http://update.juniper-updates.net/KAV_engine/i386/.
   - For SRX210, SRX220, SRX240, SRX550, and SRX650 devices, the URL is http://update.juniper-updates.net/KAV_engine/octeon32/.
4. Copy all the files to the same directory on your local server.

   **NOTE:** The Kaspersky Lab engine is automatically loadable. For updating the Kaspersky antivirus signature database offline, both pattern update files and Kaspersky Lab engine files must be placed in the same folder on the local webserver.

5. Set the directory as a sharepoint that can be accessed through HTTP from the SRX Series device.

6. Run the update command in the CLI.

   **user@host>request security utm anti-virus kaspersky-lab-engine pattern-update**

**Release History Table**

| Release | Description |
|---|---|
| 15.1X49-D10 | The full antivirus Pattern Updates is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The full antivirus Pattern Updates is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The full antivirus Pattern Updates is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The full antivirus Pattern Updates is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |

RELATED DOCUMENTATION

Full Antivirus File Scanning | 297
Virus-Detected Notifications | 100

# Full Antivirus File Scanning

IN THIS SECTION

The full file-based antivirus module is the software subsystem on the gateway device that scans specific Application Layer traffic to protect users from virus attacks and to prevent viruses from spreading. The antivirus module allows you to configure scanning options on a global level, on a UTM profile level, or on a firewall policy level. For more information, see the following topics:

## Understanding the Full Antivirus Scan Engine

The Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, the full file-based antivirus module is the software subsystem on the gateway device that scans specific Application Layer traffic to protect users from virus attacks and to prevent viruses from spreading. The antivirus software subsystem consists of a virus signature database, an application proxy, the scan manager, and the scan engine.

Kaspersky Lab provides the scan engine and it works in the following manner:

1. A client establishes a TCP connection with a server and then starts a transaction.

2. If the application protocol in question is marked for antivirus scanning, the traffic is forwarded to an application proxy for parsing.

3. When the scan request is sent, the scan engine scans the data by querying a virus pattern database.

4. The scan manager monitors antivirus scanning sessions, checking the properties of the data content against the existing antivirus settings.

5. After scanning has occurred, the result is then handled by the scan manager.

The Kaspersky Lab scan engine supports regular file scanning and script file scanning. With regular file scanning, the input object is a regular file. The engine matches the input content with all possible signatures. With script file scanning, the input object is a script file. It can be JavaScript, VBScript, mIRC script, bat scripts (DOS bat files), and other text scripts. The engine matches the input content only with signatures for script files. Script scanning is only applicable for HTML content over the HTTP protocol. There are two criteria for this scan type. First, the content-type field of this HTML document must be text or HTML. Second, there is no content encoding in the HTTP header. If those two criteria are met, an HTML parser is used to parse the HTML document for scripts.

SEE ALSO

Understanding Full Antivirus Scan Result Handling | 314

Monitoring Antivirus Scan Engine Status | 314

## Understanding Full Antivirus Scan Mode Support

The Kaspersky Lab scan engine is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, the Kaspersky Lab scan engine supports two modes of scanning:

- scan-all—This option tells the scan engine to scan all the data it receives.
- scan-by-extension—This option bases all scanning decisions on the file extensions found in the traffic in question.

When scanning content, you can use a file extension list to define a set of file extensions that are used in file extension scan mode (scan-by-extension). The antivirus module can then scan files with extensions on the scan-extension list. If an extension is not defined in an extension list, the file with that extension is not scanned in scan-by-extension mode. If there is no extension present, the file in question is scanned.

When using a file extension list to scan content, please note the following requirements:

- File extension entries are case-insensitive.
- The maximum length of the file extension list name is 29 bytes.

- The maximum length of each file extension entry is 15 bytes.
- The maximum entry number in a file extension list is 255.

SEE ALSO

Monitoring Antivirus Scan Results | 316

## Configuring Full Antivirus File Extension Scanning (CLI Procedure)

The Kaspersky Lab scan is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, to configure file-extension scanning, use the following CLI configuration statements:

```
security utm {
    custom-objects {
        filename-extension { ; set of list
            name extension-list-name; #mandatory
                value windows-extension-string;
            }
        }
    }
```

```
security utm feature-profile anti-virus kaspersky-lab-engine profile name {
    scan-options {
        scan-extension ext-list
        }
    }
```

## Example: Configuring Full Antivirus File Extension Scanning

**IN THIS SECTION**

The Kaspersky Lab scan is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, this example shows how to configure full antivirus file extension scanning.

## Requirements

Before you begin, decide the mode of scanning you require. See "Understanding Full Antivirus Scan Mode Support" on page 299.

## Overview

In this example, you perform the following tasks:

1. Create a file called extlist1 for the kasprof1 profile, and add extensions such as .zip, .js, and .vbs to the extlist1.
2. Configure the scan mode setting. You can choose to scan all files or to scan only the files that have the extensions that you specify. This example uses the scan by-extension option to configure the device to use the extlist1 file.

## Configuration

### Step-by-Step Procedure

To configure full antivirus file extension scanning:

1. Create a extension for the list and add extensions to the filename extension list.

```
[edit]
user@host# set security utm custom-objects filename-extension extlist1 value [zip js vbs]
```

2. Configure scan extension settings.

```
[edit]
user@host# set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 scan-options
    scan-extension extlist1
```

3. Configure the scan mode setting.

```
[edit]
user@host# set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 scan-options
   scan-mode by-extension
```

4. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

### Verification

To verify the configuration is working properly, enter the **show security utm** command.

SEE ALSO

Understanding Full Antivirus Scan Mode Support | 299

## Understanding Full Antivirus Scan Level Settings

The Kaspersky Lab scan is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, the antivirus module allows you to configure scanning options on a global level, on a UTM profile level, or on a firewall policy level. Each configuration level has the following implications:

- Global antivirus settings—Settings are applied to all antivirus sessions. Global settings are general overall configurations for the antivirus module or settings that are not specific for profiles.
- Profile-based settings—Antivirus settings are different for different protocols within the same policy.
- Policy-based settings—Antivirus settings are different for different policies. Policy-based antivirus settings are applied to all scan-specified traffic defined in a firewall policy.

The majority of antivirus settings are configured within an antivirus profile, bound to specified protocols, and used by designated policies. These UTM policies are then applied to the traffic according to firewall policies. If a firewall policy with an antivirus setting matches the properties of a traffic flow, the antivirus setting is applied to the traffic session. Therefore, you can apply different antivirus settings for different protocols and for different traffic sessions.

SEE ALSO

Understanding Full Antivirus Application Protocol Scanning | 324

## Example: Configuring Full Antivirus Scan Settings at Different Levels

IN THIS SECTION



The Kaspersky Lab scan is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, this example shows how to configure full antivirus scan settings at different levels.

### Requirements

Before you begin, decide the type of scanning option you require. See “Understanding Full Antivirus Scan Level Settings” on page 302.

### Overview

In this example, you define antivirus scanning options on any of the following levels:

- Global level
- UTM profile level using the kasprof1 UTM profile
- Firewall policy level using the p1 UTM policy

### Configuration

#### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm feature-profile anti-virus kaspersky-lab-engine pattern-update interval 20
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options default block
set utm-policy p1 anti-virus http-profile av-profile
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure antivirus scanning options at different levels:

1. Configure scanning options at the global level.

```
[edit security utm]
user@host# set feature-profile anti-virus kaspersky-lab-engine pattern-update interval 20
```

2. Configure scanning options at the UTM profile level.

```
[edit security utm]
user@host# set feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options default
    block
```

3. Configure scanning options at the UTM policy level.

```
[edit security utm]
user@host# set utm-policy p1 anti-virus http-profile av-profile
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this **show** command output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]
user@host# show security utm
...
    utm-policy p1 {
    anti-virus {
        http-profile av-profile
```

```
            ftp {
                upload-profile av-profile
                download-profile av-profile
            }
        }
    }
...
```

If you are done configuring the device, enter **commit** from configuration mode.

### Verification

#### *Verifying Scan Settings at Different Levels*

**Purpose**

Verify the scan settings at different levels.

**Action**

From operational mode, enter the **show configuration security utm** command.

SEE ALSO

Understanding FTP Antivirus Scanning | 326

## Understanding Full Antivirus Intelligent Prescreening

The Intelligent prescreening is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, by default, intelligent prescreening is enabled to improve antivirus scanning performance. The antivirus module generally begins to scan data after the gateway device has received all the packets of a file. Intelligent prescreening tells the antivirus module to begin scanning a file much earlier. In this case, the scan engine uses the first packet or the first several packets to determine if a file could possibly contain malicious code. The scan engine does a quick check on these first packets and if it finds that it is unlikely that the file is infected, it then decides that it is safe to bypass the normal scanning procedure.

Intelligent prescreening is only intended for use with non-encoded traffic. It is not applicable for MIME encoded traffic, mail protocols (SMTP, POP3, IMAP) and HTTP POST.

# Example: Configuring Full Antivirus Intelligent Prescreening

IN THIS SECTION



The Intelligent prescreening is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, this example shows how to configure full antivirus intelligent prescreening. By default, intelligent prescreening is enabled to improve antivirus scanning performance.

## Requirements

Before you begin, understand how intelligent prescreening enables the improvement of antivirus scanning performance. See "Understanding Full Antivirus Intelligent Prescreening" on page 305.

## Overview

In this example, you perform the following tasks:

- Enable intelligent prescreening for the kasprof1 profile.
- Disable intelligent prescreening for the kasprof1 profile.

## Configuration

### Step-by-Step Procedure

To enable or disable full antivirus intelligent prescreening:

1. Enable intelligent prescreening for the kasprof1 profile.

```
[edit]
user@host# set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 scan-options
    intelligent-prescreening
```

2. Disable intelligent prescreening for the kasprof1 profile.

```
[edit]
user@host# set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 scan-options
    no-intelligent-prescreening
```

**NOTE:** Intelligent prescreening is intended only for use with non-encoded traffic. It is not applicable to mail protocols (SMTP, POP3, IMAP) or HTTP POST.

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

### Verification

To verify the configuration is working properly, enter the **show security utm** command.

## Understanding Full Antivirus Content Size Limits

The Content Size Limit is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, due to resource constraints, there is a default, device-dependent limit on maximum content size for the database. The content size value is configurable. There is also a lower and upper limit for maximum content size. (This range is device dependent and is not configurable.)

The content size check occurs before the scan request is sent. The exact timing of this is protocol dependent. If the protocol header contains an accurate content length field, the content size check takes place when the content length field is extracted during header parsing. The content size usually refers to file size. If there is no content length field, the size is checked while the antivirus module is receiving packets. The content size, in this case, refers to accumulated TCP payload size. This setting can be used in all protocols.

## Configuring Full Antivirus Content Size Limits (CLI Procedure)

The Content Size Limit is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, to configure content size limits, use the following CLI configuration statements:

```
security utm feature-profile anti-virus kaspersky-lab-engine profile name {
    scan-options {
        content-size-limit KB;
    }
}
```

## Understanding Full Antivirus Decompression Layer Limits

The Decompression Layer Limit is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, the decompression layer limit specifies how many layers of nested compressed files and files with internal extractable objects, such as archive files (tar), MS Word and PowerPoint files, the internal antivirus scanner can decompress before it executes the virus scan. For example, if a message contains a compressed .zip file that contains another compressed .zip file, there are two compression layers. Decompressing both files requires a decompress layer setting of 2.

It is worth noting that during the transfer of data, some protocols use content encoding. The antivirus scan engine must decode this layer, which is considered a decompression level, before it scans for viruses.

There are three kinds of compressed data:

- compressed file (zip, rar, gzip)
- encoded data (MIME)
- packaged data (OLE, .CAP, .MSI, .TAR, .EML)

A decompression layer could be a layer of a zipped file or an embedded object in packaged data. The antivirus engine scans each layer before unpacking the next layer, until it either reaches the user-configured decompress limit, reaches the device decompress layer limit, finds a virus or other malware, or decompresses the data completely, whichever comes first.

As the virus signature database becomes larger and the scan algorithms become more sophisticated, the scan engine has the ability to look deeper into the data for embedded malware. As a result, it can uncover more layers of compressed data. The Juniper Networks device's level of security is limited by decompress limit, which is based on the memory allocated to the security service. If a virus is not found within the decompress limit, the user has an option to either pass or drop the data. This setting can be used in all protocols.

## Configuring Full Antivirus Decompression Layer Limits (CLI Procedure)

The Decompression Layer Limit is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, to configure decompression layer limits, use the following CLI configuration statements:

```
security utm feature-profile anti-virus kaspersky-lab-engine profile name {
    scan-options {
        decompress-layer-limit number
    }
}
```

## Understanding Full Antivirus Scanning Timeouts

The Scanning timeout parameter is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, the scanning timeout value includes the time frame from when the scan request is generated to when the scan result is returned by the scan engine. The time range can be 1 to 1800 seconds. By default, it is 180 seconds.

> **NOTE:** This timeout parameter is used by all supported protocols. Each protocol can have a different timeout value.

## Configuring Full Antivirus Scanning Timeouts (CLI Procedure)

The Scanning timeout parameter is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, to configure scanning timeouts, use the following CLI configuration statements:

```
security utm feature-profile anti-virus kaspersky-lab-engine profile name {
    scan-options {
        timeout-value seconds {
        }
    }
}
```

## Understanding Full Antivirus Scan Session Throttling

The Scan session Throttling is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, in an attempt to consume all available resources and hinder the ability of the scan engine to scan other traffic, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, a session throttle is imposed for antivirus resources, thereby restricting the amount of traffic a single source can consume at one time. The limit is an integer with 100 as the default setting. This integer refers to the maximum allowed sessions from a single source. You may change this default limit, but understand that if this limit is set high, that is comparable to no limit.

Over-limit is a fallback setting for the connection-per-client limit. The default behavior of over-limit is to block sessions. This is a per-policy setting. You can specify different settings for different UTM policies.

## Configuring Full Antivirus Scan Session Throttling (CLI Procedure)

The Scan session Throttling is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, to configure scan session throttling, use the following CLI configuration statements:

```
security utm utm-policy name
    traffic-options {
        sessions-per-client {
        limit number;
            over-limit { log-and-permit | block}
        }
    }
```

**Release History Table**

| Release | Description |
| --- | --- |
| 15.1X49-D10 | The Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Kaspersky Lab scan engine is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Kaspersky Lab scan is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Kaspersky Lab scan is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Kaspersky Lab scan is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Kaspersky Lab scan is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Intelligent prescreening is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Intelligent prescreening is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Content Size Limit is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Content Size Limit is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Decompression Layer Limit is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Decompression Layer Limit is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Scanning timeout parameter is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Scanning timeout parameter is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |

| | |
|---|---|
| 15.1X49-D10 | The Scan session Throttling is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Scan session Throttling is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |

RELATED DOCUMENTATION


- Full Antivirus Application Protocol Scanning | 323
- Virus-Detected Notifications | 100
- Full Antivirus Protection | 262


# Full Antivirus Scan Results and Fallback Options

IN THIS SECTION



Fallback options tell the system how to handle the errors returned by either the scan engine or the scan manager. Different antivirus scan results are handled in different manners. For example, if a scan result is clean, the traffic is forwarded to the receiver. If the scan result is infected, the traffic is dropped. If the scan results in an error, the result handling depends on the cause of the failure and the configuration (fallback settings). For more information, see the following topics:

## Understanding Full Antivirus Scan Result Handling

The Full Antivirus Scan Result Handling is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, different antivirus scan results are handled in different manners. For example, if a scan result is clean, the traffic is forwarded to the receiver. If the scan result is infected, the traffic is dropped. If the scan results in an error, the result handling depends on the cause of the failure and the configuration (fallback settings).

The following is a list of actions based on scan results:

- Scan Result = Pass

  The scan result handling action is to pass the message. In this case, no virus is detected and no error code is returned. Or, an error code is returned, but the fallback option for this error code is set to log-and-permit.

- Scan Result = Block

  The scan result handling action is to block the message. In this case, either a virus is detected or an error code is returned and the fallback option for this error code is BLOCK.

SEE ALSO

Understanding Full Antivirus Scan Level Settings | 302

## Monitoring Antivirus Scan Engine Status

**Purpose**

The Monitoring Antivirus Scan Engine Status is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, using the CLI, you can view the following scan engine status items:

Antivirus license key status

- View license expiration dates.

Scan engine status and settings

- View last action result.
- View default file extension list.

Antivirus pattern update server settings

- View update URL (HTTP or HTTPS-based).

- View update interval.

Antivirus pattern database status

- View auto update status.
- View last result of database loading.
- If the download completes, view database version timestamp virus record number.
- If the download fails, view failure reason.

**Action**

In the CLI, enter the **user@host> show security utm anti-virus status** command.

Example status result:

```
AV Key Expire Date: 03/01/2010 00:00:00
Update Server: http://update.juniper-updates.net/AV/device-name
interval: 60 minutes
auto update status: next update in 12 minutes
last result: new database loaded
AV signature version: 12/21/2008 00:35 GMT, virus records: 154018
Scan Engine Info: last action result: No error(0x00000000)
```

SEE ALSO

Understanding the Full Antivirus Scan Engine | 298

## Monitoring Antivirus Session Status

**Purpose**

The Monitoring Antivirus Session Status is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, using the CLI, you can view the following session status items:

Antivirus session status displays a snapshot of current antivirus sessions. It includes

- Maximum supported antivirus session numbers.
- Total allocated antivirus session numbers.
- Total freed antivirus session numbers.
- Current active antivirus session numbers.

**Action**

In the CLI, enter the **user@host> show security utm session status** command.

## Monitoring Antivirus Scan Results

**Purpose**

The Monitoring Antivirus Scan Results are not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, view statistics for antivirus requests, scan results, and fallback counters.

Scan requests provide

- The total number of scan request forwarded to the engine.
- The number of scan request being pre-windowed.
- The number of scan requests using scan-all mode.
- The number of scan requests using scan-by-extension mode.

Scan code counters provide

- Number of clean files.
- Number of infected files.
- Number of password protected files.
- Number of decompress layers.
- Number of corrupt files.
- When the engine is out of resources.
- When there is an internal error.

Fallback applied status provides either a log-and-permit or block result when the following has occurred

- Scan engine not ready.
- Maximum content size reached.
- Too many requests.
- Password protected file found.
- Decompress layer too large.
- Corrupt file found.
- Timeout occurred.

- Out of resources.
- Other.

**Action**

To view antivirus scan results using the CLI editor, enter the **user@host> show security utm anti-virus statistics status** command.

To view antivirus scan results using J-Web:

1. Select **Monitor>Security>UTM>Anti-Virus**.

   The following information becomes viewable in the right pane.

   Antivirus license key status

   - View license expiration dates.

   Antivirus pattern update server settings

   - View update URL (HTTP or HTTPS-based).
   - View update interval.

   Antivirus pattern database status

   - View auto update status.
   - View last result of database loading.
   - If the download completes, view database version timestamp virus record number.
   - If the download fails, view failure reason.

   Antivirus statistics provide

   - The number of scan request being pre-windowed.
   - The total number of scan request forwarded to the engine.
   - The number of scan requests using scan-all mode.
   - The number of scan requests using scan-by-extension mode.

   Scan code counters provide

   - Number of clean files.
   - Number of infected files.
   - Number of password protected files.
   - Number of decompress layers.
   - Number of corrupt files.

- When the engine is out of resources.
- When there is an internal error.

Fallback applied status provides either a log-and-permit or block result when the following has occurred

- Scan engine not ready.
- Password protected file found.
- Decompress layer too large.
- Corrupt file found.
- Out of resources.
- Timeout occurred.
- Maximum content size reached.
- Too many requests.
- Other.

2. You can click the **Clear Anti-Virus Statistics** button to clear all current viewable statistics and begin collecting new statistics.

## Understanding Antivirus Scanning Fallback Options

Fallback options notify the system how to handle the errors returned by either the scan engine or the scan manager. The following is a list of possible errors:

- Scan engine is not ready (engine-not-ready)

  The scan engine is initializing itself, for example, loading the signature database. During this phase, the scan engine is not ready to scan a file. A file could either pass or be blocked according to this setting.

- Corrupt file (corrupt-file)

  Corrupt file is the error returned by the scan engine when engine detects a corrupted file.

- Decompression layer (decompress-layer)

  Decompress layer error is the error returned by the scan engine when the scanned file has too many compression layers.

- Password protected file (password-file)

  Password protected file is the error returned by the scan engine when the scanned file is protected by a password.

- Max content size (content-size)

If the content size exceeds a set limit, the content is passed or blocked depending on the max-content-size fallback option.

- Too many requests (too-many-requests)

  If the total number of messages received concurrently exceeds the device limits, the content is passed or blocked depending on the too-many-request fallback option. (The allowed request limit is not configurable.)

- Timeout

  Scanning a complex file could consume resources and time. If the time taken for the scan exceeds the timeout setting in the antivirus profile, the processing is aborted and the content is passed or blocked without completing the virus checking. The decision is made based on the timeout fallback option.

- Out of resources (out-of-resources)

  Virus scanning requires a great deal of memory and CPU resources. Due to resource constraints, memory allocation requests can be denied by the system. This failure could be returned by either scan engine (as a scan-code) or scan manager. When out-of-resources occurs, scanning is aborted.

- Default

  All the errors other than those in the above list fall into this category. This could include either unhandled system exceptions (internal errors) or other unknown errors.

The default fallback action for all the error types is log-and-permit.

The Kaspersky and Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards.

## Example: Configuring Antivirus Scanning Fallback Options

**IN THIS SECTION**

The Antivirus Scanning Fallback options are not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, this example shows how to configure antivirus scanning fallback options.

### Requirements

Before you begin, understand the possible error types and the default fallback actions for those error types. See “Understanding Antivirus Scanning Fallback Options” on page 318.

### Overview

In this example, you configure a feature profile called kasprof, and set the fallback scanning options for default, content-size, corrupt-file, decompress-layer, engine-not-ready, out-of-resources, password-file, timeout, too-many-requests, as block.

**NOTE:** The command for changing the URL for the pattern database is:

```
[edit]
user@host# edit security utm feature-profile anti-virus kaspersky-lab-engine
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
user@host# set pattern-update url http://update.juniper-updates.net/AV/<device-name>
```

The default URL is http://update.juniper-updates.net/AV/<device-version>. You should not change this URL unless you are experiencing problems with it and have called for support.

### Configuration

#### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm feature-profile anti-virus type kaspersky-lab-engine
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options content-size
    block
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options corrupt-file
    block
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options decompress-layer
    block
```

```
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options default block
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options engine-not-ready
    block
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options out-of-resources
    block
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options password-file
    block
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options timeout block
set security utm feature-profile anti-virus kaspersky-lab-engine profile kasprof1 fallback-options
    too-many-requests block
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure scanning fallback options:

1. Select and configure the engine type.

```
[edit]
user@host# set security utm feature-profile anti-virus type kaspersky-lab-engine
```

2. Create a profile for the Kaspersky Lab engine and configure a list of fallback options as block or log-and-permit.

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
user@host# set profile kasprof1 fallback-options content-size block
user@host# set profile kasprof1 fallback-options corrupt-file block
user@host# set profile kasprof1 fallback-options decompress-layer block
user@host# set profile kasprof1 fallback-options default block
user@host# set profile kasprof1 fallback-options engine-not-ready block
user@host# set profile kasprof1 fallback-options out-of-resources block
user@host# set profile kasprof1 fallback-options password-file block
user@host# set profile kasprof1 fallback-options timeout block
user@host# set profile kasprof1 fallback-options too-many-requests block
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm feature-profile anti-virus** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host#show security utm feature-profile anti-virus
kaspersky-lab-engine {
    profile kasprof1 {
        fallback-options {
            default block;
            corrupt-file block;
            password-file block;
            decompress-layer block;
            content-size block;
            engine-not-ready block;
            timeout block;
            out-of-resources block;
            too-many-requests block;
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### *Verifying the Antivirus Scanning Fallback Options*

#### Purpose

Verify the antivirus scanning fallback options.

#### Action

From operational mode, enter the **show configuration security utm** command.

SEE ALSO

Understanding Full Antivirus Scan Level Settings | 302

**Release History Table**

| Release | Description |
|---|---|
| 15.1X49-D10 | The Full Antivirus Scan Result Handling is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Monitoring Antivirus Scan Engine Status is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Monitoring Antivirus Session Status is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Monitoring Antivirus Scan Results are not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Kaspersky and Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Antivirus Scanning Fallback options are not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |

RELATED DOCUMENTATION


- Virus-Detected Notifications | **100**
- Full Antivirus Application Protocol Scanning | **323**
- Full Antivirus Protection | **262**


# Full Antivirus Application Protocol Scanning

**IN THIS SECTION**

Full Antivirus uses a scanning engine and virus signature databases to protect against virus-infected files, worms, trojans, spyware, and other malware over POP3, HTTP, SMTP, IMAP, and FTP protocols. For more information, see the following topics:

## Understanding Full Antivirus Application Protocol Scanning

The Full Antivirus Application Protocol Scanning is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, you can turn antivirus scanning on and off on a per protocol basis. If scanning for a protocol is disabled in an antivirus profile, there is no application intelligence for this protocol. Therefore, in most cases, traffic using this protocol is not scanned. But if the protocol in question is based on another protocol for which scanning is enabled in an antivirus profile, then the traffic is scanned as that enabled protocol.

The internal antivirus scan engine supports scanning for specific Application Layer transactions allowing you to select the content (HTTP, FTP, SMTP, POP3, or IMAP traffic) to scan. For each content type that you are scanning, you have different configuration options.

Profile-based settings, including enable/disable, scan-mode, and scan result handling settings, may not be applicable to all supported protocols. The following table lists profile-based settings and their protocol support.

**Table 8: Supported Profile-based Settings By Protocol**

| Profile Setting | Protocol Support |
|---|---|
| Enable or disable scanning on per protocol basis | All protocols support this feature |
| "Understanding Full Antivirus Scan Mode Support" on page 299, including file extension scanning | All protocols support this feature |

**Table 8: Supported Profile-based Settings By Protocol *(continued)***

| Profile Setting | Protocol Support |
|---|---|
| "Understanding Full Antivirus Content Size Limits" on page 307 | All protocols support this feature |
| "Understanding Full Antivirus Decompression Layer Limits" on page 308 | All protocols support this feature |
| "Understanding Full Antivirus Scanning Timeouts" on page 309 | All protocols support this feature |
| "Understanding HTTP Trickling" on page 105 | HTTP only |
| "Understanding Antivirus Scanning Fallback Options" on page 318 | All protocols support this feature |
| Protocol specific messages | All protocols support this feature |
| "Understanding E-Mail Virus-Detected Notifications" on page 102 | SMTP, POP3, and IMAP only |
| "Understanding Custom Message Virus-Detected Notifications" on page 103 | All protocols support this feature |

SEE ALSO

Understanding Full Antivirus Scan Result Handling | 314

## Understanding HTTP Scanning

The HTTP antivirus scanning is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, if antivirus scanning is enabled for Hypertext Transfer Protocol (HTTP) traffic in a content security profile, TCP traffic to defined HTTP service ports (generally port 80) is monitored. For HTTP traffic, the security device scans both HTTP responses and requests (get, post, and put commands).

For HTTP antivirus scanning, both HTTP 1.0 and 1.1 are supported. If the protocol version is HTTP 0.x , the antivirus scanner attempts to scan the traffic. Unknown protocols are bypassed. For example, some application protocols use HTTP as the transport but do not comply with HTTP 1.0 or 1.1. These are considered unknown protocols and are not scanned.

This is a general description of how HTTP traffic is intercepted, scanned, and acted upon by the antivirus scanner:

1. An HTTP client sends an HTTP request to a webserver or a webserver responds to an HTTP request.

2. The security device intercepts the request and passes the data to the antivirus scanner, which scans it for viruses.

3. After completing the scan, the device follows one of two courses:
   - If there is no virus, the device forwards the request to the webserver.
   - If there is a virus, the device drops the request and sends an HTTP message reporting the infection to the client.

With script-only scanning, the input object is a script file. It can be JavaScript, VBScript, mIRC script, bat scripts (DOS bat files) and other text scripts. The engine matches the input content only with signatures for script files. Script scanning is applicable only for HTML content over the HTTP protocol. There are two criteria for this scan-type. First, the content-type field of this HTML document must be text or HTML. Second, there is no content encoding in the HTTP header. If those two criteria are met, an HTML parser is used to parse the HTML document.

SEE ALSO

Understanding Protocol-Only Virus-Detected Notifications | **101**

## Enabling HTTP Scanning (CLI Procedure)

The HTTP antivirus scanning is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, to enable antivirus scanning for HTTP traffic, enter the following CLI configuration statement:

```
user@host# set security utm utm-policy policy-name anti-virus http
```

## Understanding FTP Antivirus Scanning

The FTP antivirus scanning is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, if antivirus scanning is enabled for File Transfer Protocol (FTP) traffic in a content security profile,

the security device monitors the control channel and, when it detects one of the FTP commands for transferring data, it scans the data sent over the data channel.

This is a general description of how FTP traffic is intercepted, scanned, and acted upon by the antivirus scanner:

1. A local FTP client opens an FTP control channel to an FTP server and requests the transfer of some data.

2. The FTP client and server negotiate a data channel over which the server sends the requested data. The security device intercepts the data and passes it to the antivirus scan engine, which scans it for viruses.

3. After completing the scan, the device follows one of two courses:
   - If there is no virus, the device forwards the data to the client.
   - If there is a virus, the device replaces the data with a drop message in the data channel and sends a message reporting the infection in the control channel.

## Enabling FTP Antivirus Scanning (CLI Procedure)

The FTP antivirus scanning is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, to enable antivirus scanning for File Transfer Protocol (FTP) traffic, enter the following CLI configuration statement:

```
user@host# security utm utm-policy policy-name anti-virus ftp
```

**NOTE:** In order to scan FTP traffic, the FTP ALG must be enabled.

SEE ALSO

*FTP ALG Overview*

# Understanding SMTP Antivirus Scanning

IN THIS SECTION



Starting from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1, only Sophos Antivirus supports the SMTP antivirus scanning. If SMTP (Simple Mail Transfer Protocol) antivirus scanning is enabled in a content security profile, the security device redirects traffic from local SMTP clients to the antivirus scanner before sending it to the local mail server.

Chunking is an alternative to the data command. It provides a mechanism to transmit a large message in small chunks. It is not supported. Messages using chunking are bypassed and are not scanned.

This is a general description of how SMTP traffic is intercepted, scanned, and acted upon by the antivirus scanner:

1. An SMTP client sends an e-mail message to a local mail server or a remote mail server forwards an e-mail message via SMTP to the local mail server.

2. The security device intercepts the e-mail message and passes the data to the antivirus scanner, which scans it for viruses.

3. After completing the scan, the device follows one of two courses:
   - If there is no virus, the device forwards the message to the local server.
   - If there is a virus, the device sends a replacement message to the client.

This topic includes the following sections:

## Understanding SMTP Antivirus Mail Message Replacement

If the antivirus scanner finds a virus in an e-mail message, the original message is dropped, the message body is truncated, and the content is replaced by a message that may appear as follows:

```
nContent-Type: text/plain
```

```
Your mail <src_ip> : <src_port> — <dst_port>: <dst_port> contains contaminated file <filename> with virus
  <virusname>, so it is dropped.
```

If a scan error is returned and the fail mode is set to drop, the original message is dropped and the entire message body is truncated. The content is replaced by a message that may appear as follows:

```
nContent-Type: text/plain
Your mail <src_ip> : <src_port> — <dst_port>: <dst_port> is dropped for <reason>.
```

### Understanding SMTP Antivirus Sender Notification

If **notify-sender-on-virus** is set and the message is dropped due to a detected virus, an e-mail is sent to the mail sender. The content of the notification may appear as follows:

```
From: <admin>@<gateway_ip>
To: <sender_e-mail>
Subject: Mail Delivery Failure
This message is created automatically by mail delivery software. A message that you sent could not be delivered
  to one or more of its recipients for the reason:
<src_ip> : <src_port> — <dst_port>: <dst_port> <ENVID> contaminated file <filename> with virus <virusname>.
e-mail Header is:
<header of scanned e-mail>
```

If **notify-sender-on-error-drop** is set and the message is dropped due to a scan error, an e-mail is sent to the mail sender of the scanned message. The content of the e-mail may appear as follows:

```
From: <admin>@<gateway_ip>
To: <sender_e-mail>
Subject: Mail Delivery Failure
This message is created automatically by mail delivery software. A message that you sent could not be delivered
  to one or more of its recipients for the reason:
<src_ip> : <src_port> — <dst_port>: <dst_port> <ENVID> <reason>.
e-mail Header is:
<header of scanned e-mail>
```

**NOTE:** For information on the ENVID parameter, refer to RFC 3461.

### Understanding SMTP Antivirus Subject Tagging

If a scan error is returned and the fail mode is set to **pass**, the antivirus module passes the message through to the server. If **notify-recipient-on-error-pass** is set, the following string is appended to the end of the subject field:

```
(No virus check: <reason>)
```

SEE ALSO

Understanding E-Mail Virus-Detected Notifications | 102

## Enabling SMTP Antivirus Scanning (CLI Procedure)

The SMTP antivirus scanning is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, to enable antivirus scanning for SMTP traffic, enter the following CLI configuration statement:

```
user@host# set security utm utm-policy policy-name anti-virus smtp-profile
```

## Understanding POP3 Antivirus Scanning

IN THIS SECTION



The POP3 antivirus scanning is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, if Post Office Protocol 3 (POP3) antivirus scanning is enabled in a content security profile, the security device redirects traffic from a local mail server to antivirus scanner before sending it to the local POP3 client.

This is a general description of how POP3 traffic is intercepted, scanned, and acted upon by the antivirus scanner.

1. The POP3 client downloads an e-mail message from the local mail server.

2. The security device intercepts the e-mail message and passes the data to the antivirus scanner, which scans it for viruses.

3. After completing the scan, the security device follows one of two courses:
   - If there is no virus, the device forwards the message to the client.
   - If there is a virus, the device sends a message reporting the infection to the client.

     See "Understanding Protocol-Only Virus-Detected Notifications" on page 101 for information on protocol-only notifications for IMAP.

This topic includes the following sections:

### Understanding POP3 Antivirus Mail Message Replacement

If the antivirus scanner finds a virus in an e-mail message, the original message is dropped, the message body is truncated, and the content is replaced by a message that may appear as follows:

```
nContent-Type: text/plain
Your mail <src_ip> : <src_port> — <dst_port>: <dst_port> contains contaminated file <filename> with virus
   <virusname>, so it is dropped.
```

### Understanding POP3 Antivirus Sender Notification

If **notify-sender-on-virus** is set and the message is dropped due to a detected virus, an e-mail is sent to the mail sender.

```
From: <admin>@<gateway_ip>
To: <sender_e-mail>
Subject: Mail Delivery Failure
This message is created automatically by mail delivery software. A message that you sent could not be delivered
   to one or more of its recipients for the reason:
<src_ip> : <src_port> — <dst_port>: <dst_port> contaminated file <filename> with virus <virusname>.
e-mail Header is:
<header of scanned e-mail>
```

If **notify-sender-on-error-drop** is set and the message is dropped due to a scan error, an e-mail is sent to the mail sender of the scanned message. The content of the e-mail may appear as follows:

```
From: <admin>@<gateway_ip>
To: <sender_e-mail>
Subject: Mail Delivery Failure
This message is created automatically by mail delivery software. A message that you sent could not be delivered
   to one or more of its recipients for the reason:
<src_ip> : <src_port> — <dst_port>: <dst_port> <reason>.
e-mail Header is:
<header of scanned e-mail>
```

### Understanding POP3 Antivirus Subject Tagging

If a scan error is returned and the fail mode is set to **pass**, the antivirus module passes the message through to the server. If **notify-recipient-on-error-pass** is set, the following string is appended to the end of subject field:

```
(No virus check: <reason>)
```

SEE ALSO

Understanding Protocol-Only Virus-Detected Notifications | **101**

## Enabling POP3 Antivirus Scanning (CLI Procedure)

The POP3 antivirus scanning is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, to enable antivirus scanning for POP3 traffic, enter the following CLI configuration statement:

```
user@host# set security utm utm-policy policy-name anti-virus pop3-profile
```

# Understanding IMAP Antivirus Scanning

IN THIS SECTION



The IMAP antivirus scanning is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, if IMAP (Internet Message Access Protocol) antivirus scanning is enabled in a content security profile, the security device redirects traffic from a local mail server to the internal antivirus scanner before sending it to the local IMAP client.

This is a general description of how IMAP traffic is intercepted, scanned, and acted upon by the antivirus scanner.

1. The IMAP client downloads an e-mail message from the local mail server.

2. The security device intercepts the e-mail message and passes the data to the antivirus scanner, which scans it for viruses.

3. After completing the scan, the security device follows one of two courses:
   - If there is no virus, the device forwards the message to the client.
   - If there is a virus, the device sends a message reporting the infection to the client.

     See “Understanding Protocol-Only Virus-Detected Notifications” on page 101 for information on protocol-only notifications for IMAP.

This topic includes the following sections:

## Understanding IMAP Antivirus Mail Message Replacement

If the antivirus scanner finds a virus in an e-mail message, the original message is dropped, the message body is truncated, and the content is replaced by a message that may appear as follows:

```
nContent-Type: text/plain
```

```
Your mail <src_ip> : <src_port> — <dst_port>: <dst_port> contains contaminated file <filename> with virus
   <virusname>, so it is dropped.
```

### Understanding IMAP Antivirus Sender Notification

If **notify-sender-on-virus** is set and the message is dropped due to a detected virus, an e-mail is sent to the mail sender.

```
From: <admin>@<gateway_ip>
To: <sender_e-mail>
Subject: Mail Delivery Failure
This message is created automatically by mail delivery software. A message that you sent could not be delivered
   to one or more of its recipients for the reason:
<src_ip> : <src_port> — <dst_port>: <dst_port> contaminated file <filename> with virus <virusname>.
e-mail Header is:
<header of scanned e-mail>
```

If **notify-sender-on-error-drop** is set and the message is dropped due to a scan error, an e-mail is sent to the mail sender of the scanned message. The content of the e-mail may appear as follows:

```
From: <admin>@<gateway_ip>
To: <sender_e-mail>
Subject: Mail Delivery Failure
This message is created automatically by mail delivery software. A message that you sent could not be delivered
   to one or more of its recipients for the reason:
<src_ip> : <src_port> — <dst_port>: <dst_port> <reason>.
e-mail Header is:
<header of scanned e-mail>
```

### Understanding IMAP Antivirus Subject Tagging

If a scan error is returned and the fail mode is set to **pass**, the antivirus module passes the message through to the server. If **notify-recipient-on-error-pass** is set, the following string is appended to the end of subject field:

```
(No virus check: <reason>)
```

### Understanding IMAP Antivirus Scanning Limitations

Mail Fragments — It is possible to chop one e-mail into multiple parts and to send each part through a different response. This is called mail fragmenting and most popular mail clients support it in order to send and receive large e-mails. Scanning of mail fragments is not supported by the antivirus scanner and in such cases, the message body is not scanned.

