Juniper Networks | Engineering Simplicity

Junos® OS

Content Security User Guide

Published
2023-12-17

JUNOS

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

Junos® OS Content Security User Guide

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

About This Guide

Use this guide to configure, monitor, and manage the Content Security features in Junos OS NFX Series and SRX Series Firewalls to secure the network from viruses, malware, or malicious attachments and protect the users from security threats.

1
CHAPTER

Overview

Content Security Overview

IN THIS SECTION

Content Security provides multiple security features and services in a single device or service on the network, protecting users from security threats in a simplified way. Content Security includes functions such as antivirus, antispam, content filtering, and web filtering. Content Security 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:

Content Security Overview

IN THIS SECTION

Content Security is a term used to describe the consolidation of several security features into one device, protecting against multiple threat types. The advantage of Content Security is streamlined installation and management of these multiple security capabilities.

The security features provided as part of the Content Security 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:

  1. 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.

  2. The Juniper Local Web Filtering makes the decision for blocking or permitting Web access 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.

  3. 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 device determines if it can permit or block the request based on the information provided by the TSC. The enhanced Web filtering solution requires a separate license.

- Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, on SRX1500 Services Gateways and vSRX Virtual Firewall instances, Content Security 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 Content Security 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 Content Security 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, Content Security 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 Content Security Licensing, see, Juniper Licensing User Guide. Please refer to the Juniper Licensing Guide for general information about License Management. Please refer to the product Data Sheets at SRX Series Firewalls for details, or contact your Juniper Account Team or Juniper Partner.

- Antivirus— The Avira antivirus module in the Content Security 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 Firewall scans specific application layer traffic to protect the user from virus attacks and to prevent viruses from spreading.

Understanding Content Security Custom Objects

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

The following Content Security features make use of certain custom objects:

- Web Filtering (see "Web Filtering Overview" on page 151)
- Anti-Spam (see "Server-Based Antispam Filtering Configuration Overview" on page 107)
- Content Filtering (see "Content Filtering Configuration Overview" on page 136)

Starting in Junos OS Release 18.2R1, a new dynamic application policy match condition is added to SRX Series Firewalls, allowing an administrator to more effectively control the behavior of Layer 7 applications. To accommodate Layer 7 application-based policies in Content Security, the `[edit security utm default-configuration]` hierarchy level is introduced. If any parameter in a specific Content Security feature profile configuration is not configured, then the corresponding parameter from the Content Security 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 Content Security profiles, the SRX Series Firewall applies the default Content Security profile until a more explicit match has occurred.

SEE ALSO

Content Security Supported Features | 6

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, Content Security 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 Content Security 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:

18.2R1	Starting in Junos OS Release 18.2R1, a new dynamic application policy match condition is added to SRX Series Firewalls, allowing an administrator to more effectively control the behavior of Layer 7 applications. To accommodate Layer 7 application-based policies in Content Security, the `[edit security utm default-configuration]` hierarchy level is introduced. If any parameter in a specific Content Security feature profile configuration is not configured, then the corresponding parameter from the Content Security 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 Content Security profiles, the SRX Series Firewall applies the default Content Security 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 Content Security 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 Virtual Firewall instances, Content Security 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 | 151

Antispam Filtering Overview | 104

Express Antivirus Protection

Content Security Supported Features

IN THIS SECTION

WELF Logging for Content Security Features

IN THIS SECTION

Understanding WELF Logging for Content Security Features

Content Security 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 Content Security Features

IN THIS SECTION

This example shows how to configure WELF logging for Content Security features.

Requirements

Before you begin, review the fields used to create a WELF log file and record. See "Content Security Overview" on page 2.

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

IN THIS SECTION

Procedure

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 Content Security 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

IN THIS SECTION

- Verifying the Security Log | **11**

Verifying the Security Log

Purpose

Verify that the WELF log for Content Security features is complete.

Action

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

SEE ALSO

Content Security Support for Chassis Cluster | **22**

Explicit Proxy for Content Security

IN THIS SECTION

Content Security support the use of an explicit proxy for the cloud-based connectivity for Enhanced Web Filtering (EWF) and Sophos antivirus (SAV) on Content Security. 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 Series Firewall sends *CONNECT* request to the proxy server, the SRX Series Firewall and TSC server communicates through the HTTP connection. Then the proxy server is expected to identify the configured IP addresses, allowlist and allow SRX Series Firewall 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 Content Security Web filtering configuration, the TSC server connection is established with the proxy host instead of the Content Security 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 Content Security 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

IN THIS SECTION

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

IN THIS SECTION

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

IN THIS SECTION

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 Content Security 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 Content Security

IN THIS SECTION

Understanding Unified Policies [Content Security]

IN THIS SECTION

Unified policies are now supported on SRX Series Firewalls, 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 Firewalls, allowing an administrator to more effectively control the behavior of Layer 7 applications.

To accommodate Layer 7 application-based policies in Content Security, the `[edit security utm default-configuration]` command is introduced. If any parameter in a specific Content Security feature profile configuration is not configured, then the corresponding parameter from the Content Security 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 Content Security profiles, the SRX Series Firewall applies the default Content Security profile until a more explicit match has occurred.

Understanding Default Content Security Policy

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

If there is an existing Content Security 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 Content Security policies are evaluated prior to global policies. The predefined Content Security default policy is leveraged if multiple Content Security policies exist in the potential policy list during the Content Security session creation process.

The predefined Content Security 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 Content Security feature profile is configured (Web filtering, content filtering, antivirus, and antispam), the parameters in the predefined global Content Security configuration are applied.

The predefined Content Security 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 Content Security 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

feature-profile

Content Security Support for Chassis Cluster

IN THIS SECTION

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

Understanding Content Security Support for Active/Active Chassis Cluster

Content Security 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 Content Security 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

Content Security 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 Content Security Support for Active/Backup Chassis Cluster

Content Security 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 Content Security 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, Content Security 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, Content Security 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*
>
> Content Security Overview | 2

RELATED DOCUMENTATION

Integrated Web Filtering

Local Web Filtering | 204

Redirect Web Filtering | 221

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.

Overview

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

Configuration

IN THIS SECTION

Procedure

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

IN THIS SECTION

Verify the MIME Allowlist Configuration

Purpose

To verify the MIME allowlist configuration is working properly.

Action

From operational mode, 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 Content Security 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 Content Security 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
- Full Antivirus Scan Results and Fallback Options

Release History Table

Release	Description
17.4R1	Starting with Junos OS Release 17.4R1, the allowlisting feature is extended to support custom URL categories supported by Content Security in the allowlist configuration of SSL forward proxy.
15.1X49-D80	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 Content Security in the allowlist configuration of SSL forward proxy. For more information, see Application Security User Guide for Security Devices.

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 Firewalls to understand about installing and using Avira antivirus on your security device.

Avira Antivirus Overview

IN THIS SECTION

Junos OS Content Security 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 1 on page 30 lists the components and license details for Avira Antivirus.

Table 1: 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. The virus pattern database is available at the following locations: • Default: https://update.juniper-updates.net/avira • For SRX4100, SRX4200, and SRX4600 Series Firewalls: https://update.juniper-updates.net/AVIRA/SRXTVP • For SRX5K-SPC3 devices: https://update.juniper-updates.net/AVIRA/SPC3 • For vSRX Virtual Firewall: https://update.juniper-updates.net/AVIRA/VSRX By default, SRX Series Firewalls downloads the updates for pattern database. See "Configure Avira Antivirus Scanning Options" on page 31 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 Firewall. See "Example: Configure Avira Antivirus" on page 31 for steps to install and activate Avira Antivirus scan engine. Avira Antivirus scan engine decompresses files before scanning for virus detection. For more information, see *decompress-layer-limit*. In the following scenarios, Avira Antivirus scan engine on the SRX Series Firewall does not scan the application traffic: • The scan engine is not ready. • There are too many scanning requests. • The scanned file size is larger than a configured limit. • The scanned file has too many nested layers of compression. • The memory file system is full.

Table 1: Components and License Details for Avira Antivirus *(Continued)*

Components	Detailed Information
License details	Avira Antivirus scan engine is a licensed subscription service. 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. 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. 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

scan-options (Security Antivirus Avira Engine)

Example: Configure Avira Antivirus

IN THIS SECTION

In this example, you'll learn how to configure Avira antivirus on your security device. This topic includes the details about using default antivirus profile and customized antivirus profile to secure your device from the harmful content such as infected files, trojans, worms, spyware, and other malicious data.

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 Firewalls.
- SRX Series Firewall with Junos OS Release 18.4R1 or later.
- For vSRX Virtual Firewall, the minimum requirement is 4 CPU cores and 4 GB memory.

