White Paper

Stateful Inspection Firewalls

An overview of firewall technology and how Juniper Networks implements it

Chris Roeckl
Director, Corporate Marketing

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

Part Number: 200060-001

Contents

Firewall Technology: An Overview

Today, enterprises and service providers face ever-increasing security and performance challenges. Securing web sites, corporate networks, and online applications is absolutely essential. At the same time, security measures must not impede productivity – the best solutions are those that combine high performance with top-notch security.

Juniper Networks delivers a line of purpose-built security appliances and systems that integrate firewall, VPN, denial of service protection and traffic management functions within a single, comprehensive, high-performance platform. This white paper describes how firewall features are implemented in NetScreen firewall/VPN products. It explains how NetScreen firewalls operate at wirespeed by integrating silicon and RISC-based processing with a custom real-time operating system, designed exclusively for stateful packet inspection. It illustrates how Juniper Networks hardened ScreenOS is able to deflect an army of denial-of-service attacks. Finally, this paper shows how Juniper Networks firewalls are highly versatile and scalable, offering cost-effective solutions that range from 2,000 to 1,000,000 concurrent sessions.

Introduction

Every network-connected business must worry about perimeter security. For many enterprises, eBusiness success depends on defending its web servers against denial of service attacks. Zone Research estimates the average buyer will wait just 8 seconds for a page to download; eCommerce sales lost to unacceptable performance hit $4.35B in 1999. Instrumenting servers for high availability, capacity, and throughput is not enough -- these resources must also be protected against attack. Embarrassing denial-of-service events have shown that hackers can cripple even the biggest, baddest sites on the Internet, left unprotected.

Defending servers -- and desktops at home and at the office -- against unauthorized access is paramount to ensure the privacy of confidential data and non-stop operation of mission critical resources. From small businesses to telecommuters, large enterprises to service providers, nearly every network today is connected to the Internet and therefore vulnerable to outside attack. To control access to networked resources, businesses define and implement security architectures. Choosing the right components is critical. Let's begin by considering the role that firewalls play in enterprise security, the kinds of firewall technologies that exist today, and the tradeoffs between them.

How Firewalls Can Help

Firewalls filter the traffic exchanged between networks, enforcing each network's access control policy. Often, a firewall defends an inside "trusted" network from attack by "untrusted" outsiders. Firewalls ensure that only authorized traffic passes into and out of each connected network. To avoid compromise, the firewall itself must be hardened against attack. To enable security policy design and verification, a firewall must also provide strong monitoring and logging.

Packet Filtering

Many routers provide 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. As shown in Figure 1, 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.

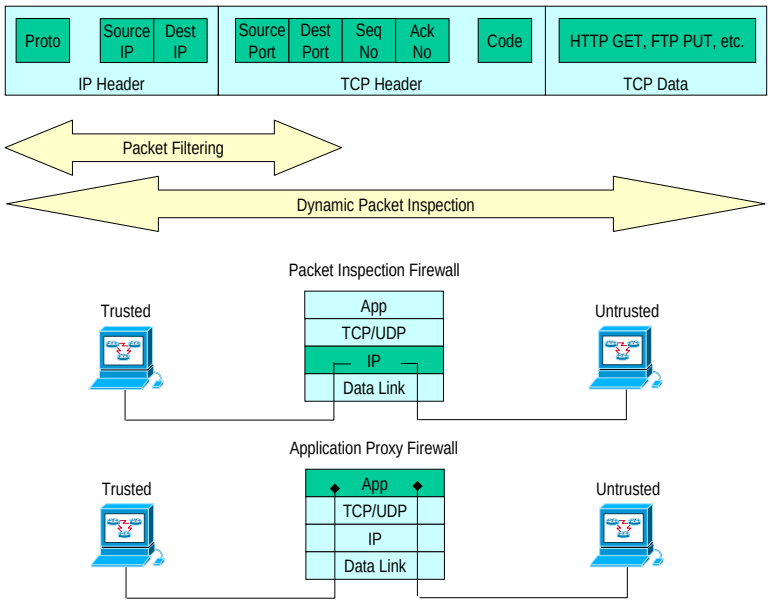

Figure 1: Types of Firewalls

Stateful Inspection

A dynamic or "stateful" packet inspection firewall 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 allow 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).