Partial Content — Some mail clients treat e-mail of different sizes differently. For example, small e-mails (less than 10 KB) are downloaded as a whole. Large e-mails (for example, less than 1 MB) are chopped into 10 KB pieces upon request from the IMAP server. Scanning of any partial content requests is not supported by the antivirus scanner.

IMAP Uploads — Only antivirus scanning of IMAP downloads is supported. IMAP upload traffic is not scanned.

## Enabling IMAP Antivirus Scanning (CLI Procedure)

The IMAP antivirus scanning is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, to enable antivirus scanning for IMAP traffic, enter the following CLI configuration statement:

```
user@host# security utm utm-policy policy-name anti-virus imap-profile
```

**Release History Table**

| Release | Description |
|---|---|
| 15.1X49-D10 | The Full Antivirus Application Protocol Scanning is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The HTTP antivirus scanning is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The HTTP antivirus scanning is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The FTP antivirus scanning is not supported from Junos OS Release 15.1X49-D10 onwards. |
| 15.1X49-D10 | The FTP antivirus scanning is not supported from Junos OS Release 15.1X49-D10 onwards. |
| 15.1X49-D10 | Starting from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1, only Sophos Antivirus supports the SMTP antivirus scanning. |
| 15.1X49-D10 | The SMTP antivirus scanning is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The POP3 antivirus scanning is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The POP3 antivirus scanning is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The IMAP antivirus scanning is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The IMAP antivirus scanning is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |

## RELATED DOCUMENTATION

Virus-Detected Notifications | **100**

HTTP Trickling to Prevent Timeouts | **105**

Full Antivirus Protection Overview | 262

# Integrated Web Filtering

IN THIS SECTION



Enhanced Web Filtering (EWF) with Websense is an integrated URL filtering solution. When you enable the solution on the device, the firewall intercepts the HTTP and the HTTPS requests and sends the HTTP URL or the HTTPS source IP to the Websense ThreatSeeker Cloud (TSC). For more information, see the following topics:

## Understanding Integrated Web Filtering

IN THIS SECTION



The Integrated Web Filtering is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, with integrated Web filtering, the firewall intercepts every HTTP request in a TCP connection and extracts the URL from the HTTP request. Each individual HTTP request is blocked or permitted based on URL filtering profiles defined by you. The decision making is done on the device after it identifies a category for a URL.

The Surf-Control feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards.

A URL category is a list of URLs grouped by content. URL categories are predefined and maintained by Surf-Control or are defined by you. Surf-Control maintains about 40 predefined categories. When defining your own URL categories, you can group URLs and create categories specific to your needs.

You define your own categories using URL pattern list and custom URL category list custom objects. Once defined, you can select your categories when you configure your Web filtering profile. Each category can have a maximum of 20 URLs. When you create a category, you can add either the URL or the IP address of a site. When you add a URL to a user-defined category, the device performs DNS lookup, resolves the host name into IP addresses, and caches this information. When a user tries to access a site with the IP address of the site, the device checks the cached list of IP addresses and tries to resolve the hostname. Many sites have dynamic IP addresses, meaning that their IP addresses change periodically. A user attempting to access a site can type an IP address that is not in the cached list on the device. Therefore, if you know the IP addresses of sites you are adding to a category, enter both the URL and the IP address(es) of the site.

If a URL appears in both a user-defined category and a predefined category, the device matches the URL to the user-defined category.

Web filtering is performed on all the methods defined in HTTP 1.0 and HTTP 1.1.

The integrated Web filtering solution intercepts every HTTP request in a TCP connection. In this case, the decision making is done on the device after it identifies the category for a URL either from user-defined categories or from a category server (SurfControl Content Portal Authority provided by Websense). The Integrated Web filtering is not supported from Junos OS Release 15.1X49-D10 onwards.

The integrated Web filtering feature is a separately licensed subscription service. When the license key for Web filtering has expired, no URLs are sent to the category server for checking, only local user-defined categories are checked.

Integrated Web filtering solution is supported only on SRX210, SRX220, SRX240, SRX550, and SRX650 devices.

This topic contains the following sections:

### Integrated Web Filtering Process

This is a general description of how Web traffic is intercepted and acted upon by the Web filtering module.

1. The device intercepts a TCP connection.

2. The device intercepts each HTTP request in the TCP connection.

3. The device extracts each URL in the HTTP request and checks its URL filter cache.

4. Global Web filtering allowlists and blocklists are checked first for block or permit.

5. If the HTTP request URL is allowed based on cached parameters, it is forwarded to the webserver. If there is no cache match, a request for categorization is sent to the SurfControl server. (If the HTTP request URL is blocked, the request is not forwarded and a notification message is logged.)

6. In the allowed case, the SurfControl server responds with the corresponding category.

7. Based on the identified category, if the URL is permitted, the device forwards the HTTP request to the webserver. If the URL is not permitted, then a deny page is sent to the HTTP client.

### Integrated Web Filtering Cache

By default, the device retrieves and caches the URL categories from the SurfControl CPA server. This process reduces the overhead of accessing the SurfControl CPA server each time the device receives a new request for previously requested URLs. You can configure the size and duration of the cache, according to the performance and memory requirements of your networking environment. The lifetime of cached items is configurable between 1 and 1800 seconds with a default value of 300 seconds.

Caches are not preserved across device reboots or power losses.

### Integrated Web Filtering Profiles

You configure Web filtering profiles that permit or block URLs according to defined categories. A Web filtering profile consists of a group of URL categories assigned one of the following actions:

- Permit — The device always allows access to the websites in this category.
- Block — The device blocks access to the websites in this category. When the device blocks access to this category of websites, it displays a message in your browser indicating the URL category.
- Blocklist — The device always blocks access to the websites in this list. You can create a user-defined category.
- Allowlist — The device always allows access to the websites in this list. You can create a user-defined category.

> **NOTE:** A predefined profile is provided and can be used if you choose not to define your own profile.

A Web filtering profile may contain one blocklist or one allowlist, multiple user-defined and/or predefined categories each with a permit or block action, and an *Other* category with a permit or block action. You can define an action for all *Other* categories in a profile to specify what to do when the incoming URL does

not belong to any of the categories defined in the profile. If the action for the *Other* category is block, the incoming URL is blocked if it does not match any of the categories explicitly defined in the profile. If an action for the *Other* category is not specified, the default action of permit is applied to the incoming URL not matching any category.

### Profile Matching Precedence

When a profile employs several categories for URL matching, those categories are checked for matches in the following order:

1. If present, the global blocklist is checked first. If a match is made, the URL is blocked. If no match is found...

2. The global allowlist is checked next. If a match is made, the URL is permitted. If no match is found...

3. User-defined categories are checked next. If a match is made, the URL is blocked or permitted as specified. If no match is found...

4. Predefined categories are checked next. If a match is made, the URL is blocked or permitted as specified. If no match is found...

5. The Other category is checked next. If a match is made, the URL is blocked or permitted as specified.

SEE ALSO


- Enhanced Web Filtering Overview | **150**
- Understanding Redirect Web Filtering | **208**
- Understanding Local Web Filtering | **192**


## Example: Configuring Integrated Web Filtering

**IN THIS SECTION**

The Integrated Web Filtering is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, this example shows how to configure integrated Web filtering.

### Requirements

Before you begin, learn more about Web filtering. See “Web Filtering Overview” on page 147.

### Overview

In this example you configure integrated Web filtering custom objects, integrated Web filtering feature profiles, and integrated Web filtering UTM policies. You also attach integrated Web filtering UTM policies to security policies.

In the first example configuration you create a custom object called urllist3 that contains the pattern http://www.example.net 1.2.3.4. The urllist3 custom object is then added to the custom URL category custurl3.

In the second example configuration, you configure the Web filtering feature profile. You set the URL blocklist filtering category to **custblacklist**, set the allowlist filtering category to **custwhitelist** and the type of Web filtering engine to surf-control-integrated. Then you set the cache size parameters for Web filtering to 500 KB, which is the default, and the cache timeout parameters to 1800.

You name the Surf Control server as surfcontrolserver and enter 8080 as the port number for communicating with it. (Default ports are 80, 8080, and 8081.) Then you create a surf-control-integrated profile name called surfprofile1.

Next you select a category from the included allowlist and blocklist categories or select a custom URL category list you created for filtering against. Then you enter an action (permit, log and permit, block) to go with the filter. You do this as many times as necessary to compile your allowlists and blocklists and their accompanying actions. This example blocks URLs in the custurl3 category.

Then you enter a custom message to be sent when HTTP requests are blocked. This example configures the device to send an ***access denied*** message. You select a default action (permit, log and permit, block) for this profile for requests that experience errors. This example sets the default action to block. You select fallback settings (block or log and permit) for this profile, in case errors occur in each configured category. This example sets fallback settings to block.

Finally, you enter a timeout value in seconds. Once this limit is reached, fail mode settings are applied. The default is 10 seconds, and you can enter a value from 10 to 240 seconds. This example sets the timeout value to 10.

In the third example configuration, you create UTM policy utmp5 and attach it to profile surfprofile1.

In the final example configuration, you attach the UTM policy utmp5 to the security policy p5.

## Configuration

IN THIS SECTION



### *Configuring Integrated Web Filtering Custom Objects*

#### CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm custom-objects url-pattern urllist3 value http://www.example.net
set security utm custom-objects url-pattern urllist3 value 1.2.3.4
set security utm custom-objects url-pattern urllistblack value http://www.untrusted.com
set security utm custom-objects url-pattern urllistblack value 13.13.13.13
set security utm custom-objects url-pattern urllistwhite value http://www.trusted.com
set security utm custom-objects url-pattern urllistwhite value 7.7.7.7
set security utm custom-objects custom-url-category custurl3 value urllist3
set security utm custom-objects custom-url-category custblacklist value urllistblack
set security utm custom-objects custom-url-category custwhiltelist value urllistwhite
```

Custom category does not take precedence over predefined categories when it has the same name as one of the predefined categories. We do not recommend having a custom category name be the same as the predefined category name.

#### Step-by-Step Procedure

To configure integrated Web filtering:

1. Create custom objects and create the URL pattern list.

```
[edit security utm]
user@host# set custom-objects url-pattern urllist3 value [http://www.example.net 1.2.3.4]
```

2. Configure the custom URL category list custom object using the URL pattern list.

```
[edit security utm]
user@host# set custom-objects custom-url-category custurl3 value urllist3
```

3. Create a list of untrusted sites.

```
[edit security utm]
user@host# set custom-objects url-pattern urllistblack value [http://www.untrusted.com 13.13.13.13]
```

4. Configure the custom URL category list custom object using the URL pattern list of untrusted sites.

```
[edit security utm]
user@host# set custom-objects custom-url-category custblacklist value urllistblack
```

5. Create a list of trusted sites.

```
[edit security utm]
user@host# set custom-objects url-pattern urllistwhite value [http://www.trusted.com 7.7.7.7]
```

6. Configure the custom URL category list custom object using the URL pattern list of trusted sites.

```
[edit security utm]
user@host# set custom-objects custom-url-category custwhitelist value urllistwhite
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm custom-objects** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this show command output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]
userhost#show security utm custom-objects
   url-pattern {
      urllist3 {
         value [ http://www.example.net ];
      }
```

```
        urllistblack {
            value [ http://www.untrusted.com 13.13.13.13 ];
        }
        urllistwhite {
            value [ http://www.trusted.com 7.7.7.7 ];
        }
    }
        custom-url-category {
            custurl3 {
                value urllist3;
            }
            custblacklist {
                value urllistblack;
            }
            custwhiltelist {
                value urllistwhite;
            }
        }
```

If you are done configuring the device, enter **commit** from configuration mode.

***Configuring the Integrated Web Filtering Feature Profiles***

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm feature-profile web-filtering url-whitelist custwhitelist
set security utm feature-profile web-filtering url-blacklist custblacklist
set security utm feature-profile web-filtering surf-control-integrated cache timeout 1800
set security utm feature-profile web-filtering surf-control-integrated cache size 500
set security utm feature-profile web-filtering surf-control-integrated server host surfcontrolserver
set security utm feature-profile web-filtering surf-control-integrated server port 8080
set security utm feature-profile web-filtering surf-control-integrated profile surfprofile1 category custurl3
    action block
set security utm feature-profile web-filtering surf-control-integrated profile surfprofile1 default block
set security utm feature-profile web-filtering surf-control-integrated profile surfprofile1 custom-block-message
    "***access denied ***"
set security utm feature-profile web-filtering surf-control-integrated profile surfprofile1 fallback-settings default
    block
set security utm feature-profile web-filtering surf-control-integrated profile surfprofile1 fallback-settings
    server-connectivity block
```

```
set security utm feature-profile web-filtering surf-control-integrated profile surfprofile1 fallback-settings timeout
    block
set security utm feature-profile web-filtering surf-control-integrated profile surfprofile1 fallback-settings
    too-many-requests block
set security utm feature-profile web-filtering surf-control-integrated profile surfprofile1 timeout 10
set security utm feature-profile content-filtering profile contentfilter1
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure integrated Web filtering feature profiles:

1. Configure the Web filtering URL Blocklist.

   ```
   [edit security utm feature-profile web-filtering]
   user@host# set url-blacklist custblacklist
   ```

2. Configure the Web filtering URL Allowlist.

   ```
   [edit security utm feature-profile web-filtering]
   user@host# set url-whitelist custwhitelist
   ```

3. Specify the surf-control-integrated Web filtering engine and set the cache size parameters.

   ```
   [edit security utm feature-profile web-filtering]
   user@host# set surf-control-integrated cache size 500
   ```

4. Set the cache timeout parameters.

   ```
   [edit security utm feature-profile web-filtering]
   user@host# set surf-control-integrated cache timeout 1800
   ```

5. Set the server name or IP address.

   ```
   [edit security utm feature-profile web-filtering]
   user@host# set surf-control-integrated server host surfcontrolserver
   ```

6. Enter the port number for communicating with the server.

```
[edit security utm feature-profile web-filtering]
user@host# set surf-control-integrated server port 8080
```

7. Create a profile name and select a category from the included allowlist and blocklist categories.

```
[edit security utm feature-profile web-filtering]
user@host# set surf-control-integrated profile surfprofile1 category custurl3 action block
```

8. Enter a custom message to be sent when HTTP requests are blocked.

```
[edit security utm feature-profile web-filtering]
user@host# set surf-control-integrated profile surfprofile1 custom-block-message “***access denied***”
```

9. Select a default action (permit, log and permit, block) for this profile for requests that experience errors.

```
[edit security utm feature-profile web-filtering]
user@host# set surf-control-integrated profile surfprofile1 default block
```

10. Select fallback settings (block or log and permit) for this profile.

```
[edit security utm feature-profile web-filtering]
user@host# set surf-control-integrated profile surfprofile1 fallback-settings default block
```

```
user@host# set surf-control-integrated profile surfprofile1 fallback-settings server-connectivity block
user@host# set surf-control-integrated profile surfprofile1 fallback-settings timeout block
user@host# set surf-control-integrated profile surfprofile1 fallback-settings too-many-requests block
```

11. Enter a timeout value, in seconds.

```
[edit security utm feature-profile web-filtering]
user@host# set surf-control-integrated profile surfprofile1 timeout 10
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm feature-profile** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
userhost#show security utm feature-profile
    web-filtering {
        url-whitelist custwhitelist;
        url-blacklist custblacklist;
    type juniper-local;
        surf-control-integrated {
            cache {
                timeout 1800;
                size 500;
            }
            server {
                host surfcontrolserver;
                port 8080;
            }
            profile surfprofile1 {
                category {
                    custurl3 {
                        action block;
                    }
                }
                default block;
                custom-block-message "***access denied ***";
                fallback-settings {
                    default block;
                    server-connectivity block;
                    timeout block;
                    too-many-requests block;
                }
                timeout 10;
            }
        }
        content-filtering {
            profile contentfilter1;
        }
```

If you are done configuring the device, enter **commit** from configuration mode.

***Configuring Integrated Web Filtering UTM Policies***

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security utm utm-policy utmp5 web-filtering http-profile surfprofile1
```

**Step-by-Step Procedure**

To configure a UTM policy:

1. Create the UTM policy referencing a profile.

```
[edit]
user@host# set security utm utm-policy utmp5 web-filtering http-profile surfprofile1
```

**Results**

From configuration mode, confirm your configuration by entering the **show security utm utm-policy** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
userhost#show security utm utm-policy
...
   utm-policy utmp5 {
      content-filtering {
         http-profile contentfilter1;
      }
      web-filtering {
         http-profile surfprofile1;
      }
   }
```

If you are done configuring the device, enter **commit** from configuration mode.

***Attaching Integrated Web Filtering UTM Policies to Security Policies***

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security policies from-zone trust to-zone untrust policy p5 match source-address any
set security policies from-zone trust to-zone untrust policy p5 match destination-address any
set security policies from-zone trust to-zone untrust policy p5 match application junos-http
set security policies from-zone trust to-zone untrust policy p5 then permit application-services utm-policy
   utmp5
```

**Step-by-Step Procedure**

To attach a UTM policy to a security policy:

1. Create and configure the security policy.

```
[edit security policies from-zone trust to-zone untrust policy p5]
user@host# set match source-address any
user@host# set match destination-address any
user@host# set match application junos-http
```

2. Attach the UTM policy to the security policy.

```
[edit security policies from-zone trust to-zone untrust policy p5]
user@host# set then permit application-services utm-policy utmp5
```

**Results**

From configuration mode, confirm your configuration by entering the **show security policies** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
userhost#show security policies
   from-zone trust to-zone untrust {
      policy p5 {
         match {
            source-address any;
            destination-address any;
            application junos-http;
         }
         then {
            permit {
               application-services {
                  utm-policy utmp5;
               }
            }
         }
      }
   }
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

IN THIS SECTION



To confirm that the configuration is working properly, perform these tasks:

***Verifying the Configuration of Integrated Web Filtering Custom Objects***

**Purpose**

Verify the configuration of integrated Web filtering custom objects.

**Action**

From the top of the configuration in configuration mode, enter the **show security utm custom-objects** command.

***Verifying the Configuration of Integrated Web Filtering Feature Profiles***

**Purpose**

Verify the configuration of integrated Web filtering feature profiles.

**Action**

From the top of the configuration in configuration mode, enter the **show security utm feature-profile** command.

***Verifying the Configuration of Integrated Web Filtering UTM Policies***

**Purpose**

Verify the configuration of integrated Web filtering UTM policies.

**Action**

From the top of the configuration in configuration mode, enter the **show security utm** command.

***Verifying the Attachment of Integrated Web Filtering UTM Policies to Security Policies***

**Purpose**

Verify the attachment of integrated Web filtering UTM policies to security policies.

**Action**

From the top of the configuration in configuration mode, enter the **show security policies** command.

SEE ALSO

Example: Enhancing Security by Configuring Redirect Web Filtering Using Custom Objects | 210

## Displaying Global SurfControl URL Categories

**Purpose**

The Surf-Control feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. For previous releases, view global URL categories defined and maintained by SurfControl.

**Action**

Enter the **user@host# show groups junos-defaults** CLI command. You can also look for **custom-url-category**.

**Release History Table**

| Release | Description |
|---|---|
| 15.1X49-D10 | The Integrated Web Filtering is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Surf-Control feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Integrated Web filtering is not supported from Junos OS Release 15.1X49-D10 onwards. |
| 15.1X49-D10 | The Integrated Web Filtering is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |
| 15.1X49-D10 | The Surf-Control feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards. |

RELATED DOCUMENTATION

Redirect Web Filtering | 207

Monitoring Web Filtering Configurations | 230

CHAPTER 7

# Configuration Statements

# action (Security UTM Web Filtering)

**Syntax**

```
action (block | log-and-permit | permit | quarantine);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated profile profile-name category
    customurl-last-name]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name category customurl-last-name]
```

**Release Information**

The Surf-Control feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for UTM Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Enter an action to go with the customurl-list filter.

**Options**

- block—Log the error and deny the traffic.
- log-and-permit—Log the error and permit the traffic.
- permit—Permit the traffic.
- quarantine—Show the warning message and permit/block the traffic based on user input.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# address-blacklist

**Syntax**

```
address-blacklist list-name;
```

**Hierarchy Level**

```
[edit security utm feature-profile anti-spam]
[edit security utm default-configuration]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Enter an address blocklist (or allowlist) custom object for local list spam filtering.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# address-whitelist

**Syntax**

```
address-whitelist list-name;
```

**Hierarchy Level**

```
[edit security utm feature-profile anti-spam]
[edit security utm default-configuration]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Enter an address-allowlist (or blocklist) custom-object for local list spam filtering.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# admin-email

**Syntax**

admin-email *email-address*;

**Hierarchy Level**

[edit security utm feature-profile anti-virus juniper-express-engine pattern-update email-notify]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update email-notify]
[edit security utm feature-profile anti-virus sophos-engine pattern-update email-notify]
[edit security utm default-configuration anti-virus avira-engine pattern-update email-notify]

**Release Information**

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for Avira engine added in Junos OS Release 18.4R1.

**Description**

You can configure the device to notify a specified administrator when patterns are updated. This is an e-mail notification with a custom message and a custom subject line.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# administrator-email (Security Fallback Block)

**Syntax**

```
administrator-email email-address;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options
    fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options
    fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options fallback-block]
```

**Release Information**

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure the administrator e-mail address that will be notified when a fallback-block occurs. This is an e-mail notification with a custom message and a custom subject line.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# administrator-email (Security Virus Detection)

**Syntax**

```
administrator-email email address;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine profile profile name notification-options virus-detection]
```

**Release Information**

Statement introduced in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure the administrator e-mail address that will be notified when a virus is detected by Sophos antivirus. This is an e-mail notification with a custom message and a custom subject line.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# allow-email (Security Fallback Block)

**Syntax**

```
allow-email;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options
    fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options
    fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options fallback-block]
```

**Release Information**

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Enable e-mail notification to notify a specified administrator when a fallback-block occurs.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# allow-email (Security Virus Detection)

**Syntax**

```
allow–email;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus profile notification-options virus-detect]
```

**Release Information**

Statement introduced in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Enable e-mail notification to notify a specified administrator when a virus is detected.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# application (Security Policies)

**Syntax**

```
application {
    [application];
    any;
}
```

**Hierarchy Level**

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name match]
```

```
[edit security policies global policy policy-name match]
```

**Release Information**

Statement introduced in Junos OS Release 8.5.

**Description**

Specify the IP or remote procedure call (RPC) application or set of applications to be used as match criteria.

Starting in Junos OS Release 19.1R1, configuring the **application** statement at the **[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match]** hierarchy level is optional if the **dynamic-application** statement is configured at the same hierarchy level.

**Options**

***application-name-or-set***—Name of the predefined or custom application or application set used as match criteria.

**any**—Any predefined or custom applications or application sets.

> **NOTE:** A custom application that does not use a predefined destination port for the application will not be included in the **any** option, and must be named explicitly.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

*Security Policies Overview*

*Configure Applications in Unified Policies*

# application-proxy (Security UTM)

**Syntax**

```
application-proxy {
    traceoptions {
        flag flag;
    }
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure trace options for the application proxy.

**Options**

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# anti-spam

**Syntax**

```
anti-spam {
    address-blacklist list-name;
    address-whitelist list-name;
    sbl {
        profile profile-name {
            custom-tag-string [string];
            (sbl-default-server | no-sbl-default-server);
            spam-action (block | tag-header | tag-subject);
        }
    }
    traceoptions flag flag;
}
```

**Hierarchy Level**

```
[edit security utm feature-profile]
[edit security utm default-configuration]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure UTM antispam features. You can also configure the default UTM configuration for antispam feature profile. If you do not configure any option in the antispam feature profile, the values configured in the default UTM configuration are applied.

The antispam feature examines transmitted e-mail messages to identify e-mail spam. When the device detects a message deemed to be spam, it blocks the e-mail message or tags the e-mail message header or subject with a preprogrammed string. Antispam filtering uses both a third-party server-based Spam Block List (SBL) and optionally created local allowlists (benign) and blocklists (malicious) for filtering against e-mail messages.

**NOTE:** A license check for the antispam configuration is performed at the time of a commit and will provide a warning if a valid license is not installed on the device. Once a valid license is installed on the device then a custom antispam profile or the default profile will be able to process traffic. If a license is expired or is not installed, the antivirus service will not process traffic.

In the default UTM profile, the antispam type is configured as SBL instead of none. This configuration enables SBL. However, to use this feature, you must enable the SBL server using the **[edit security utm default-configuration anti-spam sbl sbl-default-server]** command.

**Options**

**anti-spam**—Configure antispam feature.

**address-blacklist**—Enter an address blocklist custom object for local list spam filtering.

**address-whitelist**—Enter an address-allowlist custom-object for local list spam filtering.

**sbl**—Antispam filtering allows you to use both a third-party server-based spam block list (SBL) and to optionally create your own local allowlists and blocklists for filtering against e-mail messages.

**traceoptions**—Defines tracing operations for UTM antispam features.

**type**—Antispam type.

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# anti-spam (Security UTM Policy)

### Syntax

```
anti-spam {
    smtp-profile profile-name;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name]
[edit logical-systems logical-system-name security utm utm-policy policy-name]
[edit tenants tenant-name security utm utm-policy policy-name]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for configuration in logical systems introduced in Junos OS Release 18.3R1.
Support for configuration in tenant systems introduced in Junos OS Release 19.2R1.

### Description

Configures a UTM policy for the antispam SMTP protocol and attach this policy to a security profile to implement it. The device can block and drop detected spam at either the connection level or the e-mail level. When the SMTP sender is identified as a spam sender based on its IP address, the SMTP connection is rejected and dropped. When a particular e-mail sender is identified as spam sender based on its sender address, the e-mail is rejected and dropped.

### Options

The statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Antispam Filtering Overview | 108

# anti-virus

**Syntax**

```
anti-virus {
    mime-whitelist {
        exception;
        list;
    }
    sophos-engine {
        fallback-options {
            content-size (block | log-and-permit | permit);
            default (block | log-and-permit | permit);
            engine-not-ready (block | log-and-permit | permit);
            out-of-resources (block | log-and-permit | permit);
            timeout (block | log-and-permit | permit);
            too-many-requests (block | log-and-permit | permit);
        }
        notification-options {
            fallback-block {
                custom-message;
                custom-message-subject;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
            fallback-non-block {
                custom-message;
                custom-message-subject;
                (notify-mail-recipient | no-notify-mail-recipient);
            }
            virus-detection {
                custom-message;
                custom-message-subject;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
        }
        pattern-update {
            email-notify {
                admin-email;
                custom-message;
                custom-message-subject;
            }
            interval;
```

```
            no-autoupdate;
            proxy {
                password;
                port;
                server;
                username;
            }
            routing-instance;
            url;
        }
        scan-options {
            content-size-limit;
            timeout seconds;
            (uri-check | no-uri-check);
        }
        server {
            ip;
            routing-instance;
        }
        sxl-retry;
        sxl-timeout seconds;
        trickling timeout;
    }
    traceoptions {
        flag name;
    }
    url-whitelist;
}
```

**Hierarchy Level**

```
[edit security utm feature-profile]
[edit security utm default-configuration]
```

**Release Information**

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure UTM Sophos antivirus features. You can also configure the default UTM configuration for antivirus feature profile. If you do not configure any option in the antivirus feature profile, the values configured in the default UTM configuration are applied. Antivirus, one of several features including content filtering, antispam, and Web filtering, makes up Juniper's UTM suite, provides the ability to prevent threats at the gateway before they enter the network.

> **NOTE:** A license check for the antivirus configuration is performed at the time of a commit and will provide a warning if a valid license is not installed on the device. Once a valid license is installed on the device then a custom antivirus profile or the default profile will be able to process traffic. If a license is expired or is not installed, the antivirus service will not process traffic.

**Options**

**anti-virus**—Configure antivirus feature.

**mime-whitelist**—This is the comprehensive list for those MIME types that can bypass antivirus scanning.

**sophos-engine**—The antivirus engine that is used on the device. You can only have one engine type running and you must restart the device if you change engines.

**fallback-options**—Fallback options tell the system how to handle the errors.

**notification-options**—There are multiple notification options you can configure to trigger when a virus is detected.

**fallback-non-block**—Notifications for fallback nonblocking actions.

**virus-detection**—Notification to send when a virus is detected.

**pattern-update**—You can configure the security device to regularly update the pattern file automatically, or you can update the file manually.

**scan-options**—Antivirus sophos-engine scan options.

**server**—Sophos Antivirus (SAV) and antispam first hop DNS server.

**sxl-retry**—Number of retry attempts to the remote Sophos Extensible List (SXL) server when a request timeout occurs.

**Range:** 0 through 5

**sxl-timeout** —Timeout value for responses to a Sophos checksum or URI query.

**Range:** 1 through 5

**trickling** —HTTP trickling is a mechanism used to prevent the HTTP client or server from timing-out during a file transfer or during antivirus scanning.

**traceoptions** —Define tracing operations for UTM antivirus features.

**url-whitelist**—Antivirus URL allowlist. A URL allowlist is a unique custom list that you define in which all the URLs or IP addresses in that list for a specified category are always bypassed for scanning.

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# anti-virus (Security UTM Policy)

### Syntax

```
anti-virus {
    ftp {
        download-profile profile-name;
        upload-profile profile-name;
    }
    http-profile profile-name;
    imap-profile profile-name;
    pop3-profile profile-name;
    smtp-profile profile-name;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name]
[edit logical-systems logical-systems-name security utm utm-policy policy-name]
[edit tenants tenant-name security utm utm-policy policy-name]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for configuration in logical systems introduced in Junos OS Release 18.3R1.
Support for configuration in tenant systems introduced in Junos OS Release 19.2R1.

### Description

Configures a UTM policy for the antivirus protocols and attaches this policy to a security profile to implement it. The internal antivirus scan engine supports scanning for specific Application Layer transactions allowing you to select the content (HTTP, FTP, SMTP, POP3, or IMAP traffic) to scan.

### Options

The statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# avira-engine

**Syntax**

```
avira-engine {
    pattern-update {
        email-notify {
            admin-email admin-email;
            custom-message custom-message;
            custom-message-subject custom-message-subject;
        }
        interval interval;
        no-autoupdate;
        proxy-profile proxy-profile;
        routing-instance routing-instance;
        start-time start-time;
        url url;
    }
}
```

**Hierarchy Level**

```
[edit security utm default-configuration anti-virus]
```

**Release Information**

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Statement introduced in Junos OS Release 18.4R1.

**Description**

The Avira scan engine is a licensed feature provided as a downloadable module. Download and install the Avira scan engine either through SRX with Internet connectivity to Juniper hosted URL, user hosted URL, or manually.

The Antivirus engine provides a full file-based virus scanning function which is available through a licensed subscription service. When your antivirus license key expires, you can continue to use the locally stored antivirus signatures without any updates. In case, the local database is deleted, antivirus scanning is also disabled.

**Required Privilege Level**

security— To view this statement in the configuration.
security-control— To add this statement to the configuration.

# block-command

**Syntax**

```
block-command protocol-command-list;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Apply protocol block command custom-objects to the content-filtering profile.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# block-content-type

**Syntax**

```
block-content-type (activex | exe | http-cookie | java-applet | zip);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Apply blocks to other available content such as exe, http-cookie, java-applet. This is for HTTP only.

**Options**

- **activex**—Block ActiveX.
- **exe**—Block EXE files.
- **http-cookie**—Block cookies.
- **java-applet**—Block Java applets.
- **zip**—Block ZIP files.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# block-extension

**Syntax**

```
block-extension extension-list;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Apply block extensions to the content-filtering profile.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# block-message (Security UTM)

**Syntax**

```
block-message {
    type {
        custom-redirect-url;
    }
    url url;
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure Juniper enhanced block message settings.

**Options**

- **type**—Specify the following type of the block message:
  - **custom-redirect-url**—Specify Custom redirect URL server.
- **url *url***—Specify an URL of the block message.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# block-mime

### Syntax

```
block-mime {
    exception list-name;
    list list-name;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Apply MIME pattern list custom-objects to the content-filtering profile for blocking MIME types.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# cache

### Syntax

```
cache {
    size value;
    timeout value;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated]
[edit security utm feature-profile web-filtering juniper-enhanced]
```

### Release Information

The Surf-Control feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 for surf-control integrated.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Set the cache parameters for Surf-Control-Integrated Web filtering and Enhanced Web Filtering.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# category (Security Logging)

**Syntax**

```
category (all | content-security | fw-auth | screen | alg | nat | flow | sctp | gtp | ipsec | idp | rtlog | pst-ds-lite | appqos
    | secintel)
```

**Hierarchy Level**

```
[edit security log stream stream-name]
[edit logical-systems name security log stream stream-name]
[edit tenants tenant-name security log stream stream-name]
```

**Release Information**

Statement introduced in Junos OS Release 10.0. Statement modified in Junos OS Release 15.1X49-D40. The [edit **logical-systems** *name* security log stream *stream-name*] hierarchy level introduced in Junos OS Release 18.2R1.

The [edit **tenants** *tenant-name* security log stream *stream-name*] hierarchy levels introduced in Junos OS Release 18.3R1.

**Description**

Set the category of logging to **all** or **content-security**. Note that for the WELF format, the category must be set to **content-security**.

**Options**

- **all**—All events are logged. By default, all the events listed in the **category** parameter are logged.
- **content-security**—Only content security events are logged.
- **fw-auth**—Firewall authentication events are logged.
- **screen**—Screen events are logged.
- **alg**—Application Layer Gateway (ALG) events are logged.
- **nat**—Network Address Translation (NAT) events are logged.
- **flow**—Flow events are logged.
- **sctp**—Stream Control Transmission Protocol (SCTP) events are logged.
- **gtp**—GPRS Tunneling Protocol (GTP) events are logged.
- **ipsec**—IPsec events are logged.
- **idp**—Intrusion Detection and Prevention (IDP) events are logged.
- **rtlog**—RTLOG system log events are logged.

- **pst-ds-lite**—PST dual-stack lite (DS-Lite) events are logged.
- **appqos**—Application quality of service (AppQoS) events are logged.
- **secintel**—Juniper Networks Security Intelligence (SecIntel) events are logged.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

*Application Security User Guide for Security Devices*

*Logical Systems and Tenant Systems User Guide for Security Devices*

# category (Security Web Filtering)

### Syntax

```
category name{
    action (block | log-and-permit | permit | quarantine);
    custom-message message-name;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated profile profile-name]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name]
```

### Release Information

Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering. Support for new categories and category name updates by Websense added in Junos OS Release 12.1X47-D15 and 12.3X48-D10. Starting with Junos OS Release 15.1X49-D10, the SurfControl integrated feature is no longer supported. For previous releases, statement introduced in Junos OS Release 9.5. The **custom-message** option introduced in Junos OS Release 15.1X49-D110.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Select a custom URL category list you created (custom objects) for filtering against. The **custom-message** configuration option is used to notify the users when the URL is blocked or quarantined for each EWF category. You can customize the message with options such as user message or redirect URL. User messages indicate that website access has been blocked by an organization's access policy. Redirect URLs redirect a blocked or quarantined URL to any user-defined URL. Table 9 on page 389 shows the list of categories predefined by Websense.

Starting with Junos OS Release 17.4R1, you can download and dynamically load new Enhanced Web Filtering (EWF) categories. The downloading and dynamic loading of the new EWF categories do not require a software upgrade. Websense occasionally releases new EWF categories. EWF classifies websites into categories according to host, URL, or IP address and performs filtering based on the categories.

> **NOTE:** Existing configurations are not affected by the new categories but can be modified to make use of the new categories.