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

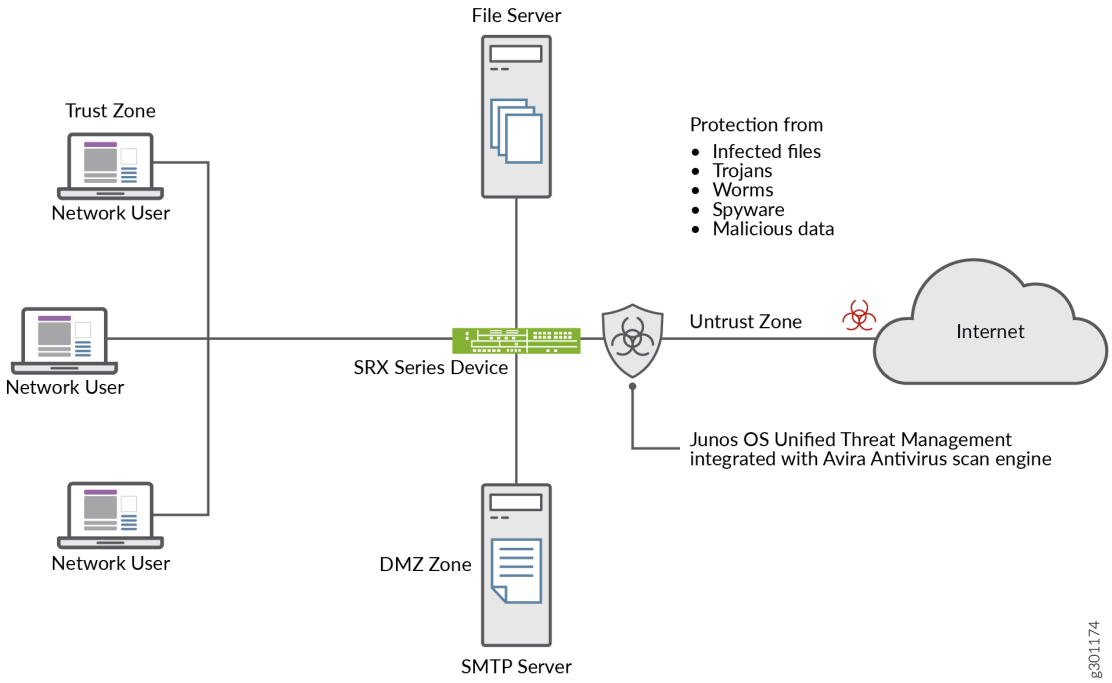
Overview

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 Firewall 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 33 shows an example of Avira antivirus on SRX Series Firewall 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" on page 34.
- To customize antivirus options as per your requirements, see "Configure Avira Antivirus Scanning Options" on page 35 .
- To set antivirus scanning options, see "Configure Avira Antivirus Scanning with Custom Profile" on page 36 .

Configuration

IN THIS SECTION

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 Content Security policy with default antivirus profiles for all protocols and apply the Content Security policy in a security policy for the permitted traffic.

Use Default Antivirus Profile to Start Antivirus Scanning

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 Content Security 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 Firewalls 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 1 on page 30 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 2 on page 37 to configure Avira antivirus with custom options on your security device.

Table 2: Steps for Avira Antivirus Scanning Using Custom Profile

Step	Details
Step 1: Define custom objects	In this step, you will define antivirus scanning options: • MIME allowlist—Include type of traffic that you want to bypass antivirus scanning • MIME exception list—Specify excluding some MIME types from the MIME allowlist • Custom URL categories—Define URLs that you want to bypass antivirus scanning. 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. • Configure antivirus scanning settings such as data file update interval, notification options for administrators, fallback options, and file size limits.
Step 3: Create Content Security policy	Associate the antivirus profile created in Step 2 for FTP, HTTP, POP3, SMTP, and IMAP traffic. Content Security policies control which protocol traffic is sent to the antivirus scanning engine.
Step 4: Apply Content Security policy to a security policy	Specify Content Security policy as application services in the security policy. The Content Security 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 "Content Security Overview" on page 2.

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 Content Security 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 Content Security 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