Application Proxy

Application proxy firewalls are also more secure than packet filtering, but are generally slower than stateful inspection. In an application proxy firewall, two TCP connections are established: one between the packet source and the firewall, another between the firewall and the packet destination. Application proxies intercept arriving packets on behalf of the destination, examine application payload, then relay permitted packets to the destination. Proxies necessarily involve more protocol stack overhead than inspecting packets at the network layer. Furthermore, because a unique proxy is required for each application, proxy firewalls can be less flexible and slower to upgrade than stateful inspection firewalls. On the other hand, proxy implementations can offer very granular application-level control (for example, blocking FTP transfers involving filenames ending in ".exe").

Hybrid Approach

To provide the best of both worlds, many firewalls are actually hybrids that combine stateful inspection and application proxy methods. As this paper will show, Juniper Networks firewalls are hybrids -- they primarily employ silicon-based stateful packet inspection for high performance, complemented by selective proxies for built-in protection against denial-of-service attacks.

Building A Secure Network

By establishing a strong perimeter defense between trusted and untrusted networks, a properly deployed firewall becomes the foundation for enterprise network security. But firewalls do not act alone -- they should always be your first line of defense, deployed in conjunction with complementary security measures that protect the entire enterprise from both outsider and insider threats. For example, most enterprises combine a strong perimeter defense with intrusion detection and desktop and server protection.

Juniper Networks devices offer integrated firewall, network address translation (NAT), and virtual private network services. Combining these security measures within a single platform can greatly simplify network design. Furthermore, Juniper Networks devices integrate smoothly with third-party security products like Websense content filtering, WebTrends log analysis and reporting, and RADIUS, SecurID, and LDAP user authentication servers. For added protection against single-point-of-failure, Juniper Networks devices provide server load balancing and can be deployed in redundant pairs for high availability.

Juniper Networks Approach

By offering fast, robust packet inspection in a seamless fashion, Juniper Networks devices can form an integral part of nearly any secure network. Juniper Networks combines a purpose-built hardware platform with custom ASICs and a finely tuned real-time operating system to achieve wirespeed firewalling without sacrificing security.

Purpose-Built Hardware

At the heart of every Juniper Networks device is a custom Application Specific Integrated Circuit (ASIC). These ASICs are specially designed chips that accelerate firewall, encryption, authentication, and PKI processing. By performing computationally intensive tasks in the ASIC, Juniper Networks can far surpass the performance of software firewalls. In fact, because Juniper Networks devices are designed around ASICs, they are more efficient than so-called hardware firewalls that simply add co-processors as an after-thought.

For optimal integration of hardware and software processing, Juniper Networks employs a high-speed multibus architecture that couples each ASIC with a RISC processor, SDRAM, and Ethernet interfaces. Unlike firewalls that employ PC hardware, Juniper Networks platforms are tightly integrated systems designed for high-performance, high-availability environments.

Three-Prong Approach for High Performance

Firewalls developed for NT or Solaris environments continually chase OS updates issued by Microsoft and Sun, re-applying kernel, stack, driver, and service patches to improve performance and security. Juniper Networks turnkey purpose-built approach avoids the on-going maintenance required by general-purpose operating systems. RISC processors used in Juniper Networks devices run ScreenOS. This security-hardened, low-maintenance real-time operating system is designed specifically for firewalling, in tandem with Juniper Networks ASICs.

ScreenOS supports configuration, management, and monitoring tasks, accessed from Juniper Networks-Global PRO, the WebUI and CLI. In addition, ScreenOS incorporates a high-performance TCP/IP engine that works in conjunction with ASICs to inspect and forward packets. This real-time operating system does not suffer from connection table and processing limits found in general-purpose operating systems. ScreenOS can establish up to 25,000 TCP connections per second, withstanding HTTP bursts that often overwhelm other firewalls. As illustrated in Table 1, the Juniper Networks NetScreen-500 can firewall up to 250,000 concurrent TCP sessions at 700 Mbps over full-duplex Fast Ethernet. The Juniper Networks NetScreen-5200 can handle 1,000,000 sessions at 4 Gbps.

