

Learn About Firewall Evolution from Packet Filter to Next Generation

How did firewalls develop to provide the strong, deep security and sophisticated capabilities that they offer us today? It's a long story that took place over a relatively short period of time, and most likely you were part of it.

The late nineteen seventies brought the emergence of local area networks (LANs) and connected systems that allowed companies to provide employees with the ability to communicate with one another and transfer data across a network.

(1977) Chase Manhattan Bank is the first commercial institution to deploy a LAN. LANs made interoffice electronic communication, referred to as e-mail, possible. The network was local to the company, private, and proprietary, and it supported a finite number of users. The principle form of LAN security was password protection.

(1975-1976) A DARPA program produces the first true IP router.

By the early nineteen eighties, multiprotocol routers interconnecting different networks and directing traffic among them were introduced. Routers and other Internet technology put global electronic reach within the grasp of computer users. Routers that were used to direct traffic across the Internet also included access control software to secure traffic transmission and data access.

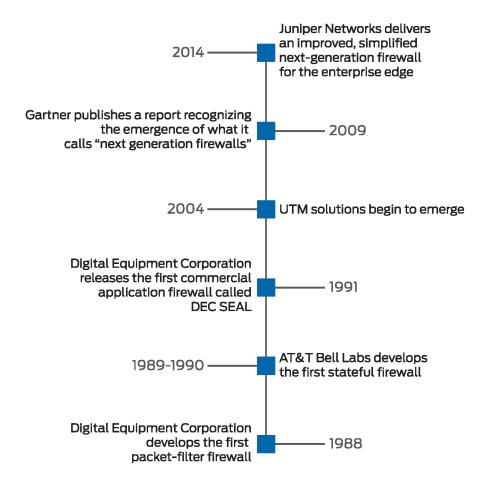


Figure 1 Firewall Evolution Timeline

(1981) Researchers at MIT and Stanford independently develop the first multiprotocol routers.

But routers could not provide the security required to meet the challenges introduced by Internet connectivity. Global communication opened the way to intrusions into connected corporate and private computers, and hackers were soon discovered breaking into private accounts. Reconnaissance missions, carried out to identify these hackers, ushered in the development of a computer-related science called digital forensics.

Mounting security concerns drove the development of computer network security and led to the first network firewalls. These firewalls allowed or blocked traffic based on policies. Network firewalls were similar in purpose to physical firewalls designed to contain fires and keep them from spreading.

Computer network firewalls established a barrier between a network that was internal to a company and considered trusted, and an external network, such as the Internet, that was considered untrusted.

References

Read about the founding of Juniper Networks and the advances that it made in the development of routers and computer network security devices: http://www.juniper.net/us/en/company/profile/history/

Browse the Computer History Museum's presentation on the development of LANs, Routers, and the Internet, the people who made it happen, and the fundamental role that DARPA played in promoting these advancements: http://www.computerhistory.org/internet_history/internet_history_70s.html

Read the DARPA RFC 823, The DARPA Internet Gateway, 1982: http://tools.ietf.org/html/rfc823

First Generation Firewalls: Packet Filter Firewalls

First generation firewalls were relatively simple filter systems called *packet filter firewalls*, but they made today's highly complex security technology for computer networks possible.

(1988) Digital Equipment Corporation develops the first stateless packet filter firewall. Packet filter firewalls, also referred to as stateless firewalls, filtered out and dropped traffic based on filtering rules. Packet filter firewalls did not maintain connection state. That is, a packet was processed as an atomic unit without regard to related packets. Packet filter firewalls were deployed largely on routers and switches.

Typically, packet processing was performed at Layer 3 and Layer 4 by matching the header fields of the packet against four tuples: who sent the packet and who was its intended recipient (source and destination IP addresses), the ports (source and destination ports), and the protocol used to transport the traffic. No higher layer information was taken into account.

The main weakness of packet filter firewalls was that hackers could craft packets to pass through the filters taking advantage of the lack of state. When packet filter firewalls were first used, operating system stacks were vulnerable and a single packet could crash the system, an event that rarely occurs today. Packet filter firewalls allowed all Web-based traffic, including Web-based attacks, to pass through the firewall. These firewalls could not differentiate between valid return packets and imposter return packets. How to handle these and other similar problems set the stage for future firewall development.

