APPLICATION NOTE

ANTIVIRUS FOR BRANCH SRX SERIES AND J SERIES

Configuring Antivirus on Branch SRX Series Services Gateways and J Series Services Routers

Table of Contents

Table of Figures

Introduction

Antivirus is an established part of any unified threat management (UTM) suite and has been available on firewalls for many years. Although the introduction of Web 2.0 has created new security requirements, antivirus remains an integral part of any security strategy. Endpoint protection is still of paramount importance, but antivirus at the gateway prevents many threats from even reaching many network devices. Additionally, if a new threat is in the wild, antivirus will provide a certain level of network protection while other defenses are being updated. Antivirus on firewalls and routers is not a new idea, but it is still an important part of any enterprise security strategy.

Scope

Juniper Networks® Junos® operating system Release 9.5 adds UTM support for Juniper Networks J Series Services Routers and selected Juniper Networks SRX Series Services Gateways. Antivirus, one of several features—including content filtering, antispam, and Web filtering—that make up Juniper's UTM suite, provides the ability to prevent threats at the gateway before they enter the network. Two different Kaspersky scan engines are explained first, and then several configuration examples are provided.

Design Considerations

When deciding to deploy antivirus, network designers should consider the performance impact of value-added security. Product guidelines can be found on SRX Series Services Gateways and J Series Services Routers datasheets.

Hardware Requirements

- Juniper Networks SRX Series Services Gateways for the branch including the SRX100, SRX210, SRX240, and SRX650 (Antivirus is not available on high-end SRX Series platforms.)
- Juniper Networks J Series Services Routers including the J2320, J2350, J4350, and J6350

Software Requirements

- Junos OS Release 9.5 or later

Description and Deployment Scenario

Starting with Release 9.5, Juniper Networks has added an antivirus feature to Junos OS for branch SRX Series Services Gateways and J Series Services Routers. Juniper Networks has partnered with Kaspersky Lab to provide both the antivirus engine and the virus/signature databases used to scan files for viruses, trojans, rootkits, and other types of malicious code. Kaspersky Lab also provides the signature database used in the Juniper ExpressAV engine.

Administrators can choose between traditional virus prevention and the ExpressAV option, a decision that involves some trade-offs. By reading this application note, readers will be able to choose which scanning engine best meets their needs and easily configure antivirus on SRX Series Services Gateways or J Series Services Routers.

Kaspersky Scan Engine

The Kaspersky scan engine provides file-scanning services to Junos OS. When scanning is enabled, SRX Series devices or J Series routers inspect data streams searching for attached files—such as in email messages and FTP downloads/uploads, or embedded scripts—such as can be found when downloading Web pages.

When the gateway flags a file for inspection, it caches the file (or embedded script) in memory and uses the scanning engine to search for viruses, trojans, rootkits, and other types of malicious code. If a virus is detected, the file will be dropped and the user/originator will be notified.

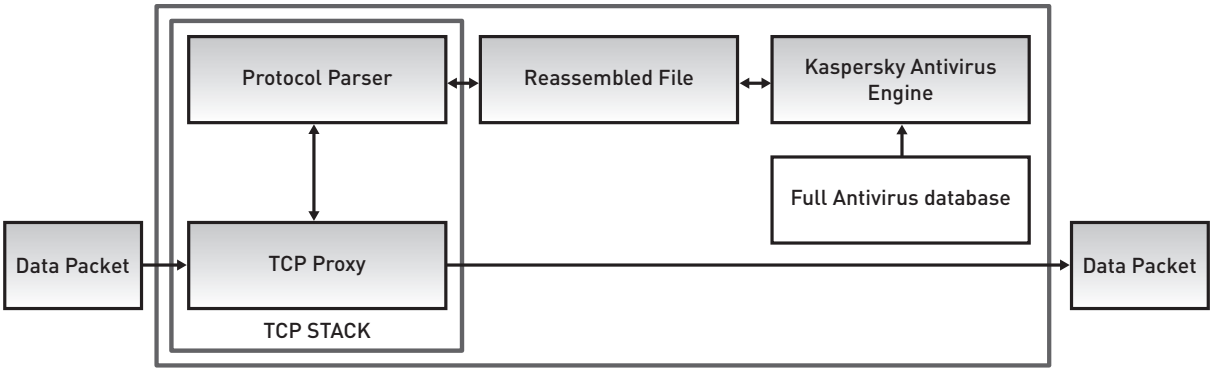

Figure 1: Full antivirus processing flow

When considering the full antivirus solution, the following factors should be evaluated:

- Full antivirus provides a high detection rate, since the scanning engine caches the entire file and can scan it in multiple passes.
- Full antivirus supports the scanning of compressed files as caching allows the files to be decompressed before the scan is performed (files compressed multiple times are supported up to a depth of 4).
- Available memory limits the size of files that can be scanned.
- Full antivirus increases transfer delays because files are locally stored before transmission.
- Available memory and CPU cycles limit the number of files that can be concurrently scanned (currently two concurrent files are permitted).
- At the time of writing, over 405,000 signatures are part of the full antivirus database—including widespread, dangerous, recent, and current viruses.

Juniper ExpressAV Engine

Leveraging the technology used for Juniper Networks IDP Series Intrusion Detection and Prevention Appliances, Juniper has added an ExpressAV scan engine that uses pattern matching to provide detection. This engine can make use of the Content Security Accelerator (CSA) available on the branch SRX Series platforms and yields higher performance at the expense of somewhat lower catch rates. Platforms not equipped with a CSA can still perform software pattern matching, but performance will be lower (UTM always requires the high-memory option).

The ExpressAV option uses a modified version of the Kaspersky signature database.

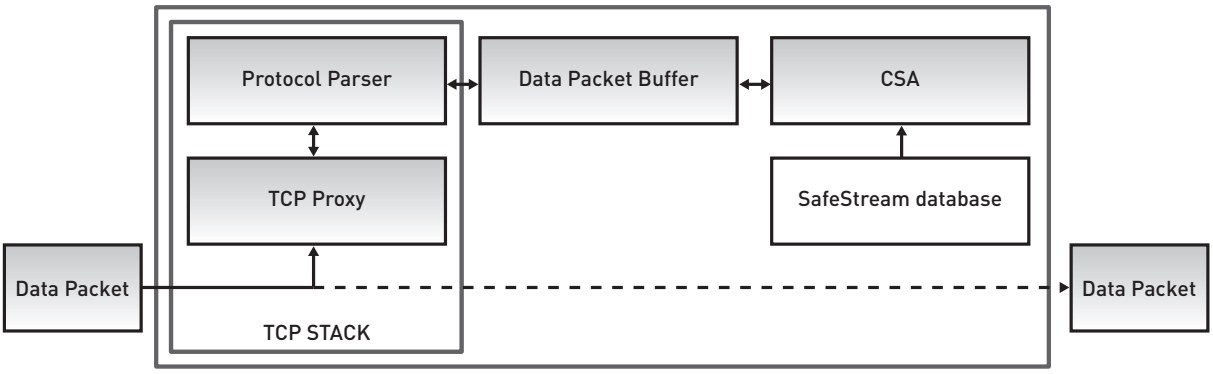

Figure 2: Juniper ExpressAV processing flow

As expected, there are some advantages and some constraints with ExpressAV scanning:

- ExpressAV catch rates are lower than full antivirus, but ExpressAV is able to catch the most common viruses.
- ExpressAV provides higher throughput, as processing can be hardware accelerated.
- Files are not locally stored, and packets can be inspected as they are forwarded through the gateway. Packets still have to go through a TCP proxy because TCP streams have to be reassembled and packets must be reordered.
- ExpressAV cannot detect polymorphic or metamorphic viruses. These viruses can change themselves, and the engine utilizes pattern recognition only and does not use other heuristics to detect these types of viruses.
- Compressed file detection is only supported for HTTP and POP3, and files compressed multiple times are not supported.
- ExpressAV minimizes transfer delays as packets can be forwarded while the scan is taking place (see Figure 3).
- At the time of writing, over 10,000 signatures are included, most of which are either dangerous or current viruses.

