

Juniper Networks ScreenOS 6.0 Frequently Asked Questions

Product Marketing Manager: Andrew Maguire
Product Manager: Abby Hassel



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Juniper Networks NetScreen ScreenOS 6.0 Frequently Asked Questions

Q: What is ScreenOS?

A: ScreenOS is the underlying operating system for Juniper Networks integrated Firewall/IPSec VPN solutions. ScreenOS contains the functionality required to implement network security policies including firewall access control, VPN encryption, and traffic management. It provides the user interfaces and tools for device configuration, management and monitoring.

Q: What are the major enhancements in ScreenOS 6.0?

A: ScreenOS 6.0 is the next major release of Juniper's purpose-built operating system. The new features and major enhancements of this release can be put into the following categories.

Hardware Support

- 16-port 10/100/1000 Ethernet PIM
- Synchronous Serial mini-PIM for SSG 20
- E-3 Support
- 8-port 10/100/1000 Ethernet PIM
- 6-port GE SFP PIM
- 1-port GE SFP mini-PIM for SSG 20
- ADSL2/2+ PIM
- G.SHDSL PIM

Virtual Private Network (VPN)

- AutoConnect-VPN (AC-VPN)
- Screen on Tunnel Interface

Firewall

- WebUI Enhancements
- FTP Get/Put Service Enhancement
- Automatic data gathering

Universal Threat Management

- Antivirus scanning for Instant Messaging (IM) Services
- AV HTTP Trickling Enhancement

IDP Enhancements

- IDP Recommended Action:
- IDP inspection of GTP and GRE-encapsulated traffic
- IMSI information in NSM logs
- IDP Detector.s0 has been updated to IDP 4.0
- DSCP marking based on IDP action:

Authentication Service Enhancements

- Add user IP address to authentication logs
- Support TACACS+ authentication servers
- Prioritize authentication between external server and local database

- Increase number of permitted administrator IPs
- Enhanced RADIUS features

Virtual System Enhancements

- Increase in the number of virtual systems on the ISG Series
- Increase in Virtual System name space to 20 characters

Routing and Networking

- DIP Pool Enhancement
- NSRP Dynamic Route Synchronization

Layer 2 Transparent Mode

- VLAN Retagging

UAC

- Infranet Authentication

Feature Extensions

- IPv6
- Jumbo Frames
- Bridge Groups for built-in Ethernet ports of ISG-1000, ISG-2000 SSG 140
- DHCP Relay Flow
- Layer 2 VSYS
- Management IP Address limit increased
- PPU Enhancement
- DSCP Enhancement
- Universal Serial Bus (USB) Support
- Coredump to USB Port

ScreenOS 6.0 Availability

Q: When will ScreenOS 6.0 be generally available?

A: ScreenOS 6.0 will be generally available for download from the Juniper Networks' customer support site on April 17th, 2007. ScreenOS 6.0 will be available at no additional charge to customers with an existing support contract for their product, or to customers who are under the 90-day software term for Product Warranty.

Platform Support

Q: Are there any platforms that will not be able to run ScreenOS 6.0?

A: Yes. The NetScreen-5XT, NetScreen-5GT Family, NetScreen-25/50, NetScreen-500 and NetScreen-5000 with 1st generation Secure Port Modules cannot be upgraded beyond ScreenOS 5.4.

Q: Can I deploy the ISG Series IDP Security Modules with ScreenOS 6.0 for both the ISG 1000 and ISG 2000?

A: Yes, the IDP Security modules for the ISG1000 and ISG2000 are now fully integrated into mainline ScreenOS.

Q: What platforms are supported in ScreenOS 6.0?

A: The following table defines the platform support for ScreenOS 6.0

Products	ScreenOS 6.0
Juniper Networks NS-HSC	No
Juniper Networks NS-5GT / 6T ADSL	No
Juniper Networks NS-5GT Wireless	No
Juniper Networks NS-5XT	No
Juniper Networks SSG 5	Yes
Juniper Networks SSG 20	Yes
Juniper Networks NS-50/25	No
Juniper Networks NS-208/204	No
Juniper Networks NS-500	No
Juniper Networks SSG 520	Yes
Juniper Networks SSG 550	Yes
Juniper Networks ISG 1000	Yes
Juniper Networks ISG 1000 with IDP	Yes
Juniper Networks ISG 2000	Yes
Juniper Networks ISG 2000 with IDP	Yes
Juniper Networks NS-5000	No
Juniper Networks NS-5000 with 2nd Gen SPM's / MGT2	Yes*(Previously ScreenOS 5.0r6)

Hardware Support

Q: Which platforms support the new 16-port Gigabit Ethernet Universal PIM (uPIM)?

