

# JUNOS Enhanced Services Frequently Asked Questions

JUNOS Enhanced Services bring high performance security and application acceleration capabilities to branch locations in the network.

## General Information

### Q. What are JUNOS Enhanced Services?

A. JUNOS Enhanced Services are based on the routing capabilities of JUNOS and add the session-based forwarding infrastructure that allow the porting of select security features from ScreenOS into JUNOS. This porting is an iterative process, and in the first release, the features supported are:

- Best-in-class high performance firewall derived from ScreenOS, including policies and zones
- Network Address Translation
- IPSec VPN
- Integrated WAN and application acceleration via WX module

### Q. What is revolutionary about JUNOS Enhanced Services?

A. JUNOS Enhanced Services changes the fundamental paradigm of secure routing. A classic router by its very nature is a promiscuous and insecure device. Once you assign IP addresses and build a routing table, all traffic is forwarded by the router. The network is immediately vulnerable to all security threats. In order to secure the network, security policies are added to deny classes of traffic. Everything is permitted unless explicitly denied.

JUNOS Enhanced Services turns the router into a security device. Traffic must be explicitly permitted to cross the router. That means that the network is secure from the moment the router is installed.

### Q. Why is Juniper delivering JUNOS Enhanced Services for the branch?

A. The key driver of integration is to reduce the number of devices at the remote site and drive the cost out of the branch. Juniper believes that integrating security, IP Telephony and application acceleration capabilities into JUNOS incorporates best-in-class technology from both internal and external (partners) sources in an intelligent manner. At the same time, management must be seamless and while performance and functionality are maintained without compromise. Businesses using Juniper can therefore achieve greater OPEX and CAPEX savings than other vendors can deliver. In many cases, however, integration by some vendors is achieved at the expense of both performance and functionality, thereby negating the cost benefits and possibly compromising security.

### Q. How should I position JUNOS Enhanced Services to customers?

A. JUNOS Enhanced Services are ideal for secure router deployments where the customer requires integrated security features (stateful firewall and IPSec VPN), Ethernet switching, IP Telephony and application acceleration in a branch location in the network. Customers seeking full UTM capabilities should deploy SSG platforms running ScreenOS. UTM integration into JUNOS is scheduled for 2008.

### Q. Will JUNOS Enhanced Services be available for the M- and T-series?

A. No. Device consolidation is a customer imperative at the branch where there is seldom any network support staff. At the aggregation and core of the network, the scalability of separate routing, IP Telephony, Ethernet switching, security, and application acceleration is essential. Therefore consolidated services at the aggregation and core of the network are not requested by most customers.

### Q. When will JUNOS Enhanced Services be available?

A. JUNOS Enhanced Services will be available in Q4 2007 in the JUNOS 8.5 ES release.

### Q. What is JUNOS release 8.5 ES?

A. JUNOS 8.5 ES is a transitional release which delivers JUNOS Enhanced Services. In the future, JUNOS Enhanced Services will be part of the regular JUNOS releases for the J-series.

**Q. Which router platforms support JUNOS Enhanced Services?**

A. JUNOS Enhanced Services are supported on the following J-series models

- J2320
- J2350
- J4350
- J6350

The SSG 320M, 350M, 520M, and 550M can be converted to J-series with the JUNOS conversion kit. Once they are converted, they can also run JUNOS with JUNOS Enhanced Services. For more information on OS conversion, visit [http://www-int.juniper.net/marketing/product\\_marketing/firewall-vpn/docs/ssg\\_550mssg\\_520m\\_faq.pdf](http://www-int.juniper.net/marketing/product_marketing/firewall-vpn/docs/ssg_550mssg_520m_faq.pdf).

**Q. What about support for the J2300, J4300 and J6300?**

A. The J2300, J4300 and J6300 do not support JUNOS releases with JUNOS Enhanced Services. These routers will continue to be supported on the JUNOS 8.5 release.