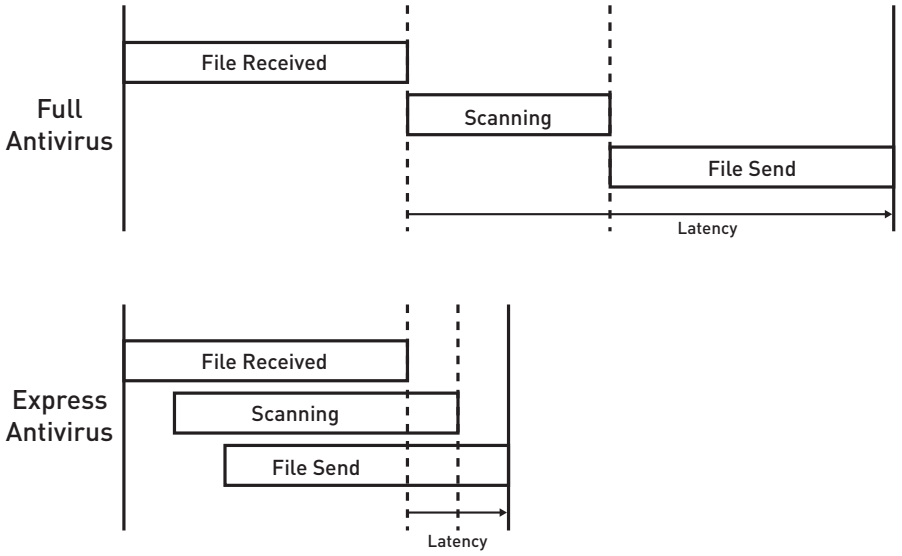

Figure 3: Transfer latency comparison

Configuration

Antivirus is part of the UTM feature set, and security policies act as the central point of control for all traffic forwarded by the gateway, as is the case with other UTM features. A security policy is used to associate a UTM policy with particular traffic, and the UTM policy specifies which parameters are used to scan traffic.

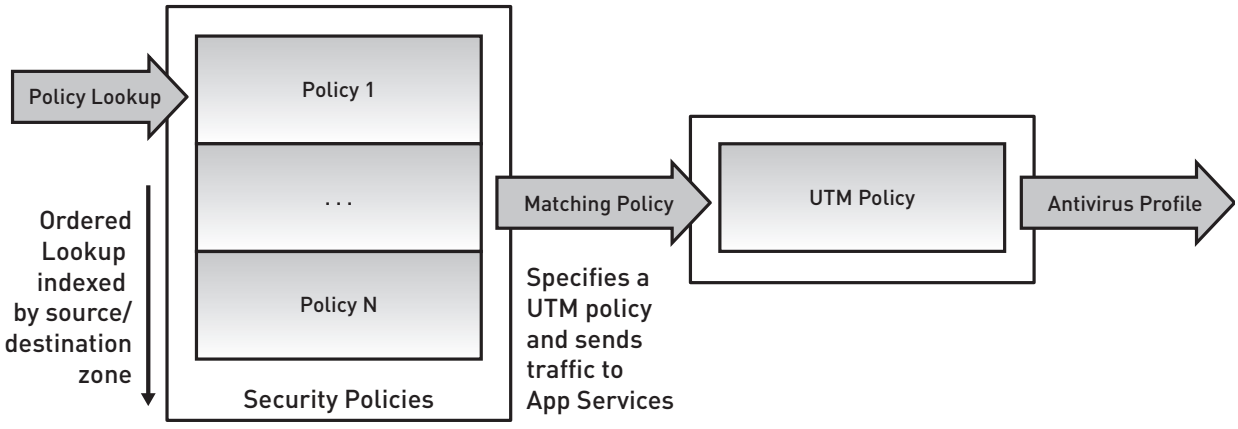

Figure 4: UTM policies

In a similar fashion, a UTM policy ties a set of protocols to one or multiple feature profiles. Each profile determines the specific configuration of each feature (antivirus, content filtering, antispam, and Web filtering). This document focuses on antivirus, so the UTM policies shown in the examples only reference antivirus profiles.