A: The 16-port 10/100/1000 Ethernet universal physical interface module (uPIM) is supported on the SSG 140 and SSG 500 series security devices. This uPIM provides connectivity to copper-based gigabit Ethernet LANs and also supports up to eight bridge groups, which let you group several Ethernet interfaces together.

Q: What are bridge groups (bgroups)? Are they supported on all platforms?

A: Bridge groups (bgroups) are supported on the SSG 5, SSG 20 and SSG 140 platforms, in addition to the ISG 1000 and ISG 2000. Bgroups are the exciting new alternative to port modes and consist of a logical interface with a single IP/subnet that can house a mix of physical Ethernet and wireless interfaces. In essence, a bgroup is creating a mini-switch on the supported devices.

Q: Which platforms support the new Synchronous Serial mini-PIM

A: The Synchronous Serial mini Physical Interface Module (mini-PIM) is supported on the SSG 20 security device and provides connectivity to Serial network media types. Its dedicated network processor forwards traffic to the SSG 20 CPU where traffic decisions are made based upon the security policy.

Q: Do the SSG 500 Series FW/VPNs now support E-3?

A: Yes, ScreenOS 6.0 now provides support for the E3 PIM on the SSG 500 series platforms.

Q: Which platforms support the new 8-port Gigabit Ethernet Universal PIM (uPIM)?

A: The 8-port 10/100/1000 Ethernet universal physical interface module (uPIM) is supported on the SSG 140 and SSG 500 series security devices. The new PIM provides connectivity to copper-based gigabit Ethernet LANs. This PIM also supports up to four bridge groups, which let you group several Ethernet interfaces together.

Q: Which platforms support the new 6-port SFP Gigabit Ethernet Universal PIM (uPIM)?

A: The 6-port small form factor pluggable (SFP) universal physical interface module (uPIM) is supported on the SSG 140 and SSG 500 series security devices and provides connectivity to fiber-based and copper-based gigabit Ethernet LANs.

Q: How many bridge groups does the 6-port GE SFP uPIM support?

A: The 6-port GE SFP uPIM supports up to three bridge groups (bgroups), which let you group several Ethernet interfaces together.

Q: Which platforms support the new 6-port 1-port GE SFP mini-PIM?

A: The single port small form factor pluggable (SFP) mini physical interface module (mini-PIM) is supported on the SSG 20 security device and provides connectivity to fiber-based and copper-based gigabit Ethernet LANs.

Q: Which platforms support the new ADSL2/2+ PIM?

A: The 1x ADSL2/2+ PIM (Annex A or Annex B) is now supported on the SSG 140, SSG 520/550, and the SSG 520M/550M platforms.

Q: What are the DTM standards supported by the ADSL2/2+ PIM?

A: The two discrete multitone (DTM) standards supported are:

- **ITU 992.3** (also known as ADSL2), which supports data rates up to 1.2 Mbps upstream and 12 Mbps downstream.
- **ITU 992.5** (also known as ADSL2+), which supports data rates up to 1.2 Mbps upstream and 24 Mbps downstream.

Q: What features and functionality does the G.SHDSL PIM provide?

A: The G.symmetric high-speed digital subscriber line (G.SHDSL) PIM supports multi-rate, high-speed, symmetrical digital subscriber line technology for data transfer between single customer premises equipment (CPE) subscriber and a central office (CO).

Q: What are the DTM standards supported by the G.SHDSL PIM?

A: ScreenOS 6.0 supports the **ITU G.991.2**, single-pair High-speed Digital Subscriber Line (SHDSL) Transceiver discrete multitone (DTM) standard.

Virtual Private Network (VPN)

Q: What is the AutoConnect VPN feature added in ScreenOS 6.0?

A: AutoConnect-Virtual Private Network (AC-VPN) enables spokes in a hub-and-spoke VPN network to dynamically create VPN tunnels directly between each other as-needed.

Q: What benefits does AutoConnect VPN provide?

A: AutoConnect-VPN addresses issues of latency between spokes, in addition to reducing processing overhead on the hub and thus improves overall network performance. Because AC-VPN creates dynamic tunnels that time out when traffic ceases to flow through them, network administrators are freed from the time-consuming task of maintaining a complex network of static VPN tunnels.