**Q. Doesn't the existing J-series support stateful firewall through the services module as with the M-series?**

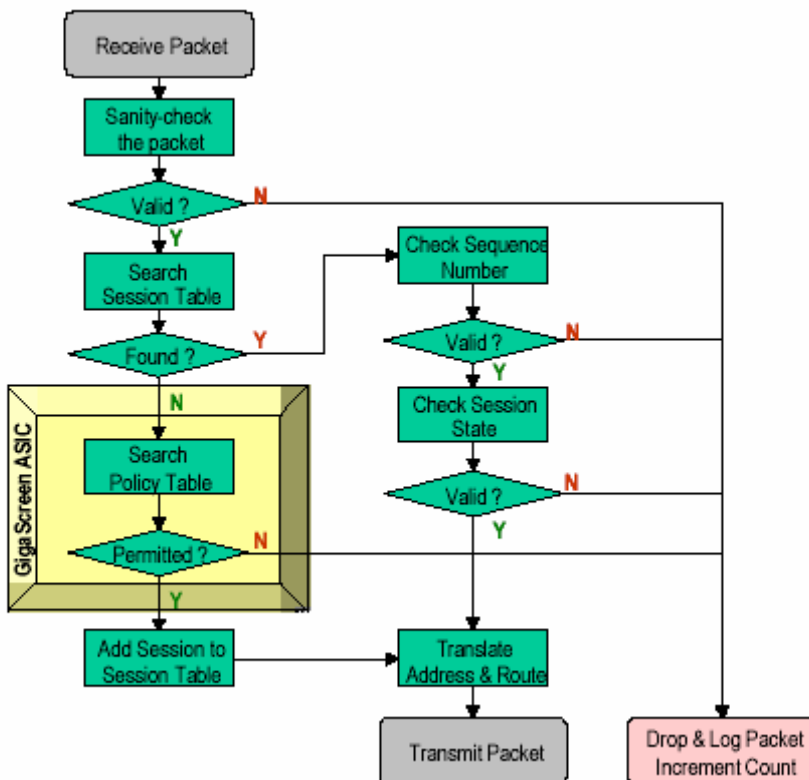
A. Firewall implementation in the M-series differs from the J-series in that the M-series utilizes a dedicated Adaptive Services PIC (ASPIC) to maintain high performance when executing security functions. Traditionally, in the J-series, this functionality is emulated in software which does not perform as efficiently, however JUNOS 8.5 ES stateful firewall implementations is different from previous JUNOS releases. Both past JUNOS releases and JUNOS 8.5 ES offer stateful inspection with ALG support, but JUNOS 8.5 ES adds significant levels of deep-packet inspection for detecting various levels of attacks, etc. ALG support is also improved in several respects as JUNOS 8.5 ES typically has both more ALGs as well as more granular support for complex protocols such as SIP and H.323. JUNOS 8.5 ES also adds stateful inter-box failover (includes full flow state information, IPSec SA, etc.) support which existing JUNOS lacks.

**Q. What does session-based processing bring to JUNOS?**

A. Traditionally, JUNOS-based branch products have provided basic packet filtering at the network layer. Packet filters – often

referred to as access control lists (ACLs) -- operate on values carried in each TCP/IP packet. These fields include protocol type, source and destination IP address, and source and destination port (application type). A few broadly defined packet filters may be trivial to create and relatively quick to process. But packet filtering grows exponentially slower and more difficult to manage in large networks with complex security policies. Packet filters alone simply cannot provide robust, high-speed firewall protection. Most secure networks today combine a screening router with a stateful packet inspection or application proxy firewall.

A dynamic or "stateful" packet inspection firewall, available in JUNOS ES, maintains a table of active TCP sessions and UDP "pseudo" sessions. Each entry records the session's source and destination IP address and port numbers, and the current TCP sequence number. Entries are created only for those TCP connections or UDP streams that satisfy a defined security policy; packets associated with these sessions are permitted to pass through the firewall. Sessions that do not match any policy are denied, as are any packets received that do not match an existing table entry.



Stateful inspection is more secure than packet filtering because it only allows packets belonging to an allowed session. For example, instead of permitting any host or program to send any kind of TCP traffic on port 80, a stateful inspection firewall ensures that packets

belong to an existing session. Furthermore, it can authenticate the user when the session is established, it can determine whether the packets really carry HTTP, and it can enforce constraints at the application layer (e.g., filtering URLs to deny access to black-listed sites).

**Q. What are the long term plans for JUNOS and ScreenOS?**

A. We believe there is a market for dedicated security devices and a market for converged routing and security devices. Our plans are to continue development on JUNOS for those markets where integrated branch routing, security, IP Telephony and application acceleration are required, and continue development on ScreenOS for those markets where dedicated branch security devices are required.

