UTM Feature Guide for NFX Devices

Modified: 2019-05-12

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

UTM Feature Guide for NFX Devices

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About the Documentation xv
Documentation and Release Notes xv
Using the Examples in This Manual xv
Merging a Full Example xvi
Merging a Snippet xvi
Documentation Conventions xvii
Documentation Feedback xix
Requesting Technical Support xix
Self-Help Online Tools and Resources xx
Creating a Service Request with JTAC xx

Chapter 1 **Overview 21**

UTM Overview 21
Unified Threat Management Overview 21
Understanding UTM Custom Objects 22
Understanding WELF Logging for UTM Features 22
Example: Configuring WELF Logging for UTM Features 23
Licensing Requirements for UTM Features on NFX Devices 26

Chapter 2 **Antivirus Protection 27**

Sophos Antivirus Protection on NFX Devices 27
Sophos Antivirus Protection Overview 27
Sophos Antivirus Features 28
Understanding Sophos Antivirus Data File Update 29
Sophos Antivirus Configuration Overview 30
Configuring Sophos Antivirus Custom Objects 30
Configuring Sophos Antivirus Feature Profile 31
Configuring Sophos Antivirus UTM Policies 35
Configuring Sophos Antivirus Firewall Security Policies 36
Managing Sophos Antivirus Data Files 37

Chapter 3 **Whitelists 39**

Whitelists 39
Understanding MIME Whitelists 39
Example: Configuring MIME Whitelists to Bypass Antivirus Scanning 40
Understanding URL Whitelists 40
Configuring URL Whitelists to Bypass Antivirus Scanning (CLI Procedure) 41
HTTP Trickling on NFX Devices 41
Understanding HTTP Trickling 42
Configuring HTTP Trickling on NFX Devices 42

Chapter 4 Antispam Filtering 43

Antispam Filtering Overview 43
Antispam Filtering Overview 43
Handling Spam Messages 43
Server-Based Antispam Filtering 44
Understanding Server-Based Antispam Filtering 45
Server-Based Antispam Filtering Configuration Overview 46
Example: Configuring Server-Based Antispam Filtering 47
Local-List Antispam Filtering 53
Understanding Local List Antispam Filtering 53
Local List Antispam Filtering Configuration Overview 54
Example: Configuring Local List Antispam Filtering 55

Chapter 5 Content Filtering 63

Content Filtering 63
Content Filtering Overview 63
Understanding Content Filtering Protocol Support 64
HTTP Support 65
FTP Support 65
E-Mail Support 65
Specifying Content Filtering Protocols (CLI Procedure) 66
Content Filtering Configuration Overview 66
Example: Configuring Content Filtering Custom Objects 67
Example: Configuring Content Filtering UTM Policies 70
Example: Attaching Content Filtering UTM Policies to Security Policies 71
Monitoring Content Filtering Configurations 74

Chapter 6 Web Filtering 77

Web Filtering Overview 77
Server Name Indication (SNI) Support 79
Enhanced Web Filtering 80
Enhanced Web Filtering Overview 80
User Messages and Redirect URLs for Enhanced Web Filtering (EWF) on SRX Series Devices 81
Understanding the Enhanced Web Filtering Process 82
Functional Requirements for Enhanced Web Filtering 83
User Messages and Redirect URLs for Enhanced Web Filtering (EWF) on SRX Series Devices 88
Predefined Category Upgrading and Base Filter Configuration Overview . . . 89
Example: Configuring Enhanced Web Filtering 90
Understanding the Quarantine Action for Enhanced Web Filtering 104
User Messages and Redirect URLs for Enhanced Web Filtering (EWF) on SRX Series devices 105
Example: Configuring Site Reputation Action for Enhanced Web Filtering 106

SRX TAP Mode Support Overview . . . 112
Local Web Filtering . . . 116
Understanding Local Web Filtering . . . 116
Local Web Filtering Process . . . 117
User-Defined Custom URL Categories . . . 117
Local Web Filtering Profiles . . . 118
User Messages and Redirect URLs for Web Filtering on SRX Series devices . . . 118
Profile Matching Precedence . . . 119
Example: Configuring Local Web Filtering . . . 119
Redirect Web Filtering . . . 129
Understanding Redirect Web Filtering . . . 129
User Messages and Redirect URLs for Web Filtering on SRX Series devices . . . 130
Dynamic Support for New Websense EWF Categories . . . 131
Example: Enhancing Security by Configuring Redirect Web Filtering Using Custom Objects . . . 131
Monitoring Web Filtering Configurations . . . 142

Chapter 7 Configuration Statements . . . 143

action (Security UTM Web Filtering) . . . 149
address-blacklist . . . 150
address-whitelist . . . 150
admin-email . . . 151
administrator-email (Security Fallback Block) . . . 152
administrator-email (Security Virus Detection) . . . 153
allow-email (Security Fallback Block) . . . 154
allow-email (Security Virus Detection) . . . 154
application (Security Policies) . . . 155
application-proxy (Security UTM) . . . 156
anti-spam (Security Feature Profile) . . . 157
anti-spam (Security UTM Policy) . . . 158
anti-virus (Security Feature Profile) . . . 159
anti-virus (Security UTM Policy) . . . 162
block-command . . . 163
block-content-type . . . 163
block-extension . . . 164
block-message (Security UTM) . . . 164
block-mime . . . 165
cache . . . 166
category (Security Logging) . . . 167
category (Security Web Filtering) . . . 169
content-filtering (Security Feature Profile) . . . 176
content-filtering (Security UTM Policy) . . . 178
content-size . . . 179
content-size (Security Antivirus Sophos Engine) . . . 180
content-size-limit . . . 181
corrupt-file . . . 182
custom-block-message . . . 183

custom-message (Security Content Filtering) . . . 183
custom-message (Security Email Notify) . . . 184
custom-message (Security Fallback Block) . . . 185
custom-message (Security Fallback Non-Block) . . . 186
custom-message (Security Virus Detection) . . . 187
custom-message-subject (Security Email Notify) . . . 188
custom-message-subject (Security Fallback Block) . . . 189
custom-message-subject (Security Fallback Non-Block) . . . 190
custom-message-subject (Security Virus Detection) . . . 191
custom-objects . . . 192
custom-tag-string . . . 193
custom-url-category . . . 194
decompress-layer . . . 195
decompress-layer-limit . . . 196
default (Security Antivirus) . . . 197
default (Security Antivirus Sophos Engine) . . . 198
default (Security UTM) . . . 199
default (Security Web Filtering) . . . 200
display-host (Security Fallback Block) . . . 201
display-host (Security Virus Detection) . . . 201
download-profile (Security Antivirus FTP) . . . 202
download-profile (Security Content Filtering FTP) . . . 202
email-notify . . . 203
engine-not-ready . . . 204
engine-not-ready (Security Antivirus Sophos Engine) . . . 205
exception (Security Antivirus Mime Whitelist) . . . 206
exception (Security Content Filtering) . . . 206
fallback-block (Security Antivirus) . . . 207
fallback-non-block (Security Antivirus) . . . 208
fallback-options (Security Antivirus Juniper Express Engine) . . . 209
fallback-options (Security Antivirus Kaspersky Lab Engine) . . . 210
fallback-options (Security Antivirus Sophos Engine) . . . 211
fallback-settings (Security Web Filtering) . . . 212
fallback-settings (Security Web Filtering Juniper Local) . . . 213
fallback-settings (Security Web Filtering Websense Redirect) . . . 214
feature-profile . . . 215
filename-extension . . . 222
flag (SMTP) . . . 223
format (Security Log Stream) . . . 224
from-zone (Security Policies) . . . 225
ftp (UTM Policy Anti-Virus) . . . 228
ftp (UTM Policy Content Filtering) . . . 229
host (Security Web Filtering) . . . 230
http-profile (Security Antivirus) . . . 230
http-profile (Security Content Filtering) . . . 231
http-profile (Security Web Filtering) . . . 231
imap-profile (Security UTM Policy Antivirus) . . . 232
imap-profile (Security UTM Policy Content Filtering) . . . 232
http-persist . . . 233

http-reassemble . . . 234
intelligent-prescreening . . . 235
interval (Security Antivirus) . . . 236
ipc . . . 237
juniper-enhanced . . . 238
juniper-express-engine . . . 240
juniper-local . . . 242
kaspersky-lab-engine . . . 243
limit (UTM Policy) . . . 245
list (Security Antivirus Mime Whitelist) . . . 245
list (Security Content Filtering Block Mime) . . . 246
log (Security) . . . 247
mime-pattern . . . 251
mime-whitelist . . . 252
no-autoupdate . . . 253
no-intelligent-prescreening . . . 254
no-notify-mail-recipient . . . 255
no-notify-mail-sender (Security Content Filtering Notification Options) . . . 256
no-notify-mail-sender (Security Fallback Block) . . . 257
no-notify-mail-sender (Security Virus Detection) . . . 258
no-sbl-default-server . . . 259
notification-options (Security Antivirus) . . . 260
notification-options (Security Content Filtering) . . . 261
notify-mail-recipient . . . 262
notify-mail-sender (Security Content Filtering Notification Options) . . . 263
notify-mail-sender (Security Fallback Block) . . . 264
notify-mail-sender (Security Virus Detection) . . . 265
no-uri-check . . . 266
out-of-resources . . . 267
out-of-resources (Security Antivirus Sophos Engine) . . . 268
over-limit . . . 269
packet-filter . . . 270
password (Security Antivirus) . . . 271
password-file . . . 272
pattern-update (Security Antivirus) . . . 273
permit-command . . . 274
policies . . . 275
pop3-profile (Security UTM Policy Antivirus) . . . 280
pop3-profile (Security UTM Policy Content Filtering) . . . 280
port (Security Antivirus) . . . 281
port (Security Web Filtering Server) . . . 281
primary-server . . . 282
profile (Security Antispam SBL) . . . 283
profile (Security Antivirus Juniper Express Engine) . . . 284
profile (Security Antivirus Kaspersky Lab Engine) . . . 286
profile (Security Content Filtering) . . . 288
profile (Security Sophos Engine Antivirus) . . . 289
profile (Security Web Filtering Juniper Enhanced) . . . 291
profile (Security Web Filtering Juniper Local) . . . 292

profile (Security Web Filtering Websense Redirect) . . . 293
protocol-command . . . 294
proxy (Security Antivirus) . . . 295
quarantine-message (Security UTM) . . . 296
routing-instance (Security UTM) . . . 297
sbl . . . 298
sbl-default-server . . . 298
scan-extension . . . 299
scan-mode . . . 300
scan-options (Security Antivirus Juniper Express Engine) . . . 301
scan-options (Security Antivirus Kaspersky Lab Engine) . . . 302
scan-options (Security Antivirus Sophos Engine) . . . 303
secondary-server . . . 304
server (Security Antivirus) . . . 304
server (Security Sophos Engine Antivirus) . . . 305
server (Security Web Filtering) . . . 306
server-connectivity . . . 307
sessions-per-client . . . 308
site-reputation-action . . . 309
size (Security Web Filtering Cache) . . . 310
smtp-profile (Security UTM Policy Antispam) . . . 310
smtp-profile (Security UTM Policy Antivirus) . . . 311
smtp-profile (Security UTM Policy Content Filtering) . . . 311
sockets . . . 312
sophos-engine . . . 313
spam-action . . . 315
sxl-retry . . . 316
sxl-timeout . . . 316
timeout (Security Antivirus Fallback Options) . . . 317
timeout (Security Antivirus Fallback Options Sophos Engine) . . . 318
timeout (Security Antivirus Scan Options) . . . 319
timeout (Security Web Filtering) . . . 319
timeout (Security Web Filtering Cache) . . . 320
timeout (Security Web Filtering Fallback Settings) . . . 321
too-many-requests (Security Antivirus Fallback Options) . . . 322
too-many-requests (Security Antivirus Fallback Options Sophos Engine) . . . 323
too-many-requests (Security Web Filtering Fallback Settings) . . . 324
to-zone (Security Policies) . . . 325
traceoptions (Security Antispam) . . . 327
traceoptions (Security Antivirus) . . . 328
traceoptions (Security Application Proxy) . . . 329
traceoptions (Security Content Filtering) . . . 330
traceoptions (Security UTM) . . . 331
traceoptions (Security Web Filtering) . . . 332
traceoptions (SMTP) . . . 333
traffic-options . . . 334
trickling . . . 335
type (Security Antivirus Feature Profile) . . . 336
type (Security Content Filtering Notification Options) . . . 336

type (Security Fallback Block) . . . 337
type (Security Virus Detection) . . . 338
type (Security Web Filtering) . . . 339
upload-profile (Security Antivirus FTP) . . . 339
upload-profile (Security Content Filtering FTP) . . . 340
uri-check . . . 340
url (Security Antivirus) . . . 341
url-blacklist . . . 341
url-pattern . . . 342
url-whitelist (Security Antivirus) . . . 343
url-whitelist (Security Web Filtering) . . . 343
username (Security Antivirus) . . . 344
utm . . . 345
utm-policy . . . 353
utm-policy (Application Services) . . . 354
virus-detection (Security Antivirus) . . . 355
web-filtering . . . 356
websense-redirect . . . 361

Chapter 8 Operational Commands . . . 363

clear security utm anti-spam statistics . . . 364
clear security utm antivirus statistics . . . 366
clear security utm content-filtering statistics . . . 368
clear security utm session . . . 370
clear security utm web-filtering statistics . . . 371
request security utm anti-virus juniper-express-engine . . . 373
request security utm anti-virus kaspersky-lab-engine . . . 374
request security utm anti-virus sophos-engine . . . 375
request security utm web-filtering category install . . . 376
request security utm web-filtering category uninstall . . . 377
request security utm web-filtering category download-install [version] . . . 378
request security utm web-filtering category download [version] . . . 379
show configuration smtp . . . 380
show groups junos-defaults . . . 381
show security log . . . 382
show security policies . . . 385
show security utm anti-spam statistics . . . 398
show security utm anti-spam status . . . 401
show security utm anti-virus statistics . . . 402
show security utm anti-virus status . . . 406
show security utm content-filtering statistics . . . 408
show security utm session . . . 410
show security utm status . . . 411
show security utm web-filtering category base-filter . . . 412
show security utm web-filtering category category . . . 415
show security utm web-filtering category status . . . 417
show security utm web-filtering statistics . . . 418
show security utm web-filtering status . . . 422

List of Figures

Chapter 6 Web Filtering 77
Figure 1: Websense Redirect Architecture 133

List of Tables

About the Documentation xv

Table 1: Notice Icons xvii
Table 2: Text and Syntax Conventions xviii

Chapter 1 Overview 21

Table 3: UTM Feature Subscription Service License Requirements 26

Chapter 6 Web Filtering 77

Table 4: Enhanced Web filtering (EWF) Configuration Type, Steps, and Parameters 91
Table 5: Local Web filtering Configuration Type, Steps, and Parameters 120

Chapter 7 Configuration Statements 143

Table 6: List of Categories Predefined by Websense 170

Chapter 8 Operational Commands 363

Table 7: show configuration smtp 380
Table 8: show security log Output Fields 383
Table 9: show security policies Output Fields 387

About the Documentation

- Documentation and Release Notes on page xv
- Using the Examples in This Manual on page xv
- Documentation Conventions on page xvii
- Documentation Feedback on page xix
- Requesting Technical Support on page xix

Documentation and Release Notes

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

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

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

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric** *metric***>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(***string1* **|** *string2* **|** *string3***)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [** *community-ids* **]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

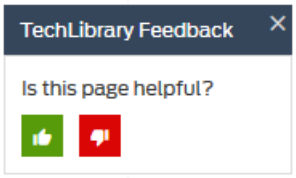
Table 2: Text and Syntax Conventions (continued)

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

Documentation Feedback

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

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



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.

- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

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

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

Creating a Service Request with JTAC

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

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

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

CHAPTER 1

Overview

- UTM Overview on page 21
- Licensing Requirements for UTM Features on NFX Devices on page 26

UTM Overview

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

- Unified Threat Management Overview on page 21
- Understanding WELF Logging for UTM Features on page 22
- Example: Configuring WELF Logging for UTM Features on page 23

Unified Threat Management Overview

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

The security features provided as part of the UTM solution for NFX devices 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 two types of Web filtering solutions. The redirect Web filtering solution intercepts HTTP requests and forwards the server URL to an external URL filtering server provided by Websense to determine whether to block or permit the requested Web access. Redirect Web filtering does not require a separate license. With Juniper Local Web Filtering, the decision-making for blocking or permitting Web access is done on the device after it identifies the category for a URL from user-defined categories stored on the device. With Local filtering, there is no additional Juniper license or remote category server required.
- Sophos Antivirus—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. Sophos antivirus is as an in-the-cloud antivirus solution. The virus pattern and malware database is located on external servers maintained by Sophos (Sophos Extensible List) servers, thus there is no need to download and maintain large pattern databases on the Juniper device. The Sophos antivirus scanner also uses a local internal cache to maintain query responses from the external list server to improve lookup performance.

NOTE: **The sessions-per-client limit CLI command, which imposes a session throttle to prevent a malicious user from generating large amounts of traffic simultaneously, supports the antispam, content filtering, and antivirus UTM features. It does not support Web filtering.**

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

Understanding UTM Custom Objects

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

The following UTM features make use of certain custom objects:

- Anti-Spam (see "Server-Based Antispam Filtering Configuration Overview" on page 46)
- Content Filtering (see "Content Filtering Configuration Overview" on page 66)

Understanding WELF Logging for UTM Features

UTM features support the WELF standard. The WELF Reference defines the WebTrends industry standard log file exchange format. Any system logging to this format is compatible

with Firewall Suite 2.0 and later, Firewall Reporting Center 1.0 and later, and Security Reporting Center 2.0 and later.

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

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

The following is a sample WELF record:

```
id=firewall time="2000-2-4 12:01:01" fw=192.168.0.238 pri=6 rule=3 proto=http

       src=192.168.0.23 dst=6.1.0.36 rg=www.example.com/index.html op=GET
result=0
       rcvd=1426
```

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

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

Example: Configuring WELF Logging for UTM Features

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

- Requirements on page 23
- Overview on page 23
- Configuration on page 24
- Verification on page 25

Requirements

Before you begin, review the fields used to create a WELF log file and record. See *Understanding WELF Logging for UTM Features*.

Overview

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

Configuration

CLI Quick Configuration

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

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

Step-by-Step Procedure

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

To configure WELF logging for UTM features:

1. Set the security log source IP address.

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

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

2. Name the security log stream.

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

3. Set the format for the log messages.

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

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

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

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

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

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

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

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

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

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

Verification

Verifying the Security Log

Purpose Verify that the WELF log for UTM features is complete.

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

See Also
- *Understanding UTM Support for Active/Backup Chassis Cluster*
- *Understanding UTM Licensing*

Related Documentation
- Antispam Filtering Overview on page 43

Licensing Requirements for UTM Features on NFX Devices

The majority of UTM features function as a subscription service requiring a license. You can redeem this license once you have purchased your subscription license SKUs. You redeem your license by entering your authorization code and chassis serial number into the Customer Service License Management System (LMS) interface. Once your entitlement is generated, you can use the CLI from your device to send a license update request to the LMS server. The LMS server then sends your subscription license directly to the device.

NOTE: UTM requires 1 GB of memory.

Table 3: UTM Feature Subscription Service License Requirements

UTM Feature	Requires License
Antispam	Yes
Antivirus: sophos	Yes
Content Filtering	No
Web Filtering: redirect	No
Web Filtering: local	No
Web Filtering: enhanced	Yes

NOTE: License enforcement is supported on all NFX150 devices. Licensed features including anti-virus or Enhanced Web Filtering will not function until a license has been installed. The license must be installed after installing or upgrading to a new Junos OS Release version. Unlicensed features such as UTM blacklists and whitelists will continue to function without a license.

To apply the UTM subscription license to NFX150 devices, use the following CLI command:

user@host> request system license add terminal

Reboot the device for the configuration to take effect.

Related Documentation

- Sophos Antivirus Protection on NFX Devices on page 27

CHAPTER 2

Antivirus Protection

- Sophos Antivirus Protection on NFX Devices on page 27

Sophos Antivirus Protection on NFX Devices

The Sophos antivirus scanner uses a local internal cache to maintain query responses from the external list server to improve lookup performance. For more information, see the following topics:

- Sophos Antivirus Protection Overview on page 27
- Sophos Antivirus Features on page 28
- Understanding Sophos Antivirus Data File Update on page 29
- Sophos Antivirus Configuration Overview on page 30
- Configuring Sophos Antivirus Custom Objects on page 30
- Configuring Sophos Antivirus Feature Profile on page 31
- Configuring Sophos Antivirus UTM Policies on page 35
- Configuring Sophos Antivirus Firewall Security Policies on page 36
- Managing Sophos Antivirus Data Files on page 37

Sophos Antivirus Protection Overview

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.

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

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

NOTE: IPv6 pass-through traffic for HTTP, HTTPS, FTP, SMTP, POP3, IMAP protocols is supported for Sophos antivirus, Web filtering and Content filtering security features of UTM.

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**— Sophos antivirus over SSL forward proxy does so by intercepting HTTPS traffic passing through the device. The security channel from the device is divided as one SSL channel between the client and the device, and another SSL channel between the device and the HTTPS server. SSL forward proxy acts as the terminal for both channels and forwards the cleartext traffic to UTM. UTM extracts the URL and the file checksum information from cleartext traffic. The Sophos antivirus scanner determines whether to block or permit the requests.

  SSL forward proxy does not support client authentication. If client authentication is required by the server, UTM bypasses the traffic. UTM bypasses the HTTPS traffic under the following conditions:
  - If SSL proxy does not parse the first handshake packet from the client, SSL forward proxy bypasses the traffic.
  - If the SSL proxy handshake with the client and server is incomplete because of compatibility issues, connection drops.
  - If the system resource is low, SSL forward proxy cannot handle the new connection and Sophos antivirus bypasses the traffic.
  - If HTTPS traffic hits the whitelist of SSL forward proxy, SSL forward proxy and Sophos antivirus bypass the traffic.
- **Sophos antivirus scan result handling**—With Sophos antivirus, the TCP, traffic is closed gracefully when a virus is found and the data content is dropped.

  The following fail mode options are supported: content-size, default, engine-not-ready, out-of-resource, timeout, and too-many-requests. You can set the following actions: block, log-and-permit, and permit. Fail mode handling of supported options with Sophos is much the same as with full antivirus.
- **Sophos Uniform Resource Identifier checking**—Sophos provides Uniform Resource Identifier (URI) checking, which is similar to antispam realtime blackhole list (RBL) lookups. URI checking is a way of analyzing URI content in HTTP traffic against the Sophos database to identify malware or malicious content. Because malware is

predominantly static, a checksum mechanism is used to identify malware to improve performance. Files that are capable of using a checksum include .exe, .zip, .rar, .swf, .pdf, and .ole2 (doc and xls).

NOTE: 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.

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.

Sophos Antivirus Configuration Overview

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

You must complete the following tasks to configure Sophos antivirus:

1. Configure UTM custom objects and MIME lists. See "Configuring Sophos Antivirus Custom Objects" on page 30.

2. Configure the Sophos antivirus feature profile. See "Configuring Sophos Antivirus Feature Profile" on page 31.

3. Configure a UTM policy. See "Configuring Sophos Antivirus UTM Policies" on page 35.

4. Configure a security policy. See "Configuring Sophos Antivirus Firewall Security Policies" on page 36.

Configuring Sophos Antivirus Custom Objects

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

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

   WARNING: When you configure the MIME whitelist feature, be aware that, because header information in HTTP traffic can be spoofed, you cannot always trust HTTP headers to be legitimate. When a Web browser is determining the appropriate action for a given file type, it detects the file type without checking the MIME header contents. However, the MIME whitelist feature does refer to the MIME encoding in the HTTP header. For these reasons, it is possible in certain cases for a malicious website to provide an invalid HTTP header. For example, a network administrator might inadvertently add a malicious website to a MIME whitelist, and, because the site is in the whitelist, it will not be blocked by Sophos even though Sophos has identified the site as malicious in its database. Internal hosts would then be able to reach this site and could become infected.

   a. Create the MIME whitelist.

      ```
      [edit security utm]
      ```

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

b. 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 (whitelist) 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 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
```

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

Configuring Sophos Antivirus Feature Profile

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

NOTE: This procedure shows you how to create a custom Sophos profile. If you want to use the Juniper Networks preconfigured profile, use the profile named junos-sophos-av-defaults in your UTM policy. See "Configuring Sophos Antivirus UTM Policies" on page 35.

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

```
[edit]
user@host# set security utm feature-profile anti-virus 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 feature-profile 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 feature-profile 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 the URL, use the following command:

```
[edit security utm feature-profile 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 feature-profile 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.

Create the profile named sophos-prof1.

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

Configure the content size fallback-option to block.

```
[edit security utm feature-profile anti-virus sophos-engine 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 sophos-engine 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 sophos-engine 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 sophos-engine 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 sophos-engine 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 sophos-engine 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 sophos-engine 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 sophos-engine 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.

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

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

```
[edit security utm feature-profile anti-virus sophos-engine profile sophos-prof1]
user@host# set scan-options content-size-limit 20000
```

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

```
[edit security utm feature-profile anti-virus sophos-engine profile sophos-prof1]
user@host# set scan-options no-uri-check
```

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

```
[edit security utm feature-profile anti-virus sophos-engine profile sophos-prof1]
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 feature-profile anti-virus sophos-engine profile sophos-prof1]
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 feature-profile anti-virus sophos-engine profile sophos-prof1]
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.

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

```
[edit security utm feature-profile anti-virus]
user@host# set sophos-engine profile sophos-prof1 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 feature-profile 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 whitelist, this is a custom URL category you have previously configured as a custom object. URL whitelists are valid only for HTTP traffic. In this example you use the lists that you set up earlier.

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

To view the antivirus status, enter the **show security utm anti-virus status** command.

Configuring Sophos Antivirus UTM Policies

After you have created an antivirus feature profile, you configure a UTM policy for an antivirus scanning protocol and attach this policy to a feature profile. In this procedure, 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.

To configure a UTM policy for Sophos antivirus:

1. Go to the edit security utm hierarchy.

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

2. Create the UTM policy utmp3 and attach it to the http-profile sophos-prof1.

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

NOTE: You can use the default Sophos feature profile settings by replacing sophos-prof1 in the above statement with junos-sophos-av-defaults.

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

Configuring Sophos Antivirus Firewall Security Policies

This procedure describes how to 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 "Configuring Sophos Antivirus Feature Profile" on page 31. Because the match application configuration is set to any, all application types will be scanned.

To configure a security policy for Sophos antivirus:

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

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

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

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

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

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

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

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

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

Managing Sophos Antivirus Data Files

In this example, you configure the device to update the data files automatically every 4320 minutes (every 3 days).

NOTE: 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
```

Related Documentation

- Antispam Filtering Overview on page 43
- Server-Based Antispam Filtering on page 44
- Local-List Antispam Filtering on page 53

CHAPTER 3

Whitelists

- Whitelists on page 39
- HTTP Trickling on NFX Devices on page 41

Whitelists

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

- Understanding MIME Whitelists on page 39
- Example: Configuring MIME Whitelists to Bypass Antivirus Scanning on page 40
- Understanding URL Whitelists on page 40
- Configuring URL Whitelists to Bypass Antivirus Scanning (CLI Procedure) on page 41

Understanding MIME Whitelists

The gateway device uses MIME (Multipurpose Internet Mail Extension) types to decide which traffic may bypass antivirus scanning. The MIME whitelist 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-whitelist 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-whitelist list. This list is a subset of MIME types found in the mime-whitelist.

  For example, if the mime-whitelist 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-whitelist 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 Whitelists to Bypass Antivirus Scanning

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

- Requirements on page 40
- Overview on page 40
- Configuration on page 40
- Verification on page 40

Requirements

Before you begin, decide the type of MIME lists used to configure MIME type antivirus scan bypassing. See "Understanding MIME Whitelists" on page 39.

Overview

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

Configuration

Step-by-Step Procedure

To configure MIME whitelists to bypass antivirus scanning:

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

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

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

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

Verification

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

Understanding URL Whitelists

A URL whitelist defines all the URLs listed for a specific category to always bypass the scanning process. The whitelist 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 whitelists. If any URLs do not require scanning, corresponding categories can be added to this whitelisting.

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

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

Configuring URL Whitelists to Bypass Antivirus Scanning (CLI Procedure)

To configure URL whitelists, 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;
  }
}
```

Release History Table

Release	Description
17.4R1	Starting with Junos OS Release 17.4R1, the whitelisting feature is extended to support custom URL categories supported by UTM in the whitelist configuration of SSL forward proxy.
15.1X49-D80	Starting with Junos OS Release 15.1X49-D80 and Junos OS Release 17.3R1, the whitelisting feature is extended to include URL categories supported by UTM in the whitelist configuration of SSL forward proxy. For more information, see *Application Security Feature Guide for Security Devices*.

Related Documentation

- *Full Antivirus File Scanning*
- *Full Antivirus Scan Results and Fallback Options*

HTTP Trickling on NFX Devices

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 on page 42
- Configuring HTTP Trickling on NFX Devices on page 42

Understanding HTTP Trickling

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 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.

NOTE: 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 on NFX Devices

To configure HTTP trickling on NFX devices, use the following command:

```
user@host# set security utm feature-profile anti-virus sophos-engine profile profile-name
    trickling timeout seconds
```

CHAPTER 4

Antispam Filtering

- Antispam Filtering Overview on page 43
- Server-Based Antispam Filtering on page 44
- Local-List Antispam Filtering on page 53

Antispam Filtering Overview

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 whitelists and blacklists for filtering against e-mail messages. For more information, see the following topics:

- Antispam Filtering Overview on page 43

Antispam Filtering Overview

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

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

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

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 on page 45
- Understanding Local List Antispam Filtering on page 53

Related Documentation

- *Full Antivirus Application Protocol Scanning*
- *Virus-Detected Notifications*

Server-Based Antispam Filtering

Server-based spam filtering supports only IP-based spam block list blacklist 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 on page 45
- Server-Based Antispam Filtering Configuration Overview on page 46
- Example: Configuring Server-Based Antispam Filtering on page 47

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 whitelists and blacklists. 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 whitelist is checked. If there is a match, no further checking is done. If there is no match...
2. The local blacklist 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 block list blacklist 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 blacklists and whitelists.

  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 on page 43
- Understanding Local List Antispam Filtering on page 53

Server-Based Antispam Filtering Configuration Overview

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

1. Configure UTM custom objects for the feature:

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

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

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

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

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

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

4. Attach the UTM policy to a security policy.

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

Example: Configuring Server-Based Antispam Filtering

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

- Requirements on page 47
- Overview on page 47
- Configuration on page 47
- Verification on page 52

Requirements

Before you begin, review how to configure the feature parameters for each UTM feature. See "Server-Based Antispam Filtering Configuration Overview" on page 46.

Overview

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

Configuration

CLI Quick Configuration

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

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

GUI Step-by-Step Procedure

To configure server-based antispam filtering:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Attach the UTM policy to a security policy.

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

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

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

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

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

f. Choose a source address.

g. Choose a destination address.

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

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

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

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

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

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

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

NOTE:

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

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

Step-by-Step Procedure

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

To configure server-based antispam filtering:

1. Create a profile.

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

2. Enable or disable the default SBL server lookup.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
[edit]
user@host# show security policies
```

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

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

Verification

Verifying Antispam Statistics

Purpose Verify the antispam statistics.

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

The following information appears:

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

```
Total connections: #
Denied connections: #
Total greetings: #
Denied greetings: #
Total e-mail scanned: #
White list hit: #
Black list hit: #
Spam total: #
Spam tagged: #
Spam dropped: #
DNS errors: #
Timeout errors: #
Return errors: #
Invalid parameter errors: #
```

Statistics start time:
Statistics for the last 10 days.

See Also

- Understanding Local List Antispam Filtering on page 53
- spam-action on page 315

Related Documentation

- Whitelists on page 39
- Content Filtering on page 63

Local-List Antispam Filtering

Antispam filtering allows you to use both a third-party server-based spam block list (SBL) and to optionally create your own local whitelists (benign) and blacklists (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 on page 53
- Local List Antispam Filtering Configuration Overview on page 54
- Example: Configuring Local List Antispam Filtering on page 55

Understanding Local List Antispam Filtering

When creating your own local whitelist and blacklist 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 whitelist, then the local blacklist, and then the SBL IP-based server (if enabled).

2. Sender Domain: The domain name is checked against the local whitelist and then against the local blacklist.

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

By default, the device first checks incoming e-mail against the local whitelist and blacklist. 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 whitelist is checked. If there is a match, no further checking is done. If there is no match...
2. The local blacklist 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: **Local blacklist and whitelist matching continues after the antispam license key is expired.**

See Also

- Antispam Filtering Overview on page 43
- Understanding Server-Based Antispam Filtering on page 45
- Server-Based Antispam Filtering Configuration Overview on page 46

Local List Antispam Filtering Configuration Overview

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

1. Configure UTM custom objects for the feature:

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

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

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

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

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

4. Attach the UTM policy to a security policy.

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

Example: Configuring Local List Antispam Filtering

This example shows how to configure local list antispam filtering.

- Requirements on page 55
- Overview on page 55
- Configuration on page 55
- Verification on page 61

Requirements

Before you begin, review how to configure the feature parameters for each UTM feature. See "Local List Antispam Filtering Configuration Overview" on page 54.

Overview

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

Configuration

CLI Quick Configuration

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

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

GUI Step-by-Step Procedure

To configure local list antispam filtering:

1. Create local whitelist and blacklist custom objects by configuring a URL pattern list.
   a. Select **Configure>Security>UTM>Custom Objects**.
   b. In the UTM custom objects configuration window, select the **URL Pattern List** tab.

c. Click **Add** to create URL pattern lists.

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

NOTE: If you are creating a whitelist, it is helpful to indicate this in the list name. The same applies to a blacklist. The name you enter here becomes available in the Address Whitelist and Address Blacklist fields when you are configuring your antispam profiles.

e. Next to URL Pattern Value, type the URL pattern for whitelist or blacklist antispam filtering.

2. Configure antispam filtering to use the whitelist and blacklist custom objects.

a. Select **Configure>Security>UTM>Global options**.

b. In the right pane, select the **Anti-Spam** tab.

c. Under Anti-Spam, select an Address Whitelist and/or an Address Blacklist 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**.

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

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

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

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

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

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

   c. Select the **Main** tab.

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

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

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

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

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

4. Attach the UTM policy to a security policy.

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

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

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

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

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

   f. Choose a source address.

g. Choose a destination address.

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

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

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

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

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

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

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

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

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

Step-by-Step Procedure

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

To configure local list antispam filtering:

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

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

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

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

NOTE: When both the whitelist and the blacklist are in use, the whitelist is checked first. If there is no match, then the blacklist is checked.

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

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

NOTE: 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.

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

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

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

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

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

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

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

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

```
user@host# set security policies from-zone trust to-zone untrust policy
  utmsecuritypolicy2 then permit application-services utm-policy spampolicy2
```

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

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

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

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

Verification

Verifying Antispam Statistics

Purpose Verify the antispam statistics.

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

The following information appears:

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

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

See Also

- spam-action on page 315
- Antispam Filtering Overview on page 43

Related Documentation

- Whitelists on page 39

CHAPTER 5

Content Filtering

- Content Filtering on page 63

Content Filtering

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 on page 63
- Understanding Content Filtering Protocol Support on page 64
- Specifying Content Filtering Protocols (CLI Procedure) on page 66
- Content Filtering Configuration Overview on page 66
- Example: Configuring Content Filtering Custom Objects on page 67
- Example: Configuring Content Filtering UTM Policies on page 70
- Example: Attaching Content Filtering UTM Policies to Security Policies on page 71
- Monitoring Content Filtering Configurations on page 74

Content Filtering Overview

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

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

You can configure the following types of content filters:

- MIME Pattern Filter — MIME patterns are used to identify the type of traffic in HTTP and MAIL protocols. There are two lists of MIME patterns that are used by the content filter to determine the action to be taken. The block MIME list contains a list of MIME type traffic that is to be blocked by the content filter. The MIME exception list contains MIME patterns that are not to be blocked by the content filter and are generally subsets

of items on the block list. Note that the exception list has a higher priority than the block list. If you have MIME entries that appear on both lists, those MIME types are not blocked by the content filter because the exception list takes priority. Therefore, when adding items to the exception list, it is to your advantage to be specific.

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

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

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

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

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

See Also
- Understanding MIME Whitelists on page 39

Understanding Content Filtering Protocol Support

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 on page 65
- FTP Support on page 65
- E-Mail Support on page 65

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.

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

See Also

- *Unified Threat Management Overview*
- *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 UTM modules, if traffic meets the criteria configured in the content filter, the content filter acts first upon this traffic.

The following procedure lists the recommended order in which you should configure content filters:

1. Configure UTM custom objects for the feature. See "Example: Configuring Content Filtering Custom Objects" on page 67.

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

3. Configure a UTM policy for each protocol and attach this policy to a profile. See "Example: Configuring Content Filtering UTM Policies" on page 70.

4. Attach the UTM policy to a security policy. See "Example: Attaching Content Filtering UTM Policies to Security Policies" on page 71.

Example: Configuring Content Filtering Custom Objects

This example shows how to configure content filtering custom objects.

- Requirements on page 67
- Overview on page 67
- Configuration on page 68
- Verification on page 70

Requirements

Before you begin:

1. Decide on the type of content filter you require. See "Content Filtering Overview" on page 63.

2. Understand the order in which content filtering parameters are configured. See "Content Filtering Configuration Overview" on page 66.

Overview

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

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

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

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

Configuration

CLI Quick Configuration

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

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

Step-by-Step Procedure

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

To configure content filtering custom objects:

1. Create two protocol command lists.

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

2. Add protocol commands to the list.

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

3. Create a filename extension list.

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

4. Add extensions to the list.

