JUNIPER NETWORKS | Engineering Simplicity

In Focus

J-Web for SRX Series Devices

IN THIS GUIDE

About This In Focus Guide

Use Cases	Use this guide to quickly learn about the most important use cases in Juniper Web Device Manager (J-Web) and how you can configure them in your network. In addition to this guide, you can find concept information and configuration details in the J-Web for SRX Series Documentation page. Want to tell us what you think about this guide? E-mail us at mailto:techpubs-comments@juniper.net.
Audience	Network operators and administrators
Knowledge Level	Familiarity with networking fundamentals and data center architectures.

Supported browsers	J-Web GUI is best viewed on the following browsers: • Google Chrome • Microsoft Internet Explorer • Mozilla Firefox

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

UTM URL Filtering Overview

Today, most of us spend an amount of 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 for our office network. This increased use of the network helps us both personally and professionally. However, it also exposes the organization to a variety of security and business risks, such as potential data loss, lack of compliance, and threats such as malware, viruses, and so on. In this

environment of increased risk, it's wise for businesses to implement Web or URL filters 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 office network has access to a website blocked:

On the Web browser, the user types **www.game.co.uk**, 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.

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.

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 simply preventing 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.

Web Filtering Workflow

IN THIS SECTION

Scope

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 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.

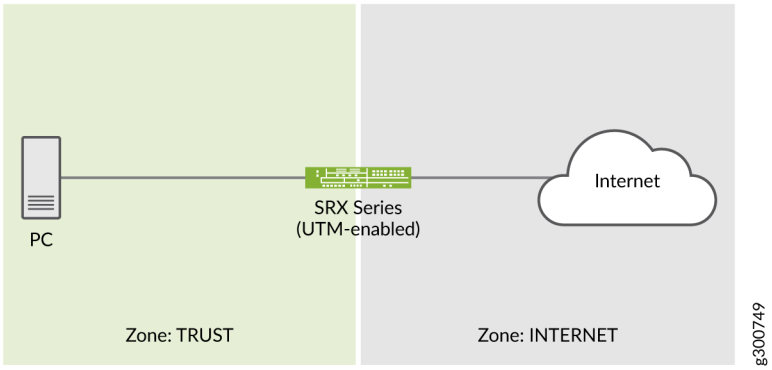
Before You Begin

- We assume that your device is set with the basic configuration. If not, see Configure Setup Wizard.
- 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. Redirect Web filtering does not need a license.

- Ensure that the SRX Series device you use in this example runs Junos OS Release 20.4R1 and later.

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/HTTPS requests sent to the Internet using 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): **Security Services** > **UTM** > **Custom Objects**.

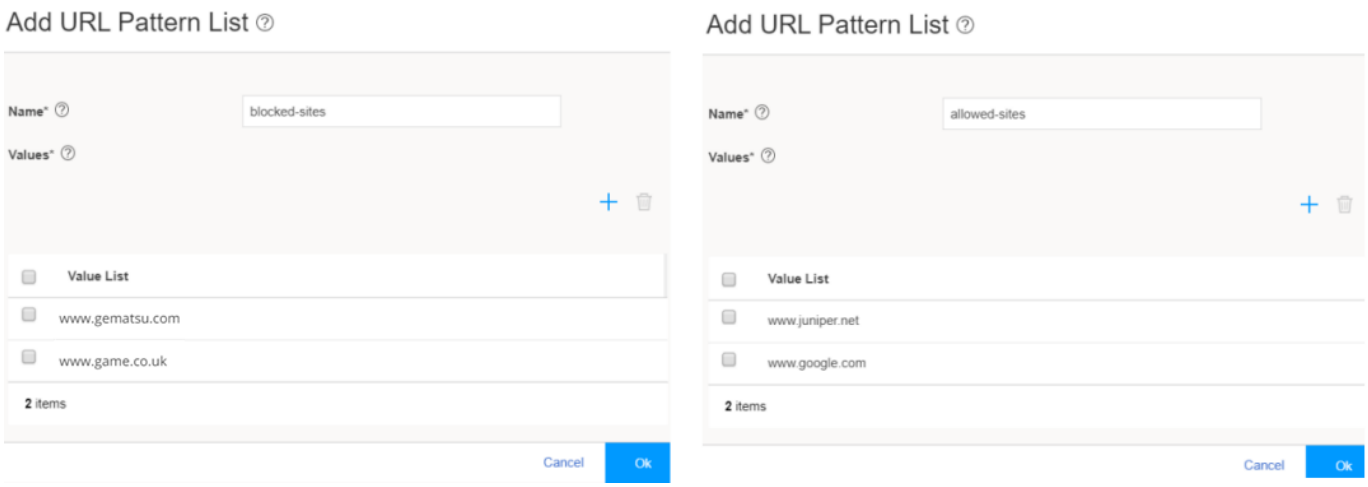
To list URLs:

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 6.
3. Complete the tasks listed in the Action column in the following table:

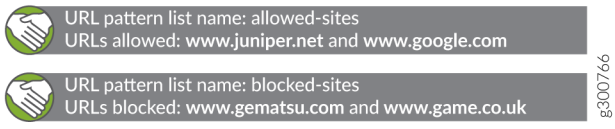
Field	Action
Name	Type **allowed-sites** or **blocked-sites**. **NOTE**: Use a string beginning with a letter or underscore and consisting of alphanumeric characters and special characters such as dashes and underscores. The maximum length is 29 characters.
Value	**a.** Click **+** to add a URL pattern value. **b.** Type the following: • For allowed-sites—**www.juniper.net** and **www.google.com** • For blocked-sites—**www.gematsu.com** and **www.game.co.uk** **c.** Click the tick icon ✓ .

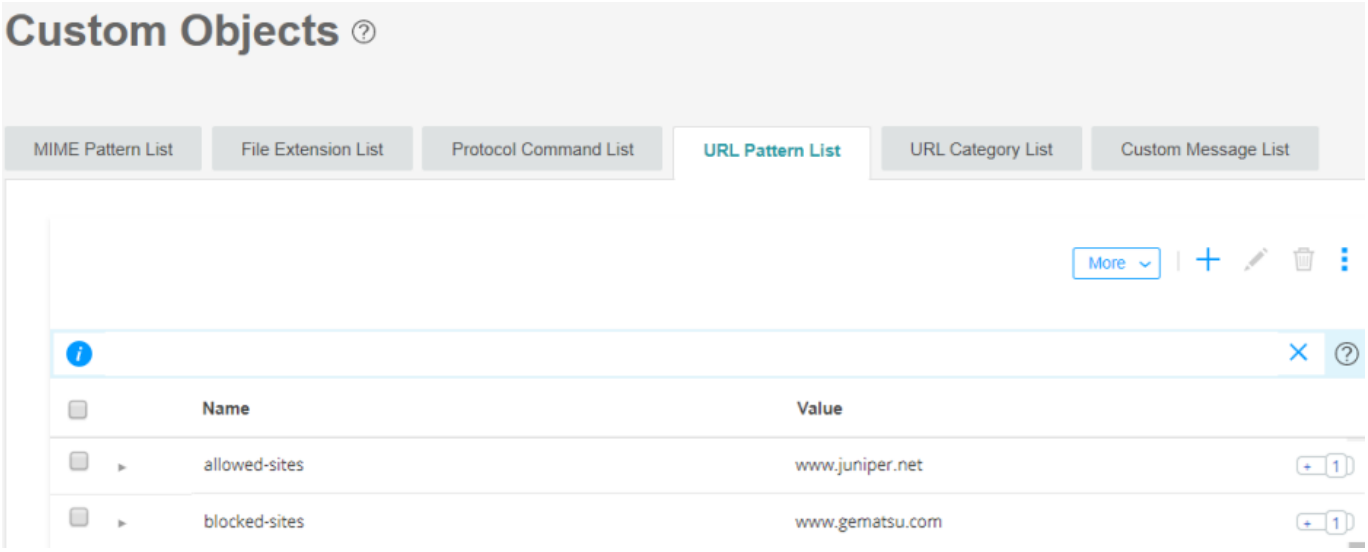
Figure 1: Add URL Pattern List



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 associated with the associated URLs. For example, the *Gambling* category should be blocked.