**Table 9: List of Categories Predefined by Websense**

| Category ID | Category Name | Parent ID |
|---|---|---|
| 1 | Adult Material | 0 |
| 2 | Business and Economy | 0 |
| 3 | Education | 0 |
| 4 | Government | 0 |
| 5 | News and Media | 0 |
| 6 | Religion | 0 |
| 7 | Society and Lifestyles | 0 |
| 8 | Special Events | 0 |
| 9 | Information Technology | 0 |
| 10 | Abortion | 0 |
| 11 | Advocacy Groups | 0 |
| 12 | Entertainment | 0 |
| 13 | Gambling | 0 |
| 14 | Games | 0 |
| 15 | Illegal or Questionable | 0 |
| 16 | Job Search | 0 |
| 17 | Shopping | 0 |
| 18 | Sports | 0 |
| 19 | Tasteless | 0 |
| 20 | Travel | 0 |
| 21 | Vehicles | 0 |

**Table 9: List of Categories Predefined by Websense *(continued)***

| Category ID | Category Name | Parent ID |
|---|---|---|
| 22 | Violence | 0 |
| 23 | Weapons | 0 |
| 24 | Drugs | 0 |
| 25 | Militancy and Extremist | 0 |
| 26 | Intolerance | 0 |
| 27 | Health | 0 |
| 28 | Website Translation | 9 |
| 29 | Advertisements | 110 |
| 64 | User-Defined | 0 |
| 65 | Nudity | 1 |
| 66 | Adult Content | 1 |
| 67 | Sex | 1 |
| 68 | Financial Data and Services | 2 |
| 69 | Cultural Institutions | 3 |
| 70 | Media File Download | 12 |
| 72 | Military | 4 |
| 73 | Political Organizations | 4 |
| 74 | General Email | 91 |
| 75 | Proxy Avoidance | 9 |
| 76 | Search Engines and Portals | 9 |
| 78 | Web Hosting | 9 |

**Table 9: List of Categories Predefined by Websense *(continued)***

| Category ID | Category Name | Parent ID |
|---|---|---|
| 79 | Web Chat | 91 |
| 80 | Hacking | 9 |
| 81 | Alternative Journals | 5 |
| 82 | Non-Traditional Religions | 6 |
| 83 | Traditional Religions | 6 |
| 84 | Restaurants and Dining | 7 |
| 85 | Gay or Lesbian or Bisexual Interest | 7 |
| 86 | Personals and Dating | 7 |
| 87 | Alcohol and Tobacco | 7 |
| 88 | Prescribed Medications | 24 |
| 89 | Nutrition | 24 |
| 90 | Abused Drugs | 24 |
| 91 | Internet Communication | 0 |
| 92 | Pro-Choice | 10 |
| 93 | Pro-Life | 10 |
| 94 | Sex Education | 1 |
| 95 | Lingerie and Swimsuit | 1 |
| 96 | Online Brokerage and Trading | 110 |
| 97 | Educational Institutions | 3 |
| 98 | Instant Messaging | 110 |
| 99 | Application and Software Download | 110 |

**Table 9: List of Categories Predefined by Websense *(continued)***

| Category ID | Category Name | Parent ID |
|---|---|---|
| 100 | Pay-to-Surf | 110 |
| 101 | Internet Auctions | 17 |
| 102 | Real Estate | 17 |
| 103 | Hobbies | 7 |
| 107 | Sport Hunting and Gun Clubs | 18 |
| 108 | Internet Telephony | 116 |
| 109 | Streaming Media | 116 |
| 110 | Productivity | 0 |
| 111 | Marijuana | 24 |
| 112 | Message Boards and Forums | 110 |
| 113 | Personal Network Storage and Backup | 116 |
| 114 | Internet Radio and TV | 116 |
| 115 | Peer-to-Peer File Sharing | 116 |
| 116 | Bandwidth | 0 |
| 117 | Social Networking and Personal Sites | 7 |
| 118 | Educational Materials | 3 |
| 121 | Reference Materials | 3 |
| 122 | Social Organizations | 0 |
| 123 | Service and Philanthropic Organizations | 122 |
| 124 | Social and Affiliation Organizations | 122 |
| 125 | Professional and Worker Organizations | 122 |

**Table 9: List of Categories Predefined by Websense *(continued)***

| Category ID | Category Name | Parent ID |
|---|---|---|
| 126 | Security | 0 |
| 128 | Malicious Web Sites | 126 |
| 138 | Computer Security | 9 |
| 146 | Miscellaneous | 0 |
| 147 | Web Infrastructure | 146 |
| 148 | Web Images | 146 |
| 149 | Private IP Addresses | 146 |
| 150 | Content Delivery Networks | 146 |
| 151 | Dynamic Content | 146 |
| 152 | Network Errors | 146 |
| 153 | Uncategorized | 146 |
| 154 | Spyware | 126 |
| 156 | File Download Servers | 146 |
| 164 | Phishing and Other Frauds | 126 |
| 166 | Keyloggers | 126 |
| 167 | Potentially Unwanted Software | 126 |
| 172 | Bot Networks | 126 |
| 191 | Extended Protection | 0 |
| 192 | Elevated Exposure | 191 |
| 193 | Emerging Exploits | 191 |
| 194 | Suspicious Content | 191 |

**Table 9: List of Categories Predefined by Websense *(continued)***

| Category ID | Category Name | Parent ID |
|---|---|---|
| 195 | Organizational Email | 91 |
| 196 | Text and Media Messaging | 91 |
| 200 | Web and Email Spam | 9 |
| 220 | Compromised Websites | 0 |
| 221 | Newly Registered Websites | 0 |
| 222 | Collaboration Office | 0 |
| 223 | Office Mail | 222 |
| 224 | Office Drive | 222 |
| 225 | Office Documents | 222 |
| 226 | Office Apps | 222 |
| 227 | Web Analytics | 9 |
| 228 | Web and Email Marketing | 9 |
| 1529 | Classifieds Posting | 0 |
| 1530 | Blog Posting | 0 |
| 1531 | Blog Commenting | 0 |

**Options**

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Understanding Redirect Web Filtering | 208

# content-filtering (Security Feature Profile)

**Syntax**

```
content-filtering {
    block-command;
    block-content-type {
        activex;
        exe;
        http-cookie;
        java-applet;
        zip;
    }
    block-extension;
    block-mime {
        exception;
        list;
    }
    notification-options {
        custom-message;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
    }
    permit-command;
    traceoptions {
        flag name;
    }
    type (content-filtering-none | local);
}
```

**Hierarchy Level**

```
[edit security utm feature-profile]
[edit security utm default-configuration]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure UTM content-filtering features. You can also configure the default UTM configuration for content filtering feature profile. If you do not configure any option in the content filtering feature profile, the values configured in the default UTM configuration are applied. The content filtering feature controls

file transfers across the gateway by checking traffic against configured filter lists. It evaluates the traffic before all other UTM features, except Web filtering.

> **NOTE:** A license check for the content filtering configuration is performed at the time of a commit and will provide a warning if a valid license is not installed on the device. Once a valid license is installed on the device then a custom content filtering profile or the default profile will be able to process traffic. If a license is expired or is not installed, the content filtering service will not process traffic.

**Options**

**block-command**—Protocol block command custom-objects to the content-filtering profile.

**block-content-type**—Blocks to other available content such as exe, http-cookie, java-applet. This is for HTTP only.

**block-extension**—Block extensions to the content-filtering profile.

**block-mime**—MIME pattern list custom-objects to the content-filtering profile for blocking MIME types.

**notification-options**—A message notification to trigger when a content filter is matched.

**permit-command**—Protocol permit command custom-objects to the content-filtering profile.

**traceoptions**—Defines tracing operations for default UTM configuration for content filtering feature.

**type**—Type of content filtering solution or URL filtering solution used by the device.

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# content-filtering (Security UTM Policy)

**Syntax**

```
content-filtering {
    ftp {
        download-profile profile-name;
        upload-profile profile-name;
    }
    http-profile profile-name;
    imap-profile profile-name;
    pop3-profile profile-name;
    smtp-profile profile-name;
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name]
[edit logical-systems logical-systems-name security utm utm-policy policy-name]
[edit tenants tenant-name security utm utm-policy policy-name]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for configuration in logical systems introduced in Junos OS Release 18.3R1.
Support for configuration in tenant systems introduced in Junos OS Release 19.2R1.

**Description**

Configures a UTM policy for the content filtering protocols and attach this policy to a security profile to implement it. Each supported protocol may implement available content filters differently. Not all filtering capabilities are supported for each protocol. The HTTP protocol supports all content filtering features. The FTP protocol supports only lock Extension List and Protocol Command Block List. The e-mail protocols (SMTP, IMAP, POP3) supports limited to Block Extension List, Protocol Command Block List, and MIME Pattern Filtering.

**Options**

The statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Content Filtering Overview | 131

# content-size

**Syntax**

```
content-size (block | log-and-permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name fallback-options]
```

**Release Information**

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

If the content size exceeds a set limit, the content is either passed or blocked. The default action is log-and-permit.

> **NOTE:** When you configure the content-size value, keep in mind that in certain cases, content size is available in the protocol headers, so the max-content-size fallback is applied before a scan request is sent. However, in many cases, content size is not provided in the protocol headers. In these cases, the TCP payload is sent to the antivirus scanner and accumulates until the end of the payload. If the accumulated payload exceeds the maximum content size value, then max-content-size fallback is applied. The default fallback action is log and permit, so you may want to change this option to block, in which case such a packet is dropped and a block message is sent to the client.

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

# content-size (Security Antivirus Sophos Engine)

**Syntax**

```
content-size (block | log-and-permit | permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name fallback-options]
```

**Release Information**

Statement introduced in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

If the content size exceeds a set limit, the content is either passed or blocked.

> **NOTE:** When you configure the content-size value, keep in mind that in certain cases, content size is available in the protocol headers, so the max-content-size fallback is applied before a scan request is sent. However, in many cases, content size is not provided in the protocol headers. In these cases, the TCP payload is sent to the antivirus scanner and accumulates until the end of the payload. If the accumulated payload exceeds the maximum content size value, then max-content-size fallback is applied. You might want to set the fallback action to block, in which case such a packet is dropped and a block message is sent to the client.

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic
- **permit**—Permit the traffic

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# content-size-limit

**Syntax**

```
content-size-limit value;
```

**Hierarchy Level**

```
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name scan-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name scan-options]
[edit security utm default-configuration anti-virus scan-options]
```

**Release Information**

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1. Support for Avira engine added in Junos OS Release 18.4R1.

**Description**

The content size check occurs before the scan request is sent. The content size refers to accumulated TCP payload size. The maximum configurable content size varies with different platforms. For example, the content size ranges from 20 through 40,000 for SRX4100.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# corrupt-file

### Syntax

```
corrupt-file (block | log-and-permit);
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name fallback-options]
```

### Release Information

The Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Corrupt file is the error returned by the scan engine when engine detects a corrupted file. The default action is log-and-permit.

### Options

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Full Antivirus Configuration Overview | 263

# custom-block-message

**Syntax**

```
custom-block-message value;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated profile profile-name]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name]
```

**Release Information**

The Surf-Control feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Enter a custom message to be sent when HTTP requests are blocked.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# custom-message (Security Content Filtering)

**Syntax**

```
custom-message message;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name notification-options]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Custom message notifications are generally used when content is blocked by the content filter.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Content Filtering Overview | 131

# custom-message (Security Email Notify)

**Syntax**

```
custom-message message;
```

**Hierarchy Level**

```
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update email-notify]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update email-notify]
[edit security utm feature-profile anti-virus sophos-engine pattern-update email-notify]
[edit security utm default-configuration anti-virus avira-engine pattern-update email-notify]
```

**Release Information**

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1. Support for Avira engine added in Junos OS Release 18.4R1.

**Description**

You can configure the device to notify a specified administrator when patterns are updated. This is an e-mail notification with a custom message.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# custom-message (Security Fallback Block)

**Syntax**

```
custom-message message;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options
    fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options
    fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options fallback-block]
```

**Release Information**

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# custom-message (Security Fallback Non-Block)

### Syntax

```
custom-message message;
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options
    fallback-non-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options
    fallback-non-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options fallback-non-block]
```

### Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# custom-message (Security Virus Detection)

**Syntax**

```
custom-message message;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options
    virus-detection]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options
    virus-detection]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options virus-detection]
```

**Release Information**

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# custom-message-subject (Security Email Notify)

**Syntax**

```
custom-message-subject message-subject;
```

**Hierarchy Level**

```
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update email-notify]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update email-notify]
[edit security utm feature-profile anti-virus sophos-engine pattern-update email-notify]
[[edit security utm default-configuration avira-engine pattern-update email-notify]
```

**Release Information**

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1. Support for Avira engine added in Junos OS Release 18.4R1.

**Description**

You can configure the device to notify a specified administrator when patterns are updated. This is an e-mail notification with a custom message and a custom subject line.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# custom-message-subject (Security Fallback Block)

**Syntax**

```
custom-message-subject message-subject;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options
    fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options
    fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options fallback-block]
```

**Release Information**

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file. As part of a custom message, you can customize the message subject line.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# custom-message-subject (Security Fallback Non-Block)

**Syntax**

```
custom-message-subject message-subject;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options
    fallback-non-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options
    fallback-non-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options fallback-non-block]
```

**Release Information**

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file. As part of a custom message, you can customize the message subject line.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# custom-message-subject (Security Virus Detection)

**Syntax**

```
custom-message-subject message-subject;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options
    virus-detection]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options
    virus-detection]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options virus-detection]
```

**Release Information**

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file. As part of a custom message, you can customize the message subject line.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# custom-objects

### Syntax

```
custom-objects {
    custom-url-category object-name {
        value [value];
    }
    custom-message {
        name message-name;
        type redirect-url | user-message;
        content redirect-url by user| user-message by user;
    }
    filename-extension object-name {
        value [value];
    }
    mime-pattern object-name {
        value [value];
    }
    protocol-command object-name {
        value [value];
    }
    url-pattern object-name {
        value [value];
    }
}
```

### Hierarchy Level

```
[edit security utm]
[edit security utm default-configuration]
[edit logical-systems logical-system-name security utm]
[edit tenants tenant-name security utm]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level introduced in Junos OS Release 18.2R1.
Support for configuration in logical systems introduced in Junos OS Release 18.3R1.
Support for configuration in tenant systems introduced in Junos OS Release 19.2R1.

### Description

Configure custom objects before configuring UTM feature-profile features.

**WARNING:** Custom category does not take precedence over predefined categories when it has the same name as one of the predefined categories. We do not recommend having a custom category name be the same as the predefined category name.

**NOTE:** Starting from Junos OS Release 17.4R1, support for custom category configuration is available for EWF, local, and Websense redirect profiles.

**Options**

The statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Unified Threat Management Overview | 28

# custom-tag-string

**Syntax**

```
custom-tag-string [string];
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-spam sbl profile profile-name]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure a custom string for identifying a message as spam.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# custom-url-category

### Syntax

```
custom-url-category object-name {
    value [value];
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm custom-objects]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Use URL pattern lists to create Custom URL category lists. These are lists of patterns that bypass scanning.

**WARNING:** Custom category does not take precedence over predefined categories when it has the same name as one of the predefined categories. We do not recommend having a custom category name be the same as the predefined category name.

### Options

- ***object-name***—Name of the URL category-list object.
- **value *value***—Value of the URL category-list object. You can configure multiple values separated by spaces and enclosed in square brackets.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

UTM Overview | 28

# decompress-layer

**Syntax**

```
decompress-layer (block | log-and-permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name fallback-options]
```

**Description**

The Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, decompress layer error is the error returned by the scan engine when the scanned file has too many compression layers. The default action is block.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Full Antivirus Configuration Overview | 263

# decompress-layer-limit

**Syntax**

```
decompress-layer-limit decompress-layer-limit;
```

**Hierarchy Level**

```
[edit security utm default-configuration anti-virus scan-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name scan-options]
[edit anti-virus scan-options]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.
The Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards.
Support at the **[edit security utm default-configuration]** hierarchy level introduced in Junos OS Release 18.2R1.
Support for Avira Antivirus scan engine added in Junos OS Release 18.4R1.

**Description**

When an antivirus scan engine scans a file for viruses, the scan engine decompresses the layers of nested compressed files and files with embedded extractable objects. Embedded extractable objects include files such as archive files (tar), MS Word, and PowerPoint files. For example, if a message contains a compressed .zip file that contains another compressed .zip file, then there are two compression layers. Decompressing both files requires a decompress layer setting of 2. You can set the decompression layer limit for the scan engine.

During the transfer of data, some protocols use content encoding. Before an antivirus scan engine scans viruses, the scan engine decodes this layer, which is considered as a decompression level.

The decompression layer limit is applicable to the following compressed files:

- zip, rar, and gzip
- Encoded data such as Multipurpose Internet Mail Extension (MIME)
- Packaged data such as OLE, CAP, MSI, TAR, EML
- Files with internal extractable objects, such as archive files (tar), MS Word, and PowerPoint files.

If a file exceeds the compression layer limit, the scan engine drops or forwards the file based on the fallback options.

The scan engine scans each layer before unpacking the next layer. The scan engine continues to scan until any of the following conditions are met, whichever happens first:

- Reaches the decompression limit
- Exceeds the system resource allocated for decompression
- Finds a virus or other malware
- Decompresses the data completely.

When the virus signature database becomes larger and the scan algorithms are more sophisticated, the scan engine can look deeper into the data for embedded malware. As a result, the scan engine uncovers more layers of compressed data.

The Juniper Networks device's level of security is limited by the decompress layer limit. You define the decompress layer limit based on the memory allocated to the security service.

**Options**

***decompress-layer-limit***—Specify the number of decompression layer limit.

**Default:** 3

**Range:** 0 through 10

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

On-Device Avira Antivirus | 54

Full Antivirus Configuration Overview | 263

# default (Security Antivirus)

**Syntax**

```
default (block | log-and-permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name fallback-options]
```

**Release Information**

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

All errors other than those specifically listed fall into this category. This could include either unhandled system exceptions (internal errors) or other unknown errors.

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# default (Security Antivirus Sophos Engine)

**Syntax**

```
default (block | log-and-permit | permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name fallback-options]
```

**Release Information**

Statement introduced in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

All errors other than those specifically listed fall into this category. This could include either unhandled system exceptions (internal errors) or other unknown errors.

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic
- **permit**—Permit the traffic

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# default (Security UTM)

**Syntax**

```
default (block |log-and-permit | permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name]
```

**Release Information**

Statement introduced in Junos OS Release 11.4.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Specify the default action to take for a URL.

**Options**

- block—Log the error and deny the traffic.
- log-and-permit—Log the error and permit the traffic.
- permit—Permit the traffic.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# default (Security Web Filtering)

**Syntax**

```
default (block | log-and-permit | permit | quarantine);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated profile profile-name fallback-settings]
[edit security utm feature-profile web-filtering websense-redirect profile profile-name fallback-settings]
[edit security utm feature-profile web-filtering juniper–local profile profile-name fallback-settings]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name fallback-settings]
```

**Release Information**

The Surf-Control feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Specify an action for the profile, for requests that experience internal errors in the Web-filtering module.

**Options**

- block—Log the error and deny the traffic.
- log-and-permit—Log the error and permit the traffic.
- permit —Permit the traffic.
- quarantine—Show the warning message and permit/block the traffic based on user input.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# display-host (Security Fallback Block)

**Syntax**

```
display-host;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options
    fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options
    fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options fallback-block]
```

**Release Information**

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Display the computer host name in the notification e-mail sent to the administrator when a fallback-block notification occurs.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# display-host (Security Virus Detection)

**Syntax**

```
display-host;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus profile profile name notification-options virus-detection]
```

**Release Information**

Statement introduced in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Display the computer host name in the notification e-mail sent to the administrator when a virus is detected by Sophos antivirus.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# download-profile (Security Antivirus FTP)

**Syntax**

```
download-profile profile-name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name anti-virus ftp]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure a UTM policy for the antivirus FTP (download) protocol and attach this policy to a security profile to implement it.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# download-profile (Security Content Filtering FTP)

**Syntax**

```
download-profile profile-name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name content-filtering ftp]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure a UTM policy for the content-filtering FTP (download) protocol and attach this policy to a security profile to implement it.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Content Filtering Overview | 131

# email-notify

### Syntax

```
email-notify {
    admin-email email-address;
    custom-message message;
    custom-message-subject message-subject;
}
```

### Hierarchy Level

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update]
[edit security utm feature-profile anti-virus sophos-engine pattern-update]
[edit security utm default-configuration anti-virus avira-engine pattern-update]
```

### Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for Avira engine added in Junos OS Release 18.4R1.

### Description

You can configure the device to notify a specified administrator when patterns are updated. This is an e-mail notification with a custom message and a custom subject line.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# engine-not-ready

**Syntax**

```
engine-not-ready (block | log-and-permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name fallback-options]
```

**Release Information**

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

The scan engine is initializing itself, for example, loading the signature database. During this phase, it is not ready to scan a file. A file could either pass or be blocked according to this setting. The default action is block.

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# engine-not-ready (Security Antivirus Sophos Engine)

**Syntax**

```
default (block | log-and-permit | permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name fallback-options]
```

**Release Information**

Statement introduced in Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

The scan engine is initializing itself, for example, loading the signature database. During this phase, it is not ready to scan a file. A file could either pass or be blocked according to this setting.

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic
- **permit**—Permit the traffic

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Sophos Antivirus Configuration Overview | 73

# exception

**Syntax**

```
exception listname;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus mime-whitelist]
[edit security utm feature-profile anti-virus mime-whitelist list listname]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure the antivirus scanner to use an exception list to the MIME bypass list (custom objects). To use the exception list, you first create a allowlist custom-object list with the **list** statement. The system will first look at any existing allowlist mime pattern. If it matches an item, it will then continue to look for any exceptions to the allowlist and will then scan any item in the exception list.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# exception (Security Content Filtering)

**Syntax**

```
exception list-name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name block-mime]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure the content filter to use an exception list to the MIME block list (custom objects).

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Content Filtering Overview | 131

# fallback-block (Security Antivirus)

### Syntax

```
fallback-block {
    administrator-email email-address;
    allow-email;
    custom-message message;
    custom-message-subject message-subject;
    display-host;
    (notify-mail-sender | no-notify-mail-sender);
    type (message | protocol-only);
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options]
```

### Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Configure notifications for fallback blocking actions. Fallback options tell the system how to handle the errors returned by either the scan engine or the scan manager.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# fallback-non-block (Security Antivirus)

### Syntax

```
fallback-non-block {
    custom-message message;
    custom-message-subject message-subject;
    (notify-mail-recipient | no-notify-mail-recipient);
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options]
```

### Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Configure notifications for fallback nonblocking actions.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# fallback-options (Security Antivirus Juniper Express Engine)

### Syntax

```
fallback-options {
    content-size (block | log-and-permit);
    default (block | log-and-permit);
    engine-not-ready (block | log-and-permit);
    out-of-resources (block | (log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name]
```

### Release Information

The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Fallback options tell the system how to handle the errors.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Express Antivirus Configuration Overview | 236

# fallback-options (Security Antivirus Kaspersky Lab Engine)

**Syntax**

```
fallback-options {
    content-size (block | log-and-permit);
    corrupt-file (block | log-and-permit);
    decompress-layer (block | log-and-permit);
    default (block | log-and-permit);
    engine-not-ready (block | log-and-permit);
    out-of-resources (block | (log-and-permit);
    password-file (block | (log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name]
```

**Release Information**

The Kaspersky feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 .

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Fallback options tell the system how to handle the errors returned by either the scan engine or the scan manager.

**Options**

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Full Antivirus Configuration Overview | 263

# fallback-options (Security Antivirus Sophos Engine)

### Syntax

```
fallback-options {
    content-size (block | log-and-permit | permit);
    default (block | log-and-permit | permit);
    engine-not-ready (block | log-and-permit | permit);
    out-of-resources (block | log-and-permit | permit);
    timeout (block | log-and-permit | permit);
    too-many-requests (block | log-and-permit | permit);
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name]
```

### Release Information

Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Configure fallback options to instruct the system how to handle errors.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Sophos Antivirus Configuration Overview | 73

# fallback-settings (Security Web Filtering)

**Syntax**

```
fallback-settings {
    default (block | log-and-permit);
    server-connectivity (block | log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated profile profile-name]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name]
```

**Release Information**

The Surf-Control feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, Statement introduced in Junos OS Release 9.5 .
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Fallback settings tell the system how to handle errors.

**Options**

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# fallback-settings (Security Web Filtering Juniper Local)

**Syntax**

```
fallback-settings {
    default (block | log-and-permit);
    server-connectivity (block | log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering juniper–local profile profile-name]
```

**Release Information**

Statement introduced in Junos OS Release 10.0.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Fallback settings tell the system how to handle errors.

**Options**

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Web Filtering Overview | 147

# fallback-settings (Security Web Filtering Websense Redirect)

**Syntax**

```
fallback-settings {
    default (block | log-and-permit);
    server-connectivity (block | log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering websense-redirect profile profile-name]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Fallback settings tell the system how to handle errors.

**Options**

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Understanding Redirect Web Filtering | 208

# feature-profile

**Syntax**

```
feature-profile {
    anti-spam {
        address-blacklist list-name;
        address-whitelist list-name;
        sbl {
            profile profile-name {
                custom-tag-string [string];
                (sbl-default-server | no-sbl-default-server);
                spam-action (block | tag-header | tag-subject);
            }
        }
        traceoptions flag flag;
    }
    anti-virus {
        juniper-express-engine {
            pattern-update {
                email-notify {
                    admin-email email-address;
                    custom-message message;
                    custom-message-subject message-subject;
                }
                interval value;
                no-autoupdate;
                proxy {
                    password password-string;
                    port port-number;
                    server address-or-url;
                    username name;
                }
                url url;
            }
            profile profile-name {
                fallback-options {
                    content-size (block | log-and-permit);
                    default (block | log-and-permit);
                    engine-not-ready (block | log-and-permit);
                    out-of-resources (block | (log-and-permit);
                    timeout (block | log-and-permit);
                    too-many-requests (block | log-and-permit);
                }
```

```
        notification-options {
            fallback-block {
                administrator-email email-address;
                allow-email;
                custom-message message;
                custom-message-subject message-subject;
                display-host;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
            fallback-non-block {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-recipient | no-notify-mail-recipient);
            }
            virus-detection {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
        }
        scan-options {
            content-size-limit value;
            (intelligent-prescreening | no-intelligent-prescreening);
            timeout value;
        }
        trickling {
            timeout value;
        }
    }
}
```

```
kaspersky-lab-engine {
    pattern-update {
        email-notify {
            admin-email email-address;
            custom-message message;
            custom-message-subject message-subject;
        }
        interval value;
        no-autoupdate;
        proxy {
            password password-string;
            port port-number;
            server address-or-url;
            username name;
        }
        url url;
    }
    profile profile-name {
        fallback-options {
            content-size (block | log-and-permit);
            corrupt-file (block | log-and-permit);
            decompress-layer (block | log-and-permit);
            default (block | log-and-permit);
            engine-not-ready (block | log-and-permit);
            out-of-resources (block | (log-and-permit);
            password-file (block | (log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        notification-options {
            fallback-block {
                administrator-email email-address;
                allow-email;
                custom-message message;
                custom-message-subject message-subject;
                display-host;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
            fallback-non-block {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-recipient | no-notify-mail-recipient);
            }
```

```
            virus-detection {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
        }
        scan-options {
            content-size-limit value;
            decompress-layer-limit value;
            (intelligent-prescreening | no-intelligent-prescreening);
            scan-extension filename;
            scan-mode (all | by-extension);
            timeout value;
        }
        trickling {
            timeout value;
        }
    }
}
mime-whitelist {
    exception listname;
    list listname {
        exception listname;
    }
}
```

```
sophos-engine {
    pattern-update {
        email-notify {
            admin-email email-address;
            custom-message message;
            custom-message-subject message-subject;
        }
        interval value;
        no-autoupdate;
        proxy {
            password password-string;
            port port-number;
            server address-or-url;
            username name;
        }
        url url;
    }
    profile <name> {
        fallback-options {
            content-size (block | log-and-permit | permit);
            default (block | log-and-permit | permit);
            engine-not-ready (block | log-and-permit | permit);
            out-of-resources (block | log-and-permit | permit);
            timeout (block | log-and-permit | permit);
            too-many-requests (block | log-and-permit | permit);
        }
        notification-options {
            fallback-block {
                administrator-email email-address;
                allow-email;
                custom-message message;
                custom-message-subject message-subject;
                display-host;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
            fallback-non-block {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-recipient | no-notify-mail-recipient);
            }
            virus-detection {
                custom-message message;
                custom-message-subject message-subject;
```

```
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
        }
        scan-options {
            content-size-limit value;
            (no-uri-check | uri-check);
            timeout value;
        }
        trickling {
            timeout value;
        }
    }
    sxl-retry value;
    sxl-timeout seconds;
  }
  traceoptions flag flag;
  type (juniper-express-engine | kaspersky-lab-engine | sophos-engine);
  url-whitelist listname;
}
content-filtering {
  profile profile-name {
    block-command protocol-command-list;
    block-content-type (activex | exe | http-cookie | java-applet | zip);
    block-extension extension-list;
    block-mime {
        exception list-name;
        list list-name;
    }
    notification-options {
        custom-message message;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
    }
    permit-command protocol-command-list;
  }
  traceoptions flag flag;
}
```

```
web-filtering {
    url-whitelist custwhitelist;
    url-blacklist custblacklist;
    http-reassemble;
    type juniper-enhanced;
    juniper-enhanced {
        cache {
            timeout 1800;
            size 500;
        }
        server {
            host rp.cloud.threatseeker.com;
            port 80;
        }
        profile junos-wf-enhanced-default {
            category {
                Enhanced_Hacking {
                    action log-and-permit;
                    }
                    Enhanced_Government {
                    action quarantine;
                }
            }
            site-reputation-action {
                very-safe permit;
                moderately-safe log-and-permit;
                fairly-safe log-and-permit;
                harmful block;
                suspicious block;
            }
            default block;
            custom-block-message "***access denied ***";
            fallback-settings {
                default block;
                server-connectivity block;
                timeout block;
                too-many-requests block;
            }
            timeout 10;
            no-safe-search;
        }
        utm-policy mypolicy {
            web-filtering {
        http-profile my_ewfprofile01;
```

```
    }
    }
}
```

```
web-filtering {
    juniper-enhanced {
        cache {
            size value;
            timeout value;
        }
        profile profile-name {
            category customurl-list name {
                action (block | log-and-permit | permit | quarantine);
            }
            custom-block-message value;
            custom-quarantine-message value;
            default (block | log-and-permit | permit | quarantine);
            fallback-settings {
                default (block | log-and-permit);
                server-connectivity (block | log-and-permit);
                timeout (block | log-and-permit);
                too-many-requests (block | log-and-permit);
            }
            no-safe-search;
            site-reputation-action {
                fairly-safe (block | log-and-permit | permit | quarantine);
                harmful (block | log-and-permit | permit | quarantine);
                moderately-safe (block | log-and-permit | permit | quarantine);
                suspicious (block | log-and-permit | permit | quarantine);
                very-safe (block | log-and-permit | permit | quarantine);
            }
            timeout value;
        }
        server {
            host host-name;
            port number;
        }
    }
    juniper-local {
        profile profile-name {
            custom-block-message value;
            default (block | log-and-permit | permit);
            fallback-settings {
                default (block | log-and-permit);
                server-connectivity (block | log-and-permit);
                timeout (block | log-and-permit);
                too-many-requests (block | log-and-permit);
            }
```

```
        timeout value;
        no-safe-search;
    }
}
surf-control-integrated {
    cache {
        size value;
        timeout value;
    }
    profile profile-name {
        category customurl-list name {
            action (block | log-and-permit | permit);
        }
        custom-block-message value;
        default (block | log-and-permit | permit);
        fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        timeout value;
    }
    server {
        host host-name;
        port number;
    }
}
traceoptions flag flag;
type (juniper-enhanced | juniper-local | surf-control-integrated | websense-redirect);
url-blacklist listname;
url-whitelist listname;
```

```
        websense-redirect {
            profile profile-name {
                account value;
                custom-block-message value;
                fallback-settings {
                    default (block | log-and-permit);
                    server-connectivity (block | log-and-permit);
                    timeout (block | log-and-permit);
                    too-many-requests (block | log-and-permit);
                }
                server {
                    host host-name;
                    port number;
                }
                sockets value;
                timeout value;
                no-safe-search;
            }
        }
    }
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm]
```

**Release Information**

The Kaspersky, Express antivirus and Surf-Control features are not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Starting with Junos OS Release 18.2R1, the following commands under the **[edit security utm feature-profile]** hierarchy level are deprecated:

- **set web-filtering type**
- **set web-filtering url-blacklist**
- **set web-filtering url-whitelist**
- **set web-filtering http-persist**
- **set web-filtering http-reassemble**
- **set web-filtering traceoptions**
- **set web-filtering juniper-enhanced cache**
- **set web-filtering juniper-enhanced reputation**
- **set web-filtering juniper-enhanced query-type**
- **set anti-virus mime-whitelist**
- **set anti-virus url-whitelist**
- **set anti-virus type**
- **set anti-virus traceoptions**
- **set anti-virus sophos-engine**
- **set anti-spam address-blacklist**
- **set anti-spam address-whitelist**
- **set anti-spam traceoptions**
- **set content-filtering traceoptions**

**no-safe-search** option added for Websense redirect and Juniper local in Junos OS Release 20.2R1.

**Description**

Configure UTM features, antivirus, antispam, content-filtering, and web-filtering by creating feature profiles.

**Options**

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

UTM Supported Features | 34

# filename-extension

**Syntax**

```
filename-extension object-name {
    value [value];
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm custom-objects]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

When scanning content, you can use a file extension list to define a set of file extensions that are used in file extension scan mode (scan-by-extension).

**Options**

- ***object-name***—Name of the extension-list object.
- **value *value***—Value of the extension-list object. You can configure multiple values separated by spaces and enclosed in square brackets.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# flag (SMTP)

**Syntax**

```
flag {
    all;
    configuration;
    IPC;
    protocol-exchange;
    send-request;
}
```

**Hierarchy Level**

```
[edit smtp traceoptions]
```

**Release Information**
Statement added in Junos OS Release 10.0.

**Description**
Set flag for the SMTP traceoptions.

**Options**
The following flag options are supported:

- **IPC**—Trace interprocesss communication.
- **all**—Trace everything.
- **configuration**—Trace configuration event.
- **protocol-exchange**—Trace SMTP protocol exchanges.
- **send-request**—Trace send mail request event.

**Required Privilege Level**
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

smtp-profile (Security UTM Policy Antispam) | 571

# format (Security Log Stream)

**Syntax**

```
format (binary | sd-syslog | syslog | welf)
```

**Hierarchy Level**

```
[edit security log stream stream-name]
[edit logical-systems name security log stream stream-name]
[edit tenants tenant-name security log stream stream-name]
```

**Release Information**

Statement introduced in Junos OS Release 10.0 . Updated in Junos OS Release 12.1 .
The [edit **logical-systems** *name* security log stream *stream-name*] hierarchy level introduced in Junos OS Release 18.2R1.
The [edit **tenants** *tenant-name* security log stream *stream-name*] hierarchy level introduced in Junos OS Release 18.3R1.

**Description**

Set the format for remote security message logging to **binary**, **syslog** (system log), **sd-syslog** (structured system log), or **welf**. Note that for the WELF format, the category must be set to **content-security** (see **category (Security Logging)**).

**Options**

- **binary**—Binary encoded text to conserve resources.
- **sd-syslog**—Structured system log file.
- **syslog**—Traditional system log file.
- **welf**—Web Trends Extended Log Format.

**Default:** By default **syslog** (system log) is enabled.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

*Application Security User Guide for Security Devices*

*Logical Systems and Tenant Systems User Guide for Security Devices*

# forwarding-mode (Security UTM Policy)

**Syntax**

```
forwarding-mode {
    hold;
    inline-tap;
}
```

**Hierarchy Level**

```
[edit security utm default-configuration anti-virus]
```

**Release Information**
Statement introduced in Junos OS Release 20.2.

**Description**
The default configuration for anti-virus is to use the continuous delivery function (CDF). It holds the last packet and sends out all other packets. It saves system memory and makes the packet transmission faster. This mode sends the last packet if the result is “permit” and sends RST message to both the client and the server to reset the connection if the result is “drop”. In CDF mode, you may save an incomplete infected file because it only holds the last packet and sends out others. This file could be executable and harmful, for example, an incomplete script file. CDF mode does not support Mail protocols. Change to **hold** mode to hold all the packets until you get the final result. Configure **inline-tap** mode to permit the traffic even if it is infected. This mode is off by default. You can set the **hold** and **inline-tap** mode separately or simultaneously. When you set both modes simultaneously, **inline-tap** over-rules the **hold** mode and permits the traffic.

To delete **hold** mode use **#delete security utm default-configuration anti-virus forwarding-mode hold**, and to delete **inline-tap** mode use **#delete security utm default-configuration anti-virus forwarding-mode inline-tap**.

**Options**
**hold** —Hold mode (hold file until analysis is complete, default is CDF mode).

**inline-tap** —Detect-only mode without blocking (default is off).

The statements are explained separately. See CLI Explorer.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

- Unified Threat Management Overview | 28

# from-zone (Security Policies)

**Syntax**

```
from-zone zone-name to-zone zone-name {
    policy policy-name {
        description description;
        match {
            application {
                [junos-defaults | application];
                any;
                junos-smtps;
                junos-imaps;
                junos-pop3s;
                }
            }
            dynamic-application {
                [dynamic-application-name |dynamic-application-group-name];
                any;
                none;
            }
            destination-address {
                [address];
                any;
                any-ipv4;
                any-ipv6;
            }
            source-address {
                [address];
                any;
                any-ipv4;
                any-ipv6;
            }
            source-identity {
                [role-name];
                any;
                authenticated-user;
                unauthenticated-user;
                unknown-user;
            }
            source-end-user-profile {
                profile-name;
            }
        }
```

```
scheduler-name scheduler-name;
```

```
then {
    count {
        alarm {
            per-minute-threshold number;
            per-second-threshold number;
        }
    }
    deny;
    log {
        session-close;
        session-init;
    }
    permit {
        application-services {
            application-firewall {
                rule-set rule-set-name;
            }
            application-traffic-control {
                rule-set rule-set-name;
            }
            gprs-gtp-profile profile-name;
            gprs-sctp-profile profile-name;
            idp;
            redirect-wx | reverse-redirect-wx;
            ssl-proxy {
                profile-name profile-name;
            }
            uac-policy {
                captive-portal captive-portal;
            }
            utm-policy policy-name;
        }
        destination-address {
            drop-translated;
            drop-untranslated;
        }
        firewall-authentication {
            pass-through {
                access-profile profile-name;
                client-match user-or-group-name;
                ssl-termination-profile profile-name;
                web-redirect;
                web-redirect-to-https;
            }
```

```
            user-firewall {
               access-profile profile-name;
               domain domain-name
               ssl-termination-profile profile-name;
            }
            web-authentication {
               client-match user-or-group-name;
            }
         }
         services-offload;
         tcp-options {
            initial-tcp-mss mss-value;
            reverse-tcp-mss mss-value;
            sequence-check-required;
            sequence-check-required;
            syn-check-required;
         }
         tunnel {
            ipsec-group-vpn group-vpn;
            ipsec-vpn vpn-name;
            pair-policy pair-policy;
         }
      }
      deny | reject;
      deny | reject [profile name];
   }
  }
}
```

**Hierarchy Level**

```
[edit security policies]
```

**Release Information**

Statement introduced in Junos OS Release 8.5. Support for the **services-offload** option added in Junos OS Release 11.4. Support for the **source-identity** option added in Junos OS Release 12.1. Support for the **description** option added in Junos OS Release 12.1. Support for the **ssl-termination-profile** and **web-redirect-to-https** options added in Junos OS Release 12.1X44-D10. Support for the **user-firewall** option added in Junos OS Release 12.1X45-D10. Support for the **initial-tcp-mss** and **reverse-tcp-mss** options added in Junos OS Release 12.3X48-D20. Support for the **dynamic-application** and **deny** options added in Junos OS Release 18.2R1.

**Description**

Specify a source zone and destination zone to be associated with the security policy.

**Options**

- **from-zone *zone-name***—Name of the source zone.
- **to-zone *zone-name***—Name of the destination zone.

