

IN FOCUS

J-Web for SRX Series

Published
2020-09-22

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

IN FOCUS J-Web for SRX Series

Copyright © 2020 Juniper Networks, Inc. All rights reserved.

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 | v

Documentation and Release Notes | v

Documentation Conventions | v

Documentation Feedback | viii

Requesting Technical Support | viii

Self-Help Online Tools and Resources | ix

Creating a Service Request with JTAC | ix

1

Start Here with J-Web for SRX Series

What You Need to Know About the In Focus Guide | 11

2

UTM Web Filtering

Allow or Block Websites by Using J-Web Integrated UTM Web Filtering | 13

Benefits of UTM Web Filtering | 13

Why URL Filtering | 14

Web Filtering Workflow | 14

Scope | 14

Before You Begin | 15

Topology | 16

Sneak Peek – J-Web UTM Web Filtering Steps | 16

Step 1: List URLs That You Want to Allow or Block | 16

Step 2: Categorize the URLs That You Want to Allow or Block | 18

Step 3: Add a Web Filtering Profile | 20

Step 4: Reference a Web Filtering Profile in a UTM Policy | 23

Step 5: Assign a UTM Policy to a Security Policy | 24

Step 6: Verify That the URLs Are Allowed or Blocked from the Server | 27

What's Next | 27

Sample Configuration Output | 28

UTM Antivirus

Prevent Virus Attacks by Using J-Web UTM Antivirus | 32

UTM Antivirus Overview | 32

Benefits of UTM Antivirus | 33

Antivirus Workflow | 34

Scope | 34

Before You Begin | 34

Topology | 34

Video | 34

Sneak Peek – J-Web UTM Antivirus Configuration Steps | 35

Step 1: Configure Antivirus Custom Object | 35

Step 1a: Configure a URL Pattern List That You Want to Bypass | 36

Step 1b: Categorize the URLs That You Want to Allow | 38

Step 2: Configure Antivirus Feature Profile | 40

Step 2a: Update Default Configuration for Antivirus | 40

Step 2b: Create Antivirus Feature Profile | 41

Step 3: Apply the Antivirus Feature Profile to a UTM Policy | 44

Step 4: Assign the UTM Policy to a Security Firewall Policy | 45

Verify That UTM Antivirus Is Working | 48

What's Next? | 49

Sample Configuration Output | 50

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | v
- Documentation Conventions | v
- Documentation Feedback | viii
- Requesting Technical Support | viii

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>.

Documentation Conventions

[Table 1 on page vi](#) 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 vi 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 |
| <i>Italic text like this</i> | <ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. | <ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i> |

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

| Convention | Description | Examples |
|--------------------------------|--|--|
| <i>Italic text like this</i> | 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 <i>domain-name</i> |
| Text like this | Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components. | <ul style="list-style-type: none"> 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 <i>metric</i> >; |
| (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 (<i>string1</i> <i>string2</i> <i>string3</i>) |
| # (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 [<i>community-ids</i>] |
| Indentation and braces ({ }) | Identifies a level in the configuration hierarchy. | [edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } } |
| ; (semicolon) | Identifies a leaf statement at a configuration hierarchy level. | |

GUI Conventions

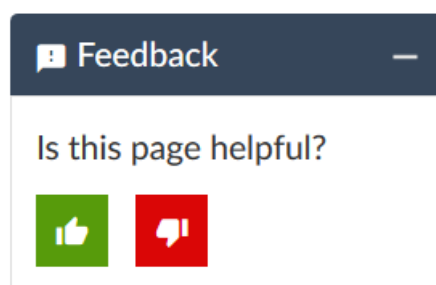
Table 2: Text and Syntax Conventions (*continued*)

| Convention | Description | Examples |
|------------------------------|--|---|
| Bold text like this | Represents graphical user interface (GUI) items you click or select. | <ul style="list-style-type: none"> 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/>.

1

CHAPTER

Start Here with J-Web for SRX Series

[What You Need to Know About the In Focus Guide](#) | **11**

What You Need to Know About the In Focus Guide

Use this guide to quickly learn about the most important features in J-Web for SRX Series Release 19.4R1 and how you can deploy them in your network.

You might also be interested in seeing the complete list of features in the [Release Notes for Junos OS Release 19.4](#). In addition to this guide, you can find concept information and configuration details in the [J-Web for SRX Series Documentation](#).

Want to tell us what you think about this guide? E-mail us at techpubs-comments@juniper.net.

2

CHAPTER

UTM Web Filtering

Allow or Block Websites by Using J-Web Integrated UTM Web Filtering | 13

Allow or Block Websites by Using J-Web Integrated UTM Web Filtering

SUMMARY

Learn about Web filtering and how to filter URLs on UTM-enabled SRX Series devices by using J-Web. Web filtering helps you to allow or block access to the Web and to monitor your network traffic.

IN THIS SECTION

- [Benefits of UTM Web Filtering | 13](#)
- [Why URL Filtering | 14](#)
- [Web Filtering Workflow | 14](#)
- [Step 1: List URLs That You Want to Allow or Block | 16](#)
- [Step 2: Categorize the URLs That You Want to Allow or Block | 18](#)
- [Step 3: Add a Web Filtering Profile | 20](#)
- [Step 4: Reference a Web Filtering Profile in a UTM Policy | 23](#)
- [Step 5: Assign a UTM Policy to a Security Policy | 24](#)
- [Step 6: Verify That the URLs Are Allowed or Blocked from the Server | 27](#)
- [What's Next | 27](#)
- [Sample Configuration Output | 28](#)

Benefits of UTM Web Filtering

- Local Web filtering:
 - Doesn't require a license.
 - Enables you to define your own lists of allowed sites (allowlist) or blocked sites (blocklist) for which you want to enforce a policy.

- Enhanced Web filtering:
 - Is the most powerful integrated filtering method and includes a granular list of URL categories, support for Google Safe Search, and a reputation engine.
 - Doesn't require additional server components.
 - Provides real-time threat score for each URL.
 - Enables you to redirect users from a blocked URL to a user-defined URL rather than blocking user access to the blocked URL.
- Redirect Web filtering:
 - Tracks all queries locally, so you don't need an Internet connection.
 - Uses the logging and reporting features of a standalone Websense solution.

Why URL Filtering

Today, most of us spend a considerable time on the Web. We surf our favorite sites, follow interesting links sent to us through e-mail, and use a variety of Web-based applications on our office network. This increased use of the network helps us both personally and professionally. However, it also exposes our organization to a variety of security and business risks, such as potential data loss, lack of compliance, and threats such as malware, virus, and so on. In this environment of increased risk, it is wise for businesses to implement Web or URL filters to control the network behaviors. To control network threats, you can use a Web or URL filter to categorize websites on the Internet and to either allow or block user access.