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

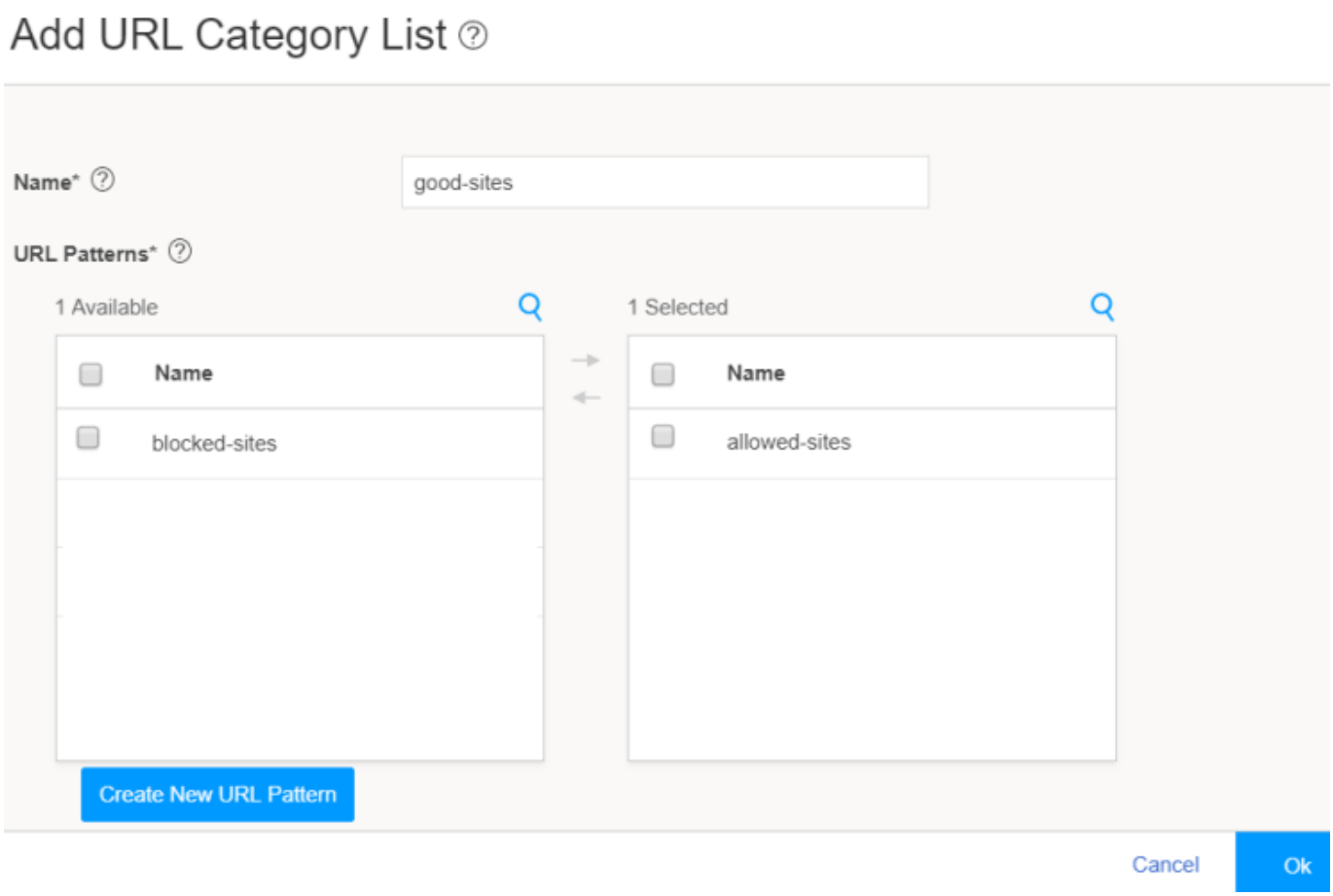
To categorize URLs:

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 8.
3. Complete the tasks listed in the Action column in the following table:

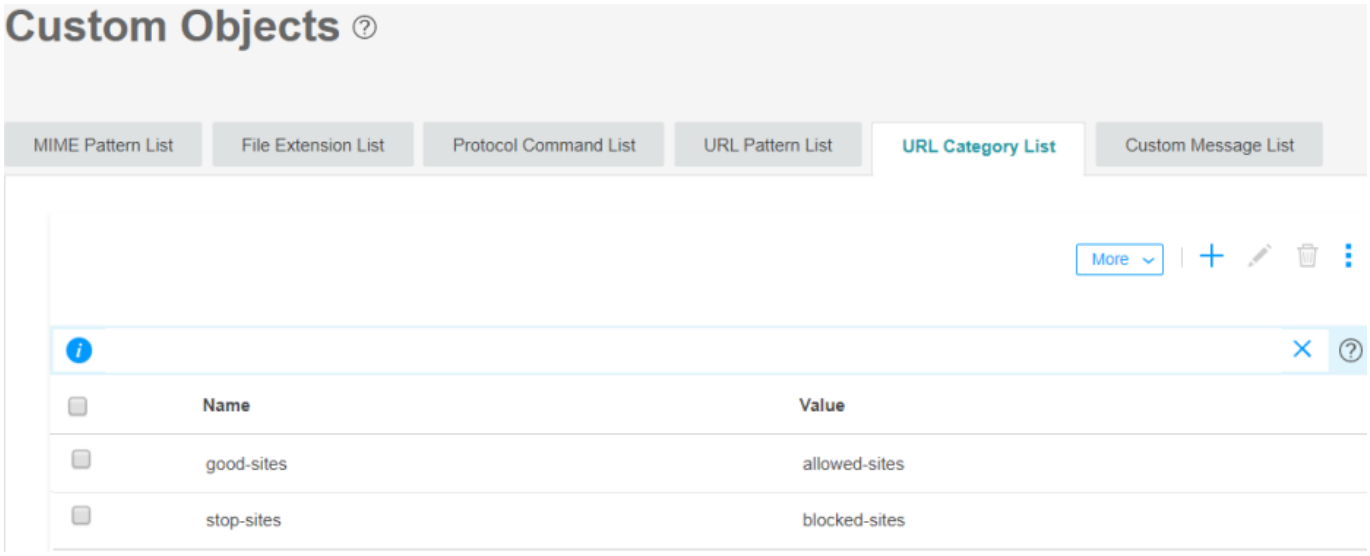
Field	Action
Name	Type the URL category list name as **good-sites** for the allowed-sites URL pattern or **stop-sites** for the blocked-sites URL pattern. **NOTE**: Use a string beginning with a letter or underscore and consisting of alphanumeric characters and special characters such as dashes and underscores. The maximum length is 59 characters.
URL Patterns	**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. **b.** Click the right arrow to move the URL pattern values to the Selected column.

Figure 2: Add URL Category List



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

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



Step 3: Add a Web Filtering Profile

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

You are here: **Security Services** > **UTM** > **Web Filtering Profiles**.

To create a Web filtering profile:

1. Click the add icon (**+**) to add a Web filtering profile.

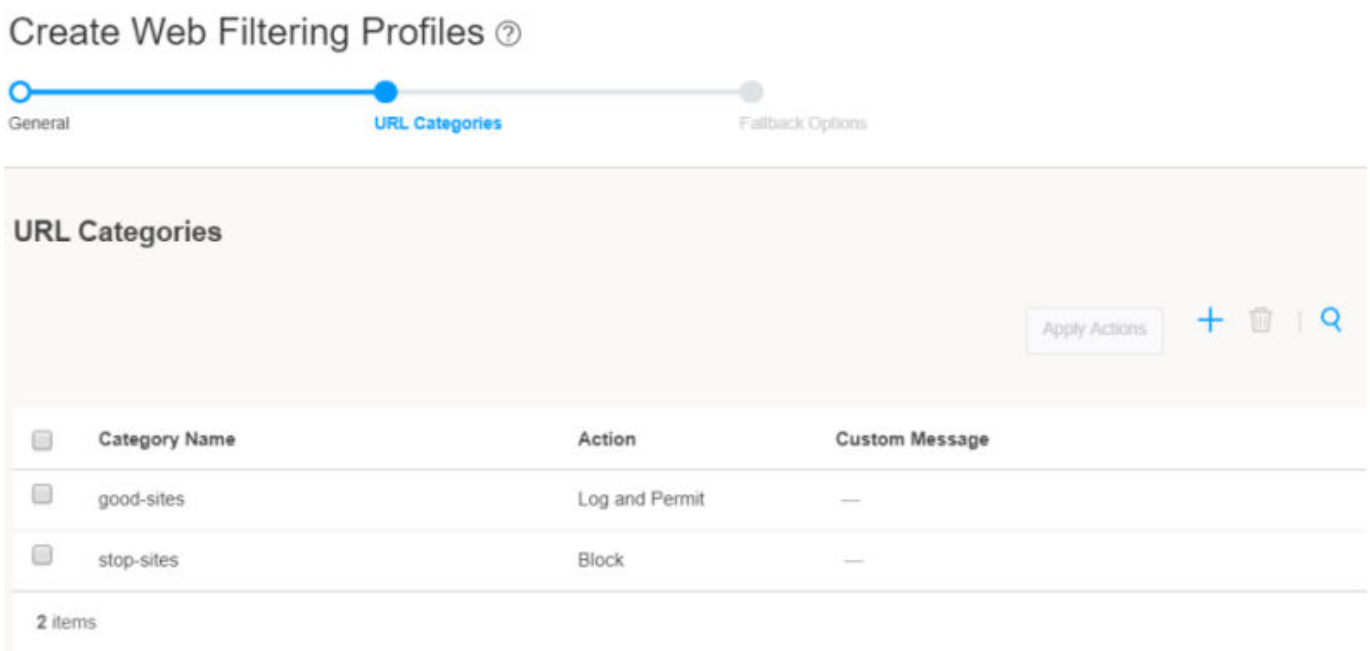
   The Create Web Filtering Profiles page appears. See Figure 3 on page 10.
2. Complete the tasks listed in the Action column in the following table:

Field	Action
General	
Name	Type **wf-local** for the Web filtering profile. **NOTE**: The maximum length is 29 characters.
Timeout	Type **30** (in seconds) to wait for a response from the Local engine. The maximum value is 1800 seconds. The default value is 15 seconds.
Engine type	Select the **Local** engine type for Web filtering. Click **Next**. **NOTE**: The default value is Juniper Enhanced.