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

- *Security Policies Overview*
- *Understanding Security Policy Rules*
- *Understanding Security Policy Elements*
- *Unified Policies Configuration Overview*

# ftp (UTM Policy Anti-Virus)

### Syntax

```
ftp {
    download-profile profile-name;
    upload-profile profile-name;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name anti-virus]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Configure a UTM policy for the antivirus FTP protocol and attach this policy to a security profile to implement it.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

- *Security Policies Overview*
- *Understanding Security Policy Rules*
- *Understanding Security Policy Elements*

# ftp (UTM Policy Content Filtering)

### Syntax

```
ftp {
    download-profile profile-name;
    upload-profile profile-name;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name content-filtering]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Configure a UTM policy for the content-filtering FTP protocol and attach this policy to a security profile to implement it.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

- *Security Policies Overview*
- *Understanding Security Policy Rules*
- *Understanding Security Policy Elements*

# host (Security Web Filtering)

**Syntax**

```
host host-name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated server]
[edit security utm feature-profile web-filtering websense-redirect profile profile-name server]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name server]
```

**Release Information**

The Surf-Control feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Set server host parameters by entering the server name or IP address.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# http-profile (Security Antivirus)

**Syntax**

```
http-profile profile-name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name anti-virus]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure a UTM policy for the antivirus HTTP protocol and attach this policy to a security profile to implement it.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# http-profile (Security Content Filtering)

**Syntax**

```
http-profile profile-name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name content-filtering]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure a UTM policy for the content-filtering HTTP protocol and attach this policy to a security profile to implement it.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Content Filtering Overview | 131

# http-profile (Security Web Filtering)

**Syntax**

```
http-profile profile-name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name web-filtering]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure a UTM policy for the Web-filtering HTTP protocol and attach this policy to a security profile to implement it.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Web Filtering Overview | 147

# imap-profile (Security UTM Policy Antivirus)

**Syntax**

```
imap-profile profile-name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name anti-virus]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure a UTM policy for the antivirus IMAP protocol and attach this policy to a security profile to implement it.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# imap-profile (Security UTM Policy Content Filtering)

**Syntax**

```
imap-profile profile-name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name content-filtering]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure a UTM policy for the content-filtering IMAP protocol and attach this policy to a security profile to implement it.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Content Filtering Overview | 131

# http-persist

**Syntax**

```
http-persist;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering]
```

**Release Information**

Statement introduced in Junos OS Release 12.3X48-D25.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Checks all HTTP requests in a connection. By default, Web filtering first checks the HTTP request method (for example, GET or PUT) in the same session. If there are multiple HTTP request methods in the subsequent HTTP request of the same session, then Web filtering checks are not performed on these methods. If **http-persist** command is enabled for clear text HTTP traffic, then Web filtering checks every HTTP request packet in the same session.

**Required Privilege Level**

view

RELATED DOCUMENTATION

Example: Configuring Enhanced Web Filtering | 161

# http-reassemble

**Syntax**

```
http-reassemble;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering]
```

**Release Information**

Statement introduced in Junos OS Release 12.3X48-D25.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Reassembles HTTP requests segments. When the **http-reassemble** option is enabled the requested fragment is reassembled. By default, Web filtering checks only HTTP requests in the first HTTP request packet. If HTTP request methods and URLs are fragmented in different packets, then these URLs are not checked. If **http-reassemble** option is enabled for clear text HTTP traffic, then Enhanced Web Filtering (EWF) reassembles the fragmented HTTP request to avoid evasion instead of packet-based inspection.

When a new URL is matched against the active Web Filtering profile and the profile dictates that the URL should be dropped, the entire HTTP session will be blocked by the device.

**Required Privilege Level**

view

RELATED DOCUMENTATION

Example: Configuring Enhanced Web Filtering | 161

# intelligent-prescreening

**Syntax**

```
intelligent-prescreening;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name scan-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name scan-options]
```

**Release Information**

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1x49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Enable intelligent prescreening.

Intelligent prescreening tells the antivirus module to begin scanning a file much earlier. In this case, the scan engine uses the first packet or the first several packets to determine if a file could possibly contain malicious code. The scan engine does a quick check on these first packets and if the scan engine finds that it is unlikely that the file is infected, it then determines that it is safe to bypass the normal scanning procedure.

You can disable intelligent prescreening with the **no-intelligent-prescreening** statement.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# interval (Security Antivirus)

### Syntax

```
interval value;
```

### Hierarchy Level

```
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]
[edit security utm feature-profile anti-virus sophos-engine pattern-update]
[edit security utm default-configuration anti-virus avira-engine pattern-update]
```

### Release Information

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 for Juniper Express engine and Kaspersky Lab engine. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1. Support for Avira engine added in Junos OS Release 18.4R1.

### Description

Set the pattern data files auto-update interval. You can choose to leave the default interval value or you can change it by using this command. You can also force a manual update, if necessary.

> **NOTE:** The data files used with Sophos are not typical virus pattern files; they are small files that help guide virus scanning logic. The full virus pattern database is stored on an external Sophos server called the Sophos Extensible List (SXL) server.

### Options

***value***—Pattern data files auto-update interval in minutes.

**Range:** 10 through 10,080 minutes (10 minutes through 7 days)

**Default:** For Juniper Express engine and Kaspersky Lab engine, 60 minutes; for Sophos engine, 1440 minutes (every 24 hours)

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# ipc

**Syntax**

```
ipc {
    traceoptions flag flag;
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure trace options for IPC.

**Options**

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Enable trace for all IPC trace options.
  - **basic**—Trace basic IPC related information.
  - **connection-manager**—Trace IPC connection manager information.
  - **connection-status**—Trace IPC connection status information.
  - **detail**—Trace IPC related detailed information.
  - **pfe**—Trace communication with PFE.
  - **utm-realtime**—Trace IPC realtime-thread information.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# juniper-enhanced

### Syntax

```
juniper-enhanced {
    cache {
        size value;
        timeout value;
    }
    profile profile-name {
        category customurl-list name {
            action (block | log-and-permit | permit | quarantine);
        }
        custom-block-message value;
        custom-quarantine-message value;
        default (block | log-and-permit | permit | quarantine);
        fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        no-safe-search;
        site-reputation-action {
            fairly-safe (block | log-and-permit | permit | quarantine);
            harmful (block | log-and-permit | permit | quarantine);
            moderately-safe (block | log-and-permit | permit | quarantine);
            suspicious (block | log-and-permit | permit | quarantine);
            very-safe (block | log-and-permit | permit | quarantine);
            }
        timeout value;
    }
    server {
        host host-name;
        port number;
        proxy-profile proxy profile name;
    }
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[set security utm feature-profile web-filtering]
```

**Release Information**

Statement introduced in Junos OS Release 11.4.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
The **proxy-profile** option is introduced under the **security utm default-configuration web-filtering juniper-enhanced server** hierarchy level in Junos OS Release 18.3R1.

**Description**

Configure the UTM Enhanced Web Filtering feature.

**Options**

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Web Filtering Overview | 147

# juniper-express-engine

**Syntax**

```
juniper-express-engine {
    pattern-update {
        email-notify {
            admin-email email-address;
            custom-message message;
            custom-message-subject message-subject;
        }
        interval value;
        no-autoupdate;
        proxy {
            password password-string;
            port port-number;
            server address-or-url;
            username name;
        }
        url url;
    }
    profile profile-name {
        fallback-options {
            content-size (block | log-and-permit);
            default (block | log-and-permit);
            engine-not-ready (block | log-and-permit);
            out-of-resources (block | (log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        notification-options {
            fallback-block {
                administrator-email email-address;
                allow-email;
                custom-message message;
                custom-message-subject message-subject;
                display-host;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
            fallback-non-block {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-recipient | no-notify-mail-recipient);
```

```
        }
        virus-detection {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
        }
    }
    scan-options {
        content-size-limit value;
        (intelligent-prescreening | no-intelligent-prescreening);
        timeout value;
    }
    trickling {
        timeout value;
    }
  }
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus]
```

**Release Information**

The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure the UTM express antivirus feature.

**Options**

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Express Antivirus Configuration Overview | 236

# juniper-local

### Syntax

```
juniper-local {
    profile profile-name {
        block-message (Security UTM) value;
        default (Security Web Filtering) (block | log-and-permit | permit);
        fallback-settings (Security Web Filtering) {
            default (Security Web Filtering) (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (Security Web Filtering Fallback Settings) (block | log-and-permit);
            too-many-requests (Security Web Filtering Fallback Settings) (block | log-and-permit);
        }
        timeout value;
        no-safe-search;
    }
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[set security utm feature-profile web-filtering]
```

### Release Information

Statement introduced in Junos OS Release 10.0.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
**no-safe-search** option added in Junos OS Release 20.2R1.

### Description

Configure the UTM Web-filtering local feature.

### Options

**no-safe-search**—Disable the safe search function.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# kaspersky-lab-engine

**Syntax**

```
kaspersky-lab-engine {
    pattern-update {
        email-notify {
            admin-email email-address;
            custom-message message;
            custom-message-subject message-subject;
        }
        interval value;
        no-autoupdate;
        proxy {
            password password-string;
            port port-number;
            server address-or-url;
            username name;
        }
        url url;
    }
    profile profile-name {
        fallback-options {
            content-size (block | log-and-permit);
            corrupt-file (block | log-and-permit);
            decompress-layer (block | log-and-permit);
            default (block | log-and-permit);
            engine-not-ready (block | log-and-permit);
            out-of-resources (block | (log-and-permit);
            password-file (block | (log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        notification-options {
            fallback-block {
                administrator-email email-address;
                allow-email;
                custom-message message;
                custom-message-subject message-subject;
                display-host;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
            fallback-non-block {
```

```
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-recipient | no-notify-mail-recipient);
        }
        virus-detection {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
        }
    }
    scan-options {
        content-size-limit value;
        decompress-layer-limit value;
        (intelligent-prescreening | no-intelligent-prescreening);
        scan-extension filename;
        scan-mode (all | by-extension);
        timeout value;
    }
    trickling {
        timeout value;
    }
  }
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus]
```

### Release Information

The Kaspersky Antivirus feature is not supported from Junos OS Release 15.1x49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Configure the UTM full file-based antivirus feature.

### Options

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# limit (UTM Policy)

**Syntax**

```
limit value;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name traffic-options sessions-per-client]
```

**Release Information**
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**
In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle to limit sessions.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# list

### Syntax

```
list listname {
    exception listname;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus mime-whitelist]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Configure the antivirus scanner to use MIME bypass lists (custom objects). If you want to have exceptions to the allowlist, create a mime-pattern list with the **exception** statement in addition to the **list** statement.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# list (Security Content Filtering Block Mime)

**Syntax**

```
list list-name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name block-mime]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure the content filter to use MIME block lists (custom objects).

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Content Filtering Overview | 131

# log (Security)

**Syntax**

```
log {
    (source-address source-address | source-interface source-interface);
    cache {
        exclude name {
            destination-address destination-address;
            destination-port destination-port;
            event-id event-id;
            failure;
            interface-name interface-name;
            policy-name policy-name;
            process process;
            protocol protocol;
            source-address source-address;
            source-port source-port;
            success;
            username username;
        }
        limit limit;
    }
    disable;
    escape;
    time-format (year | millisecond);
    event-rate logs per second;
    facility-override (authorization | daemon | ftp | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7
        | user);
    file {
        files files;
        name name;
        path path;
        size size;
    }
    format (binary | sd-syslog | syslog);
    max-database-record max-database-record;
    message-rate-limit messages per second;
    mode (event | stream | stream-event);
    rate-cap logs per second;
    report {
        logs-per-table {
            idp idp;
            ipsec-vpn ipsec-vpn;
```

```
        screen screen;
        session-all session-all;
        sky sky;
        utm utm;
    }
    table-lifetime table-lifetime;
    table-mode {
        dense;
    }
}
root-streaming;
stream stream-name {
    category (all | content-security | fw-auth | screen | alg | nat | flow | sctp | gtp | ipsec | idp | rtlog |pst-ds-lite |
        appqos |secintel |aamw);
    filter {
        threat-attack;
        }
    format (binary | sd-syslog | syslog | welf);
    host {
        ip-address;
        port port-number;
        routing-instanceinstance-name;
    }
    rate-limit {
        log-rate;
    }
    severity (alert | critical | debug | emergency | error | info | notice | warning);
    source-address {
        ip-address;
    }
    time-format (year | millisecond);
    transport {
        protocol (tcp | tls | udp);
        tcp-connections tcp-connections;
        tls-profile tls-profile;
    }
}
traceoptions {
    file <filename> <files files> <match match> <size size> <(world-readable | no-world-readable)>;
    flag name;
    no-remote-trace;
}
```

```
    transport {
        protocol (tcp | tls | udp);
        tcp-connections tcp-connections;
        tls-profile tls-profile;
    }
    utc-timestamp;
}
```

**Hierarchy Level**

```
[edit security]
[edit logical-systems name security]
[edit tenants tenant-name security]
```

**Release Information**

Statement introduced in Junos OS Release 9.2.
The [edit **logical-systems** *name* security] and [edit **tenants** *tenant-name* security] hierarchy levels introduced in Junos OS Release 19.1R1.
**escape** option added in Junos OS Release 20.2R1.
**root-streaming** option added in Junos OS Release 20.3R1.

**Description**

Configure security log. Set the mode of logging (event for traditional system logging or stream for streaming security logs through a revenue port to a server). You can also specify all the other parameters for security logging.

**Options**

**cache**—Cache security log events in the audit log buffer.

**disable**—Disable the security logging for the device.

**escape**—Escapes the stream log forwarding to avoid parsing errors. Stream mode supports escape in **sd-syslog** and **binary** format. Event mode supports escape only in **binary** format.

**time-format**—Specify the year, the millisecond, or both in the timestamp.

**event-rate *rate***—Limit the rate at which logs are streamed per second.

**Range:** 0 through 1500

**Default:** 1500

**facility-override**—Alternate facility for logging to remote host.

**file**—Specify the security log file options for logs in binary format.

**Values:**

- ***max-file-number***—Maximum number of binary log files.
  - The range is 2 through 10 and the default value is 10.
- ***file-name***—Name of binary log file.
- ***binary-log-file-path***—Path to binary log files.
- ***maximum-file-size***—Maximum size of binary log file in megabytes.
  - The range is 1 through 10 and the default value is 10.

**format**—Set the security log format for the device.

**max-database-record**—The following are the disk usage range limits for the database:

**Range:**

- SRX1500, SRX4100, and SRX4200: 0 through 15,000,000
- vSRX: 0 through 1,000,000

**Default:**

- SRX1500, SRX4100, and SRX4200: 15,000,000
- vSRX: 1,000,000

Be sure there is enough free space in **/var/log/hostlogs/**, otherwise logs might be dropped when written into the database.

**mode**—Control how security logs are processed and exported.

**rate-cap *rate-cap-value***—Work with event mode only. This option limits the rate at which data plane logs are generated per second.

**Range:** 0 through 5000 logs per second

**Default:** 5000 logs per second

**root-streaming**—Allows the user logical systems to generate the logs using the root logical system's stream configuration.

**source-address *source-address***—Specify a source IP address or IP address used when exporting security logs, which is mandatory to configure *stream host*.

**source-interface *interface-name***—Specify a source interface name, which is mandatory to configure *stream host*.

The **source-address** and **source-interface** are alternate values. Using one of the options is mandatory.

**stream**—Every stream can configure file or host.

**traceoptions**—Specify security log daemon trace options.

**transport**—Set security log transport settings.

**utc-timestamp**—Specify to use UTC time for security log timestamps.

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# mime-pattern

### Syntax

```
mime-pattern object-name {
    value [value];
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm custom-objects]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

The gateway device uses MIME (Multipurpose Internet Mail Extension) types to decide which traffic is allowed to bypass various types of scanning.

### Options

- ***object-name***—Name of the MIME object.
- **value *value***—Value of the MIME object. You can configure multiple values separated by spaces and enclosed in square brackets.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# mime-whitelist

### Syntax

```
mime-whitelist {
    exception listname;
    list listname {
        exception listname;
    }
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus]
```

### Release Information

Statement introduced in Junos OS Release 9.5. Statement updated for Sophos antivirus support in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Configure the antivirus scanner to use MIME bypass lists and exception lists. You can use your own custom object lists, or you can use the default list that ships with the device called junos-default-bypass-mime.

**WARNING:** When you configure the MIME allowlist feature, be aware that, because header information in HTTP traffic can be spoofed, you cannot always trust HTTP headers to be legitimate. When a Web browser is determining the appropriate action for a given file type, it detects the file type without checking the MIME header contents. However, the MIME allowlist feature does refer to the MIME encoding in the HTTP header. For these reasons, it is possible in certain cases for a malicious website to provide an invalid HTTP header. For example, a network administrator might inadvertently add a malicious website to a MIME allowlist, and, because the site is in the allowlist, it will not be blocked by Sophos even though Sophos has identified the site as malicious in its database. Internal hosts would then be able to reach this site and could become infected.

### Options

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# no-autoupdate

**Syntax**

```
no-autoupdate;
```

**Hierarchy Level**

```
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]
[edit security utm feature-profile anti-virus sophos-engine pattern-update]
[edit security utm default-configuration anti-virus avira-engine pattern-update]
```

**Release Information**
The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 for Juniper Express engine and Kaspersky Lab engine. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1. Support for Avira engine added in Junos OS Release 18.4R1.

**Description**
Turn off automatic data file (pattern file) update for the Kaspersky Lab, Juniper Express, or Sophos engines.

> **NOTE:** The data files used with Sophos are not typical virus pattern files; they are small files that help guide virus scanning logic. The full virus pattern database is stored on an external Sophos server called the Sophos Extensible List (SXL) server.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# no-intelligent-prescreening

**Syntax**

```
no-intelligent-prescreening;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name scan-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name scan-options]
```

**Release Information**

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Disables intelligent prescreening.

Intelligent prescreening tells the antivirus module to begin scanning a file much earlier. In this case, the scan engine uses the first packet or the first several packets to determine if a file could possibly contain malicious code. The scan engine does a quick check on these first packets and if the scan engine finds that it is unlikely that the file is infected, it then determines that it is safe to bypass the normal scanning procedure.

You can enable intelligent prescreening with the **intelligent-prescreening** statement.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# no-notify-mail-recipient

**Syntax**

```
no-notify-mail-recipient;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options
    fallback-non-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options
    fallback-non-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options fallback-non-block]
```

**Release Information**

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Do not notify the e-mail recipient about errors returned by the antivirus scan engine when a fallback nonblocking action occurs.

You can specify that the e-mail recipient is to be notified with the **notify-mail-recipient** statement.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# no-notify-mail-sender (Security Content Filtering Notification Options)

**Syntax**

```
no-notify-mail-sender;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name notification-options]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Do not notify the e-mail sender.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Content Filtering Overview | 131

# no-notify-mail-sender (Security Fallback Block)

**Syntax**

```
no-notify-mail-sender;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options
    fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options
    fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options fallback-block]
```

**Release Information**

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Do not notify the e-mail sender about errors returned by the antivirus scan engine when a fallback action occurs.

You can specify that the e-mail sender is to be notified with the **notify-mail-sender** statement.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# no-notify-mail-sender (Security Virus Detection)

**Syntax**

```
no-notify-mail-sender;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options
    virus-detection]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options
    virus-detection]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options virus-detection]
```

**Release Information**

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Do not notify the e-mail sender when a virus is detected by the antivirus engine.

You can specify that the e-mail sender is to be notified with the **notify-mail-sender** statement.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# no-sbl-default-server

**Syntax**

```
no-sbl-default-server;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-spam sbl profile profile-name]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Disable the default SBL server lookup.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Antispam Filtering Overview | 108

# notification-options (Security Antivirus)

### Syntax

```
notification-options {
    fallback-block {
        administrator-email email-address;
        allow-email;
        custom-message message;
        custom-message-subject message-subject;
        display-host;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
    }
    fallback-non-block {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-recipient | no-notify-mail-recipient);
    }
    virus-detection {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
    }
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name]
```

### Release Information

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

There are multiple notification options you can configure to trigger when a virus is detected.

**Options**

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# notification-options (Security Content Filtering)

**Syntax**

```
notification-options {
    custom-message message;
    (notify-mail-sender | no-notify-mail-sender);
    type (message | protocol-only);
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

You can configure a message notification to trigger when a content filter is matched.

**Options**

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Content Filtering Overview | 131

# notify-mail-recipient

**Syntax**

```
notify-mail-recipient;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options
    fallback-non-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options
    fallback-non-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options fallback-non-block]
```

**Release Information**

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Notify the e-mail recipient about errors returned by the antivirus scan engine when a fallback nonblocking action occurs.

You can specify that the e-mail recipient is not to be notified with the **no-notify-mail-recipient** statement.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# notify-mail-sender (Security Content Filtering Notification Options)

**Syntax**

```
notify-mail-sender;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name notification-options]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Notify the e-mail sender.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Content Filtering Overview | 131

# notify-mail-sender (Security Fallback Block)

**Syntax**

```
notify-mail-sender;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options
    fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options
    fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options fallback-block]
```

**Release Information**

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

E-mail notification is used to notify the sender or the recipient about the errors returned by either the scan engine or the scan manager when a fallback action occurs.

You can specify that the sender is not to be notified with the **no-notify-mail-sender** statement.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# notify-mail-sender (Security Virus Detection)

**Syntax**

```
notify-mail-sender;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options
    virus-detection]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options
    virus-detection]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options virus-detection]
```

**Release Information**

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

E-mail notification is used to notify the sender or the recipient about the detected viruses or the scanning errors. When a virus is detected, an e-mail is sent to the sender upon virus detection.

You can specify that the sender is not to be notified with the **no-notify-mail-sender** statement.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# no-uri-check

**Syntax**

```
no-uri-check;
```

**Hierarchy Level**

```
[edit security utm default-configuration anti-virus scan-options]
```

**Release Information**

Statement introduced in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Do not perform Sophos antivirus Uniform Resource Identifier (URI) checking. URI checking is performed by analyzing HTTP traffic URI content against a remote Sophos database server to identify malware or malicious content. URI checking is on by default.

> **NOTE:** Starting in Junos OS release 18.4R1, the URI checking is off by default.

You can enable Sophos antivirus URI checking with the **uri-check** statement.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# out-of-resources

**Syntax**

```
out-of-resources (block | (log-and-permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name fallback-options]
```

**Release Information**

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Virus scanning requires a great deal of memory and CPU resources. Due to resource constraints, memory allocation requests can be denied by the system. When out-of-resources occurs, scanning is aborted. The default action is block.

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# out-of-resources (Security Antivirus Sophos Engine)

**Syntax**

```
default (block | log-and-permit | permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name fallback-options]
```

**Release Information**

Statement introduced in Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Virus scanning requires a great deal of memory and CPU resources. Due to resource constraints, memory allocation requests can be denied by the system. When out-of-resources occurs, scanning is aborted.

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic
- **permit**—Permit the traffic

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Sophos Antivirus Configuration Overview | 73

# over-limit

**Syntax**

```
over-limit (block | log-and-permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name traffic-options sessions-per-client]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle to limit sessions and configure an action to occur when the limit is exceeded.

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

utm | 619

# packet-filter

### Syntax

```
packet-filter packet-filter-name {
    action-profile profile-name {
    destination-port (Security Forwarding Options) (port-range | protocol-name);
    destination-prefix destination-prefix;
    interface logical-interface-name;
    protocol (Security Forwarding Options) (protocol-number | protocol-name;
    source-port (Security Forwarding Options) (port-range | protocol- name);
    source-prefix source-prefix;
    }
```

### Hierarchy Level

```
[edit security datapath-debug]
```

### Release Information

Command introduced in Junos OS Release 9.6 ; Support for IPv6 addresses for the **destination-prefix** and **source-prefix** options added in Junos OS Release 10.4.

### Description

Set packet filter for taking the datapath-debug action. A filter is defined to filter traffic, then an action profile is applied to the filtered traffic. Be sure to configure multiple packet filters to capture the traffic. One packet filter only captures the traffic as specified in it, such as from one source to one destination. The same packet filter will not capture the traffic in the reverse direction. You need to configure another packet filter to capture the traffic in reverse direction and specify the source and destination according to the response packet in it. The action profile specifies a variety of actions on the processing unit. A maximum of four filters are supported at the same time. Packet filters can be configured with source and destination prefix and port (including ranges), and protocol.

Action-profile settings have no specific minimum setting, it is based on trace, count, packet summary and packet-dump. Enabling end-to-end debugging without or with a very broad filter is not recommended. This could result in a high PFE CPU usage. Therefore when selecting what to capture through a filter care must be taken. List as many and specific criteria which then results in the minimum amount of traffic to be captured.

**NOTE:** Packet filter is supported on SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices.

**Options**

- **action-profile *profile-name***—Identify the action profile to use. You can specify the name of the action profile to use. Using the request security action-profile command, you can set the action for the packet match for a specified filter. Action-profile must be defined.
- **destination-port (*port-range* | *protocol name*)**—Specify a destination port to match TCP/UDP destination port.
- **destination-prefix *destination-prefix***—Specify a destination IPv4/IPv6 address prefix.
- **interface *logical-interface-name***—Specify a logical interface name.
- **protocol (*protocol-number* | *protocol-name***—Match IP protocol type.
- **source-port (*port-range* | *protocol-name***—Match TCP/UDP source port.
- **source-prefix *source-prefix***—Specify a source IP address prefix.

**Required Privilege Level**

security—To view this in the configuration
security-control—To add this to the configuration.

# password (Security Antivirus)

**Syntax**

```
password password-string;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update proxy]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update proxy]
[edit security utm feature-profile anti-virus sophos-engine pattern-update proxy]
```

**Release Information**

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Release 11.2.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Set the password for the proxy server.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

utm | 619

# password-file

**Syntax**

```
password-file (block | (log-and-permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name fallback-options]
```

**Release Information**

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Password protected file is the error returned by the scan engine when the scanned file is protected by a password. The default action is log-and-permit.

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Full Antivirus Configuration Overview | 263

# pattern-update (Security Antivirus)

**Syntax**

```
pattern-update {
    email-notify {
        admin-email email-address;
        custom-message message;
        custom-message-subject message-subject;
    }
    interval value;
    no-autoupdate;
    proxy-profile proxy profile name;
    routing-instance name;
    start-time start-time;
    url url;
}
```

**Hierarchy Level**

```
[edit security utm feature-profile anti-virus juniper-express-engine]
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
[edit security utm feature-profile anti-virus sophos-engine]
[edit security utm default-configuration anti-virus avira-engine]
```

**Release Information**

Statement introduced in Junos OS Release 9.5 for Juniper Express engine and Kaspersky Lab engine.
Support for Sophos engine added in Junos OS Release 11.1 .
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
The **proxy-profile** option is introduced under the **security utm feature-profile anti-virus sophos-engine** hierarchy level in Junos OS Release 18.3R1.
Support for Avira engine added in Junos OS Release 18.4R1.

**Description**

Updates to the pattern file are added as new viruses are discovered. You can configure the security device to regularly update the pattern file automatically, or you can update the file manually.

**Required Privilege Level**

security— To view this statement in the configuration.
security-control— To add this statement to the configuration.

# permit-command

**Syntax**

```
permit-command protocol-command-list;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Apply protocol permit command custom-objects to the content-filtering profile.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Content Filtering Overview | 131

# policies

### Syntax

```
policies {
    default-policy (deny-all | permit-all);
    from-zone from-zone-name {
        to-zone;
        policy name {
            description description;
            match (Security Policies Global) {
                source-address (Security Policies);
                destination-address (Security Policies);
                application (Security Policies);
                source-identity;
                source-end-user-profile <source-end-user-profile-name>;
                dynamic-application (Security Policies);
                url-category;
                from-zone (Security Policies Global);
                to-zone (Security Policies Global);
                source-l3vpn-vrf-group [ source-l3vpn-vrf-group ... ];
                destination-l3vpn-vrf-group [ destination-l3vpn-vrf-group ... ];
                destination-address-excluded;
                source-address-excluded;
            }
            scheduler-name scheduler-name;
            then {
                deny;
                permit {
                    application-services {
                        (redirect-wx | reverse-redirect-wx);
                        advanced-anti-malware-policy advanced-anti-malware-policy;
                        application-traffic-control {
                            rule-set rule-set;
                        }
                        gprs-gtp-profile gprs-gtp-profile;
                        gprs-sctp-profile gprs-sctp-profile;
                        icap-redirect icap-redirect;
                        idp;
                        idp-policy idp-policy;
                        security-intelligence-policy security-intelligence-policy;
                        ssl-proxy {
                            profile-name profile-name;
                        }
```

```
    uac-policy {
        captive-portal captive-portal;
    }
    utm-policy utm-policy;
    web-proxy {
        profile-name profile-name;
    }
}
destination-address (Security IDP Policy) {
    (drop-translated | drop-untranslated);
}
firewall-authentication {
    pass-through {
        access-profile access-profile;
        auth-only-browser;
        auth-user-agent name;
        client-match [ client-match ... ];
        ssl-termination-profile ssl-termination-profile;
        web-redirect;
        web-redirect-to-https;
    }
    user-firewall {
        access-profile access-profile;
        auth-only-browser;
        auth-user-agent name;
        domain domain;
        ssl-termination-profile ssl-termination-profile;
        web-redirect;
        web-redirect-to-https;
    }
    web-authentication {
        client-match [ client-match ... ];
    }
    push-to-identity-management;
}
services-offload;
tcp-options {
    initial-tcp-mss initial-tcp-mss;
    reverse-tcp-mss reverse-tcp-mss;
    sequence-check-required;
    syn-check-required;
    window-scale;
}
```

```
            tunnel {
                ipsec-vpn ipsec-vpn;
                pair-policy pair-policy;
            }
        }
        reject {
            profile profile;
            ssl-proxy {
                profile-name profile-name;
            }
        }
        count {
        }
        log {
            session-close;
            session-init;
        }
    }
  }
}
```

```
global {
    policy name {
        description description;
        match (Security Policies Global) {
            source-address (Security Policies);
            destination-address (Security Policies);
            application (Security Policies);
            source-identity;
            source-end-user-profile <source-end-user-profile-name>;
            dynamic-application (Security Policies);
            url-category;
            from-zone (Security Policies Global);
            to-zone (Security Policies Global);
            source-l3vpn-vrf-group [ source-l3vpn-vrf-group ... ];
            destination-l3vpn-vrf-group [ destination-l3vpn-vrf-group ... ];
            destination-address-excluded;
            source-address-excluded;
        }
        scheduler-name scheduler-name;
        then {
            deny;
            permit {
                application-services {
                    (redirect-wx | reverse-redirect-wx);
                    advanced-anti-malware-policy advanced-anti-malware-policy;
                    application-traffic-control {
                        rule-set rule-set;
                    }
                    gprs-gtp-profile gprs-gtp-profile;
                    gprs-sctp-profile gprs-sctp-profile;
                    icap-redirect icap-redirect;
                    idp;
                    idp-policy idp-policy;
                    security-intelligence-policy security-intelligence-policy;
                    ssl-proxy {
                        profile-name profile-name;
                    }
                    uac-policy {
                        captive-portal captive-portal;
                    }
                    utm-policy utm-policy;
                    web-proxy {
                        profile-name profile-name;
                    }
```

```
    }
    destination-address {
        (drop-translated | drop-untranslated);
    }
    firewall-authentication {
        pass-through {
            access-profile access-profile;
            auth-only-browser;
            auth-user-agent name;
            client-match [ client-match ... ];
            ssl-termination-profile ssl-termination-profile;
            web-redirect;
            web-redirect-to-https;
        }
        user-firewall {
            access-profile access-profile;
            auth-only-browser;
            auth-user-agent name;
            domain domain;
            ssl-termination-profile ssl-termination-profile;
            web-redirect;
            web-redirect-to-https;
        }
        web-authentication {
            client-match [ client-match ... ];
        }
        push-to-identity-management;
    }
    services-offload;
    tcp-options {
        initial-tcp-mss initial-tcp-mss;
        reverse-tcp-mss reverse-tcp-mss;
        sequence-check-required;
        syn-check-required;
        window-scale;
    }
    tunnel {
        ipsec-vpn ipsec-vpn;
        pair-policy pair-policy;
    }
}
```

```
            reject {
                profile profile;
                ssl-proxy {
                    profile-name profile-name;
                }
            }
            count {
            }
            log {
                session-close;
                session-init;
            }
        }
    }
}
policy-rematch <extensive>;
policy-stats {
    system-wide (disable | enable);
}
pre-id-default-policy {
    then {
        log {
            session-close;
            session-init;
        }
        session-timeout {
            icmp seconds;
            icmp6 seconds;
            ospf seconds;
            others seconds;
            tcp seconds;
            udp seconds;
        }
    }
}
```

```
stateful-firewall-rule name {
    match-direction (input | input-output | output);
    policy name {
        description description;
        match (Security Policies Global) {
            source-address (Security Policies);
            destination-address (Security Policies);
            application (Security Policies);
            source-identity;
            source-end-user-profile <source-end-user-profile-name>;
            dynamic-application (Security Policies);
            url-category;
            from-zone (Security Policies Global);
            to-zone (Security Policies Global);
            source-l3vpn-vrf-group [ source-l3vpn-vrf-group ... ];
            destination-l3vpn-vrf-group [ destination-l3vpn-vrf-group ... ];
            destination-address-excluded;
            source-address-excluded;
        }
        scheduler-name scheduler-name;
        then {
            deny;
            permit {
                application-services {
                    (redirect-wx | reverse-redirect-wx);
                    advanced-anti-malware-policy advanced-anti-malware-policy;
                    application-traffic-control {
                        rule-set rule-set;
                    }
                    gprs-gtp-profile gprs-gtp-profile;
                    gprs-sctp-profile gprs-sctp-profile;
                    icap-redirect icap-redirect;
                    idp;
                    idp-policy idp-policy;
                    security-intelligence-policy security-intelligence-policy;
                    ssl-proxy {
                        profile-name profile-name;
                    }
                    uac-policy {
                        captive-portal captive-portal;
                    }
                    utm-policy utm-policy;
                    web-proxy {
                        profile-name profile-name;
```

```
        }
    }
    destination-address {
        (drop-translated | drop-untranslated);
    }
    firewall-authentication {
        pass-through {
            access-profile access-profile;
            auth-only-browser;
            auth-user-agent name;
            client-match [ client-match ... ];
            ssl-termination-profile ssl-termination-profile;
            web-redirect;
            web-redirect-to-https;
        }
        user-firewall {
            access-profile access-profile;
            auth-only-browser;
            auth-user-agent name;
            domain domain;
            ssl-termination-profile ssl-termination-profile;
            web-redirect;
            web-redirect-to-https;
        }
        web-authentication {
            client-match [ client-match ... ];
        }
        push-to-identity-management;
    }
    services-offload;
    tcp-options {
        initial-tcp-mss initial-tcp-mss;
        reverse-tcp-mss reverse-tcp-mss;
        sequence-check-required;
        syn-check-required;
        window-scale;
    }
    tunnel {
        ipsec-vpn ipsec-vpn;
        pair-policy pair-policy;
    }
}
```

```
            reject {
                profile profile;
                ssl-proxy {
                    profile-name profile-name;
                }
            }
            count {
            }
            log {
                session-close;
                session-init;
            }
        }
    }
    stateful-firewall-rule-set name {
        stateful-firewall-rule name;
    }
    traceoptions (Security Policies) {
        file <filename> <files files> <match match> <size size> <(world-readable | no-world-readable)>;
        flag name;
        no-remote-trace;
    }
    unified-policy {
        max-lookups max-lookups;
    }
}
```

### Hierarchy Level

```
[edit security]
```

**Release Information**

Statement introduced in Junos OS Release 8.5.
Support for the **services-offload** option added in Junos OS Release 11.4.
Support for the **source-identitiy** option added in Junos OS Release 12.1.
Support for the **description** option added in Junos OS Release 12.1.
Support for the **ssl-termination-profile** and **web-redirect-to-https** options are added starting from Junos OS Release 12.1X44-D10 and Junos OS Release 15.1X49-D40.
Support for the **user-firewall** option added in Junos OS Release 12.1X45-D10.
Support for the **domain** option, and for the **from-zone** and **to-zone** global policy match options, added in Junos OS Release 12.1X47-D10.
Support for the **initial-tcp-mss** and **reverse-tcp-mss** options added in Junos OS Release 12.3X48-D20.
Support for the **extensive** option for **policy-rematch** added in Junos OS Release 15.1X49-D20.
Starting in Junos OS Release 18.2R1, an IDP policy is available within unified security policy. The IDP policy access is simplified and made available under the unified policy as one of the policy. When an IDP policy is available within a unified security policy, configuring source or destination address, source and destination-except, from and to zone, or application is not required, because the match happens in the security policy itself.
Starting in Junos OS Release 18.3R1, when an SRX Series device is configured with a unified policies, you can configure multiple IDP policies and set one of those policies as the default IDP policy. If multiple IDP policies are configured for a session and when policy conflict occurs, the device applies the default IDP policy for that session and thus resolves any policy conflicts.

> **NOTE:** If you have configured two or more IDP policies in a unified security policy, then you must configure the default IDP policy.

**Description**

Configure a network security policies with IPv6 addresses only if flow support for IPv6 traffic is enabled on the device.

**Options**

**default-policy**—Configure a default action when no user-defined policy match.

**Values:**

- deny-all—Deny all traffic if no policy match
- permit-all—Permit all traffic if no policy match

**policy-rematch**—Re-evaluate the policy when changed.

**Values:**

- extensive—Perform policy extensive rematch

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

*Security Policies Overview*

# pop3-profile (Security UTM Policy Antivirus)

**Syntax**

```
pop3-profile profile-name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name anti-virus]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure a UTM policy for the antivirus POP3 protocol and attach this policy to a security profile to implement it.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# pop3-profile (Security UTM Policy Content Filtering)

**Syntax**

```
pop3-profile profile-name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name content-filtering]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure a UTM policy for the content filtering POP3 protocol and attach this policy to a security profile to implement it.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# port (Security Antivirus)

**Syntax**

```
port port-number;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update proxy]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update proxy]
[edit security utm feature-profile anti-virus sophos-engine pattern-update proxy]
```

**Release Information**

Statement introduced in Junos OS Release 11.2.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Set the port number for the proxy server.

**Options**

**Range:** 0 through 65,535

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# port (Security Web Filtering Server)

**Syntax**

```
port number;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated server]
[edit security utm feature-profile web-filtering websense-redirect profile profile-name server]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name server]
```

**Release Information**

Statement introduced in Junos OS Release 9.5 .

Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Enter the port number for communicating with the server. (Default ports are 80, 8080, and 8081.)

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# primary-server

### Syntax

```
primary-server {
    address ipv4-address;
    login sender-email-address {
        password password;
    }
}
```

### Hierarchy Level

```
[edit smtp]
```

### Release Information

Statement added in Junos OS Release 10.0.

### Description

Configure Simple Mail Transfer Protocol (SMTP) primary server for access authorization for SMTP requests.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

# profile (Security Antispam SBL)

### Syntax

```
profile profile-name {
    custom-tag-string [string];
    (sbl-default-server | no-sbl-default-server);
    spam-action (block | tag-header | tag-subject);
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-spam sbl]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Create a profile for the antispam sbl feature. This profile includes all subsequent configuration options.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# profile (Security Antivirus Juniper Express Engine)

**Syntax**

```
profile profile-name {
    fallback-options {
        content-size (block | log-and-permit);
        default (block | log-and-permit);
        engine-not-ready (block | log-and-permit);
        out-of-resources (block | (log-and-permit);
        timeout (block | log-and-permit);
        too-many-requests (block | log-and-permit);
    }
    notification-options {
        fallback-block {
            administrator-email email-address;
            allow-email;
            custom-message message;
            custom-message-subject message-subject;
            display-host;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
        }
        fallback-non-block {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-recipient | no-notify-mail-recipient);
        }
        virus-detection {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
        }
    }
    scan-options {
        content-size-limit value;
        (intelligent-prescreening | no-intelligent-prescreening);
        timeout value;
    }
    trickling {
        timeout value;
    }
}
```

### Hierarchy Level

[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine]

### Release Information

The express engine feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Create a profile for the Juniper express engine. This profile includes all subsequent configuration options.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

Express Antivirus Configuration Overview | 236

# profile (Security Antivirus Kaspersky Lab Engine)

**Syntax**

```
profile profile-name {
    fallback-options {
        content-size (block | log-and-permit);
        corrupt-file (block | log-and-permit);
        decompress-layer (block | log-and-permit);
        default (block | log-and-permit);
        engine-not-ready (block | log-and-permit);
        out-of-resources (block | (log-and-permit);
        password-file (block | (log-and-permit);
        timeout (block | log-and-permit);
        too-many-requests (block | log-and-permit);
    }
    notification-options {
        fallback-block {
            administrator-email email-address;
            allow-email;
            custom-message message;
            custom-message-subject message-subject;
            display-host;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
        }
        fallback-non-block {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-recipient | no-notify-mail-recipient);
        }
        virus-detection {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
        }
    }
    scan-options {
        content-size-limit value;
        decompress-layer-limit value;
        (intelligent-prescreening | no-intelligent-prescreening);
        scan-extension filename;
        scan-mode (all | by-extension);
```

```
        timeout value;
    }
    trickling {
        timeout value;
    }
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
```

**Release Information**

The Kaspersky feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Create a profile for the Kaspersky Lab engine. This profile includes all subsequent configuration options.