Q: Why is tunnel screening important?

A: ScreenOS 6.0 now supports screens to tunnel interfaces. This allows traffic exiting tunnels to be examined before and after encryption.

Firewall

WebUI Enhancements

The Web-based User Interface (WebUI) is improved to optimize work flow, display diagnostic information, enhance the Home page, and categorize the menu options.

FTP Get/Put Service Enhancement

This feature redefines the FTP-Put and FTP-Get service definitions used in firewall policies. In prior ScreenOS releases, FTP-Put and FTP-Get were configured together with different actions in a policy and service groups. In ScreenOS 6.0 however, if you configure FTP-PUT permit and FTP-GET deny in a policy together, the action will always be deny.

Automatic data gathering

This feature is a basic looping script consisting of **get** commands that run in a background process, saving the output to a FIFO file in the flash. You may record any series of commands to gather information in the background.

Universal Threat Management

Q: Why is embedded Antivirus so important?

A: Embedded antivirus will enable customers to extend gateway virus protection to remote sites. For instance, if remote sites are able to directly access the Internet, then files with viruses could be directly downloaded to user desktops without going through the central site. With embedded antivirus, organizations will be able to protect all the entry points in the network. Moreover, the virus infection could also be initiated from a remote site and then propagate through the network. With antivirus enabled at the gateway in remote sites and used in conjunction with desktop antivirus, these risks could be mitigated.

Q: What new Antivirus features have been added in ScreenOS 6.0?

A: ScreenOS 6.0 now supports antivirus scanning for P2P messaging services: AIM, ICQ, Yahoo! Messenger, and MSN Messenger. AV scanning is supported for text/group chat messages, and file transfer/file sharing.

Q: What IM client versions and protocols are supported?

A: The following versions of the IM Client and protocol are fully supported. Forward compatibility on later versions of the IM client and protocol are supported on the basis of best effort.

IM Client and Version#	Supported Protocol and version
------------------------	--------------------------------

AIM Triton 1.0.4 to 1.3.30.1 AIM 5.9.3861 to 5.9.6089 ICQ 5.04 to 5.1	OSCAR version 4 Talk to Oscar (TOC) version 4
Yahoo! Messenger 5.5.1228 (v8.0.0.506 is supported as best efforts)	Yahoo Messenger Service Gateway Protocol (YMSG) version 8, 9, 10
MSN Messenger 7.0, 7.5 Live Messenger 8.0	Mobile Status Notification Protocol (MSNP) version 11, 12, 13

Q: Do I have to have certain memory requirements to use the new features in the embedded Antivirus?

A: Platforms require a high-memory option to run AV scanning. Platforms supported are the SSG 5, SSG 20, SSG 140, SSG 520/520M, and SSG 550/550M.

Q: What is Antivirus HTTP Trickling?

A: This feature enhancement is important for low-speed links. It allows you to configure time-based thresholds to send bits through the firewall to prevent browser timeouts while the data is being scanned by the internal AV engine

Q: Do the embedded content security options run on the high end platforms?

A: High end FW/VPN platforms such as the ISG and NetScreen 5000 Series FW/VPN are typically deployed in higher performance networking environments and are usually assigned significantly different roles than the low to mid-range platforms. A sub-set of embedded content security features are available to them - IPS (Deep Inspection) for example, or various hardware upgrade options (such as the IDP Security Modules for the ISG 1000 and ISG 2000).

Q: What products can support the Juniper-Kaspersky integrated antivirus?

A: The Juniper-Kaspersky embedded Antivirus solution is available on the following platforms: HSC NS-5GT, SSG 5, SSG 20, SSG140, SSG 520/520M and SSG 550/550M.

Q: Is Antivirus functionality available on every Firewall/VPN platform?

A: No. Antivirus is available on many of the low and mid range platforms. With high end systems such as the ISG Series and NetScreen 5000 Series FW/VPN platforms, many customers prefer to offload CPU intensive operations such as content scanning to reduce any potential performance degradation. In these instances, iCAP antivirus redirection (see page xx) to a third party scanning solution allows some level of content security at the perimeter without impacting the throughput of the firewall.

Q: What Antivirus vendor options do I have when I deploy a content security enabled platform?

A: With ScreenOS 6.0, new customers will only have the option to enable the Juniper-Kaspersky embedded Antivirus solution. Existing customers that use the Trend can renew their license for another two years if they wish, however, once the renewal period has expired they will be required to transition to the Juniper-Kaspersky engine.