Here's an example of a typical situation where a user of your office network is blocked access to a website:

On the Web browser, the user types **www.gameplay.com**, a popular gaming site. The user receives a message such as **Access Denied** or **The Website is blocked**. Display of such a message means that your organization has inserted a filter for the gaming websites, and you can't access the site from your workplace.

Web Filtering Workflow

Scope

Juniper Web (J-Web) Device Manager supports UTM Web filtering on SRX Series devices.

In J-Web, a Web filtering profile defines a set of permissions and actions based on Web connections predefined by website categories. You can also create custom URL categories and URL pattern lists for a Web filtering profile.

NOTE: You cannot inspect URLs within e-mails using J-Web UTM Web filtering.

In this example, you'll:

1. Create your own custom URL pattern lists and URL categories.
2. Create a Web filtering profile using the Local engine type. Here, you define your own URL categories, which can be allowed sites (allowlist) or blocked sites (blocklist) that are evaluated on the SRX Series device. All URLs added for blocked sites are denied, while all URLs added for allowed sites are permitted.
3. Block inappropriate gaming websites and allow suitable websites (for example, www.juniper.net).
4. Define a custom message to display when users attempt to access the gaming websites.
5. Apply the Web filtering profile to a UTM policy.
6. Assign the UTM policy to a security policy rule.

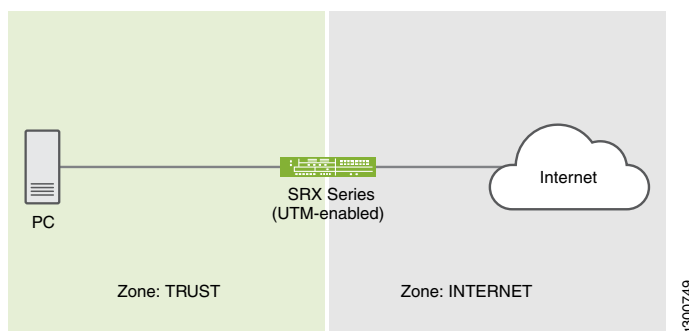
NOTE: Web filtering and URL filtering have the same meaning. We'll use the term *Web filtering* throughout our example.

Before You Begin

- You do not need a license to configure the Web filtering profile if you use the Local engine type. This is because you will be responsible for defining your own URL pattern lists and URL categories.
- You need a valid license (**wf_key_websense_ewf**) if you want to try the Juniper Enhanced engine type for the Web filtering profile.
- Ensure that the SRX Series device you use in this example runs Junos OS Release 19.4R1.

Topology

In this topology, we have a PC connected to a UTM-enabled SRX Series device that has access to the Internet. Let's use J-Web to filter the HTTP requests sent to the Internet with this simple setup.



Sneak Peek – J-Web UTM Web Filtering Steps



Step 1: List URLs That You Want to Allow or Block

In this step, we define custom objects (URLs and patterns) to handle the URLs that you want to allow or block.

You are here (in the J-Web UI): **Configure > Security Services > UTM > Custom Objects**

To list URLs:

1. Click the URL Pattern List tab.
2. Click the add icon (+) to add a URL pattern list.

The Add URL Pattern List page appears. See [Figure 1 on page 17](#).

3. Complete the tasks listed in the Action column in the following table:


| Field | Action |
|-------|--|
| Name | <p>Enter allowed-sites or blocked-sites.</p> <p>NOTE: Use a string beginning with a letter or underscore and consisting of alphanumeric characters and special characters such as dashes and underscores. The maximum length is 29 characters.</p> |
| Value | <p>a. Click + to add a URL pattern value.</p> <p>b. Enter the following:</p> <ul style="list-style-type: none"> For allowed-sites—www.juniper.net and www.google.com For blocked-sites—www.gamestu.com and www.gameplay.com <p>c. Click the tick icon .</p> |

Figure 1: Add URL Pattern List

Add URL Pattern List ?

Name* ? blocked-sites

Values* ?

+ -

Value List

www.gamestu.com

www.gameplay.com

2 items

Cancel OK

Add URL Pattern List ?

Name* ? allowed-sites

Values* ?

+ -

Value List

www.juniper.net

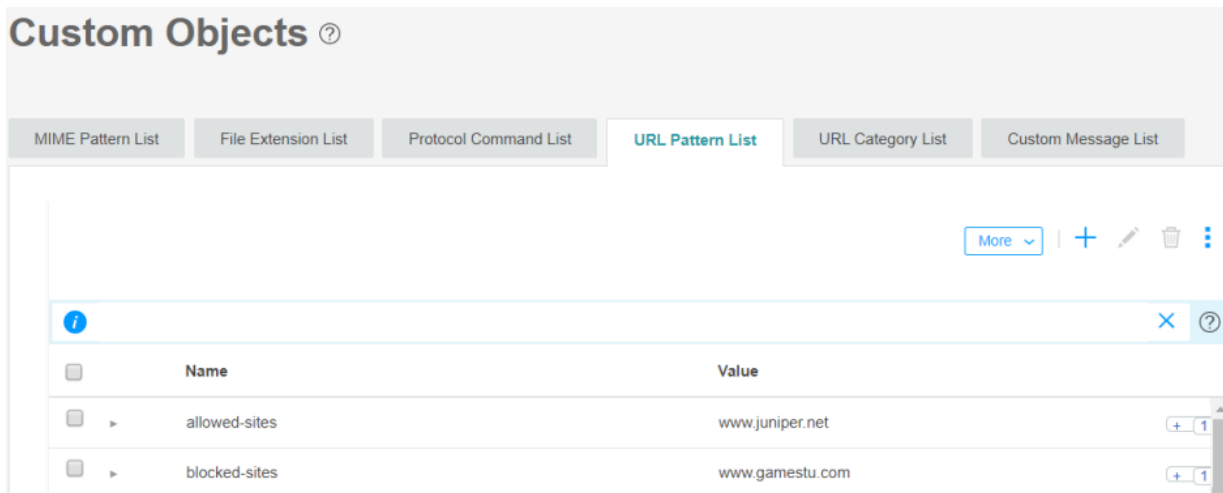
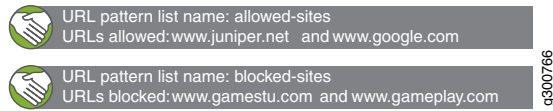
www.google.com

2 items

Cancel OK

4. Click **OK** to save the changes.

Good job! Here's the result of your configuration:



Step 2: Categorize the URLs That You Want to Allow or Block

We'll now assign the created URL patterns to URL category lists. The category list defines the action of mapping. For example, the *Gambling* category should be blocked.

You are here: **Configure > Security Services > UTM > Custom Objects**

To categorize URLs:

1. Click the URL Category List tab.
2. Click the add icon (+) to add a URL category list.

The Add URL Category List page appears. See [Figure 2 on page 19](#).