References

Read about the SRX Series stateless, packet filter firewall: http://www.juniper.net/techpubs/en_US/junos12.1x46/information-products/pathway-pages/security/security-processing-library.pdf

Read about the Junos OS packet filter firewall for routing devices: http://www.juniper.net/techpubs/en_US/junos14.1/information-products/pathway-pages/config-guide-firewall-filter/config-guide-firewall-filter.pdf

Second Generation Firewalls: Stateful Firewalls

Packet filter firewalls were followed not long afterward by *stateful firewalls*. These second generation firewalls had the same capabilities as packet filter firewalls, but they monitored and stored the session and connection state. They associated related packets in a flow based on source and destination IP addresses, source and destination ports, and the protocol used. If a packet matched this information bi-directionally, then it belonged to the flow.

(1989-1990) AT&T Bell Laboratories develops the first stateful firewall, which they refer to as a circuit-level gateway.

As use of the Internet expanded and businesses became highly networked, they could selectively provide their users with Internet services, but they wanted to do this in a manner that allowed them to secure their assets against intrusions and attacks originating outside their LANs. Businesses also wanted to protect their networks against attempts by employees and other corporate personnel, such as contractors and partners, to access network resources for which they were not authorized. Additionally, they wanted to protect their networks against attacks launched- either unwittingly or intentionally - from within the LAN and across the Internet. To solve these problems, they turned to the deployment of stateful firewalls.

Stateless packet filter firewalls did not give administrators the tools necessary to monitor the state of communications and connections within and across sessions. Stateful firewalls answered that call.

Decisions as to whether to allow traffic or filter it out based on session connections were at the core of the security that stateful firewalls provided. In its state table, the firewall maintained the state of all allowed, open connections and sessions and the communication status between a source host and a destination host. This technology gave administrators an intelligent view into network connections, and it allowed them to define rules that controlled traffic access based on the state of the connection. Stateful firewall rules encompassed the four tuples of packet filter firewalls but also included a fifth tuple to identify the connection state.

Stateful firewalls addressed the packet filter firewall problem of not being able to determine if a return packet was from a legitimate connection, but the problem of not being able to differentiate good Web traffic from bad remained. What was needed were firewall features that could detect and block Web attacks, and they followed soon afterward.

References

Read the definitive Junos Security guide to gain hands-on experience with Junos services gateways for the enterprise.

http://shop.oreilly.com/product/0636920001317.do

Read about stateful firewalls on SRX Series devices:

http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/concept/security-branch-device-stateful-firewall-functionality-understanding.html

Get to know Junos OS flow-based stateful firewall processing for the SRX Series: http://www.juniper.net/techpubs/en_US/junos12.1x46/information-products/pathway-pages/security/security-processing-index.html

4

For branch SRX Series devices, get started configuring stateful firewall security: http://www.juniper.net/techpubs/en_US/junos12.1x46/information-products/ pathway-pages/security/security-getting-started.html

For rich, comprehensive coverage of security services on SRX Series devices and an enjoyable read, see the widely acclaimed *Juniper SRX Series* hands-on reference: http://shop.oreilly.com/product/0636920026785.do

Targeted Firewall Features

As security problems became more pronounced and specific, powerful security software associated with firewalls emerged to solve them. Among these products were Antivirus (AV) applications, Intrusion Prevention Systems (IPS), URL Filtering, and Unified Threat Management applications. This section takes alook at network security promoted by these technologies.

Antivirus (AV) applications

To understand antivirus software, it helps to understand computer viruses. Long before the appearance of computer viruses, Jon von Neumann postulated in his publication the "Theory of Self-Reproducing Automata" that a self-reproducing computer program could be designed.

(1983) Peter Szor defines the computer virus as "code that recursively replicates a possibly evolved copy of itself." Although it was not intended to be a computer virus, and was not used as one, von Neumann's design is looked upon as the first computer virus. It can be assumed that "Theory of Self-Reproducing Automata" and other works like it are part of the literature referred to by computer virus designers.

Computer viruses are self-replicating computer programs that insert themselves into resources such as data files and other computer programs. They can wreak havoc on individual computers and computer networks, disrupting productivity and inflicting billions of dollars of damage.

