

## 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](http://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 | iv

Documentation and Release Notes | iv

Documentation Conventions | iv

Documentation Feedback | vii

Requesting Technical Support | vii

Self-Help Online Tools and Resources | viii

Creating a Service Request with JTAC | viii

1

## Start Here with J-Web for SRX Series

What You Need to Know About the In Focus Guide | 10

2

## UTM Web Filtering

Allow or Block Websites by Using J-Web Integrated UTM Web Filtering | 12

Benefits of UTM Web Filtering | 12

Why URL Filtering | 13

Web Filtering Workflow | 13

Scope | 13

Before You Begin | 14

Topology | 15

Sneak Peek – J-Web UTM Web Filtering Steps | 15

Step 1: List URLs That You Want to Allow or Block | 15

Step 2: Categorize the URLs That You Want to Allow or Block | 17

Step 3: Add a Web Filtering Profile | 19

Step 4: Reference a Web Filtering Profile in a UTM Policy | 22

Step 5: Assign a UTM Policy to a Security Policy | 23

Step 6: Verify That the URLs Are Allowed or Blocked from the Server | 26

What's Next | 26

Sample Configuration Output | 27

# About the Documentation

## IN THIS SECTION

- Documentation and Release Notes | iv
- Documentation Conventions | iv
- Documentation Feedback | vii
- Requesting Technical Support | vii

## Documentation and Release Notes

To obtain the most current version of all Juniper Networks<sup>®</sup> 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 v](#) 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 v defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b>  No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies guide names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS CLI User Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>

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@# <b>set system domain-name</b> <i>domain-name</i>
<b>Text like this</b>	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit <b>protocols ospf area area-id</b>] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Encloses optional keywords or variables.	<b>stub</b> <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.	<b>broadcast   multicast</b>  ( <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.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	<b>community name members [ <i>community-ids</i> ]</b>
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

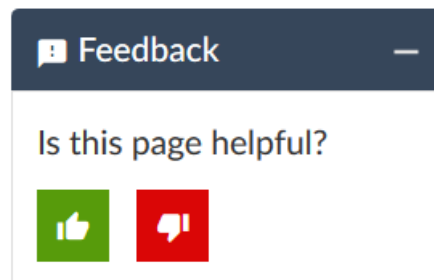
Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<b>Bold text like this</b>	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## 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](mailto: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](#) | 10

---

# 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](mailto:techpubs-comments@juniper.net).

# 2

CHAPTER

## UTM Web Filtering

---

Allow or Block Websites by Using J-Web Integrated UTM Web Filtering | 12

---

# 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 | 12](#)
- [Why URL Filtering | 13](#)
- [Web Filtering Workflow | 13](#)
- [Step 1: List URLs That You Want to Allow or Block | 15](#)
- [Step 2: Categorize the URLs That You Want to Allow or Block | 17](#)
- [Step 3: Add a Web Filtering Profile | 19](#)
- [Step 4: Reference a Web Filtering Profile in a UTM Policy | 22](#)
- [Step 5: Assign a UTM Policy to a Security Policy | 23](#)
- [Step 6: Verify That the URLs Are Allowed or Blocked from the Server | 26](#)
- [What's Next | 26](#)
- [Sample Configuration Output | 27](#)

## 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](http://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.

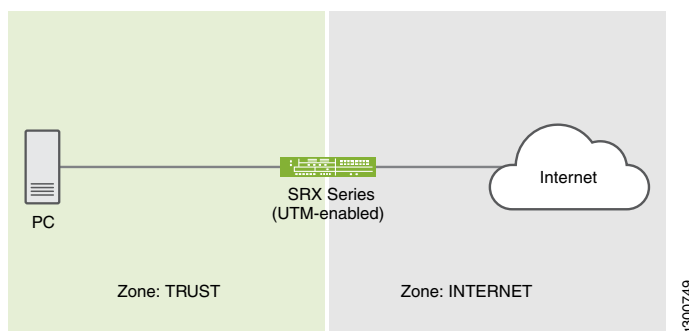
**NOTE:** Web filtering and URL filtering have the same meaning. We'll use the term *Web filtering* throughout our example.