3. Complete the tasks listed in the Action column in the following table:

| Field | Action |
|--------------|---|
| Name | <p>Enter the URL category list name as good-sites for the allowed-sites URL pattern or stop-sites for the blocked-sites URL pattern.</p> <p>NOTE: Use a string beginning with a letter or underscore and consisting of alphanumeric characters and special characters such as dashes and underscores. The maximum length is 59 characters.</p> |
| URL Patterns | <p>a. Select the URL pattern values allowed-sites or blocked-sites from the Available column to associate the URL pattern values with the URL categories good-sites or stop-sites, respectively.</p> <p>b. Click the right arrow to move the URL pattern values to the Selected column.</p> |

Figure 2: Add URL Category List

Add URL Category List ?

Name* ?

URL Patterns* ?

1 Available

| <input type="checkbox"/> | Name |
|--------------------------|---------------|
| <input type="checkbox"/> | blocked-sites |

→

←

1 Selected


| <input type="checkbox"/> | Name |
|--------------------------|---------------|
| <input type="checkbox"/> | allowed-sites |


[Create New URL Pattern](#)

[Cancel](#) [Ok](#)

4. Click **OK** to save the changes.

Good job! Here's the result of your configuration:

URL category name:good-sites
URL category values:allowed-sites

URL category name:stop-sites
URL category values:blocked-sites

9300751

Custom Objects ?

MIME Pattern ListFile Extension ListProtocol Command ListURL Pattern ListURL Category ListCustom Message List

More | + | | |

| Name | Value |
|------------|---------------|
| good-sites | allowed-sites |
| stop-sites | blocked-sites |

Step 3: Add a Web Filtering Profile

Now, let's refer the created URL objects (patterns and categories) to a UTM Web filtering profile. This mapping helps you set different values for your filtering behavior.

You are here: **Configure > Security Services > UTM > Web Filtering**

To create a Web filtering profile:

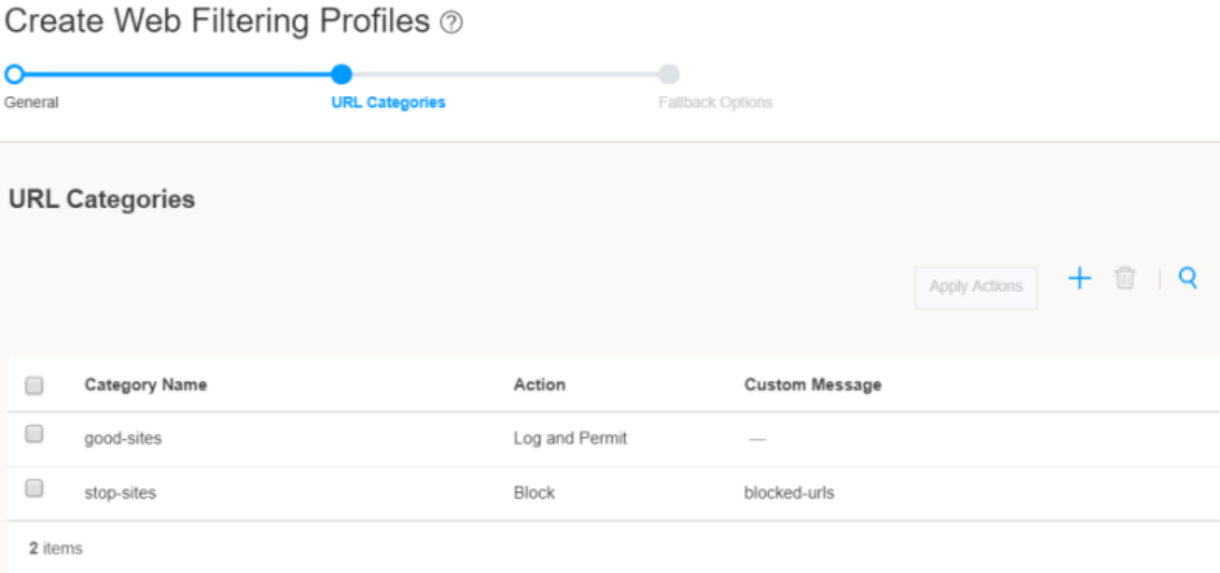
1. Click the add icon (+) to add a Web filtering profile.
The Create Web Filtering Profiles page appears. See [Figure 3 on page 22](#).

2. Complete the tasks listed in the Action column in the following table:

| Field | Action |
|---------|--------|
| General | |

| Field | Action |
|--|--|
| Name | <p>Enter wf-local for the Web filtering profile.</p> <p>NOTE: The maximum length is 29 characters.</p> |
| Timeout | <p>Enter 30 (in seconds) to wait for a response from the Local engine.</p> <p>The maximum value is 1800 seconds. The default value is 15 seconds.</p> |
| Engine type | <p>Select the Local engine type for Web filtering.</p> <p>NOTE: The default value is Juniper Enhanced.</p> |
| URL Categories | |
| + | Click the add icon to select the URL categories. |
| Select URL categories to apply to the list | Select good-sites or stop-sites . |
| Action | <p>Select Log and Permit for the good-sites category from the list.</p> <p>Select Block for the stop-sites category from the list.</p> |
| Custom Message | <p>Click Create New to add a new custom message for the stop-sites.</p> <ul style="list-style-type: none"> • Name—Enter blocked-urls. • Type—Select User Message. • Content—Enter URL request is denied. Contact your IT department for help. |

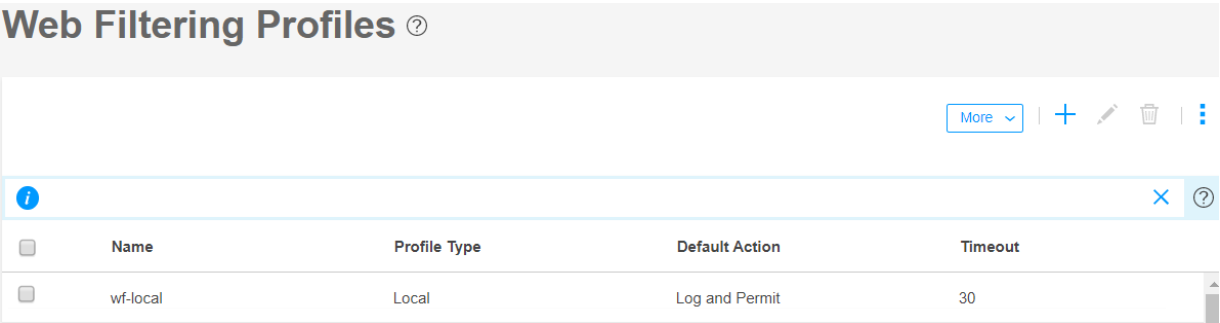
Figure 3: Create Web Filtering Profile



- Click **Finish**. Review the summary of the configuration and click **OK** to save changes.
Good job! Here's the result of your configuration:

Web filtering profile name: wf-local
 Custom message name: blocked-urls
 Custom message type: User Message
 Custom message content: URL request is denied. Contact your IT department for help.

g300752



- Click **Close** after you see a successful-configuration message.