Q: Do I have to pay for the Antivirus feature in ScreenOS 6.0?

A: Yes, if you wish to enable the Antivirus feature on your firewall, you will be required to pay an annual subscription.

Q: Does the antivirus functionality require some type of client software in conjunction with the firewall/VPN or is it fully embedded?

A: No – in the case of embedded antivirus, the virus scanning is performed by the firewall. There is no need for additional software at the end-user PCs, however, a defense-in-depth approach to security is always recommended to minimize network risk.

Q: Is the pattern file actually stored on the device?

A: Yes. With embedded Antivirus, the pattern file is stored in flash memory (non-volatile memory)

Q: Is there a trial version available and where can I get it?

A: Yes, if you evaluate the Antivirus feature on your firewall, you may download a 30-day subscription from the following URL: <http://www.juniper.net/lcrs/mylic.do?methodToCall=setUpTrial>

Q: Can virus scanning be configurable for inbound and outbound traffic?

A: Yes. Virus scanning can be enabled for both inbound and outbound policies. For instance, virus scanning can be applied to traffic traveling to and from VPN tunnels, as well as to Internet traffic.

Q: How often do AV signatures need to be updated? Will it require an OS upgrade?

A: The AV updates are automatic and update as often as needed (daily, etc). 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.

IDP Enhancements

- **IDP Recommended Action:** You can now allow recommended actions in IDP rules. If you specify “recommended” as the action in a rule, the recommended action will be applied in cases where you do not specify an action in within a policy rule. If you specify an action within a policy rule, it will take precedence over the recommended action.
- **IDP inspection of GTP and GRE-encapsulated traffic:** The ISG 1000 and ISG 2000 with IDP Security Modules can now inspect traffic that is encapsulated in GPRS Tunneling Protocol (GTP) and Generic Routing Encapsulation (GRE).
- **IMSI information in NSM logs:** NSM IDP logs now contain International Mobile Subscriber Identity (IMSI) data on the IDP security devices. This information allows you to specifically identify the end user for threats and attacks that are detected during forensic evaluation using the provided subscriber-level identifiers.
- **IDP Detector.s0 has been updated to IDP 4.0:** The IDP 4.0 engine has been synced to ScreenOS 6.0. You can now manage ISG1000/ISG2000 with IDP from the same NSM console as IDP 4.0 standalone devices. You will now have the same detection capabilities on ISG1000/ISG2000 with IDP as you do on the standalone IDP 4.0 devices.
- **DSCP marking based on IDP action:** You can now change the DSCP marking of a packet based on IDP actions performed on ISG1000/2000 with IDP. Administrators now have the ability to change the QoS based on defined IDP rules.

Authentication Service Enhancements

ScreenOS authentication service provides the following enhancements:

- Add user IP address to authentication logs
- Support TACACS+ authentication servers
- Prioritize authentication between external server and local database
- Increase number of permitted administrator IPs
- Enhance RADIUS features
 - “Framed-pool” support (IP pool supplied by RADIUS server, not local device)
 - Customizable interface description
 - Called-Station-ID attributes for differentiated billing purposes

Virtual System Enhancements

Q: What are Virtual Systems in ScreenOS?

A: Virtual systems are used in environments where customers have multiple administrators and want to segment their network into different, secure environments. These virtual systems operate as independent firewalls, giving an administrator the ability to define specific policies, but no ability to affect any other virtual system policy.

Q: How long has VSYS technology been in FW/VPN platforms?

A: Juniper was the original pioneer of Firewall Virtual Systems in 2000, and have gone through many enhancements since. With the release of 6.0, ScreenOS now has enhanced the number of supported VSYS's on the ISG Series of FW/VPN, as well as extending the VSYS functionality while the device is in transparent mode.

Q: What are the new VSYS features in ScreenOS 6.0?

A: In ScreenOS 6.0, virtual systems have been further enhanced to allow the ISG 1000 and ISG 2000 security devices to support additional virtual systems. The ISG 1000 now supports up to 50 virtual systems (increased from 10 virtual systems) and the ISG 2000 now supports up to 250 virtual systems (increased from 50 virtual systems).

Q: Do I have to install a new license for the VSYS increases on the ISG Series FW/VPN?

A: To take advantage of these increases in virtual system support, you must install a new license key.

Q: What other VSYS features were added in ScreenOS 6.0?