```
[edit security utm]
```

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

5. Create antivirus scanning lists.

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

6. Add patterns to the lists.

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

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

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

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

Verification

Verifying Content Filtering Custom Objects

Purpose Verify the content filtering custom objects.

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

See Also
- Understanding MIME Whitelists on page 39

Example: Configuring Content Filtering UTM Policies

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

- Requirements on page 70
- Overview on page 70
- Configuration on page 71
- Verification on page 71

Requirements

Before you begin:

1. Decide on the type of content filter you require. See "Content Filtering Overview" on page 63.
2. Configure UTM custom objects for each feature and define the content-filtering profile. See "Content Filtering Configuration Overview" on page 66.

Overview

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

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

Configuration

Step-by-Step Procedure

To configure a content filtering UTM policy:

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

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

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

1. Create a UTM policy.

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

2. Attach the UTM policy to the profile.

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

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

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

Verification

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

See Also

- *Unified Threat Management Overview*

Example: Attaching Content Filtering UTM Policies to Security Policies

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

- Requirements on page 72
- Overview on page 72
- Configuration on page 72
- Verification on page 73

Requirements

Before you begin:

1. Configure UTM custom objects, define the content filtering profile, and create a UTM policy. See "Content Filtering Configuration Overview" on page 66.

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

Overview

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

In this example, you create a security policy called p4 and specify that traffic from any source address to any destination address with an HTTP application matches the criteria. You then assign a UTM policy called utmp4 to the security policy p4. This UTM policy applies to any traffic that matches the criteria specified in the security policy p4.

Configuration

CLI Quick Configuration

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

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

Step-by-Step Procedure

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

To attach a UTM policy to a security policy:

1. Create a security policy.

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

2. Specify the match conditions for the policy.

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

3. Attach the UTM policy to the security policy.

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

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

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

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

Verification

Verifying Attaching Content Filtering UTM Policies to Security Policies

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

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

See Also

- *Unified Threat Management Overview*

Monitoring Content Filtering Configurations

Purpose View content filtering statistics.

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

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

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

To view content filtering statistics using J-Web:

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

   The following statistics become viewable in the right pane.

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

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

Release History Table

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

Related Documentation

- Enhanced Web Filtering on page 80
- *Full Antivirus Protection*
- *Full Antivirus Application Protocol Scanning*

CHAPTER 6

Web Filtering

- Web Filtering Overview on page 77
- Enhanced Web Filtering on page 80
- Local Web Filtering on page 116
- Redirect Web Filtering on page 129
- Monitoring Web Filtering Configurations on page 142

Web Filtering Overview

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

- Integrated Web filtering—The integrated Web filtering solution intercepts every HTTP request in a TCP connection. In this case, the decision making is done on the device after it identifies the category for a URL either from user-defined categories or from a category server (SurfControl Content Portal Authority provided by Websense). The Integrated Web filtering is not supported from Junos OS Release 15.1X49-D10 onwards.

  NOTE: The integrated Web filtering feature is a separately licensed subscription service. When the license key for Web filtering has expired, no URLs are sent to the category server for checking, only local user-defined categories are checked.

  NOTE: Integrated Web filtering solution is supported only on SRX210, SRX220, SRX240, SRX550, and SRX650 devices.

- Redirect Web filtering—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.

  NOTE: Redirect Web filtering does not require a license.

- Local Web filtering—The local Web filtering solution intercepts every HTTP 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 whitelist or blacklist based on its user-defined category.

  NOTE: 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.

  NOTE: Websense redirect do not 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.

NOTE: 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 blacklist, whitelist, 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.

NOTE: 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.

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

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.

NOTE: **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 Sophos antivirus, Web filtering and Content filtering security features of UTM.
15.1X49-D10	The Integrated Web filtering is not supported from Junos OS Release 15.1X49-D10 onwards.

Related Documentation

- *Understanding Integrated Web Filtering*
- Understanding Redirect Web Filtering on page 129
- Understanding the Enhanced Web Filtering Process on page 82
- Understanding Local Web Filtering on page 116
- Monitoring Web Filtering Configurations on page 142

Enhanced Web Filtering

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 on page 80
- Understanding the Enhanced Web Filtering Process on page 82
- Predefined Category Upgrading and Base Filter Configuration Overview on page 89
- Example: Configuring Enhanced Web Filtering on page 90
- Understanding the Quarantine Action for Enhanced Web Filtering on page 104
- Example: Configuring Site Reputation Action for Enhanced Web Filtering on page 106
- SRX TAP Mode Support Overview on page 112

Enhanced Web Filtering Overview

Enhanced Web Filtering (EWF) with Websense is an integrated URL filtering solution. When you enable the solution on the device, it intercepts the HTTP and the HTTPS requests and sends the HTTP URL or the HTTPS source IP to the Websense ThreatSeeker Cloud (TSC). The TSC categorizes the URL into one of the 95 or more categories that are predefined and also provides site reputation information. The TSC further returns the URL category and the site reputation information to the device. The device determines if it can permit or block the request based on the information provided by the TSC.

The Surf-Contol feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards.

Starting in Junos OS Release 15.1X49-D40 and Junos OS Release 17.3R1, EWF supports HTTPS traffic by intercepting HTTPS traffic passing through the SRX Series device. The security channel from the SRX Series device is divided as one SSL channel between the client and the SRX Series device and another SSL channel between the SRX Series device and the HTTPS server. SSL forward proxy acts as the terminal for both channels and forwards the cleartext traffic to the UTM. UTM extracts the URL from the HTTP request message.

You can consider the EWF solution as the next-generation URL filtering solution, building upon the existing SurfControl 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) on SRX Series Devices

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.

NOTE: 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 on page 116
- Understanding Redirect Web Filtering on page 129

Understanding the Enhanced Web Filtering Process

Web filtering enables you to manage Internet access, preventing access to inappropriate Web content. The Enhanced Web Filtering (EWF) feature intercepts, scans, and acts upon HTTP or HTTPS traffic in the following way:

1. The device creates TCP socket connections to the Websense ThreatSeeker Cloud (TSC).
2. The device intercepts an HTTP or an HTTPS connection and extracts each URL (in the HTTP request) or IP (in the HTTPS request). For an HTTPS connection, EWF is supported through SSL forward proxy.

   NOTE: 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 blacklist or whitelist.

   NOTE: A blacklist or a whitelist 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 blacklist, the device blocks the URL.
   - If the URL is in the user-configured whitelist, 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 the URL in the URL filtering cache.
   - 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 redirect response to the HTTP client and the URL is redirected to the HTTP server.
   - 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.

Functional Requirements for Enhanced Web Filtering

The following items are required to use Enhanced Web Filtering (EWF):

- **License key**—The EWF solution builds upon the SurfControl integrated feature on the device. Two different valid license keys are required for the SurfControl integrated solution and for EWF. You need to install a new license to upgrade to the EWF solution.

  NOTE: You can ignore the warning message "requires 'wf_key_websense_ewf' license" because it is generated by routine EWF license validation check.

  A grace period of 30 days, consistent with other UTM features, is provided for the EWF feature after the license key expires.

  NOTE: The device will continue to support the SurfControl integrated solution after the upgrade.

  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.

NOTE: For HTTP 1.1 persistent connections, the subsequent requests on that session are ignored by the EWF module.

If the device holds the original request for a long time, then the client will retransmit the request. The URL filtering code will detect the retransmitted packets. If the original HTTP request has already been forwarded, then EWF forwards the retransmitted packet to the server. However, if EWF is in the middle of first-packet processing or makes the calculation to block the session, then the solution drops the retransmitted packet. A counter tracks the number of retransmitted packets received by the device.

If the TSC does not respond in time to the categorization request from the device, then the original client request is blocked or permitted according to the timeout fallback setting.

- **HTTPS request interception**—Starting with Junos OS 15.1X49-D40 and Junos OS Release 17.3R1, EWF intercepts HTTPS traffic passing through the SRX Series device. The security channel from the SRX Series device is divided as one SSL channel between the client and the SRX Series device and another SSL channel between the SRX Series device and the HTTPS server. SSL forward proxy acts as the terminal for both channels and forwards the cleartext traffic to the UTM. UTM extracts the URL from the HTTP request message.
- **Blocking message**—The blocking message sent to the Web client is user-configurable and is of the following types:
  - The Juniper Networks blocking message is the default message defined in the device that can be modified by the user. The default blocking message contains the reason why the request is blocked and the category name (if it is blocked because of a category).
  - Syslog message.

  For example, if you have set the action for Enhanced_Search_Engines_and_Portals to block, and you try to access www.example.com, the blocking message is of the following form: **Juniper Web Filtering:Juniper Web Filtering has been set to block this site. CATEGORY: Enhanced_Search_Engines_and_Portals REASON: BY_PRE_DEFINED** . However, the corresponding syslog message on the device under test (DUT) is: **WEBFILTER_URL_BLOCKED: WebFilter: ACTION="URL Blocked" 56.56.56.2(59418)->74.125.224.48(80) CATEGORY="Enhanced_Search_Engines_and_Portals" REASON="by predefined category" PROFILE="web-ewf" URL=www.example.com OBJ=/** .
- **Monitoring the Websense server**—The URL filtering module uses two methods to determine if the TSC is active: socket connections and heartbeat. EWF maintains persistent TCP sockets to the TSC. The server responds with a TCP ACK if it is enabled. EWF sends an application layer NOOP keepalive to the TSC. If the device does not receive responses to three consecutive NOOP keepalives in a specific period, it determines the socket to be inactive. The EWF module attempts to open a new

connection to the TSC. If all sockets are inactive, the TSC is considered to be inactive. Therefore an error occurs. The error is displayed and logged. Subsequent requests and pending requests are either blocked or passed according to the server connectivity fallback setting until new connections to the TSC are opened again.

- **HTTP protocol communication with the TSC**—EWF uses the HTTP 1.1 protocol to communicate with the TSC. This ensures a persistent connection and transmission of multiple HTTP requests through the same connection. A single HTTP request or response is used for client or server communication. The TSC can handle queued requests; for optimal performance, an asynchronous request or response mechanism is used. The requests are sent over TCP, so TCP retransmission is used to ensure request or response delivery. TCP also ensures that valid in-order, non-retransmitted HTTP stream data is sent to the HTTP client on the device.
- **Responses**—The responses adhere to the basic HTTP conventions. Successful responses include a 20x response code (typically 200). An error response includes a 4xx or 5xx code. Error responses in the 4xx series indicate issues in the custom code. Error responses in the 5xx series indicate issues with the service.

  Error codes and meanings are as follows:

  - 400–Bad request
  - 403–Forbidden
  - 404–Not found
  - 408–Request canceled or null response
  - 500–Internal server error

  Errors in the 400 series indicate issues with the request. Errors in the 500 series indicate issues with the TSC service. Websense is notified of these errors automatically and responds accordingly.

  You can configure the default fallback setting to determine whether to pass or block the request:
  set security utm feature-profile web-filtering juniper-enhanced profile juniper-enhanced fallback-settings default ?

  The response also contains the site categorization and site reputation information.
- **Categories**—A category list is available on the device. This list consists of categories, each containing a category code, a name, and a parent ID. Categories can also be user-defined. Each category consists of a list of URLs or IP addresses. Categories are not updated dynamically and are tied to the Junos OS release because they have to be compiled into the Junos OS image. Any update in categories needs to be synchronized with the Junos OS release cycle.

  Starting with Junos OS Release 17.4R1, you can download and dynamically load new EWF categories. The downloading and dynamic loading of the new EWF categories do not require a software upgrade. Websense occasionally releases new EWF categories. EWF classifies websites into categories according to host, URL, or IP address and performs filtering based on the categories.

NOTE: On SRX Series devices, 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.

NOTE: 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 *http://images.example.com/images?hl=en&source=imghp&biw=1183&bih=626&q=adult+movies&gbv=2&aq=f&aqi=&aql=&oq=&gs_rfai= No category action is defined for this URL*. TSC returns safe-search string **safe=active**. The EWF code on the DUT generates a HTTP 302 response, with the redirect URL: *http://images.example.com/images?hl=en&source=imghp&biw=1183&bih=626&q=adult+movies&gbv=2&aq=f&aqi=&aql=&oq=&gs_rfai=&safe=active* . This response is returned to the client. The client now sends out a safe redirect request to this URL.

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 whitelist or a blacklist 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.

NOTE:

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 blacklist, whitelist, user-defined category, predefined category, safe-search, site reputation, and default action.

User Messages and Redirect URLs for Enhanced Web Filtering (EWF) on SRX Series Devices

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.

NOTE: Only one custom-message configuration option is applied for each category. The custom-message configuration is supported only on Enhanced Web Filtering (EWF). Therefore, only the Juniper EWF engine type is supported.

Starting with Junos OS Release 17.4R1, support for custom category configuration is available for local and Websense redirect profiles.

See Also
- Web Filtering Overview on page 77

Predefined Category Upgrading and Base Filter Configuration Overview

You can download and dynamically load new Enhanced Web Filtering (EWF) categories without any software upgrade. The predefined base filters defined in a category file are supported for individual EWF categories.

To configure a predefined category upgrade without any software upgrade:

1. Configure UTM custom objects for the UTM features. Set the interval, set the start time, and enter the URL of category package download:

```
user@host# set security utm custom-objects
user@host# set security utm custom-objects category-package
user@host# set security utm custom-objects category-package automatic
user@host# set security utm custom-objects category-package automatic interval
  60
user@host# set security utm custom-objects category-package automatic interval
  60 enable
user@host# set security utm custom-objects category-package automatic interval
  60 enable start-time 2017-09-05.08.08.08
user@host# set security utm custom-objects category-package automatic
  route-instance VRF
user@host# set security utm custom-objects category-package automatic
  route-instance VRF url https://update.juniper-updates.net/EWF
```

2. Configure the predefined base filters. Each EWF category has a default action in a base filter, which is attached to the user profile to act as a backup filter. If the categories are not configured in the user profile, then the base filter takes the action. You can also upgrade the base filters online.

```
user@host# set security utm feature profile web-filtering juniper-enhanced
  juniper-enhanced-profile
user@host# set security utm feature profile web-filtering juniper-enhanced
  juniper-enhanced-profile base-filter [base-filter]
```

```
user@host# set security utm feature profile web-filtering juniper-enhanced
  juniper-enhanced-profile base-filter [base-filter] category <category-action >
user@host# set security utm feature profile web-filtering juniper-enhanced
  juniper-enhanced-profile base-filter [base-filter] category category-action default
  <default-action>
user@host# set security utm feature profile web-filtering juniper-enhanced
  juniper-enhanced-profile base-filter [base-filter] category category-action default
  <default-action>site-reputation-action <reputation-action>
```

show security utm custom-objects

```
category-package{
automatic{
 interval 60;
 enable;
 start-time "2017-09-05.08.08.08";
 }
route-instance VRF;
url https://update.juniper-updates.net/EWF;
}
```

show security utm feature-profile web-filtering juniper-enhanced

```
server {
    host rp.cloud.threatseeker.com;
}
sockets 8;
profile ewf_p1 {
+ base-filter gov-filter;
default log-and-permit;
    timeout 15;
}
+reputation {
 reputation-very-safe 90;
 reputation-moderately-safe 80;
 reputation-fairly-safe 70;
 reputation-suspicious 60;
}
```

See Also

- show security utm web-filtering category status on page 417
- category (Security Web Filtering) on page 169
- request security utm web-filtering category install on page 376
- show security utm web-filtering category base-filter on page 412

Example: Configuring Enhanced Web Filtering

This example shows how to configure Enhanced Web filtering (EWF) for managing website access. This feature is supported on all SRX Series devices. The EWF solution intercepts HTTP and the HTTPS requests and sends the HTTP URL or the HTTPS source IP to the Websense ThreatSeeker Cloud (TSC). The TSC categorizes the URL into one of the 151 or more predefined categories and also provides site reputation information.

The TSC further returns the URL category and the site reputation information to the device. The SRX Series device determines whether it can permit or block the request based on the information provided by the TSC.

- Requirements on page 91
- Overview on page 91
- Configuration on page 93
- Verification on page 102

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 77 and "Understanding the Enhanced Web Filtering Process" on page 82.

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 (whitelist) of URLs or addresses that you want to bypass. After you create the URL pattern list, define the custom objects. After defining the custom objects, you apply them to feature profiles to define the activity on each profile, apply the feature profile to the UTM policy, and finally attach the Web filtering UTM policies to the security policies. Table 4 on page 91 shows information about EWF configuration type, steps, and parameters used in this example.

Table 4: 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 (whitelist) 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

Table 4: Enhanced Web filtering (EWF) Configuration Type, Steps, and Parameters (continued)

Configuration Type	Configuration Steps	Configuration Parameters
Feature profiles	Configure the Web filtering feature profile:	
	• Set the URL blacklist filtering category to custblacklist, set the whitelist 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 • type 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 whitelist and blacklist 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

	• 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

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 on page 93
- Configuring Enhanced Web Filtering Feature Profiles on page 95
- Attaching Web Filtering UTM Policies to Security Policies on page 100

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

WARNING: 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 (whitelist) of URLs or addresses that you want to bypass. After you create the URL pattern list, you create a custom URL category list and add the pattern list to it. Configure a URL pattern list custom object by creating the list name and adding values to it as follows:

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

   ```
   [edit security utm]
   user@host# set custom-objects url-pattern urllist3 value [http://www. example.net
     1.2.3.4]
   ```

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

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

2. Create a custom object called urllist3 that contains the pattern http://www.example.net and then add the urllist3 custom object to the custom URL category custurl3.

   ```
   [edit security utm]
   user@host# set custom-objects custom-url-category custurl3 value urllist3
   ```

3. Create a list of untrusted and trusted sites.

   ```
   [edit security utm]
   user@host# set custom-objects url-pattern urllistblack value
     [http://www.untrusted.com 13.13.13.13]
   user@host# set custom-objects url-pattern urllistwhite value
     [http://www.trusted.com 11.11.11.11]
   ```

4. Configure the custom URL category list custom object by using the URL pattern list of untrusted and trusted sites.

```
[edit security utm]
user@host# set custom-objects custom-url-category custblacklist value urllistblack
user@host# set custom-objects custom-url-category custwhitelist value urllistwhite
```

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

```
[edit]
userhost#show security utm custom-objects
  url-pattern {
    urllist3 {
      value [ 1.2.3.4 http://www.example.net ];
    }
    urllistblack {
      value [ 13.13.13.13 http://www.untrusted.com ];
    }
    urllistwhite {
      value [ 11.11.11.11 http://www.trusted.com ];
    }
  }
    custom-url-category {
      custurl3 {
        value urllist3;
      }
      custblacklist {
        value urllistblack;
      }
      custwhiltelist {
        value urllistwhite;
      }
    }
```

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

Configuring Enhanced Web Filtering Feature Profiles

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

NOTE: Starting in Junos OS Release 12.3X48-D25, new CLI options are available. The **http-reassemble** and **http-persist** options are added in the **show security utm feature-profile web-filtering** command.

```
[edit security utm]
set security utm feature-profile web-filtering url-whitelist custwhitelist value
set security utm feature-profile web-filtering url-blacklist custblacklist value
set security utm feature-profile web-filtering type juniper-enhanced
set security utm feature-profile web-filtering juniper-enhanced cache size 500
set security utm feature-profile web-filtering juniper-enhanced cache timeout 1800
set security utm feature-profile web-filtering juniper-enhanced server host
  rp.cloud.threatseeker.com
set security utm feature-profile web-filtering juniper-enhanced server port 80
set security utm feature-profile web-filtering http-reassemble
set security utm feature-profile web-filtering http-persist
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile
  category Enhanced_Hacking action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile
  category Enhanced_Government action quarantine
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile
  site-reputation-action very-safe permit
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile
  custom-block-message "***access denied ***"
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile
  block-message type custom-redirect-url
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile
  block-message url http://10.10.121.18
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile
  default block
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile
  fallback-settings server-connectivity block
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile
  fallback-settings timeout block
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile
  fallback-settings too-many-requests block
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile
  timeout 10
set security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile
  no-safe-search
set security utm utm-policy mypolicy web-filtering http-profile ewf_my_profile
set security policies from-zone utm_clients to-zone mgmt policy 1 then permit
  application-services utm-policy mypolicy
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
  quarantine-custom-message “**The requested webpage is blocked by your
  organization's access policy**”.
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
  quarantine-message type custom-redirect-url
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
  quarantine-message url besgas.spglab.example.net
```

Step-by-Step Procedure

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

To configure the EWF feature profiles:

1. Configure the Web filtering URL blacklist, URL whitelist, and the Web filtering engine.

```
[edit security utm feature-profile web-filtering]
user@host# set url-blacklist custblacklist
user@host# set url-whitelist custwhitelist
user@host# set type juniper-enhanced
```

2. Set the cache size and cache timeout parameters for the configured EWF engine.

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

3. Set the server name or IP address and the port number for communicating with the server. The default host value in the system is rp.cloud.threatseeker.com.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced server host rp.cloud.threatseeker.com
user@host# set juniper-enhanced server port 80
```

4. Set the **http-reassemble** statement to reassemble the requested packet and the **http-persist** statement to check every HTTP request packet in the same session. If the **http-reassemble** statement is not configured for cleartext HTTP traffic, then EWF does not reassemble the fragmented HTTP request to avoid incomplete parsing in the packet-based inspection. If the **http-persist** statement is not configured for cleartext HTTP traffic, then EWF does not check every HTTP request packet in the same session.

```
[edit security utm feature-profile web-filtering]
user@host# set http-reassemble
user@host# set http-persist
```

5. Create a profile name, and select a category from the included whitelist and blacklist categories.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf_my_profile category Enhanced_Hacking
   action log-and-permit
user@host# set security utm feature-profile web-filtering juniper-enhanced profile
   ewf_my_profile category Enhanced_Government action quarantine
```

6. Specify the action to be taken depending on the site reputation returned for the URL if there is no category match found.

```
[edit security utm feature-profile web-filtering]
user@host#set juniper-enhanced profile ewf_my_profile site-reputation-action
   very-safe permit
```

7. Enter a custom message to be sent when HTTP requests are blocked.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf_my_profile custom-block-message
  "***access denied ***"
```

8. Define a redirect URL server so that instead of the device sending a block page with plain text HTML, the device will send an HTTP 302 redirect to this redirect server with some special variables embedded in the HTTP redirect location field. These special variables can be parsed by the redirect server and serve a special block page to the client with rich images and formatting.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf_my_profile block-message type
  custom-redirect-url http://10.10.1.1
user@host# set juniper-enhanced profile ewf_my_profile block-message url
  http://10.10.121.18
```

NOTE: If you configure the **security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile block-message** statement, then the default block message configuration takes precedence over the **security utm feature-profile web-filtering juniper-enhanced profile ewf_my_profile custom-block-message** configuration.

9. Specify a default action (permit, log and permit, block, or quarantine) for the profile, when no other explicitly configured action (blacklist, whitelist, custom category, predefined category actions, or site reputation actions) is matched .

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

10. Configure the fallback settings (block or log and permit) for this profile.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf_my_profile fallback-settings default
  block
user@host# set juniper-enhanced profile ewf_my_profile fallback-settings
  server-connectivity block
user@host# set juniper-enhanced profile ewf_my_profile fallback-settings timeout
  block
user@host# set juniper-enhanced profile ewf_my_profile fallback-settings
  too-many-requests block
```

11. Enter a timeout value in seconds. When this limit is reached, fallback settings are applied. This example sets the timeout value to 10. You can also disable the safe-search functionality. By default, search requests have safe-search strings attached to them, and a redirect response is sent to ensure that all search requests are safe or strict.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf_my_profile timeout 10
user@host# set juniper-enhanced profile ewf_my_profile no-safe-search
```

NOTE: The timeout value range for SRX210, SRX220, SRX240, SRX300, SRX320, SRX345, SRX550, SRX1500, SRX4100, and SRX4200 is 0 through 1800 seconds and the default value is 15 seconds. The timeout value range for SRX3400 and SRX3600 is 1 through 120 seconds and the default value is 3 seconds.

12. Configure a UTM policy (mypolicy) for the Web-filtering HTTP protocol, associating ewf_my_profile to the UTM policy, and attach this policy to a security profile to implement it.

```
[edit security utm]
user@host# set utm-policy mypolicy web-filtering http-profile ewf_my_profile
user@host# set security policies from-zone utm_clients to-zone mgmt policy 1 then
   permit application-services utm-policy mypolicy
```

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

```
[edit]
user@host# show security utm
feature-profile{
web-filtering {
   url-whitelist custwhitelist{
   url-blacklist custblacklist;
   http-reassemble;
   http-persist;
   type juniper-enhanced;
   juniper-enhanced {
      cache {
         timeout 1800;
         size 500;
      }
      server {
         host rp.cloud.threatseeker.com;
         port 80;
      }
      profile ewf_my_profile {
         category {
            Enhanced_Hacking {
               action log-and-permit;
               }
               Enhanced_Government {
```

```
            action quarantine;
          }
        }
        site-reputation-action {
          very-safe permit;
          moderately-safe log-and-permit;
          fairly-safe log-and-permit;
          harmful block;
          suspicious block;
        }
        default block;
        custom-block-message "***access denied ***";
        fallback-settings {
          default block;
          server-connectivity block;
          timeout block;
          too-many-requests block;
        }
        timeout 10;
        no-safe-search;
      }
      utm-policy mypolicy {
        web-filtering {
      http-profile ewf_my_profile;
    }
    }
}
```

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

Attaching Web Filtering UTM Policies to Security Policies

CLI Quick Configuration

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

```
set security policies from-zone trust to-zone untrust policy sec_policy match
  source-address any
set security policies from-zone trust to-zone untrust policy sec_policy match
  destination-address any
set security policies from-zone trust to-zone untrust policy sec_policy match application
  any
set security policies from-zone trust to-zone untrust policy sec_policy then permit
  application-services utm-policy mypolicy
```

Step-by-Step Procedure

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

To attach a UTM policy to a security policy:

1. Create the security policy sec_policy.

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

2. Specify the match conditions for sec-policy.

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

3. Attach the UTM policy mypolicy to the security policy sec_policy.

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

Results

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

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

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

Verification

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

- Verifying the Status of the Web Filtering Server on page 102
- Verifying that Web Filtering Statistics Have Increased on page 102
- Verifying That the Web Filtering UTM Policy Is Attached to the Security Policy on page 103

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 whitelist and blacklist hits and custom category hits. If there is an HTTP request URL hit, then there is a increase in the Web filtering statistics from an earlier value.

Verifying That the Web Filtering UTM Policy Is Attached to the Security Policy

Purpose Verify that the Web filtering UTM policy mypolicy is attached to the security policy sec_policy.

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

```
user@host> show security policies global policy-name mypolicy detail
```

```
node0:
-
   Global policies:
Policy: mypolicy, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 1
From zones: zone1, zone2
To zones: zone3, zone4
Source addresses: any
Destination addresses: any
Applications: any
Action: permit
Unified Threat Management: enabled
```

Meaning The output displays a summary of all security policies configured on the device. If a particular policy is specified, it displays information specific to that policy. If UTM is enabled, then mypolicy is attached to sec_policy.

See Also
- Web Filtering Overview on page 77

- Monitoring Web Filtering Configurations on page 142

Understanding the Quarantine Action for Enhanced Web Filtering

UTM Enhanced Web Filtering supports block, log-and-permit, and permit actions for HTTP/HTTPS requests. In addition to this, UTM Enhanced Web Filtering now supports the quarantine action which allows or denies access to the blocked site based on the user's response to the message.

The following sequence explains how the HTTP or HTTPs request is intercepted, redirected, and acted upon by the quarantine action:

- The HTTP client requests URL access.
- The device intercepts the HTTP request and sends the extracted URL to the Websense Thread Seeker Cloud (TSC).
- The TSC returns the URL category and the site reputation information to the device.
- If the action configured for the category is quarantine, the device logs the quarantine action and sends a redirect response to HTTP client.
- The URL is sent to the HTTP server for redirecting.
- The device shows a warning message stating that the access to the URL is blocked according to the organization's security policies and prompts the user to respond.
- If the user response is "No," the session is terminated. If the user response is "Yes," the user is allowed access to the site and such access is logged and reported to the administrator.

NOTE: On all SRX Series devices, the quarantine action is supported only for UTM Enhanced Web Filtering or Juniper enhanced type of Web filtering.

Quarantine Message

The quarantine message sent to the HTTP client is user-configurable and is of the following types:

- Default message

  The default quarantine message is displayed when a user attempts to access a quarantined website and it contains the following information:

  - URL name
  - Quarantine reason
  - Category (if available)
  - Site-reputation (if available)

For example, if you have set the action for Enhanced_Search_Engines_and_Portals to quarantine, and you try to access www.search.example.com, the quarantine message is as follows:

*****The requested webpage is blocked by your organization's access policy***.**

- Syslog message.

  The syslog message will be logged by the system when the user access the web page that has already been quarantined and marked as block or permit.

  The corresponding syslog message on the device under test is:

  Jan 25 15:10:40 rodian utmd[3871]: WEBFILTER_URL_BLOCKED: WebFilter: ACTION="URL Blocked" 99.99.99.4(60525)->74.125.224.114(80) CATEGORY="Enhanced_Search_Engines_and_Portals" REASON="by predefined category(quarantine)" PROFILE="ewf-test-profile" URL=www.search.example.com OBJ=/

  Starting in Junos OS 12.1X47-D40 and Junos OS Release 17.3R1, the structured log fields have changed. The structured log field changes in the UTM Web filter logs WEBFILTER_URL_BLOCKED, WEBFILTER_URL_REDIRECTED, and WEBFILTER_URL_PERMITTED are as follows:

  - **name -> category**
  - **error-message -> reason**
  - **profile-name -> profile**
  - **object-name -> url**
  - **pathname -> obj**

User Messages and Redirect URLs for Enhanced Web Filtering (EWF) on SRX Series devices

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.

NOTE: **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 on page 116
- Understanding Redirect Web Filtering on page 129

Example: Configuring Site Reputation Action for Enhanced Web Filtering

This example shows how to configure the site reputation action for both categorized and uncategorized URLs.

- Requirements on page 106
- Overview on page 106
- Configuration on page 107
- Verification on page 110

Requirements

Before you begin, you should be familiar with Web Filtering and Enhanced Web Filtering. See "Web Filtering Overview" on page 77 and "Understanding the Enhanced Web Filtering Process" on page 82.

Overview

In this example, you configure Web Filtering profiles to URLs according to defined categories using the site reputation action. You set the URL whitelist 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 whitelist category to cust-cat-quarantine, and set the reputation action to quarantine.

You enter a custom message to be sent when HTTP requests are quarantined. In this example, the following message is sent: **The requested webpage is blocked by your organization's access policy**.

You block URLs in the Enhanced_News_and_Media category and permit URLs in the Enhanced_Education category. Then you quarantine the URLs in the Enhanced_Streaming_Media category and configure the device to send the following message: **The requested webpage is blocked by your organization's access policy**.

In this example, you set the default action to permit. You select fallback settings (block or log-and-permit) for this profile in case errors occur in each configured category. Finally, you set the fallback settings to block.

Configuration

Configuring Site Reputation Action

CLI Quick Configuration

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

```
set security utm feature-profile web-filtering set url-whitelist url-cat-white
set security utm feature-profile web-filtering juniper-enhanced cache size
set security utm feature-profile web-filtering juniper-enhanced reputation
  reputation-very-safe 85
set security utm feature-profile web-filtering juniper-enhanced reputation
  reputation-moderately-safe 75
set security utm feature-profile web-filtering juniper-enhanced reputation
  reputation-fairly-safe 65
set security utm feature-profile web-filtering juniper-enhanced reputation
  reputation-suspicious 55
set security utm feature-profile web-filtering juniper-enhanced cache timeout 1
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
  category cust-cat-quarantine action quarantine
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
  category Enhanced_News_and_Media action block
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
  category Enhanced_Education action permit
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
  category Enhanced_Education reputation-action harmful block
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
  category Enhanced_Streaming_Media action quarantine
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
  default permit
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
  default quarantine-message “*** The requested webpage is blocked by your
  organization’s access policy***”.
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
  fallback-settings server-connectivity block
set security utm feature-profile web-filtering juniper-enhanced profile ewf-test-profile
  fallback-settings timeout block
```

Step-by-Step Procedure

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

To configure the site reputation action:

1. Configure the Web Filtering URL whitelist.

```
[edit security utm feature-profile web-filtering]
user@host# set url-whitelist custwhitelist
```

2. Specify the Enhanced Web Filtering engine, and set the cache size parameters.

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

3. Configure the base reputation scores.

```
[edit security utm feature-profile web-filtering]
set juniper-enhanced reputation reputation-very-safe 85
set juniper-enhanced reputation reputation-moderately-safe 75
set juniper-enhanced reputation reputation-fairly-safe 65
set juniper-enhanced reputation reputation-suspicious 55
```

NOTE: The base reputation value must be ordered.

4. Set the cache timeout parameters.

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

5. Create a profile name, and select a category from the whitelist categories.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile category
   cust-cat-quarantine action quarantine
```

6. Create a profile name, and select a category from the whitelist categories.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile category
   Enhanced_News_and_Media action block
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile category
   Enhanced_Education action permit
```

```
user@host# set juniper-enhanced profile ewf-test-profile category
  Enhanced_Education action harmful block
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile category
  Enhanced_Streaming_Media action quarantine
```

7. Enter a warning message to be sent when HTTP requests are quarantined.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile
  quarantine-custom-message "***The requested webpage is blocked by your
  organization's access policy ***"
```

8. Select a default action (permit, log-and-permit, block, or quarantine) for the profile, when no other explicitly configured action (blacklist, whitelist, custom category, predefined category or site reputation) is matched .

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile default permit
```

9. Select fallback settings (block or log-and-permit) for this profile.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-enhanced profile ewf-test-profile fallback-settings
  server-connectivity block
user@host# set juniper-enhanced profile ewf-test-profile fallback-settings timeout
  block
```

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

```
[edit]
user@host# show security utm
feature-profile{
web-filtering {
   url-whitelist url-cat-white;
   type juniper-enhanced;
   traceoptions;
   flag all;
}
   juniper-enhanced {
      reputation {
         reputation-very-safe 85
         reputation-moderately-safe 75
         reputation-fairly-safe 65
      reputation-suspicious 55
      cache {
```



```
    timeout 1
  }
  profile ewf-test-profile {
    category {
      cust-cat-quarantine {
        action quarantine;
        }
        Enhanced_News_and_Media {
          action block;
          reputation-action;
        }
        Enhanced_Education {
        action permit;
        reputation-action;
        {
        harmful block;
        }
        }
        Enhanced_Streaming_Media {
        action quarantine;
        }
      }
    default permit;
  quarantine-custom-message "***The requested webpage is blocked by your
    organization's access policy***".
    fallback-settings {
      server-connectivity block;
      timeout block;
      }
      }
      }
    }
```

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

Verification

Confirm that the configuration is working properly.

- Verifying the Status of UTM Service on page 110
- Verifying the Status of UTM Session on page 111
- Verifying the Status of UTM Web Filtering on page 111
- Verifying the Statistics of UTM Web Filtering on page 111

Verifying the Status of UTM Service

Purpose Verify the UTM service status.

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

Sample Output

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

Verifying the Status of UTM Session

Purpose Verify the UTM session status.

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

Sample Output

```
user@host>show security utm session
UTM session info:
 Maximum sessions:                4000
 Total allocated sessions:        0
 Total freed sessions:            0
 Active sessions:                 0
```

Verifying the Status of UTM Web Filtering

Purpose Verify the UTM Web filtering status.

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

Sample Output

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

Verifying the Statistics of UTM Web Filtering

Purpose Verify the Web filtering statistics for connections including whitelist and blacklist hits and custom category hits.

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

Sample Output

```
user@host>show security utm web-filtering statistics
UTM web-filtering statistics:
    Total requests:                    2594
```

```
    white list hit:                     0
    Black list hit:                     0
    Queries to server:                  2407
    Server reply permit:                1829
    Server reply block:                 0
    Server reply quarantine:            517
    Server reply quarantine block:      0
    Server reply quarantine permit:     8
    Custom category permit:             0
    Custom category block:              0
    Custom category quarantine:         0
    Custom category qurantine block:    0
    Custom category quarantine permit:  0
    Site reputation permit:             0
    Site reputation block:              0
    Site reputation quarantine:         0
    Site reputation quarantine block:   0
    Site reputation quarantine permit:  0
    Site reputation by Category         0
    Site reputation by Global           0
    Cache hit permit:                   41
    Cache hit block:                    0
    Cache hit quarantine:               144
    Cache hit quarantine block:         0
    Cache hit quarantine permit:        1
    Safe-search redirect:               0
    Web-filtering sessions in total:    16000
    Web-filtering sessions in use:      0
    Fallback:                       log-and-permit          block
          Default                                0              0
          Timeout                                0              0
     Connectivity                                0              1
Too-many-requests                                0              0
```

See Also

- Understanding URL Whitelists on page 40

SRX TAP Mode Support Overview

The TAP (Terminal Access Point) mode is a standby device, which checks the mirrored traffic through switch. If UTM is enabled, then the TAP mode inspects the incoming and outgoing traffic by configuring the TAP interface and generating a security log report to show the number of threats detected and the user usage. If some packet gets lost in the tap interface, the UTM terminates the connection, as a result no report is generated for this connection. The UTM configuration remains the same as non-TAP mode.

Starting in Junos OS Release 19.1R1, a TAP (Terminal Access Point) mode is supported on the UTM module. When you configure the SRX Series device to operate in TAP mode, the device generates security log information to display the information on threats detected, application usage, and user details.
when configured to operate in TAP mode, the SRX Series device receives packets only from the configured TAP interface.

NOTE: You can configure only one interface to operate in TAP mode.

UTM functionality configured on SRX Series device continues to work and exchange information from server as per configuration. To use UTM functionality when the SRX Series device is configured in TAP mode, you must configure the DNS server to resolve the cloud server's IP addresses.

The connection between SRX device and Ethernet switch is a mirror connection for the connection between client and Ethernet switch. The mirror port allows copying of traffic on the switch. When you configure an interface on the SRX Series device to operate as tap mode interface and connecting it with a switch, the switch mirror port provides the SRX Series device with the mirrored traffic. SRX Series device process the incoming traffic from one TAP interface and generates security log information to display the information on threats detected, application usage, and user details.

When operating in TAP mode, the SRX Series device performs:

- Enhanced Web filtering (EWF) for mirrored HTTP traffic.
- Sophos antivirus (SAV) for mirrored HTTP/FTP/SMTP/POP3/IMAP traffic.
- Antispam (AS) for mirrored SMTP traffic.

See Also

- Antispam Filtering Overview.

Release History Table

Release	Description
17.4R1	Starting with Junos OS Release 17.4R1, support for custom category configuration is available for local and Websense redirect profiles.
17.4R1	Starting with Junos OS Release 17.4R1, you can download and dynamically load new EWF categories. The downloading and dynamic loading of the new EWF categories do not require a software upgrade. Websense occasionally releases new EWF categories. EWF classifies websites into categories according to host, URL, or IP address and performs filtering based on the categories.
17.4R1	Starting with Junos OS Release 17.4R1, predefined base filters, defined in a category file, are supported for individual EWF categories. Each EWF category has a default action in a base filter, which is attached to the user profile to act as a backup filter. If the categories are not configured in the user profile, then the base filter takes the action.
17.4R1	Starting with Junos OS Release 17.4R1, the reputation base scores are configurable. Users can apply global reputation values, provided by the Websense ThreatSeeker Cloud (TSC). For the non-category URLs, the global reputation value is used to perform filtering,
17.4R1	Starting with Junos OS Release 17.4R1, support for custom category configuration is available for local and Websense redirect profiles.
17.4R1	Starting with Junos OS Release 17.4R1, support for custom category configuration is available for local and Websense redirect profiles.
15.1X49-D40	Starting in Junos OS Release 15.1X49-D40 and Junos OS Release 17.3R1, EWF supports HTTPS traffic by intercepting HTTPS traffic passing through the SRX Series device.
15.1X49-D40	Starting with Junos OS 15.1X49-D40 and Junos OS Release 17.3R1, EWF intercepts HTTPS traffic passing through the SRX Series device. The security channel from the SRX Series device is divided as one SSL channel between the client and the SRX Series device and another SSL channel between the SRX Series device and the HTTPS server. SSL forward proxy acts as the terminal for both channels and forwards the cleartext traffic to the UTM. UTM extracts the URL from the HTTP request message.
15.1X49-D110	Starting with Junos OS Release 15.1X49-D110, a new option, **custom-message**, is added for the **custom-objects** command that enables you to configure user messages and redirect URLs to notify users when a URL is blocked or quarantined for each EWF category.
15.1X49-D110	Starting with Junos OS Release 15.1X49-D110, a new option, **custom-message**, is added for the **custom-objects** statement that enables you to configure user messages and redirect URLs to notify users when a URL is blocked or quarantined for each EWF category.
15.1X49-D110	Starting with Junos OS Release 15.1X49-D110, the "***** " in a wildcard syntax, required to create URL pattern for Web filtering profile, matches all subdomains.
15.1X49-D110	Starting with Junos OS Release 15.1X49-D110, a new option, **custom-message**, is added for the **custom-objects** statement that enables you to configure user

	messages and redirect URLs to notify users when a URL is blocked or quarantined for each EWF category.
15.1X49-D10	The Surf-Contol feature is not supported from Junos OS Release 15.1X49-D10 and Junos OS Release 17.3R1 onwards.
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 on page 142
- Redirect Web Filtering on page 129

Local Web Filtering

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
- Local Web filtering
- Enhanced Web filtering

For more information, see the following topics:

- Understanding Local Web Filtering on page 116
- Example: Configuring Local Web Filtering on page 119

Understanding Local Web Filtering

Local web filtering allows you to define custom URL categories, which can be included in blacklists and whitelists that are evaluated on the SRX Series device. All URLs for each category in a blacklist are denied, while all URLs for each category in a whitelist are permitted.