Step 4: Reference a Web Filtering Profile in a UTM Policy

We now need to assign the Web filtering profile (wf-local) to a UTM policy that acts as an action to be applied.

You are here: **Configure** > **Security Services** > **UTM** > **Policy**

To create a UTM policy:

1. Click the add icon (+) to add a UTM policy.


The Create UTM Policies page appears.

2. Complete the tasks listed in the Action column in the following table:

| Field | Action |
|---|---|
| General – General Information | |
| Name | Enter wf-custom-policy for the UTM policy and click Next . NOTE: The maximum length is 29 characters. |
| Web Filtering - Web Filtering Profiles by Traffic Protocol | |
| HTTP | Select wf-local from the list and click Next . |

3. Click **Finish**. Review the summary of the configuration and click **OK** to save changes.

Almost there! Here's the result of your configuration:

 UTM policy name: wf-custom-policy

g300753

UTM Policies ?

More ▾

+

i

×

?

| <input type="checkbox"/> | Name | Antivirus | Web Filtering | Antispam | Content Filtering |
|--------------------------|------------------|-----------|---------------|----------|-------------------|
| <input type="checkbox"/> | wf-custom-policy | — | wf-local | — | — |

4. Click **Close** after you see a successful message.
- Good news! You're done with UTM Web filtering configurations.

Step 5: Assign a UTM Policy to a Security Policy

You haven't yet assigned the UTM configurations to the security policy from the TRUST zone to the INTERNET zone. Filtering actions are taken only after you assign the UTM policy to security policy rules that act as the match criteria.

NOTE: When the security policy rules are permitted, the SRX Series device:

1. Intercepts an HTTP connection and extracts each URL (in the HTTP request) or IP address.

NOTE: For an HTTPS connection, Web filtering is supported through SSL forward proxy.

2. Searches for URLs in the user-configured blocklist or allowlist under Web Filtering (Configure > Security Services > UTM > Default Configuration). Then, if the URL is in the:
 - a. User-configured blocklist, the device blocks the URL.
 - b. User-configured allowlist, the device permits the URL.
3. Checks the user-defined categories and blocks or allows the URL based on the user-specified action for the category.
4. Allows or blocks the URL (if a category is not configured) based on the default action configured in the Web filtering profile.

You are here: **Configure > Security Services > Security Policy > Rules**

To create security policy rules for the UTM policy:

1. Click the add icon (+).

The Create Rule page appears.

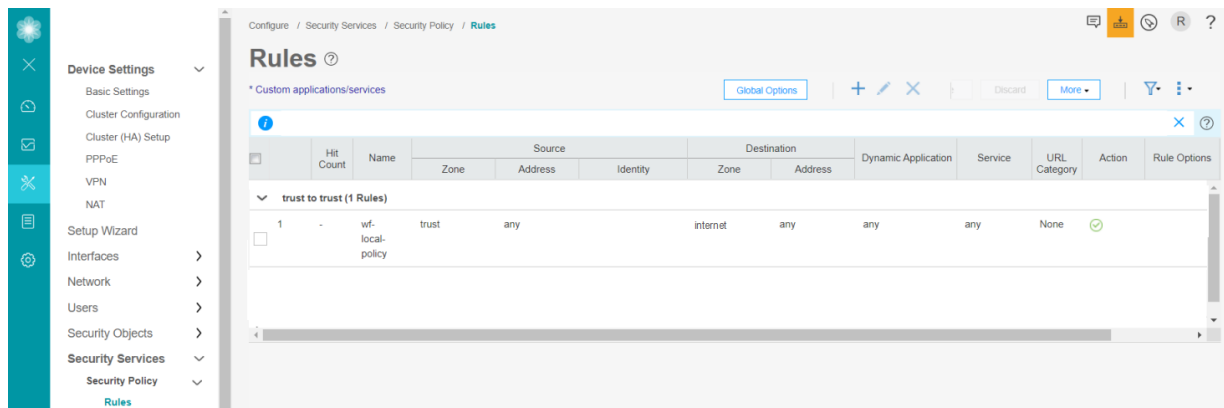
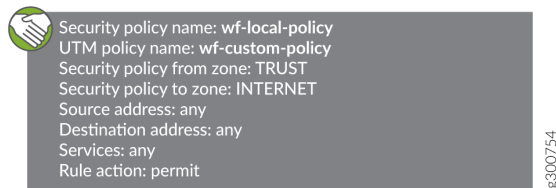
2. Complete the tasks listed in the Action column in the following table:

| Field | Action |
|--------------------------------------|--|
| General – General Information | |
| Rule Name | Enter wf-local-policy for the security policy allowing the good-sites category and denying the stop-sites category. |
| Rule Description | Enter a description for the security policy rule and click Next . |
| Source | |
| Zone | Select TRUST from the list. |
| Address(es) | Leave this field with the default value any . |

| Field | Action |
|--------------------------|--|
| Destination | |
| Zone | Select INTERNET from the list. |
| Address(es) | Leave this field with the default value any . |
| Service(s) | Leave this field with the default value any . |
| Advanced Security | |
| Rule Action | Select Permit from the list. |
| UTM | Select wf-custom-policy from the UTM list. |

3. Click **Finish**. Review the summary of the configuration and click **OK** to save changes.

Good job! Here's the result of your configuration:



4. Click the commit icon (at the right side of the top banner) and select **Commit**.

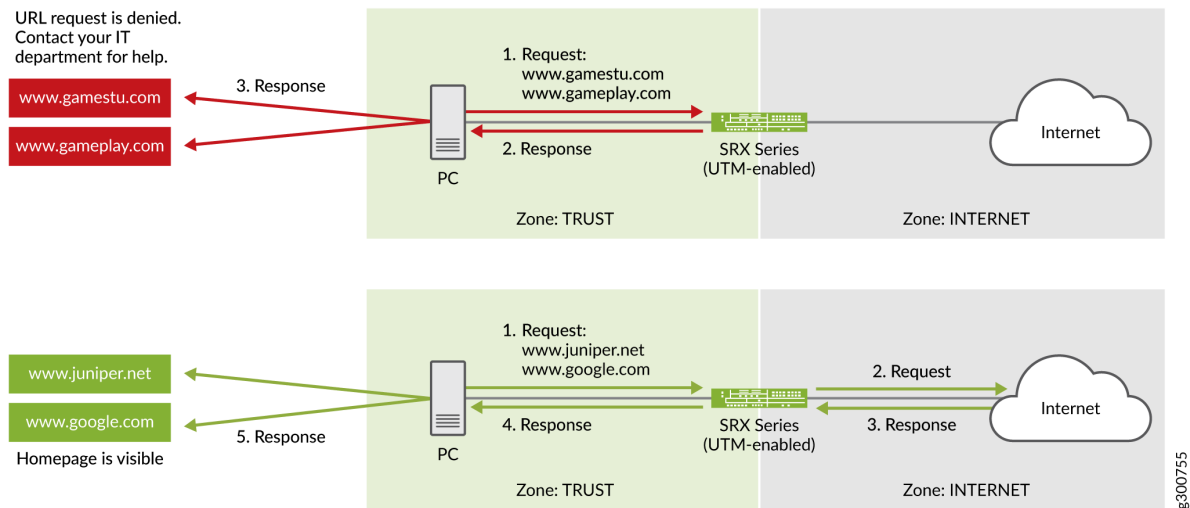
The successful-commit message appears.