(Continued)

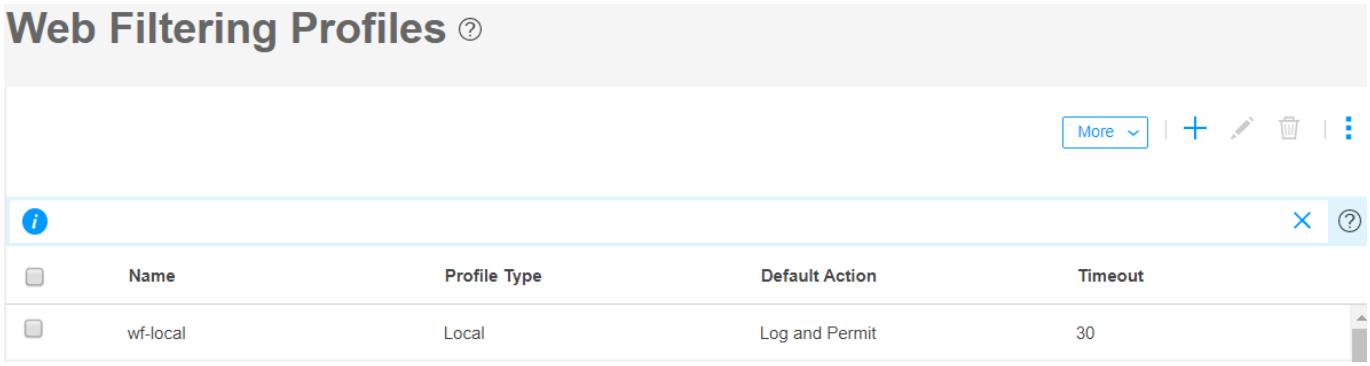
Field	Action
URL Categories	
+	Click the add icon to open the Select URL Categories window.
Select URL categories to apply to the list	Select **good-sites** or **stop-sites**.
Action	Select **Log and Permit** for the good-sites category from the list. Select **Block** for the stop-sites category from the list. Click **Next** and then click **Next** to skip the Fallback Options configuration.

Figure 3: Create Web Filtering Profile



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 **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 can be applied to a security policy.

You are here: **Security Services** > **UTM** > **UTM Policies**.

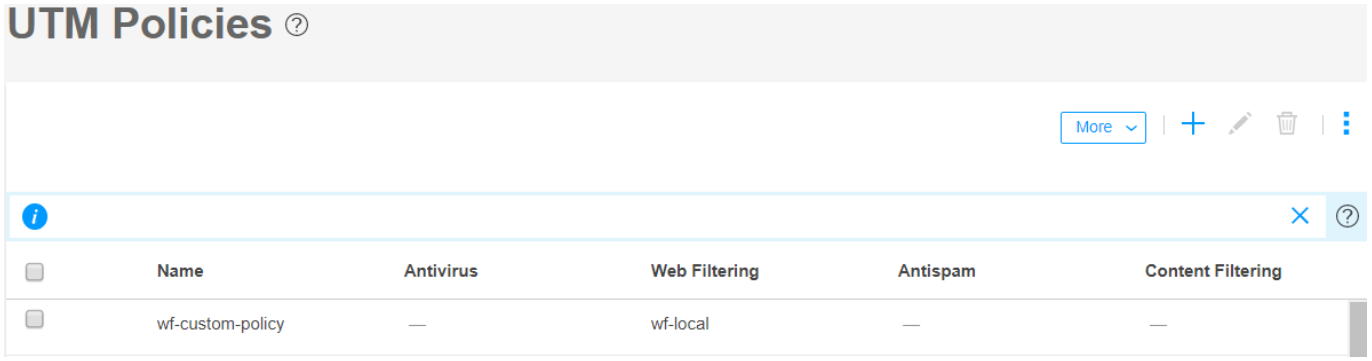
To create a UTM policy:

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	Type **wf-custom-policy** for the UTM policy. **NOTE**: The maximum length is 29 characters. Click **Next** and then click **Next** to skip the Antivirus configuration.
Web Filtering - Web Filtering Profiles by Traffic Protocol	
HTTP	Select **wf-local** from the list and click **Next** till the end of the workflow.

3. Click **Finish**. Review the summary of the configuration and click **OK** to save changes.
   Almost there! Here's the result of your configuration:

g300753



4. Click **Close** after you see a successful message.

   Almost done! Now, you create a default UTM web filtering policy that references your list of good and stop sites.

   You are here: **Security Services** > **UTM** > **Default Configuration Web Filtering**.

5. Click the edit (pencil) icon to modify the default web filtering policy.

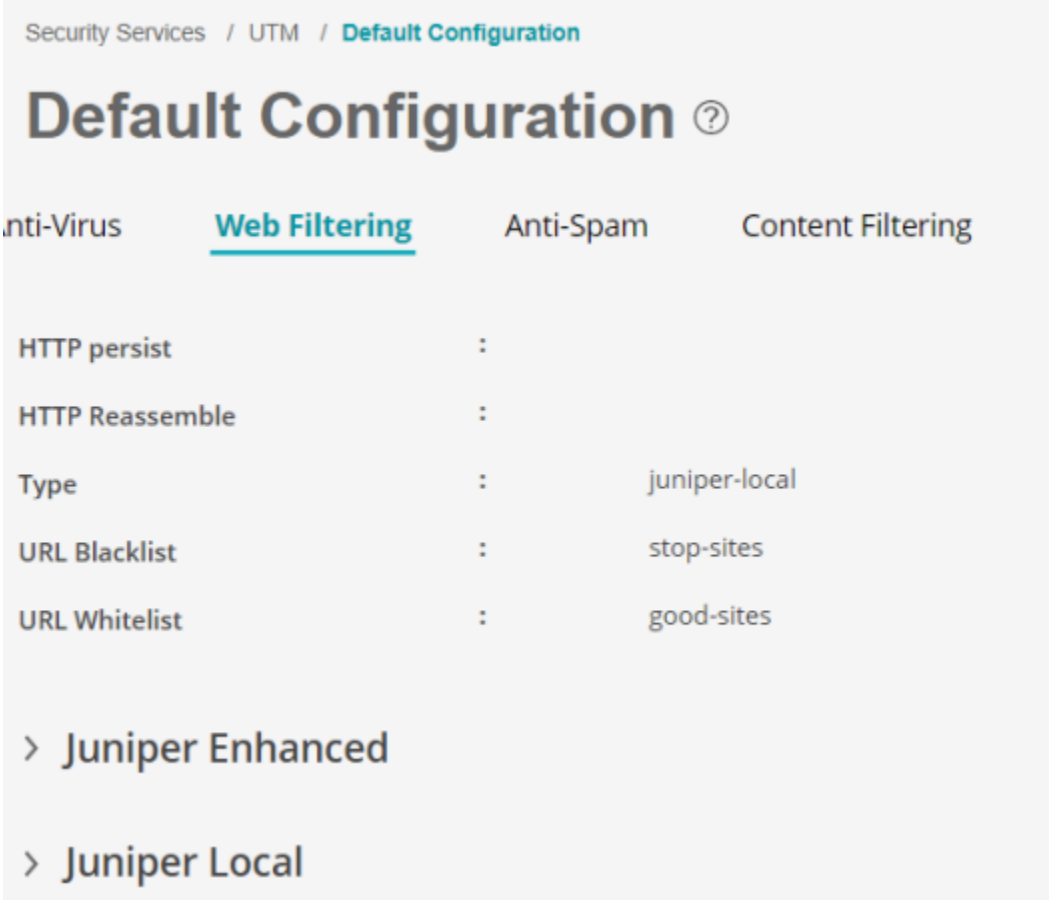
   The Web Filtering page appears.