With local Web filtering, a firewall intercepts every HTTP request in a TCP connection and extracts the URL. A decision is made by the device after it looks up a URL to determine whether it is in the whitelist or blacklist based on its user-defined category. A URL is first compared to the blacklist URLs. If a match is found, the request is blocked. If no match is found, the URL is compared to the whitelist. 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 on page 117
- User-Defined Custom URL Categories on page 117
- Local Web Filtering Profiles on page 118
- User Messages and Redirect URLs for Web Filtering on SRX Series devices on page 118
- Profile Matching Precedence on page 119

Local Web Filtering Process

The following section describes on how Web traffic is intercepted and acted upon by the Web filtering module.

1. The device intercepts a TCP connection.
2. The device intercepts each HTTP request in the TCP connection.
3. The device extracts each URL in the HTTP request and checks its URL against the user-defined whitelist and blacklist.
4. If the URL is found in the blacklist, the request is not permitted and a deny page is sent to the http client. If the URL is found in the whitelist, the request is permitted.
5. If the URL is not found in the whitelist or blacklist, 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 blacklist and whitelist 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-blacklist (block) or url-whitelist (permit) categories.

NOTE: 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:

- Blacklist — The device always blocks access to the websites in this list. Only user-defined categories are used with local Web filtering.
- Whitelist — 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 blacklist or one whitelist 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.

NOTE: Starting with Junos OS Release 17.4R1, custom category configuration is supported for local Web filtering. The custom-message option is also supported in a category for local Web filtering and Websense redirect profiles. Users can create multiple URL lists (custom categories) and apply them to a UTM Web filtering profile with actions such as permit, permit and log, block, and quarantine. To create a global whitelist or blacklist, apply a local Web filtering profile to a UTM policy and attach it to a global rule.

User Messages and Redirect URLs for Web Filtering on SRX Series devices

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 blacklist is checked first. If a match is made, the URL is blocked. If no match is found...
2. The global whitelist 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 on page 77
- Understanding Redirect Web Filtering on page 129
- Example: Configuring Local Web Filtering on page 119

Example: Configuring Local Web Filtering

This example shows how to configure local Web filtering for managing website access.

- Requirements on page 119
- Overview on page 120
- Configuration on page 121
- Verification on page 128

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 77.

Overview

In this example you configure local Web filtering custom objects, local Web filtering feature profiles, and local Web filtering UTM policies. You also attach local Web filtering UTM policies to security policies. Table 4 on page 91 shows information about local Web filtering configuration type, steps, and parameters used in this example.

Table 5: 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-black-list, and cust-permit-list respectively.	• value urllist1 • value urllist2

Table 5: Local Web filtering Configuration Type, Steps, and Parameters (continued)

Configuration Type	Configuration Steps	Configuration Parameters
Feature profiles	Configure the Web filtering feature profile:	
	• Set the URL blacklist filtering category to custurl4 and the URL whitelist filtering category to custurl3. Set the type of Web filtering engine to juniper-local.	• custurl3 • custurl4 • type juniper-local
	• Create a juniper-local profile name called localprofile1. Select a default action (permit, log-and-permit, block) for this profile for requests that experience errors. This example sets the default action to permit. Add category cust-permit-list with log-and-permit action and cus-black-list 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 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

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

Configuration

- Configuring Local Web Filtering Custom Objects and URL Patterns on page 121
- Apply Custom Objects to the Feature Profiles on page 124
- Attaching Web Filtering UTM Policies to Security Policies on page 126
- Attaching Local Web Filtering UTM Policies to Security Policies on page 127

Configuring Local Web Filtering Custom Objects and URL Patterns

CLI Quick Configuration

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

```
set security utm custom-objects url-pattern urllist1 value http://www.example1.net
set security utm custom-objects url-pattern urllist1 value 192.0.2.0
```

```
set security utm custom-objects url-pattern urllist2 value http://www.example2.net
set security utm custom-objects url-pattern urllist2 value 192.0.2.3
set security utm custom-objects url-pattern urllist3 value http://www.example3.net
set security utm custom-objects url-pattern urllist3 value 192.0.2.9
set security utm custom-objects url-pattern urllist4 value http://www.example4.net
set security utm custom-objects url-pattern urllist4 value 192.0.2.8
set security utm custom-objects custom-url-category cust-black-list value urllist1
set security utm custom-objects custom-url-category cust-permit-list value urllist2
set security utm custom-objects custom-url-category custurl3 value urllist3
set security utm custom-objects custom-url-category custurl4 value urllist4
```

Starting in Junos OS Release 15.1X49-D110, the "* " in a wildcard syntax, used for URL pattern Web filtering profile, matches all subdomains. For example, *.example.net matches:

- http://a.example.net
- http://example.net
- aaa.example.net

Step-by-Step Procedure

To configure local Web filtering using the CLI:

1. Configure a URL pattern list custom object by creating the list name and adding values to it as follows:

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

```
[edit]
user@host# set security utm custom-objects url-pattern urllist1 value
   [http://www.example1.net 192.0.2.0]
user@host# set security utm custom-objects url-pattern urllist2 value
   [http://www.example2.net 192.0.2.3]
user@host# set security utm custom-objects url-pattern urllist3 value
   [http://www.example3.net 192.0.2.9]
user@host# set security utm custom-objects url-pattern urllist4 value
   [http://www.example4.net 192.0.2.8]
```

NOTE:

- The guideline to use a URL pattern wildcard is as follows: Use ***\.[]\?*** and precede all wildcard URLs with **http://**. You can use "*" only if it is at the beginning of the URL and is followed by ".". You can use "?" only at the end of the URL.
- The following wildcard syntaxes are supported: **http://*.example.net**, **http://www.example.ne?**, **http://www.example.n??**. The following wildcard syntaxes are not supported: *.example.???, http://*example.net, http://?.

2. Applying the URL pattern to a custom URL category.

```
[edit]
user@host# set security utm custom-objects custom-url-category cust-black-list
   value urllist1
user@host# set security utm custom-objects custom-url-category cust-permit-list
   value urllist2
user@host# set security utm custom-objects custom-url-category custurl3 value
   urllist3
user@host# set security utm custom-objects custom-url-category custurl4 value
   urllist4
```

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

```
[edit]
userhost#show security utm custom-objects
  url-pattern {
    urllist1 {
      value [ http://www.example1.net 192.0.2.0 ];
    }
    urllist2 {
      value [ http://www.example2.net 192.0.2.3 ];
    }
    urllist3 {
      value [ http://www.example3.net 192.0.2.9 ];
    }
    urllist4 {
      value [ http://www.example4.net 192.0.2.8 ];
    }
  }
    custom-url-category {
      cust-black-list {
        value urllist1;
      }
      cust-permit-list {
```

```
        value urllist2;
      }
      custurl3 {
        value urllist3;
      }
      custurl4 {
        value urllist4;
      }
    }
```

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

Apply Custom Objects to the Feature Profiles

CLI Quick Configuration

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

```
set security utm feature-profile web-filtering url-whitelist custurl3
set security utm feature-profile web-filtering url-blacklist custurl4
set security utm feature-profile web-filtering type juniper-local
set security utm feature-profile web-filtering juniper-local profile localprofile1 category
  cust-black-list action block
set security utm feature-profile web-filtering juniper-local profile localprofile1 category
  cust-permit-list action log-and-permit
set security utm feature-profile web-filtering juniper-local profile localprofile1
  block-message type custom-redirect-url
set security utm feature-profile web-filtering juniper-local profile localprofile1
  block-message url http://192.0.2.10
set security utm feature-profile web-filtering juniper-local profile localprofile1
  custom-block-message "Access to this site is not permitted."
set security utm feature-profile web-filtering juniper-local profile localprofile1 default
  log-and-permit
set security utm feature-profile web-filtering juniper-local profile localprofile1
  fallback-settings default block
set security utm feature-profile web-filtering juniper-local profile localprofile1
  fallback-settings too-many-requests block
```

Step-by-Step Procedure

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

To configure local Web filtering feature profiles:

1. Configure the Web filtering URL blacklist, URL whitelist, and the Web filtering engine.

```
[edit security utm feature-profile web-filtering]
user@host# set url-whitelist custurl3
user@host# set url-blacklist custurl4
user@host# set type juniper-local
```

2. Create a profile name, and select a category from the included permit and blacklist categories. The custom category action could be block, permit, log-and-permit, and quarantine.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-local profile localprofile1 category cust-black-list action
  block
user@host# set juniper-local profile localprofile1 category cust-permit-list action
  log-and-permit
```

3. Define a redirect URL server so that instead of the device sending a block page with plain text HTML, the device send an HTTP 302 redirect to this redirect server with special variables embedded in the HTTP redirect location field. These special variables are parsed by the redirect server and serve as a special block page to the client with images and a clear text format.

```
[edit security utm feature-profile web-filtering]
user@host# set security utm feature-profile web-filtering juniper-local profile
  localprofile1 block-message type custom-redirect-url
user@host# set security utm feature-profile web-filtering juniper-local profile
  localprofile1 block-message url http://192.0.2.10
```

4. Enter a custom message to be sent when HTTP requests are blocked.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-local profile localprofile1 custom-block-message “Access
  to this site is not permitted”
```

5. Specify a default action (permit, log and permit, block, or quarantine) for the profile, when no other explicitly configured action (blacklist, whitelist, custom category, predefined category actions, or site reputation actions) is matched .

```
[edit security utm feature-profile web-filtering]
user@host# set juniper-local profile localprofile1 default log-and-permit
```

6. Configure fallback settings (block or log and permit) for this profile.

```
[edit security utm feature-profile web-filtering]
user@host# set juniper–local profile localprofile1 fallback-settings default block
user@host# set juniper–local profile localprofile1 fallback-settings
  too-many-requests block
```

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

```
[edit]
```

```
userhost#show security utm feature-profile
web-filtering {
   url-whitelist custurl3;
   url-blacklist custurl4;
   type juniper-local;
   juniper-local {
      profile localprofile1 {
         default log-and-permit;
         category {
         cust-black-list {
         action block;
         }
         cust-permit-list {
         action log-and-permit;
         }
         }
         custom-block-message "Access to this site is not permitted.";
         block-message {
         type custom-redirect-url;
         url http://192.0.2.10;
         }
         fallback-settings {
            default block;
            too-many-requests block;
         }
         }
         }
      }
   }
}
```

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

Attaching Web Filtering UTM Policies to Security Policies

CLI Quick Configuration

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

```
set security utm utm-policy utmp5 web-filtering http-profile localprofile1
```

Step-by-Step Procedure

To configure a UTM policy:

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

```
[edit]
user@host# set security utm utm-policy utmp5 web-filtering http-profile localprofile1
```

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

For brevity, this show command output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]
userhost# show security utm
utm-policy utmp5 {
   web-filtering {
      http-profile localprofile1;
   }
}
```

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

Attaching Local Web Filtering UTM Policies to Security Policies

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

```
set security policies from-zone trust to-zone untrust policy p5 match source-address any
set security policies from-zone trust to-zone untrust policy p5 match destination-address
   any
set security policies from-zone trust to-zone untrust policy p5 match application junos-http
set security policies from-zone trust to-zone untrust policy p5 then permit
   application-services utm-policy utmp5
```

Step-by-Step Procedure To attach a UTM policy to a security policy:

1. Create and configure the security policy.

```
[edit security policies from-zone trust to-zone untrust policy p5]
user@host# set match source-address any
user@host# set match destination-address any
user@host# set match application junos-http
```

2. Apply the UTM policy to the security policy.

```
[edit security policies from-zone trust to-zone untrust policy p5]
user@host# set then permit application-services utm-policy utmp5
```

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

```
[edit]
userhost# show security policies
  from-zone trust to-zone untrust {
    policy p5 {
      match {
        source-address any;
        destination-address any;
        application junos-http;
      }
      then {
        permit {
          application-services {
            utm-policy utmp5;
          }
        }
      }
    }
  }
```

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

Verification

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

- Verifying the Statistics of UTM Web Filtering on page 128

Verifying the Statistics of UTM Web Filtering

Purpose Verify the Web filtering statistics for connections including whitelist and blacklist hits and custom category hits.

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

Sample Output

user@host>**show security utm web-filtering statistics**

```
UTM web-filtering statistics:
    Total requests:                     0
    white list hit:                     0
    Black list hit:                     0
    Custom category permit:             0
    Custom category block:              0
    Custom category quarantine:         0
    Custom category qurantine block:    0
    Custom category quarantine permit:  0
    Web-filtering sessions in total:    0
    Web-filtering sessions in use:      0
    Fallback:                       log-and-permit          block
          Default                                0              0
          Timeout                                0              0
     Connectivity                                0              0
Too-many-requests                                0              0
```

See Also

- Example: Enhancing Security by Configuring Redirect Web Filtering Using Custom Objects on page 131
- Monitoring Web Filtering Configurations on page 142

Release History Table

Release	Description
17.4R1	Starting with Junos OS Release 17.4R1, custom category configuration is supported for local Web filtering. The **custom-message** option is also supported in a category for local Web filtering and Websense redirect profiles. Users can create multiple URL lists (custom categories) and apply them to a UTM Web filtering profile with actions such as permit, permit and log, block, and quarantine. To create a global whitelist or blacklist, apply a local Web filtering profile to a UTM policy and attach it to a global rule.
17.4R1	Starting with Junos OS Release 17.4R1, a new option, **custom-message**, is added for the **custom-objects** statement that enables you to configure user messages and redirect URLs to notify users when a URL is blocked or quarantined for each EWF category.
15.1X49-D110	Starting in Junos OS Release 15.1X49-D110, the "***** " in a wildcard syntax, used for URL pattern Web filtering profile, matches all subdomains.

Related Documentation

- Enhanced Web Filtering on page 80
- Whitelists on page 39

Redirect Web Filtering

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 on page 129
- Example: Enhancing Security by Configuring Redirect Web Filtering Using Custom Objects on page 131

Understanding Redirect Web Filtering

With redirect Web filtering, the Web filtering module intercepts an HTTP request. The URL in the request is then sent to the external Websense server, which makes a permit or a deny decision. If access is permitted to the URL in question, the original HTTP request and all the subsequent requests are sent to the intended HTTP server. But if access is denied to the URL in question, a blocking message is sent to the client.

This is a general description of how Web traffic is intercepted, redirected, and acted upon by the Web filtering module:

1. A Web client establishes a TCP connection with the webserver.
2. The Web client then sends an HTTP request.
3. The device intercepts the requests and extracts the URL. The URL is checked against global Web filtering whitelists and blacklists. 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.

NOTE: 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.

NOTE: Decision making from real-time options provides a higher level of accuracy, therefore caching for redirect Web filtering is not supported.

NOTE: Redirect Web filtering does not require a subscription license.

User Messages and Redirect URLs for Web Filtering on SRX Series devices

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 on page 77
- Understanding Local Web Filtering on page 116

Example: Enhancing Security by Configuring Redirect Web Filtering Using Custom Objects

This example shows how to manage Internet usage by configuring redirect Web filtering using custom objects and preventing access to inappropriate Web content.

- Requirements on page 131
- Overview on page 132
- Configuration on page 133
- Verification on page 139

Requirements

Before you begin, learn more about Web filtering. See "Web Filtering Overview" on page 77.

Overview

The benefit of using Web filtering is that it extracts the URLs from HTTP request messages and performs filtering according to the requirements. The advantage of configuring redirect Web filtering is that it extracts the URLs from the HTTP requests and sends them to an external URL filtering server to determine whether to allow or deny access.

In this example you configure redirect Web filtering custom objects, redirect Web filtering feature profiles, and redirect Web filtering UTM policies. You also attach redirect Web filtering UTM policies to security policies.

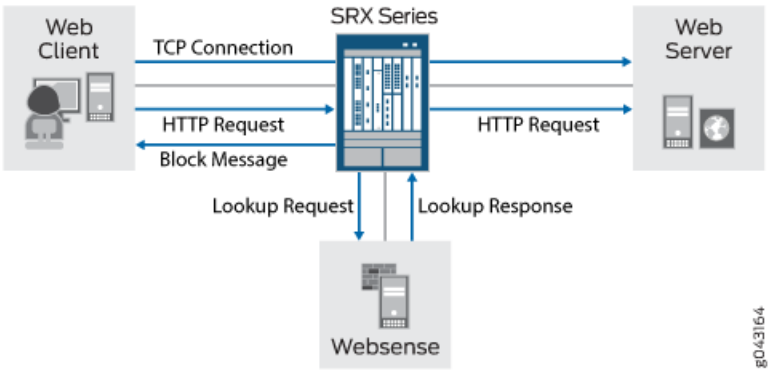
The default websense-redirect server port number is 15868.

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

Finally, you enter a timeout value in seconds. Once this limit is reached, fail mode settings are applied. The default is 15 seconds, and you can enter a value from 1 to 1800 seconds. This example sets the timeout value to 10.

Figure 1 on page 133 shows the overall architecture for the Websense redirect feature.

Figure 1: Websense Redirect Architecture



Configuration

- Configuring Redirect Web Filtering Custom Objects on page 133
- Configuring the Redirect Web Filtering Feature Profiles on page 135
- Configuring Redirect Web Filtering UTM Policies and Attaching the Redirect Web Filtering UTM Policies to Security Policies on page 137

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 blacklist.

```
[edit security utm feature-profile web-filtering]
user@host# set url-blacklist custblacklist
```

2. Configure the Web filtering URL whitelist.

```
[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 whitelist and cust-list2, respectively.

```
[edit security utm feature-profile web-filtering]
user@host# set websense-redirect profile websenseprofile1 category cust-white-list
  action log-and-permit
user@host# set websense-redirect profile websenseprofile1 category cust-list2
  action permit
```

5. Enter the port number for communicating with the server.

```
[edit security utm feature-profile web-filtering]
user@host# set websense-redirect profile websenseprofile1 server port 15868
```

6. Configure the fallback settings action **block**for this profile.

```
[edit security utm feature-profile web-filtering]
user@host# set websense-redirect profile websenseprofile1 fallback-settings default
  block
```

```
user@host# set websense-redirect profile websenseprofile1 fallback-settings
  server-connectivity block
user@host# set websense-redirect profile websenseprofile1 fallback-settings
  timeout block
user@host# set websense-redirect profile websenseprofile1 fallback-settings
  too-many-requests block
```

7. Enter the number of sockets used for communicating between the client and the server.

```
[edit security utm feature-profile web-filtering]
user@host# set websense-redirect profile websenseprofile1 sockets 1
```

8. Enter a timeout value, in seconds.

```
[edit security utm feature-profile web-filtering]
user@host# set .websense-redirect profile websenseprofile1 timeout 10
```

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

```
[edit]
userhost# show security utm feature-profile
  web-filtering {
    url-whitelist custwhitelist;
    url-blacklist custblacklist;
    type websense-redirect {
      profile websenseprofile1 {
        server {
          host Websenseserver;
          port 15868;
          }
          category {
          cust-white-list {
          action log-and-permit ;
          cust-list2 {
          action permit;
          }
          }
        }
        fallback-settings {
          server-connectivity block;
          timeout block;
          too-many-requests block;
        }
        timeout 10;
        sockets 1;
      }
    }
  }
    content-filtering {
      profile contentfilter1;
    }
```

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

Configuring Redirect Web Filtering UTM Policies and Attaching the Redirect Web Filtering UTM Policies to Security Policies

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

```
set security utm utm-policy utmp6 web-filtering http-profile websenseprofile1
```

```
set security policies from-zone trust to-zone untrust policy p6 match source-address any
set security policies from-zone trust to-zone untrust policy p6 match destination-address
   any
set security policies from-zone trust to-zone untrust policy p6 match application junos-http
set security policies from-zone trust to-zone untrust policy p6 then permit
   application-services utm-policy utmp6
```

Step-by-Step Procedure

To configure a UTM policy and attach it to a security policy:

1. Create the UTM policy referencing a profile.

```
[edit security utm]
user@host# set utm-policy utmp6 web-filtering http-profile websenseprofile1
```

2. Create and configure the security policy.

```
[edit security policies from-zone trust to-zone untrust policy p6]
user@host# set match source-address any
user@host#  set match destination-address any
user@host# set match application junos-http
```

3. Attach the UTM policy to the security policy.

```
[edit security policies from-zone trust to-zone untrust policy p6]
user@host# set then permit application-services utm-policy utmp6
```

Results

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

```
[edit]
userhost# show security utm
utm-policy utmp6 {
   web-filtering {
      http-profile websenseprofile1;
   }
}
```

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

```
[edit]
userhost# show security policies
   from-zone trust to-zone untrust {
      policy p6 {
         match {
            source-address any;
```

```
        destination-address any;
        application junos-http;
      }
      then {
        permit {
          application-services {
            utm-policy utmp6;
          }
        }
      }
    }
}
```

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

Verification

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

- Verifying the Configuration of Redirect Web Filtering Custom Objects on page 139
- Verifying the Configuration of Redirect Web Filtering Feature Profiles on page 140
- Verifying the Attachment of Redirect Web Filtering UTM Policies to Security Policies on page 140

Verifying the Configuration of Redirect Web Filtering Custom Objects

Purpose Verify the configuration of redirect Web filtering custom objects.

Action From the top of the configuration in configuration mode, enter the **show security utm custom-objects** command.

```
[edit]
userhost# show security utm custom-objects
url-pattern {
  urllist4 {
    value [ http://www.example.net 1.2.3.4 ];
  }
  urllistblack {
    value [ http://www.untrusted.com 13.13.13.13 ];
  }
  urllistwhite {
    value [ http://www.trusted.com 7.7.7.7 ];
  }
}
  custom-url-category {
    custurl4 {
      value urllist4;
    }
    custblacklist {
      value urllistblack;
    }
    custwhitelist {
```

```
        value urllistwhite;
      }
    }
```

Meaning The sample output shows the list of custom objects created.

Verifying the Configuration of Redirect Web Filtering Feature Profiles

Purpose Verify the configuration of redirect Web filtering feature profiles.

Action From the top of the configuration in configuration mode, enter the **show security utm feature-profile** command.

```
[edit]
userhost# show security utm feature-profile
  web-filtering {
    url-whitelist custwhitelist;
    url-blacklist custblacklist;
    type websense-redirect {
      profile websenseprofile1 {
        server {
          host Websenseserver;
          port 15868;
        }
        fallback-settings {
          server-connectivity block;
          timeout block;
          too-many-requests block;
        }
        timeout 10;
        sockets 1;
      }
    }
  }
    content-filtering {
      profile contentfilter1;
    }
```

Meaning The sample output shows the feature profile configured for a Websense redirect server.

Verifying the Attachment of Redirect Web Filtering UTM Policies to Security Policies

Purpose Verify the attachment of the newly created redirect Web filtering UTM policies to the security policies.

Action From the top of the configuration in configuration mode, enter the **show security utm** and **show security policies** commands.

```
[edit]
userhost# show security utm
utm-policy utmp6 {
   web-filtering {
      http-profile websenseprofile1;
   }
}
```

```
[edit]
userhost# show security policies
   from-zone trust to-zone untrust {
      policy p6 {
         match {
            source-address any;
            destination-address any;
            application junos-http;
         }
         then {
            permit {
               application-services {
                  utm-policy utmp6;
               }
            }
         }
      }
   }
```

Meaning The sample output shows the security policies to which the newly created redirect Web filtering UTM policies are attached.

See Also

- Example: Configuring Enhanced Web Filtering on page 90

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 on page 80
- Monitoring Web Filtering Configurations on page 142

Monitoring Web Filtering Configurations

Purpose View Web-filtering statistics.

Action To view Web-filtering statistics using the CLI, enter the following commands:

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

To view Web-filtering statistics using J-Web:

1. Select **Clear Web Filtering Statistics**.

   The following information is displayed in the right pane.

   ```
   Total Requests: #
   White List Hit: #
   Black List Hit: #
   Queries to Server: #
   Server Reply Permit: #
   Server Reply Block: #
   Custom Category Permit: #
   Custom Category Block: #
   Cache Hit Permit: #
   Cache Hit Block: #
   Web Filtering Session Total: #
   Web Ffiltering Session Inuse: #
   Fall Back: Log-and-Permit Block
   Default # #
   Timeout # #
   Server-Connectivity # #
   Too-Many-Requests # #
   ```

2. You can click the **Clear Web Filtering Statistics** button to clear all current viewable statistics and begin collecting new statistics.

Related Documentation

- Web Filtering Overview on page 77
- Example: Configuring Enhanced Web Filtering on page 90

CHAPTER 7

Configuration Statements

- action (Security UTM Web Filtering) on page 149
- address-blacklist on page 150
- address-whitelist on page 150
- admin-email on page 151
- administrator-email (Security Fallback Block) on page 152
- administrator-email (Security Virus Detection) on page 153
- allow-email (Security Fallback Block) on page 154
- allow-email (Security Virus Detection) on page 154
- application (Security Policies) on page 155
- application-proxy (Security UTM) on page 156
- anti-spam (Security Feature Profile) on page 157
- anti-spam (Security UTM Policy) on page 158
- anti-virus (Security Feature Profile) on page 159
- anti-virus (Security UTM Policy) on page 162
- block-command on page 163
- block-content-type on page 163
- block-extension on page 164
- block-message (Security UTM) on page 164
- block-mime on page 165
- cache on page 166
- category (Security Logging) on page 167
- category (Security Web Filtering) on page 169
- content-filtering (Security Feature Profile) on page 176
- content-filtering (Security UTM Policy) on page 178
- content-size on page 179
- content-size (Security Antivirus Sophos Engine) on page 180
- content-size-limit on page 181
- corrupt-file on page 182

- custom-block-message on page 183
- custom-message (Security Content Filtering) on page 183
- custom-message (Security Email Notify) on page 184
- custom-message (Security Fallback Block) on page 185
- custom-message (Security Fallback Non-Block) on page 186
- custom-message (Security Virus Detection) on page 187
- custom-message-subject (Security Email Notify) on page 188
- custom-message-subject (Security Fallback Block) on page 189
- custom-message-subject (Security Fallback Non-Block) on page 190
- custom-message-subject (Security Virus Detection) on page 191
- custom-objects on page 192
- custom-tag-string on page 193
- custom-url-category on page 194
- decompress-layer on page 195
- decompress-layer-limit on page 196
- default (Security Antivirus) on page 197
- default (Security Antivirus Sophos Engine) on page 198
- default (Security UTM) on page 199
- default (Security Web Filtering) on page 200
- display-host (Security Fallback Block) on page 201
- display-host (Security Virus Detection) on page 201
- download-profile (Security Antivirus FTP) on page 202
- download-profile (Security Content Filtering FTP) on page 202
- email-notify on page 203
- engine-not-ready on page 204
- engine-not-ready (Security Antivirus Sophos Engine) on page 205
- exception (Security Antivirus Mime Whitelist) on page 206
- exception (Security Content Filtering) on page 206
- fallback-block (Security Antivirus) on page 207
- fallback-non-block (Security Antivirus) on page 208
- fallback-options (Security Antivirus Juniper Express Engine) on page 209
- fallback-options (Security Antivirus Kaspersky Lab Engine) on page 210
- fallback-options (Security Antivirus Sophos Engine) on page 211
- fallback-settings (Security Web Filtering) on page 212
- fallback-settings (Security Web Filtering Juniper Local) on page 213
- fallback-settings (Security Web Filtering Websense Redirect) on page 214
- feature-profile on page 215

- filename-extension on page 222
- flag (SMTP) on page 223
- format (Security Log Stream) on page 224
- from-zone (Security Policies) on page 225
- ftp (UTM Policy Anti-Virus) on page 228
- ftp (UTM Policy Content Filtering) on page 229
- host (Security Web Filtering) on page 230
- http-profile (Security Antivirus) on page 230
- http-profile (Security Content Filtering) on page 231
- http-profile (Security Web Filtering) on page 231
- imap-profile (Security UTM Policy Antivirus) on page 232
- imap-profile (Security UTM Policy Content Filtering) on page 232
- http-persist on page 233
- http-reassemble on page 234
- intelligent-prescreening on page 235
- interval (Security Antivirus) on page 236
- ipc on page 237
- juniper-enhanced on page 238
- juniper-express-engine on page 240
- juniper-local on page 242
- kaspersky-lab-engine on page 243
- limit (UTM Policy) on page 245
- list (Security Antivirus Mime Whitelist) on page 245
- list (Security Content Filtering Block Mime) on page 246
- log (Security) on page 247
- mime-pattern on page 251
- mime-whitelist on page 252
- no-autoupdate on page 253
- no-intelligent-prescreening on page 254
- no-notify-mail-recipient on page 255
- no-notify-mail-sender (Security Content Filtering Notification Options) on page 256
- no-notify-mail-sender (Security Fallback Block) on page 257
- no-notify-mail-sender (Security Virus Detection) on page 258
- no-sbl-default-server on page 259
- notification-options (Security Antivirus) on page 260
- notification-options (Security Content Filtering) on page 261
- notify-mail-recipient on page 262

- notify-mail-sender (Security Content Filtering Notification Options) on page 263
- notify-mail-sender (Security Fallback Block) on page 264
- notify-mail-sender (Security Virus Detection) on page 265
- no-uri-check on page 266
- out-of-resources on page 267
- out-of-resources (Security Antivirus Sophos Engine) on page 268
- over-limit on page 269
- packet-filter on page 270
- password (Security Antivirus) on page 271
- password-file on page 272
- pattern-update (Security Antivirus) on page 273
- permit-command on page 274
- policies on page 275
- pop3-profile (Security UTM Policy Antivirus) on page 280
- pop3-profile (Security UTM Policy Content Filtering) on page 280
- port (Security Antivirus) on page 281
- port (Security Web Filtering Server) on page 281
- primary-server on page 282
- profile (Security Antispam SBL) on page 283
- profile (Security Antivirus Juniper Express Engine) on page 284
- profile (Security Antivirus Kaspersky Lab Engine) on page 286
- profile (Security Content Filtering) on page 288
- profile (Security Sophos Engine Antivirus) on page 289
- profile (Security Web Filtering Juniper Enhanced) on page 291
- profile (Security Web Filtering Juniper Local) on page 292
- profile (Security Web Filtering Websense Redirect) on page 293
- protocol-command on page 294
- proxy (Security Antivirus) on page 295
- quarantine-message (Security UTM) on page 296
- routing-instance (Security UTM) on page 297
- sbl on page 298
- sbl-default-server on page 298
- scan-extension on page 299
- scan-mode on page 300
- scan-options (Security Antivirus Juniper Express Engine) on page 301
- scan-options (Security Antivirus Kaspersky Lab Engine) on page 302
- scan-options (Security Antivirus Sophos Engine) on page 303

- secondary-server on page 304
- server (Security Antivirus) on page 304
- server (Security Sophos Engine Antivirus) on page 305
- server (Security Web Filtering) on page 306
- server-connectivity on page 307
- sessions-per-client on page 308
- site-reputation-action on page 309
- size (Security Web Filtering Cache) on page 310
- smtp-profile (Security UTM Policy Antispam) on page 310
- smtp-profile (Security UTM Policy Antivirus) on page 311
- smtp-profile (Security UTM Policy Content Filtering) on page 311
- sockets on page 312
- sophos-engine on page 313
- spam-action on page 315
- sxl-retry on page 316
- sxl-timeout on page 316
- timeout (Security Antivirus Fallback Options) on page 317
- timeout (Security Antivirus Fallback Options Sophos Engine) on page 318
- timeout (Security Antivirus Scan Options) on page 319
- timeout (Security Web Filtering) on page 319
- timeout (Security Web Filtering Cache) on page 320
- timeout (Security Web Filtering Fallback Settings) on page 321
- too-many-requests (Security Antivirus Fallback Options) on page 322
- too-many-requests (Security Antivirus Fallback Options Sophos Engine) on page 323
- too-many-requests (Security Web Filtering Fallback Settings) on page 324
- to-zone (Security Policies) on page 325
- traceoptions (Security Antispam) on page 327
- traceoptions (Security Antivirus) on page 328
- traceoptions (Security Application Proxy) on page 329
- traceoptions (Security Content Filtering) on page 330
- traceoptions (Security UTM) on page 331
- traceoptions (Security Web Filtering) on page 332
- traceoptions (SMTP) on page 333
- traffic-options on page 334
- trickling on page 335
- type (Security Antivirus Feature Profile) on page 336
- type (Security Content Filtering Notification Options) on page 336

- type (Security Fallback Block) on page 337
- type (Security Virus Detection) on page 338
- type (Security Web Filtering) on page 339
- upload-profile (Security Antivirus FTP) on page 339
- upload-profile (Security Content Filtering FTP) on page 340
- uri-check on page 340
- url (Security Antivirus) on page 341
- url-blacklist on page 341
- url-pattern on page 342
- url-whitelist (Security Antivirus) on page 343
- url-whitelist (Security Web Filtering) on page 343
- username (Security Antivirus) on page 344
- utm on page 345
- utm-policy on page 353
- utm-policy (Application Services) on page 354
- virus-detection (Security Antivirus) on page 355
- web-filtering on page 356
- websense-redirect on page 361

action (Security UTM Web Filtering)

Syntax

```
action (block | log-and-permit | permit | quarantine);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated profile profile-name
  category customurl-last-name]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name category
  customurl-last-name]
```

Release Information

The Surf-Control feature is not supported from Junos OS Release 15.1X49-D10 onwards.
For previous releases, statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for UTM Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Enter an action to go with the customurl-list filter.

Options

- block—Log the error and deny the traffic.
- log-and-permit—Log the error and permit the traffic.
- permit—Permit the traffic.
- quarantine—Show the warning message and permit/block the traffic based on user input.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

address-blacklist

Syntax address-blacklist *list-name*;

Hierarchy Level [edit security utm feature-profile anti-spam]
[edit security utm default-configuration]

Release Information Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description Enter an address blacklist (or whitelist) custom object for local list spam filtering.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

address-whitelist

Syntax address-whitelist *list-name*;

Hierarchy Level [edit security utm feature-profile anti-spam]
[edit security utm default-configuration]

Release Information Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description Enter an address-whitelist (or blacklist) custom-object for local list spam filtering.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

admin-email

Syntax

```
admin-email email-address;
```

Hierarchy Level

```
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update
  email-notify]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update email-notify]
[edit security utm feature-profile anti-virus sophos-engine pattern-update email-notify]
[edit security utm default-configuration anti-virus avira-engine pattern-update email-notify]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Support for Avira engine added in Junos OS Release 18.4R1.

Description

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

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

administrator-email (Security Fallback Block)

Syntax

```
administrator-email email-address;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options fallback-block]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure the administrator e-mail address that will be notified when a fallback-block occurs. This is an e-mail notification with a custom message and a custom subject line.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

administrator-email (Security Virus Detection)

Syntax

```
administrator-email email address;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine profile profile name
  notification-options virus-detection]
```

Release Information

Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure the administrator e-mail address that will be notified when a virus is detected by Sophos antivirus. This is an e-mail notification with a custom message and a custom subject line.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

allow-email (Security Fallback Block)

Syntax
```
allow-email;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options fallback-block]
```

Release Information
The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Enable e-mail notification to notify a specified administrator when a fallback-block occurs.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

allow-email (Security Virus Detection)

Syntax
```
allow–email;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus profile notification-options virus-detect]
```

Release Information
Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Enable e-mail notification to notify a specified administrator when a virus is detected.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

application (Security Policies)

Syntax

```
application {
  [application];
  any;
}
```

Hierarchy Level

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match]

[edit security policies global policy *policy-name* match]

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Specify the IP or remote procedure call (RPC) application or set of applications to be used as match criteria.

Starting in Junos OS Release 19.1R1, configuring the **application** statement at the **[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match]** hierarchy level is optional if the **dynamic-application** statement is configured at the same hierarchy level.

Options

application-name-or-set—Name of the predefined or custom application or application set used as match criteria.

any—Any predefined or custom applications or application sets.

NOTE: A custom application that does not use a well-known destination port for the application will not be included in the any option, and must be named explicitly.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Policies Overview*
- *Configuring Applications in Unified Policies*

application-proxy (Security UTM)

Syntax

```
application-proxy {
  traceoptions {
    flag flag;
  }
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure trace options for the application proxy.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

anti-spam (Security Feature Profile)

Syntax

```
anti-spam {
  address-blacklist list-name;
  address-whitelist list-name;
  sbl {
    profile profile-name {
      custom-tag-string [string];
      (sbl-default-server | no-sbl-default-server);
      spam-action (block | tag-header | tag-subject);
    }
  }
  traceoptions flag flag;
}
```

Hierarchy Level

```
[edit security utm feature-profile]
[edit security utm default-configuration]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure UTM antispam features. You can also configure the default UTM configuration for antispam feature profile. If you do not configure any option in the antispam feature profile, the values configured in the default UTM configuration are applied.

The antispam feature examines transmitted e-mail messages to identify e-mail spam. When the device detects a message deemed to be spam, it blocks the e-mail message or tags the e-mail message header or subject with a preprogrammed string. Antispam filtering uses both a third-party server-based Spam Block List (SBL) and optionally created local whitelists (benign) and blacklists (malicious) for filtering against e-mail messages.

NOTE: A license check for the antispam configuration is performed at the time of a commit and will provide a warning if a valid license is not installed on the device. Once a valid license is installed on the device then a custom antispam profile or the default profile will be able to process traffic. If a license is expired or is not installed, the antivirus service will not process traffic.

In the default UTM profile, the antispam type is configured as SBL instead of none. This configuration enables SBL. However, to use this feature, you must enable the SBL server using the **[edit security utm default-configuration anti-spam sbl sbl-default-server]** command.