Congratulations! We're ready to filter the URL requests.

Step 6: Verify That the URLs Are Allowed or Blocked from the Server

Let's verify that our configurations and security policy work fine with the defined URLs in the topology:

- If you enter www.gamestu.com and www.gameplay.com, the SRX Series device should block the URLs and send the configured block message.
- If you enter www.juniper.net and www.google.com, the SRX Series device should allow the URLs with their homepage displayed.



What's Next

| What to do? | Where? |
|--|--|
| Monitor UTM Web filtering information and statistics. | In J-Web, go to Monitor > Security Services > UTM Web Filtering . |
| Generate and view reports on URLs allowed and blocked. | In J-Web, go to Reports . Generate reports for Threat Assessment Reports and Top Blocked Applications via Webfilter logs. |
| Learn more about UTM features. | Unified Threat Management User Guide |

Sample Configuration Output

In this section, we present samples of configurations that allow and block the websites defined in this example.

You configure the following UTM configurations at the **[edit security utm]** hierarchy level.

Creating custom objects:

```
custom-objects {
  url-pattern {
    blocked-sites {
      value [ http://*.gamestu.com http://*.gameplay.com];
    }
    allowed-sites {
      value [ http://*.juniper.net http://*.google.com];
    }
  }
  custom-url-category {
    stop-sites {
      value blocked-sites;
    }
    good-sites {
      value allowed-sites;
    }
  }
  custom-message {
    blocked-urls {
      type message;
      content "URL request is denied. Contact your IT department for help.";
    }
  }
}
```

Creating the Web filtering profile:

```
default-configuration {
  web-filtering {
    type juniper-local;
  }
}
```

```
feature-profile {
```

```

web-filtering {
  juniper-local {
    profile wf-local {
      category {
        stop-sites {
          action block;
          custom-message blocked-urls;
        }
        good-sites {
          action log-and-permit;
        }
      }
      timeout 30;
    }
  }
}

```

Creating the UTM policy:

```

utm-policy wf-custom-policy {
  web-filtering {
    http-profile wf-local;
  }
}

```

You configure the security policy rules at the **[edit security policies]** hierarchy level.

Creating rules for a security policy:

```

from-zone trust to-zone internet {
  policy wf-local-policy {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          utm-policy wf-custom-policy;
        }
      }
    }
  }
}

```

```
}  
}
```

3

CHAPTER

UTM Antivirus

Prevent Virus Attacks by Using J-Web UTM Antivirus | 32

Prevent Virus Attacks by Using J-Web UTM Antivirus

SUMMARY

Learn about Unified Threat Management (UTM) antivirus protection and how to configure UTM antivirus to prevent virus attacks on SRX Series devices by using J-Web. The UTM antivirus feature on the SRX Series device scans network traffic to protect your network from virus attacks and to prevent virus spread.

IN THIS SECTION

- [UTM Antivirus Overview | 32](#)
- [Benefits of UTM Antivirus | 33](#)
- [Antivirus Workflow | 34](#)
- [Step 1: Configure Antivirus Custom Object | 35](#)
- [Step 2: Configure Antivirus Feature Profile | 40](#)
- [Step 3: Apply the Antivirus Feature Profile to a UTM Policy | 44](#)
- [Step 4: Assign the UTM Policy to a Security Firewall Policy | 45](#)
- [Verify That UTM Antivirus Is Working | 48](#)
- [What's Next? | 49](#)
- [Sample Configuration Output | 50](#)

UTM Antivirus Overview

In today's world, where cyber security threats are evolving and getting more sophisticated, protecting your network from virus attacks is extremely critical. The viruses, worms, and malware perform unwanted and malicious acts, such as damaging or deleting files, hacking personal data, affecting system performance, reformatting the hard disk, or using your computer to transmit viruses to other computers. The UTM antivirus software acts like a first line of defense against such security threats and prevents the spread of viruses into your network. It protects your network from virus attacks, unwanted computer malwares, spywares, rootkits, worms, phishing attacks, spam attacks, trojan horses, and so on.

NOTE: You must always ensure that the antivirus software and virus pattern database are up to date.

Juniper Networks offers the following UTM antivirus solutions:

- On-device antivirus protection

The on-device antivirus is an on-box solution. The on-device antivirus scan engine scans the data by accessing the virus pattern database that is locally stored on the device. It provides a full file-based antivirus scanning function that is available through a separately licensed subscription service.

NOTE:

- The on-device Express or Kaspersky scan engine is not supported from Junos OS Release 15.1X49-D10 onwards; however, it is still applicable for Junos OS Release 12.3X48.
- Starting in Junos OS Release 18.4R1, SRX Series devices support the Avira on-device antivirus scanning engine.
- Avira on-device antivirus scanning engine is not supported on SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550 HM devices.

- Sophos antivirus protection

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. The Sophos antivirus scanner also uses a local internal cache to maintain query responses from the external list server. We offer the Sophos antivirus scanning as a less CPU-intensive alternative to the full file-based antivirus feature.

Benefits of UTM Antivirus

- The on-device antivirus solution:

- Scans the application traffic locally without connecting to the Internet server to query whether the application traffic has virus.
- Minimizes processing delays because the pattern database is locally stored and the scan engine is on-device.

- The Sophos antivirus solution:

- Avoids downloading and maintaining large pattern databases on the Juniper device because the virus pattern and malware database is located on external servers maintained by Sophos.
- Improves lookup performance because the Sophos antivirus scanner uses a local internal cache to maintain query responses from the external list server.
- Effectively prevents malicious content from reaching the endpoint client or server through the use of the Uniform Resource Identifier (URI) checking functionality.

Antivirus Workflow

Scope

Juniper Web (J-Web) Device Manager supports the UTM antivirus solution on SRX Series devices. In this example, you'll use Sophos antivirus protection to do the following:

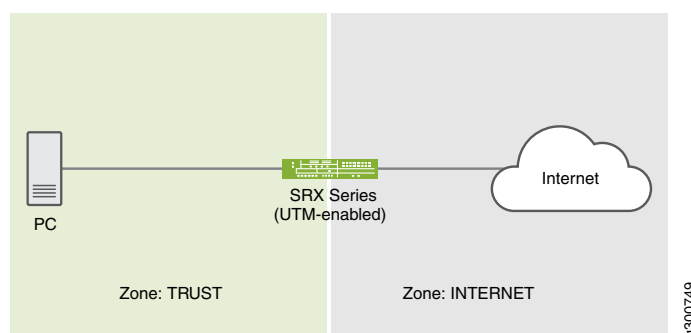
1. Scan HTTP traffic from an Internet server to your computer for virus attacks.
2. Define a custom message **Virus Found!** to be displayed when a virus is found while scanning the traffic.
3. Allow traffic from a specific server (for example, 203.0.113.1).