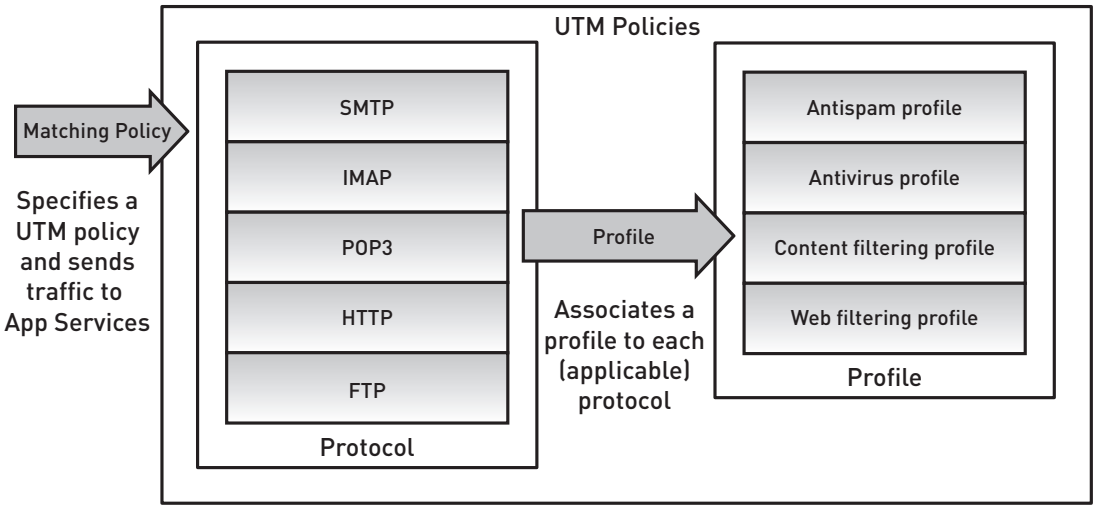

Figure 5: UTM policies and feature profiles

The antivirus configuration hierarchy is found under [security utm feature-profile] as shown in the following:

```
security {
        utm {
          feature-profile {
             anti-virus {
              type juniper-express-engine | kaspersky-lab-engine;
               mime-whitelist {
                 exception <MIME exception list>;
                 list <MIME list>;
              }


               url-whitelist <url whitelist>;
              juniper-express-engine {
                pattern-update {
                   email-notify {…}
                   interval <update check interval in minutes>;
                   no-autoupdate;
                   url <database server url>;
                 }
                profile <profile name> {
                    fallback-options  {…}
                    notification-options  {…}
                    scan-options {…}



                 trickling [<trickling timeout>];
                 }
                }
                kaspersky-lab-engine {
                  pattern-update {
                     email-notify {…}
                     interval <update check interval in minutes>;
                     no-autoupdate;
                     url <database server url>;
```

```
 }
 profile <profile name> {
   fallback-options  {…}
   notification-options  {…}
   scan-options {…}
   trickling [<trickling timeout>];
 }
}
```

Global Options

When configuring either scanning option, certain configuration parameters are common to both. Administrators have the option of identifying certain file types that are not considered harmful and subsequently not scanned. In the case of HTTP, the MIME headers can be used to obtain information about the file type being carried. The mime-whitelist is used to indicate the MIME types that do not need to be scanned. It is also possible to configure an exception list, indicating more specific MIME types that must be scanned even if their type is included in the mime-whitelist. For example, you can define a mime-whitelist that does not scan video files—except for Windows Media files—by creating a mime-whitelist with MIME type "video/" and an associated exception list for MIME type "video/x-ms-wmv."

Figure 6: HTTP traffic processing

On an SRX Series device or a J Series router, you can also create a list of trusted sites, files, or embedded scripts that does not require scanning. The url-whitelist provides this functionality by allowing administrators to list safe or permitted sites.

- Pattern update options (found under the juniper-express-engine or the kaspersky-lab-engine configuration hierarchy) allow for control of the antivirus engine and signature database updates as follows:
- no-auto-update: This option disables automatic download and update of the antivirus engine and signature database. Because the downloading of a new database is traffic disruptive, users can also choose to bypass the scan engine while the database is being upgraded.
- interval: This option specifies how often the database server is queried for a new version of the database.
- url: This option allows users to specify the URL of the database server. If no URL is specified, a default is provided, which is the recommended configuration.

MIME, URL whiteliest, and pattern update options are global, which means that they are not attached to a particular antivirus profile and all profiles will inherit these settings. The remaining options are antivirus profile specific and are configured on a per-policy or per-protocol basis.

Per-Policy and Protocol Options

Fallback options control the actions (either block or permit) an SRX Series device or a J Series router takes when traffic cannot be scanned because of special conditions—for example, when the file size exceeds the maximum allowed or when the database is being loaded.