(1971) "The Creeper" virus was the first computer virus identified. It infected mainframes and was eventually deleted by the first computer antivirus software called "The Reaper," which itself was a virus that was targeted to remove The Creeper.

The most damaging viruses are said to be "in the wild." Typically they contain a payload that can wipe out all computer files and target the computer's BIOS. To be considered "in the wild," a virus must spread uncontained among infected computers in the general public as a result of normal daily operations.

Of the approximately 50,000 known computer viruses, fewer than 600 are considered "in the wild."

The first viruses were said to be spread by the *sneaker net*, floppy disks that were traded among friends. Shareware and bootleg software was passed around hand-to-hand.

E-mail hastened the spread of computer viruses. Viruses are commonly spread through instant messaging and as Internet downloads. Computer virus development strategies that relied on exploitation of security vulnerabilities became more sophisticated, eventually involving use of social engineering. Today, computer virus creators often use scripting languages to create macro viruses that exploit social media sites.

As soon as computer viruses appeared, antivirus software designed to detect and remove them was developed. Antivirus programs scanned executable files and boot blocks against a list of known viruses, attempting to determine if they were infected, and if so to eliminate the virus and other malware. Antivirus software also included dynamic features that checked Internet downloads and constantly scanned for activity of known classes of viruses.

Antivirus programs relied on signatures to detect viruses. A signature is an algorithm or hash numeric value derived from a text string that uniquely identifies a specific virus.

The first antivirus signatures were hashes of entire files or sequences of bytes that represented the particular malware.

(1987) Fred Cohen states that "there is no algorithm that can perfectly detect all possible computer viruses." Heuristic antivirus utilities emerge: "FluShot Plus" by Ross Greenberg and "Anti4us" by Erwin Lanting were among the first.

Gradually, advanced heuristics came into play that used suspicious section names, incorrect header sizes, wildcards, and regular expressions in their analysis. To stay apace of the proliferation of malware, developers of antivirus software used increasingly more complex algorithms. Most antivirus software provided a regular signature update server to allow customers to keep up with the latest viruses.

To continue to be effective, antivirus programs had to be able to protect growing numbers of file types, and virus checkers had to be updated more frequently. Antivirus programs emerged that could prevent, detect, and remove not only viruses but also other forms of malware such as rootkits, hijackers, Trojan horses, backdoors, dialers, fraudtools, adware, and spyware.

Intrusion Prevention Systems

(2013) IPS makes a strong comeback. Rob Ayoub, research director at NSS Labs, predicts the revival of IPS saying "...don't expect IPS technology to just roll over and play dead." Not all cyber-attacks are preventable, but the proven effectiveness of preemptive systems such as Intrusion Prevention Systems considerably reduces the potential damage —security experts say by about ninety percent or more. That is why some security professionals were surprised that Intrusion Prevention Systems were on the Sverge of becoming obsolete at the beginning of the Twenty-First Century.

Using a combination of sensors and analyzers, Intrusion Prevention Systems monitored network traffic and performed heuristic analysis of flows relying on a variety of tactics, including use of file signatures. They monitored for exploit signatures that identified well-known attacks. They also looked for vulnerability signatures that targeted underlying system vulnerabilities.

One of the key characteristics of an Intrusion Prevention System (IPS) is immediacy. Directly after identifying a potential threat, an IPS can take preemptive action, often responding to the threat before the attack is launched. The action it takes is determined by a set of rules, or policies, set by an administrator based on the organization's network infrastructure requirements. These rules might direct the IPS to trigger an alarm to warn of a potential threat, or they might direct the IPS to remediate malicious flows by blocking traffic (IP source addresses), either temporarily or permanently.

Although not officially part of a firewall, IPS products were often placed in-line behind the firewall to implement layered security protection. IPS solutions resided in the direct communication path between source and destination IP addresses.

IPS products, often referred to as appliances, could be implemented in hardware or software, or both. They protected hosts from the network layer up to the application layer against known and unknown attacks.

How do they work? The majority of IPS appliances utilize one or more of three detection methods: *signature-based*, *statistical anomaly-based*, and *stateful protocol analysis*.