A: Virtual System names can now contain up to 20 characters. Previously, virtual system names could contain up to 10 characters.

Q: What is the new VSYS transparent mode support in ScreenOS 6.0?

A: Regular transparent devices do not typically support virtual systems, however, ScreenOS 6.0 permits administrators of ISG-2000 and NS-5000 with MGT2 and 8G2 modules the ability to create virtual systems (VSYS) while in transparent mode, significantly easing virtual system deployment and network integration challenges.

Layer 2 Transparent Mode

Q: What is VLAN Retagging and why is it important?

A: VLAN retagging provides a way to selectively screen VLAN traffic. You place a security device in parallel with your Layer 2 switch, and configure the switch to direct to the security device only traffic from VLANs you want screened. Traffic to and from your other VLANs meanwhile passes directly through the switch, thus avoiding any impact to throughput that might be caused by passing all VLAN traffic through the security device.

UAC

Q: What is the Juniper Networks Enterprise Infranet Solution?

A: The Juniper Networks Infranet solution provides end-point authentication and integrity, validating users and applications that access the network. Juniper Networks NetScreen devices and an Infranet Controller work together to provide granular, context-specific end-point security and firewall services to connect end users to protected resources. An end user running an Infranet Agent communicates with the Infranet Controller over HTTPS (HyperText Transfer Protocol-Secure) using SSL (Secure Socket Layer) to encrypt the transfer of authentication data. Once authenticated, the user connects to the NetScreen device through a policy configured by the Infranet Controller. When the end user logs out the policy is removed from the NetScreen device.

Q: What new feature was released in ScreenOS 6.0 to further enhance UAC?

A: The Infranet authentication includes the following enhancements:

- Visual display of Auth Table entries in the WebUI
- Additional actions field for Infranet Auth policies

This feature permits the Infranet Controller to control additional policy actions (AV, DI, logging, web filtering, and anti-spam) on a per-role basis. This allows you to make policy decisions such as activating AV for partners or untrusted machines, or turning on URL filtering for specific roles.

Q: Have any FW/VPN platforms been added as enforcement points for UAC in ScreenOS 6.0 ?

A: Yes. ScreenOS 6.0 enables platforms to act as Infranet Enforcer and includes the SSG 5/20, SSG 140, SSG 520/520M and SSG 550/550M, ISG 1000, ISG 2000 and NetScreen 5000 Series FW/VPN

Feature Extensions

ScreenOS 6.0 IPv6

Q: What is NetScreen ScreenOS 5.0.0-IPv6?

A: NetScreen ScreenOS 6.0-IPv6 includes a full IPv6 protocol stack, many transition mechanisms, and traditional networking, routing, and addressing features which enable customers to deploy these products in a production IPv6 or IPv6/IPv4 hybrid network today. The software provides “dual stack” functionality, which means that the software can secure both IPv4 and IPv6 traffic with a single software image on a single device.

Q: Which Juniper FW/VPN platforms will be able to support ScreenOS 6.0-IPv6 ?

A: In ScreenOS 6.0, IPv6 functionality is supported on the following FW/VPN platforms only.

- ISG1000
- NetScreen-5200
- NetScreen-5000 Series using 5000-M2 management module
- ISG1000: IPv6 cannot be used in conjunction with IDP modules
- ISG2000: IPv6 cannot be used in conjunction with IDP modules
- SSG 5 / SSG 20: IPv6 support available on Ethernet interfaces.

Note: IPv6 is not supported on wireless or WAN interfaces.

Q: How does Juniper’s IPv6 Security Support differ from the competition?

A: Juniper is the only company that can provide an integrated full Stateful Inspection firewall and IPSec VPN for IPv6 networks. Cisco recently announced availability of IPv6 in its IOS security routers, however, Cisco’s IOS routers are not feature comparable to NetScreen’s purpose built Stateful Inspection firewalls. Cisco has not yet delivered IPv6 in its PIX or Concentrator lines of security products.

Check Point can provide IPv6 support in its Stateful Inspection firewall, but they cannot provide support for their IPSec VPN.

The Juniper Networks integrated firewall/IPSec VPN security products also offer the most comprehensive set of transition mechanisms available on the market today. These will greatly reduce the cost and pain customers will face when transitioning from an IPv4 to IPv6 environment. Mechanisms such as “6 in 4” and “4 in 6” tunneling, “6 to 4” and “4 to 6” translation, and NAT-PTv6

offer customers the maximum choice and flexibility in easing that transition, depending on the characteristics of their networks.