Notification options are used to inform users of detected viruses; blocked traffic due to a fallback action; or permitted, but unscanned traffic. For HTTP and FTP, notifications are piggybacked in the protocols. For example, if a virus is found while doing an HTTP request, users will see a custom error message on the page they are trying to access. Mail protocols, SMTP, IMAP, and POP3 will instead generate an error mail message notifying the mail recipient—and optionally the sender—of the offending mail.

Scan options control the different scan engine options, which are specific as can be seen in Table 1.

Table 1: Scan Options

Option	Kaspersky Lab Engine	Juniper Express Engine
Content size limit	yes	yes
Intelligent pre-screening	yes	yes
Timeout	yes	yes
Scan mode/scan extension	yes	no
Decompress layer limit	yes	no (only one compression level is supported)

The content size, timeout, and the decompress layer limit control the maximum file size, time (in seconds), and nested compressions after which the engine will either drop or forward the file based on the fallback options.

Intelligent pre-screening is used to improve performance and lower forwarding delay by allowing the engine to determine if a file may contain malicious code by inspecting a few initial packets before the engine receives the whole file. If the file is deemed safe, scanning is bypassed, and the file is forwarded.

When the scan mode is set to "all," the engine scans every file regardless of its extension. In contrast, scan mode by extension allows administrators to specify a list of file extensions to be scanned.

Configuration Examples

This section starts with some simple deployment scenarios and builds on them to show the capabilities of the Junos OS antivirus feature. All of the examples are based on the following reference network:

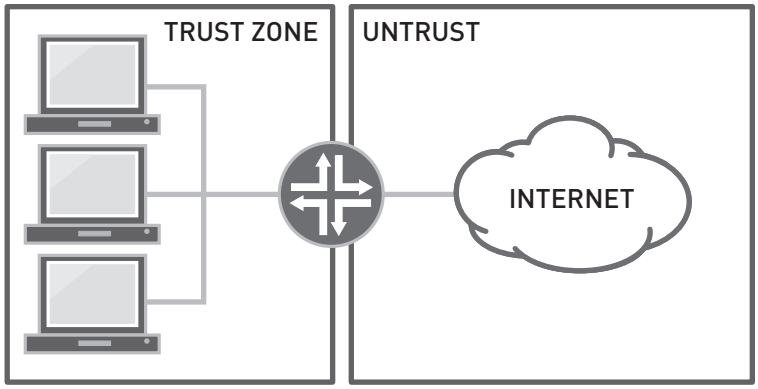

Figure 7: Reference network

Using the Juniper Default Configuration

This first example is a simple configuration where the Kaspersky full antivirus engine is used to scan for malicious code in sessions originating in the trust zone destined for the Internet—part of the untrust zone.

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

```
        }
    }
}
}
utm {
feature-profile {
    anti-virus {
        type kaspersky-lab-engine;
    }
}
```

```
utm-policy default-av {
    anti-virus {
        http-profile junos-av-defaults;
        ftp {
            upload-profile junos-av-defaults;
            download-profile junos-av-defaults;
        }
        smtp-profile junos-av-defaults;
        pop3-profile junos-av-defaults;
        imap-profile junos-av-defaults;
    }
       }
}
```

The first configuration makes use of the Junos OS default antivirus profile. The default configuration for the profile can be shown by typing, "show groups junos-defaults security utm feature-profile anti-virus kaspersky-lab-engine" from the command-line interface (CLI) in edit mode.

```
profile junos-av-defaults {
    fallback-options {
        default log-and-permit;
        corrupt-file log-and-permit;
        password-file log-and-permit;
        decompress-layer log-and-permit;
        content-size log-and-permit;
        engine-not-ready log-and-permit;
        timeout log-and-permit;
        out-of-resources log-and-permit;
        too-many-requests log-and-permit;
    }
    scan-options {
        intelligent-prescreening;
        scan-mode all;
        content-size-limit 10000;
        timeout 180;
        decompress-layer-limit 2;
    }
    notification-options {
        virus-detection {
            type message;
            notify-mail-sender;
            custom-message "VIRUS WARNING";
        }
        fallback-block {
            type message;
            notify-mail-sender;
```

```
        }
    }
}
```

A user trying to download an infected file will be presented with the following message, and the download will be blocked:

```
VIRUS WARNING
   88.198.38.136:80->10.1.1.11:42652 Download
   contaminated file: www.eicar.org/download/eicar.com
   with virus EICAR-Test-File
```