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

Field	Action
Type	Use the menu pull-down to select **Juniper Local** to configure the use of the local UTM filtering database.
URL Blocklist	Use the menu pull-down to select **stop-sites** to link to the list of URLs that are not allowed (blocked).
URL Allowlist	Use the menu pull-down to select **good-sites** to link to the list of URLs that are allowed.
Juniper Local > Global	
Custom Block Message	Enter **Juniper Web Filtering has been set to block this site**.
Default Action	Select **Block** from the list. Skip other fields and click **OK**.

7. Click **OK** to save changes.

   Almost there! Here's the result of your UTM default web filtering configuration:



Good news! You're done with UTM Web filtering configuration.

Step 5: Assign a UTM Policy to a Security Policy

You haven't yet assigned the UTM configuration 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/HTTPS connection and extracts each URL (in the HTTP/HTTPS 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 (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: **Security Policies & Objects** > **Security Policies**.

To create security policy rules for the UTM policy:

1. Click the add icon (**+**).
2. Complete the tasks listed in the Action column in Table 1 on page 14.

Table 1: Rule Settings

Field	Action
General – General Information	
Rule Name	Type **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.
Source Zone	a. Click **+**. The Select Sources page appears. b. Zone—Select **TRUST** from the list. c. Addresses—Leave this field with the default value **Any**. d. Click **OK**

Table 1: Rule Settings *(Continued)*

Field	Action
Destination Zone	**a.** Click **+**. The Select Destination page appears. **b.** Zone—Select **INTERNET** from the list. **c.** Addresses—Leave this field with the default value **Any**. **d.** Services—Leave this field with the default value **Any**. **e.** URL Category—Leave this field blank. **f.** Click **OK**
Action	By default, **Permit** is selected. Leave as is.
Advanced Security	**a.** Click **+**. The Select Advanced Security page appears. **b.** UTM—Select **wf-custom-policy** from the list. **c.** Click **OK**

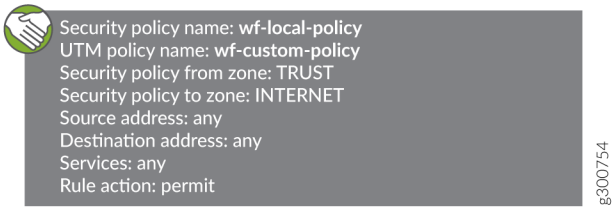
NOTE: Navigate to **Security Policies & Objects** > **Zones/Screens** to create zones. Creating zones is outside the scope of this documentation.

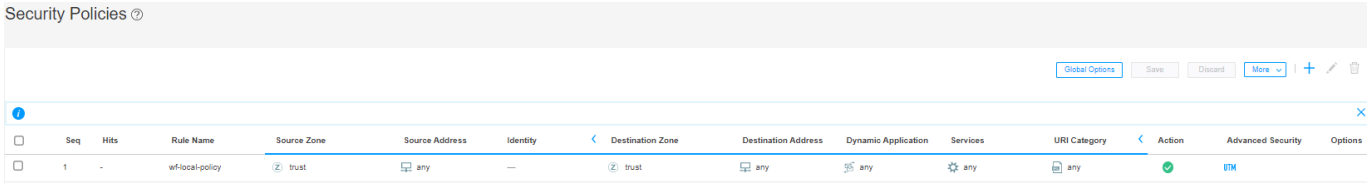
3. Click the tick icon

and then click **Save** to save changes.

NOTE: Scroll back the horizontal bar if the inline tick and cancel icons are not available when creating a new rule.

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.

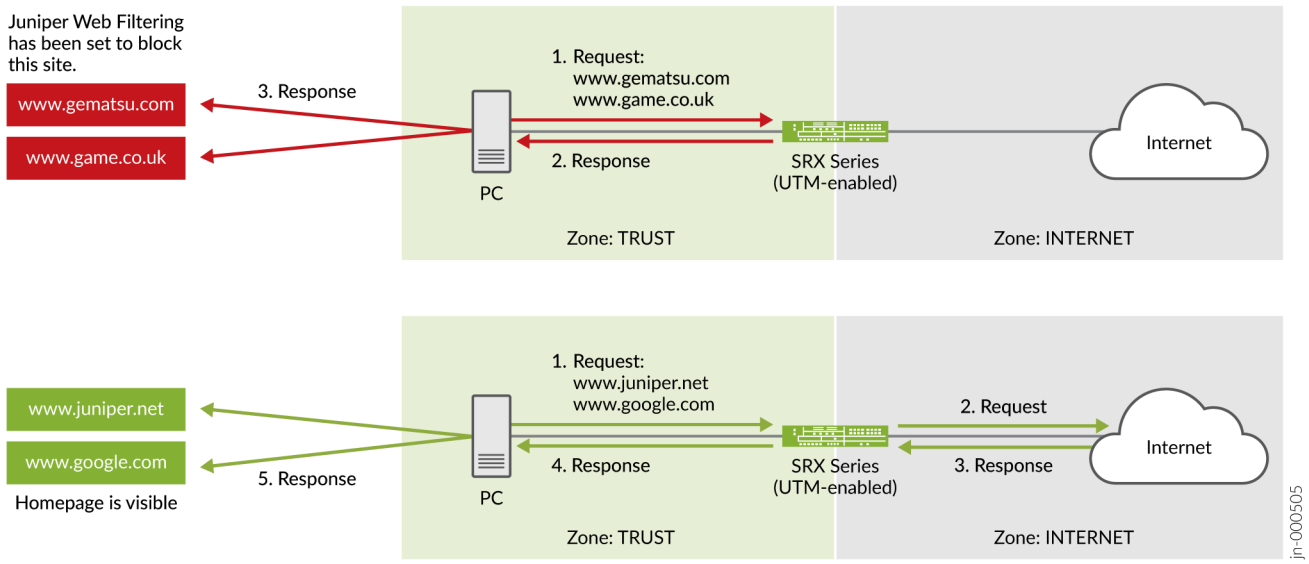
Step 6: Verify That the URLs Are Allowed or Blocked from the Server

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

- If you enter www.gematsu.com and www.game.co.uk, the SRX Series device should block the URLs and display the configured blocked site message.

  NOTE: Most sites use HTTPS. The blocked site messge is only seen for HTTP sites. For HTTPS you can expect a Secure Connection Failed error message such as "`An error occurred during a connection to <blocked-site-url> PR_CONNECT_RESET_ERROR`".

- 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://*.gematsu..com http://*.game.co.uk];
        }
        allowed-sites {
            value [ http://*.juniper.net http://*.google.com];
        }
    }
    custom-url-category {
        good-sites {
                    value allowed-sites;
                }
                stop-sites {
                    value blocked-sites;
                }
    }
 }
```

Creating the Web filtering profile:

```
default-configuration {
        web-filtering {
                url-whitelist good-sites;
                url-blacklist stop-sites;
                type juniper-local;
                juniper-local {
                    default block;
                    custom-block-message "Juniper Web Filtering has been set to block this site.";
                    fallback-settings {
                        default log-and-permit;
                        server-connectivity log-and-permit;
                        timeout log-and-permit;
                        too-many-requests log-and-permit;
                    }
               }
           }
        }
```

```
    feature-profile {
        web-filtering {
            juniper-local {
                profile wf-local {
                    category {
                    stop-sites {
                        action  block;
                    }
```