Purpose

Action

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

Sample Output

command-name

```
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

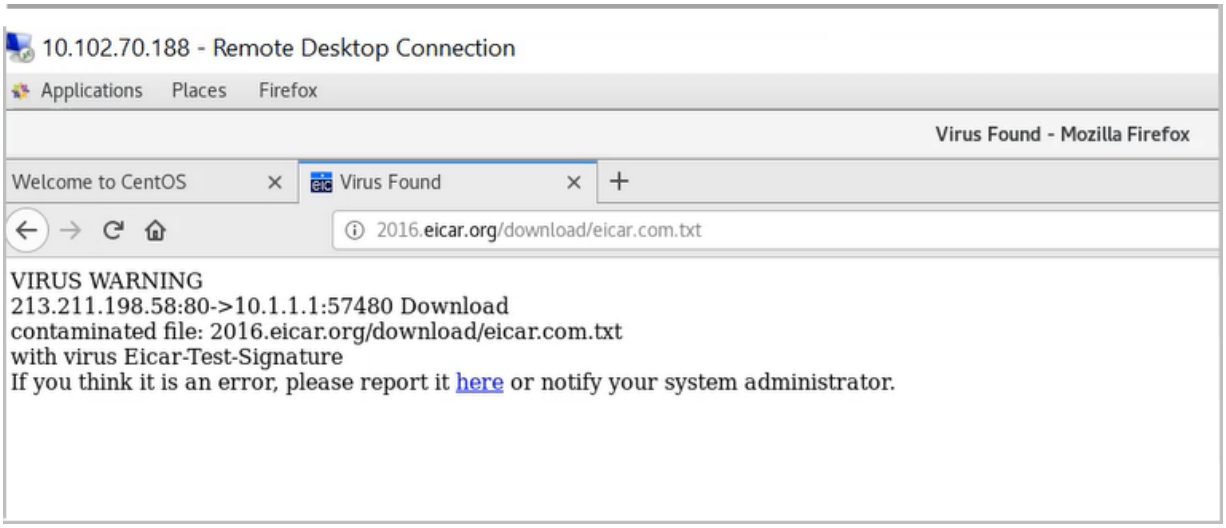
Purpose

Validate whether Avira Antivirus Solution is working on SRX Series Firewalls

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 Firewalls
- Full Antivirus Scan Results and Fallback Options
- Virus-Detected Notifications | **97**
- HTTP Trickling to Prevent Timeouts | **101**

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. Prior to Junos OS Release 23.1R1, the Sophos antivirus scanner also used 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 Content Security 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 Content Security.

Starting with Junos OS Release 12.3X48-D35 and Junos OS Release 17.3R1, the Content Security 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.

Starting in Junos OS Release 23.1R1, content security supports the new antivirus Sophos Live Protection version 2.0. The new version of Sophos antivirus uses an HTTPS connection for the device-to-server communication. For the HTTPS connection, you must create an SSL initiation profile and add the profile to the default configuration of the Sophos engine.

SEE ALSO

Understanding TCP Proxy

Enabling TCP Proxy Session to Increase the Network Transmit Speed

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 Firewall. The security channel from the SRX Series Firewall is divided as one SSL channel between the client and the SRX Series Firewall and another SSL channel between the SRX Series Firewall and the HTTPS server. SSL forward proxy acts as the terminal for both channels and forwards the cleartext traffic to Content Security. Content Security 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, Content Security bypasses the traffic. Content Security 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 null route 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
>
> Understanding Full Antivirus Scanning Timeouts

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

Understanding Antivirus Scanning Fallback Options

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

Example: Configuring Full Antivirus Intelligent Prescreening

Sophos Antivirus Configuration Overview

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

You must complete the following tasks to configure Sophos antivirus:

1. Configure Content Security custom objects and MIME lists. See "Example: Configuring Sophos Antivirus Custom Objects" on page 51,
2. Configure the Sophos antivirus feature profile. See "Example: Configuring Sophos Antivirus Feature Profile" on page 55.
3. Configure a Content Security policy. See "Example: Configuring Sophos Antivirus Content Security Policies" on page 64
4. Configure a security policy. See "Example: Configuring Sophos Antivirus Firewall Security Policies" on page 67.

Example: Configuring Sophos Antivirus Custom Objects

IN THIS SECTION

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

Requirements

Before you begin, read about Content Security custom objects. See "Content Security Overview" on page 2.

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

IN THIS SECTION

Procedure

GUI Quick Configuration

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**.

Step-by-Step Procedure

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**.

Step-by-Step Procedure

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.)

Step-by-Step Procedure

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

IN THIS SECTION

Verify the Sophos Antivirus Custom Objects Configuration

Purpose

To verify the Sophos Antivirus custom objects configuration., enter the `show security utm custom-objects` command.

Action

From the operational mode, enter the `show security utm custom-objects` command to verify the Sophos Antivirus custom objects configuration.

SEE ALSO

Allowlist | 24

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 Content Security. See "Example: Configuring Sophos Antivirus Custom Objects" on page 51.

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 "Content Security Overview" on page 2.

Configuration

IN THIS SECTION

Procedure

GUI Quick Configuration

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 Content Security policy. See "Example: Configuring Sophos Antivirus Content Security Policies" on page 64.

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

   #### Step-by-Step Procedure

   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:

   #### Step-by-Step Procedure

   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.

   #### Step-by-Step Procedure

   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.

Step-by-Step Procedure

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.

Step-by-Step Procedure

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 Content Security policy. See "Example: Configuring Sophos Antivirus Content Security Policies" on page 64.

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

IN THIS SECTION

Obtaining Information About the Current Antivirus Status

Purpose

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 | 97

Example: Configuring Antivirus Scanning Fallback Options

Allowlist | 24

Example: Configuring Sophos Antivirus Content Security Policies

IN THIS SECTION

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

Requirements

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

1. Configure Content Security custom objects and MIME lists. See "Example: Configuring Sophos Antivirus Custom Objects" on page 51.
2. Configure the Sophos antivirus feature profile. See "Example: Configuring Sophos Antivirus Feature Profile" on page 55.

Overview

After you have created an antivirus feature profile, you configure a Content Security 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

IN THIS SECTION

Procedure

GUI Quick Configuration

Step-by-Step Procedure

To configure a Content Security 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 Content Security policy for Sophos antivirus:

1. Go to the edit security Content Security hierarchy.

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

2. Create the Content Security 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

IN THIS SECTION

Verify the Content Security Policy Configuration

Purpose

To verify the Content Security policy configuration.

Action

From the operational mode, enter the `show security utm utm-policy utmp3` command.

SEE ALSO

Understanding Full Antivirus Application Protocol Scanning

Understanding HTTP Scanning

Understanding Protocol-Only Virus-Detected Notifications | 97

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 Content Security policy.

1. Configure Content Security custom objects and MIME lists. See "Example: Configuring Sophos Antivirus Custom Objects" on page 51.
2. Configure the Sophos antivirus feature profile. See "Example: Configuring Sophos Antivirus Feature Profile" on page 55.
3. Configure a Content Security policy. See "Example: Configuring Sophos Antivirus Content Security Policies" on page 64.

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 55. Because the match application configuration is set to any, all application types will be scanned.

Configuration

IN THIS SECTION

Procedure

GUI Quick Configuration

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`.

   #### Step-by-Step Procedure

   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 Content Security policy named utmp3 to the firewall security policy. This will cause matched traffic to be scanned by the Sophos antivirus feature.

   #### Step-by-Step Procedure

   a. From the Edit Policy box, click the **Application Services** tab.

b. In the Content Security 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 Content Security 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

IN THIS SECTION

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

Verify the Security Policy Configuration

Purpose

To verify the security policy configuration, enter the `show security policies` command.

Action

From the operational mode, enter the `show security policies` command.

SEE ALSO

Allowlist | 24

Example: Configure Sophos Antivirus Live Protection Version 2.0

IN THIS SECTION

Use this configuration example to configure and to verify the Sophos antivirus live protection version 2.0 on your device. Sophos antivirus is an in-the-cloud antivirus solution. The virus pattern and malware database on the external servers maintained by Sophos (Sophos Extensible List) servers isolate and protect your device. Starting in Junos OS Release 23.1R1, content security supports Sophos antivirus live protection version 2.0. The new antivirus version uses the HTTPS protocol to communicate between the SRX Series Firewall and Sophos server.

TIP:

Table 3: Estimated Timers

Readability Score	• Flesch reading ease: 34 • Flesch-Kincaid reading grade level: 11.9
Reading Time	Less than 15 minutes.
Configuration Time	Less than an hour.

Example Prerequisites

Hardware requirements	SRX Series Firewall and vSRX Virtual Firewall
Software requirements	Junos OS Release 23.1R1 or later

Licensing requirements	Sophos antivirus live protection version 2.0 license Use the `show system license` command to make sure you have a valid Sophos antivirus license installed on your device. When your antivirus license key expires, functionality will no longer work because the pattern lookup database is on the remote Sophos servers.

Before You Begin

Benefits	The virus pattern and malware database on the external servers maintained by Sophos (Sophos Extensible List) servers isolate and protect your device. Provides HTTPS based secure connection between the SRX Series Firewall and Sophos server.
Useful resources:	
Know more	"Sophos Antivirus Protection" on page 46
Hands-on experience	vLab Sandbox: Zones / Policies
Learn more	Content Security Antivirus

Functional Overview

Table 4 on page 72 provides a quick summary of the configuration components deployed in this example.

Table 4: Sophos Antivirus Functional Overview

Profiles

Initiation profile	The Sophos server configuration on the SRX Series Firewall includes the SSL initiation profile (*ssl_init_prof*). The initiation profile is mandatory to enable the SRX Series Firewall to initiate an HTTPS session with the Sophos server for checking the packets. The SSL initiation profile also encrypts and decrypts packets to and from the Sophos server.
Proxy profile	The SSL proxy profile, *ssl_pr1*, enables the SRX Series Firewall to decrypt the packets for further application service processing when the client initiates the HTTPS session to the Web server.
Feature profile	The feature profile, *content_security_sav_fp*, applies to the firewall security policy (p1) using different content security policies and match criteria. You can have more than one feature profiles for different content security policies.
Policies	
Content security policy	The content security policy, *content_security_p1*, defines the antivirus protocols (HTTP, FTP, SMTP, POP3, and IMAP) and attaches this policy to a security feature profile, *content_security_sav_fp*, to implement it.
Security policies	Two security policies (*p1* and *trust_to_internet*) have a simple match criteria to apply on the traffic between the security zones. We attach the *content_security_p1* content security policy and the *ssl_pr1* proxy profile to the application services of the *p1* security policy.
Security zones	
`trust`	Network segment at the host (Client) zone.
`untrust`	Network segment at the destination server (Web service) zone.

`internet`	Network segment through which the SRX Series Firewall interacts with the Sophos server.
Protocols	
HTTPS	HTTPS sessions establish between the client and the Web server, and the SRX Series Firewall and the Sophos server.
Primary verification tasks	• Verify the type of antivirus scan engine installed on your device. • Confirm the Sophos antivirus engine operation.

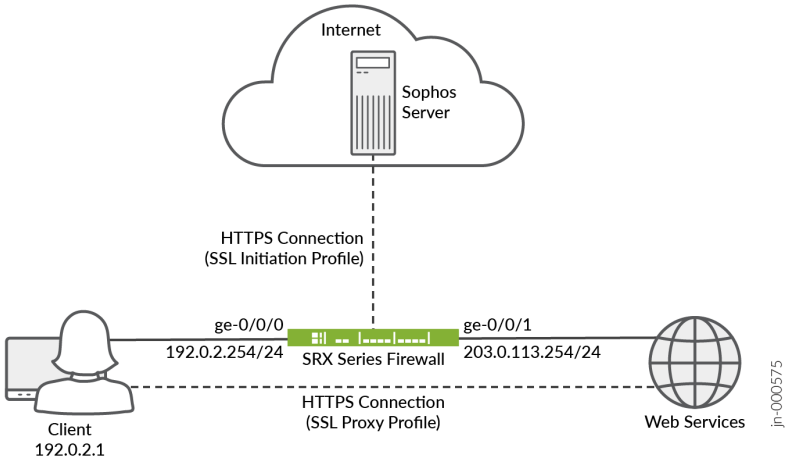
Topology Overview

In this example, the client initiates a request to Web service through the SRX Series Firewall. When the SRX Series Firewall receives the request, it contacts the Sophos server for checking the authenticity of the Web service. The Sophos antivirus version 2.0 uses HTTPS connection for the SRX Series Firewall to Sophos server communication. Based on the response received from the Sophos server, the SRX Series Firewall permits or blocks the traffic as defined in the content security policy.

Topology Components	Role	Function
Client	Requests Web service	Initiates HTTPS session with the Web server through the SRX Series Firewall.
SRX Series Firewall	Juniper Network's Firewall	Initiates HTTPS session with the Sophos antivirus server. It also encrypts and decrypts the packets for the client.
Sophos server	Antivirus server	Authenticates the content received from the SRX Series Firewall.
Web server	Web service provider	Responds to the client's request.

Topology Illustration

Figure 3: Sophos Antivirus Live Protection Topology



Step-by-step Configuration on Device-Under-Test (DUT)

NOTE: For complete sample configurations on the DUT, see:

- "Appendix 1: Set Commands on All Devices" on page 80
- "Appendix 2: Show Configuration Output on DUT" on page 81

1. Configure the device interfaces.

```
[edit interfaces]
user@host# set ge-0/0/0 unit 0 family inet address 192.0.2.254/24
user@host# set ge-0/0/1 unit 0 family inet address 203.0.113.254/24
```

2. Enable Sophos antivirus on the device. Configure the forwarding mode and type of traffic the Sophos antivirus should check.

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

```
user@host# set utm default-configuration anti-virus forwarding-mode inline-tap
user@host# set utm default-configuration anti-virus scan-options no-uri-check
```

3. Define an SSL initiation profile for adding to the Sophos server configuration on the SRX Series Firewall.

```
[edit services]
user@host# set ssl initiation profile ssl_init_prof client-certificate content_security_cert
user@host# set ssl initiation profile ssl_init_prof actions ignore-server-auth-failure
```

4. Include the SSL initiation profile into the Sophos server configuration. This configuration is mandatory to enable the SRX Series Firewall to initiate an HTTPS session with the Sophos server for checking the packets. The initiation profile also encrypts and decrypts packets to and from the Sophos server.

```
[edit security]
user@host# set utm default-configuration anti-virus sophos-engine server ssl-profile
ssl_init_prof
```

5. Define an SSL proxy profile for applying to the security policies. The SLL proxy profile enables the SRX Series Firewall to decrypt the packets for further application processing.

```
[edit services]
user@host# set ssl proxy profile ssl_pr1 root-ca content_security_cert
user@host# set ssl proxy profile ssl_pr1 actions ignore-server-auth-failure
```

6. Define the feature profile to indicate the type of traffic the Sophos antivirus should check by attaching the profile to the content security policies. You can define more than one feature profiles for different content security policies.

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

7. Define security zones.

```
[edit security zones]
user@host# set security-zone untrust description untrust
user@host# set security-zone untrust host-inbound-traffic system-services all
```

```
user@host# set security-zone untrust host-inbound-traffic protocols all
user@host# set security-zone untrust interfaces ge-0/0/1.0
user@host# set security-zone trust description trust
user@host# set security-zone trust host-inbound-traffic system-services all
user@host# set security-zone trust host-inbound-traffic protocols all
user@host# set security-zone trust interfaces ge-0/0/0.0
user@host# set security-zone internet description internet
```

8. Define a content security policy and attach a feature profile to it to indicate the type of traffic the Sophos server should check.