**Options**

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

kaspersky-lab-engine | 483

profile (Security Antivirus Juniper Express Engine) | 536

# profile (Security Content Filtering)

### Syntax

```
profile profile-name {
    block-command protocol-command-list;
    block-content-type (activex | exe | http-cookie | java-applet | zip);
    block-extension extension-list;
    block-mime {
        exception list-name;
        list list-name;
    }
    notification-options {
        custom-message message;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
    }
    permit-command protocol-command-list;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Create a profile for the content-filtering feature. This profile includes all subsequent configuration options.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Content Filtering Overview | 131

# profile (Security Sophos Engine Antivirus)

**Syntax**

```
profile <name> {
    fallback-options {
        content-size (block | log-and-permit | permit);
        default (block | log-and-permit | permit);
        engine-not-ready (block | log-and-permit | permit);
        out-of-resources (block | log-and-permit | permit);
        timeout (block | log-and-permit | permit);
        too-many-requests (block | log-and-permit | permit);
    }
    notification-options {
        fallback-block {
            administrator-email email-address;
            allow-email;
            custom-message message;
            custom-message-subject message-subject;
            display-host;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
        }
        fallback-non-block {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-recipient | no-notify-mail-recipient);
        }
        virus-detection {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
        }
    }
    scan-options {
        content-size-limit value;
        (no-uri-check | uri-check);
        timeout value;
    }
    trickling {
        timeout value;
    }
}
```

### Hierarchy Level

[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine]

### Release Information

Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Create a profile for the Sophos antivirus engine. This profile includes all subsequent configuration options.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

Sophos Antivirus Configuration Overview | 73

# profile

### Syntax

```
profile <name> {
    fallback-options {
        content-size (block | log-and-permit | permit);
        default (block | log-and-permit | permit);
        engine-not-ready (block | log-and-permit | permit);
        out-of-resources (block | log-and-permit | permit);
        timeout (block | log-and-permit | permit);
        too-many-requests (block | log-and-permit | permit);
    }
    mime-whitelist {
        exception exception;
        list list;
    }
    notification-options {
        fallback-block {
            administrator-email email-address;
            allow-email;
            custom-message message;
            custom-message-subject message-subject;
            display-host;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
        }
        fallback-non-block {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-recipient | no-notify-mail-recipient);
        }
        virus-detection {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
        }
    }
    url-whitelist url-whitelist;
}
```

### Hierarchy Level

[edit security utm default-configuration]
[edit security utm feature-profile anti-virus profile profile1]

**Release Information**

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Statement introduced in Junos OS Release 18.4R1.

**Description**

Create a profile for the Avira antivirus engine. The antivirus feature profile settings include the scanning options, such as virus detection type, allowlist, blocklist, fallback and notification options.

**Options**

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# profile (Security Web Filtering Juniper Enhanced)

### Syntax

```
profile profile-name {
    category customurl-list name {
        action (block | log-and-permit | permit | quarantine);
    }
    custom-block-message value;
    custom-quarantine-message value;
    default (block | log-and-permit | permit | quarantine);
    fallback-settings {
        default (block | log-and-permit);
        server-connectivity (block | log-and-permit);
        timeout (block | log-and-permit);
        too-many-requests (block | log-and-permit);
    }
    no-safe-search;
    site-reputation-action {
        fairly-safe (block | log-and-permit | permit | quarantine);
        harmful (block | log-and-permit | permit | quarantine);
        moderately-safe (block | log-and-permit | permit | quarantine);
        suspicious (block | log-and-permit | permit | quarantine);
        very-safe (block | log-and-permit | permit | quarantine);
    }
    timeout value;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering juniper-enhanced]
```

### Release Information

Statement introduced in Junos OS Release 11.4.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Create a profile for the juniper-enhanced feature. This profile includes all subsequent configuration options.

### Options

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

Monitoring Web Filtering Configurations | 230

# profile (Security Web Filtering Juniper Local)

### Syntax

```
profile profile-name {
    custom-block-message value;
    default (block | log-and-permit | permit);
    fallback-settings {
        default (block | log-and-permit);
        server-connectivity (block | log-and-permit);
        timeout (block | log-and-permit);
        too-many-requests (block | log-and-permit);
    }
    timeout value;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering juniper-local]
```

### Release Information

Statement introduced in Junos OS Release 10.0.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Create a profile for the web-filtering juniper–local feature. This profile includes all subsequent configuration options.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

Monitoring Web Filtering Configurations | 230
Example: Configuring Local Web Filtering | 195

# profile (Security Web Filtering Surf Control Integrated)

**Syntax**

```
profile profile-name {
    category customurl-list name {
        action (block | log-and-permit | permit);
    }
    custom-block-message value;
    default (block | log-and-permit | permit);
    fallback-settings {
        default (block | log-and-permit);
        server-connectivity (block | log-and-permit);
        timeout (block | log-and-permit);
        too-many-requests (block | log-and-permit);
    }
    timeout value;
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated]
```

**Release Information**

The Surf-Control feature is not supported from Junos OS Release 15.1x49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Create a profile for the web-filtering surf-control-integrated feature. This profile includes all subsequent configuration options.

**Options**

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# profile (Security Web Filtering Websense Redirect)

### Syntax

```
profile profile-name {
    account value;
    custom-block-message value;
    fallback-settings {
        default (block | log-and-permit);
        server-connectivity (block | log-and-permit);
        timeout (block | log-and-permit);
        too-many-requests (block | log-and-permit);
    }
    server {
        host host-name;
        port number;
    }
    sockets value;
    timeout value;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[security utm feature-profile web-filtering websense-redirect]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Create a profile for the web-filtering web-sense feature. This profile includes all subsequent configuration options.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Monitoring Web Filtering Configurations | 230

# protocol-command

**Syntax**

```
protocol-command object-name {
    value [value];
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm custom-objects]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Different protocols use different commands to communicate between servers and clients. By blocking or allowing certain commands, traffic can be controlled on the protocol command level.

**Options**

- ***object-name***—Name of the command-list object.
- **value *value***—Value of the command-list object. You can configure multiple values separated by spaces and enclosed in square brackets.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

UTM Overview | 28

# proxy (Security Antivirus)

### Syntax

```
proxy {
    password password-string;
    port port-number;
    server address-or-url;
    username name;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]
[edit security utm feature-profile anti-virus sophos-engine pattern-update]
```

### Release Information

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 11.2.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Update the pattern file on the proxy server.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# proxy-profile

**Syntax**

proxy-profile *proxy profile name*

**Hierarchy Level**

[set security utm default-configuration web-filtering juniper-enhanced server]
[edit security utm feature-profile anti-virus sophos-engine pattern-update]
[edit security utm default-configuration anti-virus avira-engine pattern-update]

**Release Information**

Statement introduced in Junos OS Release 18.3R1. Support for Avira engine added in Junos OS Release 18.4R1.

**Description**

Specify the proxy profile name and is used for configuring the explicit proxy.

**Required Privilege Level**

services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

# quarantine-message (Security UTM)

**Syntax**

```
quarantine-message {
    type {
        custom-redirect-url;
    }
    url url;
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name]
```

**Release Information**

Statement introduced in Junos OS Release 12.1X44-D10 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure Juniper enhanced quarantine message settings.

**Options**

- **type**—Specify the following type of the quarantine message:
  - **custom-redirect-url**—Specify Custom redirect URL server.
- **url *url***—Specify an URL of the quarantine message.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# routing-instance (Security UTM)

### Syntax

```
routing-instance name;
```

### Hierarchy Level

```
[edit security utm feature-profile anti-virus sophos-engine pattern-update]
[edit security utm feature-profile web-filtering juniper-enhanced server]
[edit security utm feature-profile web-filtering websense-redirect profile wr server]
[edit security utm feature-profile anti-virus sophos-engine server]
[edit security utm default-configuration anti-virus avira-engine pattern-update]
```

### Release Information

Statement introduced in Junos OS Release 15.1X49-D90.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for Avira engine added in Junos OS Release 18.4R1.

### Description

Configure the routing instance name. A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. The set of interfaces belongs to the routing tables, and the routing protocol parameters control the information in the routing tables. Each routing instance has a unique name.

### Options

***name***—Specify the name of the routing instance.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

admin-email | **363**
url (Security Antivirus) | **613**

# sbl

### Syntax

```
sbl {
    profile profile-name {
        custom-tag-string [string];
        (sbl-default-server | no-sbl-default-server);
        spam-action (block | tag-header | tag-subject);
    }
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-spam]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Configure UTM server-based antispam features.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# sbl-default-server

**Syntax**

```
sbl-default-server;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-spam sbl profile profile-name]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Enable the default SBL server lookup. You should enable this feature if you are using server-based spam filtering. (The SBL server is predefined on the device. It ships with the name and address of the SBL server.)

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# scan-extension

**Syntax**

```
scan-extension filename;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name scan-options]
```

**Release Information**

The Kaspersky feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

For antivirus file extension scanning, configure the scan extension setting by specifying the name of the defined file extension list.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# scan-mode

**Syntax**

```
scan-mode (all | by-extension);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name scan-options]
```

**Release Information**

The scan-mode is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, the statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

You can scan all content or scan content with specific file extensions. You can use a file extension list to define a set of file extensions that are used in file extension scan mode. The antivirus module can then only scan files with extensions on the scan-extension list.

**Options**

- **all**—Scan all files.
- **by-extension**—Scan only files with extensions specified in a file extension list custom object.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# scan-options (Security Antivirus Juniper Express Engine)

### Syntax

```
scan-options {
    content-size-limit value;
    (intelligent-prescreening | no-intelligent-prescreening);
    timeout value;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name]
```

### Release Information

The scan-options (Security Antivirus Juniper Express Engine) is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Configure the antivirus feature to scan specific types of traffic based on various scanning configuration parameters.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# scan-options (Security Antivirus Kaspersky Lab Engine)

### Syntax

```
scan-options {
    content-size-limit value;
    decompress-layer-limit value;
    (intelligent-prescreening | no-intelligent-prescreening);
    scan-extension filename;
    scan-mode (all | by-extension);
    timeout value;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name]
```

### Release Information

The Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Configure the antivirus feature to scan specific types of traffic based on various scanning configuration parameters.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# scan-options (Security Antivirus Sophos Engine)

**Syntax**

```
scan-options {
    content-size-limit value;
    (no-uri-check | uri-check);
    timeout value;
}
```

**Hierarchy Level**

```
[edit security utm default-configuration antivirus scan-options]
```

**Release Information**

Statement introduced in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure the antivirus feature to scan specific types of traffic based on various scanning configuration parameters.

**Options**

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# scan-options (Security Antivirus Avira Engine)

### Syntax

```
scan-options {
    content-size-limit value;
    decompress-layer-limit value;
    (no-pre-detection | pre-detection);
    timeout value;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit antivirus scan-options]
```

### Release Information

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Statement introduced in Junos OS Release 18.4R1.

### Description

Configure the antivirus feature to scan specific types of traffic based on various scanning configuration parameters. The scan engine scans the data by accessing the virus pattern database. You can download and uninstall the Avira scan engine. The antivirus module is the software subsystem on the gateway device that scans specific application layer traffic to protect the user from virus attacks and to prevent virus from spreading. The antivirus module software subsystem consists of a virus signature database, an application proxy, the scan manager, and the scan engine. The scan engine requires a valid license

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

- decompress-layer-limit
- content-size-limit

# secondary-server

### Syntax

```
secondary-server {
    address ipv4-address;
    login sender-email-address {
        password password;
    }
}
```

### Hierarchy Level

```
[edit smtp]
```

### Release Information

Statement added in Junos OS Release 10.0.

### Description

Configure Simple Mail Transfer Protocol (SMTP) secondary server for access authorization for SMTP requests.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

# server (Security Antivirus)

**Syntax**

```
server address-or-url;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update proxy]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update proxy]
[edit security utm feature-profile anti-virus sophos-engine pattern-update proxy]
```

**Release Information**

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 11.2.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Set the IP address or URL for the proxy server.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# server (Security Sophos Engine Antivirus)

**Syntax**

```
server ip;
routing-instance name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine]
```

**Release Information**

Statement introduced in Junos OS Release 15.1X49-D90.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Set server parameters by entering the server IP address.

**Options**

***ip***—Specify Sophos anitivirus and antispam first-hop DNS server IP address.

**routing-instance *name***—Specify the name of the routing instance.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

utm | 619

# server (Security Web Filtering)

### Syntax

```
server {
    host host-name;
    port number;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated]
[edit security utm feature-profile web-filtering websense-redirect profile profile-name]
[edit security utm feature-profile web-filtering juniper-enhanced]
```

### Release Information

The surf-control feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 .
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Set server parameters by entering the server name or IP address.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# server-connectivity

**Syntax**

```
server-connectivity (block | log-and-permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated profile profile-name fallback-settings]
[edit security utm feature-profile web-filtering websense-redirect profile profile-name fallback-settings]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name fallback-settings]
```

**Release Information**

The surf-control feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 .
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Fallback settings tell the system how to handle errors. This is the action that occurs when a request fails for this reason.

**Options**

- block—Log the error and deny the traffic
- log-and-permit—Log the error and permit the traffic

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# site-reputation-action

**Syntax**

```
site-reputation-action {
    harmful (block | log-and-permit | permit | quarantine);
    fairly-safe (block | log-and-permit | permit | quarantine);
    moderately-safe (block | log-and-permit | permit | quarantine);
    suspicious (block | log-and-permit | permit | quarantine);
    very-safe (block | log-and-permit | permit | quarantine);
}
```

**Hierarchy Level**

[edit security utm default-configuration]
[edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name* category *category-name*]

**Release Information**

Statement introduced in Junos OS Release 11.4.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Specify the action to be taken depending on the site reputation returned for all types of URLs whether it is categorized or uncategorized.

> **NOTE:** Starting with Junos OS Release 17.4R1, the reputation base scores are configurable. Users can apply global reputation values, provided by the Websense ThreatSeeker Cloud (TSC). For the non-category URLs, the global reputation value is used to perform filtering,

**Options**

**fairly-safe** —Permit, log-and-permit, block, or quarantine a request if a site-reputation of 70 through 79 is returned.

**harmful** —Permit, log-and-permit, block, or quarantine a request if a site-reputation of zero through 59 is returned.

**moderately-safe** —Permit, log-and-permit, block, or quarantine a request if a site-reputation of 80 through 89 is returned.

**suspicious** —Permit, log-and-permit, block, or quarantine a request if a site-reputation of 60 through 69 is returned.

**very-safe** —Permit, log-and-permit, block, or quarantine a request if a site-reputation of 90 through 100 is returned.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# size (Security Web Filtering Cache)

**Syntax**

```
size value;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated cache]
[edit security utm feature-profile web-filtering juniper-enhanced cache]
```

**Release Information**

The surf-control feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Set the cache size parameters for Web filtering.

**Options**

**Range:** 0 through 4096 kilobytes.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# smtp-profile (Security UTM Policy Antispam)

**Syntax**

```
smtp-profile profile-name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name anti-spam]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure a UTM policy for the antispam SMTP protocol and attach this policy to a security profile to implement it.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

# smtp-profile (Security UTM Policy Antivirus)

**Syntax**

```
smtp-profile profile-name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name anti-virus]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure a UTM policy for the antivirus SMTP protocol and attach this policy to a security profile to implement it.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# smtp-profile (Security UTM Policy Content Filtering)

**Syntax**

```
smtp-profile profile-name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name content-filtering]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure a UTM policy for the content-filtering SMTP protocol and attach this policy to a security profile to implement it.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# sockets

**Syntax**

```
sockets value;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering websense-redirect profile profile-name]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Enter the number of sockets used for communicating between the client and server. The default is 1.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# sophos-engine

**Syntax**

```
sophos-engine {
    pattern-update {
        email-notify {
            admin-email email-address;
            custom-message message;
            custom-message-subject message-subject;
        }
        interval value;
        no-autoupdate;
        proxy {
            password password-string;
            port port-number;
            server address-or-url;
            username name;
        }
        url url;
    }
    profile <name> {
        fallback-options {
            content-size (block | log-and-permit | permit);
            default (block | log-and-permit | permit);
            engine-not-ready (block | log-and-permit | permit);
            out-of-resources (block | log-and-permit | permit);
            timeout (block | log-and-permit | permit);
            too-many-requests (block | log-and-permit | permit);
        }
        notification-options {
            fallback-block {
                administrator-email email-address;
                allow-email;
                custom-message message;
                custom-message-subject message-subject;
                display-host;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
            fallback-non-block {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-recipient | no-notify-mail-recipient);
```

```
        }
        virus-detection {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
        }
    }
    scan-options {
        content-size-limit value;
        (no-uri-check | uri-check);
        timeout value;
    }
    trickling {
        timeout value;
    }
  }
  sxl-retry value;
  sxl-timeout seconds;
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus]
```

**Release Information**

Statement introduced in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure the UTM Sophos antivirus feature.

**Options**

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# spam-action

### Syntax

```
spam-action (block | tag-header | tag-subject);
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-spam sbl profile profile-name]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Configure the action to be taken by the device when spam is detected.

### Options

- **block**— Block e-mail.
- **tag-header**—Tag header of e-mail.
- **tag-subject**—Tag subject of e-mail.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Example: Configuring Server-Based Antispam Filtering | 112
Example: Configuring Local List Antispam Filtering | 121

# start-time

**Syntax**

```
start-time start-time;
```

**Hierarchy Level**

```
[edit security utm default-configuration anti-virus avira-engine pattern-update]
[edit security utm default-configuration anti-virus sophos-engine pattern-update]
```

**Release Information**

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1. Support for Avira engine added in Junos OS Release 18.4R1.

**Description**

Specify the time that the device automatically starts downloading the updated signature database from the specified URL.

**Options**

***start-time***—Time in MM-DD.hh:mm format.

**Required Privilege Level**

security— To view this statement in the configuration.
security-control— To add this statement to the configuration.

# surf-control-integrated

**Syntax**

```
surf-control-integrated {
    cache {
        size value;
        timeout value;
    }
    profile profile-name {
            category customurl-list name {
                action (block | log-and-permit | permit);
            }
        custom-block-message value;
        default (block | log-and-permit | permit);
        fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
            }
            timeout value;
        }
    }
    server {
        host host-name;
        port number;
    }
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[set security utm feature-profile web-filtering]
```

**Release Information**

The surf-control- integrated feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure the UTM web-filtering integrated feature.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# sxl-retry

### Syntax

```
sxl-retry value;
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine]
```

### Release Information

Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Configure the number of retry attempts to the remote Sophos Extensible List (SXL) server when a request timeout occurs.

### Options

***value*** —Number of retries.

**Range:** 0 through 5

**Default:** 1

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# sxl-timeout

**Syntax**

```
sxl-timeout seconds;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine]
```

**Release Information**

Statement introduced in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure the timeout value for responses to a Sophos checksum or URI query.

**Options**

***seconds*** —Number of seconds before timeout occurs.

**Range:** 1 through 5 seconds

**Default:** 2 seconds

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# timeout (Security Antivirus Fallback Options)

**Syntax**

```
timeout (block | log-and-permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name fallback-options]
```

**Release Information**

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Scanning a complex file could consume resources and time. If the time it is taking to scan exceeds the timeout setting in the antivirus profile, the processing is aborted and the content is either passed or blocked without completing the virus checking. The decision is made based on the timeout fallback option. The default action is block.

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# timeout (Security Antivirus Fallback Options Sophos Engine)

**Syntax**

```
default (block | log-and-permit | permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name fallback-options]
```

**Release Information**

Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Scanning a complex file could consume resources and time. If the time it is taking to scan exceeds the timeout setting in the antivirus profile, the processing is aborted and the content is either passed or blocked without completing the virus checking. The decision is made based on the timeout fallback option.

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic
- **permit**—Permit the traffic

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# timeout (Security Antivirus Scan Options)

**Syntax**

```
timeout value;
```

**Hierarchy Level**

```
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name scan-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name scan-options]
[edit security utm default-configuration anti-virus scan-options]
```

**Release Information**

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1. Support for Avira engine added in Junos OS Release 18.4R1.

**Description**

The scanning timeout value includes the time frame from when the scan request is generated to when the scan result is returned by the scan engine. The time range can be 1 to 1800 seconds. By default, it is 180 seconds.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# timeout (Security Web Filtering)

**Syntax**

```
timeout value;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering websense-redirect profile profile-name]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Enter a timeout limit for requests. Once this limit is reached, fail mode settings are applied. The default here is 15 seconds.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# timeout (Security Web Filtering Cache)

**Syntax**

```
timeout value;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated cache]
[edit security utm feature-profile web-filtering juniper-enhanced cache]
```

**Release Information**

The surf-control-integrated feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Set the cache timeout parameters for surf-control-integrated web filtering (24 hours is the default and the maximum allowed life span of cached items).

**Options**

**Range:** 1 through 1800 minutes.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# timeout (Security Web Filtering Fallback Settings)

**Syntax**

```
timeout (block | log-and-permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated profile profile-name fallback-settings]
[edit security utm feature-profile web-filtering websense-redirect profile profile-name fallback-settings]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name fallback-settings]
```

**Release Information**

The surf-control-integrated feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Fallback settings tell the system how to handle errors.

**Options**

- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# too-many-requests (Security Antivirus Fallback Options)

**Syntax**

```
too-many-requests (block | log-and-permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name fallback-options]
```

**Release Information**

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

If the total number of messages received concurrently exceeds 4000, the content is either passed or blocked depending on the too-many-request fallback option. The default action is block. (The allowed request limit is not configurable.)

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# too-many-requests (Security Antivirus Fallback Options Sophos Engine)

**Syntax**

```
default (block | log-and-permit | permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name fallback-options]
```

**Release Information**

Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

If the total number of messages received concurrently exceeds the device limits, the content is either passed or blocked depending on the too-many-request fallback option. (The allowed request limit is not configurable.)

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic
- **permit**—Permit the traffic

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# too-many-requests (Security Web Filtering Fallback Settings)

**Syntax**

```
too-many-requests (block | log-and-permit);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated profile profile-name fallback-settings]
[edit security utm feature-profile web-filtering websense-redirect profile profile-name fallback-settings]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name fallback-settings]
```

**Release Information**

The surf-control-integrated feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

If the total number of messages received concurrently exceeds the device limits, the content is either passed or blocked depending on the too-many-request fallback option. The default action is BLOCK. (The allowed request limit is not configurable.)

**Options**

- block—Log the error and deny the traffic
- log-and-permit—Log the error and permit the traffic

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# to-zone (Security Policies)

**Syntax**

```
to-zone zone-name {
    policy policy-name {
        description description;
        match {
            application {
                [application];
                any;
            }
            destination-address {
                [address];
                any;
                any-ipv4;
                any-ipv6;
            }
            source-address {
                [address];
                any;
                any-ipv4;
                any-ipv6;
            }
            source-identity {
                [role-name];
                any;
                authenticated-user;
                unauthenticated-user;
                unknown-user;
            }
        }
        scheduler-name scheduler-name;
        then {
            count {
                alarm {
                    per-minute-threshold number;
                    per-second-threshold number;
                }
            }
            deny;
            log {
                session-close;
                session-init;
```

```
    }
```

```
permit {
    application-services {
        application-firewall {
            rule-set rule-set-name;
        }
        application-traffic-control {
            rule-set rule-set-name;
        }
        gprs-gtp-profile profile-name;
        gprs-sctp-profile profile-name;
        idp;
        redirect-wx | reverse-redirect-wx;
        ssl-proxy {
            profile-name profile-name;
        }
        uac-policy {
            captive-portal captive-portal;
        }
        utm-policy policy-name;
    }
    destination-address {
        drop-translated;
        drop-untranslated;
    }
    firewall-authentication {
        pass-through {
            access-profile profile-name;
            client-match user-or-group-name;
            ssl-termination-profile profile-name;
            web-redirect;
            web-redirect-to-https;
        }
        web-authentication {
            client-match user-or-group-name;
        }
    }
    services-offload;
    tcp-options {
        sequence-check-required;
        syn-check-required;
    }
    tunnel {
        ipsec-group-vpn group-vpn;
        ipsec-vpn vpn-name;
```

```
                pair-policy pair-policy;
            }
        }
        reject;
    }
  }
}
```

**Hierarchy Level**

```
[edit security policies from-zone zone-name]
```

**Release Information**

Statement introduced in Junos OS Release 8.5. Support for the **services-offload** and **junos-host** options added in Junos OS Release 11.4. Support for the **source-identity** option added in Junos OS Release 12.1. Support for the **ssl-termination-profile** and **web-redirect-to-https** options added in Junos OS Release 12.1X44-D10.

**Description**

Specify a destination zone to be associated with the security policy.

**Options**

- **zone-name**—Name of the destination zone object.
- **junos-host**—Default security zone for self-traffic of the device.

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

- *Security Policies Overview*
- *Understanding Security Policy Rules*
- *Understanding Security Policy Elements*

# traceoptions (Security Antispam)

**Syntax**

```
traceoptions flag flag;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-spam]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Define tracing operations for UTM antispam features.

**Options**

- ***flag***:
  - **all**—Enable all antispam trace flags.
  - **manager** —Trace antispam manager information.
  - **sbl**—Trace SBL server information.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# traceoptions (Security Antivirus)

**Syntax**

```
traceoptions flag flag;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Define tracing operations for UTM antivirus features.

**Options**

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Enable trace all antivirus trace options.
  - **basic**—Trace antivirus module generic basic information.
  - **detail**—Trace antivirus module generic detail information.
  - **engine**—Trace scan engine information.
  - **event**—Trace communication events between routing engine side processes.
  - **ipc**—Trace communication events with Packet Forwarding Engine.
  - **manager**—Trace antivirus manager process activities.
  - **pattern**—Trace detail information of pattern loading.
  - **sendmail**—Trace mail notifying process activities.
  - **statistics**—Trace statistics information.
  - **updater**—Trace pattern updater process activities.
  - **worker**—Trace antivirus worker process activities.

**Required Privilege Level**

trace—To view this statement in the configuration.

trace-control—To add this statement to the configuration.

# traceoptions (Security Application Proxy)

### Syntax

```
traceoptions {
    flag flag;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm application-proxy]
[edit logical-system logical-system-name security]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
The logical system option is introduced in Junos OS Release 18.3R1.

### Description

Configure tracing options for application proxy.

### Options

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **abort**—Trace aborted sessions for application proxy.
  - **all**—Trace with all flags enabled.
  - **anti-virus**—Trace anti-virus information.
  - **application-objects**—Trace application-proxy objects information.
  - **basic**—Trace application-proxy related basic information.
  - **buffer**— Trace application-proxy data buffer information.
  - **connection-rating**—Trace connection rating information.
  - **detail**—Trace application-proxy related detailed information.
  - **express-anti-virus**—Trace anti-virus express engine information.
  - **ftp-control**—Trace FTP control connection information.
  - **ftp-data**—Trace FTP data connection information.
  - **http**—Trace HTTP protocol information.

- **imap**—Trace IMAP protocol information.
- **memory**—Trace memory usage.
- **mime**—Trace MIME parser information.
- **parser**— Trace protocol parser information.
- **pfe**—Trace communication with PFE.
- **pop3**—Trace POP3 protocol information.
- **queue**—Trace queue information.
- **regex-engine**—Trace Pattern Match Engine (PME) information.
- **smtp**—Trace SMTP protocol information.
- **sophos-anti-virus**—Trace anti-virus sophos engine information.
- **tcp**—Trace TCP level information.
- **timer**—Trace timer processing.
- **utm-realtime**—Trace application-proxy realtime-thread information

**Required Privilege Level**
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

# traceoptions (Security Content Filtering)

**Syntax**

```
traceoptions flag flag;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Define tracing options for content filtering features.

**Options**

- ***flag***:
  - **all**—Enable all content filtering trace flags.
  - **basic** —Trace content filtering basic information.
  - **detail**—Trace content filtering detailed information.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# traceoptions (Security UTM)

**Syntax**

```
traceoptions flag flag;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Define tracing operations for UTM features.

**Options**

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Enable trace for all UTM trace options.
  - **cli**—Trace CLI configuration activity and command changes.
  - **daemon**—Trace daemon information.
  - **ipc**—Trace communication events with Packet Forwarding Engine (PFE).
  - **pfe**—Trace PFE information.

**Required Privilege Level**

trace—To view this statement in the configuration.

trace-control—To add this statement to the configuration.

# traceoptions (Security Web Filtering)

**Syntax**

```
traceoptions flag flag;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering]
```

**Release Information**

Command introduced in Junos OS Release 10.1.
Command introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Define tracing operations for individual Web filtering modules. To specify more than one tracing operation, include multiple flag statements.

**Options**

- ***flag***:
  - **all**—Enable all Web filtering trace flags.
  - **basic** —Trace basic information on the Web filtering module.
  - **cache**—Enable Web filtering flags for the Web filtering cache maintained on the Web filtering module.
  - **enhanced**—Enable Web filtering flags for processing through Enhanced Web Filtering.
  - **heartbeat**—Trace connectivity information with Web filter server.
  - **ipc**—Trace Web filtering IPC messages.
  - **packet**—Trace packet information from session management.
  - **profile**—Trace profile configuration information.
  - **requests**—Trace requests sent to Web filter server.
  - **response**—Trace response received from Web filter server.
  - **session manager**—Trace session management information.
  - **socket**—Trace the communication socket with Web filter server.
  - **timer**—Trace aging information for requests sent to server.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# traceoptions (SMTP)

**Syntax**

```
traceoptions {
    flag {
        all;
        configuration;
        IPC;
        protocol-exchange;
        send-request;
    }
}
```

**Hierarchy Level**

```
[edit smtp]
```

**Release Information**
Statement added in Junos OS Release 10.0.

**Description**
Set the Simple Mail Transfer Protocol (SMTP) traceoptions.

**Options**
The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

utm | 619

# traffic-options

### Syntax

```
traffic-options {
    sessions-per-client {
        limit value;
        over-limit (block | log-and-permit);
    }
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# trickling

### Syntax

```
trickling {
    timeout value;
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name]
```

### Release Information

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1. The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Statement updated for Sophos support in Junos OS Release 11.1.

### Description

HTTP trickling is a mechanism used to prevent the HTTP client or server from timing-out during a file transfer or during antivirus scanning. HTTP Trickling is time-based and there is only one parameter to configure for this feature, which is the timeout Interval. By default, trickling is disabled.

**WARNING:** When you enable the trickling option, keep in mind that trickling might send part of a file to the client during its antivirus scan. It is therefore possible that some of the content could be received by the client before the file has been fully scanned.

### Options

***value***—Timeout interval in seconds.

**Range:** 0 through 600 seconds

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# type (Security Antivirus Feature Profile)

**Syntax**

```
type (juniper-express-engine | kaspersky-lab-engine | sophos-engine);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus]
```

**Release Information**

The Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Statement updated for Sophos in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Set the antivirus engine that will be used on the device. You can only have one engine type running and you must restart the device if you change engines.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# type (Security Content Filtering Notification Options)

**Syntax**

```
type (message | protocol-only);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name notification-options]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

When content is blocked, the client generally still receives a successful response code but with modified content (file replacement) containing a warning message. But with protocol-only notifications, a protocol-specific error code might be returned to the client.

**Options**

- **message**—Send a generic notification.
- **protocol-only**—Send a protocol-specific notification.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# type (Security Fallback Block)

**Syntax**

```
type (message | protocol-only);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options
    fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options
    fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options fallback-block]
```

**Release Information**

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1. The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1 .

**Description**

You can configure notifications for both fallback blocking and fallback nonblocking actions. With protocol-only notifications, a protocol-specific error code may be returned to the client.

**Options**

- message—Send a generic notification.
- protocol-only—Send a protocol-specific notification.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# type (Security Virus Detection)

**Syntax**

```
type (message | protocol-only);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options
    virus-detection]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options
    virus-detection]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options virus-detection]
```

**Release Information**

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1. The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

**Description**

When content is blocked because a virus is found or a scan error occurs, the client generally still receives a successful response code but with modified content (file replacement) containing a warning message. But with protocol-only notifications, a protocol-specific error code might be returned to the client.

**Options**

- message—Send a generic notification.
- protocol-only—Send a protocol-specific notification.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# type (Security Web Filtering)

**Syntax**

```
type (juniper-enhanced | juniper-local | surf-control-integrated | websense-redirect);
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering]
```

**Release Information**

The surf-control-integrated feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, command introduced in Junos OS Release 9.5.
Command introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Define the type of Web filtering solution or URL filtering solution used by the device.

**Options**

- **juniper-enhanced**—Enable Enhanced Web Filtering on the device.
- **juniper-local** —Enable Juniper Networks local URL filtering on the device.
- **surf-control-integrated**—Enable integrated Web filtering on the device.
- **websense-redirect**—Redirect the URL to the Websense server.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# upload-profile (Security Antivirus FTP)

**Syntax**

```
upload-profile profile-name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name anti-virus ftp]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure a UTM policy for the antivirus FTP (upload) protocol and attach this policy to a security profile to implement it.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# upload-profile (Security Content Filtering FTP)

**Syntax**

```
upload-profile profile-name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name content-filtering ftp]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure a UTM policy for the content-filtering FTP (upload) protocol and attach this policy to a security profile to implement it.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# uri-check

**Syntax**

```
uri-check;
```

**Hierarchy Level**

```
[edit security utm default-configuration anti-virus scan-options]
```

**Release Information**

Statement introduced in Junos OS Release 11.1.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Perform Sophos antivirus Uniform Resource Identifier (URI) checking. URI checking is a way of analyzing URI content in HTTP traffic against a remote Sophos database to identify malware or malicious content. URI checking is on by default.

> **NOTE:** Starting in Junos OS release 18.4R1, the URI checking is off by default.

You can disable Sophos antivirus URI checking with the **no-uri-check** statement.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# url (Security Antivirus)

**Syntax**

```
url url;
```

**Hierarchy Level**

```
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]
[edit security utm feature-profile anti-virus sophos-engine pattern-update]
[edit security utm default-configuration anti-virus avira-engine pattern-update]
```

**Release Information**

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 for Juniper Express engine and Kaspersky Lab engine. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1. Support for Avira engine added in Junos OS Release 18.4R1.

**Description**

Specify the URL for the pattern database. You should not change the default URL unless you are experiencing problems with it and have called for support.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# url-blacklist

### Syntax

```
url-blacklist listname;
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

This is a global blocklist category, blocking content for Web filtering.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# url-pattern

### Syntax

```
url-pattern object-name {
    value [value];
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm custom-objects]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

Use URL pattern lists to create custom URL category lists. These are lists of patterns that bypass scanning.

**WARNING:** Custom category does not take precedence over predefined categories when it has the same name as one of the predefined categories. We do not recommend having a custom category name be the same as the predefined category name.

