Juniper UTM Components

**Web Filtering**

Allows you to permit or block access to specific websites by URL, or by category using cloud-based lookups, a local database, or external Websense server.

**Antivirus**

Checks files transmitted over several protocols to determine if the files exchanged are malicious (for example, viruses, Trojans, rootkits, and worms).

**Antispam**

Offers a lightweight solution that can block spam by scanning inbound and outbound SMTP email traffic.

**Content Filtering**

Provides basic data loss prevention functionality. Filters traffic based on MIME type, file extension, protocol commands, and embedded object type.

**Enhanced Web Filtering**

Functions similarly to integrated Web filtering. Also, assigns a reputation score to a site to determine actions based on the reputation score.

**Local Web Filtering**

Blocks or permits Web access based on the user-defined categories stored on the device.

**Redirect Web Filtering**

Intercepts HTTP requests and forwards the server URL to an external URL filtering server. The external Websense server determines whether to block or permit access.

**Kaspersky Full Antivirus**

Uses a comprehensive integrated signature, heuristics, and behavior-based scanning engine to help prevent malicious code from reaching devices on your network.

**Juniper Express Antivirus**

Uses a stream scanning engine and virus signature databases to help prevent malicious code from reaching devices on your network.

**Sophos Antivirus**

Uses a cloud-based stream scanning engine with integrated URL reputation features for faster decision-making to help prevent malicious code from reaching devices on your network.

**Server-Based Antispam Filtering**

Blocks and filters unwanted email traffic by scanning inbound and outbound SMTP email traffic using an external spam block list server.

**Quick Tip:** How to Configure a UTM Feature

1. Configure Custom Objects (if needed)
2. Configure Component Feature Profiles
3. Create UTM Policy and Add Feature Profiles
4. Assign UTM Policy to a Security Policy

**Juniper UTM Components**

Juniper Networks® Unified Threat Management provides a solution to IT’s most challenging security problems. It is available with Juniper Networks SRX Series Services gateways, the only carrier-class security solution consolidating UTM content security services with routing and switching in a single, high-performance, and cost-effective network device. This consolidation enables organizations to securely, reliably, and economically deliver powerful new services and applications to all locations and users with superior service quality.

SRX Series gateways are powered by Juniper Networks® Junos® operating system, the same industry-leading OS platform that keeps the world’s largest networks available, manageable, and secure.

©2015 by Juniper Networks, Inc. All rights reserved. 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.
# Juniper UTM Features and Benefits

## UTM Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Module</th>
<th>License Required</th>
<th>Supported Platforms</th>
<th>Supported Protocols</th>
<th>Management</th>
<th>Benefits</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web Filtering</strong></td>
<td><strong>Enhanced Web Filtering</strong></td>
<td>Yes</td>
<td>SRX Series, Firefly Perimeter/vSRX</td>
<td>HTTP, HTTPS</td>
<td>J-Web Security Director</td>
<td>The most powerful integrated method in terms of detection and the integrated package, includes a granular list of URL categories, support for Google Safe Search, and a reputation engine. No additional server components are required. This feature can also redirect users to a custom URL for block pages.</td>
<td>Requires an internet connection to contact the Threatseeker cloud.</td>
</tr>
<tr>
<td><strong>Local Web Filtering</strong></td>
<td>No</td>
<td>SRX Series, Firefly Perimeter/vSRX</td>
<td>HTTP</td>
<td>J-Web Security Director</td>
<td>Does not require a license. Good for defining your own blacklist or whitelist. Good if you only have a handful of URLs for which you want to enforce a policy.</td>
<td>Not ideal for broad URL filtering support; only geared for specific URLs.</td>
<td></td>
</tr>
<tr>
<td><strong>Redirect Web Filtering</strong></td>
<td>No</td>
<td>Branch SRX Series, Firefly Perimeter/vSRX</td>
<td>HTTP, HTTPS</td>
<td>J-Web Security Director</td>
<td>All queries are tracked locally, so an internet connection is not required. Can use the logging and reporting of a standalone Websense solution. Slightly lower latency because the server is onsite. You own the entire solution.</td>
<td>Requires a separate Websense server.</td>
<td></td>
</tr>
<tr>
<td><strong>Antivirus</strong></td>
<td><strong>Kaspersky</strong></td>
<td>Yes*</td>
<td>SRX Series</td>
<td>SMTP, POP3, IMAP, HTTP, FTP</td>
<td>J-Web Security Director</td>
<td>Deep security scanning. Built in antivirus capabilities. Ability to inspect compressed content. Good detection capabilities for content loaded on device. Does not require URL information to be sent, but requires internet connection for downloads.</td>
<td>Might impact network performance. No reputation feed for URL, which impacts performance. Database is limited by device memory. Limited detection for complicated attacks if they are not identified by patterns or heuristics.</td>
</tr>
<tr>
<td><strong>Juniper Express Antivirus</strong></td>
<td>Yes</td>
<td>Branch SRX Series</td>
<td>SMTP, POP3, IMAP, HTTP, FTP</td>
<td>J-Web Security Director</td>
<td>Least performance impact. Does not require URL information to be sent, but requires internet connection for downloads.</td>
<td>Less comprehensive signature database. No reputation feed; pattern matching only. Limited ability to detect complicated or compressed malware.</td>
<td></td>
</tr>
<tr>
<td><strong>Sophos Antivirus</strong></td>
<td>Yes</td>
<td>SRX Series, Firefly Perimeter/vSRX</td>
<td>SMTP, POP3, IMAP, HTTP, FTP</td>
<td>J-Web Security Director</td>
<td>Very good detection, particularly with the URL checks. Database is unlimited because it leverages the Sophos cloud. Can detect complicated malware.</td>
<td>Requires an internet connection to query the Sophos cloud for URL checks.</td>
<td></td>
</tr>
<tr>
<td><strong>Antispam</strong></td>
<td><strong>Server-based Antispam Filtering</strong></td>
<td>Yes</td>
<td>SRX Series</td>
<td>SMTP</td>
<td>J-Web Security Director</td>
<td>Blacklist-based solution to filter inbound spam over SMTP.</td>
<td>The solution is based on an IP reputation list offered from the cloud via Sophos.</td>
</tr>
<tr>
<td><strong>Local List Antispam Filtering</strong></td>
<td>Yes</td>
<td>SRX Series, Firefly Perimeter/vSRX</td>
<td>SMTP</td>
<td>J-Web Security Director</td>
<td>Local blacklist and whitelist matching does not require a license.</td>
<td>Pattern matching for domain names uses a longest suffix match algorithm. IP address matching, however, does not allow for partial matches.</td>
<td></td>
</tr>
<tr>
<td><strong>Content Filtering</strong></td>
<td>No</td>
<td>SRX Series, Firefly Perimeter/vSRX</td>
<td>SMTP, POP3, IMAP, HTTP, FTP</td>
<td>J-Web Security Director</td>
<td>Either permits or blocks specific commands or extensions on a protocol-by-protocol basis.</td>
<td>Blocks files according to extensions and payload data.</td>
<td></td>
</tr>
</tbody>
</table>


**Benefits**
- Comprehensive, all-in-one, layered security solution
- Simplified security operations through Junos OS, a single operating system platform
- Reduced costs and complexity in a single, integrated device
- Better performance through optimized hardware with separate data and control plane
- More management options and control with user-role based policy
- Flexibility with cloud-based and on-box anti-malware options

**Limitations**
- Requires an internet connection to contact the Threatseeker cloud.
- Not ideal for broad URL filtering support; only geared for specific URLs.
- Requires a separate Websense server.