Options

anti-spam—Configure antispam feature.

address-blacklist—Enter an address blacklist custom object for local list spam filtering.

address-whitelist—Enter an address-whitelist custom-object for local list spam filtering.

sbl—Antispam filtering allows you to use both a third-party server-based spam block list (SBL) and to optionally create your own local whitelists and blacklists for filtering against e-mail messages.

traceoptions—Defines tracing operations for UTM antispam features.

type—Antispam type.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

anti-spam (Security UTM Policy)

Syntax

```
anti-spam {
  smtp-profile profile-name;
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name]
[edit logical-systems logical-system-name security utm utm-policy policy-name]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for configuration in logical systems introduced in Junos OS Release 18.3R1.

Description
Configures a UTM policy for the antispam SMTP protocol and attach this policy to a security profile to implement it. The device can block and drop detected spam at either the connection level or the e-mail level. When the SMTP sender is identified as a spam sender based on its IP address, the SMTP connection is rejected and dropped. When a particular e-mail sender is identified as spam sender based on its sender address, the e-mail is rejected and dropped.

Options
The statements are explained separately. See CLI Explorer.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Antispam Filtering Overview on page 43

anti-virus (Security Feature Profile)

Syntax

```
anti-virus {
  mime-whitelist {
    exception;
    list;
  }
  sophos-engine {
    fallback-options {
      content-size (block | log-and-permit | permit);
      default (block | log-and-permit | permit);
      engine-not-ready (block | log-and-permit | permit);
      out-of-resources (block | log-and-permit | permit);
      timeout (block | log-and-permit | permit);
      too-many-requests (block | log-and-permit | permit);
    }
    notification-options {
      fallback-block {
        custom-message;
        custom-message-subject;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
      fallback-non-block {
        custom-message;
        custom-message-subject;
        (notify-mail-recipient | no-notify-mail-recipient);
      }
      virus-detection {
        custom-message;
        custom-message-subject;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
    }
    pattern-update {
      email-notify {
        admin-email;
        custom-message;
        custom-message-subject;
      }
      interval;
      no-autoupdate;
      proxy {
        password;
        port;
        server;
        username;
      }
      routing-instance;
      url;
    }
    scan-options {
```

```
        content-size-limit;
        timeout seconds;
        (uri-check | no-uri-check);
    }
    server {
        ip;
        routing-instance;
    }
    sxl-retry;
    sxl-timeout seconds;
    trickling timeout;
  }
  traceoptions {
    flag name;
  }
  url-whitelist;
}
```

Hierarchy Level

```
[edit security utm feature-profile]
[edit security utm default-configuration]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure UTM Sophos antivirus features. You can also configure the default UTM configuration for antivirus feature profile. If you do not configure any option in the antivirus feature profile, the values configured in the default UTM configuration are applied. Antivirus, one of several features including content filtering, antispam, and Web filtering, makes up Juniper's UTM suite, provides the ability to prevent threats at the gateway before they enter the network.

NOTE: A license check for the antivirus configuration is performed at the time of a commit and will provide a warning if a valid license is not installed on the device. Once a valid license is installed on the device then a custom antivirus profile or the default profile will be able to process traffic. If a license is expired or is not installed, the antivirus service will not process traffic.

Options

anti-virus—Configure antivirus feature.

mime-whitelist—This is the comprehensive list for those MIME types that can bypass antivirus scanning.

sophos-engine—The antivirus engine that is used on the device. You can only have one engine type running and you must restart the device if you change engines.

fallback-options—Fallback options tell the system how to handle the errors.

notification-options—There are multiple notification options you can configure to trigger when a virus is detected.

fallback-non-block—Notifications for fallback nonblocking actions.

virus-detection—Notification to send when a virus is detected.

pattern-update—You can configure the security device to regularly update the pattern file automatically, or you can update the file manually.

scan-options—Antivirus sophos-engine scan options.

server—Sophos Antivirus (SAV) and antispam first hop DNS server.

sxl-retry—Number of retry attempts to the remote Sophos Extensible List (SXL) server when a request timeout occurs.

Range: 0 through 5

sxl-timeout —Timeout value for responses to a Sophos checksum or URI query.

Range: 1 through 5

trickling —HTTP trickling is a mechanism used to prevent the HTTP client or server from timing-out during a file transfer or during antivirus scanning.

traceoptions —Define tracing operations for UTM antivirus features.

url-whitelist—Antivirus URL white list. A URL whitelist is a unique custom list that you define in which all the URLs or IP addresses in that list for a specified category are always bypassed for scanning.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

anti-virus (Security UTM Policy)

Syntax

```
anti-virus {
  ftp {
    download-profile profile-name;
    upload-profile profile-name;
  }
  http-profile profile-name;
  imap-profile profile-name;
  pop3-profile profile-name;
  smtp-profile profile-name;
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name]
[edit logical-systems logical-systems-name security utm utm-policy policy-name]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for configuration in logical systems introduced in Junos OS Release 18.3R1.

Description

Configures a UTM policy for the antivirus protocols and attaches this policy to a security profile to implement it. The internal antivirus scan engine supports scanning for specific Application Layer transactions allowing you to select the content (HTTP, FTP, SMTP, POP3, or IMAP traffic) to scan.

Options

The statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Unified Threat Management Overview*

block-command

Syntax
block-command *protocol-command-list*;

Hierarchy Level
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile *profile-name*]

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Apply protocol block command custom-objects to the content-filtering profile.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

block-content-type

Syntax
block-content-type (activex | exe | http-cookie | java-applet | zip);

Hierarchy Level
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile *profile-name*]

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Apply blocks to other available content such as exe, http-cookie, java-applet. This is for HTTP only.

Options
- **activex**—Block ActiveX.
- **exe**—Block EXE files.
- **http-cookie**—Block cookies.
- **java-applet**—Block Java applets.
- **zip**—Block ZIP files.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

block-extension

Syntax

```
block-extension extension-list;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Apply block extensions to the content-filtering profile.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

block-message (Security UTM)

Syntax

```
block-message {
  type {
    custom-redirect-url;
  }
  url url;
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure Juniper enhanced block message settings.

Options

- **type**—Specify the following type of the block message:
  - **custom-redirect-url**—Specify Custom redirect URL server.
- **url *url***—Specify an URL of the block message.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

block-mime

Syntax

```
block-mime {
  exception list-name;
  list list-name;
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Apply MIME pattern list custom-objects to the content-filtering profile for blocking MIME types.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

cache

Syntax

```
cache {
  size value;
  timeout value;
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated]
[edit security utm feature-profile web-filtering juniper-enhanced]
```

Release Information

The Surf-Control feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 for surf-control integrated.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Set the cache parameters for Surf-Control-Integrated Web filtering and Enhanced Web Filtering.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

category (Security Logging)

Syntax

```
category (all | content-security | fw-auth | screen | alg | nat | flow | sctp | gtp | ipsec | idp |
  rtlog | pst-ds-lite | appqos | secintel)
```

Hierarchy Level

```
[edit security log stream stream-name]
[edit logical-systems name security log stream stream-name]
[edit tenants tenant-name security log stream stream-name]
```

Release Information

Statement introduced in Junos OS Release 10.0. Statement modified in Junos OS Release 15.1X49-D40.
The [edit **logical-systems** *name* security log stream *stream-name*] hierarchy level introduced in Junos OS Release 18.2R1.
The [edit **tenants** *tenant-name* security log stream *stream-name*] hierarchy levels introduced in Junos OS Release 18.3R1.

Description

Set the category of logging to **all** or **content-security**. Note that for the WELF format, the category must be set to **content-security**.

Options

- **all**—All events are logged. By default, all the events listed in the **category** parameter are logged.
- **content-security**—Only content security events are logged.
- **fw-auth**—Firewall authentication events are logged.
- **screen**—Screen events are logged.
- **alg**—Application Layer Gateway (ALG) events are logged.
- **nat**—Network Address Translation (NAT) events are logged.
- **flow**—Flow events are logged.
- **sctp**—Stream Control Transmission Protocol (SCTP) events are logged.
- **gtp**—GPRS Tunneling Protocol (GTP) events are logged.
- **ipsec**—IPsec events are logged.
- **idp**—Intrusion Detection and Prevention (IDP) events are logged.
- **rtlog**—RTLOG system log events are logged.
- **pst-ds-lite**—PST dual-stack lite (DS-Lite) events are logged.
- **appqos**—Application quality of service (AppQoS) events are logged.
- **secintel**—Juniper Networks Security Intelligence (SecIntel) events are logged.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Application Security Feature Guide for Security Devices*
- *Logical Systems and Tenant Systems Feature Guide for Security Devices*

category (Security Web Filtering)

Syntax

```
category name{
  action (block | log-and-permit | permit | quarantine);
  custom-message message-name;
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated profile profile-name]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering. Support for new categories and category name updates by Websense added in Junos OS Release 12.1X47-D15 and 12.3X48-D10.
Starting with Junos OS Release 15.1X49-D10, the SurfControl integrated feature is no longer supported. For previous releases, statement introduced in Junos OS Release 9.5.
The **custom-message** option introduced in Junos OS Release 15.1X49-D110.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Select a custom URL category list you created (custom objects) for filtering against. The **custom-message** configuration option is used to notify the users when the URL is blocked or quarantined for each EWF category. You can customize the message with options such as user message or redirect URL. User messages indicate that website access has been blocked by an organization's access policy. Redirect URLs redirect a blocked or quarantined URL to any user-defined URL. Table 6 on page 170 shows the list of categories predefined by Websense.

Starting with Junos OS Release 17.4R1, you can download and dynamically load new Enhanced Web Filtering (EWF) categories. The downloading and dynamic loading of the new EWF categories do not require a software upgrade. Websense occasionally releases new EWF categories. EWF classifies websites into categories according to host, URL, or IP address and performs filtering based on the categories.

NOTE: Existing configurations are not affected by the new categories but can be modified to make use of the new categories.

Table 6: List of Categories Predefined by Websense

Category ID	Category Name	Parent ID
1	Adult Material	0
2	Business and Economy	0
3	Education	0
4	Government	0
5	News and Media	0
6	Religion	0
7	Society and Lifestyles	0
8	Special Events	0
9	Information Technology	0
10	Abortion	0
11	Advocacy Groups	0
12	Entertainment	0
13	Gambling	0
14	Games	0
15	Illegal or Questionable	0
16	Job Search	0
17	Shopping	0
18	Sports	0
19	Tasteless	0
20	Travel	0
21	Vehicles	0
22	Violence	0
23	Weapons	0
24	Drugs	0

Table 6: List of Categories Predefined by Websense (continued)

Category ID	Category Name	Parent ID
25	Militancy and Extremist	0
26	Intolerance	0
27	Health	0
28	Website Translation	9
29	Advertisements	110
64	User-Defined	0
65	Nudity	1
66	Adult Content	1
67	Sex	1
68	Financial Data and Services	2
69	Cultural Institutions	3
70	Media File Download	12
72	Military	4
73	Political Organizations	4
74	General Email	91
75	Proxy Avoidance	9
76	Search Engines and Portals	9
78	Web Hosting	9
79	Web Chat	91
80	Hacking	9
81	Alternative Journals	5
82	Non-Traditional Religions	6
83	Traditional Religions	6
84	Restaurants and Dining	7

Table 6: List of Categories Predefined by Websense (continued)

Category ID	Category Name	Parent ID
85	Gay or Lesbian or Bisexual Interest	7
86	Personals and Dating	7
87	Alcohol and Tobacco	7
88	Prescribed Medications	24
89	Nutrition	24
90	Abused Drugs	24
91	Internet Communication	0
92	Pro-Choice	10
93	Pro-Life	10
94	Sex Education	1
95	Lingerie and Swimsuit	1
96	Online Brokerage and Trading	110
97	Educational Institutions	3
98	Instant Messaging	110
99	Application and Software Download	110
100	Pay-to-Surf	110
101	Internet Auctions	17
102	Real Estate	17
103	Hobbies	7
107	Sport Hunting and Gun Clubs	18
108	Internet Telephony	116
109	Streaming Media	116
110	Productivity	0
111	Marijuana	24

Table 6: List of Categories Predefined by Websense (continued)

Category ID	Category Name	Parent ID
112	Message Boards and Forums	110
113	Personal Network Storage and Backup	116
114	Internet Radio and TV	116
115	Peer-to-Peer File Sharing	116
116	Bandwidth	0
117	Social Networking and Personal Sites	7
118	Educational Materials	3
121	Reference Materials	3
122	Social Organizations	0
123	Service and Philanthropic Organizations	122
124	Social and Affiliation Organizations	122
125	Professional and Worker Organizations	122
126	Security	0
128	Malicious Web Sites	126
138	Computer Security	9
146	Miscellaneous	0
147	Web Infrastructure	146
148	Web Images	146
149	Private IP Addresses	146
150	Content Delivery Networks	146
151	Dynamic Content	146
152	Network Errors	146
153	Uncategorized	146
154	Spyware	126

Table 6: List of Categories Predefined by Websense (continued)

Category ID	Category Name	Parent ID
156	File Download Servers	146
164	Phishing and Other Frauds	126
166	Keyloggers	126
167	Potentially Unwanted Software	126
172	Bot Networks	126
191	Extended Protection	0
192	Elevated Exposure	191
193	Emerging Exploits	191
194	Suspicious Content	191
195	Organizational Email	91
196	Text and Media Messaging	91
200	Web and Email Spam	9
220	Compromised Websites	0
221	Newly Registered Websites	0
222	Collaboration Office	0
223	Office Mail	222
224	Office Drive	222
225	Office Documents	222
226	Office Apps	222
227	Web Analytics	9
228	Web and Email Marketing	9
1529	Classifieds Posting	0
1530	Blog Posting	0
1531	Blog Commenting	0

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Understanding Redirect Web Filtering on page 129

content-filtering (Security Feature Profile)

Syntax

```
content-filtering {
  block-command;
  block-content-type {
    activex;
    exe;
    http-cookie;
    java-applet;
    zip;
  }
  block-extension;
  block-mime {
    exception;
    list;
  }
  notification-options {
    custom-message;
    (notify-mail-sender | no-notify-mail-sender);
    type (message | protocol-only);
  }
  permit-command;
  traceoptions {
    flag name;
  }
  type (content-filtering-none | local);
}
```

Hierarchy Level

```
[edit security utm feature-profile]
[edit security utm default-configuration]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure UTM content-filtering features. You can also configure the default UTM configuration for content filtering feature profile. If you do not configure any option in the content filtering feature profile, the values configured in the default UTM configuration are applied. The content filtering feature controls file transfers across the gateway by checking traffic against configured filter lists. It evaluates the traffic before all other UTM features, except Web filtering.

NOTE: A license check for the content filtering configuration is performed at the time of a commit and will provide a warning if a valid license is not installed on the device. Once a valid license is installed on the device then a custom content filtering profile or the default profile will be able to process traffic. If a license is expired or is not installed, the content filtering service will not process traffic.

Options

block-command—Protocol block command custom-objects to the content-filtering profile.

block-content-type—Blocks to other available content such as exe, http-cookie, java-applet. This is for HTTP only.

block-extension—Block extensions to the content-filtering profile.

block-mime—MIME pattern list custom-objects to the content-filtering profile for blocking MIME types.

notification-options—A message notification to trigger when a content filter is matched.

permit-command—Protocol permit command custom-objects to the content-filtering profile.

traceoptions—Defines tracing operations for default UTM configuration for content filtering feature.

type—Type of content filtering solution or URL filtering solution used by the device.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

content-filtering (Security UTM Policy)

Syntax

```
content-filtering {
  ftp {
    download-profile profile-name;
    upload-profile profile-name;
  }
  http-profile profile-name;
  imap-profile profile-name;
  pop3-profile profile-name;
  smtp-profile profile-name;
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name]
[edit logical-systems logical-systems-name security utm utm-policy policy-name]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for configuration in logical systems introduced in Junos OS Release 18.3R1.

Description

Configures a UTM policy for the content filtering protocols and attach this policy to a security profile to implement it. Each supported protocol may implement available content filters differently. Not all filtering capabilities are supported for each protocol. The HTTP protocol supports all content filtering features. The FTP protocol supports only lock Extension List and Protocol Command Block List. The e-mail protocols (SMTP, IMAP, POP3) supports limited to Block Extension List, Protocol Command Block List, and MIME Pattern Filtering.

Options

The statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- Content Filtering Overview on page 63

content-size

Syntax

```
content-size (block | log-and-permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  fallback-options]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

If the content size exceeds a set limit, the content is either passed or blocked. The default action is log-and-permit.

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

Options

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

content-size (Security Antivirus Sophos Engine)

Syntax

```
content-size (block | log-and-permit | permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  fallback-options]
```

Release Information

Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

If the content size exceeds a set limit, the content is either passed or blocked.

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

Options

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic
- **permit**—Permit the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Sophos Antivirus Configuration Overview*

content-size-limit

Syntax

```
content-size-limit value;
```

Hierarchy Level

```
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  scan-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  scan-options]
[edit security utm default-configuration anti-virus scan-options]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for Avira engine added in Junos OS Release 18.4R1.

Description

The content size check occurs before the scan request is sent. The content size refers to accumulated TCP payload size. The maximum configurable content size varies with different platforms. For example, the content size ranges from 20 through 40,000 for SRX4100.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

corrupt-file

Syntax

```
corrupt-file (block | log-and-permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  fallback-options]
```

Release Information

The Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Corrupt file is the error returned by the scan engine when engine detects a corrupted file. The default action is log-and-permit.

Options

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Full Antivirus Configuration Overview*

custom-block-message

Syntax
custom-block-message *value*;

Hierarchy Level
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated profile *profile-name*]
[edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name*]

Release Information
The Surf-Control feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Enter a custom message to be sent when HTTP requests are blocked.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

custom-message (Security Content Filtering)

Syntax
custom-message *message*;

Hierarchy Level
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile *profile-name* notification-options]

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Custom message notifications are generally used when content is blocked by the content filter.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Content Filtering Overview on page 63

custom-message (Security Email Notify)

Syntax

```
custom-message message;
```

Hierarchy Level

```
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update
  email-notify]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update email-notify]
[edit security utm feature-profile anti-virus sophos-engine pattern-update email-notify]
[edit security utm default-configuration anti-virus avira-engine pattern-update email-notify]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for Avira engine added in Junos OS Release 18.4R1.

Description

You can configure the device to notify a specified administrator when patterns are updated. This is an e-mail notification with a custom message.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

custom-message (Security Fallback Block)

Syntax

```
custom-message message;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options fallback-block]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

custom-message (Security Fallback Non-Block)

Syntax

```
custom-message message;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options fallback-non-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options fallback-non-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options fallback-non-block]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

custom-message (Security Virus Detection)

Syntax

```
custom-message message;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options virus-detection]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options virus-detection]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options virus-detection]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

custom-message-subject (Security Email Notify)

Syntax

```
custom-message-subject message-subject;
```

Hierarchy Level

```
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update
  email-notify]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update email-notify]
[edit security utm feature-profile anti-virus sophos-engine pattern-update email-notify]
[[edit security utm default-configuration avira-engine pattern-update email-notify]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for Avira engine added in Junos OS Release 18.4R1.

Description

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

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

custom-message-subject (Security Fallback Block)

Syntax

```
custom-message-subject message-subject;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options fallback-block]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file. As part of a custom message, you can customize the message subject line.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

custom-message-subject (Security Fallback Non-Block)

Syntax

```
custom-message-subject message-subject;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options fallback-non-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options fallback-non-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options fallback-non-block]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file. As part of a custom message, you can customize the message subject line.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

custom-message-subject (Security Virus Detection)

Syntax

```
custom-message-subject message-subject;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options virus-detection]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options virus-detection]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options virus-detection]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file. As part of a custom message, you can customize the message subject line.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

custom-objects

Syntax

```
custom-objects {
  custom-url-category object-name {
    value [value];
  }
  custom-message {
    name message-name;
    type redirect-url | user-message;
    content redirect-url by user| user-message by user;
  }
  filename-extension object-name {
    value [value];
  }
  mime-pattern object-name {
    value [value];
  }
  protocol-command object-name {
    value [value];
  }
  url-pattern object-name {
    value [value];
  }
}
```

Hierarchy Level

```
[edit security utm]
[edit security utm default-configuration]
[edit logical-systems logical-system-name security utm]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level introduced in Junos OS Release 18.2R1.
Support for configuration in logical systems introduced in Junos OS Release 18.3R1.

Description

Configure custom objects before configuring UTM feature-profile features.

WARNING: Custom category does not take precedence over predefined categories when it has the same name as one of the predefined categories. We do not recommend having a custom category name be the same as the predefined category name.

NOTE: Starting from Junos OS Release 17.4R1, support for custom category configuration is available for EWF, local, and Websense redirect profiles.

Options The statements are explained separately. See CLI Explorer.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Unified Threat Management Overview*

custom-tag-string

Syntax
```
custom-tag-string [string];
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm feature-profile anti-spam sbl profile profile-name]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

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

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

custom-url-category

Syntax

```
custom-url-category object-name {
  value [value];
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm custom-objects]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Use URL pattern lists to create Custom URL category lists. These are lists of patterns that bypass scanning.

WARNING: Custom category does not take precedence over predefined categories when it has the same name as one of the predefined categories. We do not recommend having a custom category name be the same as the predefined category name.

Options

- ***object-name***—Name of the URL category-list object.
- **value *value***—Value of the URL category-list object. You can configure multiple values separated by spaces and enclosed in square brackets.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *UTM Overview*

decompress-layer

Syntax

```
decompress-layer (block | log-and-permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  fallback-options]
```

Description

The Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, decompress layer error is the error returned by the scan engine when the scanned file has too many compression layers. The default action is block.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Options

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Full Antivirus Configuration Overview*

decompress-layer-limit

Syntax

```
decompress-layer-limit value;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  scan-options]
[edit anti-virus scan-options]
[edit security utm default-configuration anti-virus scan-options]
```

Release Information

The Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for Avira engine added in Junos OS Release 18.4R1.

Description

The decompression layer limit specifies how many layers of nested compressed files and files with internal extractable objects, such as archive files (tar), the internal antivirus scanner can decompress before it executes the virus scan.

Range: 0 through 10

Default: 3

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Full Antivirus Configuration Overview*

default (Security Antivirus)

Syntax

```
default (block | log-and-permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  fallback-options]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

All errors other than those specifically listed fall into this category. This could include either unhandled system exceptions (internal errors) or other unknown errors.

Options

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

default (Security Antivirus Sophos Engine)

Syntax

```
default (block | log-and-permit | permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  fallback-options]
```

Release Information

Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

All errors other than those specifically listed fall into this category. This could include either unhandled system exceptions (internal errors) or other unknown errors.

Options

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic
- **permit**—Permit the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

default (Security UTM)

Syntax

```
default (block |log-and-permit | permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 11.4.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Specify the default action to take for a URL.

Options

- block—Log the error and deny the traffic.
- log-and-permit—Log the error and permit the traffic.
- permit—Permit the traffic.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

default (Security Web Filtering)

Syntax

```
default (block | log-and-permit | permit | quarantine);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated profile profile-name
  fallback-settings]
[edit security utm feature-profile web-filtering websense-redirect profile profile-name
  fallback-settings]
[edit security utm feature-profile web-filtering juniper–local profile profile-name
  fallback-settings]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name
  fallback-settings]
```

Release Information

The Surf-Control feature is not supported from Junos OS Release 15.1X49-D10 onwards.
For previous releases, statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Specify an action for the profile, for requests that experience internal errors in the Web-filtering module.

Options

- block—Log the error and deny the traffic.
- log-and-permit—Log the error and permit the traffic.
- permit —Permit the traffic.
- quarantine—Show the warning message and permit/block the traffic based on user input.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

display-host (Security Fallback Block)

Syntax

```
display-host;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options fallback-block]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Display the computer host name in the notification e-mail sent to the administrator when a fallback-block notification occurs.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

display-host (Security Virus Detection)

Syntax

```
display-host;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus profile profile name notification-options
  virus-detection]
```

Release Information

Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Display the computer host name in the notification e-mail sent to the administrator when a virus is detected by Sophos antivirus.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

download-profile (Security Antivirus FTP)

Syntax
```
download-profile profile-name;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name anti-virus ftp]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Configure a UTM policy for the antivirus FTP (download) protocol and attach this policy to a security profile to implement it.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

download-profile (Security Content Filtering FTP)

Syntax
```
download-profile profile-name;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name content-filtering ftp]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Configure a UTM policy for the content-filtering FTP (download) protocol and attach this policy to a security profile to implement it.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Content Filtering Overview on page 63

email-notify

Syntax

```
email-notify {
  admin-email email-address;
  custom-message message;
  custom-message-subject message-subject;
}
```

Hierarchy Level

```
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update]
[edit security utm feature-profile anti-virus sophos-engine pattern-update]
[edit security utm default-configuration anti-virus avira-engine pattern-update]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for Avira engine added in Junos OS Release 18.4R1.

Description

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

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

engine-not-ready

Syntax

```
engine-not-ready (block | log-and-permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  fallback-options]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

The scan engine is initializing itself, for example, loading the signature database. During this phase, it is not ready to scan a file. A file could either pass or be blocked according to this setting. The default action is block.

Options

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

engine-not-ready (Security Antivirus Sophos Engine)

Syntax

```
default (block | log-and-permit | permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  fallback-options]
```

Release Information

Statement introduced in Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

The scan engine is initializing itself, for example, loading the signature database. During this phase, it is not ready to scan a file. A file could either pass or be blocked according to this setting.

Options

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic
- **permit**—Permit the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Sophos Antivirus Configuration Overview*

exception (Security Antivirus Mime Whitelist)

Syntax
```
exception listname;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus mime-whitelist]
[edit security utm feature-profile anti-virus mime-whitelist list listname]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Configure the antivirus scanner to use an exception list to the MIME bypass list (custom objects). To use the exception list, you first create a whitelist custom-object list with the **list** statement. The system will first look at any existing whitelist mime pattern. If it matches an item, it will then continue to look for any exceptions to the whitelist and will then scan any item in the exception list.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

exception (Security Content Filtering)

Syntax
```
exception list-name;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name block-mime]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Configure the content filter to use an exception list to the MIME block list (custom objects).

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Content Filtering Overview on page 63

fallback-block (Security Antivirus)

Syntax

```
fallback-block {
  administrator-email email-address;
  allow-email;
  custom-message message;
  custom-message-subject message-subject;
  display-host;
  (notify-mail-sender | no-notify-mail-sender);
  type (message | protocol-only);
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure notifications for fallback blocking actions. Fallback options tell the system how to handle the errors returned by either the scan engine or the scan manager.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

fallback-non-block (Security Antivirus)

Syntax

```
fallback-non-block {
  custom-message message;
  custom-message-subject message-subject;
  (notify-mail-recipient | no-notify-mail-recipient);
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options]
```

Release Information

The Express and Kaspersky antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure notifications for fallback nonblocking actions.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

fallback-options (Security Antivirus Juniper Express Engine)

Syntax

```
fallback-options {
  content-size (block | log-and-permit);
  default (block | log-and-permit);
  engine-not-ready (block | log-and-permit);
  out-of-resources (block | (log-and-permit);
  timeout (block | log-and-permit);
  too-many-requests (block | log-and-permit);
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name]
```

Release Information

The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Fallback options tell the system how to handle the errors.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Express Antivirus Configuration Overview*

fallback-options (Security Antivirus Kaspersky Lab Engine)

Syntax

```
fallback-options {
  content-size (block | log-and-permit);
  corrupt-file (block | log-and-permit);
  decompress-layer (block | log-and-permit);
  default (block | log-and-permit);
  engine-not-ready (block | log-and-permit);
  out-of-resources (block | (log-and-permit);
  password-file (block | (log-and-permit);
  timeout (block | log-and-permit);
  too-many-requests (block | log-and-permit);
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name]
```

Release Information

The Kaspersky feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 .
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Fallback options tell the system how to handle the errors returned by either the scan engine or the scan manager.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Full Antivirus Configuration Overview*

fallback-options (Security Antivirus Sophos Engine)

Syntax

```
fallback-options {
  content-size (block | log-and-permit | permit);
  default (block | log-and-permit | permit);
  engine-not-ready (block | log-and-permit | permit);
  out-of-resources (block | log-and-permit | permit);
  timeout (block | log-and-permit | permit);
  too-many-requests (block | log-and-permit | permit);
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure fallback options to instruct the system how to handle errors.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Sophos Antivirus Configuration Overview*

fallback-settings (Security Web Filtering)

Syntax

```
fallback-settings {
  default (block | log-and-permit);
  server-connectivity (block | log-and-permit);
  timeout (block | log-and-permit);
  too-many-requests (block | log-and-permit);
}
```

Hierarchy Level

[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated profile *profile-name*]
[edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name*]

Release Information

The Surf-Control feature is not supported from Junos OS Release 15.1X49-D10 onwards.
For previous releases, Statement introduced in Junos OS Release 9.5 .
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Fallback settings tell the system how to handle errors.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

fallback-settings (Security Web Filtering Juniper Local)

Syntax

```
fallback-settings {
  default (block | log-and-permit);
  server-connectivity (block | log-and-permit);
  timeout (block | log-and-permit);
  too-many-requests (block | log-and-permit);
}
```

Hierarchy Level

[edit security utm default-configuration]
[edit security utm feature-profile web-filtering juniper–local profile *profile-name*]

Release Information

Statement introduced in Junos OS Release 10.0.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Fallback settings tell the system how to handle errors.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- Web Filtering Overview on page 77

fallback-settings (Security Web Filtering Websense Redirect)

Syntax

```
fallback-settings {
  default (block | log-and-permit);
  server-connectivity (block | log-and-permit);
  timeout (block | log-and-permit);
  too-many-requests (block | log-and-permit);
}
```

Hierarchy Level

[edit security utm default-configuration]
[edit security utm feature-profile web-filtering websense-redirect profile *profile-name*]

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Fallback settings tell the system how to handle errors.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- Understanding Redirect Web Filtering on page 129

feature-profile

Syntax

```
feature-profile {
  anti-spam {
    address-blacklist list-name;
    address-whitelist list-name;
    sbl {
      profile profile-name {
        custom-tag-string [string];
        (sbl-default-server | no-sbl-default-server);
        spam-action (block | tag-header | tag-subject);
      }
    }
    traceoptions flag flag;
  }
  anti-virus {
    juniper-express-engine {
      pattern-update {
        email-notify {
          admin-email email-address;
          custom-message message;
          custom-message-subject message-subject;
        }
        interval value;
        no-autoupdate;
        proxy {
          password password-string;
          port port-number;
          server address-or-url;
          username name;
        }
        url url;
      }
      profile profile-name {
        fallback-options {
          content-size (block | log-and-permit);
          default (block | log-and-permit);
          engine-not-ready (block | log-and-permit);
          out-of-resources (block | (log-and-permit);
          timeout (block | log-and-permit);
          too-many-requests (block | log-and-permit);
        }
        notification-options {
          fallback-block {
            administrator-email email-address;
            allow-email;
            custom-message message;
            custom-message-subject message-subject;
            display-host;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
          }
          fallback-non-block {
```

```
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-recipient | no-notify-mail-recipient);
          }
          virus-detection {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
          }
        }
        scan-options {
          content-size-limit value;
          (intelligent-prescreening | no-intelligent-prescreening);
          timeout value;
        }
        trickling {
          timeout value;
        }
      }
    }
    kaspersky-lab-engine {
      pattern-update {
        email-notify {
          admin-email email-address;
          custom-message message;
          custom-message-subject message-subject;
        }
        interval value;
        no-autoupdate;
        proxy {
          password password-string;
          port port-number;
          server address-or-url;
          username name;
        }
        url url;
      }
      profile profile-name {
        fallback-options {
          content-size (block | log-and-permit);
          corrupt-file (block | log-and-permit);
          decompress-layer (block | log-and-permit);
          default (block | log-and-permit);
          engine-not-ready (block | log-and-permit);
          out-of-resources (block | (log-and-permit);
          password-file (block | (log-and-permit);
          timeout (block | log-and-permit);
          too-many-requests (block | log-and-permit);
        }
        notification-options {
          fallback-block {
            administrator-email email-address;
            allow-email;
            custom-message message;
```

```
            custom-message-subject message-subject;
            display-host;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
          }
          fallback-non-block {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-recipient | no-notify-mail-recipient);
          }
          virus-detection {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
          }
        }
        scan-options {
          content-size-limit value;
          decompress-layer-limit value;
          (intelligent-prescreening | no-intelligent-prescreening);
          scan-extension filename;
          scan-mode (all | by-extension);
          timeout value;
        }
        trickling {
          timeout value;
        }
      }
    }
    mime-whitelist {
      exception listname;
      list listname {
        exception listname;
      }
    }
    sophos-engine {
      pattern-update {
        email-notify {
          admin-email email-address;
          custom-message message;
          custom-message-subject message-subject;
        }
        interval value;
        no-autoupdate;
        proxy {
          password password-string;
          port port-number;
          server address-or-url;
          username name;
        }
        url url;
      }
      profile <name> {
        fallback-options {
```

```
            content-size (block | log-and-permit | permit);
            default (block | log-and-permit | permit);
            engine-not-ready (block | log-and-permit | permit);
            out-of-resources (block | log-and-permit | permit);
            timeout (block | log-and-permit | permit);
            too-many-requests (block | log-and-permit | permit);
          }
          notification-options {
            fallback-block {
              administrator-email email-address;
              allow-email;
              custom-message message;
              custom-message-subject message-subject;
              display-host;
              (notify-mail-sender | no-notify-mail-sender);
              type (message | protocol-only);
            }
            fallback-non-block {
              custom-message message;
              custom-message-subject message-subject;
              (notify-mail-recipient | no-notify-mail-recipient);
            }
            virus-detection {
              custom-message message;
              custom-message-subject message-subject;
              (notify-mail-sender | no-notify-mail-sender);
              type (message | protocol-only);
            }
          }
          scan-options {
            content-size-limit value;
            (no-uri-check | uri-check);
            timeout value;
          }
          trickling {
            timeout value;
          }
        }
        sxl-retry value;
        sxl-timeout seconds;
      }
      traceoptions flag flag;
      type (juniper-express-engine | kaspersky-lab-engine | sophos-engine);
      url-whitelist listname;
    }
    content-filtering {
      profile profile-name {
        block-command protocol-command-list;
        block-content-type (activex | exe | http-cookie | java-applet | zip);
        block-extension extension-list;
        block-mime {
          exception list-name;
          list list-name;
        }
        notification-options {
```

```
        custom-message message;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
      permit-command protocol-command-list;
    }
    traceoptions flag flag;
}
web-filtering {
    url-whitelist custwhitelist;
    url-blacklist custblacklist;
    http-reassemble;
    type juniper-enhanced;
    juniper-enhanced {
      cache {
        timeout 1800;
        size 500;
      }
      server {
        host rp.cloud.threatseeker.com;
        port 80;
      }
      profile junos-wf-enhanced-default {
        category {
          Enhanced_Hacking {
            action log-and-permit;
            }
            Enhanced_Government {
            action quarantine;
          }
        }
        site-reputation-action {
          very-safe permit;
          moderately-safe log-and-permit;
          fairly-safe log-and-permit;
          harmful block;
          suspicious block;
        }
        default block;
        custom-block-message "***access denied ***";
        fallback-settings {
          default block;
          server-connectivity block;
          timeout block;
          too-many-requests block;
        }
        timeout 10;
        no-safe-search;
      }
      utm-policy mypolicy {
        web-filtering {
      http-profile my_ewfprofile01;
    }
    }
}
```

```
web-filtering {
  juniper-enhanced {
    cache {
      size value;
      timeout value;
    }
    profile profile-name {
      category customurl-list name {
        action (block | log-and-permit | permit | quarantine);
      }
      custom-block-message value;
      custom-quarantine-message value;
      default (block | log-and-permit | permit | quarantine);
      fallback-settings {
        default (block | log-and-permit);
        server-connectivity (block | log-and-permit);
        timeout (block | log-and-permit);
        too-many-requests (block | log-and-permit);
      }
      no-safe-search;
      site-reputation-action {
        fairly-safe (block | log-and-permit | permit | quarantine);
        harmful (block | log-and-permit | permit | quarantine);
        moderately-safe (block | log-and-permit | permit | quarantine);
        suspicious (block | log-and-permit | permit | quarantine);
        very-safe (block | log-and-permit | permit | quarantine);
      }
      timeout value;
    }
    server {
      host host-name;
      port number;
    }
  }
  juniper-local {
    profile profile-name {
      custom-block-message value;
      default (block | log-and-permit | permit);
      fallback-settings {
        default (block | log-and-permit);
        server-connectivity (block | log-and-permit);
        timeout (block | log-and-permit);
        too-many-requests (block | log-and-permit);
      }
      timeout value;
    }
  }
  surf-control-integrated {
    cache {
      size value;
      timeout value;
    }
    profile profile-name {
      category customurl-list name {
        action (block | log-and-permit | permit);
```

```
        }
        custom-block-message value;
        default (block | log-and-permit | permit);
        fallback-settings {
          default (block | log-and-permit);
          server-connectivity (block | log-and-permit);
          timeout (block | log-and-permit);
          too-many-requests (block | log-and-permit);
        }
        timeout value;
      }
      server {
        host host-name;
        port number;
      }
    }
    traceoptions flag flag;
    type (juniper-enhanced | juniper-local | surf-control-integrated | websense-redirect);
    url-blacklist listname;
    url-whitelist listname;
    websense-redirect {
      profile profile-name {
        account value;
        custom-block-message value;
        fallback-settings {
          default (block | log-and-permit);
          server-connectivity (block | log-and-permit);
          timeout (block | log-and-permit);
          too-many-requests (block | log-and-permit);
        }
        server {
          host host-name;
          port number;
        }
        sockets value;
        timeout value;
      }
    }
  }
}
```

Hierarchy Level

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

Release Information

The Kaspersky, Express antivirus and Surf-Control features are not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure UTM features, antivirus, antispam, content-filtering, and web-filtering by creating feature profiles.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

filename-extension

Syntax

```
filename-extension object-name {
  value [value];
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm custom-objects]
```

Release Information Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description When scanning content, you can use a file extension list to define a set of file extensions that are used in file extension scan mode (scan-by-extension).

Options

- ***object-name***—Name of the extension-list object.
- **value *value***—Value of the extension-list object. You can configure multiple values separated by spaces and enclosed in square brackets.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

flag (SMTP)

Syntax

```
flag {
  all;
  configuration;
  IPC;
  protocol-exchange;
  send-request;
}
```

Hierarchy Level

```
[edit smtp traceoptions]
```

Release Information Statement added in Junos OS Release 10.0.

Description Set flag for the SMTP traceoptions.

Options The following flag options are supported:

- **IPC**—Trace interprocesss communication.
- **all**—Trace everything.
- **configuration**—Trace configuration event.
- **protocol-exchange**—Trace SMTP protocol exchanges.
- **send-request**—Trace send mail request event.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- smtp-profile (Security UTM Policy Antispam) on page 310

format (Security Log Stream)

Syntax