The default profile can also be used with the Juniper ExpressAV engine and can be configured as follows:

```
policy {
from-zone trust to-zone untrust {
    policy match-all {
        match {
            source-address any;
            destination-address any;


application any;
        }
        then {
            permit {
                application-services {
                    utm-policy default-av;
                }
            }
        }
    }
       }
}
utm {
    feature-profile {
        anti-virus {
            type juniper-express-engine;
        }
    }
    utm-policy default-av {
        anti-virus {
            http-profile junos-eav-defaults;
            ftp {
                upload-profile junos-eav-defaults;
                download-profile junos-eav-defaults;
            }
            smtp-profile junos-eav-defaults;
            pop3-profile junos-eav-defaults;
            imap-profile junos-eav-defaults;
        }
    }
}
```

Changing the Default Automatic Database Upgrade

The default configuration of the Kaspersky engine checks for database updates every hour. By default, if a database upgrade is in process while traffic needs to be inspected, the scan engine will permit the traffic and generate a log message displaying the traffic endpoints, an error message, and the name of the file (or URL in case of an HTTP request).

```
Jan 21 08:42:39 172.19.101.42 RT_UTM: AV_SCANNER_ERROR_SKIPPED_MT: AntiVirus: Content from
88.198.38.136:80 to 10.1.1.11:42659 www.eicar.org/anti_virus_test_file.htm was not scanned
because scan-engine error or constraint with code 14 for scan engine is not ready.
```

In this example, the default configuration will be modified to drop traffic when a new database is being loaded. Also, in order to reduce traffic disruption, the database will be upgraded at most once a day by modifying the frequency of the update checks. While a database upgrade is in process, users will receive a notification message asking them to retry the operation in a few minutes.

```
policies {
    from-zone trust to-zone untrust {
        policy match-all {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit {
                    application-services {
                        utm-policy av;
                    }
                }
                       }
        }
    }
}
utm {
    feature-profile {
        anti-virus {
```

```
type kaspersky-lab-engine;
            kaspersky-lab-engine {
                pattern-update {
                    interval 1440;
                }
                profile drop-on-error {
                    fallback-options {
                        default log-and-permit;
                        engine-not-ready block;
                    }
                    notification-options {
                        fallback-block {
                            custom-message “File dropped due to db upgrade, please retry in a
few minutes”;
                        }
                    }
                }
            }
```

```
        }
    }
    utm-policy av {
        anti-virus {
            http-profile drop-on-error;
            ftp {
                upload-profile drop-on-error;
                download-profile drop-on-error;
            }
            smtp-profile drop-on-error;
            pop3-profile drop-on-error;
            imap-profile drop-on-error;
        }
    }
}
```

With the previous configuration, a user trying to access a Web page will see the following notification message during an upgrade:

```
Request was dropped

   File dropped due to db upgrade, please retry in a few minutes
   88.198.38.136:80->10.1.1.11:42687 Download request was dropped due to AV scan engine not
ready.
And administrators will still receive a syslog message indicating that some data was dropped.
```

```
Jan 21 09:05:59 172.19.101.42 RT_UTM: AV_SCANNER_DROP_FILE_MT: AntiVirus: Content from
88.198.38.136:80 to 10.1.1.11:42687 www.eicar.org/anti_virus_test_file.htm was dropped because
 scan-engine error or constraint with code 14 for scan engine is not ready.
```

Excluding Selected File Types

Since some file types are not inherently harmful, it is sometimes safe to allow certain file types to bypass the scan engine based on the extension and MIME type. (This would increase performance, at the expense of lower security). The previous example will be updated to allow files with MIME type of text/ to bypass the scan engine, while files of type text/html will be scanned.