### Options

- ***object-name***—Name of the URL list object.
- **value *value***—Value of the URL list object. You can configure multiple values separated by spaces and enclosed in square brackets.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

*Security Policies User Guide for Security Devices*

# url-whitelist

**Syntax**

```
url-whitelist listname;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

A URL allowlist is a unique custom list that you define in which all the URLs or IP addresses in that list for a specified category are always bypassed for scanning.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# url-whitelist

### Syntax

```
url-whitelist listname;
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering]
```

### Release Information

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

### Description

A URL allowlist is a unique custom list that you define in which all the URLs or IP addresses in that list for a specified category are always bypassed for filtering

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# username (Security Antivirus)

**Syntax**

```
username name;
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update proxy]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update proxy]
[edit security utm feature-profile anti-virus sophos-engine pattern-update proxy]
```

**Release Information**

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 11.2.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Set the username for the proxy server.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

# utm

**Syntax**

```
utm {
    application-proxy {
        traceoptions {
            flag flag;
        }
    }
    custom-objects {
        custom-url-category object-name {
            value [value];
        }
        filename-extension object-name {
            value [value];
        }
        mime-pattern object-name {
            value [value];
        }
        protocol-command object-name {
            value [value];
        }
        url-pattern object-name {
            value [value];
        }
    }
    feature-profile {
        anti-spam {
            address-blacklist list-name;
            address-whitelist list-name;
            sbl {
                profile profile-name {
                    custom-tag-string [string];
                    (sbl-default-server | no-sbl-default-server);
                    spam-action (block | tag-header | tag-subject);
                }
            }
            traceoptions {
                flag flag;
            }
        }
        anti-virus {
            juniper-express-engine {
```

```
pattern-update {
    email-notify {
        admin-email email-address;
        custom-message message;
        custom-message-subject message-subject;
    }
    interval value;
    no-autoupdate;
    proxy {
        password password-string;
        port port-number;
        server address-or-url;
        username name;
    }
    url url;
}
```

```
    profile profile-name {
        fallback-options {
            content-size (block | log-and-permit);
            default (block | log-and-permit);
            engine-not-ready (block | log-and-permit);
            out-of-resources (block | (log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        notification-options {
            fallback-block {
                administrator-email email-address;
                allow-email;
                custom-message message;
                custom-message-subject message-subject;
                display-host;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
            fallback-non-block {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-recipient | no-notify-mail-recipient);
            }
            virus-detection {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
        }
        scan-options {
            content-size-limit value;
            (intelligent-prescreening | no-intelligent-prescreening);
            timeout value;
        }
        trickling {
            timeout value;
        }
    }
}
```

```
kaspersky-lab-engine {
    pattern-update {
        email-notify {
            admin-email email-address;
            custom-message message;
            custom-message-subject message-subject;
        }
        interval value;
        no-autoupdate;
        proxy {
            password password-string;
            port port-number;
            server address-or-url;
            username name;
        }
        url url;
    }
    profile profile-name {
        fallback-options {
            content-size (block | log-and-permit);
            corrupt-file (block | log-and-permit);
            decompress-layer (block | log-and-permit);
            default (block | log-and-permit);
            engine-not-ready (block | log-and-permit);
            out-of-resources (block | (log-and-permit);
            password-file (block | (log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        notification-options {
            fallback-block {
                administrator-email email-address;
                allow-email;
                custom-message message;
                custom-message-subject message-subject;
                display-host;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
            fallback-non-block {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-recipient | no-notify-mail-recipient);
            }
```

```
            virus-detection {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
        }
        scan-options {
            content-size-limit value;
            decompress-layer-limit value;
            (intelligent-prescreening | no-intelligent-prescreening);
            scan-extension filename;
            scan-mode (all | by-extension);
            timeout value;
        }
        trickling {
            timeout value;
        }
    }
}
mime-whitelist {
    exception listname;
    list listname {
        exception listname;
    }
}
```

```
sophos-engine {
    pattern-update {
        email-notify {
            admin-email email-address;
            custom-message message;
            custom-message-subject message-subject;
        }
        interval value;
        no-autoupdate;
        proxy {
            password password-string;
            port port-number;
            server address-or-url;
            username name;
        }
        url url;
    }
    profile <name> {
        fallback-options {
            content-size (block | log-and-permit | permit);
            default (block | log-and-permit | permit);
            engine-not-ready (block | log-and-permit | permit);
            out-of-resources (block | log-and-permit | permit);
            timeout (block | log-and-permit | permit);
            too-many-requests (block | log-and-permit | permit);
        }
        notification-options {
            fallback-block {
                administrator-email email-address;
                allow-email;
                custom-message message;
                custom-message-subject message-subject;
                display-host;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
            fallback-non-block {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-recipient | no-notify-mail-recipient);
            }
            virus-detection {
                custom-message message;
                custom-message-subject message-subject;
```

```
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
        }
        scan-options {
            content-size-limit value;
            (no-uri-check | uri-check);
            timeout value;
        }
        trickling {
            timeout value;
        }
    }
    sxl-retry value;
    sxl-timeout seconds;
  }
  traceoptions {
    flag flag;
  }
  type (juniper-express-engine | kaspersky-lab-engine | sophos-engine);
  url-whitelist listname;
}
content-filtering {
  profile profile-name {
    block-command protocol-command-list;
    block-content-type (activex | exe | http-cookie | java-applet | zip);
    block-extension extension-list;
    block-mime {
      exception list-name;
      list list-name;
    }
    notification-options {
      custom-message message;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
    permit-command protocol-command-list;
  }
  traceoptions {
    flag flag;
  }
}
```

```
web-filtering {
    juniper-enhanced {
        cache {
            size value;
            timeout value;
        }
        profile profile-name {
            block-message {
                type {
                    custom-redirect-url;
                }
                url url;
                }
            quarantine-message {
                type {
                    custom-redirect-url;
                }
                    url url;
                    }
            category customurl-list name {
                action (block | log-and-permit | permit | quarantine);
            }
            custom-block-message value;
            custom-quarantine-message value;
            default (block | log-and-permit | permit | quarantine);
            fallback-settings {
                default (block | log-and-permit);
                server-connectivity (block | log-and-permit);
                timeout (block | log-and-permit);
                too-many-requests (block | log-and-permit);
            }
            no-safe-search;
            site-reputation-action {
                fairly-safe (block | log-and-permit | permit | quarantine);
                harmful (block | log-and-permit | permit | quarantine);
                moderately-safe (block | log-and-permit | permit | quarantine);
                suspicious (block | log-and-permit | permit | quarantine);
                very-safe (block | log-and-permit | permit |quarantine);
            }
            timeout value;
        }
        server {
            host host-name;
            port number;
```

```
    }
}
juniper-local {
    profile profile-name {
        custom-block-message value;
        default (block | log-and-permit | permit);
        fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        timeout value;
    }
}
surf-control-integrated {
    cache {
        size value;
        timeout value;
    }
    profile profile-name {
        category customurl-list name {
            action (block | log-and-permit | permit);
        }
        custom-block-message value;
        default (block | log-and-permit | permit);
        fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        timeout value;
    }
    server {
        host host-name;
        port number;
    }
}
traceoptions {
    flag flag;
}
type (juniper-enhanced | juniper-local | surf-control-integrated | websense-redirect);
url-blacklist listname;
```

```
        url-whitelist listname;
        websense-redirect {
            profile profile-name {
                account value;
                custom-block-message value;
                fallback-settings {
                    default (block | log-and-permit);
                    server-connectivity (block | log-and-permit);
                    timeout (block | log-and-permit);
                    too-many-requests (block | log-and-permit);
                }
                server {
                    host host-name;
                    port number;
                }
                sockets value;
                timeout value;
            }
        }
    }
}
ipc {
    traceoptions flag flag;
}
traceoptions {
    flag flag;
}
```

```
    utm-policy policy-name {
        anti-spam {
            smtp-profile profile-name;
        }
        anti-virus {
            ftp {
                download-profile profile-name;
                upload-profile profile-name;
            }
            http-profile profile-name;
            imap-profile profile-name;
            pop3-profile profile-name;
            smtp-profile profile-name;
        }
        content-filtering {
            ftp {
                download-profile profile-name;
                upload-profile profile-name;
            }
            http-profile profile-name;
            imap-profile profile-name;
            pop3-profile profile-name;
            smtp-profile profile-name;
        }
        traffic-options {
            sessions-per-client {
                limit value;
                over-limit (block | log-and-permit);
            }
        }
        web-filtering {
            http-profile profile-name;
        }
    }
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security]
```

**Release Information**

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1. The Kaspersky, surf-control-integrated, and express antivirus features are not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 .

**Description**

Configure UTM features.

**Options**

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# utm default-configuration

**Syntax**

```
utm {
    default-configuration {
        anti-spam {
            address-blacklist;
            address-whitelist;
            sbl {
                custom-tag-string;
                (sbl-default-server | no-sbl-default-server);
                spam-action (block | tag-header | tag-subject);
            }
            traceoptions {
                flag name;
            }
            type (anti-spam-none | sbl);
        }
        anti-virus {
            mime-whitelist {
                exception;
                list;
            }
            sophos-engine {
                fallback-options {
                    content-size (block | log-and-permit | permit);
                    default (block | log-and-permit | permit);
                    engine-not-ready (block | log-and-permit | permit);
                    out-of-resources (block | log-and-permit | permit);
                    timeout (block | log-and-permit | permit);
                    too-many-requests (block | log-and-permit | permit);
                }
                    forwarding-mode {
                        hold;
                        inline-tap;
                    }
                notification-options {
                    fallback-block {
                        custom-message;
                        custom-message-subject;
                        (notify-mail-sender | no-notify-mail-sender);
                        type (message | protocol-only);
                    }
```

```
        fallback-non-block {
            custom-message;
            custom-message-subject;
            (notify-mail-recipient | no-notify-mail-recipient);
        }
        virus-detection {
            custom-message;
            custom-message-subject;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
        }
    }
    pattern-update {
        email-notify {
            admin-email;
            custom-message;
            custom-message-subject;
        }
        interval;
        no-autoupdate;
        proxy {
            password;
            port;
            server;
            username;
        }
        routing-instance;
        url;
    }
    scan-options {
        content-size-limit;
        timeout seconds;
        (uri-check | no-uri-check);
    }
    server {
        ip;
        routing-instance;
    }
    sxl-retry;
    sxl-timeout seconds;
    trickling timeout;
}
```

```
    traceoptions {
        flag name;
    }
    url-whitelist;
}
content-filtering {
    block-command;
    block-content-type {
        activex;
        exe;
        http-cookie;
        java-applet;
        zip;
    }
    block-extension;
    block-mime {
        exception;
        list;
    }
    notification-options {
        custom-message;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
    }
    permit-command;
    traceoptions {
        flag name;
    }
    type (content-filtering-none | local);
}
```

```
web-filtering {
    http-persist;
    http-reassemble;
    juniper-enhanced {
        base-filter;
        block-message {
            type custom-redirect-url;
            url;
        }
        cache {
            size kilobytes;
            timeout minutes;
        }
        category name {
            action (block | log-and-permit | permit | quarantine);
            custom-message;
        }
        custom-block-message;
        default (block | log-and-permit | permit | quarantine);
        fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        no-safe-search;
        quarantine-custom-message;
        quarantine-message {
            type custom-redirect-url;
            url;
        }
        reputation {
            reputation-fairly-safe;
            reputation-moderately-safe;
            reputation-suspicious;
            reputation-very-safe;
        }
        server {
            host;
            port;
            routing-instance;
        }
        site-reputation-action {
            fairly-safe (block | log-and-permit | permit | quarantine);
```

```
        harmful (block | log-and-permit | permit | quarantine);
        moderately-safe (block | log-and-permit | permit | quarantine);
        suspicious (block | log-and-permit | permit | quarantine);
        very-safe (block | log-and-permit | permit | quarantine);
    }
    timeout seconds;
}
juniper-local {
    block-message {
        type custom-redirect-url;
        url;
    }
    category name {
        action (block | log-and-permit | permit | quarantine);
        custom-message;
    }
    custom-block-message;
    default (block | log-and-permit | permit);
    fallback-settings {
        default (block | log-and-permit);
        server-connectivity (block | log-and-permit);
        timeout (block | log-and-permit);
        too-many-requests (block | log-and-permit);
    }
    quarantine-custom-message;
    quarantine-message {
        type custom-redirect-url;
        url;
    }
    timeout seconds;
}
traceoptions {
    flag name;
}
url-blacklist;
url-whitelist;
```

```
        websense-redirect {
            account;
            block-message {
                type custom-redirect-url;
                url;
            }
            category name {
                action (block | log-and-permit | permit | quarantine);
                custom-message;
            }
            custom-block-message;
            fallback-settings {
                default (block | log-and-permit);
                server-connectivity (block | log-and-permit);
                timeout (block | log-and-permit);
                too-many-requests (block | log-and-permit);
            }
            quarantine-custom-message;
            quarantine-message {
                type custom-redirect-url;
                url;
            }
            server {
                host;
                port;
                routing-instance;
            }
            sockets;
            timeout seconds;
        }
    }
    application-proxy;
    custom-objects;
    feature-profile;
    traceoptions;
    utm-policy junos-default-utm-policy;
    }
}
```

### Hierarchy Level

```
[edit security utm]
```

**Release Information**

Statement introduced in Junos OS Release 18.2R1.

**Description**

The UTM default configuration is used in two scenarios.

- **UTM default configuration for unified policies**—For security policies that enable UTM with no custom UTM policy defined, the default UTM policy will be used.
- **UTM default configuration for existing UTM policies**—For existing security policies that have a UTM policy enabled, the default UTM policy will NOT be used.

**Options**

**default-configuration**—Global default UTM configurations.

**anti-spam**—Configure the default UTM configuration for antispam feature profile.

**anti-virus**—Configure the default UTM configuration for antivirus feature profile.

**content-filtering**—Configure the default UTM configuration for content filtering feature profile.

**web-filtering**—Configure the default UTM configuration for Web filtering feature profile.

**utm-policy**—Configure a UTM policy for antivirus, antispam, content filtering, traffic options, and Web filtering protocols and attach this policy to a security profile to implement it.

**traceoptions**—Define tracing operations for UTM features.

**feature-profile**—Configure UTM features, antivirus, antispam, content filtering, and Web filtering by creating feature profiles.

**application-proxy**—Application proxy settings.

**custom-objects**—Configure custom objects before configuring UTM feature-profile features. Custom category does not take precedence over predefined categories when it has the same name as one of the predefined categories. It is not recommended to have a custom category name be the same as the predefined category name.

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

*Unified Threat Management (UTM) support within Unified Policy*

# utm-policy

### Syntax

```
utm-policy policy-name {
    anti-spam {
        smtp-profile profile-name;
    }
    anti-virus {
        ftp {
            download-profile profile-name;
            upload-profile profile-name;
        }
        http-profile profile-name;
        imap-profile profile-name;
        pop3-profile profile-name;
        smtp-profile profile-name;
    }
    content-filtering {
        ftp {
            download-profile profile-name;
            upload-profile profile-name;
        }
        http-profile profile-name;
        imap-profile profile-name;
        pop3-profile profile-name;
        smtp-profile profile-name;
    }
    traffic-options {
        sessions-per-client {
            limit value;
            over-limit (block | log-and-permit);
        }
    }
    web-filtering {
        http-profile profile-name;
    }
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure a UTM policy for antivirus, antispam, content-filtering, traffic-options, and Web-filtering protocols and attach this policy to a security profile to implement it.

**Options**

***policy-name***—Specify name of the UTM policy.

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

- *Security Policies Overview*
- *Understanding Security Policy Rules*
- *Understanding Security Policy Elements*

# utm-policy (Application Services)

**Syntax**

```
utm-policy policy-name;
```

**Hierarchy Level**

```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name then permit application-services]
```

**Release Information**
Statement introduced in Junos OS Release 11.1.

**Description**
Configure a UTM policy for application services and attach this policy to a security profile to implement it.

**Options**
***policy-name***—Specify the name of the UTM policy.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# virus-detection (Security Antivirus)

### Syntax

```
virus-detection {
    custom-message message;
    custom-message-subject message-subject;
    (notify-mail-sender | no-notify-mail-sender);
    type (message | protocol-only);
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name notification-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name notification-options]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name notification-options]
```

### Release Information

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1. The Express and Kaspersky Antivirus features are not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

### Description

Configure a notification to send when a virus is detected.

### Options

The remaining statements are explained separately. See CLI Explorer.

### Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

# web-filtering

**Syntax**

```
web-filtering {
    http-persist;
    http-reassemble;
    juniper-enhanced {
        base-filter;
        block-message {
            type custom-redirect-url;
            url;
        }
        cache {
            size kilobytes;
            timeout minutes;
        }
        category name {
            action (block | log-and-permit | permit | quarantine);
            custom-message;
        }
        custom-block-message;
        default (block | log-and-permit | permit | quarantine);
        fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        no-safe-search;
        quarantine-custom-message;
        quarantine-message {
            type custom-redirect-url;
            url;
        }
        reputation {
            reputation-fairly-safe;
            reputation-moderately-safe;
            reputation-suspicious;
            reputation-very-safe;
        }
        server {
            host;
            port;
```

```
        routing-instance;
    }
    site-reputation-action {
        fairly-safe (block | log-and-permit | permit | quarantine);
        harmful (block | log-and-permit | permit | quarantine);
        moderately-safe (block | log-and-permit | permit | quarantine);
        suspicious (block | log-and-permit | permit | quarantine);
        very-safe (block | log-and-permit | permit | quarantine);
    }
    timeout seconds;
}
juniper-local {
    block-message {
        type custom-redirect-url;
        url;
    }
    category name {
        action (block | log-and-permit | permit | quarantine);
        custom-message;
    }
    custom-block-message;
    default (block | log-and-permit | permit);
    fallback-settings {
        default (block | log-and-permit);
        server-connectivity (block | log-and-permit);
        timeout (block | log-and-permit);
        too-many-requests (block | log-and-permit);
    }
    quarantine-custom-message;
    quarantine-message {
        type custom-redirect-url;
        url;
    }
    timeout seconds;
}
traceoptions {
    flag name;
}
url-blacklist;
url-whitelist;
```

```
    websense-redirect {
        account;
        block-message {
            type custom-redirect-url;
            url;
        }
        category name {
            action (block | log-and-permit | permit | quarantine);
            custom-message;
        }
        custom-block-message;
        fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        quarantine-custom-message;
        quarantine-message {
            type custom-redirect-url;
            url;
        }
        server {
            host;
            port;
            routing-instance;
        }
        sockets;
        timeout seconds;
    }
}
```

**Hierarchy Level**

```
[edit security utm feature-profile]
[edit security utm default-configuration]
```

**Release Information**

The surf-control-integrated feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

**Description**

Configure UTM web filtering features. You can also configure the default UTM configuration for web filtering feature profile. If you do not configure any option in the web filtering feature profile, the values configured in the default UTM configuration are applied. The default UTM Web filtering configuration for HTTP is also applicable for the HTTPS sessions. Web filtering feature's potential policies conflict check is independent of the content filtering, antivirus, and antispam features.

**Options**

**http-persist**—Check all HTTP request in a connection. If **http-persist** option is enabled for clear text HTTP traffic, then Web filtering checks every HTTP request packet in the same session.

**http-reassemble**—Reassemble HTTP request segments. If http-reassemble option is enabled for clear text HTTP traffic, then Enhanced Web Filtering (EWF) reassembles the fragmented HTTP request to avoid evasion instead of packet-based inspection.

**juniper-enhanced**—Enable enhanced Web filtering on the device.

**base-filter**—A base filter is an object that contains a category-action pair for all categories defined in the category file.

**block-message**—Juniper enhanced block message settings.

**cache**—Set the cache parameters for Surf-Control-Integrated Web filtering and Enhanced Web Filtering.

**category**—Select a custom URL category list you created (custom objects) for filtering against.

**custom-block-message**—Enter a custom message to be sent when HTTP requests are blocked.

**default**—Specify an action for the profile, for requests that experience internal errors in the Web filtering module.

**fallback-settings**—Fallback settings tell the system how to handle errors.

**no-safe-search**— Do not perform safe-search for Juniper enhanced protocol. Safe-search redirect supports HTTP only. Therefore it is not possible to generate a redirect response for HTTPS search URLs. Safe-search redirects can be disabled by using the CLI option **no-safe-search**.

**quarantine-custom-message**—Juniper enhanced quarantine custom message.

**quarantine-message**—Juniper enhanced quarantine message settings.

**reputation**—Customize reputation level. The ThreatSeeker Cloud (TSC) provides site reputation information. Based on these reputations, you can choose a block or a permit action.

**server**—Set server parameters by entering the server name or IP address.

**site-reputation-action**—Specify the action to be taken depending on the site reputation returned for all types of URLs whether it is categorized or uncategorized.

**timeout**—Enter a timeout limit for requests. Once this limit is reached, fail mode settings are applied.

**Range:** 1 through 120

**juniper-local**—Enable Juniper Networks local URL filtering on the device.

**block-message**—Juniper local block message settings.

**traceoptions**—Trace options for Web filtering feature.

**url-blacklist**—This is a global blocklist category, blocking content for Web filtering.

**url-whitelist**—A URL allowlist is a unique custom list that you define in which all the URLs or IP addresses in that list for a specified category are always bypassed for filtering.

**websense-redirect**—Web filtering websense redirect engine. Websense occasionally releases new EWF categories. EWF classifies websites into categories according to host, URL, or IP address and performs filtering based on the categories.

**type**—Type of Web filtering solution or URL filtering solution used by the device.

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

Understanding Local Web Filtering | 192
Monitoring Web Filtering Configurations | 230

# web-filtering (Security UTM Policy)

**Syntax**

```
web-filtering {
    http-profile http-profile;
}
```

**Hierarchy Level**

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name]
[edit logical-systems logical-systems-name security utm utm-policy policy-name]
[edit tenants tenant-name security utm utm-policy policy-name]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.
Support in default configuration introduced in Junos OS Release 18.2R1.
Support for configuration in logical systems introduced in Junos OS Release 18.3R1.
Support for configuration in tenant systems introduced in Junos OS Release 19.2R1.

**Description**

Configures a UTM policy for the Web filtering protocols and attach this policy to a security profile to implement it. Web filtering allows you to manage Internet usage by preventing access to inappropriate Web content.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Web Filtering Overview | 147

# websense-redirect

### Syntax

```
websense-redirect {
    profile profile-name {
        account value;
        custom-block-message value;
        fallback-settings{
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        server {
            host host-name;
            port number;
        }
        sockets value;
        timeout value;
        no-safe-search;
    }
}
```

### Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering]
```

### Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
**no-safe-search** option added in Junos OS Release 20.2R1.

### Description

Configure the Websense redirect engine features.

Starting with Junos OS Release 17.4R1, you can download and dynamically load new Enhanced Web Filtering (EWF) categories. The downloading and dynamic loading of the new EWF categories do not require a software upgrade. Websense occasionally releases new EWF categories. EWF classifies websites into categories according to host, URL, or IP address and performs filtering based on the categories.

The new categories do not affect the existing configurations. You can modify the existing configurations to make use of the new categories.

**Options**

**no-safe-search**—Disable the safe search function.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

Example: Enhancing Security by Configuring Redirect Web Filtering Using Custom Objects | 210

CHAPTER 8

# Operational Commands

# clear security utm anti-spam statistics

**Syntax**

```
clear security utm anti-spam statistics
<root-logical-system>
<logical-system (logical-system-name | all)>
<all-logical-systems-tenants>
<tenant (tenant-name | all)>
```

**Release Information**

Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4.
Support for UTM in logical system added in Junos OS Release 18.3R1.
Support for UTM in tenant system added in Junos OS Release 19.2R1.

**Description**

Clears antispam statistics information. With chassis cluster support for UTM, statistics from both the nodes is cleared.

Starting in Junos OS Release 18.3R1, you can clear the antispam statistics information for the master logical system or for a specific user logical system or for all the user logical systems.

Starting in Junos OS Release 19.2R1, you can clear the antispam statistics information for a specific tenant system or for all the tenant systems.

**Options**

**none**—Clears the antispam statistics information for the master logical system.

***root-logical-system***—(Optional) Clears the antispam statistics information for the master logical system.

**logical-system *logical-system-name***—(Optional) Clears the antispam statistics information for a specific user logical system.

**all**—(Optional) Clears the antispam statistics information for all the user logical systems.

**all-logical-systems-tenants**—(Optional) Clears the antispam statistics information for all the logical systems and tenant systems.

**tenant *tenant-name***—(Optional) Clears the antispam statistics information for a specific tenant system.

**all**—(Optional) Clears the antispam statistics information for all the tenant systems.

**Required Privilege Level**

clear

RELATED DOCUMENTATION

show security utm anti-spam statistics | 704

show security utm anti-spam status | 709

## Sample Output

**clear security utm anti-spam statistics**

```
user@host> clear security utm anti-spam statistics
```

```
Anti-spam clear statistics result: clear done
```

**clear security utm anti-spam statistics root-logical-system**

```
user@host> clear security utm anti-spam statistics root-logical-system
```

```
Anti-spam clear statistics result: clear done
```

**clear security utm anti-spam statistics logical-system LSYS1**

```
user@host> clear security utm anti-spam statistics logical-system LSYS1
```

```
Anti-spam clear statistics result: clear done
```

**clear security utm anti-spam statistics logical-system all**

```
user@host> clear security utm anti-spam statistics logical-system all
```

```
Anti-spam clear statistics result: clear done
```

**clear security utm anti-spam statistics tenant TSYS1**

```
user@host> clear security utm anti-spam statistics tenant TSYS1
```

```
Anti-spam clear statistics result: clear done
```

**clear security utm anti-spam statistics tenant all**

```
user@host> clear security utm anti-spam statistics tenant all
```

```
Anti-spam clear statistics result: clear done
```

**clear security utm anti-spam statistics all-logical-systems-tenants**

user@host> **clear security utm anti-spam statistics all-logical-systems-tenants**

```
Anti-spam clear statistics result: clear done
```

# clear security utm antivirus statistics

**Syntax**

```
clear security utm anti-virus statistics
<root-logical-system>
<logical-system (logical-system-name | all)>
<all-logical-systems-tenants>
<tenant (tenant-name | all)>
```

**Release Information**

Command introduced in Junos OS Release 9.5.
Support for Sophos Antivirus added in Junos OS Release 11.1.
Support for UTM in chassis cluster added in Junos OS Release 11.4.
Support for UTM in logical system added in Junos OS Release 18.3R1.
Support for UTM in tenant system added in Junos OS Release 19.2R1.

**Description**

Clears antivirus statistics information. With chassis cluster support for UTM, statistics from both the nodes are cleared.

Starting in Junos OS Release 18.3R1, you can clear the antivirus statistics information for the master logical system or for a specific user logical system or for all the user logical systems.

Starting in Junos OS Release 19.2R1, you can clear the antivirus statistics information for a specific tenant system or for all the tenant systems.

**Options**

**none**—Clears the antivirus statistics information for the master logical system.

***root-logical-system***—(Optional) Clears the antivirus statistics information for the master logical system.

**logical-system *logical-system-name***—(Optional) Clears the antivirus statistics information for a specific user logical system.

**all**—(Optional) Clears the antivirus statistics information for all the user logical systems.

**all-logical-systems-tenants**—(Optional) Clears the antivirus statistics information for all the logical systems and tenant systems.

**tenant *tenant-name***—(Optional) Clears the antivirus statistics information for a specific tenant system.

**all**—(Optional) Clears the antivirus statistics information for all the tenant systems.

**Required Privilege Level**

clear

RELATED DOCUMENTATION


- show security utm anti-virus statistics | 711
- show security utm anti-virus status | 718
- request security utm anti-virus juniper-express-engine | 666
- request security utm anti-virus kaspersky-lab-engine | 668


## Sample Output

**clear security utm anti-virus statistics**

```
user@host> clear security utm anti-virus statistics
```

```
Anti-virus clear statistics result: clear done
```

**clear security utm anti-virus statistics root-logical-system**

```
user@host> clear security utm anti-virus statistics root-logical-system
```

```
Anti-virus clear statistics result: clear done
```

**clear security utm anti-virus statistics logical-system LSYS1**

```
user@host> clear security utm anti-virus statistics logical-system LSYS1
```

```
Anti-virus clear statistics result: clear done
```

**clear security utm anti-virus statistics logical-system all**

```
user@host> clear security utm anti-virus statistics logical-system all
```

```
Anti-virus clear statistics result: clear done
```

**clear security utm anti-virus statistics tenant TSYS1**

```
user@host> clear security utm anti-virus statistics tenant TSYS1
```

```
Anti-virus clear statistics result: clear done
```

**clear security utm anti-virus statistics tenant all**

```
user@host> clear security utm anti-virus statistics tenant all
```

```
Anti-virus clear statistics result: clear done
```

**clear security utm anti-virus statistics all-logical-systems-tenants**

```
user@host> clear security utm anti-virus statistics all-logical-systems-tenants
```

```
Anti-virus clear statistics result: clear done
```

# clear security utm content-filtering statistics

**Syntax**

```
clear security utm content-filtering statistics
<root-logical-system>
<logical-system (logical-system-name | all)>
<all-logical-systems-tenants>
<tenant (tenant-name | all)>
```

**Release Information**

Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4.
Support for UTM in logical system added in Junos OS Release 18.3R1.
Support for UTM in tenant system added in Junos OS Release 19.2R1.

**Description**

Clears content-filtering statistics information. With chassis cluster support for UTM, statistics from both the nodes are cleared.

Starting in Junos OS Release 18.3R1, you can clear the content filtering statistics information for the master logical system or for a specific user logical system or for all the user logical systems.

Starting in Junos OS Release 19.2R1, you can clear the content filtering statistics information for a specific tenant system or for all the tenant systems.

**Options**

**none**—Clears the content filtering statistics information for the master logical system.

***root-logical-system***—(Optional) Clears the content filtering statistics information for the master logical system.

**logical-system *logical-system-name***—(Optional) Clears the content filtering statistics information for a specific user logical system.

**all**—(Optional) Clears the content filtering statistics information for all the user logical systems.

**all-logical-systems-tenants**—(Optional) Clears the content filtering statistics information for all the logical systems and tenant systems.

**tenant *tenant-name***—(Optional) Clears the content filtering statistics information for a specific tenant system.

**all**—(Optional) Clears the content filtering statistics information for all the tenant systems.

**Required Privilege Level**

clear

RELATED DOCUMENTATION

show security utm content-filtering statistics | 721

## Sample Output

**clear security utm content-filtering statistics**

```
user@host> clear security utm content-filtering statistics

Content-filtering clear statistics result: clear done
```

**clear security utm content-filtering statistics root-logical-system**

```
user@host> clear security utm content-filtering statistics root-logical-system

Content-filtering clear statistics result: clear done
```

**clear security utm content-filtering statistics logical-system LSYS1**

```
user@host> clear security utm content-filtering statistics logical-system LSYS1

Content-filtering clear statistics result: clear done
```

**clear security utm content-filtering statistics logical-system all**

```
user@host> clear security utm content-filtering statistics logical-system all

Content-filtering clear statistics result: clear done
```

**clear security utm content-filtering statistics tenant TSYS1**

```
user@host> clear security utm content-filtering statistics tenant TSYS1

Content-filtering clear statistics result: clear done
```

**clear security utm content-filtering statistics tenant all**

```
user@host> clear security utm content-filtering statistics tenant all
```

```
Content-filtering clear statistics result: clear done
```

**clear security utm content-filtering statistics all-logical-systems-tenants**

```
user@host> clear security utm content-filtering statistics all-logical-systems-tenants
```

```
Content-filtering clear statistics result: clear done
```

# clear security utm session

**Syntax**

```
clear security utm session
```

**Release Information**

Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4.

**Description**

Clear UTM session information. With chassis cluster support for UTM, sessions on both the nodes are cleared.

**Required Privilege Level**

clear

RELATED DOCUMENTATION

show security utm session | 725
show security utm status | 726

**Output Fields**

This command produces no output.

# clear security utm web-filtering statistics

**Syntax**

```
clear security utm web-filtering statistics
<root-logical-system>
<logical-system (logical-system-name | all)>
<all-logical-systems-tenants>
<tenant (tenant-name | all)>
```

**Release Information**

Command introduced in Junos OS Release 9.5 .
Support for UTM in chassis cluster added in Junos OS Release 11.4 .
Support for UTM in logical system added in Junos OS Release 18.3R1.
Support for UTM in tenant system added in Junos OS Release 19.2R1.

**Description**

Clear web filtering statistics information. With chassis cluster support for UTM, statistics from both the nodes is cleared.

Starting in Junos OS Release 18.3R1, you can clear the Web filtering statistics information for the master logical system or for a specific user logical system or for all the user logical systems.

Starting in Junos OS Release 19.2R1, you can clear the Web filtering statistics information for a specific tenant system or for all the tenant systems.

**Options**

**none**—Clears the Web filtering statistics information for the master logical system.

***root-logical-system***—(Optional) Clears the Web filtering statistics information for the master logical system.

**logical-system *logical-system-name***—(Optional) Clears the Web filtering statistics information for a specific user logical system.

**all**—(Optional) Clears the Web filtering statistics information for all the user logical systems.

**all-logical-systems-tenants**—(Optional) Clears the Web filtering statistics information for all the logical systems and tenant systems.

**tenant *tenant-name***—(Optional) Clears the Web filtering statistics information for a specific tenant system.

**all**—(Optional) Clears the Web filtering statistics information for all the tenant systems.

**Required Privilege Level**

clear

RELATED DOCUMENTATION

show security utm web-filtering statistics | 733

show security utm web-filtering status | 740

## Sample Output

**clear security utm web-filtering statistics**

```
user@host> clear security utm web-filtering statistics
```

```
Web-filtering clear statistics result: clear done
```

**clear security utm web-filtering statistics root-logical-system**

```
user@host> clear security utm web-filtering statistics root-logical-system
```

```
Web-filtering clear statistics result: clear done
```

**clear security utm web-filtering statistics logical-system LSYS1**

```
user@host> clear security utm web-filtering statistics logical-system LSYS1
```

```
Web-filtering clear statistics result: clear done
```

**clear security utm web-filtering statistics logical-system all**

```
user@host> clear security utm web-filtering statistics logical-system all
```

```
Web-filtering clear statistics result: clear done
```

**clear security utm web-filtering statistics tenant TSYS1**

```
user@host> clear security utm web-filtering statistics tenant TSYS1
```

```
Web-filtering clear statistics result: clear done
```

**clear security utm web-filtering statistics tenant all**

```
user@host> clear security utm web-filtering statistics tenant all
```

```
Web-filtering clear statistics result: clear done
```

**clear security utm web-filtering statistics all-logical-systems-tenants**

`user@host>` **clear security utm web-filtering statistics all-logical-systems-tenants**

```
Web-filtering clear statistics result: clear done
```

# request security utm anti-virus juniper-express-engine

**Syntax**

```
request security utm anti-virus juniper-express-engine
```

**Release Information**

The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4 .

**Description**

The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, manually update the express antivirus pattern database using the command described. You can update the express antivirus pattern database automatically or manually. With full chassis cluster support for UTM this command is operational on both the nodes.

**Options**

- **pattern-delete** — Delete the current express antivirus pattern database.
- **pattern-reload** — Reload the express antivirus pattern database.
- **pattern-update** — Update the express antivirus pattern database with the latest signatures.

**Required Privilege Level**

maintenance

RELATED DOCUMENTATION

clear security utm antivirus statistics | 656
show security utm anti-virus statistics | 711
show security utm anti-virus status | 718

**List of Sample Output**

request security utm anti-virus juniper-express-engine pattern-update on page 667

**Output Fields**

request security utm anti-virus juniper-express-engine pattern-update

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

**request security utm anti-virus juniper-express-engine pattern-update**

```
user@host> request security utm anti-virus juniper-express-engine pattern-update
```

# request security utm anti-virus kaspersky-lab-engine

**Syntax**

```
request security utm anti-virus kaspersky-lab-engine
```

**Release Information**

Command introduced in Junos OS Release 11.1 .
Support for UTM in chassis cluster added in Junos OS Release 11.4 .

**Description**

The Kaspersky Antivirus feature is not supported from Junos OS Release 15.1x49-D10 onwards.For previous releases, manually update the full file-based antivirus pattern database using the commands described. You can update the full file-based antivirus pattern database automatically or manually. With full chassis cluster support for UTM this command is operational on both the nodes.

**Options**

- **pattern-delete** — Delete the current full file-based antivirus pattern database.
- **pattern-reload** — Reload the full file-based antivirus pattern database.
- **pattern-update** — Update the full file-based antivirus pattern database with the latest signatures.

**Required Privilege Level**

maintenance

RELATED DOCUMENTATION


request security utm anti-virus juniper-express-engine | 666

clear security utm antivirus statistics | 656

show security utm anti-virus statistics | 711

show security utm anti-virus status | 718


**List of Sample Output**

request security utm anti-virus kaspersky-lab-engine pattern-update on page 669

**Output Fields**

request security utm anti-virus kaspersky-lab-engine pattern-update

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

**request security utm anti-virus kaspersky-lab-engine pattern-update**

```
user@host> request security anti-virus kaspersky-lab-engine pattern-update
```

# request security utm anti-virus sophos-engine

**Syntax**

```
request security utm anti-virus sophos-engine
```

**Release Information**

Command introduced in Junos OS Release 11.1 .
Support for UTM in chassis cluster added in Junos OS Release 11.4 .

**Description**

Manually update the Sophos antivirus pattern database using the command described. To update automatically you use the configuration statement **set security utm feature-profile anti-virus sophos-engine pattern-update interval *seconds***. With full chassis cluster support for UTM this command is operational on both the nodes.

**Options**

- **pattern-delete** — Delete the current Sophos antivirus pattern database.
- **pattern-reload** — Reload the Sophos antivirus pattern database.
- **pattern-update** — Update the Sophos antivirus pattern database with the latest signatures.

**Required Privilege Level**

maintenance

RELATED DOCUMENTATION

clear security utm antivirus statistics | 656
show security utm anti-virus statistics | 711
show security utm anti-virus status | 718

**List of Sample Output**

**request security utm anti-virus sophos-engine pattern-update on page 671**

**Output Fields**

request security utm anti-virus sophos-engine pattern-update

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

**request security utm anti-virus sophos-engine pattern-update**

```
user@host> request security utm anti-virus sophos-engine pattern-update
```

# request security utm anti-virus avira-engine

**Syntax**

```
request security utm anti-virus avira-engine
```

**Release Information**

Command introduced in Junos OS Release 18.4R1.

**Description**

Manually update the Avira antivirus pattern database using the command described. To update automatically you use the configuration statement **set security utm default-configuration anti-virus avira-engine pattern-update interval *seconds***. Avira is an internal scan engine that provides a full file-based anitvirus scanning feature. The full file-based antivirus scanning feature is a separately licensed subscription service. The Avira scan engine is provided as a downloadable UTM module. You can download and install virus signature database.

**Options**

- **pattern-delete** — Delete the current Avira antivirus pattern database.
- **pattern-local-update** — Update the Avira antivirus pattern database from local folder.
- **pattern-reload** — Reload the Avira antivirus pattern database.
- **pattern-update** — Update the Avira antivirus pattern database with the latest signatures.

**Required Privilege Level**

maintenance

RELATED DOCUMENTATION

clear security utm antivirus statistics | 656
show security utm anti-virus statistics | 711
show security utm anti-virus status | 718

**List of Sample Output**



**Output Fields**

request security utm anti-virus avira-engine pattern-delete

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

**request security utm anti-virus avira-engine pattern-delete**

```
user@host> request security utm anti-virus avira-engine pattern-delete
```

```
Anti-virus update request results:
Anti-virus update request results: Starting to delete avira files.
```

## Sample Output

**request security utm anti-virus avira-engine pattern-local-update <path>**

```
user@host> request security utm anti-virus avira-engine pattern-local-update from </var/tmp/db_0531>
```

```
Anti-virus update request results:
av_mgr: pattern updater 30445 is started, updating from /var/tmp/db_0531
```

## Sample Output

**request security utm anti-virus avira-engine pattern-reload**

```
user@host> request security utm anti-virus avira-engine pattern-reload
```

```
Anti-virus update request results:
     Reloading good database starts ...
```

## Sample Output

**request security utm anti-virus avira-engine pattern-update**

```
user@host> request security utm anti-virus avira-engine pattern-update
```

```
Anti-virus update request results:
av_mgr: pattern updater 44934 is started, downloading from
https://update.juniper-updates.net/avira.
```

# request security utm web-filtering category install

**Syntax**

```
request security utm web-filtering category install
```

**Release Information**

Command introduced in Junos OS Release 17.4.

**Description**

Install the predefined category and predefined filter on the system. Users could check the category or filter using the following command: **show security utm web-filtering category base-filter**.

> **NOTE:** During new category file installation, if the category filename is changed, then the new category file overwrites the old category file in the internal system and all related output information is replaced with the new category name.

**Required Privilege Level**

maintenance

RELATED DOCUMENTATION


- category (Security Web Filtering) | 388
- request security utm web-filtering category uninstall | 676


## Sample Output

**request security utm web-filtering category install**

`user@host>` **request security utm web-filtering category install**

```
Category updater result: install done
```

# request security utm web-filtering category uninstall

**Syntax**

```
request security utm web-filtering category uninstall
```

**Release Information**

Command introduced in Junos OS Release 17.4.

**Description**

Reset the predefined category and the base filters to the factory default. This option helps for category rollback.

**Required Privilege Level**

maintenance

RELATED DOCUMENTATION


- category (Security Web Filtering) | 388
- request security utm web-filtering category install | 675


## Sample Output

**request security utm web-filtering category uninstall**

`user@host>` **request security utm web-filtering category uninstall**

```
Category updater result: Uninstall done
```

# request security utm web-filtering category download-install [version]

**Syntax**

```
request security utm web-filtering category download-install version;
```

**Release Information**

Command introduced in Junos OS Release 17.4.

**Description**

Download and install the category file, if no version is specified, the latest version is downloaded and installed during category upgrade.

**Required Privilege Level**

maintenance

RELATED DOCUMENTATION


- category (Security Web Filtering) | 388
- request security utm web-filtering category install | 675
- request security utm web-filtering category download [version] | 678


## Sample Output

**request security utm web-filtering category download-install version 5**

```
user@host> request security utm web-filtering category download-install version 5

Category updater result: Download scheduled
```

# request security utm web-filtering category download [version]

**Syntax**

```
request security utm web-filtering category download version;
```

**Release Information**

Command introduced in Junos OS Release 17.4.

**Description**

Download the category file, if no version is specified, the latest version of the category file is downloaded during category upgrade.

**Required Privilege Level**

maintenance

RELATED DOCUMENTATION


- category (Security Web Filtering) | 388
- request security utm web-filtering category install | 675
- request security utm web-filtering category uninstall | 676
- request security utm web-filtering category download-install [version] | 677


## Sample Output

**request security utm web-filtering category download version 3**

```
user@host> request security utm web-filtering category download version 3

Category updater result: Download done
```

# show configuration smtp

**Syntax**

```
show configuration smtp
```

**Release Information**

Command introduced in Junos OS Release 10.0 .

**Description**

Display complete SMTP information.

**Options**

- apply-groups—Groups from which SMTP inherits configuration data.
- apply-groups-except—Groups from which SMTP restricts inheriting configuration data.

**Required Privilege Level**

view

RELATED DOCUMENTATION

utm | 619

**List of Sample Output**

**show configuration smtp on page 680**

**Output Fields**

Table 10 on page 679 describes the output fields for the **show configuration smtp** command.

**Table 10: show configuration smtp**

| Field Name | Field Description | Level of Output |
|---|---|---|
| **address** | SMTP server's IPv4 address | All levels |
| login | Configure a mail sender account to the server | All levels |
| password | Default sender password for user authentication | All levels |

## Sample Output

**show configuration smtp**

```
user@host> show configuration smtp
```

```
primary-server {
    address 218.102.48.213;
    login "dayone@example.com" {
        password "$ABC123"; ## SECRET-DATA
    }
}
```

# show groups junos-defaults

**Syntax**

```
show groups junos-defaults
```

**Release Information**

Command introduced before Junos OS Release 7.4.

**Description**

Display the full set of available preset statements from the Junos OS defaults group.