Integrated Policy Management

Juniper Networks devices provide integrated single-point enforcement of firewall, VPN, and traffic management policies, classified by source and destination IP address, protocol, source and destination port (service), and time-of-day or week. More than 40 common Internet services, including DNS, FTP, and the hard-to-firewall H.323, are built-in. Custom services can be added by port number.

Juniper Networks policies are applied to (virtual) interfaces to create security domains. For example, the Juniper Networks NetScreen-5XT offers five interfaces: four Trusted and one Untrusted. The Juniper Networks NetScreen-25 and Juniper Networks NetScreen-50 add a demilitarized zone (DMZ) interface to isolate and protect public servers. The NetScreen-500 and NetScreen-5200 support up to 500 and 4,000 virtual interfaces respectively, using industry standard 802.1q VLAN technology.

Because each network is somewhat different, Juniper Networks devices can be deployed in three modes, illustrated in Figure 2.

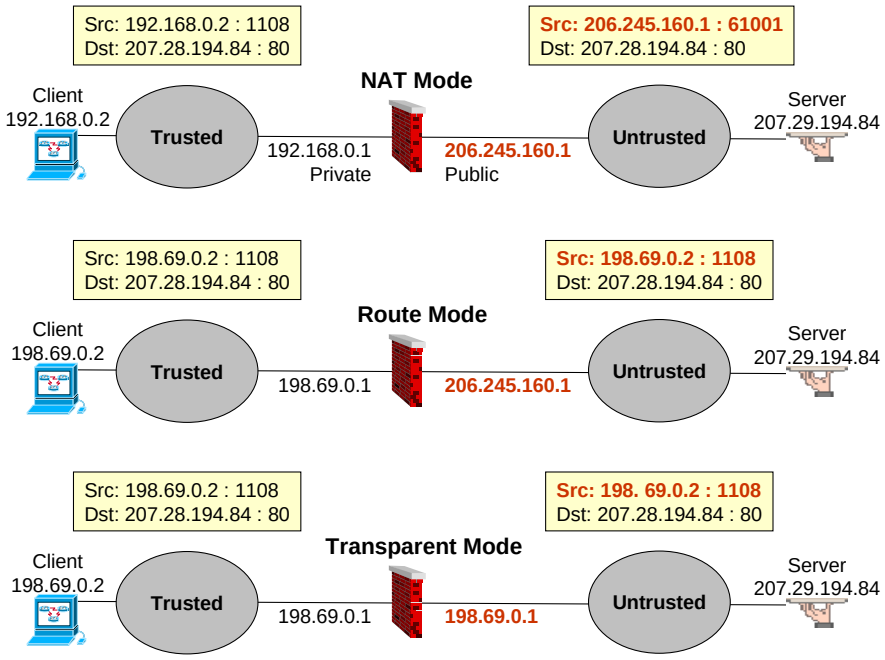

Figure 2: Operates In Three Modes

Network Address Translation (NAT) Mode lets an entire network of privately-addressed hosts share the firewall's public IP -- the address assigned to the firewall's Untrusted interface. In this mode, the firewall differentiates between sessions by assigning a unique source port number. For example, suppose trusted hosts 192.168.0.2 and 192.168.0.3 both send packets from source port 1108. The firewall may translate these to a single public IP address 206.245.160.1 and two different source ports, say 61001 and 61002. Response packets received for port 61001 are routed back to 192.168.0.2:1108, while port 61002 packets are routed back to 192.168.0.3:1108. NAT can be useful to avoid renumbering trusted networks, to eliminate purchase of public address blocks, and to hide trusted addresses from the outside world.

Route Mode lets the firewall be inserted between networks that do not require address translation. This mode can be used to firewall LANs within the same enterprise network -- for example, protecting the finance department subnet from insider snooping or theft. It can also be useful for inserting the firewall behind a NAT router or in front of a network with existing public addresses (for example, firewalling an eCommerce server farm).