Before You Begin

- Install a Sophos antivirus license. See the [Installation and Upgrade Guide](#) and [Licensing Guide](#).
- Ensure that the SRX Series device you use in this example runs Junos OS Release 19.4R1.

Topology

The topology used in this example comprises a PC connected to a UTM-enabled SRX Series device that has access to the Internet. You'll use J-Web to scan the HTTP requests sent to the Internet with this simple setup. You'll then use Sophos antivirus protection to prevent virus attacks from the Internet to your PC.



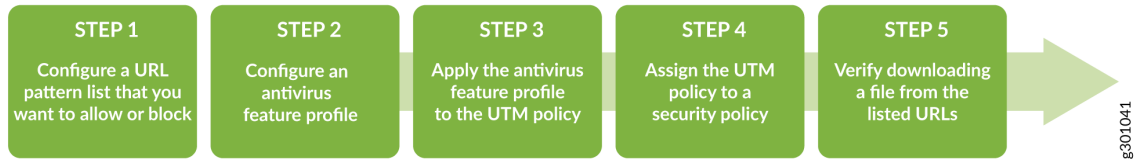
Video

See the following video to learn how to configure UTM antivirus using J-Web.



Video: [Configure UTM Antivirus Using J-Web](#)

Sneak Peek – J-Web UTM Antivirus Configuration Steps



| Step | Action |
|--------|--|
| Step 1 | <p>Configure antivirus custom object.</p> <p>Here, you define the URL pattern list (safelist) of URLs or addresses that will be bypassed by antivirus scanning. After you create the URL pattern list, you will create a custom URL category list and add the pattern list to it.</p> |
| Step 2 | <p>Configure an antivirus feature profile using the Sophos engine.</p> <p>Here, you first define the default engine as Sophos. After the default configuration, you define the parameters that will be used for virus scanning in the feature profile.</p> <p>NOTE: You must configure DNS servers before creating the antivirus profiles.</p> |
| Step 3 | <p>Create a UTM policy for Sophos antivirus and apply the antivirus feature profile to the UTM policy.</p> <p>Here, you use a UTM policy to bind a set of protocols (for example, HTTP) to the Sophos UTM feature profile. 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.</p> |
| Step 4 | <p>Create a security policy for Sophos antivirus and assign the UTM policy to the security policy.</p> <p>Here, you use the security firewall and feature profile settings to scan the traffic from the untrust zone (INTERNET) to the trust zone (TRUST).</p> |
| Step 5 | <p>Try to download an HTTP file from the safelisted URL and from the Internet.</p> |

Step 1: Configure Antivirus Custom Object

IN THIS SECTION

- [Step 1a: Configure a URL Pattern List That You Want to Bypass | 36](#)
- [Step 1b: Categorize the URLs That You Want to Allow | 38](#)

Step 1a: Configure a URL Pattern List That You Want to Bypass

In this step, you define a URL pattern list (safelist) of URLs or addresses that will be bypassed by antivirus scanning.

You are here (in the J-Web UI): **Configure > Security Services > UTM > Custom Objects**

To configure the safelist of URLs:

- 1. Click the **URL Pattern List** tab.
- 2. Click the add icon (+) to add a URL pattern list.

The Add URL Pattern List page appears. See [Figure 4 on page 37](#).

- 3. Complete the tasks listed in the Action column in [Table 3 on page 36](#).

Table 3: URL Pattern List Settings


| Field | Action |
|-------|--|
| Name | Type LB-Pattern . NOTE: Use a string beginning with a letter or underscore and consisting of alphanumeric characters and special characters such as dashes and underscores. You can use a maximum of 29 characters. |
| Value | a. Click + to add a URL pattern value. b. Type http://203.0.113.1 . c. Click the tick icon  . |

Figure 4: Add URL Pattern List

Add URL Pattern List ?

Name* ?

Values* ?

1 selected +

☒ Value List ✓ ✕

☒

1 items

Cancel Ok

4. Click **OK** to save the URL pattern list configuration.

Good job! Here's the result of your configuration:



Custom Objects ?

MIME Pattern List

File Extension List

Protocol Command List

URL Pattern List

URL Category List

Custom Message List

More ▾

i

| <div><input type="checkbox"/></div> | Name | Value |
|-------------------------------------|------------|--------------------|
| <div><input type="checkbox"/></div> | LB-Pattern | http://203.0.113.1 |

1 items

Step 1b: Categorize the URLs That You Want to Allow

You'll now assign the created URL pattern to a URL category list. The category list defines the action of mapping. For example, the *Safelist* category should be permitted.

You are here: **Configure > Security > UTM > Custom Objects**

To categorize URLs:

1. Click the **URL Category List** tab.
2. Click the add icon (+) to add a URL category list.

The Add URL Category List page appears. See [Figure 5 on page 39](#).

3. Complete the tasks listed in the Action column in [Table 4 on page 38](#).

Table 4: URL Category List Settings

| Field | Action |
|--------------|---|
| Name | Type LB-AV as the URL category list name for the safelisted URL pattern. NOTE: Use a string beginning with a letter or underscore and consisting of alphanumeric characters and special characters such as dashes and underscores. You can use a maximum of 59 characters. |
| URL Patterns | Select the URL pattern value LB-Pattern from the Available column and click the right arrow to move the URL pattern values to the Selected column. By doing this, you associate the URL pattern value LB-Pattern with the URL category list LB-AV. |

Figure 5: Add URL Category List

Add URL Category List ?

Name* ?

URL Patterns* ?

0 Available

☐ Name

No available items

Create New URL Pattern

1 Selected

☐ Name
☐ LB-Pattern

Cancel **Ok**

- Click **OK** to save the category list configuration.

Good job! Here's the result of your configuration:

 URL category name: LB-AV
 URL pattern list name: LB-Pattern

Custom Objects ?

MIME Pattern List | File Extension List | Protocol Command List | URL Pattern List | **URL Category List** | Custom Message List

More | + | ✎ | 🗑

| Name | Value |
|-------|------------|
| LB-AV | LB-Pattern |

1 items

Step 2: Configure Antivirus Feature Profile

IN THIS SECTION

- [Step 2a: Update Default Configuration for Antivirus | 40](#)
- [Step 2b: Create Antivirus Feature Profile | 41](#)

You now need to refer the created URL objects (patterns and categories) to a UTM antivirus profile. This mapping helps you set different values for the filtering behavior of your device.