```
[edit security utm]
user@host# set utm-policy content_security_p1 anti-virus http-profile content_security_sav_fp
user@host# set utm-policy content_security_p1 anti-virus ftp upload-profile
content_security_sav_fp
user@host# set utm-policy content_security_p1 anti-virus ftp download-profile
content_security_sav_fp
user@host# set utm-policy content_security_p1 anti-virus smtp-profile content_security_sav_fp
user@host# set utm-policy content_security_p1 anti-virus pop3-profile content_security_sav_fp
user@host# set utm-policy content_security_p1 anti-virus imap-profile content_security_sav_fp
```

9. Define security policies and configure match criteria to apply to traffic between the different security zones.

```
[edit security policies]
user@host# set from-zone trust to-zone untrust policy p1 match source-address any
user@host# set from-zone trust to-zone trust policy p1 match destination-address any
user@host# set from-zone trust to-zone trust policy p1 match application any
user@host# set from-zone trust to-zone trust policy p1 then permit application-services ssl-
proxy profile-name ssl_pr1
user@host# set from-zone trust to-zone trust policy p1 then permit application-services utm-
policy content_security_p1
user@host# set from-zone trust to-zone trust policy trust_to_internet match source-address any
user@host# set from-zone trust to-zone trust policy trust_to_internet match destination-
address any
user@host# set from-zone trust to-zone trust policy trust_to_internet match application any
user@host# set from-zone trust to-zone trust policy trust_to_internet then permit
user@host# set default-policy permit-all
```

Verification

IN THIS SECTION

Provide a list of show commands used to verify the feature in this example.

Command	Verification Task
show security utm anti-virus status	Displays the type and status of the antivirus installed on your device.
show security utm anti-virus statistics	Displays the performance statistics of the antivirus on your device.

Antivirus Scan Engine Type Verification

Purpose

Verify the antivirus scan engine type installed on your device.

Action

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

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

    Anti-virus key expire date: 2024-02-23 16:00:00
    Forwarding-mode: continuous delivery
    Scan engine type: sophos-engine
    Scan engine information: running
```

Meaning

The sample output confirms the Sophos antivirus is available on your device.

Antivirus Scan Engine Performance Verification

Purpose

Verify the antivirus scan engine performance on your device.

Action

From operational mode, enter the **show security utm anti-virus statistics** to view the performance statistics of the antivirus on your device.

```
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
2                 1               1             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 `Threat-found` value shows that the antivirus detected 1 threat. The other statistics values are safe.

Appendix 1: Set Commands on All Devices

Set command output on all devices.

```
set security utm default-configuration anti-virus type sophos-engine
set security utm default-configuration anti-virus forwarding-mode inline-tap
set security utm default-configuration anti-virus scan-options no-uri-check
set security utm default-configuration anti-virus sophos-engine server ssl-profile ssl_init_prof
set security utm feature-profile anti-virus profile content_security_sav_fp
set security utm utm-policy content_security_p1 anti-virus http-profile content_security_sav_fp
set security utm utm-policy content_security_p1 anti-virus ftp upload-profile
content_security_sav_fp
set security utm utm-policy content_security_p1 anti-virus ftp download-profile
content_security_sav_fp
set security utm utm-policy content_security_p1 anti-virus smtp-profile content_security_sav_fp
set security utm utm-policy content_security_p1 anti-virus pop3-profile content_security_sav_fp
set security utm utm-policy content_security_p1 anti-virus imap-profile content_security_sav_fp
set security zones security-zone untrust description untrust
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone trust description trust
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 ge-0/0/0.0
set security zones security-zone internet description internet
set security policies from-zone trust to-zone untrust policy p1 match source-address any
set security policies from-zone trust to-zone untrust policy p1 match destination-address any
set security policies from-zone trust to-zone untrust policy p1 match application any
set security policies from-zone trust to-zone untrust policy p1 then permit application-services
ssl-proxy profile-name ssl_pr1
set security policies from-zone trust to-zone untrust policy p1 then permit application-services
utm-policy content_security_p1
set security policies from-zone trust to-zone internet policy trust_to_internet match source-
address any
set security policies from-zone trust to-zone internet policy trust_to_internet match
destination-address any
set security policies from-zone trust to-zone internet policy trust_to_internet match
application any
set security policies from-zone trust to-zone internet policy trust_to_internet then permit
set security policies default-policy permit-all
set services ssl initiation profile ssl_init_prof client-certificate content_security-cert
```

```
set services ssl initiation profile ssl_init_prof actions ignore-server-auth-failure
set services ssl proxy profile ssl_pr1 root-ca content_security-cert
set services ssl proxy profile ssl_pr1 actions ignore-server-auth-failure
```

Appendix 2: Show Configuration Output on DUT

Show command output on the DUT.

From configuration mode, confirm your configuration by entering the `show security utm`, `show interfaces`, `show security zones`, `show security policies`, and `show services ssl` 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
default-configuration {
    anti-virus {
        type sophos-engine;
        forwarding-mode {
            inline-tap;
        }
        scan-options {
            no-uri-check;
        }
        sophos-engine {
            server {
                ssl-profile ssl_init_prof;
            }
        }
    }
}
utm-policy P1 {
    anti-virus {
        http-profile junos-sophos-av-defaults;
    }
}
utm-policy content_security_p1 {
    anti-virus {
        http-profile content_security_sav_fp;
        ftp {
            upload-profile content_security_sav_fp;
            download-profile content_security_sav_fp;
        }
        smtp-profile content_security_sav_fp;
```

```
        pop3-profile content_security_sav_fp;
        imap-profile content_security_sav_fp;
    }
}
```

```
user@host# show show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 192.0.2.254/24;
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 203.0.113.254/24;
        }
    }
}
```

```
user@host# show security zones
security-zone untrust {
    description untrust;
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}
security-zone trust {
    description trust;
    host-inbound-traffic {
        system-services {
```

```
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone internet {
    description internet;
}
```

```
user@host# show security policies
from-zone trust to-zone untrust {
    policy p1 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    ssl-proxy {
                        profile-name ssl_pr1;
                    }
                    utm-policy content_security_p1;
                }
            }
        }
    }
}
from-zone trust to-zone internet {
    policy trust_to_internet {
        match {
            source-address any;
            destination-address any;
            application any;
        }
```

```
        then {
            permit;
        }
    }
}
default-policy {
    permit-all;
}
```

```
user@host# show services ssl
initiation {
    profile ssl_init_prof {
        client-certificate content_security-cert;
        actions {
            ignore-server-auth-failure;
        }
    }
}
proxy {
    profile ssl_pr1 {
        root-ca content_security-cert;
        actions {
            ignore-server-auth-failure;
        }
    }
}
```

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 Firewalls.

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 48.

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 Content Security 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 "Content Security Overview" on page 2.

Configuration

IN THIS SECTION

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
```

Procedure

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 Content Security Antivirus Statistics

Purpose

Verify Content Security 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 Content Security antivirus statistics.

Verifying Content Security Antivirus Statistics Details

Purpose

Verify Content Security 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 Content Security Antivirus Status

Purpose

Verify Content Security 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 55. 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
```

Release History Table

Release	Description
23.1R1	Starting in Junos OS Release 23.1R1, content security supports the new antivirus Sophos Live Protection version 2.0. The new version of Sophos antivirus uses an HTTPS connection for the device-to-server communication. For the HTTPS connection, you must create an SSL initiation profile and add the profile to the default configuration of the Sophos engine.
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 Content Security.
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 Content Security 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 | 97

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 "Content Security Overview" on page 2.

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 "Content Security Overview" on page 2.

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 "Content Security Overview" on page 2.

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

Full Antivirus Scan Results and Fallback Options

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
- Full Antivirus File Scanning

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

IN THIS SECTION

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 | **106**

Understanding Local List Antispam Filtering | **117**

RELATED DOCUMENTATION

Full Antivirus Application Protocol Scanning

Virus-Detected Notifications | 97

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 | 104

Understanding Local List Antispam Filtering | 117

Server-Based Antispam Filtering Configuration Overview

For each Content Security feature, configure feature parameters in the following order:

1. Configure Content Security 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 Content Security 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 Content Security 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 Content Security feature. See "Server-Based Antispam Filtering Configuration Overview" on page 107.

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

IN THIS SECTION

Procedure

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 Quick Configuration

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**.

   #### Step-by-Step Procedure

   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 Content Security policy for SMTP to which you attach the antispam profile.

   #### Step-by-Step Procedure

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

   b. In the Content Security 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 Content Security 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 Content Security 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 Content Security policy.

3. Attach the Content Security policy to a security policy.

Step-by-Step Procedure

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

b. In the Security Policy window, click **Add** to configure a security policy with Content Security 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 Content Security Policy.

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

k. Next to Content Security Policy, select the appropriate policy from the list. This attaches your Content Security 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 Firewalls 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 Content Security policy.

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

6. Configure a security policy for Content Security to which to attach the Content Security 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

IN THIS SECTION

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 | 117

spam-action

RELATED DOCUMENTATION

Allowlist | 24

Content Filtering | 129

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 | **104**

Understanding Server-Based Antispam Filtering | **106**

Server-Based Antispam Filtering Configuration Overview | **107**

Local List Antispam Filtering Configuration Overview

For each Content Security feature, configure feature parameters in the following order:

1. Configure Content Security 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 Content Security 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 Content Security 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 Content Security feature. See "Local List Antispam Filtering Configuration Overview" on page 117.

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

IN THIS SECTION

Procedure

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 default-configuration 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 Quick Configuration

Step-by-Step Procedure

To configure local list antispam filtering:

1. Create local allowlist and blocklist custom objects by configuring a URL pattern list.

   #### Step-by-Step Procedure

   a. Select **Configure>Security>UTM>Custom Objects**.

   b. In the Content Security 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.