```
format (binary | sd-syslog | syslog | welf)
```

Hierarchy Level

```
[edit security log stream stream-name]
[edit logical-systems name security log stream stream-name]
[edit tenants tenant-name security log stream stream-name]
```

Release Information

Statement introduced in Junos OS Release 10.0 . Updated in Junos OS Release 12.1 .
The [edit **logical-systems** *name* security log stream *stream-name*] hierarchy level introduced in Junos OS Release 18.2R1.
The [edit **tenants** *tenant-name* security log stream *stream-name*] hierarchy level introduced in Junos OS Release 18.3R1.

Description

Set the format for remote security message logging to **binary**, **syslog** (system log), **sd-syslog** (structured system log), or **welf**. Note that for the WELF format, the category must be set to **content-security** (see category (Security Logging)).

Options

- **binary**—Binary encoded text to conserve resources.
- **sd-syslog**—Structured system log file.
- **syslog**—Traditional system log file.
- **welf**—Web Trends Extended Log Format.

Default: By default **syslog** (system log) is enabled.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Application Security Feature Guide for Security Devices*
- *Logical Systems and Tenant Systems Feature Guide for Security Devices*

from-zone (Security Policies)

Syntax

```
from-zone zone-name to-zone zone-name {
  policy policy-name {
    description description;
    match {
      application {
        [junos-defaults | application];
        any;
      }
      dynamic-application {
        [dynamic-application-name |dynamic-application-group-name];
        any;
        none;
      }
      destination-address {
        [address];
        any;
        any-ipv4;
        any-ipv6;
      }
      source-address {
        [address];
        any;
        any-ipv4;
        any-ipv6;
      }
      source-identity {
        [role-name];
        any;
        authenticated-user;
        unauthenticated-user;
        unknown-user;
      }
      source-end-user-profile {
        profile-name;
      }
    }
    scheduler-name scheduler-name;
    then {
      count {
        alarm {
          per-minute-threshold number;
          per-second-threshold number;
        }
      }
      deny;
      log {
        session-close;
        session-init;
      }
      permit {
        application-services {
```

```
        application-firewall {
          rule-set rule-set-name;
        }
        application-traffic-control {
          rule-set rule-set-name;
        }
        gprs-gtp-profile profile-name;
        gprs-sctp-profile profile-name;
        idp;
        redirect-wx | reverse-redirect-wx;
        ssl-proxy {
          profile-name profile-name;
        }
        uac-policy {
          captive-portal captive-portal;
        }
        utm-policy policy-name;
      }
      destination-address {
        drop-translated;
        drop-untranslated;
      }
      firewall-authentication {
        pass-through {
          access-profile profile-name;
          client-match user-or-group-name;
          ssl-termination-profile profile-name;
          web-redirect;
          web-redirect-to-https;
        }
        user-firewall {
          access-profile profile-name;
          domain domain-name
          ssl-termination-profile profile-name;
        }
        web-authentication {
          client-match user-or-group-name;
        }
      }
      services-offload;
      tcp-options {
        initial-tcp-mss mss-value;
        reverse-tcp-mss mss-value;
        sequence-check-required;
        sequence-check-required;
        syn-check-required;
      }
      tunnel {
        ipsec-group-vpn group-vpn;
        ipsec-vpn vpn-name;
        pair-policy pair-policy;
      }
    }
    deny | reject;
    deny | reject [profile name];
```

```
    }
  }
}
```

Hierarchy Level [edit security policies]

Release Information Statement introduced in Junos OS Release 8.5. Support for the **services-offload** option added in Junos OS Release 11.4. Support for the **source-identity** option added in Junos OS Release 12.1. Support for the **description** option added in Junos OS Release 12.1. Support for the **ssl-termination-profile** and **web-redirect-to-https** options added in Junos OS Release 12.1X44-D10. Support for the **user-firewall** option added in Junos OS Release 12.1X45-D10. Support for the **initial-tcp-mss** and **reverse-tcp-mss** options added in Junos OS Release 12.3X48-D20. Support for the **dynamic-application** and **deny** options added in Junos OS Release 18.2R1.

Description Specify a source zone and destination zone to be associated with the security policy.

Options

- **from-zone** ***zone-name***—Name of the source zone.
- **to-zone** ***zone-name***—Name of the destination zone.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Policies Overview*
- *Understanding Security Policy Rules*
- *Understanding Security Policy Elements*
- *Unified Policies Configuration Overview*

ftp (UTM Policy Anti-Virus)

Syntax

```
ftp {
  download-profile profile-name;
  upload-profile profile-name;
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure a UTM policy for the antivirus FTP protocol and attach this policy to a security profile to implement it.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Policies Overview*
- *Understanding Security Policy Rules*
- *Understanding Security Policy Elements*

ftp (UTM Policy Content Filtering)

Syntax

```
ftp {
  download-profile profile-name;
  upload-profile profile-name;
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name content-filtering]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure a UTM policy for the content-filtering FTP protocol and attach this policy to a security profile to implement it.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Policies Overview*
- *Understanding Security Policy Rules*
- *Understanding Security Policy Elements*

host (Security Web Filtering)

Syntax
host *host-name*;

Hierarchy Level
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated server]
[edit security utm feature-profile web-filtering websense-redirect profile *profile-name* server]
[edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name* server]

Release Information
The Surf-Control feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Set server host parameters by entering the server name or IP address.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

http-profile (Security Antivirus)

Syntax
http-profile *profile-name*;

Hierarchy Level
[edit security utm default-configuration]
[edit security utm utm-policy *policy-name* anti-virus]

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Configure a UTM policy for the antivirus HTTP protocol and attach this policy to a security profile to implement it.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

http-profile (Security Content Filtering)

Syntax
```
http-profile profile-name;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name content-filtering]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Configure a UTM policy for the content-filtering HTTP protocol and attach this policy to a security profile to implement it.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Content Filtering Overview on page 63

http-profile (Security Web Filtering)

Syntax
```
http-profile profile-name;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name web-filtering]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Configure a UTM policy for the Web-filtering HTTP protocol and attach this policy to a security profile to implement it.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Web Filtering Overview on page 77

imap-profile (Security UTM Policy Antivirus)

Syntax
```
imap-profile profile-name;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name anti-virus]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Configure a UTM policy for the antivirus IMAP protocol and attach this policy to a security profile to implement it.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

imap-profile (Security UTM Policy Content Filtering)

Syntax
```
imap-profile profile-name;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name content-filtering]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Configure a UTM policy for the content-filtering IMAP protocol and attach this policy to a security profile to implement it.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Content Filtering Overview on page 63

http-persist

Syntax

```
http-persist;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering]
```

Release Information

Statement introduced in Junos OS Release 12.3X48-D25.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Checks all HTTP requests in a connection. By default, Web filtering first checks the HTTP request method (for example, GET or PUT) in the same session. If there are multiple HTTP request methods in the subsequent HTTP request of the same session, then Web filtering checks are not performed on these methods. If **http-persist** command is enabled for clear text HTTP traffic, then Web filtering checks every HTTP request packet in the same session.

Required Privilege Level

view

Related Documentation

- Example: Configuring Enhanced Web Filtering on page 90

http-reassemble

Syntax

```
http-reassemble;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering]
```

Release Information

Statement introduced in Junos OS Release 12.3X48-D25.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Reassembles HTTP requests segments. When the **http-reassemble** option is enabled the requested fragment is reassembled. By default, Web filtering checks only HTTP requests in the first HTTP request packet. If HTTP request methods and URLs are fragmented in different packets, then these URLs are not checked. If **http-reassemble** option is enabled for clear text HTTP traffic, then Enhanced Web Filtering (EWF) reassembles the fragmented HTTP request to avoid evasion instead of packet-based inspection.

On SRX Series devices, when a new URL is matched against the active Web Filtering profile and the profile dictates that the URL should be dropped, the entire HTTP session will be blocked by the device.

Required Privilege Level

view

Related Documentation

- Example: Configuring Enhanced Web Filtering on page 90

intelligent-prescreening

Syntax

```
intelligent-prescreening;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  scan-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  scan-options]
```

Release Information

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1x49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Enable intelligent prescreening.

Intelligent prescreening tells the antivirus module to begin scanning a file much earlier. In this case, the scan engine uses the first packet or the first several packets to determine if a file could possibly contain malicious code. The scan engine does a quick check on these first packets and if the scan engine finds that it is unlikely that the file is infected, it then determines that it is safe to bypass the normal scanning procedure.

You can disable intelligent prescreening with the **no-intelligent-prescreening** statement.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

interval (Security Antivirus)

Syntax interval *value*;

Hierarchy Level
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]
[edit security utm feature-profile anti-virus sophos-engine pattern-update]
[edit security utm default-configuration anti-virus avira-engine pattern-update]

Release Information The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 for Juniper Express engine and Kaspersky Lab engine. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for Avira engine added in Junos OS Release 18.4R1.

Description Set the pattern data files auto-update interval. You can choose to leave the default interval value or you can change it by using this command. You can also force a manual update, if necessary.

NOTE: The data files used with Sophos are not typical virus pattern files; they are small files that help guide virus scanning logic. The full virus pattern database is stored on an external Sophos server called the Sophos Extensible List (SXL) server.

Options ***value***—Pattern data files auto-update interval in minutes.

Range: 10 through 10,080 minutes (10 minutes through 7 days)

Default: For Juniper Express engine and Kaspersky Lab engine, 60 minutes; for Sophos engine, 1440 minutes (every 24 hours)

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

ipc

Syntax

```
ipc {
  traceoptions flag flag;
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure trace options for IPC.

Options

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Enable trace for all IPC trace options.
  - **basic**—Trace basic IPC related information.
  - **connection-manager**—Trace IPC connection manager information.
  - **connection-status**—Trace IPC connection status information.
  - **detail**—Trace IPC related detailed information.
  - **pfe**—Trace communication with PFE.
  - **utm-realtime**—Trace IPC realtime-thread information.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

juniper-enhanced

Syntax

```
juniper-enhanced {
  cache {
    size value;
    timeout value;
  }
  profile profile-name {
    category customurl-list name {
      action (block | log-and-permit | permit | quarantine);
    }
    custom-block-message value;
    custom-quarantine-message value;
    default (block | log-and-permit | permit | quarantine);
    fallback-settings {
      default (block | log-and-permit);
      server-connectivity (block | log-and-permit);
      timeout (block | log-and-permit);
      too-many-requests (block | log-and-permit);
    }
    no-safe-search;
    site-reputation-action {
      fairly-safe (block | log-and-permit | permit | quarantine);
      harmful (block | log-and-permit | permit | quarantine);
      moderately-safe (block | log-and-permit | permit | quarantine);
      suspicious (block | log-and-permit | permit | quarantine);
      very-safe (block | log-and-permit | permit | quarantine);
      }
    timeout value;
  }
  server {
    host host-name;
    port number;
    proxy-profile proxy profile name;
  }
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[set security utm feature-profile web-filtering]
```

Release Information

Statement introduced in Junos OS Release 11.4.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
The **proxy-profile** option is introduced under the **security utm default-configuration web-filtering juniper-enhanced server** hierarchy level in Junos OS Release 18.3R1.

Description

Configure the UTM Enhanced Web Filtering feature.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Web Filtering Overview on page 77

juniper-express-engine

Syntax

```
juniper-express-engine {
  pattern-update {
    email-notify {
      admin-email email-address;
      custom-message message;
      custom-message-subject message-subject;
    }
    interval value;
    no-autoupdate;
    proxy {
      password password-string;
      port port-number;
      server address-or-url;
      username name;
    }
    url url;
  }
  profile profile-name {
    fallback-options {
      content-size (block | log-and-permit);
      default (block | log-and-permit);
      engine-not-ready (block | log-and-permit);
      out-of-resources (block | (log-and-permit);
      timeout (block | log-and-permit);
      too-many-requests (block | log-and-permit);
    }
    notification-options {
      fallback-block {
        administrator-email email-address;
        allow-email;
        custom-message message;
        custom-message-subject message-subject;
        display-host;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
      fallback-non-block {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-recipient | no-notify-mail-recipient);
      }
      virus-detection {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
    }
    scan-options {
      content-size-limit value;
      (intelligent-prescreening | no-intelligent-prescreening);
```

```
        timeout value;
    }
    trickling {
        timeout value;
    }
  }
}
```

Hierarchy Level

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

Release Information

The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure the UTM express antivirus feature.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Express Antivirus Configuration Overview*

juniper-local

Syntax

```
juniper-local {
  profile profile-name {
    custom-block-message value;
    default (block | log-and-permit | permit);
    fallback-settings {
      default (block | log-and-permit);
      server-connectivity (block | log-and-permit);
      timeout (block | log-and-permit);
      too-many-requests (block | log-and-permit);
    }
    timeout value;
  }
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[set security utm feature-profile web-filtering]
```

Release Information

Statement introduced in Junos OS Release 10.0.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure the UTM Web-filtering local feature.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

kaspersky-lab-engine

Syntax

```
kaspersky-lab-engine {
  pattern-update {
    email-notify {
      admin-email email-address;
      custom-message message;
      custom-message-subject message-subject;
    }
    interval value;
    no-autoupdate;
    proxy {
      password password-string;
      port port-number;
      server address-or-url;
      username name;
    }
    url url;
  }
  profile profile-name {
    fallback-options {
      content-size (block | log-and-permit);
      corrupt-file (block | log-and-permit);
      decompress-layer (block | log-and-permit);
      default (block | log-and-permit);
      engine-not-ready (block | log-and-permit);
      out-of-resources (block | (log-and-permit);
      password-file (block | (log-and-permit);
      timeout (block | log-and-permit);
      too-many-requests (block | log-and-permit);
    }
    notification-options {
      fallback-block {
        administrator-email email-address;
        allow-email;
        custom-message message;
        custom-message-subject message-subject;
        display-host;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
      fallback-non-block {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-recipient | no-notify-mail-recipient);
      }
      virus-detection {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
    }
```

```
    scan-options {
      content-size-limit value;
      decompress-layer-limit value;
      (intelligent-prescreening | no-intelligent-prescreening);
      scan-extension filename;
      scan-mode (all | by-extension);
      timeout value;
    }
    trickling {
      timeout value;
    }
  }
}
```

Hierarchy Level

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

Release Information

The Kaspersky Antivirus feature is not supported from Junos OS Release 15.1x49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure the UTM full file-based antivirus feature.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

limit (UTM Policy)

Syntax

```
limit value;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name traffic-options sessions-per-client]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle to limit sessions.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

list (Security Antivirus Mime Whitelist)

Syntax

```
list listname {
  exception listname;
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus mime-whitelist]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure the antivirus scanner to use MIME bypass lists (custom objects). If you want to have exceptions to the whitelist, create a mime-pattern list with the **exception** statement in addition to the **list** statement.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

list (Security Content Filtering Block Mime)

Syntax

```
list list-name;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name block-mime]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure the content filter to use MIME block lists (custom objects).

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- Content Filtering Overview on page 63

log (Security)

Syntax

```
log {
  cache {
    exclude exclude-name {
      destination-address destination-address;
      destination-port destination-port;
      event-id event-id;
      failure;
      interface-name interface-name;
      policy-name policy-name;
      process process-name;
      protocol protocol;
      source-address source-address;
      source-port source-port;
      success;
      user-name user-name;
    }
    limit value;
  }
  disable;
  event-rate rate;
  facility-override (authorization | daemon | ftp | kernel | local | user);
  file {
    files max-file-number;
    name file-name;
    path binary-log-file-path;
    size maximum-file-size;
  }
  format (binary | sd-syslog | syslog);
  max-database-record <max-database-record>;
  mode (event | stream);
  rate-cap <rate-cap-value>;
  report;
  (source-address source-address | source-interface interface-name);
  stream stream-name {
    category (all | content-security | fw-auth | screen | alg | nat | flow | sctp | gtp | ipsec | idp
      | rtlog |pst-ds-lite | appqos |secintel);
    file {
      name file-name;
      size file-size;
      rotation max-rotation-number;
    }
    filter {
      threat-attack;
      }
    format (binary | sd-syslog | syslog | welf);
    host {
      ip-address;
      port port-number;
    }
    rate-limit {
      log-rate;
```

```
    }
    severity (alert | critical | debug | emergency | error | info | notice | warning);
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag (all | configuration | hpl | report | source);
    no-remote-trace;
  }
  transport {
    protocol (udp | tcp | tls);
    tcp-connections tcp-connections;
    tls-profile tls-profile-name;
  }
  utc-timestamp;
}
```

Hierarchy Level

[edit security]
[edit **logical-systems** *name* security]
[edit **tenants** *tenant-name* security]

Release Information

Statement introduced in Junos OS Release 9.2.
The [edit **logical-systems** *name* security] and [edit **tenants** *tenant-name* security] hierarchy levels introduced in Junos OS Release 19.1R1.

Description

Configure security log. Set the mode of logging (event for traditional system logging or stream for streaming security logs through a revenue port to a server). You can also specify all the other parameters for security logging.

Options

cache—Cache security log events in the audit log buffer.

disable—Disable the security logging for the device.

event-rate *rate*—Limit the rate at which logs are streamed per second.

Range: 0 through 1500

Default: 1500

facility-override—Alternate facility for logging to remote host.

file—Specify the security log file options for logs in binary format.

Values:

- ***max-file-number***—Maximum number of binary log files.
  - The range is 2 through 10 and the default value is 10.
- ***file-name***—Name of binary log file.
- ***binary-log-file-path***—Path to binary log files.
- ***maximum-file-size***—Maximum size of binary log file in megabytes.
  - The range is 1 through 10 and the default value is 10.

format—Set the security log format for the device.

max-database-record—The following are the disk usage range limits for the database:

Range:

- SRX1500, SRX4100, and SRX4200: 0 through 15,000,000
- vSRX: 0 through 1,000,000

Default:

- SRX1500, SRX4100, and SRX4200: 15,000,000
- vSRX: 1,000,000

NOTE: **Be sure there is enough free space in /var/log/hostlogs/, otherwise logs might be dropped when written into the database.**

mode—Control how security logs are processed and exported.

rate-cap *rate-cap-value*—Work with event mode only. This option limits the rate at which data plane logs are generated per second.

Range: 0 through 5000 logs per second

Default: 5000 logs per second

source-address *source-address*—Specify a source IP address or IP address used when exporting security logs, which is mandatory to configure *stream host*.

source-interface *interface-name*—Specify a source interface name, which is mandatory to configure *stream host*.

NOTE: The source-address and source-interface are alternate values. Using one of the options is mandatory.

stream—Every stream can configure file or host.

- ***category***— Type of events that might be logged.
- ***file name***—Specify the filename.
- ***file size***—Specify the file size.
  - SRX1500, SRX4100, and SRX4200—The default value is 25 MB and the range is 10 MB through 50 MB.
  - vSRX - The default value is 2 MB and the range is 1 MB through 3 MB.
- ***rotation***—Configure the maximum file number for rotation.
  - The default value is 10 and the range is 2 through 19.
- ***rate-limit***—Rate-limit for security logs.
  - The range is 1 through 65,535 logs per second and the default value is 65,535 .
- ***filter***—Selects the filter to filter the logs to be logged.
- ***format***—Specify the log stream format.
- ***host***—Destination to send security logs.
- ***severity***—Severity threshold for security logs.

traceoptions—Specify security log daemon trace options.

transport—Set security log transport settings.

utc-timestamp—Specify to use UTC time for security log timestamps.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

mime-pattern

Syntax

```
mime-pattern object-name {
  value [value];
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm custom-objects]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

The gateway device uses MIME (Multipurpose Internet Mail Extension) types to decide which traffic is allowed to bypass various types of scanning.

Options

- ***object-name***—Name of the MIME object.
- **value *value***—Value of the MIME object. You can configure multiple values separated by spaces and enclosed in square brackets.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

mime-whitelist

Syntax

```
mime-whitelist {
  exception listname;
  list listname {
    exception listname;
  }
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.5. Statement updated for Sophos antivirus support in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure the antivirus scanner to use MIME bypass lists and exception lists. You can use your own custom object lists, or you can use the default list that ships with the device called junos-default-bypass-mime.

WARNING: When you configure the MIME whitelist feature, be aware that, because header information in HTTP traffic can be spoofed, you cannot always trust HTTP headers to be legitimate. When a Web browser is determining the appropriate action for a given file type, it detects the file type without checking the MIME header contents. However, the MIME whitelist feature does refer to the MIME encoding in the HTTP header. For these reasons, it is possible in certain cases for a malicious website to provide an invalid HTTP header. For example, a network administrator might inadvertently add a malicious website to a MIME whitelist, and, because the site is in the whitelist, it will not be blocked by Sophos even though Sophos has identified the site as malicious in its database. Internal hosts would then be able to reach this site and could become infected.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

no-autoupdate

Syntax

```
no-autoupdate;
```

Hierarchy Level

```
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]
[edit security utm feature-profile anti-virus sophos-engine pattern-update]
[edit security utm default-configuration anti-virus avira-engine pattern-update]
```

Release Information

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 for Juniper Express engine and Kaspersky Lab engine. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for Avira engine added in Junos OS Release 18.4R1.

Description

Turn off automatic data file (pattern file) update for the Kaspersky Lab, Juniper Express, or Sophos engines.

NOTE: The data files used with Sophos are not typical virus pattern files; they are small files that help guide virus scanning logic. The full virus pattern database is stored on an external Sophos server called the Sophos Extensible List (SXL) server.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

no-intelligent-prescreening

Syntax

```
no-intelligent-prescreening;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  scan-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  scan-options]
```

Release Information

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Disables intelligent prescreening.

Intelligent prescreening tells the antivirus module to begin scanning a file much earlier. In this case, the scan engine uses the first packet or the first several packets to determine if a file could possibly contain malicious code. The scan engine does a quick check on these first packets and if the scan engine finds that it is unlikely that the file is infected, it then determines that it is safe to bypass the normal scanning procedure.

You can enable intelligent prescreening with the **intelligent-prescreening** statement.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

no-notify-mail-recipient

Syntax

```
no-notify-mail-recipient;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options fallback-non-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options fallback-non-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options fallback-non-block]
```

Release Information

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Do not notify the e-mail recipient about errors returned by the antivirus scan engine when a fallback nonblocking action occurs.

You can specify that the e-mail recipient is to be notified with the **notify-mail-recipient** statement.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

no-notify-mail-sender (Security Content Filtering Notification Options)

Syntax

```
no-notify-mail-sender;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name notification-options]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Do not notify the e-mail sender.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- Content Filtering Overview on page 63

no-notify-mail-sender (Security Fallback Block)

Syntax

```
no-notify-mail-sender;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options fallback-block]
```

Release Information

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Do not notify the e-mail sender about errors returned by the antivirus scan engine when a fallback action occurs.

You can specify that the e-mail sender is to be notified with the **notify-mail-sender** statement.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

no-notify-mail-sender (Security Virus Detection)

Syntax

```
no-notify-mail-sender;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options virus-detection]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options virus-detection]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options virus-detection]
```

Release Information

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Do not notify the e-mail sender when a virus is detected by the antivirus engine.

You can specify that the e-mail sender is to be notified with the **notify-mail-sender** statement.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

no-sbl-default-server

Syntax

```
no-sbl-default-server;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-spam sbl profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Disable the default SBL server lookup.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- Antispam Filtering Overview on page 43

notification-options (Security Antivirus)

Syntax

```
notification-options {
  fallback-block {
    administrator-email email-address;
    allow-email;
    custom-message message;
    custom-message-subject message-subject;
    display-host;
    (notify-mail-sender | no-notify-mail-sender);
    type (message | protocol-only);
  }
  fallback-non-block {
    custom-message message;
    custom-message-subject message-subject;
    (notify-mail-recipient | no-notify-mail-recipient);
  }
  virus-detection {
    custom-message message;
    custom-message-subject message-subject;
    (notify-mail-sender | no-notify-mail-sender);
    type (message | protocol-only);
  }
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name]
```

Release Information

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

There are multiple notification options you can configure to trigger when a virus is detected.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

notification-options (Security Content Filtering)

Syntax

```
notification-options {
  custom-message message;
  (notify-mail-sender | no-notify-mail-sender);
  type (message | protocol-only);
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

You can configure a message notification to trigger when a content filter is matched.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- Content Filtering Overview on page 63

notify-mail-recipient

Syntax

```
notify-mail-recipient;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options fallback-non-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options fallback-non-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options fallback-non-block]
```

Release Information

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Notify the e-mail recipient about errors returned by the antivirus scan engine when a fallback nonblocking action occurs.

You can specify that the e-mail recipient is not to be notified with the **no-notify-mail-recipient** statement.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

notify-mail-sender (Security Content Filtering Notification Options)

Syntax

```
notify-mail-sender;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name notification-options]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Notify the e-mail sender.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- Content Filtering Overview on page 63

notify-mail-sender (Security Fallback Block)

Syntax

```
notify-mail-sender;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options fallback-block]
```

Release Information

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

E-mail notification is used to notify the sender or the recipient about the errors returned by either the scan engine or the scan manager when a fallback action occurs.

You can specify that the sender is not to be notified with the **no-notify-mail-sender** statement.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

notify-mail-sender (Security Virus Detection)

Syntax

```
notify-mail-sender;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options virus-detection]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options virus-detection]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options virus-detection]
```

Release Information

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

E-mail notification is used to notify the sender or the recipient about the detected viruses or the scanning errors. When a virus is detected, an e-mail is sent to the sender upon virus detection.

You can specify that the sender is not to be notified with the **no-notify-mail-sender** statement.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

no-uri-check

Syntax no-uri-check;

Hierarchy Level [edit security utm default-configuration anti-virus scan-options]

Release Information Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description Do not perform Sophos antivirus Uniform Resource Identifier (URI) checking. URI checking is performed by analyzing HTTP traffic URI content against a remote Sophos database server to identify malware or malicious content. URI checking is on by default.

NOTE: Starting in Junos OS release 18.4R1, the URI checking is off by default.

You can enable Sophos antivirus URI checking with the **uri-check** statement.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

out-of-resources

Syntax

```
out-of-resources (block | (log-and-permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  fallback-options]
```

Release Information

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Virus scanning requires a great deal of memory and CPU resources. Due to resource constraints, memory allocation requests can be denied by the system. When out-of-resources occurs, scanning is aborted. The default action is block.

Options

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

out-of-resources (Security Antivirus Sophos Engine)

Syntax

```
default (block | log-and-permit | permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  fallback-options]
```

Release Information

Statement introduced in Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Virus scanning requires a great deal of memory and CPU resources. Due to resource constraints, memory allocation requests can be denied by the system. When out-of-resources occurs, scanning is aborted.

Options

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic
- **permit**—Permit the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Sophos Antivirus Configuration Overview*

over-limit

Syntax

```
over-limit (block | log-and-permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name traffic-options sessions-per-client]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle to limit sessions and configure an action to occur when the limit is exceeded.

Options

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- utm on page 345

packet-filter

Syntax

```
packet-filter packet-filter-name {
  action-profile profile-name {
  destination-port (port-range | protocol-name);
  destination-prefix destination-prefix;
  interface logical-interface-name;
  protocol (protocol-number | protocol-name;
  source-port (port-range | protocol- name);
  source-prefix source-prefix;
  }
```

Hierarchy Level

```
[edit security datapath-debug]
```

Release Information Command introduced in Junos OS Release 9.6 ; Support for IPv6 addresses for the **destination-prefix** and **source-prefix** options added in Junos OS Release 10.4.

Description Set packet filter for taking the datapath-debug action. A filter is defined to filter traffic, then an action profile is applied to the filtered traffic. Be sure to configure multiple packet filters to capture the traffic. One packet filter only captures the traffic as specified in it, such as from one source to one destination. The same packet filter will not capture the traffic in the reverse direction. You need to configure another packet filter to capture the traffic in reverse direction and specify the source and destination according to the response packet in it. The action profile specifies a variety of actions on the processing unit. A maximum of four filters are supported at the same time. Packet filters can be configured with source and destination prefix and port (including ranges), and protocol.

Action-profile settings have no specific minimum setting, it is based on trace, count, packet summary and packet-dump. Enabling end-to-end debugging without or with a very broad filter is not recommended. This could result in a high PFE CPU usage. Therefore when selecting what to capture through a filter care must be taken. List as many and specific criteria which then results in the minimum amount of traffic to be captured.

NOTE: Packet filter is supported on SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices.

Options

- **action-profile *profile-name***—Identify the action profile to use. You can specify the name of the action profile to use. Using the request security action-profile command, you can set the action for the packet match for a specified filter. Action-profile must be defined.
- **destination-port (*port-range* | *protocol name*)**—Specify a destination port to match TCP/UDP destination port.
- **destination-prefix *destination-prefix***—Specify a destination IPv4/IPv6 address prefix.

- **interface** ***logical-interface-name***—Specify a logical interface name.
- **protocol (*protocol-number* | *protocol-name***—Match IP protocol type.
- **source-port (*port-range* | *protocol-name***—Match TCP/UDP source port.
- **source-prefix** ***source-prefix***—Specify a source IP address prefix.

Required Privilege Level
security—To view this in the configuration
security-control—To add this to the configuration.

password (Security Antivirus)

Syntax

```
password password-string;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update proxy]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update proxy]
[edit security utm feature-profile anti-virus sophos-engine pattern-update proxy]
```

Release Information
The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Release 11.2.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Set the password for the proxy server.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- utm on page 345

password-file

Syntax

```
password-file (block | (log-and-permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  fallback-options]
```

Release Information

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Password protected file is the error returned by the scan engine when the scanned file is protected by a password. The default action is log-and-permit.

Options

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Full Antivirus Configuration Overview*

pattern-update (Security Antivirus)

Syntax

```
pattern-update {
  email-notify {
    admin-email email-address;
    custom-message message;
    custom-message-subject message-subject;
  }
  interval value;
  no-autoupdate;
  proxy-profile proxy profile name;
  routing-instance name;
  start-time start-time;
  url url;
}
```

Hierarchy Level

```
[edit security utm feature-profile anti-virus juniper-express-engine]
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
[edit security utm feature-profile anti-virus sophos-engine]
[edit security utm default-configuration anti-virus avira-engine]
```

Release Information

Statement introduced in Junos OS Release 9.5 for Juniper Express engine and Kaspersky Lab engine. Support for Sophos engine added in Junos OS Release 11.1 .
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
The **proxy-profile** option is introduced under the **security utm feature-profile anti-virus sophos-engine** hierarchy level in Junos OS Release 18.3R1.
Support for Avira engine added in Junos OS Release 18.4R1.

Description

Updates to the pattern file are added as new viruses are discovered. You can configure the security device to regularly update the pattern file automatically, or you can update the file manually.

Required Privilege Level

security— To view this statement in the configuration.
security-control— To add this statement to the configuration.

permit-command

Syntax

permit-command *protocol-command-list*;

Hierarchy Level

[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile *profile-name*]

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Apply protocol permit command custom-objects to the content-filtering profile.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- Content Filtering Overview on page 63

policies

Syntax

```
policies {
  default-policy (deny-all | permit-all);
  from-zone zone-name to-zone zone-name {
    policy policy-name {
      description description;
      match {
        application {
          [application];
          any;
        }
        destination-address {
          [address];
          any;
          any-ipv4;
          any-ipv6;
        }
        source-address {
          [address];
          any;
          any-ipv4;
          any-ipv6;
        }
        source-identity {
          [role-name];
          any;
          authenticated-user;
          unauthenticated-user;
          unknown-user;
        }
      }
      scheduler-name scheduler-name;
      then {
        count {
          alarm {
            per-minute-threshold number;
            per-second-threshold number;
          }
        }
        deny;
        log {
          session-close;
          session-init;
        }
        permit {
          application-services {
            application-firewall {
              rule-set rule-set-name;
            }
            application-traffic-control {
              rule-set rule-set-name;
            }
```

```
            gprs-gtp-profile profile-name;
            gprs-sctp-profile profile-name;
            idp;
            idp-policy idp-policy;
            redirect-wx | reverse-redirect-wx;
            ssl-proxy {
              profile-name profile-name;
            }
            uac-policy {
              captive-portal captive-portal;
            }
            utm-policy policy-name;
          }
          destination-address {
            drop-translated;
            drop-untranslated;
          }
          firewall-authentication {
            pass-through {
              access-profile profile-name;
              client-match user-or-group-name;
              ssl-termination-profile profile-name;
              web-redirect;
              web-redirect-to-https;
            }
            user-firewall {
              access-profile profile-name;
              domain domain-name
              ssl-termination-profile profile-name;
            }
            web-authentication {
              client-match user-or-group-name;
            }
          }
          services-offload;
          tcp-options {
            sequence-check-required;
            syn-check-required;
          }
          tunnel {
            ipsec-group-vpn group-vpn;
            ipsec-vpn vpn-name;
            pair-policy pair-policy;
          }
        }
        reject;
      }
    }
}
global {
    policy policy-name {
      description description;
      match {
        application {
          [application];
```

```
        any;
      }
      destination-address {
        [address];
        any;
        any-ipv4;
        any-ipv6;
      }
      from-zone {
        [zone-name];
        any;
      }
      source-address {
        [address];
        any;
        any-ipv4;
        any-ipv6;
      }
      source-identity {
        [role-name];
        any;
        authenticated-user;
        unauthenticated-user;
        unknown-user;
      }
      to-zone {
        [zone-name];
        any;
      }
    }
    scheduler-name scheduler-name;
    then {
      count {
        alarm {
          per-minute-threshold number;
          per-second-threshold number;
        }
      }
      deny;
      log {
        session-close;
        session-init;
      }
      permit {
        application-services {
          application-firewall {
            rule-set rule-set-name;
          }
          application-traffic-control {
            rule-set rule-set-name;
          }
          gprs-gtp-profile profile-name;
          gprs-sctp-profile profile-name;
          idp;
          idp-policy idp-policy;
```

```
            redirect-wx | reverse-redirect-wx;
            ssl-proxy {
              profile-name profile-name;
            }
            uac-policy {
              captive-portal captive-portal;
            }
            utm-policy policy-name;
          }
          destination-address {
            drop-translated;
            drop-untranslated;
          }
          firewall-authentication {
            pass-through {
              access-profile profile-name;
              client-match user-or-group-name;
              ssl-termination-profile profile-name;
              web-redirect;
              web-redirect-to-https;
            }
            web-authentication {
              client-match user-or-group-name;
            }
          }
          services-offload;
          tcp-options {
            initial-tcp-mss mss-value;
            reverse-tcp-mss mss-value;
            sequence-check-required;
            syn-check-required;
          }
        }
        reject;
      }
    }
  }
  policy-rematch;
  policy-stats {
    system-wide (disable | enable) ;
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 8.5.
Support for the **services-offload** option added in Junos OS Release 11.4.
Support for the **source-identitiy** option added in Junos OS Release 12.1.
Support for the **description** option added in Junos OS Release 12.1.
Support for the **ssl-termination-profile** and **web-redirect-to-https** options are added starting from Junos OS Release 12.1X44-D10 and Junos OS Release 15.1X49-D40.
Support for the **user-firewall** option added in Junos OS Release 12.1X45-D10.
Support for the **domain** option, and for the **from-zone** and **to-zone** global policy match options, added in Junos OS Release 12.1X47-D10.
Support for the **initial-tcp-mss** and **reverse-tcp-mss** options added in Junos OS Release 12.3X48-D20. Support for the **extensive** option for **policy-rematch** added in Junos OS Release 15.1X49-D20.
Starting in Junos OS Release 18.2R1, an IDP policy is available within unified security policy. The IDP policy access is simplified and made available under the unified policy as one of the policy. When an IDP policy is available within a unified security policy, configuring source or destination address, source and destination-except, from and to zone, or application is not required, because the match happens in the security policy itself.
Starting in Junos OS Release 18.3R1, when an SRX Series device is configured with a unified policies, you can configure multiple IDP policies and set one of those policies as the default IDP policy. If multiple IDP policies are configured for a session and when policy conflict occurs, the device applies the default IDP policy for that session and thus resolves any policy conflicts.

NOTE: If you have configured two or more IDP policies in a unified security policy, then you must configure the default IDP policy.

Description Configure network security policies.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Security Policies Overview*

pop3-profile (Security UTM Policy Antivirus)

Syntax
```
pop3-profile profile-name;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name anti-virus]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Configure a UTM policy for the antivirus POP3 protocol and attach this policy to a security profile to implement it.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

pop3-profile (Security UTM Policy Content Filtering)

Syntax
```
pop3-profile profile-name;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name content-filtering]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Configure a UTM policy for the content filtering POP3 protocol and attach this policy to a security profile to implement it.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

port (Security Antivirus)

Syntax
port *port-number*;

Hierarchy Level
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update proxy]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update proxy]
[edit security utm feature-profile anti-virus sophos-engine pattern-update proxy]

Release Information
Statement introduced in Junos OS Release 11.2.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Set the port number for the proxy server.

Options
Range: 0 through 65,535

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

port (Security Web Filtering Server)

Syntax
port *number*;

Hierarchy Level
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated server]
[edit security utm feature-profile web-filtering websense-redirect profile *profile-name* server]
[edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name* server]

Release Information
Statement introduced in Junos OS Release 9.5 .
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Enter the port number for communicating with the server. (Default ports are 80, 8080, and 8081.)

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

primary-server

Syntax

```
primary-server {
   address ipv4-address;
   login sender-email-address {
      password password;
   }
}
```

Hierarchy Level

```
[edit smtp]
```

Release Information Statement added in Junos OS Release 10.0.

Description Configure Simple Mail Transfer Protocol (SMTP) primary server for access authorization for SMTP requests.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

profile (Security Antispam SBL)

Syntax

```
profile profile-name {
  custom-tag-string [string];
  (sbl-default-server | no-sbl-default-server);
  spam-action (block | tag-header | tag-subject);
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-spam sbl]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Create a profile for the antispam sbl feature. This profile includes all subsequent configuration options.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

profile (Security Antivirus Juniper Express Engine)

Syntax

```
profile profile-name {
  fallback-options {
    content-size (block | log-and-permit);
    default (block | log-and-permit);
    engine-not-ready (block | log-and-permit);
    out-of-resources (block | (log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  notification-options {
    fallback-block {
      administrator-email email-address;
      allow-email;
      custom-message message;
      custom-message-subject message-subject;
      display-host;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
    fallback-non-block {
      custom-message message;
      custom-message-subject message-subject;
      (notify-mail-recipient | no-notify-mail-recipient);
    }
    virus-detection {
      custom-message message;
      custom-message-subject message-subject;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
  }
  scan-options {
    content-size-limit value;
    (intelligent-prescreening | no-intelligent-prescreening);
    timeout value;
  }
  trickling {
    timeout value;
  }
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine]
```

Release Information

The express engine feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description Create a profile for the Juniper express engine. This profile includes all subsequent configuration options.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Express Antivirus Configuration Overview*

profile (Security Antivirus Kaspersky Lab Engine)

Syntax

```
profile profile-name {
  fallback-options {
    content-size (block | log-and-permit);
    corrupt-file (block | log-and-permit);
    decompress-layer (block | log-and-permit);
    default (block | log-and-permit);
    engine-not-ready (block | log-and-permit);
    out-of-resources (block | (log-and-permit);
    password-file (block | (log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  notification-options {
    fallback-block {
      administrator-email email-address;
      allow-email;
      custom-message message;
      custom-message-subject message-subject;
      display-host;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
    fallback-non-block {
      custom-message message;
      custom-message-subject message-subject;
      (notify-mail-recipient | no-notify-mail-recipient);
    }
    virus-detection {
      custom-message message;
      custom-message-subject message-subject;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
  }
  scan-options {
    content-size-limit value;
    decompress-layer-limit value;
    (intelligent-prescreening | no-intelligent-prescreening);
    scan-extension filename;
    scan-mode (all | by-extension);
    timeout value;
  }
  trickling {
    timeout value;
  }
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
```

Release Information The Kaspersky feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description Create a profile for the Kaspersky Lab engine. This profile includes all subsequent configuration options.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- kaspersky-lab-engine on page 243
- profile (Security Antivirus Juniper Express Engine) on page 284

profile (Security Content Filtering)

Syntax

```
profile profile-name {
  block-command protocol-command-list;
  block-content-type (activex | exe | http-cookie | java-applet | zip);
  block-extension extension-list;
  block-mime {
    exception list-name;
    list list-name;
  }
  notification-options {
    custom-message message;
    (notify-mail-sender | no-notify-mail-sender);
    type (message | protocol-only);
  }
  permit-command protocol-command-list;
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Create a profile for the content-filtering feature. This profile includes all subsequent configuration options.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- Content Filtering Overview on page 63

profile (Security Sophos Engine Antivirus)

Syntax

```
profile <name> {
  fallback-options {
    content-size (block | log-and-permit | permit);
    default (block | log-and-permit | permit);
    engine-not-ready (block | log-and-permit | permit);
    out-of-resources (block | log-and-permit | permit);
    timeout (block | log-and-permit | permit);
    too-many-requests (block | log-and-permit | permit);
  }
  notification-options {
    fallback-block {
      administrator-email email-address;
      allow-email;
      custom-message message;
      custom-message-subject message-subject;
      display-host;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
    fallback-non-block {
      custom-message message;
      custom-message-subject message-subject;
      (notify-mail-recipient | no-notify-mail-recipient);
    }
    virus-detection {
      custom-message message;
      custom-message-subject message-subject;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
  }
  scan-options {
    content-size-limit value;
    (no-uri-check | uri-check);
    timeout value;
  }
  trickling {
    timeout value;
  }
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine]
```

Release Information

Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description Create a profile for the Sophos antivirus engine. This profile includes all subsequent configuration options.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Sophos Antivirus Configuration Overview*

profile (Security Web Filtering Juniper Enhanced)

Syntax

```
profile profile-name {
  category customurl-list name {
    action (block | log-and-permit | permit | quarantine);
  }
  custom-block-message value;
  custom-quarantine-message value;
  default (block | log-and-permit | permit | quarantine);
  fallback-settings {
    default (block | log-and-permit);
    server-connectivity (block | log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  no-safe-search;
  site-reputation-action {
    fairly-safe (block | log-and-permit | permit | quarantine);
    harmful (block | log-and-permit | permit | quarantine);
    moderately-safe (block | log-and-permit | permit | quarantine);
    suspicious (block | log-and-permit | permit | quarantine);
    very-safe (block | log-and-permit | permit | quarantine);
  }
  timeout value;
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering juniper-enhanced]
```

Release Information

Statement introduced in Junos OS Release 11.4.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Create a profile for the juniper-enhanced feature. This profile includes all subsequent configuration options.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- Monitoring Web Filtering Configurations on page 142

profile (Security Web Filtering Juniper Local)

Syntax

```
profile profile-name {
  custom-block-message value;
  default (block | log-and-permit | permit);
  fallback-settings {
    default (block | log-and-permit);
    server-connectivity (block | log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  timeout value;
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering juniper-local]
```

Release Information

Statement introduced in Junos OS Release 10.0.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Create a profile for the web-filtering juniper–local feature. This profile includes all subsequent configuration options.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- Monitoring Web Filtering Configurations on page 142
- Example: Configuring Local Web Filtering on page 119

profile (Security Web Filtering Websense Redirect)

Syntax

```
profile profile-name {
  account value;
  custom-block-message value;
  fallback-settings {
    default (block | log-and-permit);
    server-connectivity (block | log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  server {
    host host-name;
    port number;
  }
  sockets value;
  timeout value;
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[security utm feature-profile web-filtering websense-redirect]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Create a profile for the web-filtering web-sense feature. This profile includes all subsequent configuration options.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- Monitoring Web Filtering Configurations on page 142

protocol-command

Syntax

```
protocol-command object-name {
  value [value];
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm custom-objects]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Different protocols use different commands to communicate between servers and clients. By blocking or allowing certain commands, traffic can be controlled on the protocol command level.

Options

- ***object-name***—Name of the command-list object.
- **value *value***—Value of the command-list object. You can configure multiple values separated by spaces and enclosed in square brackets.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *UTM Overview*

proxy (Security Antivirus)

Syntax

```
proxy {
  password password-string;
  port port-number;
  server address-or-url;
  username name;
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]
[edit security utm feature-profile anti-virus sophos-engine pattern-update]
```

Release Information

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 11.2.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Update the pattern file on the proxy server.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

quarantine-message (Security UTM)

Syntax

```
quarantine-message {
  type {
    custom-redirect-url;
  }
  url url;
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 12.1X44-D10 for Enhanced Web Filtering. The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure Juniper enhanced quarantine message settings.