## 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 16](#).

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


Field	Action
Name	<p>Enter <b>allowed-sites</b> or <b>blocked-sites</b>.</p> <p><b>NOTE:</b> 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"> <li>• For allowed-sites—<b>www.juniper.net</b> and <b>www.google.com</b></li> <li>• For blocked-sites—<b>www.gamestu.com</b> and <b>www.gameplay.com</b></li> </ul> <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

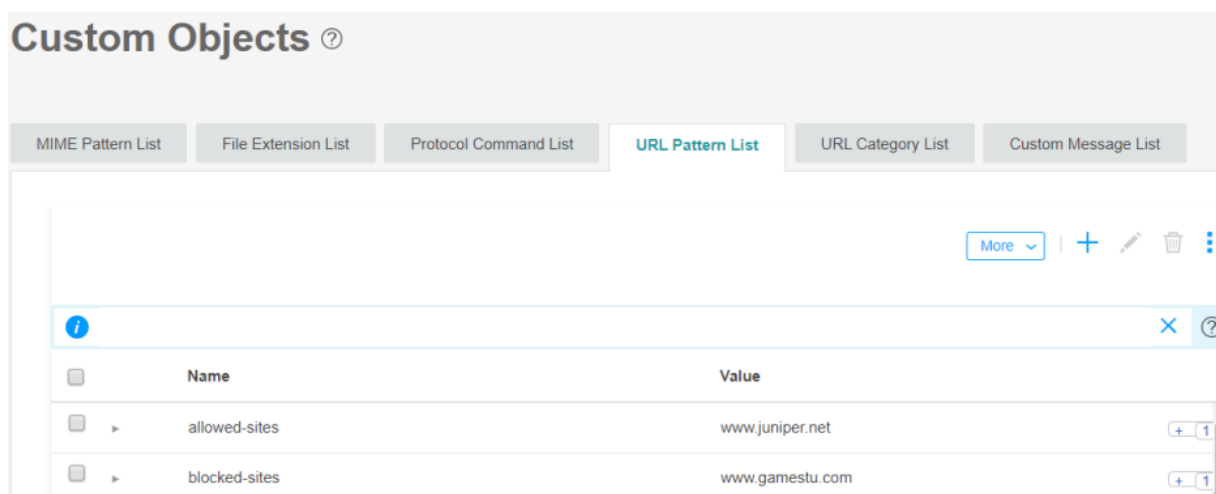
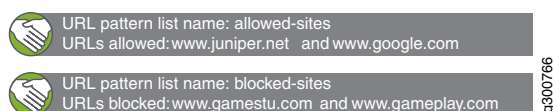
2 items

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 18](#).

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

Field	Action
Name	<p>Enter the URL category list name as <b>good-sites</b> for the allowed-sites URL pattern or <b>stop-sites</b> for the blocked-sites URL pattern.</p> <p><b>NOTE:</b> 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 <b>allowed-sites</b> or <b>blocked-sites</b> 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 ▾+✎🗑⋮

<span>!</span>			<span>×</span> <span>?</span>
<input type="checkbox"/>	Name	Value	
<input type="checkbox"/>	good-sites	allowed-sites	
<input type="checkbox"/>	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:

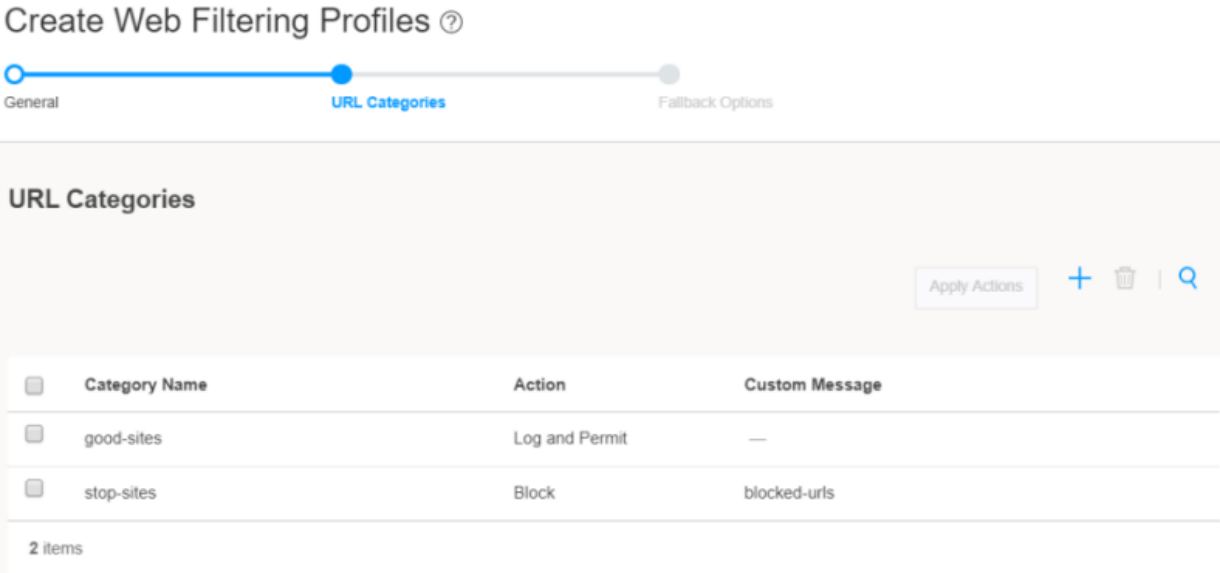
- 1. Click the add icon (+) to add a Web filtering profile.  
The Create Web Filtering Profiles page appears. See [Figure 3 on page 21](#).

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

Field	Action
General	


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

Figure 3: Create Web Filtering Profile



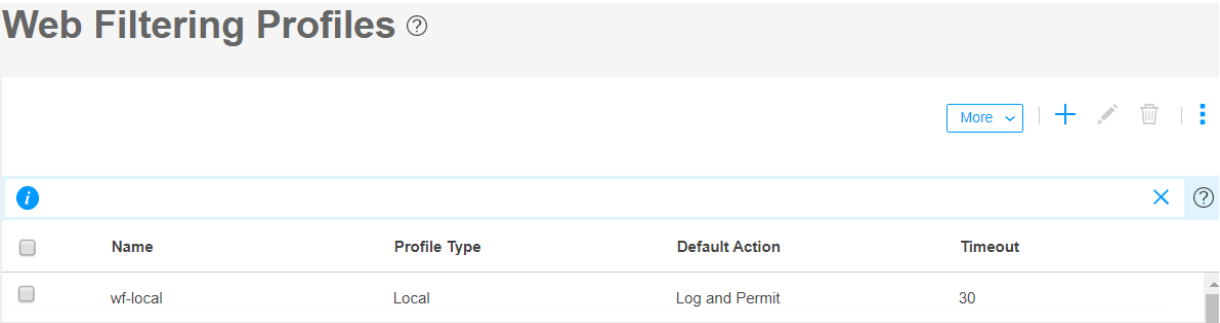
3. Click **Finish**. Review the summary of the configuration and click **OK** to save changes.

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



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



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

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:

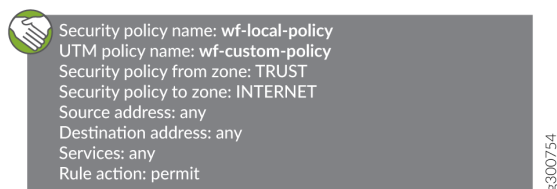
Field	Action
<b>General – General Information</b>	
Rule Name	Enter <b>wf-local-policy</b> for the security policy allowing the good-sites category and denying the stop-sites category.
Rule Description	Enter a description for the security policy rule and click <b>Next</b> .
<b>Source</b>	
Zone	Select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