```
                    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;
                }
            }
        }
    }
}
```

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

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 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

IN THIS SECTION

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 and FTP traffic from a server (10.102.70.89) 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. Create Allowlist URL (http://10.102.70.89) where AV scanning is skipped.

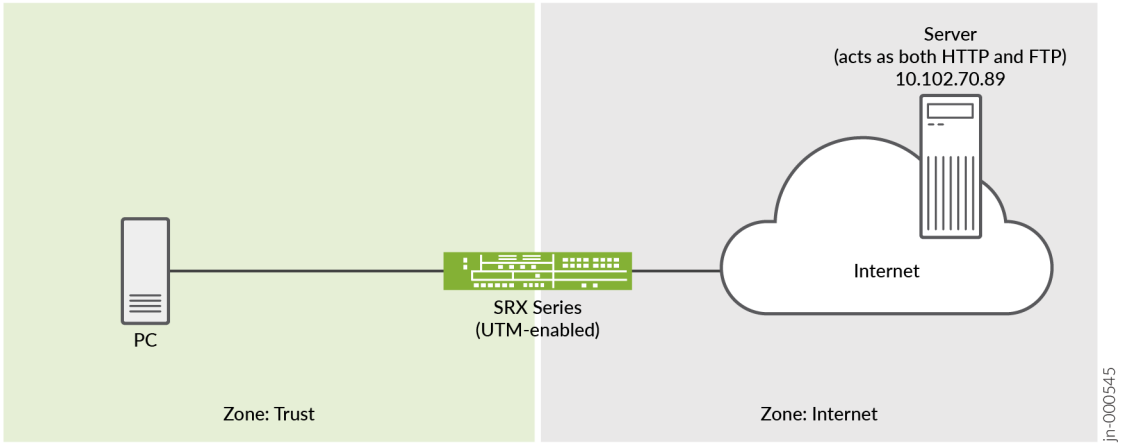
> **NOTE**: Assumption is that you must be able to route to the example URLs.

Before You Begin

- Install a valid Sophos antivirus license and application identification feature license. See Installation and Upgrade Guide, Licensing Administration Guide, and Licensing User Guide.
- Install an application signatures package for application identification. See Application Security User Guide for Security Devices.
- Ensure that the SRX Series device you use in this example runs Junos OS Release 20.4R1.

Topology

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

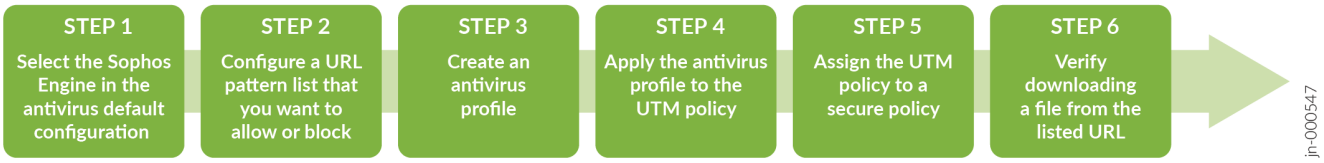


Table 2: J-Web UTM Antivirus Configuration Steps

Step	Action
Step 1	Configure the Sophos engine in Default Configuration. Here, you first define the default engine as Sophos in Default Configuration.
Step 2	Configure antivirus custom object. Here, you define the URL pattern list (allowlist) of URLs or addresses that will be bypassed by antivirus scanning. After you create the URL pattern list, you will create a custom URL category list and add the pattern list to it.
Step 3	Configure an antivirus feature profile using the Sophos engine. After the default configuration, you define the parameters that will be used for virus scanning in the antivirus profile. **NOTE**: You must configure DNS servers before creating the antivirus profiles. To configure DNS servers, go to **Device Administration** > **Basic Settings** > **System Identity** > **DNS servers**.
Step 4	Create a UTM policy for Sophos antivirus and apply the antivirus profile to the UTM policy. 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.
Step 5	Create a security policy for Sophos antivirus and assign the UTM policy to the security policy. Here, you use the security firewall and antivirus profile settings to scan the traffic from the trust zone (trust) to the untrust zone (Internet).
Step 6	Access a URL from the allowlist URL (http://10.102.70.89) and try to download a test virus file (eicar.txt) which is made available on the 10.102.70.89 server.

Step 1: Update Default Configuration for Antivirus

You are here: **Security Services** > **UTM** > **Default Configuration**.

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

To update the default antivirus profile:

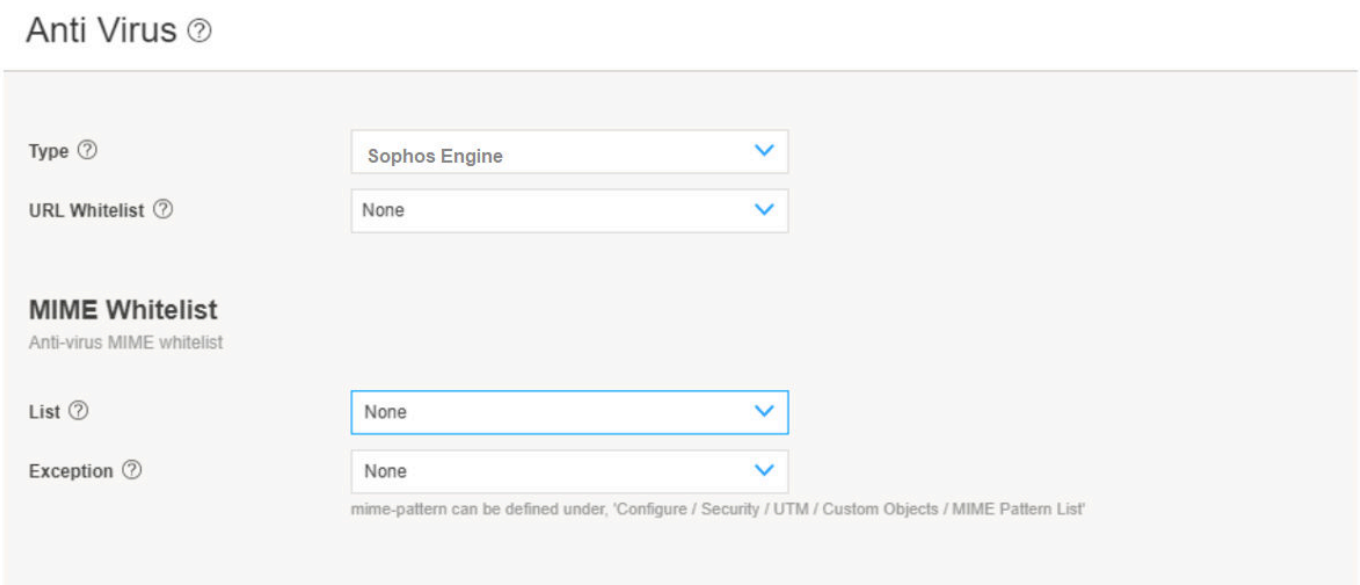
1. On the **Anti-Virus** tab, click the edit icon (pencil) to edit the default configuration.
   The Anti Virus page appears. See Figure 4 on page 25.

2. Complete the tasks listed in the Action column in Table 3 on page 25.

Table 3: 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 4: Default Antivirus Configuration