Options

- **type**—Specify the following type of the quarantine message:
  - **custom-redirect-url**—Specify Custom redirect URL server.
- **url *url***—Specify an URL of the quarantine message.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

routing-instance (Security UTM)

Syntax

```
routing-instance name;
```

Hierarchy Level

```
[edit security utm feature-profile anti-virus sophos-engine pattern-update]
[edit security utm feature-profile web-filtering juniper-enhanced server]
[edit security utm feature-profile web-filtering websense-redirect profile wr server]
[edit security utm feature-profile anti-virus sophos-engine server]
[edit security utm default-configuration anti-virus avira-engine pattern-update]
```

Release Information

Statement introduced in Junos OS Release 15.1X49-D90.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for Avira engine added in Junos OS Release 18.4R1.

Description

Configure the routing instance name. A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. The set of interfaces belongs to the routing tables, and the routing protocol parameters control the information in the routing tables. Each routing instance has a unique name.

Options

name—Specify the name of the routing instance.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- admin-email on page 151
- url (Security Antivirus) on page 341

sbl

Syntax

```
sbl {
  profile profile-name {
    custom-tag-string [string];
    (sbl-default-server | no-sbl-default-server);
    spam-action (block | tag-header | tag-subject);
  }
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-spam]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure UTM server-based antispam features.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

sbl-default-server

Syntax

```
sbl-default-server;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-spam sbl profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Enable the default SBL server lookup. You should enable this feature if you are using server-based spam filtering. (The SBL server is predefined on the device. It ships with the name and address of the SBL server.)

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

scan-extension

Syntax

```
scan-extension filename;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  scan-options]
```

Release Information

The Kaspersky feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

For antivirus file extension scanning, configure the scan extension setting by specifying the name of the defined file extension list.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

scan-mode

Syntax

```
scan-mode (all | by-extension);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  scan-options]
```

Release Information

The scan-mode is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, the statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

You can scan all content or scan content with specific file extensions. You can use a file extension list to define a set of file extensions that are used in file extension scan mode. The antivirus module can then only scan files with extensions on the scan-extension list.

Options

- **all**—Scan all files.
- **by-extension**—Scan only files with extensions specified in a file extension list custom object.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

scan-options (Security Antivirus Juniper Express Engine)

Syntax

```
scan-options {
  content-size-limit value;
  (intelligent-prescreening | no-intelligent-prescreening);
  timeout value;
}
```

Hierarchy Level

[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name*]

Release Information

The scan-options (Security Antivirus Juniper Express Engine) is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure the antivirus feature to scan specific types of traffic based on various scanning configuration parameters.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

scan-options (Security Antivirus Kaspersky Lab Engine)

Syntax

```
scan-options {
  content-size-limit value;
  decompress-layer-limit value;
  (intelligent-prescreening | no-intelligent-prescreening);
  scan-extension filename;
  scan-mode (all | by-extension);
  timeout value;
}
```

Hierarchy Level

[edit security utm default-configuration]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name*]

Release Information

The Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure the antivirus feature to scan specific types of traffic based on various scanning configuration parameters.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

scan-options (Security Antivirus Sophos Engine)

Syntax

```
scan-options {
  content-size-limit value;
  (no-uri-check | uri-check);
  timeout value;
}
```

Hierarchy Level

[edit security utm default-configuration antivirus scan-options]

Release Information

Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure the antivirus feature to scan specific types of traffic based on various scanning configuration parameters.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

secondary-server

Syntax

```
secondary-server {
  address ipv4-address;
  login sender-email-address {
    password password;
  }
}
```

Hierarchy Level

```
[edit smtp]
```

Release Information Statement added in Junos OS Release 10.0.

Description Configure Simple Mail Transfer Protocol (SMTP) secondary server for access authorization for SMTP requests.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

server (Security Antivirus)

Syntax

```
server address-or-url;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update proxy]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update proxy]
[edit security utm feature-profile anti-virus sophos-engine pattern-update proxy]
```

Release Information The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 11.2.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description Set the IP address or URL for the proxy server.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

server (Security Sophos Engine Antivirus)

Syntax

```
server ip;
routing-instance name;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine]
```

Release Information

Statement introduced in Junos OS Release 15.1X49-D90.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Set server parameters by entering the server IP address.

Options

ip—Specify Sophos anitivirus and antispam first-hop DNS server IP address.

routing-instance *name*—Specify the name of the routing instance.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- utm on page 345

server (Security Web Filtering)

Syntax

```
server {
   host host-name;
   port number;
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated]
[edit security utm feature-profile web-filtering websense-redirect profile profile-name]
[edit security utm feature-profile web-filtering juniper-enhanced]
```

Release Information

The surf-control feature is not supported from Junos OS Release 15.1X49-D10 onwards.
For previous releases, statement introduced in Junos OS Release 9.5 .
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Set server parameters by entering the server name or IP address.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

server-connectivity

Syntax

```
server-connectivity (block | log-and-permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated profile profile-name
  fallback-settings]
[edit security utm feature-profile web-filtering websense-redirect profile profile-name
  fallback-settings]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name
  fallback-settings]
```

Release Information

The surf-control feature is not supported from Junos OS Release 15.1X49-D10 onwards.
For previous releases, statement introduced in Junos OS Release 9.5 .
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Fallback settings tell the system how to handle errors. This is the action that occurs when a request fails for this reason.

Options

- block—Log the error and deny the traffic
- log-and-permit—Log the error and permit the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

sessions-per-client

Syntax

```
sessions-per-client {
  limit value;
  over-limit (block | log-and-permit);
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name traffic-options]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle.

NOTE: The sessions-per-client limit command supports the antispam, content filtering, and antivirus UTM features. It does not support Web filtering.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

site-reputation-action

Syntax

```
site-reputation-action {
  harmful (block | log-and-permit | permit | quarantine);
  fairly-safe (block | log-and-permit | permit | quarantine);
  moderately-safe (block | log-and-permit | permit | quarantine);
  suspicious (block | log-and-permit | permit | quarantine);
  very-safe (block | log-and-permit | permit | quarantine);
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name category
  category-name]
```

Release Information

Statement introduced in Junos OS Release 11.4.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Specify the action to be taken depending on the site reputation returned for all types of URLs whether it is categorized or uncategorized.

NOTE: Starting with Junos OS Release 17.4R1, the reputation base scores are configurable. Users can apply global reputation values, provided by the Websense ThreatSeeker Cloud (TSC). For the non-category URLs, the global reputation value is used to perform filtering,

Options

fairly-safe —Permit, log-and-permit, block, or quarantine a request if a site-reputation of 70 through 79 is returned.

harmful —Permit, log-and-permit, block, or quarantine a request if a site-reputation of zero through 59 is returned.

moderately-safe —Permit, log-and-permit, block, or quarantine a request if a site-reputation of 80 through 89 is returned.

suspicious —Permit, log-and-permit, block, or quarantine a request if a site-reputation of 60 through 69 is returned.

very-safe —Permit, log-and-permit, block, or quarantine a request if a site-reputation of 90 through 100 is returned.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

size (Security Web Filtering Cache)

Syntax
```
size value;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated cache]
[edit security utm feature-profile web-filtering juniper-enhanced cache]
```

Release Information
The surf-control feature is not supported from Junos OS Release 15.1X49-D10 onwards.
For previous releases, statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Set the cache size parameters for Web filtering.

Options
Range: 0 through 4096 kilobytes.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

smtp-profile (Security UTM Policy Antispam)

Syntax
```
smtp-profile profile-name;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name anti-spam]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Configure a UTM policy for the antispam SMTP protocol and attach this policy to a security profile to implement it.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

smtp-profile (Security UTM Policy Antivirus)

Syntax
```
smtp-profile profile-name;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name anti-virus]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Configure a UTM policy for the antivirus SMTP protocol and attach this policy to a security profile to implement it.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

smtp-profile (Security UTM Policy Content Filtering)

Syntax
```
smtp-profile profile-name;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name content-filtering]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Configure a UTM policy for the content-filtering SMTP protocol and attach this policy to a security profile to implement it.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

sockets

Syntax sockets *value*;

Hierarchy Level [edit security utm default-configuration]
[edit security utm feature-profile web-filtering websense-redirect profile *profile-name*]

Release Information Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description Enter the number of sockets used for communicating between the client and server. The default is 1.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

sophos-engine

Syntax

```
sophos-engine {
  pattern-update {
    email-notify {
      admin-email email-address;
      custom-message message;
      custom-message-subject message-subject;
    }
    interval value;
    no-autoupdate;
    proxy {
      password password-string;
      port port-number;
      server address-or-url;
      username name;
    }
    url url;
  }
  profile <name> {
    fallback-options {
      content-size (block | log-and-permit | permit);
      default (block | log-and-permit | permit);
      engine-not-ready (block | log-and-permit | permit);
      out-of-resources (block | log-and-permit | permit);
      timeout (block | log-and-permit | permit);
      too-many-requests (block | log-and-permit | permit);
    }
    notification-options {
      fallback-block {
        administrator-email email-address;
        allow-email;
        custom-message message;
        custom-message-subject message-subject;
        display-host;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
      fallback-non-block {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-recipient | no-notify-mail-recipient);
      }
      virus-detection {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
    }
    scan-options {
      content-size-limit value;
      (no-uri-check | uri-check);
```

```
        timeout value;
    }
    trickling {
        timeout value;
    }
  }
  sxl-retry value;
  sxl-timeout seconds;
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure the UTM Sophos antivirus feature.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

spam-action

Syntax

```
spam-action (block | tag-header | tag-subject);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-spam sbl profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure the action to be taken by the device when spam is detected.

Options

- **block**— Block e-mail.
- **tag-header**—Tag header of e-mail.
- **tag-subject**—Tag subject of e-mail.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Server-Based Antispam Filtering on page 47
- Example: Configuring Local List Antispam Filtering on page 55

sxl-retry

Syntax sxl-retry *value;*

Hierarchy Level [edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine]

Release Information Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description Configure the number of retry attempts to the remote Sophos Extensible List (SXL) server when a request timeout occurs.

Options *value* —Number of retries.
Range: 0 through 5
Default: 1

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

sxl-timeout

Syntax sxl-timeout *seconds;*

Hierarchy Level [edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine]

Release Information Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description Configure the timeout value for responses to a Sophos checksum or URI query.

Options *seconds* —Number of seconds before timeout occurs.
Range: 1 through 5 seconds
Default: 2 seconds

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

timeout (Security Antivirus Fallback Options)

Syntax

```
timeout (block | log-and-permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  fallback-options]
```

Release Information

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Scanning a complex file could consume resources and time. If the time it is taking to scan exceeds the timeout setting in the antivirus profile, the processing is aborted and the content is either passed or blocked without completing the virus checking. The decision is made based on the timeout fallback option. The default action is block.

Options

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

timeout (Security Antivirus Fallback Options Sophos Engine)

Syntax

```
default (block | log-and-permit | permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  fallback-options]
```

Release Information

Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Scanning a complex file could consume resources and time. If the time it is taking to scan exceeds the timeout setting in the antivirus profile, the processing is aborted and the content is either passed or blocked without completing the virus checking. The decision is made based on the timeout fallback option.

Options

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic
- **permit**—Permit the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

timeout (Security Antivirus Scan Options)

Syntax
```
timeout value;
```

Hierarchy Level
```
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  scan-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  scan-options]
[edit security utm default-configuration anti-virus scan-options]
```

Release Information
The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 . Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for Avira engine added in Junos OS Release 18.4R1.

Description
The scanning timeout value includes the time frame from when the scan request is generated to when the scan result is returned by the scan engine. The time range can be 1 to 1800 seconds. By default, it is 180 seconds.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

timeout (Security Web Filtering)

Syntax
```
timeout value;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering websense-redirect profile profile-name]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name]
```

Release Information
Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Enter a timeout limit for requests. Once this limit is reached, fail mode settings are applied. The default here is 15 seconds.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

timeout (Security Web Filtering Cache)

Syntax

```
timeout value;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated cache]
[edit security utm feature-profile web-filtering juniper-enhanced cache]
```

Release Information

The surf-control-integrated feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Set the cache timeout parameters for surf-control-integrated web filtering (24 hours is the default and the maximum allowed life span of cached items).

Options

Range: 1 through 1800 minutes.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

timeout (Security Web Filtering Fallback Settings)

Syntax

```
timeout (block | log-and-permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated profile profile-name
  fallback-settings]
[edit security utm feature-profile web-filtering websense-redirect profile profile-name
  fallback-settings]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name
  fallback-settings]
```

Release Information

The surf-control-integrated feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Fallback settings tell the system how to handle errors.

Options

- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

too-many-requests (Security Antivirus Fallback Options)

Syntax

```
too-many-requests (block | log-and-permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  fallback-options]
```

Release Information

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

If the total number of messages received concurrently exceeds 4000, the content is either passed or blocked depending on the too-many-request fallback option. The default action is block. (The allowed request limit is not configurable.)

Options

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

too-many-requests (Security Antivirus Fallback Options Sophos Engine)

Syntax

```
default (block | log-and-permit | permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  fallback-options]
```

Release Information

Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

If the total number of messages received concurrently exceeds the device limits, the content is either passed or blocked depending on the too-many-request fallback option. (The allowed request limit is not configurable.)

Options

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic
- **permit**—Permit the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

too-many-requests (Security Web Filtering Fallback Settings)

Syntax

```
too-many-requests (block | log-and-permit);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering surf-control-integrated profile profile-name
  fallback-settings]
[edit security utm feature-profile web-filtering websense-redirect profile profile-name
  fallback-settings]
[edit security utm feature-profile web-filtering juniper-enhanced profile profile-name
  fallback-settings]
```

Release Information

The surf-control-integrated feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

If the total number of messages received concurrently exceeds the device limits, the content is either passed or blocked depending on the too-many-request fallback option. The default action is BLOCK. (The allowed request limit is not configurable.)

Options

- block—Log the error and deny the traffic
- log-and-permit—Log the error and permit the traffic

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

to-zone (Security Policies)

Syntax

```
to-zone zone-name {
  policy policy-name {
    description description;
    match {
      application {
        [application];
        any;
      }
      destination-address {
        [address];
        any;
        any-ipv4;
        any-ipv6;
      }
      source-address {
        [address];
        any;
        any-ipv4;
        any-ipv6;
      }
      source-identity {
        [role-name];
        any;
        authenticated-user;
        unauthenticated-user;
        unknown-user;
      }
    }
    scheduler-name scheduler-name;
    then {
      count {
        alarm {
          per-minute-threshold number;
          per-second-threshold number;
        }
      }
      deny;
      log {
        session-close;
        session-init;
      }
      permit {
        application-services {
          application-firewall {
            rule-set rule-set-name;
          }
          application-traffic-control {
            rule-set rule-set-name;
          }
          gprs-gtp-profile profile-name;
          gprs-sctp-profile profile-name;
```

```
            idp;
            redirect-wx | reverse-redirect-wx;
            ssl-proxy {
              profile-name profile-name;
            }
            uac-policy {
              captive-portal captive-portal;
            }
            utm-policy policy-name;
          }
          destination-address {
            drop-translated;
            drop-untranslated;
          }
          firewall-authentication {
            pass-through {
              access-profile profile-name;
              client-match user-or-group-name;
              ssl-termination-profile profile-name;
              web-redirect;
              web-redirect-to-https;
            }
            web-authentication {
              client-match user-or-group-name;
            }
          }
          services-offload;
          tcp-options {
            sequence-check-required;
            syn-check-required;
          }
          tunnel {
            ipsec-group-vpn group-vpn;
            ipsec-vpn vpn-name;
            pair-policy pair-policy;
          }
        }
        reject;
      }
    }
}
```

Hierarchy Level

```
[edit security policies from-zone zone-name]
```

Release Information

Statement introduced in Junos OS Release 8.5. Support for the **services-offload** and **junos-host** options added in Junos OS Release 11.4. Support for the **source-identity** option added in Junos OS Release 12.1. Support for the **ssl-termination-profile** and **web-redirect-to-https** options added in Junos OS Release 12.1X44-D10.

Description

Specify a destination zone to be associated with the security policy.

Options

- **zone-name**—Name of the destination zone object.
- **junos-host**—Default security zone for self-traffic of the device.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Policies Overview*
- *Understanding Security Policy Rules*
- *Understanding Security Policy Elements*

traceoptions (Security Antispam)

Syntax

```
traceoptions flag flag;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-spam]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Define tracing operations for UTM antispam features.

Options

- *flag*:
  - **all**—Enable all antispam trace flags.
  - **manager** —Trace antispam manager information.
  - **sbl**—Trace SBL server information.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

traceoptions (Security Antivirus)

Syntax

```
traceoptions flag flag;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Define tracing operations for UTM antivirus features.

Options

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Enable trace all antivirus trace options.
  - **basic**—Trace antivirus module generic basic information.
  - **detail**—Trace antivirus module generic detail information.
  - **engine**—Trace scan engine information.
  - **event**—Trace communication events between routing engine side processes.
  - **ipc**—Trace communication events with Packet Forwarding Engine.
  - **manager**—Trace antivirus manager process activities.
  - **pattern**—Trace detail information of pattern loading.
  - **sendmail**—Trace mail notifying process activities.
  - **statistics**—Trace statistics information.
  - **updater**—Trace pattern updater process activities.
  - **worker**—Trace antivirus worker process activities.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

traceoptions (Security Application Proxy)

Syntax

```
traceoptions {
  flag flag;
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm application-proxy]
[edit logical-system logical-system-name security]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
The logical system option is introduced in Junos OS Release 18.3R1.

Description

Configure tracing options for application proxy.

Options

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **abort**—Trace aborted sessions for application proxy.
  - **all**—Trace with all flags enabled.
  - **anti-virus**—Trace anti-virus information.
  - **application-objects**—Trace application-proxy objects information.
  - **basic**—Trace application-proxy related basic information.
  - **buffer**— Trace application-proxy data buffer information.
  - **connection-rating**—Trace connection rating information.
  - **detail**—Trace application-proxy related detailed information.
  - **express-anti-virus**—Trace anti-virus express engine information.
  - **ftp-control**—Trace FTP control connection information.
  - **ftp-data**—Trace FTP data connection information.
  - **http**—Trace HTTP protocol information.
  - **imap**—Trace IMAP protocol information.
  - **memory**—Trace memory usage.
  - **mime**—Trace MIME parser information.
  - **parser**— Trace protocol parser information.
  - **pfe**—Trace communication with PFE.
  - **pop3**—Trace POP3 protocol information.

- **queue**—Trace queue information.
- **regex-engine**—Trace Pattern Match Engine (PME) information.
- **smtp**—Trace SMTP protocol information.
- **sophos-anti-virus**—Trace anti-virus sophos engine information.
- **tcp**—Trace TCP level information.
- **timer**—Trace timer processing.
- **utm-realtime**—Trace application-proxy realtime-thread information

Required Privilege Level
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

traceoptions (Security Content Filtering)

Syntax

```
traceoptions flag flag;
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Define tracing options for content filtering features.

Options

- *flag*:
  - **all**—Enable all content filtering trace flags.
  - **basic** —Trace content filtering basic information.
  - **detail**—Trace content filtering detailed information.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

traceoptions (Security UTM)

Syntax

```
traceoptions flag flag;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Define tracing operations for UTM features.

Options

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Enable trace for all UTM trace options.
  - **cli**—Trace CLI configuration activity and command changes.
  - **daemon**—Trace daemon information.
  - **ipc**—Trace communication events with Packet Forwarding Engine (PFE).
  - **pfe**—Trace PFE information.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

traceoptions (Security Web Filtering)

Syntax traceoptions flag *flag*;

Hierarchy Level [edit security utm default-configuration]
[edit security utm feature-profile web-filtering]

Release Information Command introduced in Junos OS Release 10.1.
Command introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description Define tracing operations for individual Web filtering modules. To specify more than one tracing operation, include multiple flag statements.

Options

- *flag*:
  - **all**—Enable all Web filtering trace flags.
  - **basic** —Trace basic information on the Web filtering module.
  - **cache**—Enable Web filtering flags for the Web filtering cache maintained on the Web filtering module.
  - **enhanced**—Enable Web filtering flags for processing through Enhanced Web Filtering.
  - **heartbeat**—Trace connectivity information with Web filter server.
  - **ipc**—Trace Web filtering IPC messages.
  - **packet**—Trace packet information from session management.
  - **profile**—Trace profile configuration information.
  - **requests**—Trace requests sent to Web filter server.
  - **response**—Trace response received from Web filter server.
  - **session manager**—Trace session management information.
  - **socket**—Trace the communication socket with Web filter server.
  - **timer**—Trace aging information for requests sent to server.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

traceoptions (SMTP)

Syntax

```
traceoptions {
  flag {
    all;
    configuration;
    IPC;
    protocol-exchange;
    send-request;
  }
}
```

Hierarchy Level

```
[edit smtp]
```

Release Information Statement added in Junos OS Release 10.0.

Description Set the Simple Mail Transfer Protocol (SMTP) traceoptions.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- utm on page 345

traffic-options

Syntax

```
traffic-options {
  sessions-per-client {
    limit value;
    over-limit (block | log-and-permit);
  }
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

trickling

Syntax

```
trickling {
  timeout value;
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name]
```

Release Information

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Statement updated for Sophos support in Junos OS Release 11.1.

Description

HTTP trickling is a mechanism used to prevent the HTTP client or server from timing-out during a file transfer or during antivirus scanning. HTTP Trickling is time-based and there is only one parameter to configure for this feature, which is the timeout Interval. By default, trickling is disabled.

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

Options

value—Timeout interval in seconds.

Range: 0 through 600 seconds

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

type (Security Antivirus Feature Profile)

Syntax
```
type (juniper-express-engine | kaspersky-lab-engine | sophos-engine);
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus]
```

Release Information
The Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Statement updated for Sophos in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Set the antivirus engine that will be used on the device. You can only have one engine type running and you must restart the device if you change engines.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

type (Security Content Filtering Notification Options)

Syntax
```
type (message | protocol-only);
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm feature-profile content-filtering profile profile-name notification-options]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
When content is blocked, the client generally still receives a successful response code but with modified content (file replacement) containing a warning message. But with protocol-only notifications, a protocol-specific error code might be returned to the client.

Options
- **message**—Send a generic notification.
- **protocol-only**—Send a protocol-specific notification.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

type (Security Fallback Block)

Syntax

```
type (message | protocol-only);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options fallback-block]
```

Release Information

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1 .

Description

You can configure notifications for both fallback blocking and fallback nonblocking actions. With protocol-only notifications, a protocol-specific error code may be returned to the client.

Options

- message—Send a generic notification.
- protocol-only—Send a protocol-specific notification.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

type (Security Virus Detection)

Syntax

```
type (message | protocol-only);
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options virus-detection]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options virus-detection]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options virus-detection]
```

Release Information

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

Description

When content is blocked because a virus is found or a scan error occurs, the client generally still receives a successful response code but with modified content (file replacement) containing a warning message. But with protocol-only notifications, a protocol-specific error code might be returned to the client.

Options

- message—Send a generic notification.
- protocol-only—Send a protocol-specific notification.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

type (Security Web Filtering)

Syntax
```
type (juniper-enhanced | juniper-local | surf-control-integrated | websense-redirect);
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering]
```

Release Information
The surf-control-integrated feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, command introduced in Junos OS Release 9.5.
Command introduced in Junos OS Release 11.4 for Enhanced Web Filtering.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Define the type of Web filtering solution or URL filtering solution used by the device.

Options
- **juniper-enhanced**—Enable Enhanced Web Filtering on the device.
- **juniper-local** —Enable Juniper Networks local URL filtering on the device.
- **surf-control-integrated**—Enable integrated Web filtering on the device.
- **websense-redirect**—Redirect the URL to the Websense server.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

upload-profile (Security Antivirus FTP)

Syntax
```
upload-profile profile-name;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm utm-policy policy-name anti-virus ftp]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
Configure a UTM policy for the antivirus FTP (upload) protocol and attach this policy to a security profile to implement it.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

upload-profile (Security Content Filtering FTP)

Syntax upload-profile *profile-name*;

Hierarchy Level [edit security utm default-configuration]
[edit security utm utm-policy *policy-name* content-filtering ftp]

Release Information Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description Configure a UTM policy for the content-filtering FTP (upload) protocol and attach this policy to a security profile to implement it.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

uri-check

Syntax uri-check;

Hierarchy Level [edit security utm default-configuration anti-virus scan-options]

Release Information Statement introduced in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description Perform Sophos antivirus Uniform Resource Identifier (URI) checking. URI checking is a way of analyzing URI content in HTTP traffic against a remote Sophos database to identify malware or malicious content. URI checking is on by default.

NOTE: **Starting in Junos OS release 18.4R1, the URI checking is off by default.**

You can disable Sophos antivirus URI checking with the **no-uri-check** statement.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

url (Security Antivirus)

Syntax
```
url url;
```

Hierarchy Level
```
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]
[edit security utm feature-profile anti-virus sophos-engine pattern-update]
[edit security utm default-configuration anti-virus avira-engine pattern-update]
```

Release Information
The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 for Juniper Express engine and Kaspersky Lab engine. Support for Sophos engine added in Junos OS Release 11.1.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
Support for Avira engine added in Junos OS Release 18.4R1.

Description
Specify the URL for the pattern database. You should not change the default URL unless you are experiencing problems with it and have called for support.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

url-blacklist

Syntax
```
url-blacklist listname;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
This is a global blacklist category, blocking content for Web filtering.

Options
The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

url-pattern

Syntax

```
url-pattern object-name {
  value [value];
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm custom-objects]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Use URL pattern lists to create custom URL category lists. These are lists of patterns that bypass scanning.

WARNING: Custom category does not take precedence over predefined categories when it has the same name as one of the predefined categories. We do not recommend having a custom category name be the same as the predefined category name.

Options

- ***object-name***—Name of the URL list object.
- **value *value***—Value of the URL list object. You can configure multiple values separated by spaces and enclosed in square brackets.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Policies Feature Guide for Security Devices*

url-whitelist (Security Antivirus)

Syntax
```
url-whitelist listname;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus]
```

Release Information
Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
A URL whitelist is a unique custom list that you define in which all the URLs or IP addresses in that list for a specified category are always bypassed for scanning.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

url-whitelist (Security Web Filtering)

Syntax
```
url-whitelist listname;
```

Hierarchy Level
```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering]
```

Release Information
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description
A URL whitelist is a unique custom list that you define in which all the URLs or IP addresses in that list for a specified category are always bypassed for filtering

Options
The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

username (Security Antivirus)

Syntax

username *name*;

Hierarchy Level

[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update proxy]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update proxy]
[edit security utm feature-profile anti-virus sophos-engine pattern-update proxy]

Release Information

The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 11.2.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Set the username for the proxy server.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

utm

Syntax

```
utm {
  application-proxy {
    traceoptions {
      flag flag;
    }
  }
  custom-objects {
    custom-url-category object-name {
      value [value];
    }
    filename-extension object-name {
      value [value];
    }
    mime-pattern object-name {
      value [value];
    }
    protocol-command object-name {
      value [value];
    }
    url-pattern object-name {
      value [value];
    }
  }
  feature-profile {
    anti-spam {
      address-blacklist list-name;
      address-whitelist list-name;
      sbl {
        profile profile-name {
          custom-tag-string [string];
          (sbl-default-server | no-sbl-default-server);
          spam-action (block | tag-header | tag-subject);
        }
      }
      traceoptions {
        flag flag;
      }
    }
    anti-virus {
      juniper-express-engine {
        pattern-update {
          email-notify {
            admin-email email-address;
            custom-message message;
            custom-message-subject message-subject;
          }
          interval value;
          no-autoupdate;
          proxy {
            password password-string;
            port port-number;
```

```
            server address-or-url;
            username name;
          }
          url url;
        }
        profile profile-name {
          fallback-options {
            content-size (block | log-and-permit);
            default (block | log-and-permit);
            engine-not-ready (block | log-and-permit);
            out-of-resources (block | (log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
          }
          notification-options {
            fallback-block {
              administrator-email email-address;
              allow-email;
              custom-message message;
              custom-message-subject message-subject;
              display-host;
              (notify-mail-sender | no-notify-mail-sender);
              type (message | protocol-only);
            }
            fallback-non-block {
              custom-message message;
              custom-message-subject message-subject;
              (notify-mail-recipient | no-notify-mail-recipient);
            }
            virus-detection {
              custom-message message;
              custom-message-subject message-subject;
              (notify-mail-sender | no-notify-mail-sender);
              type (message | protocol-only);
            }
          }
          scan-options {
            content-size-limit value;
            (intelligent-prescreening | no-intelligent-prescreening);
            timeout value;
          }
          trickling {
            timeout value;
          }
        }
      }
      kaspersky-lab-engine {
        pattern-update {
          email-notify {
            admin-email email-address;
            custom-message message;
            custom-message-subject message-subject;
          }
          interval value;
          no-autoupdate;
```

```
        proxy {
            password password-string;
            port port-number;
            server address-or-url;
            username name;
        }
        url url;
    }
    profile profile-name {
        fallback-options {
            content-size (block | log-and-permit);
            corrupt-file (block | log-and-permit);
            decompress-layer (block | log-and-permit);
            default (block | log-and-permit);
            engine-not-ready (block | log-and-permit);
            out-of-resources (block | (log-and-permit);
            password-file (block | (log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        notification-options {
            fallback-block {
                administrator-email email-address;
                allow-email;
                custom-message message;
                custom-message-subject message-subject;
                display-host;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
            fallback-non-block {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-recipient | no-notify-mail-recipient);
            }
            virus-detection {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
        }
        scan-options {
            content-size-limit value;
            decompress-layer-limit value;
            (intelligent-prescreening | no-intelligent-prescreening);
            scan-extension filename;
            scan-mode (all | by-extension);
            timeout value;
        }
        trickling {
            timeout value;
        }
    }
}
```

```
mime-whitelist {
  exception listname;
  list listname {
    exception listname;
  }
}
sophos-engine {
  pattern-update {
    email-notify {
      admin-email email-address;
      custom-message message;
      custom-message-subject message-subject;
    }
    interval value;
    no-autoupdate;
    proxy {
      password password-string;
      port port-number;
      server address-or-url;
      username name;
    }
    url url;
  }
  profile <name> {
    fallback-options {
      content-size (block | log-and-permit | permit);
      default (block | log-and-permit | permit);
      engine-not-ready (block | log-and-permit | permit);
      out-of-resources (block | log-and-permit | permit);
      timeout (block | log-and-permit | permit);
      too-many-requests (block | log-and-permit | permit);
    }
    notification-options {
      fallback-block {
        administrator-email email-address;
        allow-email;
        custom-message message;
        custom-message-subject message-subject;
        display-host;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
      fallback-non-block {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-recipient | no-notify-mail-recipient);
      }
      virus-detection {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
    }
    scan-options {
```

```
            content-size-limit value;
            (no-uri-check | uri-check);
            timeout value;
          }
          trickling {
            timeout value;
          }
        }
        sxl-retry value;
        sxl-timeout seconds;
      }
      traceoptions {
        flag flag;
      }
      type (juniper-express-engine | kaspersky-lab-engine | sophos-engine);
      url-whitelist listname;
    }
    content-filtering {
      profile profile-name {
        block-command protocol-command-list;
        block-content-type (activex | exe | http-cookie | java-applet | zip);
        block-extension extension-list;
        block-mime {
          exception list-name;
          list list-name;
        }
        notification-options {
          custom-message message;
          (notify-mail-sender | no-notify-mail-sender);
          type (message | protocol-only);
        }
        permit-command protocol-command-list;
      }
      traceoptions {
        flag flag;
      }
    }
    web-filtering {
      juniper-enhanced {
        cache {
          size value;
          timeout value;
        }
        profile profile-name {
          block-message {
            type {
              custom-redirect-url;
            }
            url url;
            }
          quarantine-message {
            type {
              custom-redirect-url;
            }
              url url;
```

```
            }
        category customurl-list name {
          action (block | log-and-permit | permit | quarantine);
        }
        custom-block-message value;
        custom-quarantine-message value;
        default (block | log-and-permit | permit | quarantine);
        fallback-settings {
          default (block | log-and-permit);
          server-connectivity (block | log-and-permit);
          timeout (block | log-and-permit);
          too-many-requests (block | log-and-permit);
        }
        no-safe-search;
        site-reputation-action {
          fairly-safe (block | log-and-permit | permit | quarantine);
          harmful (block | log-and-permit | permit | quarantine);
          moderately-safe (block | log-and-permit | permit | quarantine);
          suspicious (block | log-and-permit | permit | quarantine);
          very-safe (block | log-and-permit | permit |quarantine);
        }
        timeout value;
      }
      server {
        host host-name;
        port number;
      }
    }
    juniper-local {
      profile profile-name {
        custom-block-message value;
        default (block | log-and-permit | permit);
        fallback-settings {
          default (block | log-and-permit);
          server-connectivity (block | log-and-permit);
          timeout (block | log-and-permit);
          too-many-requests (block | log-and-permit);
        }
        timeout value;
      }
    }
    surf-control-integrated {
      cache {
        size value;
        timeout value;
      }
      profile profile-name {
        category customurl-list name {
          action (block | log-and-permit | permit);
        }
        custom-block-message value;
        default (block | log-and-permit | permit);
        fallback-settings {
          default (block | log-and-permit);
          server-connectivity (block | log-and-permit);
```

```
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
          }
          timeout value;
        }
        server {
          host host-name;
          port number;
        }
      }
      traceoptions {
        flag flag;
      }
      type (juniper-enhanced | juniper-local | surf-control-integrated | websense-redirect);
      url-blacklist listname;
      url-whitelist listname;
      websense-redirect {
        profile profile-name {
          account value;
          custom-block-message value;
          fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
          }
          server {
            host host-name;
            port number;
          }
          sockets value;
          timeout value;
        }
      }
    }
}
ipc {
    traceoptions flag flag;
}
traceoptions {
    flag flag;
}
utm-policy policy-name {
    anti-spam {
      smtp-profile profile-name;
    }
    anti-virus {
      ftp {
        download-profile profile-name;
        upload-profile profile-name;
      }
      http-profile profile-name;
      imap-profile profile-name;
      pop3-profile profile-name;
      smtp-profile profile-name;
```

```
    }
    content-filtering {
      ftp {
        download-profile profile-name;
        upload-profile profile-name;
      }
      http-profile profile-name;
      imap-profile profile-name;
      pop3-profile profile-name;
      smtp-profile profile-name;
    }
    traffic-options {
      sessions-per-client {
        limit value;
        over-limit (block | log-and-permit);
      }
    }
    web-filtering {
      http-profile profile-name;
    }
  }
}
```

Hierarchy Level

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

Release Information

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

The Kaspersky, surf-control-integrated, and express antivirus features are not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5 .