Q: Is there a cost to upgrade?

A: ScreenOS 6.0-IPv6 is available at no cost to customers with current software subscriptions.

Q: What version of ScreenOS is the IPv6 software release based on?

A: This release of IPv6 code is based on ScreenOS 6.0 and has the same exact feature set as the ScreenOS 5.0.0-IPv6 release.

Q: Is the same feature set that currently exists in ScreenOS 6.0 available in the IPv6 software release?

A: No, the product does not have complete feature parity with IPv4 but it does include the most important features to secure a production IPv6 network today. Juniper Networks has worked very closely with many of our customers who are innovators in IPv6 and who represent several of a handful of companies actually offering IPv6 services today to prioritize and develop features according to their needs, such that our product could be deployed in working networks today.

Q: What are some of the main features NOT included in ScreenOS 6.0-IPv6 that are available in ScreenOS 6.0?

A: Following are some notable features which are not supported in this current IPv6 release:

- Deep Inspection
- BGP, OSPF, or IS/IS routing
- Transparent mode
- High Availability (NSRP) for IPv6
- Full SNMP MIBs
- Multicastv6

Q: Does this release of ScreenOS 6.0-IPv6 provide hardware acceleration of v6 packets?

A: No, this version of IPv6 is a software release only. Our currently shipping ASIC does not support IPv6 natively. However, when the firewall is running in dual stack mode, IPv4 traffic would still be hardware accelerated. Today none of the security vendors offer a hardware accelerated IPv6 firewall or VPN.

Q: Will there be NetScreen Security Manager (NSM) support of ScreenOS 6.0-IPv6?

A: Yes. NetScreen Security Manager 2007.1 has zero –day support for all new releases of ScreenOS.

Q: Are there any performance deviations from IPv6 and IPv4?

A: Sustained throughput for established IPv6 sessions is expected to be very similar to that of IPv4. There is some degradation of performance, depending on the packet size, however, that degradation is minimal in most cases (5% for large packets and 10 to 15% for small packets). In our initial deployment of IPv6, Juniper Networks expects that there will be more degradation in the session ramp rate, due to the lack of hardware acceleration in this release.

Q: What types of customers are interested in IPv6?

A: IPv6 is ideal for customers looking to install “greenfield” IPv6 networks or customers who are looking to migrate gradually from IPv4 to IPv6. Some organizations include Universities, telecommunications carriers and ISPs, government agencies, wireless 3G network providers, and online gaming providers.

Q: What does it mean to be ready for a production environment?

A: This product has the required features, quality, and support to be deployed in a real commercial network.

Q: Do the Juniper Networks IPv6 integrated firewall/IPSec VPN products work with Juniper's routers supporting IPv6?

A: Yes, the Juniper Networks firewall/IPSec VPN products do interoperate. Juniper Networks is unique, leading the industry with the most scalable IPv6 solutions for secure networking - from CPE to service provider edge and core. By using Juniper's routing and security products together, this reduces the deployment risk by having a single vendor tested, verified solution.

Feature Extensions

Jumbo Frames

Jumbo frames are supported on the ISG 1000 and ISG 2000 devices without IDP security modules. Jumbo frames are also supported on the NS-5000 series running MGT2 and SPM2 cards.

Bridge Groups for built-in Ethernet ports of ISG-1000, ISG-2000 SSG 140

Bridge groups (bgroups) let you group several Ethernet interfaces together. Starting with ScreenOS 6.0, the SSG 140 security device is preconfigured with three bgroups to which you can add the built-in Ethernet ports.

DHCP Relay Flow

No DHCP Relay: By default, ScreenOS relays DHCP request packets from all zones except the V1-Untrust zone and V1-DMZ zone. Enable this feature to prevent relay of DHCP request packets from a specified zone.

Layer 2 Vsys

Layer 2 Vsys is now supported on the Integrated Services Gateway (ISG) 1000, ISG 1000-IDP, the ISG 2000, ISG 2000-IDP, and the NetScreen-5000 series.

Management IP Address limit increased

The total number of IP addresses from which a security device can be managed is increased to 50 plus one times the number of Vsys. By making the number of manager IPs a function of the number of Vsys, memory is not wasted on low-end devices that require relatively few manager IPs, while high-end devices are not restricted to an artificially selected number.