```
user@host# show groups junos-defaults
    groups {
        junos-defaults {
            applications {
                # File Transfer Protocol
                application junos-ftp {
                    application-protocol ftp;
                    protocol tcp;
                    destination-port 21;
                }
                # Trivial File Transfer Protocol
                application junos-tftp {
                    application-protocol tftp;
                    protocol udp;
                    destination-port 69;
                }
                # RPC port mapper on TCP
                application junos-rpc-portmap-tcp {
                    application-protocol rpc-portmap;
                    protocol tcp;
                    destination-port 111;
                }
                # RPC port mapper on UDP
            }
        }
    }
```

**Required Privilege Level**

view

RELATED DOCUMENTATION

- Using Junos OS Defaults Groups.

# show security log

**Syntax**

```
show security log {all| destination-address| destination-port| event-id| failure|interface-name| newer-than| older-than|
    process| protocol|report| severity| sort-by| source-address| source-port| success| user}
```

**Release Information**
Command introduced in Junos OS Release 11.2 .

**Description**
Display security event logs. This command continuously displays security events on the screen. To stop the display, press Ctrl+c.

**Options**
**all**—Display all audit event logs stored in the device memory.

**destination-address**—Display audit event logs with the specified destination address.

**destination-port**—Display audit event logs with the specified destination port.

**event-id**—Display audit event logs with the specified event identification number.

**failure**—Display failed audit event logs.

**interface-name**—Display audit event logs with the specified interface.

**newer-than**—Display audit event logs newer than the specified date and time.

**older-than**—Display audit event logs older than the specified date and time.

**process**—Display audit event logs with the specified process that generated the event.

**protocol**—Display audit event logs generated through the specified protocol.

**report**—Display on-box reports for system traffic logs.

**severity**—Display audit event logs generated with the specified severity.

**sort-by**—Display audit event logs generated sorted with the specified options.

**source-address**—Display audit event logs with the specified source address.

**source-port**—Display audit event logs with the specified source port.

**success**—Display successful audit event logs.

**username**—Display audit event logs generated for the specified user.

**Required Privilege Level**
view

RELATED DOCUMENTATION

*exclude (Security Log)*

*clear security log*

**List of Sample Output**
**show security log on page 684**

**Output Fields**
Table 11 on page 684 lists the output fields for the **show security log** command. Output fields are listed in the approximate order in which they appear.

**Table 11: show security log Output Fields**

| Field Name | Field Description |
|---|---|
| **Event time** | The timestamp of the events received.<br><br>Security logs were always timestamped using the UTC time zone by running **set system time-zone utc** and **set security log utc-timestamp** CLI commands. Now, time zone can be defined using the local time zone by running the **set system time-zone time-zone** command to specify the local time zone that the system should use when timestamping the security logs. |
| **Message** | Security events are listed. |

## Sample Output

**show security log**

```
user@host> show security log
```

```
Event time               Message
2010-10-22 13:28:37 CST  session created 1.1.1.2/1-->2.2.2.2/1308
 icmp 1.1.1.2/1-->2.2.2.2/1308
 None None 1 policy1 trustZone untrustZone 52 N/A(N/A) ge-0/0/1.0
2010-10-22 13:28:38 CST  session created 1.1.1.2/1-->2.2.2.2/1308 icmp
1.1.1.2/1-->2.2.2.2/1308 None None 1 policy1 trustZone untrustZone 54 N/A(N/A)
ge-0/0/1.0
```

```
...
```

```
2010-10-22 13:36:12 CST  session denied m icmp 1(8) policy1 trustZone untrustZone
 N/A(N/A) ge-0/0/1.0
2010-10-22 13:36:14 CST  session denied 1.1.1.2/2-->2.2.2.2/54812  icmp 1(8) policy1
 trustZone untrustZone N/A(N/A) ge-0/0/1.0

...
```

```
2010-10-27 15:50:11 CST  IP spoofing! source: 2.2.2.20, destination: 2.2.2.2,
protocol-id: 17, zone name: trustZone, interface name: ge-0/0/1.0, action: drop
2010-10-27 15:50:11 CST  IP spoofing! source: source: 2.2.2.20, destination:
2.2.2.2, protocol-id: 17, zone name: trustZone, interface name: ge-0/0/1.0, action:
 drop

...
```

```
2011-02-18 15:53:34 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/certification-authority/ca-profile1-ca1.cert
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/crl/ca-profile1.crl
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/system-key-pair/system-generated.priv
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/system-cert/system-generated.cert
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/key-pair/cert1.priv
2011-02-18 15:53:42 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/key-pair/test2.priv

...
```

```
2011-03-14 23:00:40 PDT  IDP_COMMIT_COMPLETED: IDP policy commit is complete.
                         IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;poli
cy[/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]
 ,failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT  ]
                         IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;poli
cy[/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]
```

```
 ,failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT  ]
                         IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;poli
cy[/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]
 ,failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT  ]

...
```

```
Event time               Message
2011-03-21 14:21:49 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
 9.9.9.1 source-address 6.6.6.1 '
2011-03-21 14:23:01 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
 9.9.9.1 source-address 6.6.6.1 .5 '
2011-03-21 14:23:05 CST  KMD_PM_SA_ESTABLISHED: Local gateway: 7.7.7.1, Remote
gateway: 8.8.8.1, Local ID: ipv4(any:0,[0..3]=6.6.6.1), Remote ID:
ipv4(any:0,[0..3]=9.9.9.1), Direction: inbound, SPI: 37a2a179, AUX-SPI: 0, Mode:
tunnel, Type: dynamic
2011-03-21 14:23:05 CST  KMD_PM_SA_ESTABLISHED: Local gateway: 7.7.7.1, Remote
gateway: 8.8.8.1, Local ID: ipv4(any:0,[0..3]=6.6.6.1), Remote ID:
ipv4(any:0,[0..3]=9.9.9.1), Direction: outbound, SPI: b2231c1f, AUX-SPI: 0, Mode:
 tunnel, Type: dynamic
2011-03-21 14:23:08 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
 9.9.9.1 source-address 6.6.6.1 '
2011-03-21 14:23:13 CST  UI_CMDLINE_READ_LINE: User 'root', command 'show security
 log '
```

# show security policies

**Syntax**

```
show security policies
<all-logical-systems-tenants>
<checksum>
<count>
<detail>
<from-zone zone-name>
<global>
<hit-count>
<information>
<logical-system logical-system-name>
<policy-name policy-name>
<root-logical-system>
<service-set>
<start>
<tenant tenant-name>
<to-zone zone-name>
<unknown-source-identity>
<zone-context>
```

**Release Information**

Command modified in Junos OS Release 9.2.
Support for IPv6 addresses is added in Junos OS Release 10.2.
Support for wildcard addresses is added in Junos OS Release 11.1.
Support for global policy and services offloading is added in Junos OS Release 11.4.
Support for source-identities and the **Description** output field is added in Junos OS Release 12.1.
Support for negated address added in Junos OS Release 12.1X45-D10.
The output fields for Policy Statistics expanded, and the output fields for the **global** and **policy-name** options are expanded to include from-zone and to-zone global match criteria in Junos OS Release 12.1X47-D10.
Support for the **initial-tcp-mss** and **reverse-tcp-mss** options is added in Junos OS Release 12.3X48-D20.
Output field and description for **source-end-user-profile** option is added in Junos OS Release 15.1x49-D70.
Output field and description for **dynamic-applications** option is added in Junos OS Release 15.1x49-D100.
Output field and description for **dynapp-redir-profile** option is added in Junos OS Release 18.2R1.
The **tenant** option is introduced in Junos OS Release 18.3R1.
The **<all-logical-systems-tenants>** option is introduced in Junos OS Release 18.4R1.
The **information** option is introduced in Junos OS Release 18.4R1.
The **checksum** option is introduced in Junos OS Release 18.4R1.

**Description**

Displays a summary of all security policies configured on the device. If a particular policy is specified, display information specific to that policy. The existing show commands for displaying the policies configured with multiple tenant support are enhanced. A security policy controls the traffic flow from one zone to another zone. The security policies allow you to deny, permit, reject (deny and send a TCP RST or ICMP port unreachable message to the source host), encrypt and decrypt, authenticate, prioritize, schedule, filter, and monitor the traffic attempting to cross from one security zone to another.

**Options**

- **all-logical-systems-tenants**—Displays all multitenancy systems.
- **checksum**—Displays the policy information checksum.
- **count**—Displays the number of policies to show. Range is 1 through 65,535.
- **detail**—(Optional) Displays a detailed view of all of the policies configured on the device.
- **from-zone**—Displays the policy information matching the given source zone.
- **global**—(Optional) Displays the policy information about global policies.
- **hit-count**—Displays the policies hit count.
- **information**—Displays the policy information.
- **logical-system**—Displays the logical system name.
- **policy-name**—(Optional) Displays the policy information matching the given policy name.
- **root-logical-system**—Displays root logical system as default.
- **service-set**—Displays the name of the service set.
- **start**—Displays the policies from a given position. Range is 1 through 65,535.
- **tenant**—Displays the name of the tenant system.
- **to-zone**—Displays the policy information matching the given destination zone.
- **unknown-source-identity**—Displays the unknown-source-identity of a policy.
- **zone-context**—Displays the count of policies in each context (from-zone and to-zone).

**Required Privilege Level**

view

## RELATED DOCUMENTATION

*Security Policies Overview*

*Understanding Security Policy Rules*

*Understanding Security Policy Elements*

*Unified Policies Configuration Overview*

**List of Sample Output**



**Output Fields**

Table 12 on page 689 lists the output fields for the **show security policies** command. Output fields are listed in the approximate order in which they appear.

**Table 12: show security policies Output Fields**

| Field Name | Field Description |
|---|---|
| **From zone** | Name of the source zone. |
| **To zone** | Name of the destination zone. |
| **Policy-name** | Name of the applicable policy. |
| **Description** | Description of the applicable policy. |
| **State** | Status of the policy:<br>• **enabled**: The policy can be used in the policy lookup process, which determines access rights for a packet and the action taken in regard to it.<br>• **disabled**: The policy cannot be used in the policy lookup process, and therefore it is not available for access control. |
| **Index** | Internal number associated with the policy. |
| **Sequence number** | Number of the policy within a given context. For example, three policies that are applicable in a from-zoneA-to-zoneB context might be ordered with sequence numbers 1, 2, 3. Also, in a from-zoneC-to-zoneD context, four policies might have sequence numbers 1, 2, 3, 4. |

**Table 12: show security policies Output Fields *(continued)***

| Field Name | Field Description |
|---|---|
| **Source addresses** | For standard display mode, the names of the source addresses for a policy. Address sets are resolved to their individual names.<br><br>For detail display mode, the names and corresponding IP addresses of the source addresses for a policy. Address sets are resolved to their individual address name-IP address pairs. |
| **Destination addresses** | Name of the destination address (or address set) as it was entered in the destination zone's address book. A packet's destination address must match this value for the policy to apply to it. |
| **source-end-user-profile** | Name of the device identity profile (referred to as **end-user-profile** in the CLI) that contains attributes, or characteristics of a device. Specification of the device identity profile in the **source-end-user-profile** field is part of the device identity feature. If a device matches the attributes specified in the profile and other security policy parameters, then the security policy's action is applied to traffic issuing from the device. |
| **Source addresses (excluded)** | Name of the source address excluded from the policy. |
| **Destination addresses (excluded)** | Name of the destination address excluded from the policy. |
| **Source identities** | One or more user roles specified for a policy. |
| **Applications** | Name of a preconfigured or custom application whose type the packet matches, as specified at configuration time.<br><br>• **IP protocol**: The Internet protocol used by the application—for example, TCP, UDP, ICMP.<br>• **ALG**: If an ALG is explicitly associated with the policy, the name of the ALG is displayed. If **application-protocol ignore** is configured, **ignore** is displayed. Otherwise, **0** is displayed.<br><br>However, even if this command shows **ALG: 0**, ALGs might be triggered for packets destined to well-known ports on which ALGs are listening, unless ALGs are explicitly disabled or when **application-protocol ignore** is not configured for custom applications.<br>• **Inactivity timeout**: Elapsed time without activity after which the application is terminated.<br>• **Source port range**: The low-high source port range for the session application. |
| **Dynamic Applications** | Application identification-based Layer 7 dynamic applications. |

**Table 12: show security policies Output Fields *(continued)***

| Field Name | Field Description |
|---|---|
| **Destination Address Translation** | Status of the destination address translation traffic:<br>• **drop translated**—Drop the packets with translated destination addresses.<br>• **drop untranslated**—Drop the packets without translated destination addresses. |
| **Application Firewall** | An application firewall includes the following:<br>• **Rule-set**—Name of the rule set.<br>• **Rule**—Name of the rule.<br>  ◦ **Dynamic applications**—Name of the applications.<br>  ◦ **Dynamic application groups**—Name of the application groups.<br>  ◦ **Action**—The action taken with respect to a packet that matches the application firewall rule set. Actions include the following:<br>  ▪ **permit**<br>  ▪ **deny**<br>• **Default rule**—The default rule applied when the identified application is not specified in any rules of the rule set. |
| **Action or Action-type** | • The action taken for a packet that matches the policy's tuples. Actions include the following:<br>  ◦ **permit**<br>  ◦ **feed**<br>  ◦ **firewall-authentication**<br>  ◦ **tunnel ipsec-vpn *vpn-name***<br>  ◦ **pair-policy *pair-policy-name***<br>  ◦ **source-nat pool *pool-name***<br>  ◦ **pool-set *pool-set-name***<br>  ◦ **interface**<br>  ◦ **destination-nat *name***<br>  ◦ **deny**<br>  ◦ **reject**<br>  ◦ **services-offload** |
| **Session log** | Session log entry that indicates whether the **at-create** and **at-close** flags were set at configuration time to log session information. |
| **Scheduler name** | Name of a preconfigured scheduler whose schedule determines when the policy is active and can be used as a possible match for traffic. |

**Table 12: show security policies Output Fields *(continued)***

| Field Name | Field Description |
|---|---|
| **Policy statistics** | • **Input bytes**—The total number of bytes presented for processing by the device.<br>  ◦ **Initial direction**—The number of bytes presented for processing by the device from the initial direction.<br>  ◦ **Reply direction**—The number of bytes presented for processing by the device from the reply direction.<br>• **Output bytes**—The total number of bytes actually processed by the device.<br>  ◦ **Initial direction**—The number of bytes from the initial direction actually processed by the device.<br>  ◦ **Reply direction**—The number of bytes from the reply direction actually processed by the device.<br>• **Input packets**—The total number of packets presented for processing by the device.<br>  ◦ **Initial direction**—The number of packets presented for processing by the device from the initial direction.<br>  ◦ **Reply direction**—The number of packets presented for processing by the device from the reply direction.<br>• **Output packets**—The total number of packets actually processed by the device.<br>  ◦ **Initial direction**—The number of packets actually processed by the device from the initial direction.<br>  ◦ **Reply direction**—The number of packets actually processed by the device from the reply direction.<br>• **Session rate**—The total number of active and deleted sessions.<br>• **Active sessions**—The number of sessions currently present because of access control lookups that used this policy.<br>• **Session deletions**—The number of sessions deleted since system startup.<br>• **Policy lookups**—The number of times the policy was accessed to check for a match. |
| **dynapp-redir-profile** | Displays unified policy redirect profile. See *profile(dynamic-application)*. |
| **Per policy TCP Options** | Configured syn and sequence checks, and the configured TCP MSS value for the initial direction, the reverse direction or, both. |

## Sample Output

**show security policies**

user@host> **show security policies**

```
From zone: trust, To zone: untrust
Policy: p1, State: enabled, Index: 4, Sequence number: 1
  Source addresses:
  sa-1-ipv4: 198.51.100.11/24
  sa-2-ipv6: 2001:db8:a0b:12f0::1/32
  sa-3-ipv6: 2001:db8:a0b:12f0::22/32
  sa-4-wc:   203.0.113.1/255.255.0.255
  Destination addresses:
  da-1-ipv4: 2.2.2.2/24
  da-2-ipv6: 2001:db8:a0b:12f0::8/32
  da-3-ipv6: 2001:db8:a0b:12f0::9/32
  da-4-wc:   192.168.22.11/255.255.0.255
  Source identities: role1, role2, role4
  Applications: any
  Action: permit, application services, log, scheduled
  Application firewall : my_ruleset1
Policy: p2, State: enabled, Index: 5, Sequence number: 2
  Source addresses:
  sa-1-ipv4:  198.51.100.11/24
  sa-2-ipv6:  2001:db8:a0b:12f0::1/32
  sa-3-ipv6:  2001:db8:a0b:12f0::22/32
  Destination addresses:
  da-1-ipv4:  2.2.2.2/24
  da-2-ipv6:  2001:db8:a0b:12f0::1/32
  da-3-ipv6:  2001:db8:a0b:12f0::9/32
  Source identities: role1, role4
  Applications: any
  Action: deny, scheduled
```

**show security policies (Dynamic Applications)**

user@host>**show security policies**

```
Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
  Source addresses: any
  Destination addresses: any
```

```
    Applications: any
    Dynamic Applications: junos:YAHOO
    Action: deny, log
  Policy: p2, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 2
    Source addresses: any
    Destination addresses: any
    Applications: any
    Dynamic Applications: junos:web, junos:web:social-networking:facebook,
    junos:TFTP, junos:QQ
    Action: permit, log
  Policy: p3, State: enabled, Index: 6, Scope Policy: 0, Sequence number: 3
    Source addresses: any
    Destination addresses: any
    Applications: any
    Dynamic Applications: junos:HTTP, junos:SSL
    Action: permit, application services, log
```

The following example displays the output with unified policies configured.

`user@host>` **show security policies**

```
Default policy: deny-all
Pre ID default policy: permit-all
From zone: trust, To zone: untrust
  Policy: p2, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Applications: junos-defaults
    Dynamic Applications: junos:GMAIL, junos:FACEBOOK-CHAT
    dynapp-redir-profile: profile1
```

**show security policies policy-name p2**

`user@host>` **show security policies policy-name p2**

```
  Policy: p2, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    From zones: any
    To zones: any
    Source vrf group: any
    Destination vrf group: any
    Source addresses: any
    Destination addresses: any
```

```
    Applications: any
    Dynamic Applications: any
    Action: permit, application services, feed
```

**show security policies policy-name detail**

user@host> **show security policies policy-name p2 detail**

```
Policy: p2, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured, global
  Sequence number: 1
  From zones:
    any
  To zones:
    any
  Source vrf group:
    any
  Destination vrf group:
    any
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination ports: [0-0]
  Dynamic Application:
    any: 0
  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
  Intrusion Detection and Prevention: disabled
  Unified Access Control: disabled
  Feed: add-source-ip-to-feed
```

user@host> **show security policies policy-name p1 detail**

```
  Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
  Description: The policy p1 is for the sales team
  Sequence number: 1
```

```
 From zone: trust, To zone: untrust
 Source addresses:
   sa-1-ipv4:  198.51.100.11/24
   sa-2-ipv6:  2001:db8:a0b:12f0::1/32
   sa-3-ipv6:  2001:db8:a0b:12f0::9/32
   sa-4-wc:    203.0.113.1/255.255.0.255
 Destination addresses:
   da-1-ipv4: 192.0.2.0/24
   da-2-ipv6: 2001:db8:a0b:12f0::1/32
   da-3-ipv6: 2001:db8:a0b:12f0::9/32
   da-4-wc:   192.168.22.11/255.255.0.255
Source identities:
 role1
 role2
 role4
 Application: any
   IP protocol: 0, ALG: 0, Inactivity timeout: 0
     Source port range: [0-0]
     Destination port range: [0-0]
 Destination Address Translation: drop translated
 Application firewall :
 Rule-set: my_ruleset1
   Rule: rule1
     Dynamic Applications: junos:FACEBOOK-ACCESS, junos:YMSG
     Dynamic Application groups: junos:web, junos:chat
     Action: deny
   Default rule: permit
 Session log: at-create, at-close
 Scheduler name: sch20
 Per policy TCP Options: SYN check: No, SEQ check: No
 Policy statistics:
   Input  bytes       :               18144                 545 bps
     Initial direction:                9072                272 bps
     Reply direction  :                9072                 272 bps
   Output bytes       :               18144                 545 bps
     Initial direction:                9072                 272 bps
     Reply direction  :                9072                 272 bps
   Input  packets     :                 216                   6 pps
     Initial direction:                 108                   3 bps
     Reply direction  :                 108                   3 bps
   Output packets     :                 216                   6 pps
     Initial direction:                 108                   3 bps
     Reply direction  :                 108                   3 bps
   Session rate       :                 108                   3 sps
```

```
    Active sessions    :                  93
    Session deletions  :                  15
    Policy lookups     :                 108
```

**show security policies (Services-Offload)**

user@host> **show security policies**

```
  Policy: p1, action-type: reject, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: trust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  dynapp-redir-profile: profile1(1)
  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
```

**show security policies (Device Identity)**

user@host> **show security policies**

```
From zone: trust, To zone: untrust
      Policy: dev-id-marketing, State: enabled, Index: 5, Scope Policy: 0, Sequence
 number: 1
         Source addresses: any
         Destination addresses: any
         source-end-user-profile: marketing-profile
         Applications: any
         Action: permit
```

**show security policies detail**

user@host> **show security policies detail**

```
Default policy: deny-all
Policy: p1, action-type: permit, services-offload:enabled , State: enabled, Index:
 4, Scope Policy: 0
  Policy Type: Configured
  Description: The policy p1 is for the sales team
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    any-ipv4(global):  0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global):  0.0.0.0/0
    any-ipv6(global): ::/0
 Source identities:
  role1
  role2
  role4
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No
  Policy statistics:
    Input  bytes       :               18144                  545 bps
      Initial direction:                9072                272 bps
      Reply direction  :                9072                 272 bps
    Output bytes       :               18144                  545 bps
      Initial direction:                9072                 272 bps
      Reply direction  :                9072                 272 bps
    Input  packets     :                 216                    6 pps
      Initial direction:                 108                    3 bps
      Reply direction  :                 108                    3 bps
    Output packets     :                 216                    6 pps
      Initial direction:                 108                    3 bps
      Reply direction  :                 108                    3 bps
    Session rate       :                 108                    3 sps
    Active sessions    :                  93
    Session deletions  :                  15
    Policy lookups     :                 108
Policy: p2, action-type: permit, services-offload:enabled , State: enabled, Index:
 5, Scope Policy: 0
  Policy Type: Configured
  Description: The policy p2 is for the sales team
```

```
  Sequence number: 1
  From zone: untrust, To zone: trust
  Source addresses:
    any-ipv4(global):  0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global):  0.0.0.0/0
    any-ipv6(global): ::/0
 Source identities:
  role1
  role2
  role4
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No
```

The following example displays the output with unified policies configured.

user@host> **show security policies detail**

```
Default policy: deny-all
Pre ID default policy: permit-all
Policy: p2, action-type: reject, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: junos-defaults
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [443-443]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [5432-5432]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
```

```
      Destination port range: [80-80]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [3128-3128]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [8000-8000]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [8080-8080]
    IP protocol: 17, ALG: 0, Inactivity timeout: 60
      Source port range: [0-0]
      Destination port range: [1-65535]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [443-443]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [5432-5432]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [80-80]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [3128-3128]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [8000-8000]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [8080-8080]
    IP protocol: 17, ALG: 0, Inactivity timeout: 60
      Source port range: [0-0]
      Destination port range: [1-65535]
  Dynamic Application:
    junos:FACEBOOK-CHAT: 10704
    junos:GMAIL: 51
  dynapp-redir-profile: profile1(1)
  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
```

**show security policies detail (TCP Options)**

user@host> **show security policies policy-name p2 detail**

```
node0:
--------------------------------------------------------------------------
Policy:p2, action-type:permit, State: enabled,Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: trust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: junos-defaults
    IP protocol: tcp, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
 Destination port range: [80-80]
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
  Dynamic-application: junos:HTTP
```

**show security policies policy-name (Negated Address)**

`user@host>` **show security policies policy-name p1**

```
node0:
--------------------------------------------------------------------------
From zone: trust, To zone: untrust
  Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses(excluded): as1
    Destination addresses(excluded): as2
    Applications: any
    Action: permit
```

**show security policies policy-name detail (Negated Address)**

`user@host>` **show security policies policy-name p1 detail**

```
node0:
--------------------------------------------------------------------------
Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses(excluded):
```

```
    ad1(ad): 255.255.255.255/32
    ad2(ad):  198.51.100.1/24
    ad3(ad):  198.51.100.6  ~ 198.51.100.56
    ad4(ad):  192.0.2.8/24
    ad5(ad):  198.51.100.99 ~ 198.51.100.199
    ad6(ad):  203.0.113.9/24
    ad7(ad):  203.0.113.23/24
  Destination addresses(excluded):
    ad13(ad2): 198.51.100.76/24
    ad12(ad2): 198.51.100.88/24
    ad11(ad2): 192.0.2.23 ~ 192.0.2.66
    ad10(ad2): 192.0.2.93
    ad9(ad2):  203.0.113.76 ~ 203.0.113.106
    ad8(ad2):  203.0.113.199
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No
```

**show security policies global**

`user@host>` **show security policies global policy-name Pa**

```
node0:
--------------------------------------------------------------------------
  Global policies:
  Policy: Pa, State: enabled, Index: 6, Scope Policy: 0, Sequence number: 1
    From zones: any
    To zones: any
    Source addresses: H0
    Destination addresses: H1
    Applications: junos-http
    Action: permit
```

**show security policies detail tenant**

`user@host>` **show security policies detail tenant TN1**

```
Default policy: deny-all
Pre ID default policy: permit-all
```

```
Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
Policy Type: Configured
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses: any
Destination addresses: any
Application: junos-ping
IP protocol: 1, ALG: 0, Inactivity timeout: 60
ICMP Information: type=255, code=0
Application: junos-telnet
IP protocol: tcp, ALG: 0, Inactivity timeout: 1800
Source port range: [0-0]
Destination port range: [23-23]
Application: app_udp
IP protocol: udp, ALG: 0, Inactivity timeout: 1800
Source port range: [0-0]
Destination port range: [5000-5000]
Application: junos-icmp6-all
IP protocol: 58, ALG: 0, Inactivity timeout: 60
ICMP Information: type=255, code=0
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
Session log: at-create, at-close
Policy statistics:
Input  bytes     :                   0                   0 bps
Initial direction:                   0                   0 bps
Reply direction  :                   0                   0 bps
Output bytes     :                   0                   0 bps
Initial direction:                   0                   0 bps
Reply direction  :                   0                   0 bps
Input  packets   :                   0                   0 pps
Initial direction:                   0                   0 bps
Reply direction  :                   0                   0 bps
Output packets   :                   0                   0 pps
Initial direction:                   0                   0 bps
Reply direction  :                   0                   0 bps
Session rate     :                   0                   0 sps
Active sessions  :                   0
Session deletions:                   0
Policy lookups   :                   0
```

# show security utm anti-spam statistics

**Syntax**

```
show security utm anti-spam statistics
<root-logical-system>
<logical-system (logical-system-name | all)>
<all-logical-systems-tenants>
<tenant (tenant-name | all)>
```

**Release Information**

Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4.
Support for UTM in logical system added in Junos OS Release 18.3R1.
Support for UTM in tenant system added in Junos OS Release 19.2R1.

**Description**

Displays antispam statistics for connections including total e-mail scanned, tagged, and dropped connections.

Statistics from both the nodes (with full chassis cluster support for UTM) are displayed.

Starting in Junos OS Release 18.2R1, on SRX5000 Series devices, the options **pic** and **fpc** to view the physical interface cards (PICs) and Flexible PIC Concentrator (FPC) statistics are not supported.

Starting in Junos OS Release 18.3R1, you can view the antispam statistics for the master logical system or for a specific user logical system or for all the user logical systems.

Starting in Junos OS Release 19.2R1, you can view the antispam statistics for the tenant system.

**Options**

**none**—Displays antispam statistics for the master logical system.

***root-logical-system***—(Optional) Displays antispam statistics for the master logical system.

**logical-system *logical-system-name***—(Optional) Displays antispam statistics for a specific user logical system.

**all**—(Optional) Displays antispam statistics for all the user logical systems.

**<all-logical-systems-tenants>**—(Optional) Displays antispam statistics for all the logical systems and tenant systems.

**tenant *tenant-name***—(Optional) Displays antispam statistics for a specific tenant system.

**all**—(Optional) Displays antispam statistics for all the tenant systems.

**Required Privilege Level**

view

RELATED DOCUMENTATION

clear security utm anti-spam statistics | 653

show security utm anti-spam status | 709

**List of Sample Output**



## Sample Output

**show security utm anti-spam statistics**

```
user@host> show security utm anti-spam statistics
```

```
Total connections:     0
Denied connections:    0
Total greetings:       0
Denied greetings:      0
Total e-mail scanned:  0
White list hit:        0
Black list hit:        0
Spam total:            0
Spam tagged:           0
Spam dropped:          0
DNS errors:            0
Timeout errors:        0
Return errors:         0
Invalid parameter errors: 0
```

**show security utm anti-spam statistics root-logical-system**

```
user@host> show security utm anti-spam statistics root-logical-system
```

```
 UTM Anti Spam statistics:

Total connections:     0
```

```
Denied connections:    0
Total greetings:       0
Denied greetings:      0
Total e-mail scanned:  0
White list hit:        0
Black list hit:        0
Spam total:            0
Spam tagged:           0
Spam dropped:          0
DNS errors:            0
Timeout errors:        0
Return errors:         0
Invalid parameter errors: 0
```

**show security utm anti-spam statistics logical-system LSYS1**

user@host> **show security utm anti-spam statistics logical-system LSYS1**

```
 UTM Anti Spam statistics:

Total connections:     0
Denied connections:    0
Total greetings:       0
Denied greetings:      0
Total e-mail scanned:  0
White list hit:        0
Black list hit:        0
Spam total:            0
Spam tagged:           0
Spam dropped:          0
DNS errors:            0
Timeout errors:        0
Return errors:         0
Invalid parameter errors: 0
```

**show security utm anti-spam statistics logical-system all**

user@host> **show security utm anti-spam statistics logical-system all**

```
 UTM Anti Spam statistics:

Total connections:     0
Denied connections:    0
```

```
Total greetings:       0
Denied greetings:      0
Total e-mail scanned:  0
White list hit:        0
Black list hit:        0
Spam total:            0
Spam tagged:           0
Spam dropped:          0
DNS errors:            0
Timeout errors:        0
Return errors:         0
Invalid parameter errors: 0
```

**show security utm anti-spam statistics tenant TSYS1**

```
user@host> show security utm anti-spam statistics tenant TSYS1
```

```
 UTM Anti Spam statistics:

Total connections:     0
Denied connections:    0
Total greetings:       0
Denied greetings:      0
Total e-mail scanned:  0
White list hit:        0
Black list hit:        0
Spam total:            0
Spam tagged:           0
Spam dropped:          0
DNS errors:            0
Timeout errors:        0
Return errors:         0
Invalid parameter errors: 0
```

**show security utm anti-spam statistics tenant all**

```
user@host> show security utm anti-spam statistics tenant all
```

```
 UTM Anti Spam statistics:

Total connections:     0
Denied connections:    0
Total greetings:       0
```

```
Denied greetings:      0
Total e-mail scanned:  0
White list hit:        0
Black list hit:        0
Spam total:            0
Spam tagged:           0
Spam dropped:          0
DNS errors:            0
Timeout errors:        0
Return errors:         0
Invalid parameter errors: 0
```

**show security utm anti-spam statistics all-logical-systems-tenants**

user@host> **show security utm anti-spam statistics all-logical-systems-tenants**

```
 UTM Anti Spam statistics:

Total connections:     0
Denied connections:    0
Total greetings:       0
Denied greetings:      0
Total e-mail scanned:  0
White list hit:        0
Black list hit:        0
Spam total:            0
Spam tagged:           0
Spam dropped:          0
DNS errors:            0
Timeout errors:        0
Return errors:         0
Invalid parameter errors: 0
```

# show security utm anti-spam status

**Syntax**

```
show security utm anti-spam status
```

**Release Information**

Command introduced in Junos OS Release 9.5 .
Support for UTM in chassis cluster added in Junos OS Release 11.4 .

**Description**

Display antispam status for connections including allowlist and blocklist server information. Status of both the nodes (with full chassis cluster support for UTM) is displayed.

**Required Privilege Level**

view

RELATED DOCUMENTATION

clear security utm anti-spam statistics | 653
show security utm anti-spam statistics | 704

**Output Fields**

show security utm anti-spam status

Output fields are listed in the approximate order in which they appear.

## show security utm anti-spam status

`user@host>` **show security utm anti-spam status**

```
SBL Whitelist Server:
SBL Blacklist Server:
    msgsecurity.example.net
```

```
DNS Server:
    Primary  :     1.2.3.4, Src Interface: ge-0/0/0
    Secondary:     0.0.0.0, Src Interface: ge-0/0/1
```

```
    Ternary  :     0.0.0.0, Src Interface: fe-0/0/2
```

# show security utm anti-virus statistics

**Syntax**

```
show security utm anti-virus statistics
<root-logical-system>
<logical-system (logical-system-name | all)>
<tenant (tenant-name | all)>
<all-logical-systems-tenants>
<fpc <fpc-slot fpc-slot pic-slot pic-slot>>
```

**Release Information**

Command introduced in Junos OS Release 9.5.
Support for Sophos Antivirus added in Junos OS Release 11.1.
Support for UTM in chassis cluster added in Junos OS Release 11.4.
Support for Flexible PIC Concentrator (FPC) and PIC status added in Junos OS Release 12.1X46-D10.
Starting in Junos OS Release 18.2R1, on SRX5000 Series devices, the options **pic** and **fpc** are deprecated—rather than immediately removed—to provide backward compatibility.
Support for UTM in logical system added in Junos OS Release 18.3R1.
Support for UTM in tenant system added in Junos OS Release 19.2R1.

**Description**

Displays antivirus statistics for connections including clean and infected files, scan engine status, and aggregated statistics from all FPCs and PICs. Statistics from both the nodes (with full chassis cluster support for UTM) are displayed.

Starting in Junos OS Release 18.3R1, you can view the antivirus statistics for the master logical system or for a specific user logical system or for all the user logical systems.

Starting in Junos OS Release 19.2R1, you can view the antivirus statistics for a specific tenant system or for all the tenant systems.

**Options**

**none**—Displays antivirus statistics for the master logical system.

***root-logical-system***—(Optional) Displays antivirus statistics for the master logical system.

**logical-system *logical-system-name***—(Optional) Displays antivirus statistics for a specific user logical system.

**all**—(Optional) Displays antivirus statistics for all the user logical systems.

**all-logical-systems-tenants**—(Optional) Displays antivirus statistics for all the logical systems and tenant systems.

**tenant *tenant-name***—(Optional) Displays antivirus statistics for a specific tenant system.

**all**—(Optional) Displays antispam statistics for all the tenant systems.

**Required Privilege Level**
view

RELATED DOCUMENTATION

- clear security utm antivirus statistics | **656**
- show security utm anti-virus status | **718**
- The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards.request security utm anti-virus juniper-express-engine | **666**
- request security utm anti-virus kaspersky-lab-engine | **668**

**List of Sample Output**



## Sample Output

**show security utm anti-virus statistics**

```
user@host> show security utm anti-virus statistics
```

```
UTM Anti Virus statistics:
MIME-whitelist passed:               0
URL-whitelist passed:                0
Scan Request:

 Total           Clean         Threat-found    Fallback
     0               0              0               0

Fallback:
                             Log-and-Permit    Block             Permit
```

```
Engine not ready:                0                0                0
Out of resources:                0                0                0
Timeout:                         0                0                0
Maximum content size:            0                0                0
Too many requests:               0                0                0
Others:                          0                0                0
```

**show security utm anti-virus statistics fpc**

```
user@host> show security utm anti-virus statistics fpc
```

```
fpc-slot 5 pic-slot 0
UTM Anti Virus statistics:
MIME-whitelist passed:               0
URL-whitelist passed:                0
Scan Request:

 Total           Clean         Threat-found    Fallback
      0               0              0               0

Fallback:
                             Log-and-Permit    Block             Permit
Engine not ready:                0                0                0
Out of resources:                0                0                0
Timeout:                         0                0                0
Maximum content size:            0                0                0
Too many requests:               0                0                0
Others:                          0                0                0
```

**show security utm anti-virus statistics fpc fpc-slot 5 pic-slot 0**