Step 2a: Update Default Configuration for Antivirus

You are here: **Configure** > **Security Services** > **UTM**

In this step, you'll set up **Sophos Engine** as the default engine type.

To update the default antivirus profile:

1. Click **Default Configuration**.
The Default Configuration page appears.
2. On the **Anti-Virus** tab, click the edit icon (pencil) to edit the default configuration.
The Anti Virus page appears. See [Figure 6 on page 41](#).
3. Complete the tasks listed in the Action column in [Table 5 on page 40](#).

Table 5: Default Configuration Settings

| Field | Action |
|-----------------------|---|
| Type | Select the Sophos Engine type for the antivirus. |
| URL Whitelist | Select None . |
| MIME Whitelist | |
| List | Select None . |
| Exception | Select None . |

Figure 6: Default Antivirus Configuration

Anti Virus ⓘ

Type ⓘ Sophos Engine ▼

URL Whitelist ⓘ None ▼

MIME Whitelist
Anti-virus MIME whitelist

List ⓘ None ▼

Exception ⓘ None ▼

mime-pattern can be defined under, 'Configure / Security / UTM / Custom Objects / MIME Pattern List'

4. Click **OK** to save the new default configuration.

Step 2b: Create Antivirus Feature Profile

You are here: **Configure** > **Security Services** > **UTM**

In this step, you'll create a new UTM antivirus profile, refer the created URL objects (patterns and categories) to the profile, and specify the notification details.

To create the new antivirus profile:

1. Select **Configure** > **Security Services** > **UTM** > **Antivirus Profiles**.

The Antivirus Profiles page appears.

2. Click the add icon (+) to add a new antivirus profile.

The Create Antivirus Profiles page appears. See [Figure 7 on page 42](#).

3. Complete the tasks listed in the Action column in [Table 6 on page 41](#).

Table 6: Antivirus Profile Settings

| Field | Action |
|----------------|--------|
| General | |

Table 6: Antivirus Profile Settings (continued)

| Field | Action |
|-----------------------------|--|
| Name | Type UTM-LB-AV for the new antivirus profile. NOTE: You can use a maximum of 29 characters. |
| URL Whitelist | Select LB-AV from the drop-down list. |
| Fallback Options | |
| Content Size | Select Log and Permit . |
| Notification Options | |
| Virus Detection | Select Notify Mail Sender . |
| Notification Type | Select Message . |
| Custom Message Subject | Type ***Antivirus Alert*** . |
| Custom Message | Type Virus Found ! . |

Figure 7: Create Antivirus Profile General Settings

Create Antivirus Profiles ?

General
Fallback Options
Notification Options

General Information

Name* ?

URL Whitelist ?

MIME Whitelist

Anti-virus MIME whitelist

MIME Whitelist ? ▼ [Create New MIME list](#)

Exception MIME Whitelist ? ▼ [Create New MIME list](#)

Figure 8: Create Antivirus Profile Notification Settings

Create Antivirus Profiles ?

General Fallback Options **Notification Options**

Notification Options

Use notification options to specify how users are notified when a fallback occurs or a virus is detected.

Fallback Deny ? ☐ Notify Mail Sender

Fallback Non-Deny ? ☐ Notify Mail Recipient

Virus Detection ? ☒ Notify Mail Sender

Notification Type Message ▼

Custom Message Subject ***Antivirus Alert***
255 characters maximum

Custom Message Virus Found !
512 characters maximum

Cancel Back Finish

- Click **Finish**. Review the summary of the configuration and click **OK** to save your configuration.
- Click **Close** after you see a successful-configuration message.

Good job! Here's the result of your configuration:



Antivirus profile name: UTM-LB-AV
 Custom notification type: Message
 Custom message subject: ***Antivirus Alert***
 Custom message: Virus Found !

8301044

Antivirus Profiles

| <div>More </div> | | | |
|--------------------------|--------------------------|---------------|----------------|
| <div> </div> | | | |
| <input type="checkbox"/> | Name | URL Whitelist | Default Action |
| <input type="checkbox"/> | junos-av-defaults | — | — |
| <input type="checkbox"/> | junos-sophos-av-defaults | — | — |
| <input type="checkbox"/> | UTM-LB-AV | LB-AV | Block |
| 3 items | | | |

Step 3: Apply the Antivirus Feature Profile to a UTM Policy

After you've created the antivirus feature profile, you configure a UTM policy for an antivirus scanning protocol and attach this policy to the feature profile created in [“Step 2: Configure Antivirus Feature Profile” on page 40](#). In this example, you'll scan HTTP traffic for viruses.

You are here: **Configure** > **Security Services** > **UTM** > **Policy**

To create a UTM policy:

1. Click the add icon (+).

The Create UTM Policies page appears.


2. Complete the tasks listed in the Action column in [Table 7 on page 44](#):

Table 7: Create UTM Policies Settings

| Field | Action |
|------------------|--|
| General | |
| Name | Type UTM-LB as the name of the UTM policy and click Next . NOTE: You can use a maximum of 29 characters. |
| Antivirus | |
| HTTP | Select UTM-LB-AV from the drop-down list and click OK . |

- 3. Click **Finish**. Review the summary of the configuration and click **OK** to save the changes.
- 4. Click **Close** after you see a successful-configuration message.

Almost there! Here's the result of your configuration:

 UTM policy name: UTM-LB

UTM Policies ⓘ

More ▾

+

| | Name | Antivirus | Web Filtering | Antispam | Content Filtering |
|--|--------------------------|-----------------------------|---------------------------|----------|-------------------|
| | junos-default-utm-policy | — | — | — | — |
| | junos-av-policy | HTTP : junos-av-defaults 5 | — | — | — |
| | junos-wf-policy | — | junos-wf-enhanced-default | — | — |
| | junos-av-wf-policy | HTTP : junos-av-defaults 5 | junos-wf-enhanced-default | — | — |
| | UTM-LB | HTTP : UTM-LB-AV | | | — |

5 items

Step 4: Assign the UTM Policy to a Security Firewall Policy

In this step, you create a firewall security policy that will cause traffic passing from the untrust zone (INTERNET) to the trust zone (TRUST) to be scanned by Sophos antivirus using the feature profile settings.

You haven't yet assigned the UTM configurations to the security policy from the TRUST zone to the INTERNET zone. Filtering actions are taken only after you assign the UTM policy to security policy rules that act as the match criteria.

NOTE: When the security policy rules are permitted, the SRX Series device:

1. Intercepts an HTTP connection and extracts each URL (in the HTTP request) or IP address.

NOTE: For an HTTPS connection, antivirus is supported through SSL forward proxy.

2. Searches for URLs in the user-configured safelist under Antivirus (Configure > Security Services > UTM > Default Configuration). Then, if the URL is in the user-configured safelist, the device permits the URL.
3. Allows or blocks the URL (if a category is not configured) based on the default action configured in the antivirus profile.