- Signature-based detection: Monitors traffic packets for patterns of well-known attacks, relying on a database of predefined signatures.
- Profile or statistical anomaly-based detection: Determines normal network activity.
 Based on this information, IPS detects for abnormal behavior or activity. Anomaly detection techniques do not necessarily target malicious traffic.
- Stateful protocol analysis detection: Behaves similar to signature-based detection, but performs much deeper packet inspection. IPS identifies deviations of protocol states by comparing observed events with predetermined profiles of benign behavior.

In discussing IPS, it's important to consider *Intrusion Detection Systems (IDS)* software. IPS is sometimes considered the next generation of IDS, but these technologies differ in important ways. IDS applications, considered passive-monitoring systems, typically monitored for suspicious activity and potential intrusions, and they warned the administrator that such intrusions were taking place. Where IDS only informed of a potential attack, IPS prevented it, perhaps also sending an alarm.

URL Filtering

URL Filtering allows the user to control access to Internet websites. You can control which sites your employees, family members, and other users have access to by blocking or allowing anything, from an entire category of web sites to a single URL.

Unified Threat Management

(2004) Solutions emerge to stop hacking, virus, and worm attacks on corporate confidential data systems. Although they did not mark a formal stage in firewall evolution, *Unified Threat Management* (UTM) solutions brought together a suite of security services integrated on a single platform. They encompassed a wide range of features in addition to standard firewall features such as AV, VPNs, content filtering, load-balancing, and reporting. They provided defense-in-depth security, but performance remained an issue for larger enterprises.

References

Antivirus

Check out the Juniper Networks SRX Series documentation for information on antivirus protection:

http://www.juniper.net/techpubs/en_US/junos12.1x46/information-products/pathway-pages/srx-series/book-software-srx-series-volume-1.pdf

Read about the Juniper Networks predefined antivirus policies:

http://www.juniper.net/techpubs/en_US/junos12.1x45/information-products/topic-collections/security/software-all/getting-started-guide/security-getting-started-guide.pdf#search=%22SRX%20Series%20Kaspersky%20antivirus%20protection%22

Read about Juniper Networks Sophos antivirus protection:

http://www.juniper.net/techpubs/en_US/junos12.1x44/topics/concept/utm-antivirus-sophos-overview.html

Read the Juniper Networks knowledge base article on how to get started configuring Kaspersky, Sophos, and Antivirus Express protection:

http://kb.juniper.net/InfoCenter/index?page=content&id=KB16620

Take a look at reports on some of the more common widespread computer viruses:

- 1999: Melissa: http://malware.wikia.com/wiki/Melissa; Bubble boy: http://bubbleboy.8m.com/bubble-boy.html
- 2001: Nimda: http://nakedsecurity.sophos.com/2011/09/16/memories-of-thenimda-virus/
- 2003: SoBig.F: http://virus.wikidot.com/sobig

See the list of computer viruses that are still found "in the wild" published by Wild-List Organization International:

http://www.wildlist.org/CurrentList.txt

Intrusion Prevention Systems

Get an overview of Juniper Networks' Intrusion Prevention System product: http://www.juniper.net/uk/en/products-services/software/router-services/ips/

Take a look at the Juniper Networks library of information on Intrusion Detection and Prevention:

http://www.juniper.net/techpubs/en_US/junos12.1x47/information-products/pathway-pages/security/security-idp-index.html

If you want to steep yourself in the Junos Intrusion Prevention Systems product and gain expertise, take a course on it offered by Juniper Networks:

https://learningportal.juniper.net/juniper/user_activity_info.aspx?id=2320

Get some of the best information on Juniper Networks' Intrusion Prevention product by reading the chapter on it in the widely acclaimed *Juniper SRX Series* hands-on reference:

http://chimera.labs.oreilly.com/books/1234000001633/ch13.html

Then buy the book at:

http://shop.oreilly.com/product/0636920026785.do

Watch the Juniper Networks YouTube video *How to Configure IDP for SRX Series Devices*:

https://www.youtube.com/watch?v=0a1-Qr3IODo

Unified Threat Management

Get a high-level view of Juniper Networks' Unified Threat Management software: http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/concept/utm-over-view.html

http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/general/security-feature-utm-support.html

For information on Juniper's implementation of UTM, sift through the *Junos OS Attack Detection and Prevention Library for Security Devices*: http://www.juniper.net/techpubs/en_US/junos12.1x46/information-products/pathway-pages/security/security-adp-index.html

Third-Generation Firewalls: Application Firewalls

(1991) DEC releases the first commercial application firewall called *DEC SEAL*, based on Marcus Ranum's research and design.