Description

Configure UTM features.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

utm-policy

Syntax

```
utm-policy policy-name {
  anti-spam {
    smtp-profile profile-name;
  }
  anti-virus {
    ftp {
      download-profile profile-name;
      upload-profile profile-name;
    }
    http-profile profile-name;
    imap-profile profile-name;
    pop3-profile profile-name;
    smtp-profile profile-name;
  }
  content-filtering {
    ftp {
      download-profile profile-name;
      upload-profile profile-name;
    }
    http-profile profile-name;
    imap-profile profile-name;
    pop3-profile profile-name;
    smtp-profile profile-name;
  }
  traffic-options {
    sessions-per-client {
      limit value;
      over-limit (block | log-and-permit);
    }
  }
  web-filtering {
    http-profile profile-name;
  }
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure a UTM policy for antivirus, antispam, content-filtering, traffic-options, and Web-filtering protocols and attach this policy to a security profile to implement it.

Options

policy-name—Specify name of the UTM policy.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Security Policies Overview*
- *Understanding Security Policy Rules*
- *Understanding Security Policy Elements*

utm-policy (Application Services)

Syntax
```
utm-policy policy-name;
```

Hierarchy Level
```
[edit security policies from-zone zone-name to-zone zone-name policy policy-name then
  permit application-services]
```

Release Information
Statement introduced in Junos OS Release 11.1.

Description
Configure a UTM policy for application services and attach this policy to a security profile to implement it.

Options
policy-name—Specify the name of the UTM policy.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

virus-detection (Security Antivirus)

Syntax

```
virus-detection {
  custom-message message;
  custom-message-subject message-subject;
  (notify-mail-sender | no-notify-mail-sender);
  type (message | protocol-only);
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile anti-virus juniper-express-engine profile profile-name
  notification-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile profile-name
  notification-options]
[edit security utm feature-profile anti-virus sophos-engine profile profile-name
  notification-options]
```

Release Information

The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.
The Express and Kaspersky Antivirus features are not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5. Support for Sophos engine added in Junos OS Release 11.1.

Description

Configure a notification to send when a virus is detected.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

web-filtering

Syntax

```
web-filtering {
  http-persist;
  http-reassemble;
  juniper-enhanced {
    base-filter;
    block-message {
      type custom-redirect-url;
      url;
    }
    cache {
      size kilobytes;
      timeout minutes;
    }
    category name {
      action (block | log-and-permit | permit | quarantine);
      custom-message;
    }
    custom-block-message;
    default (block | log-and-permit | permit | quarantine);
    fallback-settings {
      default (block | log-and-permit);
      server-connectivity (block | log-and-permit);
      timeout (block | log-and-permit);
      too-many-requests (block | log-and-permit);
    }
    no-safe-search;
    quarantine-custom-message;
    quarantine-message {
      type custom-redirect-url;
      url;
    }
    reputation {
      reputation-fairly-safe;
      reputation-moderately-safe;
      reputation-suspicious;
      reputation-very-safe;
    }
    server {
      host;
      port;
      routing-instance;
    }
    site-reputation-action {
      fairly-safe (block | log-and-permit | permit | quarantine);
      harmful (block | log-and-permit | permit | quarantine);
      moderately-safe (block | log-and-permit | permit | quarantine);
      suspicious (block | log-and-permit | permit | quarantine);
      very-safe (block | log-and-permit | permit | quarantine);
    }
    timeout seconds;
  }
```

```
juniper-local {
  block-message {
    type custom-redirect-url;
    url;
  }
  category name {
    action (block | log-and-permit | permit | quarantine);
    custom-message;
  }
  custom-block-message;
  default (block | log-and-permit | permit);
  fallback-settings {
    default (block | log-and-permit);
    server-connectivity (block | log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  quarantine-custom-message;
  quarantine-message {
    type custom-redirect-url;
    url;
  }
  timeout seconds;
}
traceoptions {
  flag name;
}
url-blacklist;
url-whitelist;
websense-redirect {
  account;
  block-message {
    type custom-redirect-url;
    url;
  }
  category name {
    action (block | log-and-permit | permit | quarantine);
    custom-message;
  }
  custom-block-message;
  fallback-settings {
    default (block | log-and-permit);
    server-connectivity (block | log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  quarantine-custom-message;
  quarantine-message {
    type custom-redirect-url;
    url;
  }
  server {
    host;
    port;
    routing-instance;
```

```
    }
    sockets;
    timeout seconds;
  }
}
```

Hierarchy Level

```
[edit security utm feature-profile]
[edit security utm default-configuration]
```

Release Information

The surf-control-integrated feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure UTM web filtering features. You can also configure the default UTM configuration for web filtering feature profile. If you do not configure any option in the web filtering feature profile, the values configured in the default UTM configuration are applied. The default UTM Web filtering configuration for HTTP is also applicable for the HTTPS sessions. Web filtering feature's potential policies conflict check is independent of the content filtering, antivirus, and antispam features.

Options **http-persist**—Check all HTTP request in a connection. If **http-persist** option is enabled for clear text HTTP traffic, then Web filtering checks every HTTP request packet in the same session.

http-reassemble—Reassemble HTTP request segments. If http-reassemble option is enabled for clear text HTTP traffic, then Enhanced Web Filtering (EWF) reassembles the fragmented HTTP request to avoid evasion instead of packet-based inspection.

juniper-enhanced—Enable enhanced Web filtering on the device.

base-filter—A base filter is an object that contains a category-action pair for all categories defined in the category file.

block-message—Juniper enhanced block message settings.

cache—Set the cache parameters for Surf-Control-Integrated Web filtering and Enhanced Web Filtering.

category—Select a custom URL category list you created (custom objects) for filtering against.

custom-block-message—Enter a custom message to be sent when HTTP requests are blocked.

default—Specify an action for the profile, for requests that experience internal errors in the Web filtering module.

fallback-settings—Fallback settings tell the system how to handle errors.

no-safe-search— Do not perform safe-search for Juniper enhanced protocol. Safe-search redirect supports HTTP only. Therefore it is not possible to generate a redirect response for HTTPS search URLs. Safe-search redirects can be disabled by using the CLI option **no-safe-search**.

quarantine-custom-message—Juniper enhanced quarantine custom message.

quarantine-message—Juniper enhanced quarantine message settings.

reputation—Customize reputation level. The ThreatSeeker Cloud (TSC) provides site reputation information. Based on these reputations, you can choose a block or a permit action.

server—Set server parameters by entering the server name or IP address.

site-reputation-action—Specify the action to be taken depending on the site reputation returned for all types of URLs whether it is categorized or uncategorized.

timeout—Enter a timeout limit for requests. Once this limit is reached, fail mode settings are applied.

Range: 1 through 120

juniper-local—Enable Juniper Networks local URL filtering on the device.

block-message—Juniper local block message settings.

traceoptions—Trace options for Web filtering feature.

url-blacklist—This is a global blacklist category, blocking content for Web filtering.

url-whitelist—A URL whitelist is a unique custom list that you define in which all the URLs or IP addresses in that list for a specified category are always bypassed for filtering.

websense-redirect—Web filtering websense redirect engine. Websense occasionally releases new EWF categories. EWF classifies websites into categories according to host, URL, or IP address and performs filtering based on the categories.

type—Type of Web filtering solution or URL filtering solution used by the device.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- Understanding Local Web Filtering on page 116
- Monitoring Web Filtering Configurations on page 142

websense-redirect

Syntax

```
websense-redirect {
  profile profile-name {
    account value;
    custom-block-message value;
    fallback-settings {
      default (block | log-and-permit);
      server-connectivity (block | log-and-permit);
      timeout (block | log-and-permit);
      too-many-requests (block | log-and-permit);
    }
    server {
      host host-name;
      port number;
    }
    sockets value;
    timeout value;
  }
}
```

Hierarchy Level

```
[edit security utm default-configuration]
[edit security utm feature-profile web-filtering]
```

Release Information

Statement introduced in Junos OS Release 9.5.
The **[edit security utm default-configuration]** hierarchy level is introduced in Junos OS Release 18.2R1.

Description

Configure the Websense redirect engine features.

Starting with Junos OS Release 17.4R1, you can download and dynamically load new Enhanced Web Filtering (EWF) categories. The downloading and dynamic loading of the new EWF categories do not require a software upgrade. Websense occasionally releases new EWF categories. EWF classifies websites into categories according to host, URL, or IP address and performs filtering based on the categories.

NOTE: Existing configurations are not affected by the new categories but can be modified to make use of the new categories.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- Example: Enhancing Security by Configuring Redirect Web Filtering Using Custom Objects on page 131

CHAPTER 8

Operational Commands

- clear security utm anti-spam statistics
- clear security utm antivirus statistics
- clear security utm content-filtering statistics
- clear security utm session
- clear security utm web-filtering statistics
- request security utm anti-virus juniper-express-engine
- request security utm anti-virus kaspersky-lab-engine
- request security utm anti-virus sophos-engine
- request security utm web-filtering category install
- request security utm web-filtering category uninstall
- request security utm web-filtering category download-install [version]
- request security utm web-filtering category download [version]
- show configuration smtp
- show groups junos-defaults
- show security log
- show security policies
- show security utm anti-spam statistics
- show security utm anti-spam status
- show security utm anti-virus statistics
- show security utm anti-virus status
- show security utm content-filtering statistics
- show security utm session
- show security utm status
- show security utm web-filtering category base-filter
- show security utm web-filtering category category
- show security utm web-filtering category status
- show security utm web-filtering statistics
- show security utm web-filtering status

clear security utm anti-spam statistics

Syntax

```
clear security utm anti-spam statistics
<root-logical-system>
<logical-system (logical-system-name | all)>
```

Release Information

Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4.
Support for UTM in logical system added in Junos OS Release 18.3R1.

Description

Clears antispam statistics information. With chassis cluster support for UTM, statistics from both the nodes is cleared.

Starting in Junos OS Release 18.3R1, you can clear the antispam statistics information for the master logical system or for a specific user logical system or for all the user logical systems.

Options

none—Clears the antispam statistics information for the master logical system.

root-logical-system—(Optional) Clears the antispam statistics information for the master logical system.

logical-system *logical-system-name*—(Optional) Clears the antispam statistics information for a specific user logical system.

all—(Optional) Clears the antispam statistics information for all the user logical systems.

Required Privilege Level

clear

Related Documentation

- show security utm anti-spam statistics on page 398
- show security utm anti-spam status on page 401

Sample Output

clear security utm anti-spam statistics

```
user@host> clear security utm anti-spam statistics
Anti-spam clear statistics result: clear done
```

clear security utm anti-spam statistics root-logical-system

```
user@host> clear security utm anti-spam statistics root-logical-system
Anti-spam clear statistics result: clear done
```

clear security utm anti-spam statistics logical-system LSYS1

```
user@host> clear security utm anti-spam statistics logical-system LSYS1
Anti-spam clear statistics result: clear done
```

clear security utm anti-spam statistics logical-system all

```
user@host> clear security utm anti-spam statistics logical-system all
Anti-spam clear statistics result: clear done
```

clear security utm antivirus statistics

Syntax

```
clear security utm anti-virus statistics
<root-logical-system>
<logical-system (logical-system-name | all)>
```

Release Information

Command introduced in Junos OS Release 9.5.
Support for Sophos Antivirus added in Junos OS Release 11.1.
Support for UTM in chassis cluster added in Junos OS Release 11.4.
Support for UTM in logical system added in Junos OS Release 18.3R1.

Description

Clears antivirus statistics information. With chassis cluster support for UTM, statistics from both the nodes are cleared.

Starting in Junos OS Release 18.3R1, you can clear the antivirus statistics information for the master logical system or for a specific user logical system or for all the user logical systems.

Options

none—Clears the antivirus statistics information for the master logical system.

root-logical-system—(Optional) Clears the antivirus statistics information for the master logical system.

logical-system *logical-system-name*—(Optional) Clears the antivirus statistics information for a specific user logical system.

all—(Optional) Clears the antivirus statistics information for all the user logical systems.

Required Privilege Level

clear

Related Documentation

- show security utm anti-virus statistics on page 402
- show security utm anti-virus status on page 406
- request security utm anti-virus juniper-express-engine on page 373
- request security utm anti-virus kaspersky-lab-engine on page 374

Sample Output

clear security utm anti-virus statistics

```
user@host> clear security utm anti-virus statistics
Anti-virus clear statistics result: clear done
```

clear security utm anti-virus statistics root-logical-system

```
user@host> clear security utm anti-virus statistics root-logical-system
```

```
Anti-virus clear statistics result: clear done
```

clear security utm anti-virus statistics logical-system LSYS1

```
user@host> clear security utm anti-virus statistics logical-system LSYS1
Anti-virus clear statistics result: clear done
```

clear security utm anti-virus statistics logical-system all

```
user@host> clear security utm anti-virus statistics logical-system all
Anti-virus clear statistics result: clear done
```

clear security utm content-filtering statistics

Syntax

```
clear security utm content-filtering statistics
<root-logical-system>
<logical-system (logical-system-name | all)>
```

Release Information

Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4.
Support for UTM in logical system added in Junos OS Release 18.3R1.

Description

Clears content-filtering statistics information. With chassis cluster support for UTM, statistics from both the nodes are cleared.

Starting in Junos OS Release 18.3R1, you can clear the content filtering statistics information for the master logical system or for a specific user logical system or for all the user logical systems.

Options

none—Clears the content filtering statistics information for the master logical system.

root-logical-system—(Optional) Clears the content filtering statistics information for the master logical system.

logical-system *logical-system-name*—(Optional) Clears the content filtering statistics information for a specific user logical system.

all—(Optional) Clears the content filtering statistics information for all the user logical systems.

Required Privilege Level

clear

Related Documentation

- show security utm content-filtering statistics on page 408

Sample Output

clear security utm content-filtering statistics

```
user@host> clear security utm content-filtering statistics
Content-filtering clear statistics result: clear done
```

clear security utm content-filtering statistics root-logical-system

```
user@host> clear security utm content-filtering statistics root-logical-system
Content-filtering clear statistics result: clear done
```

clear security utm content-filtering statistics logical-system LSYS1

```
user@host> clear security utm content-filtering statistics logical-system LSYS1
Content-filtering clear statistics result: clear done
```

clear security utm content-filtering statistics logical-system all

```
user@host> clear security utm content-filtering statistics logical-system all
Content-filtering clear statistics result: clear done
```

clear security utm session

Syntax

```
clear security utm session
```

Release Information

Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4.

Description

Clear UTM session information. With chassis cluster support for UTM, sessions on both the nodes are cleared.

Required Privilege Level

clear

Related Documentation

- show security utm session on page 410
- show security utm status on page 411

Output Fields

This command produces no output.

clear security utm web-filtering statistics

Syntax

```
clear security utm web-filtering statistics
<root-logical-system>
<logical-system (logical-system-name | all)>
```

Release Information

Command introduced in Junos OS Release 9.5 .
Support for UTM in chassis cluster added in Junos OS Release 11.4 .
Support for UTM in logical system added in Junos OS Release 18.3R1.

Description

Clear web filtering statistics information. With chassis cluster support for UTM, statistics from both the nodes is cleared.

Starting in Junos OS Release 18.3R1, you can clear the Web filtering statistics information for the master logical system or for a specific user logical system or for all the user logical systems.

Options

none—Clears the Web filtering statistics information for the master logical system.

root-logical-system—(Optional) Clears the Web filtering statistics information for the master logical system.

logical-system *logical-system-name*—(Optional) Clears the Web filtering statistics information for a specific user logical system.

all—(Optional) Clears the Web filtering statistics information for all the user logical systems.

Required Privilege Level

clear

Related Documentation

- show security utm web-filtering statistics on page 418
- show security utm web-filtering status on page 422

Sample Output

clear security utm web-filtering statistics

```
user@host> clear security utm web-filtering statistics
Web-filtering clear statistics result: clear done
```

clear security utm web-filtering statistics root-logical-system

```
user@host> clear security utm web-filtering statistics root-logical-system
Web-filtering clear statistics result: clear done
```

clear security utm web-filtering statistics logical-system LSYS1

```
user@host> clear security utm web-filtering statistics logical-system LSYS1
Web-filtering clear statistics result: clear done
```

clear security utm web-filtering statistics logical-system all

```
user@host> clear security utm web-filtering statistics logical-system all
Web-filtering clear statistics result: clear done
```

request security utm anti-virus juniper-express-engine

Syntax request security utm anti-virus juniper-express-engine

Release Information The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, command introduced in Junos OS Release 9.5. Support for UTM in chassis cluster added in Junos OS Release 11.4 .

Description The Express Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards. For previous releases, manually update the express antivirus pattern database using the command described. You can update the express antivirus pattern database automatically or manually. With full chassis cluster support for UTM this command is operational on both the nodes.

Options

- **pattern-delete** — Delete the current express antivirus pattern database.
- **pattern-reload** — Reload the express antivirus pattern database.
- **pattern-update** — Update the express antivirus pattern database with the latest signatures.

Required Privilege Level maintenance

Related Documentation

- clear security utm antivirus statistics on page 366
- show security utm anti-virus statistics on page 402
- show security utm anti-virus status on page 406

List of Sample Output request security utm anti-virus juniper-express-engine pattern-update on page 373

Output Fields request security utm anti-virus juniper-express-engine pattern-update

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security utm anti-virus juniper-express-engine pattern-update

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

request security utm anti-virus kaspersky-lab-engine

Syntax

```
request security utm anti-virus kaspersky-lab-engine
```

Release Information

Command introduced in Junos OS Release 11.1 .
Support for UTM in chassis cluster added in Junos OS Release 11.4 .

Description

The Kaspersky Antivirus feature is not supported from Junos OS Release 15.1x49-D10 onwards.For previous releases, manually update the full file-based antivirus pattern database using the commands described. You can update the full file-based antivirus pattern database automatically or manually. With full chassis cluster support for UTM this command is operational on both the nodes.

Options

- **pattern-delete** — Delete the current full file-based antivirus pattern database.
- **pattern-reload** — Reload the full file-based antivirus pattern database.
- **pattern-update** — Update the full file-based antivirus pattern database with the latest signatures.

Required Privilege Level

maintenance

Related Documentation

- request security utm anti-virus juniper-express-engine on page 373
- clear security utm antivirus statistics on page 366
- show security utm anti-virus statistics on page 402
- show security utm anti-virus status on page 406

List of Sample Output

request security utm anti-virus kaspersky-lab-engine pattern-update on page 374

Output Fields

request security utm anti-virus kaspersky-lab-engine pattern-update

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security utm anti-virus kaspersky-lab-engine pattern-update

```
user@host> request security anti-virus kaspersky-lab-engine pattern-update
```

request security utm anti-virus sophos-engine

Syntax request security utm anti-virus sophos-engine

Release Information Command introduced in Junos OS Release 11.1 .
Support for UTM in chassis cluster added in Junos OS Release 11.4 .

Description Manually update the Sophos antivirus pattern database using the command described. To update automatically you use the configuration statement **set security utm feature-profile anti-virus sophos-engine pattern-update interval *seconds***. With full chassis cluster support for UTM this command is operational on both the nodes.

Options
- **pattern-delete** — Delete the current Sophos antivirus pattern database.
- **pattern-reload** — Reload the Sophos antivirus pattern database.
- **pattern-update** — Update the Sophos antivirus pattern database with the latest signatures.

Required Privilege Level maintenance

Related Documentation
- clear security utm antivirus statistics on page 366
- show security utm anti-virus statistics on page 402
- show security utm anti-virus status on page 406

List of Sample Output request security utm anti-virus sophos-engine pattern-update on page 375

Output Fields request security utm anti-virus sophos-engine pattern-update

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security utm anti-virus sophos-engine pattern-update

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

request security utm web-filtering category install

Syntax request security utm web-filtering category install

Release Information Command introduced in Junos OS Release 17.4.

Description Install the predefined category and predefined filter on the system. Users could check the category or filter using the following command: **show security utm web-filtering category base-filter**.

NOTE: During new category file installation, if the category filename is changed, then the new category file overwrites the old category file in the internal system and all related output information is replaced with the new category name.

Required Privilege Level maintenance

Related Documentation

- category (Security Web Filtering) on page 169
- request security utm web-filtering category uninstall on page 377

Sample Output

request security utm web-filtering category install

```
user@host> request security utm web-filtering category install
Category updater result: install done
```

request security utm web-filtering category uninstall

Syntax request security utm web-filtering category uninstall

Release Information Command introduced in Junos OS Release 17.4.

Description Reset the predefined category and the base filters to the factory default. This option helps for category rollback.

Required Privilege Level maintenance

Related Documentation

- category (Security Web Filtering) on page 169
- request security utm web-filtering category install on page 376

Sample Output

request security utm web-filtering category uninstall

```
user@host> request security utm web-filtering category uninstall
Category updater result: Uninstall done
```

request security utm web-filtering category download-install [version]

Syntax

```
request security utm web-filtering category download-install version;
```

Release Information

Command introduced in Junos OS Release 17.4.

Description

Download and install the category file, if no version is specified, the latest version is downloaded and installed during category upgrade.

Required Privilege Level

maintenance

Related Documentation

- category (Security Web Filtering) on page 169
- request security utm web-filtering category install on page 376
- request security utm web-filtering category download [version] on page 379

Sample Output

request security utm web-filtering category download-install version 5

```
user@host> request security utm web-filtering category download-install version 5
Category updater result: Download scheduled
```

request security utm web-filtering category download [version]

Syntax

```
request security utm web-filtering category download version;
```

Release Information Command introduced in Junos OS Release 17.4.

Description Download the category file, if no version is specified, the latest version of the category file is downloaded during category upgrade.

Required Privilege Level maintenance

Related Documentation

- category (Security Web Filtering) on page 169
- request security utm web-filtering category install on page 376
- request security utm web-filtering category uninstall on page 377
- request security utm web-filtering category download-install [version] on page 378

Sample Output

request security utm web-filtering category download version 3

```
user@host> request security utm web-filtering category download version 3
Category updater result: Download done
```

show configuration smtp

Syntax show configuration smtp

Release Information Command introduced in Junos OS Release 10.0 .

Description Display complete SMTP information.

Options
- apply-groups—Groups from which SMTP inherits configuration data.
- apply-groups-except—Groups from which SMTP restricts inheriting configuration data.

Required Privilege Level view

Related Documentation
- utm on page 345

List of Sample Output show configuration smtp on page 380

Output Fields Table 7 on page 380 describes the output fields for the **show configuration smtp** command.

Table 7: show configuration smtp

Field Name	Field Description	Level of Output
address	SMTP server's IPv4 address	All levels
login	Configure a mail sender account to the server	All levels
password	Default sender password for user authentication	All levels

Sample Output

show configuration smtp

```
user@host> show configuration smtp
primary-server {
    address 218.102.48.213;
    login "dayone@example.com" {
        password "$ABC123"; ## SECRET-DATA
    }
}
```

show groups junos-defaults

Syntax

```
show groups junos-defaults
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Display the full set of available preset statements from the Junos OS defaults group.

```
user@host# show groups junos-defaults
  groups {
    junos-defaults {
      applications {
        # File Transfer Protocol
        application junos-ftp {
          application-protocol ftp;
          protocol tcp;
          destination-port 21;
        }
        # Trivial File Transfer Protocol
        application junos-tftp {
          application-protocol tftp;
          protocol udp;
          destination-port 69;
        }
        # RPC port mapper on TCP
        application junos-rpc-portmap-tcp {
          application-protocol rpc-portmap;
          protocol tcp;
          destination-port 111;
        }
        # RPC port mapper on UDP
      }
    }
  }
```

Required Privilege Level

view

Related Documentation

- Using Junos OS Defaults Groups.

show security log

Syntax

show security log {*all*| *destination-address*| *destination-port*| *event-id*| *failure*|*interface-name*| *newer-than*| *older-than*| *process*| *protocol*|*report*| *severity*| *sort-by*| *source-address*| *source-port*| *success*| *user*}

Release Information

Command introduced in Junos OS Release 11.2 .

Description

Display security event logs. This command continuously displays security events on the screen. To stop the display, press Ctrl+c.

Options

all—Display all audit event logs stored in the device memory.

destination-address—Display audit event logs with the specified destination address.

destination-port—Display audit event logs with the specified destination port.

event-id—Display audit event logs with the specified event identification number.

failure—Display failed audit event logs.

interface-name—Display audit event logs with the specified interface.

newer-than—Display audit event logs newer than the specified date and time.

older-than—Display audit event logs older than the specified date and time.

process—Display audit event logs with the specified process that generated the event.

protocol—Display audit event logs generated through the specified protocol.

report—Display on-box reports for system traffic logs.

severity—Display audit event logs generated with the specified severity.

sort-by—Display audit event logs generated sorted with the specified options.

source-address—Display audit event logs with the specified source address.

source-port—Display audit event logs with the specified source port.

success—Display successful audit event logs.

username—Display audit event logs generated for the specified user.

Required Privilege Level

view

Related Documentation

- *exclude (Security Log)*
- *clear security log*

List of Sample Output show security log on page 383

Output Fields Table 8 on page 383 lists the output fields for the **show security log** command. Output fields are listed in the approximate order in which they appear.

Table 8: show security log Output Fields

Field Name	Field Description
Event time	The timestamp of the events received. On SRX Series devices, security logs were always timestamped using the UTC time zone by running **set system time-zone utc** and **set security log utc-timestamp** CLI commands. Now, time zone can be defined using the local time zone by running the **set system time-zone time-zone** command to specify the local time zone that the system should use when timestamping the security logs.
Message	Security events are listed.

Sample Output

show security log

```
user@host> show security log
```

```
Event time               Message
2010-10-22 13:28:37 CST  session created 1.1.1.2/1-->2.2.2.2/1308
 icmp 1.1.1.2/1-->2.2.2.2/1308
 None None 1 policy1 trustZone untrustZone 52 N/A(N/A) ge-0/0/1.0
2010-10-22 13:28:38 CST  session created 1.1.1.2/1-->2.2.2.2/1308 icmp
1.1.1.2/1-->2.2.2.2/1308 None None 1 policy1 trustZone untrustZone 54 N/A(N/A)
ge-0/0/1.0

...
```

```
2010-10-22 13:36:12 CST  session denied m icmp 1(8) policy1 trustZone untrustZone
 N/A(N/A) ge-0/0/1.0
2010-10-22 13:36:14 CST  session denied 1.1.1.2/2-->2.2.2.2/54812  icmp 1(8)
policy1 trustZone untrustZone N/A(N/A) ge-0/0/1.0

...
```

```
2010-10-27 15:50:11 CST  IP spoofing! source: 2.2.2.20, destination: 2.2.2.2,
protocol-id: 17, zone name: trustZone, interface name: ge-0/0/1.0, action: drop
2010-10-27 15:50:11 CST  IP spoofing! source: source: 2.2.2.20, destination:
2.2.2.2, protocol-id: 17, zone name: trustZone, interface name: ge-0/0/1.0, action:
 drop

...
```

```
2011-02-18 15:53:34 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/certification-authority/ca-profile1-ca1.cert
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/crl/ca-profile1.crl
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/system-key-pair/system-generated.priv
```

```
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/system-cert/system-generated.cert
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/key-pair/cert1.priv
2011-02-18 15:53:42 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/key-pair/test2.priv

...
```

```
2011-03-14 23:00:40 PDT  IDP_COMMIT_COMPLETED: IDP policy commit is complete.
                         IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;poli
cy[/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]

 ,failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT  ]
                         IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;poli
cy[/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]

 ,failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT  ]
                         IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;poli
cy[/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]

 ,failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT  ]

...
```

```
Event time               Message
2011-03-21 14:21:49 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
 9.9.9.1 source-address 6.6.6.1 '
2011-03-21 14:23:01 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
 9.9.9.1 source-address 6.6.6.1 .5 '
2011-03-21 14:23:05 CST  KMD_PM_SA_ESTABLISHED: Local gateway: 7.7.7.1, Remote
gateway: 8.8.8.1, Local ID: ipv4(any:0,[0..3]=6.6.6.1), Remote ID:
ipv4(any:0,[0..3]=9.9.9.1), Direction: inbound, SPI: 37a2a179, AUX-SPI: 0, Mode:
 tunnel, Type: dynamic
2011-03-21 14:23:05 CST  KMD_PM_SA_ESTABLISHED: Local gateway: 7.7.7.1, Remote
gateway: 8.8.8.1, Local ID: ipv4(any:0,[0..3]=6.6.6.1), Remote ID:
ipv4(any:0,[0..3]=9.9.9.1), Direction: outbound, SPI: b2231c1f, AUX-SPI: 0, Mode:
 tunnel, Type: dynamic
2011-03-21 14:23:08 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
 9.9.9.1 source-address 6.6.6.1 '
2011-03-21 14:23:13 CST  UI_CMDLINE_READ_LINE: User 'root', command 'show security
 log '
```

show security policies

Syntax

```
show security policies
application-firewall
count
detail
from-zone <zone-name>
global
hit-count
interface
logical-system <logical-system-name>
policy <policy-name>
root-logical-system
service-set
start
tenant <tenant-name>
to-zone <zone-name>
unknown-source-identity
zone-context
```

Release Information

Command modified in Junos OS Release 9.2.
Support for IPv6 addresses is added in Junos OS Release 10.2.
Support for wildcard addresses is added in Junos OS Release 11.1.
Support for global policy and services offloading is added in Junos OS Release 11.4.
Support for source-identities and the **Description** output field is added in Junos OS Release 12.1.
Support for negated address added in Junos OS Release 12.1X45-D10.
The output fields for Policy Statistics expanded, and the output fields for the **global** and **policy-name** options are expanded to include from-zone and to-zone global match criteria in Junos OS Release 12.1X47-D10.
Support for the **initial-tcp-mss** and **reverse-tcp-mss** options is added in Junos OS Release 12.3X48-D20.
Output field and description for **source-end-user-profile** option is added in Junos OS Release 15.1x49-D70.
Output field and description for **dynamic-applications** option is added in Junos OS Release 15.1x49-D100.
Output field and description for **dynapp-redir-profile** option is added in Junos OS Release 18.2R1.
The **tenant** option is introduced in Junos OS Release 18.3R1.

Description

Displays a summary of all security policies configured on the device. If a particular policy is specified, display information specific to that policy. The existing show commands for displaying the policies configured with multiple tenant support are enhanced. A security policy controls the traffic flow from one zone to another zone. The security policies allow you to deny, permit, reject (deny and send a TCP RST or ICMP port unreachable message to the source host), encrypt and decrypt, authenticate, prioritize, schedule, filter, and monitor the traffic attempting to cross from one security zone to another.

Options

- **application-firewall**—Displays the information of application-firewall.
- **count**—Displays the number of policies. Range is 1 through 65,535.
- **detail**—(Optional) Displays a detailed view of all of the policies configured on the device.
- **from-zone**—Displays the policy information matching the given source zone.
- **global**—(Optional) Displays information about global policies.
- **hit-count**—Displays the policies hit count.
- **interface**—Displays the name of the adaptive services interface.
- **logical-system**—Displays the logical system name.
- **policy-name**—(Optional) Displays the information about a specified policy.
- **root-logical-system**—Displays root logical system as default.
- **service-set**—Displays the name of the service set.
- **start**—Displays the policies from a given position. Range is 1 through 65,535.
- **tenant**—Displays the name of the tenant system.
- **to-zone**—Displays the policy information matching the given destination zone.
- **unknown-source-identity**—Displays the unknown-source-identity of a policy.
- **zone-context**—Displays the count of policies in each context (from-zone and to-zone).

Required Privilege Level

view

Related Documentation

- *Security Policies Overview*
- *Understanding Security Policy Rules*
- *Understanding Security Policy Elements*
- *Unified Policies Configuration Overview*

List of Sample Output

show security policies on page 389
show security policies (Dynamic Applications) on page 390
show security policies policy-name detail on page 391
show security policies (Services-Offload) on page 392
show security policies (Device Identity) on page 392
show security policies detail on page 392
show security policies detail (TCP Options) on page 395
show security policies policy-name (Negated Address) on page 395
show security policies policy-name detail (Negated Address) on page 395
show security policies global on page 396
show security policies detail tenant on page 396

Output Fields Table 9 on page 387 lists the output fields for the **show security policies** command. Output fields are listed in the approximate order in which they appear.

Table 9: show security policies Output Fields

Field Name	Field Description
From zone	Name of the source zone.
To zone	Name of the destination zone.
Policy	Name of the applicable policy.
Description	Description of the applicable policy.
State	Status of the policy: • **enabled**: The policy can be used in the policy lookup process, which determines access rights for a packet and the action taken in regard to it. • **disabled**: The policy cannot be used in the policy lookup process, and therefore it is not available for access control.
Index	Internal number associated with the policy.
Sequence number	Number of the policy within a given context. For example, three policies that are applicable in a from-zoneA-to-zoneB context might be ordered with sequence numbers 1, 2, 3. Also, in a from-zoneC-to-zoneD context, four policies might have sequence numbers 1, 2, 3, 4.
Source addresses	For standard display mode, the names of the source addresses for a policy. Address sets are resolved to their individual names. For detail display mode, the names and corresponding IP addresses of the source addresses for a policy. Address sets are resolved to their individual address name-IP address pairs.
Destination addresses	Name of the destination address (or address set) as it was entered in the destination zone's address book. A packet's destination address must match this value for the policy to apply to it.
source-end-user-profile	Name of the device identity profile (referred to as **end-user-profile** in the CLI) that contains attributes, or characteristics of a device. Specification of the device identity profile in the **source-end-user-profile** field is part of the device identity feature. If a device matches the attributes specified in the profile and other security policy parameters, then the security policy's action is applied to traffic issuing from the device.
Source addresses (excluded)	Name of the source address excluded from the policy.
Destination addresses (excluded)	Name of the destination address excluded from the policy.
Source identities	One or more user roles specified for a policy.

Table 9: show security policies Output Fields (continued)

Field Name	Field Description
Applications	Name of a preconfigured or custom application whose type the packet matches, as specified at configuration time. • **IP protocol**: The Internet protocol used by the application—for example, TCP, UDP, ICMP. • **ALG**: If an ALG is explicitly associated with the policy, the name of the ALG is displayed. If **application-protocol ignore** is configured, **ignore** is displayed. Otherwise, **0** is displayed. However, even if this command shows **ALG: 0**, ALGs might be triggered for packets destined to well-known ports on which ALGs are listening, unless ALGs are explicitly disabled or when **application-protocol ignore** is not configured for custom applications. • **Inactivity timeout**: Elapsed time without activity after which the application is terminated. • **Source port range**: The low-high source port range for the session application.
Dynamic Applications	Application identification-based Layer 7 dynamic applications.
Destination Address Translation	Status of the destination address translation traffic: • **drop translated**—Drop the packets with translated destination addresses. • **drop untranslated**—Drop the packets without translated destination addresses.

Application Firewall	An application firewall includes the following:
	• **Rule-set**—Name of the rule set.
	• **Rule**—Name of the rule.
	  • **Dynamic applications**—Name of the applications.
	  • **Dynamic application groups**—Name of the application groups.
	  • **Action**—The action taken with respect to a packet that matches the application firewall rule set. Actions include the following:
	  • **permit**
	  • **deny**
	• **Default rule**—The default rule applied when the identified application is not specified in any rules of the rule set.

Action or Action-type	• The action taken for a packet that matches the policy's tuples. Actions include the following:
	  • **permit**
	  • **firewall-authentication**
	  • **tunnel ipsec-vpn** *vpn-name*
	  • **pair-policy** *pair-policy-name*
	  • **source-nat pool** *pool-name*
	  • **pool-set** *pool-set-name*
	  • **interface**
	  • **destination-nat** *name*
	  • **deny**
	  • **reject**
	  • **services-offload**

Table 9: show security policies Output Fields (continued)

Field Name	Field Description
Session log	Session log entry that indicates whether the **at-create** and **at-close** flags were set at configuration time to log session information.
Scheduler name	Name of a preconfigured scheduler whose schedule determines when the policy is active and can be used as a possible match for traffic.

Policy statistics	• **Input bytes**—The total number of bytes presented for processing by the device.
	  ◦ **Initial direction**—The number of bytes presented for processing by the device from the initial direction.
	  ◦ **Reply direction**—The number of bytes presented for processing by the device from the reply direction.
	• **Output bytes**—The total number of bytes actually processed by the device.
	  ◦ **Initial direction**—The number of bytes from the initial direction actually processed by the device.
	  ◦ **Reply direction**—The number of bytes from the reply direction actually processed by the device.
	• **Input packets**—The total number of packets presented for processing by the device.
	  ◦ **Initial direction**—The number of packets presented for processing by the device from the initial direction.
	  ◦ **Reply direction**—The number of packets presented for processing by the device from the reply direction.
	• **Output packets**—The total number of packets actually processed by the device.
	  ◦ **Initial direction**—The number of packets actually processed by the device from the initial direction.
	  ◦ **Reply direction**—The number of packets actually processed by the device from the reply direction.
	• **Session rate**—The total number of active and deleted sessions.
	• **Active sessions**—The number of sessions currently present because of access control lookups that used this policy.
	• **Session deletions**—The number of sessions deleted since system startup.
	• **Policy lookups**—The number of times the policy was accessed to check for a match.

dynapp-redir-profile	Displays unified policy redirect profile. See *profile(dynamic-application)*.
Per policy TCP Options	Configured syn and sequence checks, and the configured TCP MSS value for the initial direction, the reverse direction or, both.