PPU Enhancement

To increase throughput, tcp-syn-bit checking is now done in the Programmable Processing Unit (the ASIC), and supported on the NetScreen 5200 and NetScreen 5400.

DSCP Enhancement

Differentiated services code point (DSCP) marking is now supported on the Integrated Services Gateway (ISG) 1000 and ISG 2000 with IDP Security Modules and NetScreen 5200/5400.

Universal Serial Bus (USB) Support

USB ports allows file transfers such as device configurations, user certifications, and update version images between an external USB storage device and the internal flash storage. The USB functionality is available on the SSG devices.

Coredump to USB Port

ScreenOS supports full coredump file and full memory dump file transfers to the USB port on the SSG 5 Series and SSG 20 and USB ports/compact flash cards on the SSG 140 and SSG 500 series security devices.

Licensing

Q: What are content security subscriptions?

A: 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.

Q: What types of content security subscriptions does Juniper offer?

A: The table below represents the content security subscriptions that Juniper currently offers.

Type	Description
AV (Juniper-Kaspersky)	1 year subscription to Juniper-Kaspersky AV pattern file updates
Deep Inspection	1 year subscription to one of four Deep Inspection signature updates – Base, Server, Client and Worm
Web Filtering	1 year subscription to URL Filtering
Anti Spam	1 year subscription to anti spam subscriptions
Main Office Pack	1 year subscription to Juniper-Kaspersky AV + Deep Inspection + Web Filtering + Anti Spam
Remote/Branch Office Pack	1 year subscription to Juniper-Kaspersky AV + Deep Inspection + Web Filtering

Q: What are the packaged content security offerings?

A: Packaged content security offerings bundle two or more content security subscriptions. The Main Office content security pack targets small and medium sized companies that require AV, DI, Anti-spam and Web Filtering. The remote and branch office solution is targeted for large enterprises for use in their remote and branch offices. It includes AV, DI and Web-Filtering but not Anti-spam as customers do not typically need anti-spam in each branch/remote location.

Q: What are the benefits of these integrated offerings?

A: The packaged offerings are beneficial for customers and Juniper channel partners;

- The integrated offerings simplify the selling process
- The integrated offerings simplify the license life cycle management for subscriptions
- They enhances Juniper's market position in the emerging unified threat management market
- They create a price incentive for customers to buy the comprehensive package rather than individual subscriptions.
- There is a 30% reduction in price for the Main Office pack when compared to the sum of the individual subscriptions.
- There is a 25% reduction in Remote/Branch Office solution. This creates an incentive for customers to buy the integrated offering if they are looking to buy two subscriptions for a single device.

Q: How does licensing work for content security subscriptions?

A: 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). To activate a subscription on a device, customers should do the following:

- Purchase a license for the subscription/s for each device they want to use it on
- Register their device & subscription with Juniper
- Download a license key onto the device

Q: When can I purchase a subscription?

A: Subscriptions can either be purchased at the time of a new product order or can be purchased after product purchase. If a customer wants to buy a new device with subscriptions, they must purchase two SKU's – one for the device and one for the subscription.

Q: How are subscription orders fulfilled?

A: Orders for subscriptions are fulfilled via “authorization codes” delivered via email. Distributors will receive a copy of the email message by default. Distributors should provide a destination email address(es) where the authorization codes are to be sent (if they want it sent directly to VAR or end customer). If an order contains purchases for more than one end customer/VAR, each order line should contain one email address.

Q: What discounts do channel partners get for content security subscriptions?

A: Channel discounts for subscriptions = channel discount for product

Q: Do subscriptions have to be registered? If yes, how?

A: Subscriptions and the devices on which they run must be registered with Juniper before license keys can be generated. Juniper encourages VARs to register devices and subscriptions on behalf of end customers. If the VAR/Channel partner does not register on behalf of the end customer, it is their responsibility to inform the end customer to register the device and subscription. Products and subscription authorization codes can be registered at <http://tools.juniper.net/subreg/>

Q: What is the process if a large number of devices and subscriptions need to be registered?

A: For 20 or more devices and subscriptions registration, Juniper provides a bulk registration utility. This tool can be found at <http://tools.juniper.net/subreg/>. Customers or partners should create a text file (not excel) with device serial number, subscription authorization code and e-certificate number optional for registering support) and upload the file to register all the device/subscriptions specified in that file. Please note that a single file can register subscriptions for a single customer, single location and a maximum of 500 devices. For multiple customers, locations or greater than 500 units, multiple upload files should be used.