   #### Step-by-Step Procedure

   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 Content Security policy for SMTP to which you attach the antispam profile.

   Step-by-Step Procedure

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

   b. In the Content Security policy configuration window, click **Add** to configure a Content Security 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 Content Security 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 Content Security policy.

4. Attach the Content Security policy to a security policy.

   Step-by-Step Procedure

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

   b. In the Security Policy window, click **Add** to configure a security policy with Content Security. 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 Content Security Policy.

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

k. Next to Content Security Policy, select the appropriate policy from the list. This attaches your Content Security 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 security utm default-configuration 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 Content Security policy.

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

7. Configure a security policy for Content Security, and attach the Content Security 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;
        sbl {
            profile localprofile1 {
                spam-action block;
                custom-tag-string ***spam***;
            }
        }
    }
default-configuration {
    anti-spam {
        address-whitelist as-white;
    }
}
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

IN THIS SECTION

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

Antispam Filtering Overview | 104

RELATED DOCUMENTATION

Allowlist | 24

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

IN THIS SECTION

Content Filtering Based on File Type

Previously, content filtering was performed to block or permit 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. This type of evaluation based on file type is supported only on Junos OS Releases prior to Junos OS Release 21.4R1.

Starting in Junos OS Release 21.4R1, content evaluation is done based of the file content. The file type-based evaluation of content is deprecated and the related configurations are hidden.

You can use the legacy functionality if you do not want to migrate to enhanced content filtering functionality. You will be allowed to use the legacy configurations, but all the legacy configuration knobs are deprecated and hidden. Also, you will receive system logs and error message warnings when you use the legacy configuration options.

In this type of evaluation the content filter module evaluates the traffic before all other Content Security 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 blocklist. Note that the exception list has a higher priority than the blocklist. 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 blocklist.

  If a protocol command appears on the both the permit list and the blocklist, 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 Content Security.

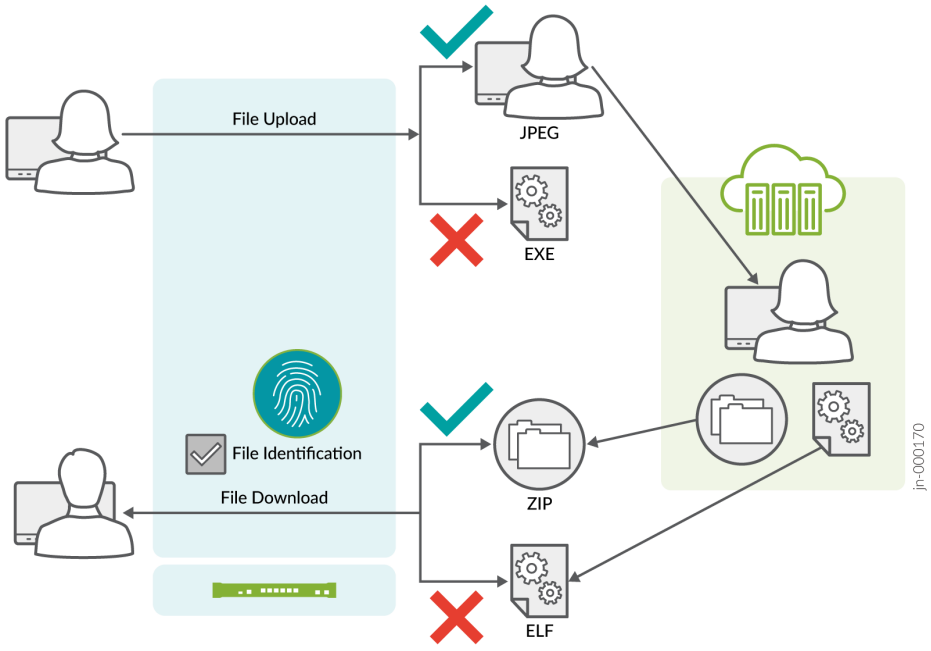
Because not all harmful files or components can be controlled by the MIME type or by the file extension, you can also use the content filter module to block ActiveX, Java Applets, and other types of content. The following types of content blocking are supported only for HTTP:

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

Content Filtering Based on File Content

Content filtering was previously performed based on file type, mime-type, content-type, and protocol command. File detection using the MIME type, protocol command filters, or by file extension filters is not reliable always.The easiest way to identify a file type is by file name extensions, but it is not authentic as any extension can be given to any kind of file.

Starting in Junos OS Release 21.4R1, Content Security performs content filtering to determine the file type based on the file content and not based on the file extensions. The file content is first analyzed to accurately determine the file type. This feature complements application identification (App ID) and allows you to configure the firewall for identifying and controlling access to Web (HTTP and HTTPS) traffic and to protect your network from attacks. When the final application match is confirmed by App ID, the matching Content Security policy is considered for content filtering.



Content filtering based on file content is performed as follows:

- File identification: For every file type, there are rules defined to examine the content and determine the file type. Content Security process uses the file content and matches it against the rules defined to determine the file type.

- Define content filtering rules for traffic direction: The Content Security process reads configuration from CLI, parses and interprets rule-sets and rules. You can define the content filtering rules and enforce the rules to direct the traffic.

  Rule-set and rules configurations are added under the `[edit security utm utm-policy <utm-policy-name> content-filtering]` hierarchy level.

  You can configure connection reset option in the content filter rule. When the content listed within the rule is detected, protocol handlers perform TCP connection reset with the client and server exactly as configured in the policy.

  > **NOTE**: Content filtering options based on mime-type, content-type, and protocol command is not supported. After you upgrade to Junos OS Release 21.4R1, previously existing file extension based content filtering options under the `[edit security utm utm-policy <utm-policy-name> content-filtering]` and `[edt security utm feature-profile content-filtering profile <profile-name>` hierarchies are not supported.

- Use the rules and rules sets defined for content filtering: You can use the rules and rule sets defined above from the `[edit security utm default-configuration content-filtering` hierarchy. These rules and rule-set allows you to configure direction specific content filters and connection reset.

- Content Security policy selection for content filtering: Once final application match is confirmed by APP ID, the matching potential Content Security policy in which content filtering rules are defined is chosen for processing.

  For every Content Security policy, a chain is created with list of rule-set nodes and all rules configured under a rule-set are added to a list and then attached to the respective rule-set node.

  After all checks are passed, a unique ID is allocated for each rule-set and rule configured to preserve and organize respective information in the local memory. This storage in the local memory is required to track the configuration changes you make and to synchronize the updates.

- Verification: Use the following commands to view the content-filtering system statistics and errors.

  - To display content filtering statistics in a policy within root-logical-system use the `show security utm content-filtering statistics utm policy <utm policy name>` and `show security utm content-filtering statistics root-logical-system utm-policy <utm policy name>` commands.

- To display content filtering statistics in a policy within a specified logical system use the `show security utm content-filtering statistics logical-system <logical-system-name> utm-policy <utm policy name>` command.

If you migrate to this new feature and if there are legacy options in your configurations, then you will receive the following error messages and commit will fail.

Deprecated features can't go together with enhanced content filtering (rule-set/rule)\n");Remove configuration marked as deprecated to get ahead (For details: show security utm)\n")
You can use legacy content filtering functionality if you don’t want to migrate to the enhanced content filtering feature. The legacy configuration options are deprecated and are hidden. You will receive the following error message when you use the deprecated legacy options.

ERRMSG (“The config \'%s\' is deprecated”, “security utm utm-policy <> content-filtering http-profile")

Benefits

- Provides safe web access and protects your network from attacks using accurately detected file-types in the content filtering rules.
- Controls the traffic that traverses your network and enforces content filtering rules based on traffic direction.
- Improved log messages to include user and source identity, session ID, and packet direction information.

Starting in Junos OS Release 22.4R1, Content Security content filtering module is integrated with the JDPI parser and the JDPI contexts are used to invoke the content filtering functionalities.

Content Security content filtering packet and stream plug-ins are added to handle plain traffic.

While taking actions for mail protocols, TCP proxy dependency is removed. `notify-mail-sender` CLI configuration support is removed for mail protocols.

SEE ALSO

> *content-filtering (Security Content Security Policy)*
>
> *utm*
>
> *utm default-configuration*
>
> Allowlist | 24

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

Content Security Overview | 2

Understanding HTTP Scanning

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 Content Security 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 Content Security custom objects for the feature. See "Example: Configuring Content Filtering Custom Objects" on page 137.

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

3. Configure a Content Security policy for each protocol and attach this policy to a profile. See "Example: Configuring Content Filtering Content Security Policies" on page 141.

4. Attach the Content Security policy to a security policy. See "Example: Attaching Content Filtering Content Security Policies to Security Policies" on page 144.

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 129.

2. Understand the order in which content filtering parameters are configured. See "Content Filtering Configuration Overview" on page 136.

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

IN THIS SECTION

Procedure

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

IN THIS SECTION

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

Allowlist | 24

Example: Configuring Content Filtering Content Security Policies

IN THIS SECTION

This example describes how to create a content filtering Content Security 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 129.
2. Configure Content Security custom objects for each feature and define the content-filtering profile. See "Content Filtering Configuration Overview" on page 136.

Overview

You configure Content Security policies to selectively enforce various Content Security solutions on network traffic passing through a Content Security 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 Content Security policy called utmp4, and then assign the preconfigured feature profile confilter1 to this policy.

Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

To configure a content filtering Content Security policy:

You can configure different protocol applications in the Content Security 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 Content Security policy.

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

2. Attach the Content Security 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

IN THIS SECTION

Verify the Security Content Security Configuration

Purpose

To verify the security Content Security configuration is working properly.