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

Step 2: Configure Antivirus Custom Object

IN THIS SECTION

Step 2a: 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): **Security Services** > **UTM** > **Custom Objects**.

To configure the safelist of URLs:

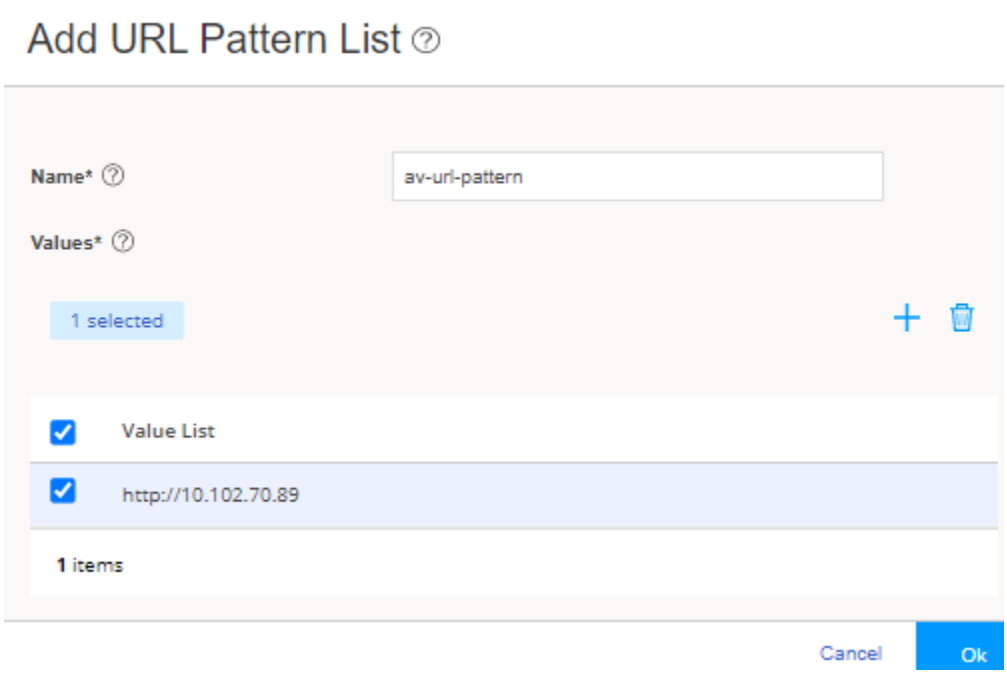
1. Click the **URL Pattern List** tab.
2. Click the add icon (**+**) to add a URL pattern list.

   The Add URL Pattern List page appears. See Figure 5 on page 27.
3. Complete the tasks listed in the Action column in Table 4 on page 26.

Table 4: URL Pattern List Settings

Field	Action
Name	Type **av-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 29 characters.
Value	**a.** Click **+** to add a URL pattern value. **b.** Type **http://10.102.70.89**. **c.** Click the tick icon ✓ .

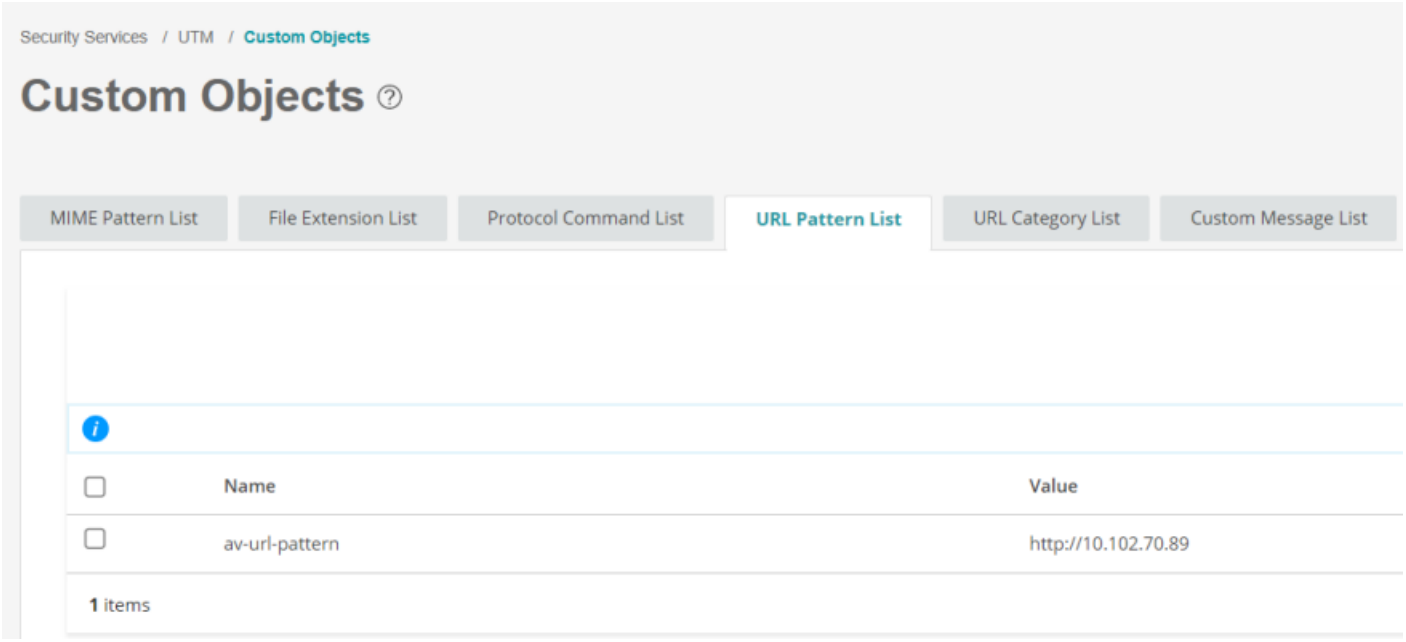
Figure 5: Add URL Pattern List



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

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

jn-000549



Step 2b: 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: **Security Services** > **UTM** > **Custom Objects**.

To categorize URLs:

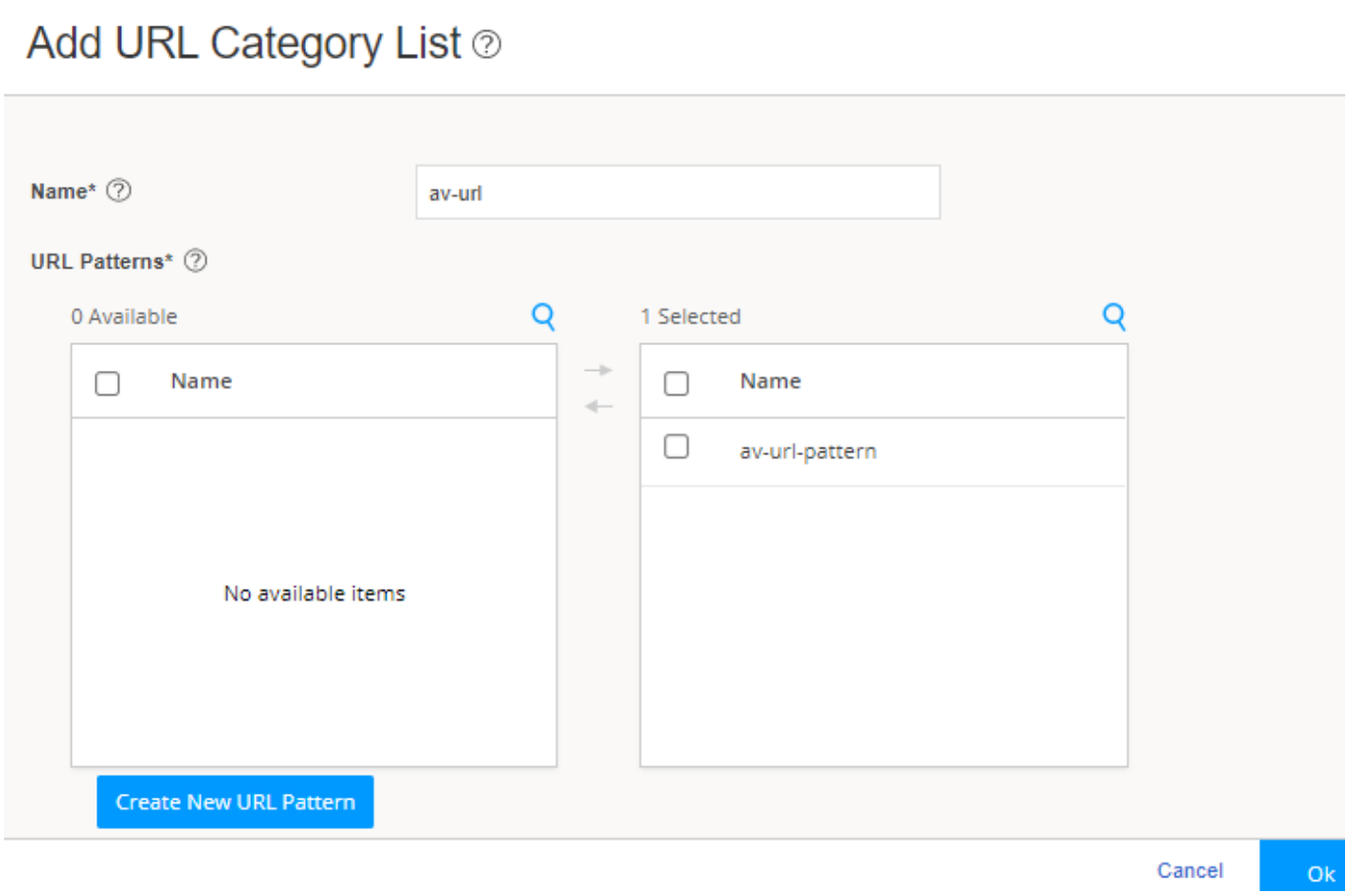
1. Click the **URL Category List** tab.
2. Click the add icon (**+**) to add a URL category list.

   The Add URL Category List page appears. See Figure 6 on page 29.
3. Complete the tasks listed in the Action column in Table 5 on page 28.

Table 5: URL Category List Settings

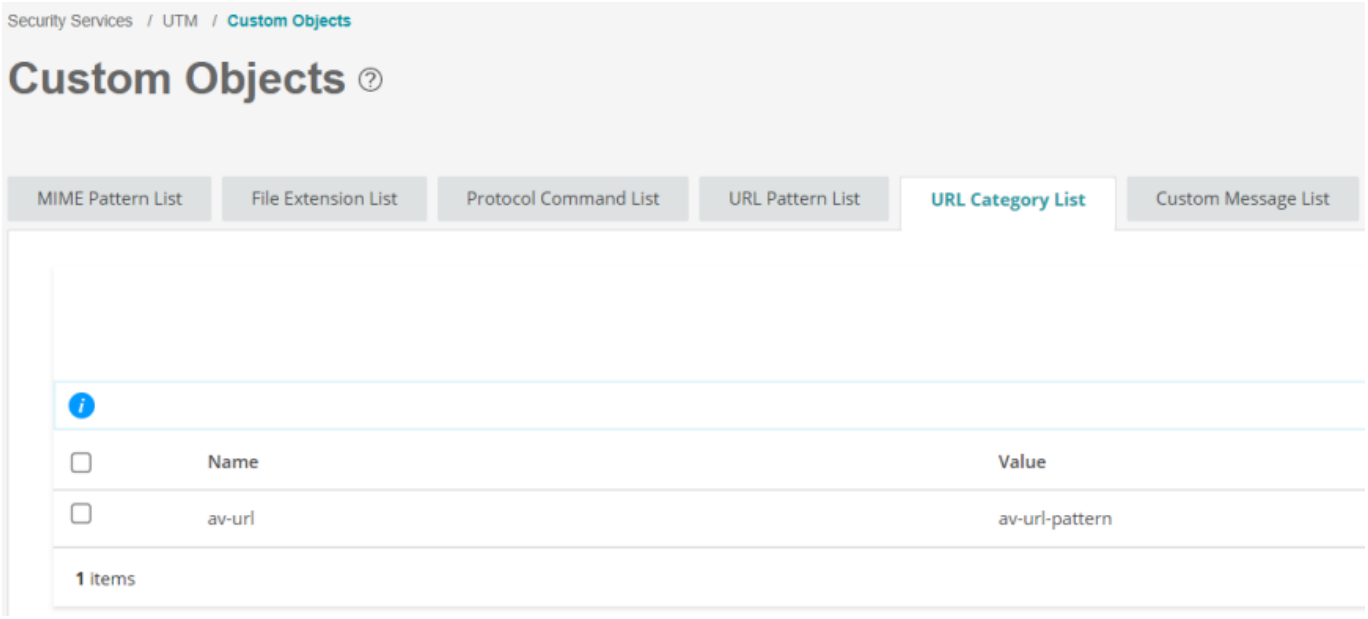
Field	Action
Name	Type **av-url** as the URL category list name for the safelisted URL pattern. **NOTE**: Use a string beginning with a letter or underscore and consisting of alphanumeric characters and special characters such as dashes and underscores. You can use a maximum of 59 characters.
URL Patterns	Select the URL pattern value **av-url-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 **av-url-pattern** with the URL category list **av-url**.

Figure 6: Add URL Category List



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

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



Step 3: Create an Antivirus Profile

You are here: **Security Services** > **UTM** > **Antivirus Profiles**.

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

   The Create Antivirus Profiles page appears. See Figure 7 on page 31.
2. Complete the tasks listed in the Action column in Table 6 on page 30.

Table 6: Antivirus Profile Settings

Field	Action
General	
Name	Type **av-profile** for the new antivirus profile. **NOTE**: You can use a maximum of 29 characters.
URL Allowlist	Select **av-url** from the drop-down list.
Fallback Options	

Table 6: Antivirus Profile Settings *(Continued)*

Field	Action
Content Size	Select **Log and Permit**.
Default Action	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

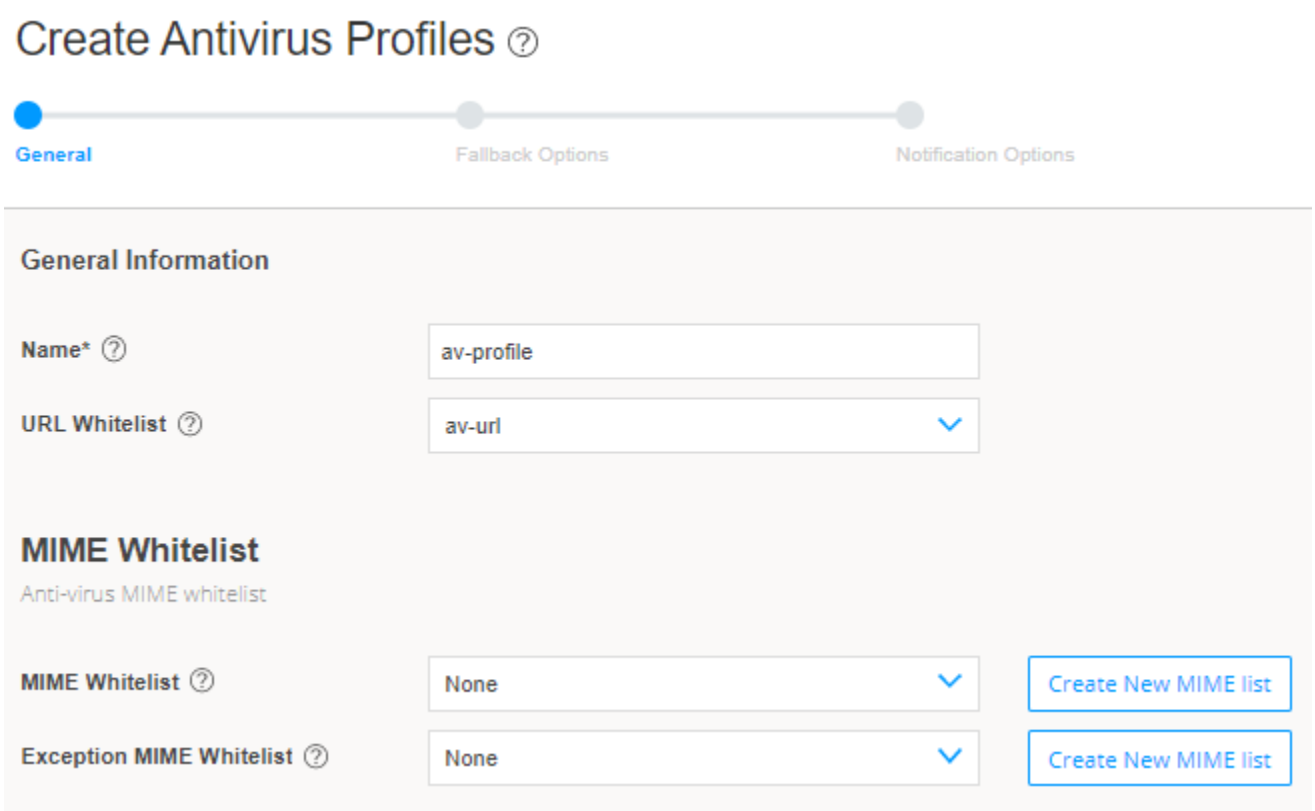
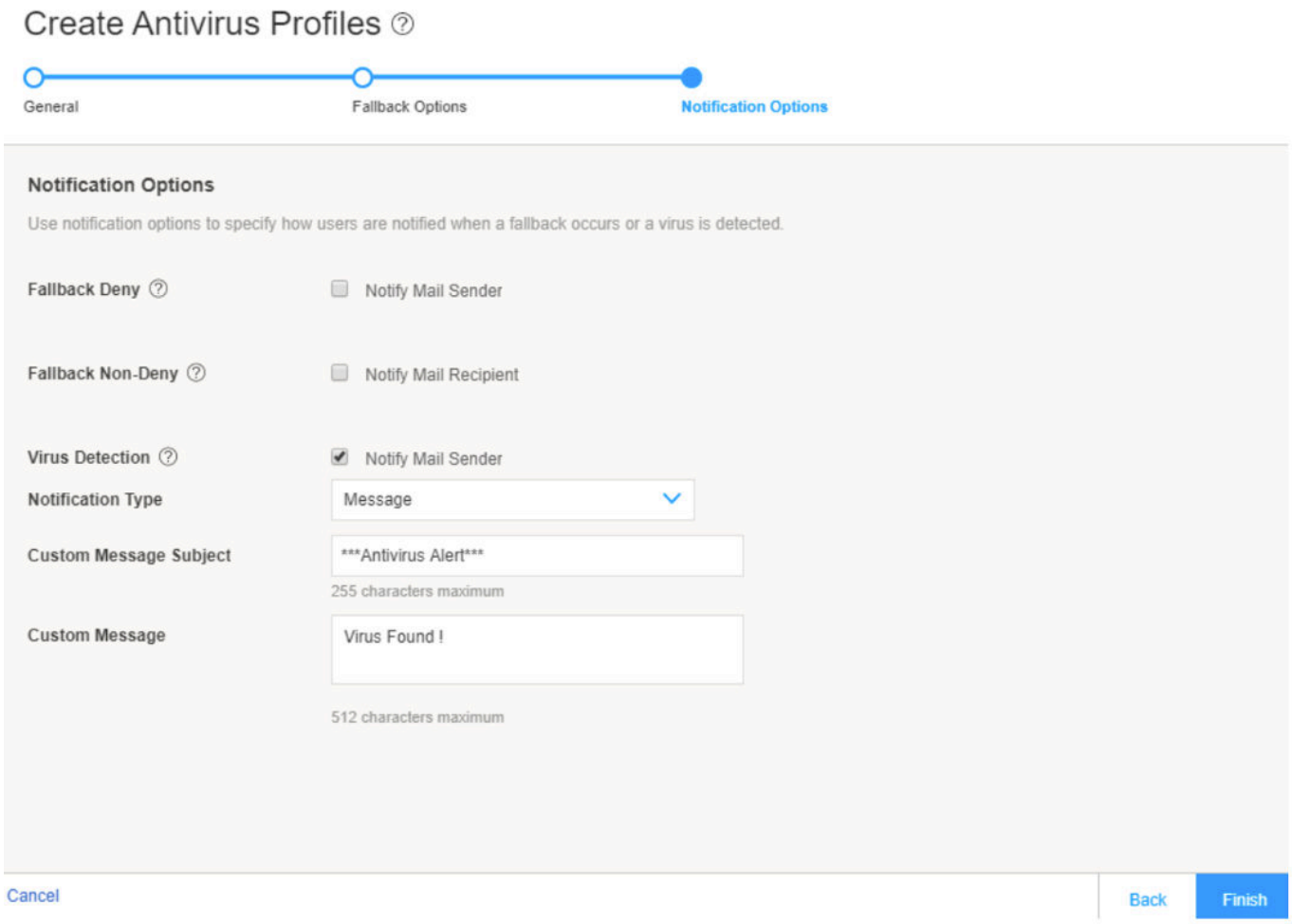


Figure 8: Create Antivirus Profile Notification Settings



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

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

jn-000551