Sample Output

show security policies

```
user@host> show security policies

From zone: trust, To zone: untrust
Policy: p1, State: enabled, Index: 4, Sequence number: 1
  Source addresses:
  sa-1-ipv4: 198.51.100.11/24
```

```
    sa-2-ipv6: 2001:db8:a0b:12f0::1/32
    sa-3-ipv6: 2001:db8:a0b:12f0::22/32
    sa-4-wc:   203.0.113.1/255.255.0.255
    Destination addresses:
    da-1-ipv4: 2.2.2.2/24
    da-2-ipv6: 2001:db8:a0b:12f0::8/32
    da-3-ipv6: 2001:db8:a0b:12f0::9/32
    da-4-wc:   192.168.22.11/255.255.0.255
    Source identities: role1, role2, role4
    Applications: any
    Action: permit, application services, log, scheduled
    Application firewall : my_ruleset1
  Policy: p2, State: enabled, Index: 5, Sequence number: 2
    Source addresses:
    sa-1-ipv4:  198.51.100.11/24
    sa-2-ipv6:  2001:db8:a0b:12f0::1/32
    sa-3-ipv6:  2001:db8:a0b:12f0::22/32
    Destination addresses:
    da-1-ipv4:  2.2.2.2/24
    da-2-ipv6:  2001:db8:a0b:12f0::1/32
    da-3-ipv6:  2001:db8:a0b:12f0::9/32
    Source identities: role1, role4
    Applications: any
    Action: deny, scheduled
```

show security policies (Dynamic Applications)

```
user@host>show security policies

  Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Dynamic Applications: junos:YAHOO
    Action: deny, log
  Policy: p2, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 2
    Source addresses: any
    Destination addresses: any
    Applications: any
    Dynamic Applications: junos:web, junos:web:social-networking:facebook,
    junos:TFTP, junos:QQ
    Action: permit, log
  Policy: p3, State: enabled, Index: 6, Scope Policy: 0, Sequence number: 3
    Source addresses: any
    Destination addresses: any
    Applications: any
    Dynamic Applications: junos:HTTP, junos:SSL
    Action: permit, application services, log
```

The following example displays the output with unified policies configured.

```
user@host>  show security policies

Default policy: deny-all
Pre ID default policy: permit-all
From zone: trust, To zone: untrust
  Policy: p2, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
```

```
   Destination addresses: any
   Applications: junos-defaults
   Dynamic Applications: junos:GMAIL, junos:FACEBOOK-CHAT
   dynapp-redir-profile: profile1
```

show security policies policy-name detail

```
user@host> show security policies policy-name p1 detail
```

```
 Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
 Description: The policy p1 is for the sales team
 Sequence number: 1
 From zone: trust, To zone: untrust
 Source addresses:
   sa-1-ipv4:  198.51.100.11/24
   sa-2-ipv6:  2001:db8:a0b:12f0::1/32
   sa-3-ipv6:  2001:db8:a0b:12f0::9/32
   sa-4-wc:    203.0.113.1/255.255.0.255
 Destination addresses:
   da-1-ipv4: 192.0.2.0/24
   da-2-ipv6: 2001:db8:a0b:12f0::1/32
   da-3-ipv6: 2001:db8:a0b:12f0::9/32
   da-4-wc:   192.168.22.11/255.255.0.255
Source identities:
 role1
 role2
 role4
 Application: any
   IP protocol: 0, ALG: 0, Inactivity timeout: 0
     Source port range: [0-0]
     Destination port range: [0-0]
 Destination Address Translation: drop translated
 Application firewall :
 Rule-set: my_ruleset1
   Rule: rule1
     Dynamic Applications: junos:FACEBOOK-ACCESS, junos:YMSG
     Dynamic Application groups: junos:web, junos:chat
     Action: deny
   Default rule: permit
 Session log: at-create, at-close
 Scheduler name: sch20
 Per policy TCP Options: SYN check: No, SEQ check: No
 Policy statistics:
   Input  bytes       :               18144                 545 bps
     Initial direction:                9072                272 bps
     Reply direction  :                9072                 272 bps
   Output bytes       :               18144                 545 bps
     Initial direction:                9072                 272 bps
     Reply direction  :                9072                 272 bps
   Input  packets     :                 216                   6 pps
     Initial direction:                 108                   3 bps
     Reply direction  :                 108                   3 bps
   Output packets     :                 216                   6 pps
     Initial direction:                 108                   3 bps
     Reply direction  :                 108                   3 bps
   Session rate       :                 108                   3 sps
   Active sessions    :                  93
   Session deletions  :                  15
   Policy lookups     :                 108
```

The following example displays the output with unified policies configured.

```
user@host> show security policies policy-name p1 detail

Default policy: permit-all
Pre ID default policy: permit-all
From zone: trust, To zone: trust
  Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: reject
    dynapp-redir-profile: profile1
```

show security policies (Services-Offload)

```
user@host> show security policies

  Policy: p1, action-type: reject, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: trust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  dynapp-redir-profile: profile1(1)
  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
```

show security policies (Device Identity)

```
user@host> show security policies
From zone: trust, To zone: untrust
       Policy: dev-id-marketing, State: enabled, Index: 5, Scope Policy: 0,
Sequence number: 1
         Source addresses: any
         Destination addresses: any
         source-end-user-profile: marketing-profile
         Applications: any
         Action: permit
```

show security policies detail

```
user@host> show security policies detail

Default policy: deny-all
Policy: p1, action-type: permit, services-offload:enabled , State: enabled, Index:
 4, Scope Policy: 0
  Policy Type: Configured
  Description: The policy p1 is for the sales team
```

```
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    any-ipv4(global):  0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global):  0.0.0.0/0
    any-ipv6(global): ::/0
 Source identities:
  role1
  role2
  role4
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No
  Policy statistics:
    Input  bytes       :               18144                  545 bps
      Initial direction:                9072                 272 bps
      Reply direction  :                9072                  272 bps
    Output bytes       :               18144                  545 bps
      Initial direction:                9072                  272 bps
      Reply direction  :                9072                  272 bps
    Input  packets     :                 216                    6 pps
      Initial direction:                 108                    3 bps
      Reply direction  :                 108                    3 bps
    Output packets     :                 216                    6 pps
      Initial direction:                 108                    3 bps
      Reply direction  :                 108                    3 bps
    Session rate       :                 108                    3 sps
    Active sessions    :                  93
    Session deletions  :                  15
    Policy lookups     :                 108
Policy: p2, action-type: permit, services-offload:enabled , State: enabled, Index:
 5, Scope Policy: 0
  Policy Type: Configured
  Description: The policy p2 is for the sales team
  Sequence number: 1
  From zone: untrust, To zone: trust
  Source addresses:
    any-ipv4(global):  0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global):  0.0.0.0/0
    any-ipv6(global): ::/0
 Source identities:
  role1
  role2
  role4
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No
```

The following example displays the output with unified policies configured.

```
user@host> show security policies detail
```

```
Default policy: deny-all
Pre ID default policy: permit-all
Policy: p2, action-type: reject, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: junos-defaults
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [443-443]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [5432-5432]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [80-80]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [3128-3128]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [8000-8000]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [8080-8080]
    IP protocol: 17, ALG: 0, Inactivity timeout: 60
      Source port range: [0-0]
      Destination port range: [1-65535]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [443-443]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [5432-5432]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [80-80]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [3128-3128]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [8000-8000]
    IP protocol: 6, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [8080-8080]
    IP protocol: 17, ALG: 0, Inactivity timeout: 60
      Source port range: [0-0]
      Destination port range: [1-65535]
  Dynamic Application:
    junos:FACEBOOK-CHAT: 10704
    junos:GMAIL: 51
```

```
  dynapp-redir-profile: profile1(1)
  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
```

show security policies detail (TCP Options)

```
user@host> show security policies policy-name p2 detail
node0:
--------------------------------------------------------------------------
Policy:p2, action-type:permit, State: enabled,Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: trust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: junos-defaults
    IP protocol: tcp, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
 Destination port range: [80-80]
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
  Dynamic-application: junos:HTTP
```

show security policies policy-name (Negated Address)

```
user@host> show security policies policy-name p1
node0:
--------------------------------------------------------------------------
From zone: trust, To zone: untrust
  Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses(excluded): as1
    Destination addresses(excluded): as2
    Applications: any
    Action: permit
```

show security policies policy-name detail (Negated Address)

```
user@host> show security policies policy-name p1 detail
node0:
--------------------------------------------------------------------------
Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses(excluded):
    ad1(ad): 255.255.255.255/32
    ad2(ad):  198.51.100.1/24
    ad3(ad):  198.51.100.6  ~ 198.51.100.56
    ad4(ad):  192.0.2.8/24
    ad5(ad):  198.51.100.99 ~ 198.51.100.199
    ad6(ad):  203.0.113.9/24
    ad7(ad):  203.0.113.23/24
  Destination addresses(excluded):
    ad13(ad2): 198.51.100.76/24
```

```
    ad12(ad2): 198.51.100.88/24
    ad11(ad2): 192.0.2.23 ~ 192.0.2.66
    ad10(ad2): 192.0.2.93
    ad9(ad2):  203.0.113.76 ~ 203.0.113.106
    ad8(ad2):  203.0.113.199
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No
```

show security policies global

```
user@host> show security policies global policy-name Pa
```

```
node0:
--------------------------------------------------------------------------
  Global policies:
  Policy: Pa, State: enabled, Index: 6, Scope Policy: 0, Sequence number: 1
    From zones: any
    To zones: any
    Source addresses: H0
    Destination addresses: H1
    Applications: junos-http
    Action: permit
```

show security policies detail tenant

```
user@host> show security policies detail tenant TN1
```

```
Default policy: deny-all
Pre ID default policy: permit-all
Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
Policy Type: Configured
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses: any
Destination addresses: any
Application: junos-ping
IP protocol: 1, ALG: 0, Inactivity timeout: 60
ICMP Information: type=255, code=0
Application: junos-telnet
IP protocol: tcp, ALG: 0, Inactivity timeout: 1800
Source port range: [0-0]
Destination port range: [23-23]
Application: app_udp
IP protocol: udp, ALG: 0, Inactivity timeout: 1800
Source port range: [0-0]
Destination port range: [5000-5000]
Application: junos-icmp6-all
IP protocol: 58, ALG: 0, Inactivity timeout: 60
ICMP Information: type=255, code=0
Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
Session log: at-create, at-close
Policy statistics:
Input  bytes     :                   0                   0 bps
Initial direction:                   0                   0 bps
```

```
Reply direction  :                0                0 bps
Output bytes     :                0                0 bps
Initial direction:                0                0 bps
Reply direction  :                0                0 bps
Input  packets   :                0                0 pps
Initial direction:                0                0 bps
Reply direction  :                0                0 bps
Output packets   :                0                0 pps
Initial direction:                0                0 bps
Reply direction  :                0                0 bps
Session rate     :                0                0 sps
Active sessions  :                0
Session deletions:                0
Policy lookups   :                0
```

show security utm anti-spam statistics

Syntax

```
show security utm anti-spam statistics
<root-logical-system>
<logical-system (logical-system-name | all)>
```

Release Information

Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4.
Support for UTM in logical system added in Junos OS Release 18.3R1.

Description

Displays antispam statistics for connections including total e-mail scanned, tagged, and dropped connections.

Statistics from both the nodes (with full chassis cluster support for UTM) are displayed.

Starting in Junos OS Release 18.2R1, on SRX5000 Series devices, the options **pic** and **fpc** to view the physical interface cards (PICs) and Flexible PIC Concentrator (FPC) statistics are not supported.

Starting in Junos OS Release 18.3R1, you can view the antispam statistics for the master logical system or for a specific user logical system or for all the user logical systems.

Options

none—Displays antispam statistics for the master logical system.

root-logical-system—(Optional) Displays antispam statistics for the master logical system.

logical-system *logical-system-name*—(Optional) Displays antispam statistics for a specific user logical system.

all—(Optional) Displays antispam statistics for all the user logical systems.

Required Privilege Level

view

Related Documentation

- clear security utm anti-spam statistics on page 364
- show security utm anti-spam status on page 401

List of Sample Output

show security utm anti-spam statistics on page 399
show security utm anti-spam statistics root-logical-system on page 399
show security utm anti-spam statistics logical-system LSYS1 on page 399
show security utm anti-spam statistics logical-system all on page 400

Sample Output

show security utm anti-spam statistics

```
user@host> show security utm anti-spam statistics
Total connections:     0
Denied connections:    0
Total greetings:       0
Denied greetings:      0
Total e-mail scanned:  0
White list hit:        0
Black list hit:        0
Spam total:            0
Spam tagged:           0
Spam dropped:          0
DNS errors:            0
Timeout errors:        0
Return errors:         0
Invalid parameter errors: 0
```

show security utm anti-spam statistics root-logical-system

```
user@host> show security utm anti-spam statistics root-logical-system
 UTM Anti Spam statistics:

Total connections:     0
Denied connections:    0
Total greetings:       0
Denied greetings:      0
Total e-mail scanned:  0
White list hit:        0
Black list hit:        0
Spam total:            0
Spam tagged:           0
Spam dropped:          0
DNS errors:            0
Timeout errors:        0
Return errors:         0
Invalid parameter errors: 0
```

show security utm anti-spam statistics logical-system LSYS1

```
user@host> show security utm anti-spam statistics logical-system LSYS1
 UTM Anti Spam statistics:

Total connections:     0
Denied connections:    0
Total greetings:       0
Denied greetings:      0
Total e-mail scanned:  0
White list hit:        0
Black list hit:        0
Spam total:            0
Spam tagged:           0
Spam dropped:          0
DNS errors:            0
```

```
Timeout errors:        0
Return errors:         0
Invalid parameter errors: 0
```

show security utm anti-spam statistics logical-system all

```
user@host> show security utm anti-spam statistics logical-system all
```

```
 UTM Anti Spam statistics:

Total connections:     0
Denied connections:    0
Total greetings:       0
Denied greetings:      0
Total e-mail scanned:  0
White list hit:        0
Black list hit:        0
Spam total:            0
Spam tagged:           0
Spam dropped:          0
DNS errors:            0
Timeout errors:        0
Return errors:         0
Invalid parameter errors: 0
```

show security utm anti-spam status

Syntax

```
show security utm anti-spam status
```

Release Information

Command introduced in Junos OS Release 9.5 .
Support for UTM in chassis cluster added in Junos OS Release 11.4 .

Description

Display antispam status for connections including whitelist and blacklist server information. Status of both the nodes (with full chassis cluster support for UTM) is displayed.

Required Privilege Level

view

Related Documentation

- clear security utm anti-spam statistics on page 364
- show security utm anti-spam statistics on page 398

Output Fields

show security utm anti-spam status

Output fields are listed in the approximate order in which they appear.

show security utm anti-spam status

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

```
SBL Whitelist Server:
SBL Blacklist Server:
    msgsecurity.example.net
```

```
DNS Server:
    Primary  :     1.2.3.4, Src Interface: ge-0/0/0
    Secondary:     0.0.0.0, Src Interface: ge-0/0/1
    Ternary  :     0.0.0.0, Src Interface: fe-0/0/2
```

show security utm anti-virus statistics

Syntax

```
show security utm anti-virus statistics
<root-logical-system>
<logical-system (logical-system-name | all)>
<fpc <fpc-slot fpc-slot pic-slot pic-slot>>
```

Release Information

Command introduced in Junos OS Release 9.5.
Support for Sophos Antivirus added in Junos OS Release 11.1.
Support for UTM in chassis cluster added in Junos OS Release 11.4.
Support for Flexible PIC Concentrator (FPC) and PIC status added in Junos OS Release 12.1X46-D10.
Starting in Junos OS Release 18.2R1, on SRX5000 Series devices, the options **pic** and **fpc** are deprecated—rather than immediately removed—to provide backward compatibility.
Support for UTM in logical system added in Junos OS Release 18.3R1.

Description

Displays antivirus statistics for connections including clean and infected files, scan engine status, and aggregated statistics from all FPCs and PICs. Statistics from both the nodes (with full chassis cluster support for UTM) are displayed.

Starting in Junos OS Release 18.3R1, you can view the antivirus statistics for the master logical system or for a specific user logical system or for all the user logical systems.

Options

none—Displays antivirus statistics for the master logical system.

root-logical-system—(Optional) Displays antivirus statistics for the master logical system.

logical-system *logical-system-name*—(Optional) Displays antivirus statistics for a specific user logical system.

all—(Optional) Displays antivirus statistics for all the user logical systems.

Required Privilege Level

view

Related Documentation

- clear security utm antivirus statistics on page 366
- show security utm anti-virus status on page 406
- The Express and Kaspersky Antivirus feature is not supported from Junos OS Release 15.1X49-D10 onwards.request security utm anti-virus juniper-express-engine on page 373
- request security utm anti-virus kaspersky-lab-engine on page 374

List of Sample Output

show security utm anti-virus statistics on page 403
show security utm anti-virus statistics fpc on page 403
show security utm anti-virus statistics fpc fpc-slot 5 pic-slot 0 on page 403

show security utm anti-virus statistics root-logical-system on page 404
show security utm anti-virus statistics logical-system LSYS1 on page 404
show security utm anti-virus statistics logical-system all on page 404

Sample Output

show security utm anti-virus statistics

```
user@host> show security utm anti-virus statistics
UTM Anti Virus statistics:
MIME-whitelist passed:                0
URL-whitelist passed:                 0
Scan Request:

 Total           Clean         Threat-found    Fallback
     0               0              0               0

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

show security utm anti-virus statistics fpc

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

fpc-slot 5 pic-slot 0
UTM Anti Virus statistics:
MIME-whitelist passed:                0
URL-whitelist passed:                 0
Scan Request:

 Total           Clean         Threat-found    Fallback
     0               0              0               0

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

show security utm anti-virus statistics fpc fpc-slot 5 pic-slot 0

```
user@host> show security utm anti-virus statistics fpc fpc-slot 5 pic-slot 0
UTM Anti Virus statistics:
MIME-whitelist passed:                0
URL-whitelist passed:                 0
Scan Request:

 Total           Clean         Threat-found    Fallback
```

```
      0               0              0               0

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

show security utm anti-virus statistics root-logical-system

```
user@host> show security utm anti-virus statistics root-logical-system
UTM Anti Virus statistics:
MIME-whitelist passed:                0
URL-whitelist passed:                 0
Session abort:                        0
Scan Request:

 Total           Clean         Threat-found    Fallback
      0               0              0               0
Fallback:

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

show security utm anti-virus statistics logical-system LSYS1

```
user@host> show security utm anti-virus statistics logical-system LSYS1
UTM Anti Virus statistics:
MIME-whitelist passed:                0
URL-whitelist passed:                 0
Session abort:                        0
Scan Request:

 Total           Clean         Threat-found    Fallback
      0               0              0               0
Fallback:

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

show security utm anti-virus statistics logical-system all

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

```
UTM Anti Virus statistics:
MIME-whitelist passed:               0
URL-whitelist passed:                0
Session abort:                       0
Scan Request:

 Total           Clean         Threat-found    Fallback
     0               0              0               0
Fallback:

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

show security utm anti-virus status

Syntax show security utm anti-virus status <fpc <fpc-slot *fpc-slot* pic-slot *pic-slot*>>

Release Information Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4. Support for Flexible PIC Concentrator (FPC) and PIC status added in Junos OS Release 12.1X46-D10.
Starting in Junos OS Release 18.2R1, on SRX5000 Series devices, the options **pic** and **fpc** to display PIC and FPC statistics are not supported.

Description Display antivirus status for connections including clean and infected files, scan engine status, and aggregated status from all FPCs and PICs. Status of both the nodes (with full chassis cluster support for UTM) is displayed.

Required Privilege Level view

Related Documentation
- clear security utm antivirus statistics on page 366
- show security utm anti-virus statistics on page 402

List of Sample Output
show security utm anti-virus status on page 406
show security utm anti-virus status fpc on page 406
show security utm anti-virus status fpc fpc-slot 5 pic-slot 0 on page 407
show security utm anti-virus status on page 407

Output Fields show security utm anti-virus status

Output fields are listed in the approximate order in which they appear.

Sample Output

show security utm anti-virus status

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

   Anti-virus key expire date: 2017-04-01 00:00:00
   Update server: https://update.juniper-updates.net/SAV/
   Interval: 1440 minutes
   Pattern update status: next update in 1439 minutes
   Last result: new database downloaded
   Anti-virus signature version: 1.13 (1.02)
   Scan engine type: sophos-engine
   Scan engine information: last action result: No error
```

show security utm anti-virus status fpc

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

```
fpc-slot 5 pic-slot 0
UTM anti-virus status:

   Anti-virus key expire date: license not installed
   Update server: http://update.juniper-updates.net/SAV/
          Interval: 1440 minutes
          Pattern update status: update disabled due to no license
          Last result: already have latest database
   Anti-virus signature version:  000000_00
   Scan engine type: sophos-engine
   Scan engine information: last action result: No error
```

show security utm anti-virus status fpc fpc-slot 5 pic-slot 0

user@host> **show security utm anti-virus status fpc fpc-slot 5 pic-slot 0**

```
UTM anti-virus status:

   Anti-virus key expire date: license not installed
   Update server: http://update.juniper-updates.net/SAV/
          Interval: 1440 minutes
          Pattern update status: update disabled due to no license
          Last result: already have latest database
   Anti-virus signature version: 000000_00
   Scan engine type: sophos-engine
   Scan engine information: last action result: No error
```

show security utm anti-virus status

Refer the sample output for Avira scan engine. Support for Avira is added in 18.4R1 release.

```
UTM anti-virus status:
 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
```

show security utm content-filtering statistics

Syntax

```
show security utm content-filtering statistics
<root-logical-system>
<logical-system (logical-system-name | all)>
```

Release Information

Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4.
Starting in Junos OS Release 18.2R1, on SRX5000 Series devices, the options **pic** and **fpc** to display physical interface cards (PICs) and Flexible PIC Concentrator (FPC) statistics are not supported.
Support for UTM in logical system added in Junos OS Release 18.3R1.

Description

Displays the content filtering statistics for connections including lists of blocked files and the reasons for blocking. Statistics from both the nodes (with full chassis cluster support for UTM) are displayed.

Starting in Junos OS Release 18.3R1, you can view the content filtering statistics for the master logical system or for a specific user logical system or for all the user logical systems.

Options

none—Displays content filtering statistics for the master logical system.

root-logical-system—(Optional) Displays content filtering statistics for the master logical system.

logical-system *logical-system-name*—(Optional) Displays content filtering statistics for a specific user logical system.

all—(Optional) Displays content filtering statistics for all the user logical systems.

Required Privilege Level

view

Related Documentation

- clear security utm content-filtering statistics on page 368

List of Sample Output

show security utm content-filtering statistics on page 408
show security utm content-filtering statistics root-logical-system on page 409
show security utm content-filtering statistics logical-system LSYS1 on page 409
show security utm content-filtering statistics logical-system all on page 409

Sample Output

show security utm content-filtering statistics

```
user@host> show security utm content-filtering statistics
```

```
Content-filtering-statistic:         Blocked
    Base on command list:                    0
    Base on mime list:                       0
    Base on extension list:                  0
    ActiveX plugin:                          0
    Java applet:                             0
    EXE files:                               0
    ZIP files:                               0
    HTTP cookie:                             0
```

show security utm content-filtering statistics root-logical-system

```
user@host> show security utm content-filtering statistics root-logical-system
Content-filtering-statistic:         Blocked
    Base on command list:                    0
    Base on mime list:                       0
    Base on extension list:                  0
    ActiveX plugin:                          0
    Java applet:                             0
    EXE files:                               0
    ZIP files:                               0
    HTTP cookie:                             0
```

show security utm content-filtering statistics logical-system LSYS1

```
user@host> show security utm content-filtering statistics logical-system LSYS1
Content-filtering-statistic:         Blocked
    Base on command list:                    0
    Base on mime list:                       0
    Base on extension list:                  0
    ActiveX plugin:                          0
    Java applet:                             0
    EXE files:                               0
    ZIP files:                               0
    HTTP cookie:                             0
```

show security utm content-filtering statistics logical-system all

```
user@host> show security utm content-filtering statistics logical-system all
Content-filtering-statistic:         Blocked
    Base on command list:                    0
    Base on mime list:                       0
    Base on extension list:                  0
    ActiveX plugin:                          0
    Java applet:                             0
    EXE files:                               0
    ZIP files:                               0
    HTTP cookie:                             0
```

show security utm session

Syntax

```
show security utm session
```

Release Information

Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4.
Starting in Junos OS Release 18.2R1, on SRX5000 Series devices, the options **pic** and **fpc** to display physical interface cards (PICs) and Flexible PIC Concentrator (FPC) statistics are not supported.

Description

Display general UTM session information including all allocated sessions and active sessions. Also, display information from both nodes in a chassis cluster.

Required Privilege Level

view

Related Documentation

- clear security utm session on page 370
- show security utm status on page 411

Output Fields

show security utm session

When you enter this command, you are provided feedback on the status of your request.

show security utm session

```
user@host> show security utm session
Maximum sessions:           4000
 Total allocated sessions:         0
 Total freed sessions:             0
 Active sessions:                  0
```

show security utm status

Syntax

```
show security utm status
```

Release Information

Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4.

Description

Display whether the UTM service is running or not and status of both the nodes (with full chassis cluster support for UTM).

Required Privilege Level

view

Related Documentation

- clear security utm session on page 370
- show security utm session on page 410

Output Fields

show security utm status

When you enter this command, you are provided feedback on the status of your request.

show security utm status

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

show security utm web-filtering category base-filter

Syntax show security utm web-filtering category base-filter

Release Information Command introduced in Junos OS Release 17.4.

Description Show the list of predefined base filters. A base filter is an object that contains a category-action pair for all categories defined in the category file. A base filter is a structured object, and is defined with the help of a filter name and an array of category-action pairs. Each Enhanced Web Filtering (EWF) category has a default action in a base filter, which is attached to the user profile to act as a backup filter. If the categories are not configured in the user profile, the base filter takes the action. Junos OS Release 17.4R1 also supports online upgradation of base filters.

Required Privilege Level view

Related Documentation

- category (Security Web Filtering) on page 169
- request security utm web-filtering category install on page 376
- show security utm web-filtering category status on page 417

Sample Output

show security utm web-filtering category base-filter

```
user@host> show security utm web-filtering category base-filter
Base-filter: ewf-default-filter
    Enhanced_Adult_Material                                      block
    Enhanced_Business_and_Economy                                permit
    Enhanced_Education                                           permit
    Enhanced_Government                                          permit
    Enhanced_News_and_Media                                      permit
    Enhanced_Religion                                            permit
    Enhanced_Society_and_Lifestyles                              permit
    Enhanced_Special_Events                                      permit
    Enhanced_Information_Technology                              permit
    Enhanced_Abortion                                            block
    Enhanced_Advocacy_Groups                                     permit
    Enhanced_Entertainment                                       permit
```

```
Enhanced_Gambling                                    block
Enhanced_Games                                       block
Enhanced_Illegal_or_Questionable                     block
Enhanced_Job_Search                                  permit
Enhanced_Shopping                                    permit
Enhanced_Sports                                      permit
Enhanced_Tasteless                                   permit
Enhanced_Travel                                      permit
Enhanced_Vehicles                                    permit
Enhanced_Violence                                    block
Enhanced_Weapons                                     block
Enhanced_Drugs                                       block
Enhanced_Militancy_and_Extremist                     block
Enhanced_Intolerance                                 permit
Enhanced_Health                                      permit
Enhanced_Website_Translation                         permit
Enhanced_Advertisements                              permit
Enhanced_User_Defined                                permit
Enhanced_Nudity                                      block
Enhanced_Adult_Content                               block
Enhanced_Sex                                         block
Enhanced_Financial_Data_and_Services                 permit
Enhanced_Cultural_Institutions                       permit
Enhanced_Media_File_Download                         permit
Enhanced_Military                                    permit
Enhanced_Political_Organizations                     permit
Enhanced_General_Email                               permit
Enhanced_Proxy_Avoidance                             block
Enhanced_Search_Engines_and_Portals                  permit
Enhanced_Web_Hosting                                 permit
```

```
Enhanced_Web_Chat                                    permit
Enhanced_Hacking                                      block
Enhanced_Alternative_Journals                        permit
Enhanced_Non_Traditional_Religions                    block
Enhanced_Traditional_Religions                       permit
Enhanced_Restaurants_and_Dining                      permit
Enhanced_Gay_or_Lesbian_or_Bisexual_Interest         permit
Enhanced_Personals_and_Dating                        permit
Enhanced_Alcohol_and_Tobacco                         permit
Enhanced_Prescribed_Medications                      permit
```

show security utm web-filtering category category

Syntax show security utm web-filtering category category

Release Information Command introduced in Junos OS Release 17.4.

Description Show the list of categories predefined by Websense. A category list is available on the device. This list consists of categories, each containing a category code, a name, and a parent ID. Categories can also be user-defined. Each category consists of a list of URLs or IP addresses. Categories are not updated dynamically and are tied to the Junos OS release because they have to be compiled into the Junos OS image. Any update in categories needs to be synchronized with the Junos OS release cycle.

NOTE: Starting with Junos OS Release 17.4R1, you can download and dynamically load new Enhanced Web Filtering (EWF) categories. The downloading and dynamic loading of the new EWF categories do not require a software upgrade.

Required Privilege Level view

Related Documentation

- category (Security Web Filtering) on page 169
- request security utm web-filtering category install on page 376
- show security utm web-filtering category base-filter on page 412
- Predefined Category Upgrading and Base Filter Configuration Overview on page 89

Sample Output

show security utm web-filtering category category

```
user@host> show security utm web-filtering category category
Enhanced_Adult_Material
    Enhanced_Business_and_Economy
    Enhanced_Education
    Enhanced_Government
    Enhanced_News_and_Media
    Enhanced_Religion
    Enhanced_Society_and_Lifestyles
    Enhanced_Special_Events
    Enhanced_Information_Technology
    Enhanced_Abortion
    Enhanced_Advocacy_Groups
    Enhanced_Entertainment
    Enhanced_Gambling
    Enhanced_Games
```

```
    Enhanced_Illegal_or_Questionable
    Enhanced_Job_Search
    Enhanced_Shopping
    Enhanced_Sports
    Enhanced_Tasteless
    Enhanced_Travel
    Enhanced_Vehicles
    Enhanced_Violence
```

show security utm web-filtering category status

Syntax show security utm web-filtering category status

Release Information Command introduced in Junos OS Release 17.4.

Description Show the current running version of the downloaded category file or the status of the installed predefined file.

Required Privilege Level view

Related Documentation

- category (Security Web Filtering) on page 169
- request security utm web-filtering category install on page 376
- show security utm web-filtering category base-filter on page 412

Sample Output

show security utm web-filtering category status

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

show security utm web-filtering statistics

Syntax

```
show security utm web-filtering statistics
<root-logical-system>
<logical-system (logical-system-name | all)>
<fpc <fpc-slot fpc-slot pic-slot pic-slot>>
```

Release Information

Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4.
Support for Flexible PIC Concentrator (FPC) and PIC statistics added in Junos OS Release 12.1X46-D10.
Starting in Junos OS Release 18.2R1, on SRX5000 Series devices, the options **pic** and **fpc** are deprecated—rather than immediately removed—to provide backward compatibility.
Support for UTM in logical system added in Junos OS Release 18.3R1.

Description

Displays Web filtering statistics for connections including whitelist and blacklist hits and custom category hits. The aggregated statistics from all FPCs and PICs and statistics from both the nodes (with full chassis cluster support for UTM) are also displayed.

Starting in Junos OS Release 18.3R1, you can view the Web filtering statistics for the master logical system or for a specific user logical system or for all the user logical systems.

Options

none—Displays Web filtering statistics for the master logical system.

root-logical-system—(Optional) Displays Web filtering statistics for the master logical system.

logical-system *logical-system-name*—(Optional) Displays Web filtering statistics for a specific user logical system.

all—(Optional) Displays Web filtering statistics for all the user logical systems.

Required Privilege Level

view

Related Documentation

- clear security utm web-filtering statistics on page 371
- show security utm web-filtering status on page 422

List of Sample Output

show security utm web-filtering statistics on page 419
show security utm web-filtering statistics fpc on page 419
show security utm web-filtering statistics fpc fpc-slot 5 pic-slot 0 on page 420
show security utm web-filtering statistics root-logical-system on page 421
show security utm web-filtering statistics logical-system LSYS1 on page 421
show security utm web-filtering statistics logical-system all on page 421

Sample Output

show security utm web-filtering statistics

```
user@host> show security utm web-filtering statistics
UTM web-filtering statistics:
   Total requests:                     0
   white list hit:                     0
   Black list hit:                     0
   Queries to server:                  0
   Server reply permit:                0
   Server reply block:                 0
   Server reply quarantine:            0
   Server reply quarantine block:      0
   Server reply quarantine permit:     0
   Custom category permit:             0
   Custom category block:              0
   Custom category quarantine:         0
   Custom category qurantine block:    0
   Custom category quarantine permit:  0
   Site reputation permit:             0
   Site reputation block:              0
   Site reputation quarantine:         0
   Site reputation quarantine block:   0
   Site reputation quarantine permit:  0
   Site reputation by Category         0
   Site reputation by Global           0
   Cache hit permit:                   0
   Cache hit block:                    0
   Cache hit quarantine:               0
   Cache hit quarantine block:         0
   Cache hit quarantine permit:        0
   Safe-search redirect:               0
  SNI pre-check queries to server:    1
   SNI pre-check server responses:     1
   Web-filtering sessions in total:    128000
   Web-filtering sessions in use:      0
   Fallback:                       log-and-permit           block
         Default                                0               0
         Timeout                                0               0
    Connectivity                                0               0
Too-many-requests                               0               0
```

show security utm web-filtering statistics fpc

```
user@host> show security utm web-filtering statistics fpc

fpc-slot 5 pic-slot 0
UTM web-filtering statistics:
   Total requests:                     0
   white list hit:                     0
   Black list hit:                     0
   Queries to server:                  0
   Server reply permit:                0
   Server reply block:                 0
   Server reply quarantine:            0
   Server reply quarantine block:      0
```

```
   Server reply quarantine permit:     0
   Custom category permit:             0
   Custom category block:              0
   Custom category quarantine:         0
   Custom category qurantine block:    0
   Custom category quarantine permit:  0
   Site reputation permit:             0
   Site reputation block:              0
   Site reputation quarantine:         0
   Site reputation quarantine block:   0
   Site reputation quarantine permit:  0
   Site reputation by Category         0
   Site reputation by Global           0
   Cache hit permit:                   0
   Cache hit block:                    0
   Cache hit quarantine:               0
   Cache hit quarantine block:         0
   Cache hit quarantine permit:        0
   Safe-search redirect:               0
 SNI pre-check queries to server:   1
   SNI pre-check server responses:     1
   Web-filtering sessions in total:    128000
   Web-filtering sessions in use:      0
   Fallback:                       log-and-permit           block
         Default                                0               0
         Timeout                                0               0
    Connectivity                                0               0
Too-many-requests                               0               0
```

show security utm web-filtering statistics fpc fpc-slot 5 pic-slot 0

```
user@host> show security utm web-filtering statistics fpc fpc-slot 5 pic-slot 0
```

```
UTM web-filtering statistics:
   Total requests:                     0
   white list hit:                     0
   Black list hit:                     0
   Queries to server:                  0
   Server reply permit:                0
   Server reply block:                 0
   Server reply quarantine:            0
   Server reply quarantine block:      0
   Server reply quarantine permit:     0
   Custom category permit:             0
   Custom category block:              0
   Custom category quarantine:         0
   Custom category qurantine block:    0
   Custom category quarantine permit:  0
   Site reputation permit:             0
   Site reputation block:              0
   Site reputation quarantine:         0
   Site reputation quarantine block:   0
   Site reputation quarantine permit:  0
   Site reputation by Category         0
   Site reputation by Global           0
   Cache hit permit:                   0
   Cache hit block:                    0
   Cache hit quarantine:               0
   Cache hit quarantine block:         0
   Cache hit quarantine permit:        0
```

```
   Safe-search redirect:              0
  SNI pre-check queries to server:   1
   SNI pre-check server responses:     1
   Web-filtering sessions in total:    128000
   Web-filtering sessions in use:      0
   Fallback:                       log-and-permit           block
         Default                                 0               0
         Timeout                                 0               0
    Connectivity                                 0               0
Too-many-requests                                0               0
```

show security utm web-filtering statistics root-logical-system

```
user@host> show security utm web-filtering statistics root-logical-system
```

```
UTM web-filtering statistics:
   Web-filtering sessions in total:    2048000
   Web-filtering sessions in use:      0
   Fallback:                       log-and-permit           block
         Default                                 0               0
         Timeout                                 0               0
    Connectivity                                 0               0
Too-many-requests                                0               0
```

show security utm web-filtering statistics logical-system LSYS1

```
user@host> show security utm web-filtering statistics logical-system LSYS1
```

```
UTM web-filtering statistics:
   Web-filtering sessions in total:    2048000
   Web-filtering sessions in use:      0
   Fallback:                       log-and-permit           block
         Default                                 0               0
         Timeout                                 0               0
    Connectivity                                 0               0
Too-many-requests                                0               0
```

show security utm web-filtering statistics logical-system all

```
user@host> show security utm web-filtering statistics logical-system all
```

```
UTM web-filtering statistics:
   Web-filtering sessions in total:    2048000
   Web-filtering sessions in use:      0
   Fallback:                       log-and-permit           block
         Default                                 0               0
         Timeout                                 0               0
    Connectivity                                 0               0
Too-many-requests                                0               0
```

show security utm web-filtering status

Syntax

```
show security utm web-filtering status <fpc <fpc-slot fpc-slot pic-slot pic-slot>>
```

Release Information

Command introduced in Junos OS Release 9.5.
Support for UTM in chassis cluster added in Junos OS Release 11.4. Support for Flexible PIC Concentrator (FPC) and PIC status added in Junos OS Release 12.1X46-D10.
Starting in Junos OS Release 18.2R1, on SRX5000 Series devices, the options **pic** and **fpc** to display PIC and FPC statistics are not supported.

Description

Display whether the Web filtering server connection is up or not. The aggregated status from all FPCs and PICs and status of both the nodes (with full chassis cluster support for UTM) are also displayed.

Required Privilege Level

view

Related Documentation

- clear security utm web-filtering statistics on page 371
- show security utm web-filtering statistics on page 418

List of Sample Output

show security utm web-filtering status on page 422
show security utm web-filtering status fpc on page 422
show security utm web-filtering status fpc fpc-slot 5 pic-slot 0 on page 423
show security utm web-filtering chassis cluster status on page 423

Output Fields

show security utm web-filtering status

Output fields are listed in the approximate order in which they appear.

Sample Output

show security utm web-filtering status

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

show security utm web-filtering status fpc

```
user@host> show security utm web-filtering status fpc
UTM web-filtering status fpc:
fpc-slot 5 pic-slot 0
Connectivity status: UP
fpc-slot 0 pic-slot 1
Connectivity status: UP
```

show security utm web-filtering status fpc fpc-slot 5 pic-slot 0

```
user@host> show security utm web-filtering status fpc fpc-slot 5 pic-slot 0
UTM web-filtering status:
Connectivity status: UP
```

show security utm web-filtering chassis cluster status

```
{primary:node0}
user@host>  show security utm web-filtering status
node0:
--------------------------------------------------------------------------
UTM web-filtering status:
   Server status: Juniper Enhanced using Websense server UP

node1:
--------------------------------------------------------------------------
UTM web-filtering status:
   Server status: Juniper Enhanced using Websense server DOWN
```

Starting with 12.3X48-D10 and Junos OS Release 17.3R1, on SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, and SRX550M devices, the UTM process has been moved to the Packet Forwarding Engine (PFE). Starting with 12.1X46-D10 and Junos OS Release 17.3R1, on SRX1400, SRX1500, SRX3400, SRX3600, SRX4100, SRX4200, SRX4600, SRX5400, and SRX5600 devices, the UTM process has been moved to the PFE. Hence, the status shows down on the secondary node of the cluster.