Action

From the operational mode, enter the `show security utm` command.

SEE ALSO

Content Security Overview | 2

Example: Attaching Content Filtering Content Security Policies to Security Policies

IN THIS SECTION

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

Requirements

Before you begin:

1. Configure Content Security custom objects, define the content filtering profile, and create a Content Security policy. See "Content Filtering Configuration Overview" on page 136.
2. Enable and configure a security policy. See *Example: Configuring a Security Policy to Permit or Deny All Traffic*.

Overview

By attaching content filtering Content Security 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 Content Security policy called utmp4 to the security policy p4. This Content Security policy applies to any traffic that matches the criteria specified in the security policy p4.

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly attach a content filtering Content Security 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 Content Security 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 Content Security 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

IN THIS SECTION

Verifying Attaching Content Filtering Content Security Policies to Security Policies

Purpose

Verify the attachment of the content filtering Content Security policy to the security policy.

Action

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

SEE ALSO

Content Security Overview | 2

Monitoring Content Filtering Configurations

IN THIS SECTION

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 Content Security.

RELATED DOCUMENTATION

5

CHAPTER

Web Filtering

Web Filtering Overview

IN THIS SECTION

The Web filtering lets you to manage Internet usage by preventing access to inappropriate Web content. There are three 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 Content Security.

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 Content Security.

RELATED DOCUMENTATION

Understanding Integrated Web Filtering

Understanding Redirect Web Filtering | 222

Understanding the Enhanced Web Filtering Process | 155

Understanding Local Web Filtering | 204

Monitoring Web Filtering Configurations | 248

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

IN THIS SECTION

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 Firewall. 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 Content Security. Content Security extracts the URL from the HTTP request message.

Starting in Junos OS Release 22.2R1, the web filtering uses JDPI-Decoder support for processing the application data. You must enable the JDPI-Decoder to enforce the web filtering functionality.

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

Understanding Local Web Filtering | 204

Understanding Redirect Web Filtering | 222

Understanding the Enhanced Web Filtering Process

IN THIS SECTION

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 Content Security features, is provided for the EWF feature after the license key expires.

  This feature requires a license. Please refer to the Licensing Guide for general information about License Management. Please refer to the product Data Sheets at SRX Series Firewalls 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 Firewall. 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 Content Security. Content Security 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.

Cache Preload for Enhanced Web Filtering

Starting in Junos OS Release 23.2R1, cache is loaded with the top-rated, frequently visited URL list along with the classification information at the system startup stage. This is useful for users with a slow internet connection who experience high latency while accessing the Web due to the remote categorization service. It ensures that there is no lag even when the first request is made as the Web filter policy decision is based on the URL category information that is preloaded in the cache.

Cache is not enabled by default. Ensure that caching is enabled to use this feature. The following configurations are required to enable caching for Enhanced Web Filtering (EWF) and they are available in SRX Series Firewalls.

- `security utm default-configuration web-filtering juniper-enhanced cache timeout`
- `security utm default-configuration web-filtering juniper-enhanced cache size`

Use the following CLI configuration statement options for the Cache Preload for Enhanced Web Filtering:

```
security {
    utm {
        default-configuration {
            web-filtering {
                juniper-enhanced {
                    cache-preload {
                        feed-url <URL>;
                        automatic {
                            interval 1;
                            retry 1;
                            feed-type <server-names-feed>;
                          }
                        }
                      }
                    }
                  }
               }
            }
```

Table 5: Options

feed-url	Used to download an alternate file instead of the default hard-coded file. It is not mandatory. Hard-coded defaults are used if it is not set. Default feed URL: https://update.juniper-updates.net/EWF-CACHE-PRELOAD/ One of the following defaults are used based on the feed type: https://update.juniper-updates.net/EWF-CACHE-PRELOAD/abs_urls_feed.tgz https://update.juniper-updates.net/EWF-CACHE-PRELOAD/server_names_feed.tgz

automatic	Used to set download and preload cache automatically without user interaction.
automatic interval <time-in-hours>	Used to schedule automatic cache preload. It is mandatory if the automatic option is specified.
automatic retry <time-in-hours>	Used to schedule retry if automatic cache preload fails for some reason. It is mandatory if the automatic option is specified.
automatic feed-type <abs-urls-feed or server-names-feed>	Used to specify feed type to use by auto download and preload functions. It is mandatory if the automatic option is specified.

NOTE: You can limit the maximum number of entries in the cache using the following command:

```
set security utm default-configuration web-filtering juniper-enhanced cache size ?
```

Possible completions:

```
<size> Juniper enhanced cache size (0..4096 kilobytes)
```

New operational commands are available from the CLI for the Enhanced Web Filtering Cache Preload feature.

You can use the operational commands to download the URL feed of your choice from the remote server. The Feed-URL option is useful for downloading an alternate file instead of the default hard coded file. Even with the Feed-URL option, server-names-feed option and abs-urls-feed option are required to indicate the type of feed that is available in the package you have specified.

- `request security utm web-filtering cache-preload download abs-urls-feed`
- `request security utm web-filtering cache-preload download server-names-feed`
- `request security utm web-filtering cache-preload download server-names-feed feed-url https://update.juniper-updates.net/EWF-CACHE-PRELOAD/server_names_fp_feed.tgz`
- `request security utm web-filtering cache-preload download abs-urls-feed feed-url https://update.juniper-updates.net/EWF-CACHE-PRELOAD/abs_urls_fp_feed.tgz`

NOTE: The user specified package of type **server-names-feed** must contain the **server_names_feed.csv** and **server_names_feed.ver** files.

The user specified package of type **abs-urls-feed must** contain the **abs_urls_feed.csv** and **abs_urls_feed.ver** files.

The following are the hard coded links. The program chooses a link based on the feed-type.

https://update.juniper-updates.net/EWF-CACHE-PRELOAD/abs_urls_feed.tgz

https://update.juniper-updates.net/EWF-CACHE-PRELOAD/server_names_feed.tgz

Use the following operational commands to trigger the cache preloading using the existing URL feed within the system. These commands load the cache if the package was already installed using the commands for downloading. Use server-names-feed option to preload categorized server names. Use abs-urls-feed to preload categorized URL feed.

- `request security utm web-filtering cache-preload load-active-local server-names-feed`
- `request security utm web-filtering cache-preload load-active-local abs-urls-feed`

Use the following to download, install the default URL feed from remote server, and also load the cache. Use server-names-feed option to download categorized server names. Use abs-urls-feed to download categorized URL feed.

- `request security utm web-filtering cache-preload load-active server-names-feed`
- `request security utm web-filtering cache-preload load-active abs-urls-feed`

To check the status of the cache preload function, use the following command:

```
user@host> show security utm web-filtering cache-preload status
```

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.

Intelligent Web Filtering Profile Selection

Starting in Junos OS Release 23.2R1, dynamic app information from JDPI is used to retrieve policy information before the final policy match is done. The Web Filter profile is updated again after the final policy selection based on the final application match.

The Content Security profile that is retrieved based on the dynamic app information is more accurate than applying the default profile, which was the earlier approach.

The dynamic app-based policy detection is now the default behavior. The following knob is added in the Web Filtering default configuration hierarchy to disable the dynamic app profile detection feature if required.

```
set security utm default-configuration web-filtering disable-dynapp-profile-selection
```

To make one of the Content Security policy as default, the following command is introduced:

```
set security utm default-policy <pol_name>
```

You can choose any Content Security policy as the default policy by using this command. If the default policy is configured in a unified multi-policy configuration scenario, the default Content Security Web Filtering policy is used. If it is not configured, junos-default-utm-policy is used as the default policy.

NOTE: The default policy changes apply only to Web Filtering and not to Content Filtering, Antivirus, or Antispam.

The following CLI command is used to display the configuration of dynapp-profile-selection:

```
show security utm web-filtering status
```

Content Security Web-filtering status:

```
Server status: Juniper Enhanced using Websense server UP
```

```
JDPI Parser : Enabled
```

```
Dynapp-profile-selection: Enabled
```

Use the following command to display the debug counter values for policy lookup activities:

```
show security utm l7-app-policy statistics
```

New counters are added to the web filtering statistics for debugging.

Table 6: New Counters Added to Web Filtering Statistics

Sessions matched with dynapp policy	Increases whenever the policy associated with a uf_ng session changes based on the newly identified app-id.
Sessions matched with default policy	Increases when the Content Security policy action taken for a connection is based on the user configured default policy. This counter increases when the user configured default policy is same as the policy identified by new dynamic-app or when the user configured default policy has a valid Content Security Web Filtering profile and the no policy has matched with existing firewall policy.

Sessions matched with final policy	Increases when action is taken on an Content Security policy without any conflict of policies.

NOTE: Use the `show services application-identification application-system-cache` command to check the dynamic application identified by AppID module.

SEE ALSO

Web Filtering Overview | 151

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 Content Security custom objects for the Content Security 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 Content Security 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 Content Security 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

category (Security Web Filtering)

request security utm web-filtering category install

show security utm web-filtering category base-filter

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 Firewalls. 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 Firewall 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 151 and "Understanding Enhanced Web Filtering Process" on page 155.

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 Content Security policy, and finally attach the Web filtering Content Security policies to the security policies. Table 7 on page 171 shows information about EWF configuration type, steps, and parameters used in this example.