Firewall technology development continued its rapid advance; as attackers made their way up the OSI model layers looking for vulnerabilities, firewall technology development also moved up the OSI model utilizing the higher layers to provide increased traffic and access protection, as well as visibility into attempted attacks.

Traditional stateful firewalls, which provided protection based on control over protocols and ports and which restricted traffic to and from specific IP addresses, were considered inadequate to protect against the growing numbers and kinds of Web-based attacks that became increasingly common as the Internet matured.

Web-based attacks easily passed through well-known ports – HTTP (port 80), HTTPS (port 443), and e-mail (port 25) – because firewalls based on protocols and ports were unable to distinguish legitimate applications that relied on those proto-

(1993) Under a DARPA contract, Marcus Ranum, Wei Xu, and Peter Churchyard develop the first freely available application firewall called *Firewall Tookit* (FWTK) to provide a common base for others to build upon.

(1999) Perfecto Software's AppShield takes the lead in delivering Web application firewall (WAF) technology. cols and ports from illegitimate attacks and applications. They were unable to distinguish one kind of Web traffic that used the port from another.

Application firewalls solved the problems stemming from the fact that any application could run on any port. They gave administrators the ability to control and secure a network up to the application layer. They identified application attempts to breach or bypass the firewall on an allowed, or open, port. They allowed administrators to identify and block applications and service calls that could be malicious.

Because most applications ran on port 80, it became essential for security software to be able to distinguish one type of application from another. Web-based attacks could easily pass through well-known ports – HTTP (port 80), and also HTTPS (port 443), and e-mail (port 25). Packet-filter and stateful firewalls that were based on protocols and ports were unable to distinguish legitimate applications that relied on those protocols and ports from illegitimate applications and attacks.

Application firewalls could inspect traffic contents and block specific content such as Web services and known viruses. They solved many of the problems related to Webbased attacks.

Host-based application firewalls monitored application input, output, and system service calls related to the application.

The Web Application Firewall (WAF) was delivered as an appliance or server plug-in to filter out traffic by applying a set of rules to HTTP conversations.

Web Application Firewalls continued to evolve alongside ongoing radical advances in firewall technology that gave visibility into the contents of packets themselves, not just information about them or the applications with which they were associated.

References

Read about Juniper Networks AppSecure, a product that provides a collection of application security features for SRX Series devices:

http://www.juniper.net/us/en/products-services/security/appsecure/

Take a look at the entire AppSecure basics chapter in the widely acclaimed *Juniper SRX Series* hands-on reference:

http://chimera.labs.oreilly.com/books/1234000001633/ch12.html

Then buy the book at:

http://shop.oreilly.com/product/0636920026785.do

Take a short course on SRX Series AppSecure. Find out what it is and how to configure it in this YouTube video *Basic Application Firewall Learning Byte*: http://www.youtube.com/watch?v=_chtTmzrJTY&list=PLqANiksldRZd1uw0E7UxdSu4qtvcN7GF-&index=10

Go directly to the main documentation on Junos OS AppSecure Services Library for Security Devices: http://www.juniper.net/techpubs/en_US/junos12.1x46/information-products/path-way-pages/security/security-appsecure-index.html

Next-Generation Firewalls

(2009) Greg Young and John Pescatore of Gartner publish *Defining* the Next Generation Firewall.

(2014) The Juniper Networks NGFW solutions include application awareness, intrusion prevention system, role-based user control options, and best-in-class unified threat management. In 2003, Gartner began investigating the idea of the Next-Generation Firewall (NGFW), and in 2004 they began publishing notes on it. In 2009 they published an official report that defined the Next-Generation Firewall after realizing that early versions of enterprise NGFWs had begun to appear. NGFWs brought together in a collusive synthesis many existing security technologies and newly developed ones.

Application visibility and control, deep packet inspection, advanced threat protection, and quality of service formed the firmament for NGFWs that were characterized non-disruptive, in-line, bump-in-the-wire configuration, and performance and management improvements.

The portfolio of services that NGFWs provided included some of the traditional firewall services but without the perceived performance problems. These solutions also included support for user, user group, and user role-based features that revealed the user identity separately from an IP address assigned to their system.