**Q. Is JUNOS without JUNOS Enhanced Services going away?**

A. No. Moving forward, the M-series and T-series will continue to be packet-based, but the J-series will be session-based, allowing maximum flexibility for branch office deployments.

**Q. Does the addition of advanced security into JUNOS mean ScreenOS is going away?**

A. No. We plan to continue to develop ScreenOS as our premier security-focused OS.

**Q. Is JUNOS Enhanced Services running ScreenOS in the background?**

A. No. It is all JUNOS. New security features that are added to JUNOS are derived from internal sources and partnerships.

**Q. Is the command line interface (CLI) JUNOS or ScreenOS based?**

A. The CLI is JUNOS.

**Q. Integration of new technologies into JUNOS was announced as part of the Branch Office launch. When will application acceleration, security and other components be available in JUNOS on J-series products?**

A. It is important to remember that integration will be an evolutionary process. Our goal is to execute the integration efforts in a manner that ensures addresses customer issues and maintains a competitive advantage. Estimated timescales are shown below.

Technology	Integrated into JUNOS on J-series
Stateful Inspection Firewall	JUNOS 8.5 ES
High Availability	First half 2008
IPSec VPN	JUNOS 8.5 ES
Application Acceleration (WXC ISM 200)	JUNOS 8.5 ES
Integrated IP Telephony (Avaya IG 550)	First half 2008
IPv6 (not session-based)	JUNOS 8.5 ES
MPLS (not session-based)	First half 2008
Integrated Ethernet Switching	JUNOS 8.5 ES
UTM Security Features (AV, IDP, web filtering)	First half 2008
NSM Support	2008

**Q. Which Physical Interface Modules (PIMS) are supported in JUNOS ES?**

A. JUNOS 8.5 ES supports the following interfaces.

- 1-port 100/1000 Ethernet SFP UPIM
- 8-port 10/100/1000 Ethernet Copper UPIM

- 16-port 10/100/1000 Copper UPIM
- 1xGigabit SFP EPIM
- 6xGigabit SFP UPIM
- 4xFE EPIM
- 2xT1 PIM
- 2xE1 PIM
- 2xChannelized T1/E1 PIM
- 2xSerial PIM
- 1xDS3 PIM
- 1xADSL Annex A PIM
- 1xADSL Annex B PIM
- 1xE3 PIM
- 4xISDN BRI - S Interface
- 4xISDN BRI - U Interface
- 2x2-wire/1x4-wire G.SHDSL
- WXC ISM 200 WAN optimization and application acceleration

**Q. Will JUNOS ES support the Avaya IG550 Integrated Gateway (VoIP Module)?**

A. Although the J2320, J2350, J4350, and J6350 support the Avaya IG550 modules in the JUNOS 8.5 release, they are not supported in JUNOS 8.5 ES. Support is scheduled for the first half of 2008.

**Q. What are the JUNOS Enhanced Services competitive advantages when compared to Cisco IOS?**

A. Integrated session-based processing will provide drastically improved performance with services when compared to the Cisco ISR whose IOS services, such as firewall, are an add-on at additional cost. JUNOS will continue to provide scalability, modularity, and processes that give customers performance, quality, a single predictable mainline release, and unmatched feature velocity, allowing the J-series to compete effectively against Cisco IOS.

**Q. How will JUNOS Enhanced Services be managed?**

A. Upon release of JUNOS 8.5ES, configuration can be performed through CLI and JWEB functions, and monitoring can be performed by JWEB and JUNOScope. Additional support is also planned for NSM in 2008.

**Q. Will NSM eventually manage all the JUNOS Security and Routing functionality?**

A. Yes, NSM will manage all security and routing functions in 2008

**Q. What is the plan for JUNOScope and SDX to manage JUNOS ES?**

A. SDX will not support JUNOS 8.5 ES. JUNOScope will support JUNOS 8.5 ES.

## About Juniper Networks

Juniper Networks develops purpose-built, high-performance IP platforms that enable customers to support a wide variety of services and applications at scale. Service providers, enterprises, governments and research and education institutions rely on Juniper to deliver a portfolio of proven networking, security and application acceleration solutions that solve highly complex, fast-changing problems in the world's most demanding networks. Additional information can be found at [www.juniper.net](http://www.juniper.net).