Q: How is the start and end dates of a subscription determined?

A: The start date of subscriptions is the date of registration of subscriptions with Juniper. The end date is equal to one (1) year from start date. Please note that multi-year SKUs are not currently available. If customers would like to purchase multiple year subscriptions, they can purchase multiple units of the subscription and register against the same device.

Q: How are license keys generated and installed on the device?

A: License keys can be retrieved directly from the Juniper device on which it runs. To generate and install license keys the following actions should be performed.

To generate license keys on the device, confirm that the device has Internet connectivity.

Subscription keys can be retrieved in one of three ways:

- **WebUI:** Click the Retrieve Subscriptions Now button from the Configuration > Update > ScreenOS/Keys page
- **CLI:** Run the following command: `exec license-key update`

Q: Can I use NSM to retrieve and install license keys?

A: License keys can also be retrieved via NSM. On the main menu in NSM, select Devices > Entitlement > Get Entitlement from entitlement server > Choose a device

Please note that the device must be reset after the key has been loaded.

Q: How do customers get post sale support?

A: Customers can contact Customer Care in case of issues with fulfillment of licenses

1-800-638-8296 (US and Canada)

1-408-745-9500 (International)

Customers who have purchased Juniper support can contact Juniper Networks Technical Support at: support@juniper.net

1-888-314-JTAC (within the United States)

408-745-9500 (from outside the United States)

Q: What is the RMA process for licenses if customers purchased Juniper direct J-Care Support?

A: If customers have received an RMA replacement, they can go to the following License Management System link to transfer their existing license to the replacement unit. <https://www.juniper.net/lcms>. They should use your CSC User ID and Password to access LMS.

If they have any issues with transferring their license, they should contact Customer Care via Case Manager.

Q: What is the RMA process for licenses if customers purchased support from a JNASC partner?

A: If customers purchased support from a JNASC partner, the following process should be followed:

- Customer requests RMA from JNASC
- JNASC sends replacement box to customer
- JNASC opens a RMA with Juniper. Juniper provides RMA number to JNASC
- JNASC or customer use Juniper RMA number in LMS and transfers licenses from original device serial number(failed) to new device serial number (the one that JNASC provided to customer) that JNASC/customer inputs

Q: How can a customer migrate from Trend AV to a Juniper-Kaspersky AV solution?

A: Customers must buy subscriptions for the Juniper-Kaspersky AV solution in order to migrate. Once they purchase the subscription, they should follow the process of registering the device/subscription and loading the license key onto the device. Please note that the Juniper-Kaspersky AV solution operates on a different ScreenOS image. Therefore, the customer should change the ScreenOS image on the device before they attempt to load the key for the new Juniper-Kaspersky AV solution.

Q: If I have Trend AV and want to switch to Juniper-Kaspersky AV, will I get a credit?

A: If customers still have time left on their Trend AV license, Juniper will not credit the time towards the Juniper-Kaspersky AV solution.

Q: What is the process for renewing content security subscriptions?

A: The process for content security subscription renewals is similar to that of Juniper direct support offerings. The Juniper renewal team notifies customers and channel partners when subscriptions are coming up for renewal (up to 90 days in advance). They will work with the channel partner and the end customer to create a quote for renewals. Once the quote is accepted and an order is booked through the channel with Juniper, the contracts team will setup the correct entitlements in LMS. The devices then can download the updated license key so that the subscriptions can be valid for another year. Please note that the device will automatically download the new license keys only if the renewal is completed prior to the original key expiring.

Q: Can content security subscriptions be trialed by customers? If yes, how?

A: Evaluation and trial capability is critical to customers to try new solutions. Robust trial capability can also help increase subscription business for Juniper's channel partners. In the past, trial and evaluation license keys could be obtained via manual mechanisms. However, these processes are neither scalable nor customer friendly. Hence Juniper has introduced a self-service model. If a device capable of running a content security subscription is connected to the Internet, the device can request a trial key. Alternatively, customers or partners can also use Juniper's License Management System portal for requesting subscription trials.

Q: Is there a URL available for me to download the trial versions?

A: Yes, if you evaluate content security features on your firewall, you may download a trial subscription from the following URL: <http://www.juniper.net/lcrs/mylic.do?methodToCall=setUpTrial>

Q: How long does the trial subscription last?

A: Trial keys typically work for 30 days. A device can only get a trial key for 30 days for a specific subscription in a year.