```
user@host> show security utm anti-virus statistics fpc fpc-slot 5 pic-slot 0
```

```
UTM Anti Virus statistics:
MIME-whitelist passed:               0
URL-whitelist passed:                0
Scan Request:

 Total           Clean         Threat-found    Fallback
      0               0              0               0

Fallback:
```

```
                            Log-and-Permit    Block             Permit
Engine not ready:                0                0                 0
Out of resources:                0                0                 0
Timeout:                         0                0                 0
Maximum content size:            0                0                 0
Too many requests:               0                0                 0
Others:                          0                0                 0
```

**show security utm anti-virus statistics root-logical-system**

`user@host>` **show security utm anti-virus statistics root-logical-system**

```
UTM Anti Virus statistics:
MIME-whitelist passed:               0
URL-whitelist passed:                0
Session abort:                       0
Scan Request:

 Total           Clean         Threat-found    Fallback
      0               0              0               0
Fallback:

                          Log-and-permit         Block
 Engine not ready:                0                      0
 Out of resources:                0                      0
 Timeout:                         0                      0
 Maximum content size:            0                      0
 Too many requests:               0                      0
 Others:                          0                      0
```

**show security utm anti-virus statistics logical-system LSYS1**

`user@host>` **show security utm anti-virus statistics logical-system LSYS1**

```
UTM Anti Virus statistics:
MIME-whitelist passed:               0
URL-whitelist passed:                0
Session abort:                       0
Scan Request:

 Total           Clean         Threat-found    Fallback
      0               0              0               0
Fallback:
```

```
                        Log-and-permit         Block
 Engine not ready:               0                     0
 Out of resources:               0                     0
 Timeout:                        0                     0
 Maximum content size:           0                     0
 Too many requests:              0                     0
 Others:                         0                     0
```

**show security utm anti-virus statistics logical-system all**

```
user@host> show security utm anti-virus statistics logical-system all
```

```
UTM Anti Virus statistics:
MIME-whitelist passed:               0
URL-whitelist passed:                0
Session abort:                       0
Scan Request:

 Total           Clean         Threat-found    Fallback
      0               0              0               0
Fallback:

                        Log-and-permit         Block
 Engine not ready:               0                     0
 Out of resources:               0                     0
 Timeout:                        0                     0
 Maximum content size:           0                     0
 Too many requests:              0                     0
 Others:                         0                     0
```

**show security utm anti-virus statistics tenant TSYS1**

```
user@host> show security utm anti-virus statistics tenant TSYS1
```

```
UTM Anti Virus statistics:
MIME-whitelist passed:               0
URL-whitelist passed:                0
Session abort:                       0
Scan Request:

 Total           Clean         Threat-found    Fallback
      0               0              0               0
```

```
Fallback:

                         Log-and-permit         Block
 Engine not ready:               0                      0
 Out of resources:               0                      0
 Timeout:                        0                      0
 Maximum content size:           0                      0
 Too many requests:              0                      0
 Decompress error:               0                      0
 Others:                         0                      0
```

**show security utm anti-virus statistics tenant all**

user@host> **show security utm anti-virus statistics tenant all**

```
UTM Anti Virus statistics:
MIME-whitelist passed:               0
URL-whitelist passed:                0
Session abort:                       0
Scan Request:

 Total           Clean         Threat-found    Fallback
      0               0              0               0
Fallback:

                         Log-and-permit         Block
 Engine not ready:               0                      0
 Out of resources:               0                      0
 Timeout:                        0                      0
 Maximum content size:           0                      0
 Too many requests:              0                      0
 Decompress error:               0                      0
 Others:                         0                      0
```

**show security utm anti-virus statistics all-logical-systems-tenants**

user@host> **show security utm anti-virus statistics all-logical-systems-tenants**

```
UTM Anti Virus statistics:
MIME-whitelist passed:               0
URL-whitelist passed:                0
Session abort:                       0
Scan Request:
```

```
 Total           Clean         Threat-found    Fallback
      0               0              0               0
Fallback:

                          Log-and-permit         Block
 Engine not ready:                 0                    0
 Out of resources:                 0                    0
 Timeout:                          0                    0
 Maximum content size:             0                    0
 Too many requests:                0                    0
 Decompress error:                 0                    0
 Others:                           0                    0
```

# show security utm anti-virus status

**Syntax**

```
show security utm anti-virus status <fpc <fpc-slot fpc-slot pic-slot pic-slot>>
```

**Release Information**

Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4. Support for Flexible PIC Concentrator (FPC) and PIC status added in Junos OS Release 12.1X46-D10.
Starting in Junos OS Release 18.2R1, on SRX5000 Series devices, the options **pic** and **fpc** to display PIC and FPC statistics are not supported.

**Description**

Display antivirus status for connections including clean and infected files, scan engine status, and aggregated status from all FPCs and PICs. Status of both the nodes (with full chassis cluster support for UTM) is displayed.

**Required Privilege Level**

view

RELATED DOCUMENTATION

clear security utm antivirus statistics | 656
show security utm anti-virus statistics | 711

**List of Sample Output**



**Output Fields**

show security utm anti-virus status

Output fields are listed in the approximate order in which they appear.

## Sample Output

**show security utm anti-virus status**

user@host> **show security utm anti-virus status**

```
UTM anti-virus status:

   Anti-virus key expire date: 2021-05-10 18:23:43
   Update server: https://update.juniper-updates.net/AVIRA/VSRX
          Interval: 1440 minutes
          Pattern update status: next update in 1228 minutes
          Last result: Downloading file failed
   Forwarding-mode: hold
   Onbox AV load flavor: running Light, configure Light
   Scan engine type: avira-engine
   Scan engine information: 8.3.60.28
   Anti-virus signature version: 8.16.46.24
```

**show security utm anti-virus status fpc**

user@host> **show security utm anti-virus status fpc**

```
fpc-slot 5 pic-slot 0
UTM anti-virus status:

   Anti-virus key expire date: 2021-06-07 00:00:00
   Update server: https://update.juniper-updates.net/SAV/
          Interval: 1440 minutes
          Pattern update status: next update in 467 minutes
          Last result: already have latest database
   Forwarding-mode: continuous delivery, inline-tap
   Scan engine type: sophos-engine
   Scan engine information: last action result: No error
   Anti-virus signature version: 1.13 (1.02)
```

**show security utm anti-virus status fpc fpc-slot 5 pic-slot 0**

user@host> **show security utm anti-virus status fpc fpc-slot 5 pic-slot 0**

```
UTM anti-virus status:
```

```
   Anti-virus key expire date: license not installed
   Update server: http://update.juniper-updates.net/SAV/
          Interval: 1440 minutes
          Pattern update status: update disabled due to no license
          Last result: already have latest database
   Anti-virus signature version: 000000_00
   Forwarding-mode: continuous delivery, inline-tap
   Scan engine type: sophos-engine
   Scan engine information: last action result: No error
```

**show security utm anti-virus status**

Refer the sample output for Avira scan engine. Support for Avira is added in 18.4R1 release.

```
UTM anti-virus status:
   Anti-virus key expire date: 2021-03-12 08:00:00
   Update server: https://update.juniper-updates.net/AVIRA/VSRX
          Interval: 1440 minutes
          Pattern update status: av updater is running
          Last result: downloading signature files
   Forwarding-mode: hold
   Scan engine type: sophos-engine
   Scan engine information: last action result: No error
   Anti-virus signature version: 1.13 (1.02)
```

# show security utm content-filtering statistics

**Syntax**

```
show security utm content-filtering statistics
<root-logical-system>
<logical-system (logical-system-name | all)>
<all-logical-systems-tenants>
<tenant (tenant-name | all)>
```

**Release Information**

Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4.
Starting in Junos OS Release 18.2R1, on SRX5000 Series devices, the options **pic** and **fpc** to display physical interface cards (PICs) and Flexible PIC Concentrator (FPC) statistics are not supported.
Support for UTM in logical system added in Junos OS Release 18.3R1.
Support for UTM in tenant system added in Junos OS Release 19.2R1.

**Description**

Displays the content filtering statistics for connections including lists of blocked files and the reasons for blocking. Statistics from both the nodes (with full chassis cluster support for UTM) are displayed.

Starting in Junos OS Release 18.3R1, you can view the content filtering statistics for the master logical system or for a specific user logical system or for all the user logical systems.

Starting in Junos OS Release 19.2R1, you can view the content filtering statistics for a specific tenant system or for all the tenant systems.

**Options**

**none**—Displays content filtering statistics for the master logical system.

***root-logical-system***—(Optional) Displays content filtering statistics for the master logical system.

**logical-system *logical-system-name***—(Optional) Displays content filtering statistics for a specific user logical system.

**all**—(Optional) Displays content filtering statistics for all the user logical systems.

**all-logical-systems-tenants**—(Optional) Displays content filtering statistics for all logical systems and tenant systems.

**tenant *tenant-name***—(Optional) Displays content filtering statistics for a specific tenant system.

**all**—(Optional) Displays content filtering statistics for all the tenant systems.

**Required Privilege Level**

view

RELATED DOCUMENTATION

clear security utm content-filtering statistics | 659

**List of Sample Output**



## Sample Output

**show security utm content-filtering statistics**

```
user@host> show security utm content-filtering statistics
```

```
Content-filtering-statistic:         Blocked
     Base on command list:                    0
     Base on mime list:                       0
     Base on extension list:                  0
     ActiveX plugin:                          0
     Java applet:                             0
     EXE files:                               0
     ZIP files:                               0
     HTTP cookie:                             0
```

**show security utm content-filtering statistics root-logical-system**

```
user@host> show security utm content-filtering statistics root-logical-system
```

```
 Content-filtering-statistic:         Blocked
     Base on command list:                    0
     Base on mime list:                       0
     Base on extension list:                  0
     ActiveX plugin:                          0
     Java applet:                             0
```

```
    EXE files:                              0
    ZIP files:                              0
    HTTP cookie:                            0
```

**show security utm content-filtering statistics logical-system LSYS1**

```
user@host> show security utm content-filtering statistics logical-system LSYS1
```

```
Content-filtering-statistic:         Blocked
    Base on command list:                   0
    Base on mime list:                      0
    Base on extension list:                 0
    ActiveX plugin:                         0
    Java applet:                            0
    EXE files:                              0
    ZIP files:                              0
    HTTP cookie:                            0
```

**show security utm content-filtering statistics logical-system all**

```
user@host> show security utm content-filtering statistics logical-system all
```

```
Content-filtering-statistic:         Blocked
    Base on command list:                   0
    Base on mime list:                      0
    Base on extension list:                 0
    ActiveX plugin:                         0
    Java applet:                            0
    EXE files:                              0
    ZIP files:                              0
    HTTP cookie:                            0
```

**show security utm content-filtering statistics tenant TSYS1**

```
user@host> show security utm content-filtering statistics tenant TSYS1
```

```
Content-filtering-statistic:         Blocked
    Base on command list:                   0
    Base on mime list:                      0
    Base on extension list:                 0
    ActiveX plugin:                         0
    Java applet:                            0
```

```
    EXE files:                              0
    ZIP files:                              0
    HTTP cookie:                            0
```

**show security utm content-filtering statistics tenant all**

```
user@host> show security utm content-filtering statistics tenant all
```

```
Content-filtering-statistic:         Blocked
    Base on command list:                   0
    Base on mime list:                      0
    Base on extension list:                 0
    ActiveX plugin:                         0
    Java applet:                            0
    EXE files:                              0
    ZIP files:                              0
    HTTP cookie:                            0
```

**show security utm content-filtering statistics all-logical-systems-tenants**

```
user@host> show security utm content-filtering statistics all-logical-systems-tenants
```

```
Content-filtering-statistic:         Blocked
    Base on command list:                   0
    Base on mime list:                      0
    Base on extension list:                 0
    ActiveX plugin:                         0
    Java applet:                            0
    EXE files:                              0
    ZIP files:                              0
    HTTP cookie:                            0
```

# show security utm session

**Syntax**

```
show security utm session
```

**Release Information**

Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4.
Starting in Junos OS Release 18.2R1, on SRX5000 Series devices, the options **pic** and **fpc** to display physical interface cards (PICs) and Flexible PIC Concentrator (FPC) statistics are not supported.

**Description**

Display general UTM session information including all allocated sessions and active sessions. Also, display information from both nodes in a chassis cluster.

**Required Privilege Level**

view

RELATED DOCUMENTATION

clear security utm session | 662
show security utm status | 726

**Output Fields**

show security utm session

When you enter this command, you are provided feedback on the status of your request.

## show security utm session

```
user@host> show security utm session
```

```
Maximum sessions:           4000
 Total allocated sessions:         0
 Total freed sessions:             0
 Active sessions:                  0
```

# show security utm status

**Syntax**

```
show security utm status
```

**Release Information**

Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4.

**Description**

Display whether the UTM service is running or not and status of both the nodes (with full chassis cluster support for UTM).

**Required Privilege Level**

view

RELATED DOCUMENTATION

clear security utm session | 662
show security utm session | 725

**Output Fields**

show security utm status

When you enter this command, you are provided feedback on the status of your request.

## show security utm status

```
user@host> show security utm status
```

```
UTM service status: Running
```

# show security utm web-filtering category base-filter

**Syntax**

```
show security utm web-filtering category base-filter
```

**Release Information**

Command introduced in Junos OS Release 17.4.

**Description**

Show the list of predefined base filters. A base filter is an object that contains a category-action pair for all categories defined in the category file. A base filter is a structured object, and is defined with the help of a filter name and an array of category-action pairs. Each Enhanced Web Filtering (EWF) category has a default action in a base filter, which is attached to the user profile to act as a backup filter. If the categories are not configured in the user profile, the base filter takes the action. Junos OS Release 17.4R1 also supports online upgradation of base filters.

**Required Privilege Level**

view

RELATED DOCUMENTATION


- category (Security Web Filtering) | 388
- request security utm web-filtering category install | 675
- show security utm web-filtering category status | 732


## Sample Output

**show security utm web-filtering category base-filter**

`user@host>` **show security utm web-filtering category base-filter**

```
Base-filter: ewf-default-filter
    Enhanced_Adult_Material                                          block
    Enhanced_Business_and_Economy                                    permit

    Enhanced_Education                                               permit

    Enhanced_Government                                              permit
```

```
Enhanced_News_and_Media                                    permit

Enhanced_Religion                                          permit

Enhanced_Society_and_Lifestyles                            permit

Enhanced_Special_Events                                    permit

Enhanced_Information_Technology                            permit

Enhanced_Abortion                                          block
Enhanced_Advocacy_Groups                                   permit

Enhanced_Entertainment                                     permit

Enhanced_Gambling                                          block
Enhanced_Games                                             block
Enhanced_Illegal_or_Questionable                           block
Enhanced_Job_Search                                        permit

Enhanced_Shopping                                          permit

Enhanced_Sports                                            permit

Enhanced_Tasteless                                         permit

Enhanced_Travel                                            permit

Enhanced_Vehicles                                          permit

Enhanced_Violence                                          block
Enhanced_Weapons                                           block
Enhanced_Drugs                                             block
Enhanced_Militancy_and_Extremist                           block
Enhanced_Intolerance                                       permit

Enhanced_Health                                            permit

Enhanced_Website_Translation                               permit

Enhanced_Advertisements                                    permit

Enhanced_User_Defined                                      permit
```

```
Enhanced_Nudity                                                  block
Enhanced_Adult_Content                                           block
Enhanced_Sex                                                     block
Enhanced_Financial_Data_and_Services                             permit

Enhanced_Cultural_Institutions                                   permit

Enhanced_Media_File_Download                                     permit

Enhanced_Military                                                permit

Enhanced_Political_Organizations                                 permit

Enhanced_General_Email                                           permit

Enhanced_Proxy_Avoidance                                         block
Enhanced_Search_Engines_and_Portals                              permit

Enhanced_Web_Hosting                                             permit

Enhanced_Web_Chat                                                permit

Enhanced_Hacking                                                 block
Enhanced_Alternative_Journals                                    permit

Enhanced_Non_Traditional_Religions                               block
Enhanced_Traditional_Religions                                   permit

Enhanced_Restaurants_and_Dining                                  permit

Enhanced_Gay_or_Lesbian_or_Bisexual_Interest                     permit

Enhanced_Personals_and_Dating                                    permit

Enhanced_Alcohol_and_Tobacco                                     permit

Enhanced_Prescribed_Medications                                  permit
```

# show security utm web-filtering category category

**Syntax**

```
show security utm web-filtering category category
```

**Release Information**

Command introduced in Junos OS Release 17.4.

**Description**

Show the list of categories predefined by Websense. A category list is available on the device. This list consists of categories, each containing a category code, a name, and a parent ID. Categories can also be user-defined. Each category consists of a list of URLs or IP addresses. Categories are not updated dynamically and are tied to the Junos OS release because they have to be compiled into the Junos OS image. Any update in categories needs to be synchronized with the Junos OS release cycle.

> **NOTE:** Starting with Junos OS Release 17.4R1, you can download and dynamically load new Enhanced Web Filtering (EWF) categories. The downloading and dynamic loading of the new EWF categories do not require a software upgrade.

**Required Privilege Level**

view

RELATED DOCUMENTATION


- category (Security Web Filtering) | 388
- request security utm web-filtering category install | 675
- show security utm web-filtering category base-filter | 727
- Predefined Category Upgrading and Base Filter Configuration Overview | 159


## Sample Output

**show security utm web-filtering category category**

```
user@host> show security utm web-filtering category category
```

```
Enhanced_Adult_Material
    Enhanced_Business_and_Economy
    Enhanced_Education
    Enhanced_Government
    Enhanced_News_and_Media
    Enhanced_Religion
    Enhanced_Society_and_Lifestyles
    Enhanced_Special_Events
    Enhanced_Information_Technology
    Enhanced_Abortion
    Enhanced_Advocacy_Groups
    Enhanced_Entertainment
    Enhanced_Gambling
    Enhanced_Games
    Enhanced_Illegal_or_Questionable
    Enhanced_Job_Search
    Enhanced_Shopping
    Enhanced_Sports
    Enhanced_Tasteless
    Enhanced_Travel
    Enhanced_Vehicles
    Enhanced_Violence
```

# show security utm web-filtering category status

**Syntax**

```
show security utm web-filtering category status
```

**Release Information**

Command introduced in Junos OS Release 17.4.

**Description**

Show the current running version of the downloaded category file or the status of the installed predefined file.

**Required Privilege Level**

view

RELATED DOCUMENTATION

- category (Security Web Filtering) | 388
- request security utm web-filtering category install | 675
- show security utm web-filtering category base-filter | 727

## Sample Output

**show security utm web-filtering category status**

```
user@host> show security utm web-filtering category status

Installed version:  1
      Download version:   0
      Update status:      Done
```

# show security utm web-filtering statistics

**Syntax**

```
show security utm web-filtering statistics
<root-logical-system>
<logical-system (logical-system-name | all)>
<all-logical-systems-tenants>
<tenant (tenant-name | all)>
<fpc <fpc-slot fpc-slot pic-slot pic-slot>>
```

**Release Information**

Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4.
Support for Flexible PIC Concentrator (FPC) and PIC statistics added in Junos OS Release 12.1X46-D10.
Starting in Junos OS Release 18.2R1, on SRX5000 Series devices, the options **pic** and **fpc** are deprecated—rather than immediately removed—to provide backward compatibility.
Support for UTM in logical system added in Junos OS Release 18.3R1.
Support for UTM in tenant system added in Junos OS Release 19.2R1.

**Description**

Displays Web filtering statistics for connections including allowlist and blocklist hits and custom category hits. The aggregated statistics from all FPCs and PICs and statistics from both the nodes (with full chassis cluster support for UTM) are also displayed.

Starting in Junos OS Release 18.3R1, you can view the Web filtering statistics for the master logical system or for a specific user logical system or for all the user logical systems.

Starting in Junos OS Release 19.2R1, you can view the Web filtering statistics for a specific tenant system or for all the tenant systems.

**Options**

**none**—Displays Web filtering statistics for the master logical system.

***root-logical-system***—(Optional) Displays Web filtering statistics for the master logical system.

**logical-system *logical-system-name***—(Optional) Displays Web filtering statistics for a specific user logical system.

**all**—(Optional) Displays Web filtering statistics for all the user logical systems.

**all-logical-systems-tenants**—(Optional) Displays Web filtering statistics for all the logical systems and tenant systems.

**tenant *tenant-name***—(Optional) Displays Web filtering statistics for a specific tenant system.

**all**—(Optional) Displays Web filtering statistics for all the tenant systems.

**Required Privilege Level**
view

RELATED DOCUMENTATION

clear security utm web-filtering statistics | 663
show security utm web-filtering status | 740

**List of Sample Output**



## Sample Output

**show security utm web-filtering statistics**

```
user@host> show security utm web-filtering statistics
```

```
UTM web-filtering statistics:
    Total requests:                   0
    white list hit:                   0
    Black list hit:                   0
    No license permit:                0
    Queries to server:                0
    Server reply permit:              0
    Server reply block:               0
    Server reply quarantine:          0
    Server reply quarantine block:    0
    Server reply quarantine permit:   0
    Custom category permit:           0
    Custom category block:            0
    Custom category quarantine:       0
```

```
    Custom category qurantine block:    0
    Custom category quarantine permit:  0
    Site reputation permit:             0
    Site reputation block:              0
    Site reputation quarantine:         0
    Site reputation quarantine block:   0
    Site reputation quarantine permit:  0
    Site reputation by Category         0
    Site reputation by Global           0
    Cache hit permit:                   0
    Cache hit block:                    0
    Cache hit quarantine:               0
    Cache hit quarantine block:         0
    Cache hit quarantine permit:        0
Safe-search redirect:               0
+Safe-search rewrite:               0
    SNI pre-check queries to server:    0
    SNI pre-check server responses:     0
    Web-filtering sessions in total:    64000
    Web-filtering sessions in use:      0
    Fallback:                       log-and-permit          block
          Default                                   0              0
          Timeout                                   0              0
     Connectivity                                   0              0
Too-many-requests                                   0              0
```

**show security utm web-filtering statistics fpc**

user@host> **show security utm web-filtering statistics fpc**

```
 fpc-slot 5 pic-slot 0
 UTM web-filtering statistics:
    Total requests:                   0
    white list hit:                   0
    Black list hit:                   0
    Queries to server:                0
    Server reply permit:              0
    Server reply block:               0
    Server reply quarantine:          0
    Server reply quarantine block:    0
    Server reply quarantine permit:   0
    Custom category permit:           0
    Custom category block:            0
```

```
    Custom category quarantine:         0
    Custom category qurantine block:    0
    Custom category quarantine permit:  0
    Site reputation permit:             0
    Site reputation block:              0
    Site reputation quarantine:         0
    Site reputation quarantine block:   0
    Site reputation quarantine permit:  0
    Site reputation by Category         0
    Site reputation by Global           0
    Cache hit permit:                   0
    Cache hit block:                    0
    Cache hit quarantine:               0
    Cache hit quarantine block:         0
    Cache hit quarantine permit:        0
    Safe-search redirect:               0
  SNI pre-check queries to server:   1
    SNI pre-check server responses:     1
    Web-filtering sessions in total:    128000
    Web-filtering sessions in use:      0
    Fallback:                       log-and-permit           block
          Default                                0               0
          Timeout                                0               0
     Connectivity                                0               0
Too-many-requests                                0               0
```

**show security utm web-filtering statistics fpc fpc-slot 5 pic-slot 0**

user@host> **show security utm web-filtering statistics fpc fpc-slot 5 pic-slot 0**

```
 UTM web-filtering statistics:
    Total requests:                   0
    white list hit:                   0
    Black list hit:                   0
    Queries to server:                0
    Server reply permit:              0
    Server reply block:               0
    Server reply quarantine:          0
    Server reply quarantine block:    0
    Server reply quarantine permit:   0
    Custom category permit:           0
    Custom category block:            0
    Custom category quarantine:       0
    Custom category qurantine block:  0
```

```
    Custom category quarantine permit:  0
    Site reputation permit:             0
    Site reputation block:              0
    Site reputation quarantine:         0
    Site reputation quarantine block:   0
    Site reputation quarantine permit:  0
    Site reputation by Category         0
    Site reputation by Global           0
    Cache hit permit:                   0
    Cache hit block:                    0
    Cache hit quarantine:               0
    Cache hit quarantine block:         0
    Cache hit quarantine permit:        0
    Safe-search redirect:               0
  SNI pre-check queries to server:   1
    SNI pre-check server responses:     1
    Web-filtering sessions in total:    128000
    Web-filtering sessions in use:      0
    Fallback:                       log-and-permit           block
          Default                                 0               0
          Timeout                                 0               0
     Connectivity                                 0               0
Too-many-requests                                 0               0
```

**show security utm web-filtering statistics root-logical-system**

`user@host>` **show security utm web-filtering statistics root-logical-system**

```
 UTM web-filtering statistics:
    Web-filtering sessions in total:    2048000
    Web-filtering sessions in use:      0
    Fallback:                       log-and-permit           block
          Default                                 0               0
          Timeout                                 0               0
     Connectivity                                 0               0
Too-many-requests                                 0               0
```

**show security utm web-filtering statistics logical-system LSYS1**

`user@host>` **show security utm web-filtering statistics logical-system LSYS1**

```
 UTM web-filtering statistics:
    Web-filtering sessions in total:    2048000
```

```
    Web-filtering sessions in use:      0
    Fallback:                       log-and-permit          block
          Default                                0              0
          Timeout                                0              0
     Connectivity                                0              0
Too-many-requests                                0              0
```

**show security utm web-filtering statistics logical-system all**

`user@host>` **show security utm web-filtering statistics logical-system all**

```
 UTM web-filtering statistics:
    Web-filtering sessions in total:    2048000
    Web-filtering sessions in use:      0
    Fallback:                       log-and-permit          block
          Default                                0              0
          Timeout                                0              0
     Connectivity                                0              0
Too-many-requests                                0              0
```

**show security utm web-filtering statistics tenant TSYS1**

`user@host>` **show security utm web-filtering statistics tenant TSYS1**

```
 UTM web-filtering statistics:
    Web-filtering sessions in total:    1536000
    Web-filtering sessions in use:      0
    Fallback:                       log-and-permit          block
          Default                                0              0
          Timeout                                0              0
     Connectivity                                0              0
Too-many-requests                                0              0
```

**show security utm web-filtering statistics tenant all**

`user@host>` **show security utm web-filtering statistics tenant all**

```
 UTM web-filtering statistics:
    Web-filtering sessions in total:    1536000
    Web-filtering sessions in use:      0
    Fallback:                       log-and-permit          block
          Default                                0              0
```

```
          Timeout                                 0               0
     Connectivity                                 0               0
Too-many-requests                                 0               0
```

**show security utm web-filtering statistics all-logical-system-tenants**

`user@host>` **show security utm web-filtering statistics all-logical-system-tenants**

```
 UTM web-filtering statistics:
    Web-filtering sessions in total:    1536000
    Web-filtering sessions in use:      0
    Fallback:                       log-and-permit           block
          Default                               0               0
          Timeout                               0               0
     Connectivity                               0               0
Too-many-requests                               0               0
```

# show security utm web-filtering status

**Syntax**

```
show security utm web-filtering status <fpc <fpc-slot fpc-slot pic-slot pic-slot>>
```

**Release Information**

Command introduced in Junos OS Release 9.5.

Support for UTM in chassis cluster added in Junos OS Release 11.4. Support for Flexible PIC Concentrator (FPC) and PIC status added in Junos OS Release 12.1X46-D10.

Starting in Junos OS Release 18.2R1, on SRX5000 Series devices, the options **pic** and **fpc** to display PIC and FPC statistics are not supported.

**Description**

Display whether the Web filtering server connection is up or not. The aggregated status from all FPCs and PICs and status of both the nodes (with full chassis cluster support for UTM) are also displayed.

**Required Privilege Level**

view

RELATED DOCUMENTATION

clear security utm web-filtering statistics | 663

show security utm web-filtering statistics | 733

**List of Sample Output**



**Output Fields**

show security utm web-filtering status

Output fields are listed in the approximate order in which they appear.

## Sample Output

**show security utm web-filtering status**

```
user@host> show security utm web-filtering status
```

```
UTM web-filtering status:
   Server status: Juniper Enhanced using Websense server UP
```

**show security utm web-filtering status fpc**

```
user@host> show security utm web-filtering status fpc
```

```
UTM web-filtering status fpc:
fpc-slot 5 pic-slot 0
Connectivity status: UP
fpc-slot 0 pic-slot 1
Connectivity status: UP
```

**show security utm web-filtering status fpc fpc-slot 5 pic-slot 0**

```
user@host> show security utm web-filtering status fpc fpc-slot 5 pic-slot 0
```

```
UTM web-filtering status:
Connectivity status: UP
```

**show security utm web-filtering chassis cluster status**

```
{primary:node0}
user@host>  show security utm web-filtering status
node0:
--------------------------------------------------------------------------
 UTM web-filtering status:
    Server status: Juniper Enhanced using Websense server UP

node1:
--------------------------------------------------------------------------
 UTM web-filtering status:
    Server status: Juniper Enhanced using Websense server DOWN
```

Starting with 12.3X48-D10 and Junos OS Release 17.3R1, on SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, and SRX550M devices, the UTM process has been moved to the Packet Forwarding Engine (PFE). Starting with 12.1X46-D10 and Junos OS Release 17.3R1, on SRX1400, SRX1500, SRX3400, SRX3600, SRX4100, SRX4200, SRX4600, SRX5400, and SRX5600 devices, the UTM process has been moved to the PFE. Hence, the status shows down on the secondary node of the cluster.

# test security utm anti-spam

**Syntax**

```
test security utm anti-spam ip-check <test-IP>
<test-IP> test security utm anti-spam.
```

**Release Information**

Command introduced in Junos OS Release 20.2.

**Description**

Use this command to check if the IP (Internet Protocol) is a spam source or it is a configuration problem when the device doesn't block the spam. The anti-spam feature requires internet connectivity with the Spam Block List (SBL) server. Domain Name Service (DNS) must be available to access the SBL server.

**Options**

***test-IP***—Supports both IPv4 and IPv6.

**Required Privilege Level**

view

RELATED DOCUMENTATION

anti-spam (Security UTM Policy) | 372

**List of Sample Output**

**test security utm anti-spam on page 743**

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

Table 13 on page 742 lists the output fields for the **test security utm anti-spam** command. Output fields are listed in the approximate order in which they appear.

**Table 13: test security utm anti-spam**

| Field Name | Field Description |
|---|---|
| **SBL Server** | Spam block list (SBL) contains the list of the disallowed IPs. |
| **DNS Server** | The firewall performs SBL lookups through the Domain Name Service (DNS) protocol. |

## Sample Output

**test security utm anti-spam**

The following examples test IP 1.0.0.1 in SBL server msgsecurity.juniper.net through DNS server 172.29.151.60:

`user@host>` **test security utm anti-spam ip-check *1.0.0.1***

```
UTM anti-spam IP-check result:

    SBL Server:
        msgsecurity.juniper.net

    DNS Server:
        172.29.151.60

    Test result for IP check:
        SPAM (Match sbl server blacklist)
```

The following examples test IP 1.0.0.2 in SBL server msgsecurity.juniper.net through DNS server 172.29.151.60:

`user@host>`**test security utm anti-spam ip-check *1.0.0.2***

```
UTM anti-spam IP-check result:

    SBL Server:
        msgsecurity.juniper.net

    DNS Server:
        172.29.151.60

    Test result for IP check:
        NON SPAM (No match)
```

The following examples test IP 1.0.0.2 in SBL server msgsecurity.juniper.net through DNS server 172.29.151.60:

`user@host>`**test security utm anti-spam ip-check *1.0.0.2***

```
UTM anti-spam IP-check result:

    SBL Server:
        msgsecurity.juniper.net

    DNS Server:
        172.29.151.60

    Test result for IP check:
        NON SPAM (DNS error)
```

The following examples test IP 1.0.0.3 in SBL server msgsecurity.juniper.net through DNS server 172.29.151.66:

user@host>**test security utm anti-spam ip-check *1.0.0.3***

```
UTM anti-spam IP-check result:

    SBL Server:
        msgsecurity.juniper.net

    DNS Server:
        172.29.151.66

    Test result for IP check:
        NON SPAM (Timeout error)
```

The following examples test IP 1.0.0.4 in SBL server msgsecurity.juniper.net through DNS server 172.29.151.66:

user@host>**test security utm anti-spam ip-check *1.0.0.4***

```
UTM anti-spam IP-check result:

    SBL Server:
        msgsecurity.juniper.net

    DNS Server:
        172.29.151.66
```

```
    Test result for IP check:
        NON SPAM (Anti-Spam is not enable)
```

The following examples test IP 1.0.0.4 in SBL server msgsecurity.juniper.net through DNS server 172.29.151.66:

user@host>**test security utm anti-spam ip-check *1.0.0.4***

```
UTM anti-spam IP-check result:

    SBL Server:
        msgsecurity.juniper.net

    DNS Server:
        172.29.151.66

    Test result for IP check:
       No license
```

# test security utm enhanced-web-filtering url-check

**Syntax**

```
test security utm enhanced-web-filtering url-check
test-url Enhanced-web-filtering threat-check test URL
```

**Release Information**

Command introduced in Junos OS Release 20.2.

**Description**

Use this test command to send the test-string to web-filtering server (example: Websense ThreatSeeker Cloud) to test the category and reputation of the test-string.

**Options**

***<test-url>***— Enhanced-web-filtering threat-check test URL. The maximum length of test URL is 249.

**Required Privilege Level**

view

RELATED DOCUMENTATION

Enhanced Web Filtering | 149

**List of Sample Output**

**test security utm enhanced-web-filtering on page 747**

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

Table 14 on page 746 lists the output fields for the **test security utm enhanced-web-filtering url-check** command. Output fields are listed in the approximate order in which they appear.

**Table 14: test security utm enhanced-web-filtering**

| Field Name | Field Description |
|---|---|
| **Enhance web-filtering server** | Enhanced Web Filtering (EWF) supports HTTP methods. |

## Sample Output

**test security utm enhanced-web-filtering**

The following example sends URL www.google.com to EWF rp.cloud.threatseeker.com check the category and reputation:

`user@host>` **test security utm enhanced-web-filtering url-check *www.google.com***

```
UTM enhanced-web-filtering URL-check result:

    Enhance web-filtering server:
        rp.cloud.threatseeker.com

    Test result for URL check:
        Category name: Enhanced_Search_Engines_and_Portals
        Reputation: 90
        Threat level: very-safe
```

The following example sends URL www.aaa.com to EWF rp.cloud.threatseeker.com check the category and reputation:

`user@host>`**test security utm enhanced-web-filtering url-check *www.aaa.com***

```
 UTM enhanced-web-filtering URL-check result:

     Enhance web-filtering server:
         rp.cloud.threatseeker.com

     Test result for URL check:
      URL does not match on remote server
```

The following example sends URL www.bbb.com to EWF rp.cloud.threatseeker.com check the category and reputation:

`user@host>`**test security utm enhanced-web-filtering url-check *www.bbb.com***

```
UTM enhanced-web-filtering URL-check result:
```

```
    Enhance web-filtering server:
        rp.cloud.threatseeker.com

    Test result for URL check:
     UTM enhanced web filtering URL check test failed
```

The following example sends URL www.bbb.com to EWF rp.cloud.threatseeker.com check the category and reputation:

`user@host>` **test security utm enhanced-web-filtering url-check *www.bbb.com***

```
UTM enhanced-web-filtering URL-check result:

    Enhance web-filtering server:
        rp.cloud.threatseeker.com

    Test result for URL check:
     No license
```

The following example sends URL www.google.com to EWF rp.cloud.threatseeker.com check the category and reputation:

`user@host>` **test security utm enhanced-web-filtering url-check *www.google.com***

```
UTM enhanced-web-filtering URL-check result:

    Enhanced web-filtering server:
        rp.cloud.threatseeker.com

    Test result for URL check:
        EWF query timeout
```

# test security utm web-filtering profile

**Syntax**

```
test security utm web-filtering profile <profile-name>
<test-url> Web-filtering test URL
```

**Release Information**

Command introduced in Junos OS Release 20.2R1.

**Description**

Use this command to check if the test-string matches the specific profile in the Web filtering server.

**Options**

***test-url***— Enhanced Web filtering threat-check test URL. The maximum length of test URL is 249.

**Required Privilege Level**

view

RELATED DOCUMENTATION

Enhanced Web Filtering | 149

## Sample Output

**test security utm web-filtering profile**

The following example sends profile *sportclass* and test url *www.google.com* to the Web filtering server to check whether the test string matches the specific profile:

`user@host>` **test security utm web-filtering profile *sportclass www.google.com***

```
UTM web-filtering profile test:

    Test result:       Match EWF category
    Execute action:    Permit
```

```
    Match category:    Enhanced_Search_Engines_and_Portals
```

The following example sends profile *dangerclass* and test url *www.gun-clubs.com* to the Web filtering server to check whether the test string matches the specific profile:

`user@host>` **test security utm web-filtering profile *dangerclass www.gun-clubs.com***

```
 UTM web-filtering profile test:

    Test result:       Match custom category
    Execute action:    Permit
    Match category:    custom_category
```

The following example sends profile *dangerclass* and test url *www.gun-clubs.com* to the Web filtering server to check whether the test string matches the specific profile:

`user@host>` **test security utm web-filtering profile *dangerclass www.gun-clubs.com***

```
UTM web-filtering profile test:

    Test result:       Hit global reputation action
    Execute action:    Permit
    Match category:    N/A
```

The following example sends profile *dangerclass* and test url *www.gun-clubs.com* to the Web filtering server to check whether the test string matches the specific profile:

`user@host>` **test security utm web-filtering profile *dangerclass www.gun-clubs.com***

```
UTM web-filtering profile test:
```

```
  Test result: Web filtering engine is not ready, please try again later
```

The following example sends profile *dangerclass* and test url *www.gun-clubs.com* to the Web filtering server to check whether the test string matches the specific profile:

user@host> **test security utm web-filtering profile *dangerclass www.gun-clubs.com***

```
UTM web-filtering profile test:

  Test result: Can't find webfilter profile dangerclass
```

The following example sends profile *dangerclass* and test url *www.gun-clubs.com* to the Web filtering server to check whether the test string matches the specific profile:

user@host> **test security utm web-filtering profile *dangerclass www.gun-clubs.com***

```
UTM web-filtering profile test:

    Test result:       No license
    Execute action:    Permit
    Match category:    N/A
```

The following example sends profile *junos-wf-enhanced-default* and test *www.google.com* to the Web filtering server to check whether the test string matches the specific profile:

user@host> **test security utm web-filtering profile *junos-wf-enhanced-default www.google.com***

```
UTM web-filtering profile test:

    Test result:       Fallback (query timeout)
    Execute action:    Log and permit
    Match category:    N/A
```