You are here: **Configure > Security Services > Security Policy > Rules**

To create security policy rules for the UTM policy:

1. Click the add icon (+).

The Create Rule page appears.

2. Complete the tasks listed in the Action column in [Table 8 on page 46](#):

Table 8: Rule Settings

| Field | Action |
|--------------------|---|
| General | |
| Rule Name | Type UTM-AV-LB as the security policy rule name. This rule allows the URLs in the LB-AV category list. |
| Rule Description | Enter a description for the security policy rule and click Next . |
| Source | |
| Zone | Select TRUST from the drop-down list. |
| Address(es) | Leave this field with the default value any . |
| Destination | |
| Zone | Select INTERNET from the drop-down list. |


Table 8: Rule Settings (*continued*)

| Field | Action |
|--------------------------|--|
| Addresses | Leave this field with the default value any . |
| Service(s) | Leave this field with the default value any . |
| Advanced Security | |
| Rule Action | Select Permit from the drop-down list. |
| UTM | Select UTM-LB from the UTM drop-down list. |

NOTE: Navigate to **Configure > Security Services > Security Policy > Objects > Zones/Screens** to create Zones. Creating zones is outside the scope of this documentation.

- Click **Finish**. Review the summary of the configuration and click **OK** to save your configuration.

Good job! Here's the result of your configuration:



UTM policy name: UTM-LB
Security policy name: UTM-AV-LB
Security policy From Zone: trust
Security policy To Zone: untrust
Source address: any
Destination address: any
Services: any
Rule action: Permit

8301046

Create Rule

Summary - Review the summary of the configuration changes

| | |
|------------------------------|-------------------------------|
| General Information | Edit |
| Rule Name | UTM-AV-LB |
| Description | Security rule for UTM policy. |
| Identify Traffic Source | Edit |
| Zone | trust |
| Address | any |
| Identify Traffic Destination | Edit |
| Zone | untrust |
| Address | any |
| Services | any |
| Dynamic Applications | any |
| URL Category | None |
| Advance Security | Edit |

Cancel

BackOK

4. Click the commit icon (at the right side of the top banner) and select **Commit**.

The successful-commit message appears.

Congratulations! We're now ready to scan the traffic for virus attacks.

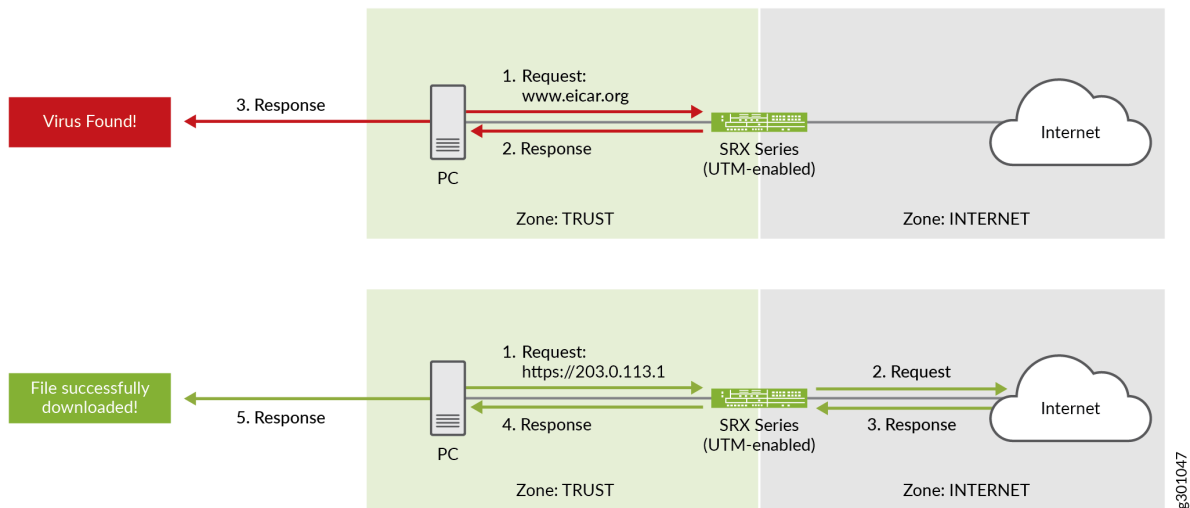
Verify That UTM Antivirus Is Working

Purpose

Verify that your configured UTM antivirus is preventing virus attacks from the Internet server and allowing traffic from the safelist server.

Action

- Open a browser, enter www.eicar.org, and try to download a file using standard HTTP protocol.
Sorry! The SRX Series device has blocked downloading the file and sent you a custom block message *****Antivirus Alert***- Virus Found!**.
- Open a browser, enter <https://203.0.113.1>, and try to download a file using standard HTTP protocol.
Good job! The file is successfully downloaded to your system.



What's Next?

| If you want to | Then |
|--|--|
| Monitor UTM antivirus details and statistics | In J-Web, go to Monitor > Security Services > UTM > Anti Virus |

| If you want to | Then |
|---|---|
| Generate and view reports on URLs allowed and blocked | <p>To generate and view reports:</p> <ol style="list-style-type: none"> 1. Log in to J-Web UI and click Reports. The Reports page appears. 2. Select any of the following predefined report name. <ul style="list-style-type: none"> • Threat Assessment Report • Viruses Blocked <p>NOTE: You can't generate more than one report at the same time.</p> 3. Click Generate Report. The Report Title page appears. 4. Enter the required information and click Save. A reported is generated. |
| Learn more about UTM features | See Unified Threat Management User Guide |

Sample Configuration Output

In this section, we present samples of configurations that block virus attacks from the websites defined in this example.

You configure the following UTM configurations at the **[edit security utm]** hierarchy level.

Creating custom objects at the **[edit security utm]** hierarchy level:

```

custom-objects {
  url-pattern {
    LB-Pattern {
      value http://203.0.113.1 ;
    }
  }
  custom-url-category {
    LB-AV {
      value LB-Pattern;
    }
  }
}

```

```

    }
  }
}

```

Creating the antivirus profile at the **[edit security utm]** hierarchy level:

```

default-configuration {
  anti-virus {
    type sophos-engine;
  }
}

```

```

feature-profile {
  anti-virus {
    profile UTM-LB-AV {
      notification-options {
        virus-detection {
          type message;
          notify-mail-sender;
          custom-message "Virus-Found!";
          custom-message-subject "****Antivirus Alert****";
        }
      }
    }
  }
}

```

Creating the UTM policy:

```

utm-policy UTM-LB {
  anti-virus {
    http-profile UTM-LB-AV;
  }
}

```

Creating rules for a security policy at the **[edit security policies]** hierarchy level.:

```

from-zone trust to-zone internet {
  policy UTM-AV-LB {
    match {
      source-address any;
      destination-address any;
    }
  }
}

```

```
    application any;
  }
  then {
    permit {
      application-services {
        utm-policy UTM-LB;
      }
    }
  }
}
```