In addition to solving some of the remaining network security problems, NGFWs allowed administrators to put in place security that kept pace with leaps in computer technology and the changing Internet landscape, which gave users the option to use *untethered* computers (systems not connected to a USB cable), supported *device discovery technology* and *over-the-air configuration*, provided *self-service portals*, and allowed users to "*bring their own devices*" (BYOD) to the network.

NGFWs encompassed the strengths of predecessor firewalls while widening and deepening reconnaissance and control without sacrificing performance. Their deep packet inspection features ensured that attempted attacks were recognized and remediated. These features could examine traffic closely to determine if it presented an attack.

The Juniper Networks NGFW solutions include:

- High performance deep (or complete) packet inspection (DPI) that gave full inspection of packets generating a large amount of information about traffic that could be used to normalize standard communications. It also provided for faster and more effective anomaly detection. The data that DPI systems gathered provided administrators with a comprehensive view of network traffic.
- End-to-end Network Access Control (NAC) and application awareness that maintained application state and resource requirements information. Application awareness features allowed for intelligent traffic analysis and they gave administrators the ability to thwart distributed denial of service (DDoS) attacks intended to disrupt availability and data breaches executed by Web applications.
- Active Directory (AD) integration and user identity management. User firewalls
 widened the security policy by adding a user identity tuple. Users could be identified by their roles (user role-based firewalls), by the groups that they belonged to,
 or by individual user identification (user firewalls).
- Definitive attacker profiling protection against exfiltration, or data loss, which promoted global sharing of intelligence on hackers to speed detection and monitoring.

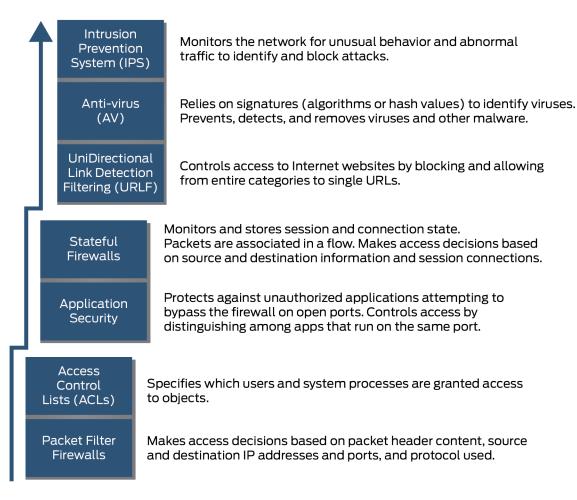


Figure 2 Next-Generation Firewall Capabilities

References

Take a look at the Junos OS SRX Series IDP technology:

http://www.juniper.net/techpubs/en_US/junos12.1x46/information-products/ pathway-pages/security/security-idp-index.html

Read about AppSecure:

http://www.juniper.net/us/en/products-services/security/appsecure/

Read about Spotlight Secure, the Juniper Networks' cloud-based hacker device intelligence service that identifies individual attacker devices and tracks them in a global database:

http://www.juniper.net/us/en/products-services/security/webapp-secure/

View the YouTube video Hacker Interrupted: Detecting and Preventing Hackers on Your Website:

http://www.youtube.com/watch?v=9jXXL5S_e4M



Learn About Firewall Evolution from Packet Filter to Next Generation

by Judy Thompson-Melanson

How did firewalls develop to provide the strong, deep security and sophisticated capabilities that they offer us today? Learn how firewalls developed over the course of the past four decades from packet filter to true next-generation devices that constrain attackers and make it possible to navigate the Internet more securely. It's a fascinating story that took place over a relatively short period of time, and most likely you were part of it. *Learn About* it!

Judy Thompson-Melanson is a Juniper Networks staff technical writer with over twenty-five years in the industry. She has written API documentation, design guides, and networking and security documentation for many companies including Apple, Sun Microsystems, Cisco Systems, and Intuit. The author thanks the following for their engagement in this project: Patrick Ames, Editor in Chief; Nancy Koerbal, Copyeditor; Karen Joice, Illustrator; and Linnea Wickstrom, Project Promoter.

© 2014 by Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. 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.

ISBN: 1-941441-0-08 Version History: v2, Jan. 2015 3 4 5 6 7 8 9

Learn About It! juniper.net/documentation