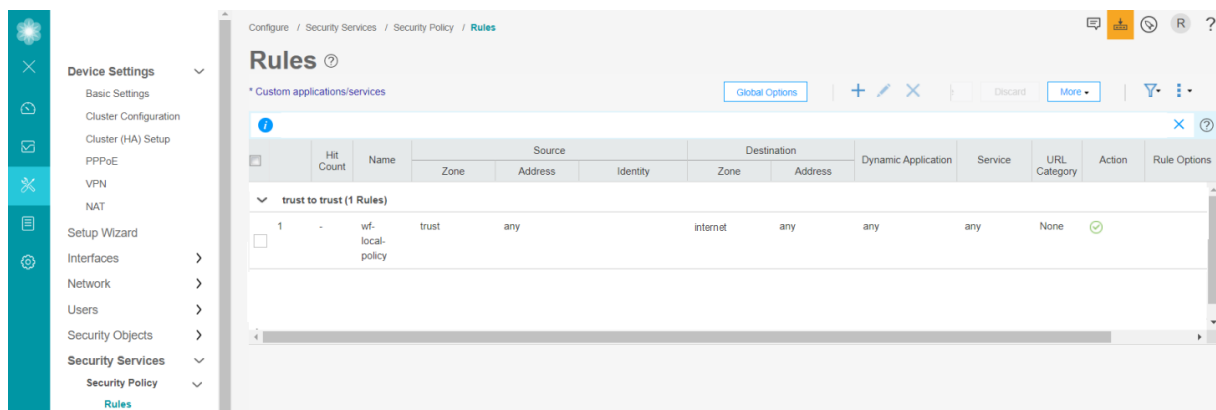
Field	Action
<b>Destination</b>	
Zone	Select <b>INTERNET</b> from the list.
Address(es)	Leave this field with the default value <b>any</b> .
Service(s)	Leave this field with the default value <b>any</b> .
<b>Advanced Security</b>	
Rule Action	Select <b>Permit</b> from the list.
UTM	Select <b>wf-custom-policy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



g300754



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

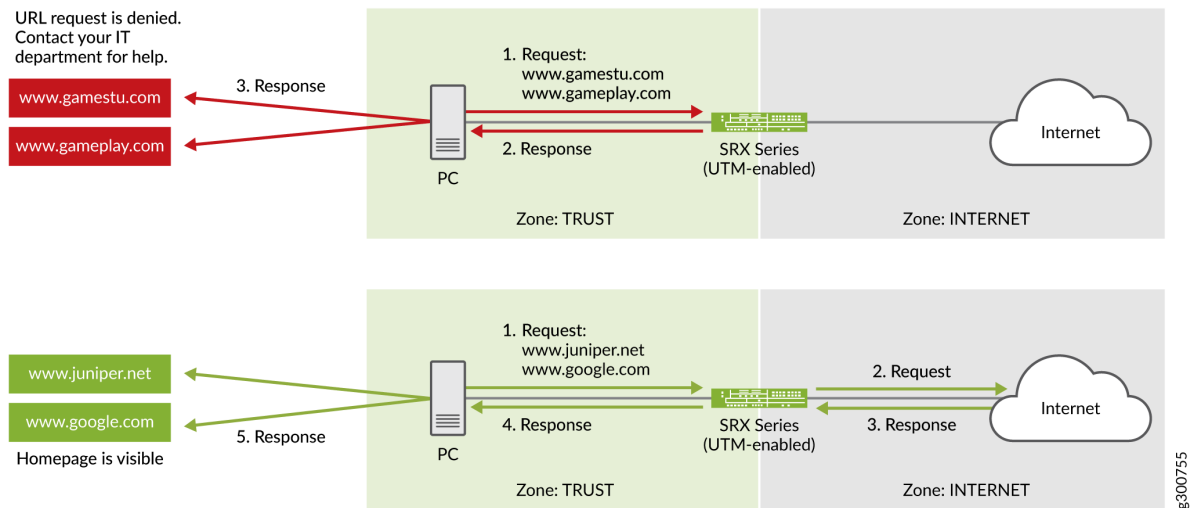
The successful-commit message appears.

*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](http://www.gamestu.com) and [www.gameplay.com](http://www.gameplay.com), the SRX Series device should block the URLs and send the configured block message.
- If you enter [www.juniper.net](http://www.juniper.net) and [www.google.com](http://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 <b>Monitor &gt; Security Services &gt; UTM Web Filtering</b> .
Generate and view reports on URLs allowed and blocked.	In J-Web, go to <b>Reports</b> . Generate reports for Threat Assessment Reports and Top Blocked Applications via Webfilter logs.
Learn more about UTM features.	<a href="#">Unified Threat Management User Guide</a>

## 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;
        }
      }
    }
  }
}

```

```
}  
}
```