Note: The following is an example only and not a security strategy that Juniper recommends. Security strategies are deployment specific and the trade-off between performance and security must be considered on an individual basis.

```
policies {
    from-zone trust to-zone untrust {
        policy match-all {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
```

```
permit {
                    application-services {
                        utm-policy av;
                    }
```

```
                }
                log {
                    session-init;
                    session-close;
                }
            }
        }
    }
}
utm {
    custom-objects {
        mime-pattern {
            bypass {
                value text/;
            }
            force {
                value text/html;
            }
        }
    }
    feature-profile {
        anti-virus {
            mime-whitelist {
                list bypass;
                exception force;
            }
            type kaspersky-lab-engine;
            kaspersky-lab-engine {
                pattern-update {
                    interval 1440;
                }
                profile bypass-text {
                    fallback-options {
                        default log-and-permit;
                        engine-not-ready block;
                    }
                    notification-options {
                        fallback-block {
                            custom-message “File dropped due to db upgrade, please retry in a
few minutes”;
                        }
                    }
                }
            }
        }
    }
    utm-policy av {
        anti-virus {
            http-profile bypass-text;
            ftp {
                upload-profile bypass-text;
                download-profile bypass-text;
            }
            smtp-profile bypass-text;
            pop3-profile bypass-text;
            imap-profile bypass-text;
        }
    }
}
```

Updating the Antivirus Database

The antivirus database can be manually upgraded using the following operational mode command:

```
>request security utm anti-virus [kaspersky-lab-engine|juniper-express-engine] pattern-update
```

You can view database update results by issuing the following command:

```
>show security utm anti-virus status
 UTM anti-virus status:

    Anti-virus key expire date: 2009-11-21
    Update server: http://update.juniper-updates.net/AV/SRX210/
           Interval: 1440 minutes
           Pattern update status: next update in 1438 minutes
           Last result: already have latest database
    Anti-virus signature version: 01/20/2009 04:33 GMT, virus records: 488620
    Anti-virus signature compiler version: N/A
    Scan engine type: kaspersky-lab-engine
    Scan engine information: last action result: No error(0x00000000)
```

Operational-mode commands are also provided to delete the database, which is useful to free up space if antivirus use is discontinued or to force a database reload as seen in the following. (Database reloads are helpful for testing notification messages.)

```
>request security utm anti-virus [kaspersky-lab-engine|juniper-express-engine] pattern-delete
>request security utm anti-virus [kaspersky-lab-engine|juniper-express-engine] pattern-reload
```

Monitoring

The status of the antivirus engine can be seen with the "show security utm anti-virus status" command, as shown in the following. Counters are provided, which show protocol parsing and scanning information.

```
>show security utm anti-virus statistics
 UTM Anti Virus statistics:

 Intelligent-prescreening passed:      0


 MIME-whitelist passed:                1
 URL-whitelist passed:                 0
 Forwarded to scan engine:             13

 Scan Mode:
     scan-all:                         13
     Scan-extension:                   0

 Scan Code:
     clear:                            6
     Infected:                         7
     Password files                    0
     Decompress layers:                0
     Corrupt files:                    0
     Out of resources:                 0
     Internal errors:                  0
```

```
 Fall back:                       log-and-permit           block
     Engine not ready:                         2             2
     Password file:                            0             0
     Decompress layer:                         0             0
     Corrupt files:                            0             0
     Out of resources:                         0             0
     Timeout:                                  0             0
     Maximum content size:                     0             0
     Too many requests:                        0             0
     Others:                                   0             0
```

It is sometimes useful to verify that traffic is indeed being processed by the correct security policy (the policy where the UTM profile is applied). The "show security flow session" command examines the session table and verifies which policy is processing specific traffic.

```
Session ID: 3686, Policy name: match-all/6, Timeout: 4


In: 10.1.1.11/42756 --> 88.198.38.136/80;tcp, If: fe-0/0/5.0
  Out: 88.198.38.136/80 --> 172.19.101.42/1090;tcp, If: ge-0/0/0.0
            …
```

Licensing

A license is required to enable the antivirus feature, regardless of the engine used. Installed licenses can be displayed with the "show system license" command.

```
pato@SRX210-1# run show system license
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  av_key_kaspersky_engine               1            1           0    2009-11-20 00:00:00 UTC
  anti_spam_key_symantec_sbl            0            1           0    2009-11-20 00:00:00 UTC
  wf_key_surfcontrol_cpa                0            1           0    2009-11-20 00:00:00 UTC
  idp-sig                               0            1           0    2009-11-20 00:00:00 UTC
…
```

Summary

The antivirus feature introduced in Junos OS Release 9.5 for SRX Series Services Gateways and J Series Services Routers provides an effective defense against viruses, trojans, rootkits, and worms. Although this has been a common firewall feature for many years, it still remains an integral part of any security strategy by stopping malware at the gateway before even reaching the endpoint.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

3500158-002-EN May 2010