Table 7: 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. 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] • value urllist3 • http://www.untrusted.com • http://www.trusted.com
	Add the urllist3 custom object to the custom URL category custurl3.	• `urllistblack` • `urllistwhite`
Feature profiles	Configure the Web filtering feature profile:	

Table 7: Enhanced Web filtering (EWF) Configuration Type, Steps, and Parameters *(Continued)*

Configuration Type	Configuration Steps	Configuration Parameters
	• 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` • `custblacklist` • `juniper-enhanced` • `cache size 500` • `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` • `port 80` • `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` • `http-persist` • `Action: log-and-permit` • `site-reputation-action:` • `very-safe permit`

Table 7: Enhanced Web filtering (EWF) Configuration Type, Steps, and Parameters *(Continued)*

Configuration Type	Configuration Steps	Configuration Parameters

	• Enter a custom message to be sent when HTTP requests are blocked. Finally, enter a timeout value in seconds.	• `ewf_my_profile-default block`
		• `custom-block-message "***access denied ***"`
		• `fallback-settings:`
		  • `server-connectivity block`
		  • `timeout block`
		  • `too-many-requests block`
		• `quarantine-custom-message “**The requested webpage is blocked by your organization's access policy**”.`
		• `quarantine-message type custom-redirect-url`
		• `quarantine-message url besgas.spglab.example.net`
		• `ewf_my_profile-default:`
		  • `timeout 10`
		  • `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]
user@host# 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.

```
set security utm default-configuration web-filtering juniper-enhanced
set security utm default-configuration web-filtering juniper-enhanced cache size 500
set security utm default-configuration web-filtering juniper-enhanced cache timeout 1800
set security utm default-configuration web-filtering juniper-enhanced server host
rp.cloud.threatseeker.com
set security utm default-configuration web-filtering juniper-enhanced server port 80
set security utm default-configuration web-filtering http-reassemble
set security utm default-configuration 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 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
```

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 EWF engine and set the cache size and cache timeout parameters.

```
[edit security utm default-configuration web-filtering]
user@host# set juniper-enhanced cache size 500
user@host# set juniper-enhanced cache timeout 1800
```

2. 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 default-configuration web-filtering]
user@host# set juniper-enhanced server host rp.cloud.threatseeker.com
user@host# set juniper-enhanced server port 80
```

3. 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 default-configuration web-filtering]
user@host# set http-reassemble
user@host# set http-persist
```

4. 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
```

5. Specify a default action for the profile, when no other explicitly configured action is matched.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf_my_profile default block
```

6. 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
```

7. 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.

8. Configure a Content Security policy (mypolicy) for the Web-filtering HTTP protocol, associating ewf_my_profile to the Content Security 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
default-configuration {
    web-filtering {
        http-reassemble;
        http-persist;
        juniper-enhanced {
            cache {
                timeout 1800;
                size 500;
            }
            server {
                host rp.cloud.threatseeker.com;
                port 80;
            }
        }
    }
}
feature-profile {
 web-filtering {
    http-reassemble;
    http-persist;
    juniper-enhanced {
        profile ewf_my_profile {
            category {
                Enhanced_Hacking {
                    action log-and-permit;
                    }
                    Enhanced_Government {
                    action quarantine;
                }
            }
            site-reputation-action {
                very-safe permit;
            }
            default block;
```

```
            fallback-settings {
                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 Content Security 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 Content Security 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 Content Security 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 Content Security Policy Is Attached to the Security Policy

Purpose

Verify that the Web filtering Content Security 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 Content Security is enabled, then mypolicy is attached to sec_policy.

SEE ALSO

Web Filtering Overview | 151

Monitoring Web Filtering Configurations | 248

Understanding the Quarantine Action for Enhanced Web Filtering

IN THIS SECTION

Content Security Enhanced Web Filtering supports block, log-and-permit, and permit actions for HTTP/HTTPS requests. In addition to this, Content Security 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 Content Security 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 Content Security 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

Understanding Local Web Filtering | 204

Understanding Redirect Web Filtering | 222

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 151 and "Understanding Enhanced Web Filtering Process" on page 155.

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

IN THIS SECTION

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 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. 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
```

2. 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.

3. Set the cache timeout parameters.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced cache timeout 1
```

4. 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
```

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 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
```

6. 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 ***"
```

7. 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
```

8. 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 {

    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 Content Security Service

Purpose

Verify the Content Security service status.

Action

From operational mode, enter the `show security utm status` command.

Sample Output

command-name

```
user@host>show security utm status
UTM service status: Running
```

Verifying the Status of Content Security Session

Purpose

Verify the Content Security session status.

Action

From operational mode, enter the `show security utm session` command.

Sample Output

command-name

```
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 Content Security Web Filtering

Purpose

Verify the Content Security Web filtering status.

Action

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

Sample Output

command-name

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

Verifying the Statistics of Content Security 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

command-name

```
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 Content Security 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

command-name

```
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

Allowlist | 24

TAP Mode Support Overview for Content Security

In TAP mode, an SRX Series Firewall will be connected to a mirror port of the switch, which provides a copy of the traffic traversing the switch. An SRX Series Firewall 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 Content Security module. When you enable TAP mode on Content Security module, the SRX Series Firewall inspects the incoming and outgoing traffic that matches a firewall policy or policies with the enabled Content Security 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 Content Security terminates the connection, and the TAP mode do not generate any security logs, reports, and statistics for this connection. The Content Security configuration remains the same as non-TAP mode.

Content Security functionality configured on an SRX Series Firewall continues to work and exchange information from the server. To use Content Security functionality when the SRX Series Firewall 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 Series Firewall will be connected to a mirror port of the switch, which provides a copy of the traffic traversing the switch. SRX Series Firewall 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 Firewall 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
>
> Example: Configuring Security Flow Sessions in TAP mode
>
> [SRX] Example - Configuring TAP Mode Interface
>
> https://www.juniper.net/documentation/us/en/software/junos/utm/topics/ref/statement/security-utm-default-configuration.html

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 Firewall.
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 Firewall. 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 Content Security. Content Security 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

Monitoring Web Filtering Configurations | **248**

Redirect Web Filtering | **221**

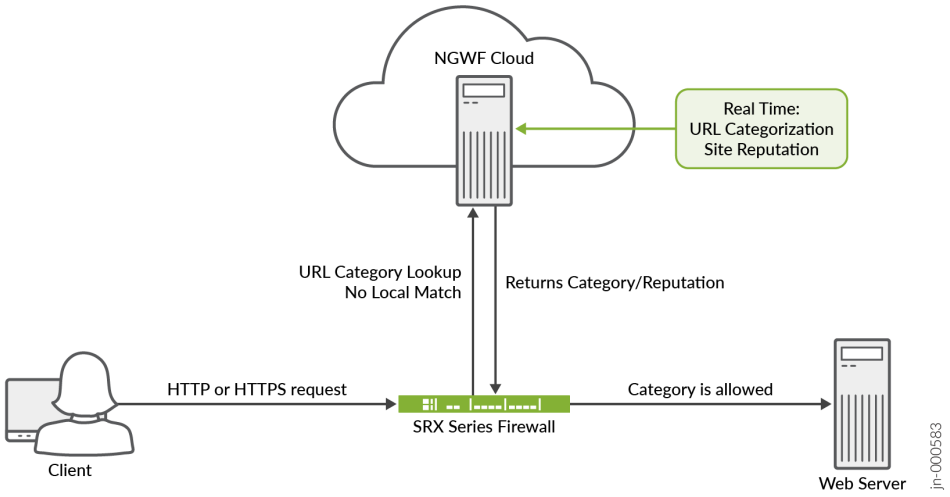
Juniper NextGen Web Filtering Overview

IN THIS SECTION

Juniper NextGen Web Filtering (NGWF) acts as a first line of defense by enabling the SRX Series Firewall to permit or deny access to specific URLs based on the reputation and category to which the URLs belong. It intercepts, scans, and acts upon HTTP or HTTPS traffic to prevent inappropriate Web content access. It also provides better visibility into the URL traffic.

Let's learn how NGWF works.

Figure 4: Juniper NextGen Web Filtering



1. SRX Series Firewall receives HTTP/HTTPS traffic.
2. The NGWF intercepts the HTTP/HTTPS traffic and sends the URL or the destination IP address to the Juniper NGWF cloud. The NGWF cloud hosts the Web filtering service across the globe and delivers the services to all the different users around the world.

3. The NGWF cloud categorizes the URL into one of the categories. It also provides the site reputation information.
4. The NGWF cloud shares the URL categorization and site reputation information with the SRX Series Firewall. The device stores the result as cache for a faster look up for the subsequent look ups.
5. Based on the URL categorization and site reputation information, the SRX Series Firewall permits or blocks the traffic as per the configured policy.

The NGWF provides the re-categorization and categorization features. You can request to recategorize incorrectly categorized URLs and submit uncategorized URLs. Use the following commands to recategorize or categorize a URL:

- `request security utm web-filtering recategorize`
- `request security utm web-filtering categorize`

Use the `request security utm web-filtering recategorize url <url> status` command to view the status of your recategorization request.

Starting in Junos OS Release 23.4R1, the SRX Series Firewall license installs have the NGWF license by default. Customers using the Enhanced Web Filtering (EWF) have an option to manually migrate from the existing EWF to the NGWF. The EWF and the NGWF require separate licenses. You can also migrate to Juniper NGWF with your current Websense license.

Starting in Junos OS Release 23.4R1, during new installs or in case of an upgrade, the wf_key_ng_juniper key is installed. Juniper NextGen Web Filtering and URL category download and installation work when wf_key_websense_ewf or wf_key_ng_juniper is present.

Starting in Junos OS Release 23.4R1, you can use Juniper NextGen Web Filtering feature with wf_key_ng_juniper key.