Step 4: Apply the Antivirus 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 antivirus profile created in "Step 3: Create an Antivirus Profile" on page 30. In this example, you'll scan HTTP and FTP traffic for viruses.

You are here: **Security Services** > **UTM** > **UTM Policies**.

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 33.

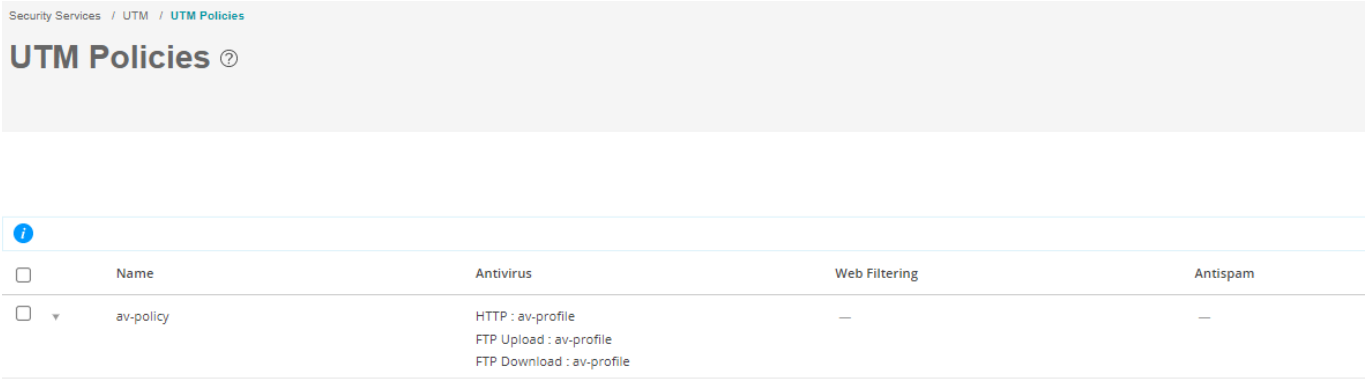
   Table 7: Create UTM Policies Settings

Field	Action
General	
Name	Type **av-policy** as the name of the UTM policy and click **Next**. **NOTE**: You can use a maximum of 29 characters.
Antivirus	
HTTP	Select **av-profile** from the list.
FTP Upload	Select **av-profile** from the list.
FTP Download	Select **av-profile** from the list and click **Next** till end of the page.

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:

jn-000552



Step 6: 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 trust zone (trust) to the untrust zone (internet) 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 (**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: **Security Policies & Objects** > **Security Policies**.

To create security policy rules for the UTM policy:

1. Click the add icon (**+**).
2. Complete the tasks listed in the Action column in Table 8 on page 34.

Table 8: Rule Settings

Field	Action
General	
Rule Name	Type **av-security-policy** as the security policy rule name. This rule allows the URLs in the av-url category list.
Rule Description	Enter a description for the security policy rule and click **Next**.
Source Zone	**a.** Click **+**. The Select Sources page appears. **b.** Zone—Select **trust** from the list. **c.** Addresses—Leave this field with the default value **any**. **d.** Click **OK**

Table 8: Rule Settings *(Continued)*

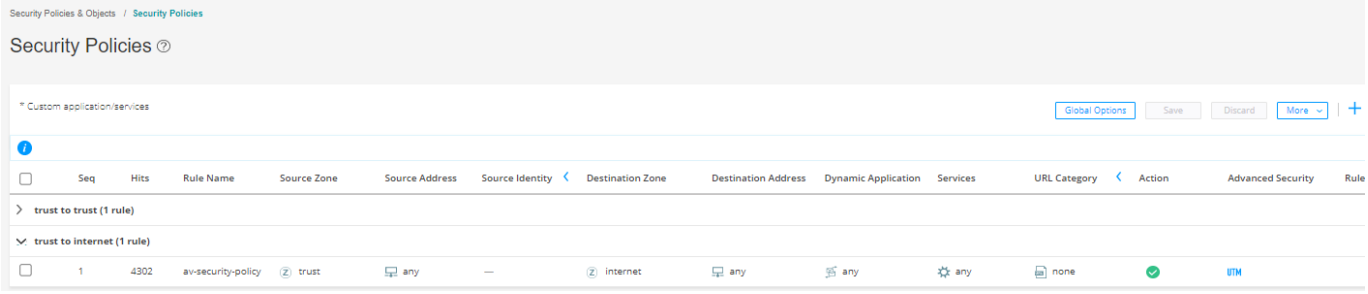
Field	Action
Destination Zone	**a.** Click **+**. The Select Destination page appears. **b.** Zone—Select **internet** from the list. **c.** Addresses—Leave this field with the default value **any**. **d.** Services—Leave this field with the default value **any**. **e.** Click **OK**
Action	Select **Permit** from the list.
Advanced Security	**a.** Click **+**. The Select Advanced Security page appears. **b.** UTM—Select **av-policy** from the list. **c.** Click **OK**

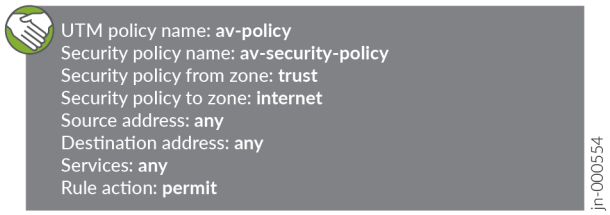
NOTE: Navigate to **Security Policies & Objects** > **Zones/Screens** to create zones. Creating zones is outside the scope of this documentation.

3. Click the tick icon

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 now ready to scan the traffic for virus attacks.

Step 7: Verify That UTM Antivirus Is Working

IN THIS SECTION

Purpose

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

Action

1. Using the PC, send a HTTP request to http://10.102.70.89.

   Good job! You can access the http://10.102.70.89 server.

2. Using the PC, send a FTP request to the 10.102.70.89 server to download the eicar.txt file. The eicar.txt file is a test virus file which is made available on the 10.102.70.89 server.

   Sorry! The SRX Series device has blocked downloading the file and sent you a custom block message *****Antivirus Alert***- Virus Found!**.

Here is an example output when you try to download the eicar.txt file and the SRX device sends a virus alert:

```
[centos-01 ~]$ ftp 10.102.70.89
Connected to 10.102.70.89 (10.102.70.89).
220 XX FTP server (Version 6.00LS) ready.
Name (10.102.70.89:lab): root
331 Password required for root.
Password:
230 User root logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get eicar.txt
local: eicar.txt remote: eicar.txt
227 Entering Passive Mode (10,102,70,89,197,55)
150 Opening BINARY mode data connection for 'eicar.txt' (70 bytes).
netin: Connection reset by peer
426 10.102.70.89:21->10.0.1.1:36240 ***Antivirus Alert***- Virus Found!
```

Here is an example of the anti-virus statistics output when you find a threat:

```
[edit]
root@srx> show security utm anti-virus statistics
 UTM Anti Virus statistics:

 Intelligent-prescreening passed:      0
 MIME-whitelist passed:                0
 URL-whitelist passed:                 1
 Session abort:                        0
 Scan Request:

  Total           Clean         Threat-found    Fallback
       2               0              1               0

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

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**
Generate and view reports on URLs allowed and blocked	To generate and view reports: 1. Log in to J-Web UI and click **Monitor** > **Reports**. The Reports page appears. 2. Select any of the following predefined report name. • **Threat Assessment Report** • **Viruses Blocked** **NOTE**: You can't generate more than one report at the same time. 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 {
        av-url-pattern {
            value http://10.102.70.89 ;
        }
    }
    custom-url-category {
```

```
        av-url {
            value av-url-pattern;
        }
    }
}
```

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

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

```
    feature-profile {
        anti-virus {
            profile av-profile {
                notification-options {
                    virus-detection {
                    type message;
                    notify-mail-sender;
                    custom-message “Virus-Found!”;
                    custom-message-subject “***Antivirus Alert***”;
                    }
                }
            }
        }
    }
```

Creating the UTM policy:

```
utm-policy av-policy {
            anti-virus {
                http-profile av-profile;
                ftp {
                    upload-profile av-profile;
                    download-profile av-profile;
                }
            }
        }
```

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

```
from-zone trust to-zone internet {
    policy av-security-policy {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    utm-policy av-policy;
                }
            }
        }
    }
}
```