

# *Juniper Networks*

## *Embedded Gateway Anti-Virus Solutions*



Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
408 745 2000 or 888 JUNIPER  
[www.juniper.net](http://www.juniper.net)

## Embedded Gateway Anti-Virus Solutions

### Gateway Anti-Virus (Juniper-Kaspersky / Trend)

Remote sites and branch offices that are able to directly access the Internet can easily be infected with viruses directly downloaded to user desktops. Anti-Virus enabled at the gateway in remote sites and used in conjunction with desktop Anti-Virus help mitigate these risks. With embedded Anti-Virus enabled on Juniper Networks firewall/VPN solutions, organizations are able to protect all the entry points in the network against malicious threats and network attack.

With the release of ScreenOS 5.3, customers can choose between two different Anti-Virus vendors as their gateway solution embedded directly into Juniper’s Firewall/VPN solutions. Embedded Anti-Virus enables customers to extend virus protection from the corporate headquarters gateway down to remote sites or branch offices.

The two different solutions require two different versions of ScreenOS 5.3 – one that supports the Juniper-Kaspersky AV solutions and one for the Trend solution. The Juniper-Kaspersky Anti-Virus engine provides a number of features and benefits beyond the Trend solution by offering the ability to stop inbound, spyware, keylogging, adware and phishing as well as configurable scanning options. The Trend Anti-Virus engine does not have this additional capability.

The differences between the two solutions are highlighted below:

	Juniper-Kaspersky	Trend
Embedded in ScreenOS 5.3	Yes	Yes
Protocols Supported	SMTP, POP3, Webmail, FTP, IMAP and HTTP	SMTP, POP3, Webmail, FTP, IMAP and HTTP
Granular AV Policies	Yes	Yes
Configurable Scanning Level	Yes	No
Inbound Spyware/Adware/Keylogger Protection	Yes - Inbound	No
Platform Support	HSC, 5GT (ADSL & WLAN)	HSC, 5GT (ADSL & WLAN)

### Configurable Scanning Options (Juniper-Kaspersky Engine Only)

The Juniper-Kaspersky solution also provides three levels of scanning for end-user flexibility. This feature is not available on the Trend Anti-Virus solution.

- **Standard:** The default and recommended option – gives the highest coverage with the lowest false positive rate (includes spyware as well)
- **In-The-Wild:** Less coverage than standard – offers higher performance by only looking for “in-the-wild” viruses (i.e. does not scan for many of the less frequently seen viruses)
- **Extended:** Adds some of the traditionally more noisy pieces of adware to the scan

The Anti-Virus updates are automatic and update as often as required. Updates are dependent on the creation and proliferation of new or modified (variant) virus. The virus signatures update dynamically and are independent of the operating system, so therefore, no system reboot is required when updating.

### Gateway Anti-Spyware (Juniper-Kaspersky Engine Only)

Spyware is any technology that aids in gathering information about a person or organization without their knowledge. Spyware installs tracking software on your system, which is continuously “phoning home”, using your Internet connection, and reporting statistical and personal data about you. Spyware can be installed via a virus,

installation of a program, P2P programs (Kazaa) or visiting a website (ActiveX) etc. The purpose of some Spyware is merely to force a user to visit a web site of the hijacker's choice so that they can artificially inflate their web site's traffic for higher advertising revenues. Typically, the browser settings are hijacked forcibly by malicious code that can sometimes modify your default home and search pages. Sometimes internet shortcuts may be added to your favorite's folder without your knowledge. Other types of Spyware will harvest sensitive information such as credit card or bank account information.

In some cases, the changes made by some forms of Spyware are reversible simply by going into the browser settings and switching them back. For more pervasive Spyware, sometimes it will be necessary to edit the windows registry to undo any changes made. More complex Spyware infections usually leave a combination of registry setting and files clandestinely placed on your computer and restore themselves every time the system is rebooted – making it very difficult to eradicate.

Less malicious types of Spyware are often called “advertising supported” software (adware) and are usually installed during the installation of a program, such as downloaded music or shareware applications.

The Juniper-Kaspersky Anti-Virus solution prevents both spyware and adware from entering the enterprise network at the remote office gateway when the user is accessing the internet.

### Gateway Phishing Protection (Juniper-Kaspersky Engine Only)

Phishing is the deliberate deception of users (typically by email) by a malicious party to route them to “fake” Web site specifically engineered to harvest their personal or sensitive information. In many instances, the fake Web sites are exact replicas of the legitimate site. Phishing web sites are used to harvest credit card information and/or other personal information such as username, password, name, address and social security information that may aid in identity theft.

Phishing emails are detected inbound into the network from the internet. The Juniper-Kaspersky Anti-Virus engine looks within the content of an email for URLs of known phishing web sites. If a known URL is detected, the system blocks the email from being delivered to the recipient.

### Platform Support

The Juniper Networks NetScreen-5GT and the NetScreen-HSC are currently the only products offered by Juniper Networks that will be upgradeable to support integrated Anti-Virus for an additional fee. Customers using non-AV enabled NetScreen-5GTs can buy an AV upgrade SKU to enable AV. Anti-Virus functionality will be available on other platforms in the up and coming releases of ScreenOS.

AV Engine	Platform Support
AV (Juniper-Kaspersky)	HSC, HSC Plus, 5GT Family
AV (Trend)	HSC, 5GT Family

### Licensing

Content security subscriptions are a yearly service that entitles customers to download and utilize content security updates delivered by Juniper. Content security updates are delivered in the form of new pattern files or signature files or access to the latest lists and are updated frequently. Updates provide protection against newly discovered security threats.

License keys are required to activate a content security subscription on a device. A valid license key is required on each device for each subscription. A license key is unique to a device serial number and is valid for a specific period of time - typically one year.