You can configure the NGWF using:

- CLI. See CLI Support for Juniper NextGen Web Filtering.
- J-Web. See *Content Security Default Configuration chapter* in the *J-Web User Guide for SRX Series Devices*.

Differences Between NGWF and EWF

Table 1 describes the key differences between Juniper NGWF and EWF.

Table 8: Differences Between NGWF and EWF

Functionality	NGWF	EWF
Cloud support	Juniper URL filtering acts as the gateway for SRX Series Firewall seeking URL category/reputation from Juniper NGWF cloud.	URL requests directly go to vendor cloud from SRX Series Firewall.
URL categorization	Provides the URL re-categorization and categorization features.	Customers cannot perform URL re-categorization and categorization.
URL categorization status	Enables the customers to view the URL re-categorization status.	Customers cannot perform URL re-categorization directly.
URL traffic visibility	Provides better visibility into the URL traffic and use the rich telemetry into actionable best practices or automated orchestration for customers.	Less visibility on the customer URL traffic.
Regional language support	Provides more than 200 regional language support.	Provides less regional language support.
Site reputation	You need not provide a site reputation range of a URL to block or permit the URL.	You can configure the site reputation range value of a URL to block or permit the URL.

Benefits of NGWF

- Granular control on the Web filtering.
- URL categories are available in the Juniper NGWF cloud.
- More regional language support.
- Enables users to recategorize and categorize URLs, which reduces the dependency on the Juniper support team to recategorize and categorize URLs.

RELATED DOCUMENTATION

Web Filtering Overview

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 Firewall. 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 and HTTPS 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 and HTTPS request in the TCP connection.
3. The device extracts each URL in the HTTP and HTTPS 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 or https 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 Content Security 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 Content Security 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 | 151

Redirect Web Filtering | 221

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 151.

Overview

In this example you configure local Web filtering custom objects, local Web filtering feature profiles, and local Web filtering Content Security policies. You also attach local Web filtering Content Security policies to security policies. Table 9 on page 209 shows information about local Web filtering configuration type, steps, and parameters used in this example.

Table 9: 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. Create a custom object called urllis1 that contains the pattern [http://www.example1.net 192.0.2.0] Create a custom object called urllist2 that contains the pattern [http://www.example2.net 192.0.2.3] Create a custom object called urllist3 that contains the pattern [http://www.example3.net 192.0.2.9] 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] • [http://www.example2.net 192.0.2.3] • [http://www.example3.net 192.0.2.9] • [http://www.example4.net 192.0.2.8] • `value urllist3` • `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` • `value urllist2`
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` • `custurl4` • `type juniper-local`

Table 9: Local Web filtering Configuration Type, Steps, and Parameters *(Continued)*

Configuration Type	Configuration Steps	Configuration Parameters
	• 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` • `Action: block` • `Action: log-and-permit` • `cust-black-list` • `cust-permit-list`

	• Define redirect url. Enter a custom message to be sent when HTTP and HTTPS requests are blocked.
	• 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`
		• `block-message url 192.0.2.10`
		• `custom-block-message “**Access to this site is not permitted**”.`
		• `fallback-settings:`
		  • `block`
		  • `log-and-permit`

Content Security policies	Create the Content Security policy `utmp5` and attach it to the profile `localprofile1`. In the final configuration example, attach the Content Security policy `utmp5` to the security policy `p5`.	• `utm policy utmp5` • `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 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. 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
```

2. 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
```

3. Enter a custom message to be sent when HTTP or HTTPS 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”
```

4. 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
```

5. 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 {
    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 Content Security 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 Content Security policy:

1. Create the Content Security policy referencing a profile. Apply the Web filtering profile to the Content Security 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 Content Security 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 Content Security 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 Content Security 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

- Verifying the Statistics of Content Security Web Filtering | 220

To confirm that the configuration is working properly, perform the following task:

Verifying the Statistics of Content Security 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

command-name

```
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 | 224

Monitoring Web Filtering Configurations | 248

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 Content Security 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 Content Security 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 | 153

Allowlist | 24

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

IN THIS SECTION

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 | 151

Understanding Local Web Filtering | 204

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 151.

Overview

IN THIS SECTION

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 Content Security policies. You also attach redirect Web filtering Content Security policies to security policies.

The default websense-redirect server port number is 15868.

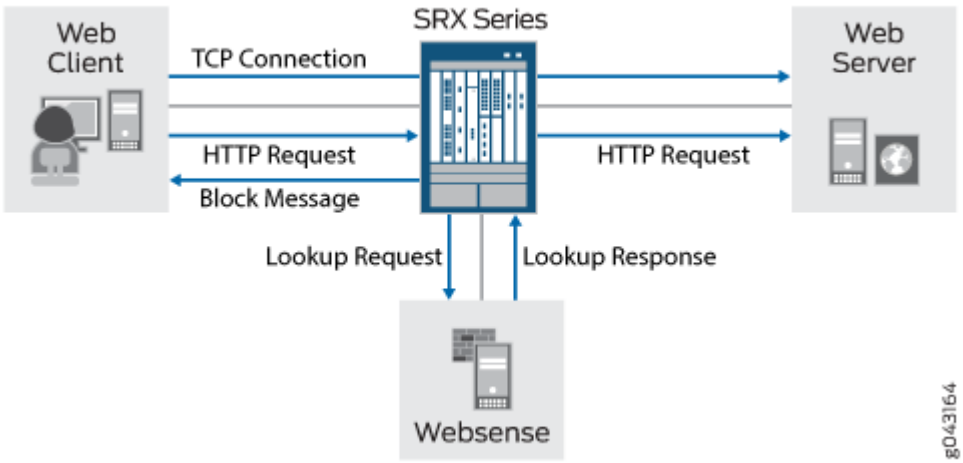
You select fallback settings (block or log-and-permit) for this profile, in case errors occur in each configured category. This example sets fallback settings to block the profile. You enter the number of sockets used for communicating between the client and the server. The default is 32 for SRX Series Firewalls.

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.

Topology

Figure 5 on page 225 shows the overall architecture for the Websense redirect feature.

Figure 5: 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 Content Security Policies and Attaching the Redirect Web Filtering Content Security 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 Content Security policy and attach it to a security policy:

1. Create the Content Security 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 Content Security 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 Content Security Policies to Security Policies

Purpose

Verify the attachment of the newly created redirect Web filtering Content Security 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 Content Security policies are attached.

SEE ALSO

Example: Configuring Enhanced Web Filtering | 170

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 | 153

Monitoring Web Filtering Configurations | 248

Safe Search Enhancement for Web Filtering

SUMMARY

Learn about our safe search enhancement for Content Security Web filtering solutions to enforce the safest Web browsing mode available, by default.

IN THIS SECTION

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.

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 Content Security 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 Content Security Web filtering solutions to provide an extremely safe search environment for the Web user. Table 10 on page 240 describes the features of the safe search enhancement.

Table 10: 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.
	
	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.
	
	Here're a few examples of requested and converted URLs:
	
	• Google search engine:
	  • Requested URL: https://www.google.com/search?q=test
	  • Converted URL: https://www.google.com/search?q=test&safe=active
	• Bing search engine:
	  • Requested URL: https://www.bing.com/search?q=test
	  • Converted URL: https://www.bing.com/search?q=test&adlt=strict
	• Yahoo search engine:
	  • Requested URL: https://search.yahoo.com/search?q=test
	  • Converted URL: https://search.yahoo.com/search?q=test&vm=r
	• Yandex search engine:
	  • Requested URL: https://yandex.com/search/?text=test&lr=10619
	  • 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. 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 Content Security Web filtering solutions and verify the safe search enhancement for Content Security Web filtering.

IN THIS SECTION

Requirements

This example uses the following hardware and software components:

- An SRX Series Firewall
- 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

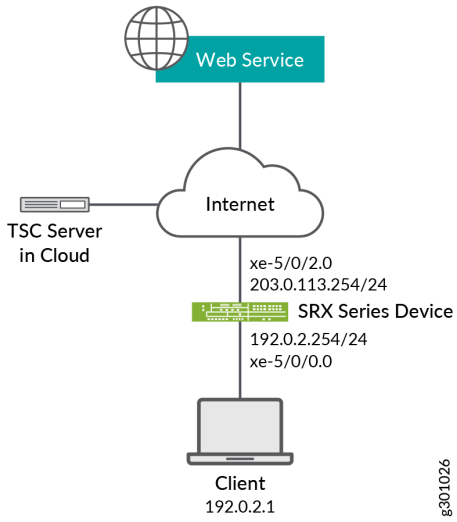
In this example, you configure the following policies and Web filtering profiles on your security device:

- Content Security 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 6 on page 242 shows the basic Content Security 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 6: Topology for Web Filtering Basic Function



Configuration

IN THIS SECTION

- Procedure | 243

Procedure

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 Content Security Web filtering:

1. Configure Content Security Web filtering 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

IN THIS SECTION

Verify Safe Search Function

Purpose

Verify that the safe search feature is enabled for Content Security 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.

Monitoring Web Filtering Configurations

IN THIS SECTION

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 | 151

Example: Configuring Enhanced Web Filtering | 170

CHAPTER 6

Configuration Statements and Operational Commands

Junos CLI Reference Overview

We've consolidated all Junos CLI commands and configuration statements in one place. Learn about the syntax and options that make up the statements and commands and understand the contexts in which you'll use these CLI elements in your network configurations and operations.

- Junos CLI Reference

Click the links to access Junos OS and Junos OS Evolved configuration statement and command summary topics.

- Configuration Statements
- Operational Commands