Transparent Mode lets the firewall be dropped seamlessly into any existing network, without renumbering, network re-design, or downtime. In this mode, the firewall bridges segments of the same subnet. It is given one IP address from that subnet for management and server communication, but is otherwise completely transparent. The firewall automatically teaches itself which packets to forward and which to ignore by building a MAC Learning Table:

- When the firewall receives a frame with unknown source and destination addresses, it searches for a matching policy. If permitted, a Session Table entry is created, the source address is added to the MAC Learning Table, and the frame is forwarded out the opposite interface. When a reply is received, that source address is also added to the MAC Learning Table.

- When the firewall receives a frame with known source and destination addresses, it floods the frame out of the opposite interface. If responses indicate the source and destination are in the same segment (i.e., on the same side of the firewall), the MAC Learning Table is updated and subsequent traffic between these two addresses is ignored.

For optimal transparent mode performance, granular policies should be defined, minimizing the number of Session and MAC Learning Table entries. The DMZ can also be used in transparent mode.

By offering a choice of modes, Juniper Networks devices adapt to your topology instead of requiring you to accommodate it through network redesign.

Packet Processing

To understand how Juniper Networks ASICs and ScreenOS cooperate to accelerate firewalling, let's examine how packets are inspected (Figure 3). When a packet is received through any interface, it is intercepted at the network layer. ScreenOS performs format and frame "sanity checks" to verify the packet is valid. For example, if the MAC address is all zeros, then the packet is dropped and no further checking is done.

If the packet is valid, ScreenOS searches the session table to determine whether this packet is part of an existing TCP session. (Although UDP is connectionless, Juniper Networks creates a "pseudo session" to represent each unique UDP stream.)

- If the session already exists, ScreenOS checks the TCP packet's sequence number and code fields to ensure the packet really belongs to this session. For example, an invalid sequence number can indicate a hijacked session; Juniper Networks verifies that the sequence number is within 64,000 (16 bits) of the last received for this session. Packets that pass these checks are translated and routed as needed, then transmitted. (VPN and traffic management functions, also performed at this point, are beyond the scope of this paper.)
- If the session does not exist, the packet must be classified -- that is, we must find the policy that defines how this packet should be handled. This is where other firewalls fall short, requiring administrators to choose between security and performance. The bigger the

network, and the more granular the access control, the larger the policy table. Juniper Networks performs packet classification in silicon to search up to 40,000 policies at wirespeed. If no policy is found, the packet is dropped. If a matching policy is found, a new session table entry is created and processing continues as described above.

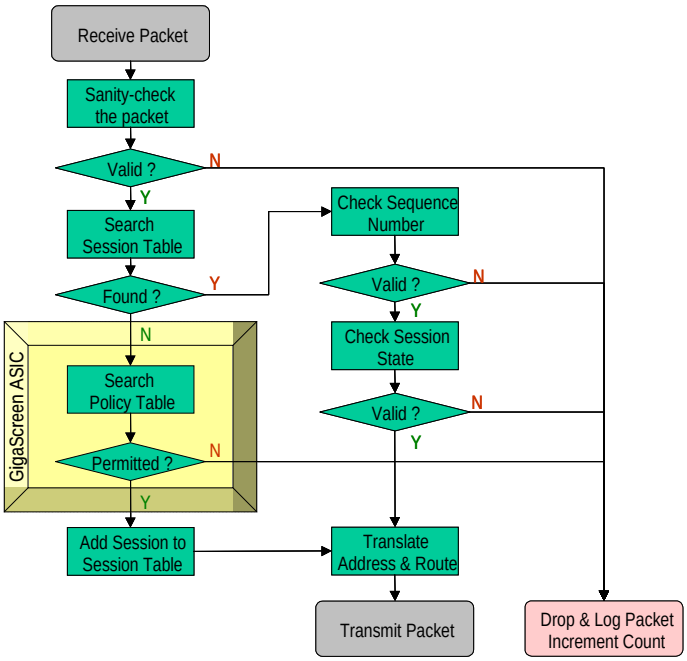

Figure 3: Firewall Packet Processing

The GigaScreen ASIC, based on .25 micron technology, is Juniper Networks second-generation security accelerator. This ASIC delivers a "Triple Crown" of security industry firsts: the first to encrypt IPSec at Gigabit speed, the first to combine encryption, authentication, PKI and firewall acceleration in a single chip, and the first silicon-based stateful packet inspection firewall. The ASIC's firewall acceleration functions include hardware assisted policy search, TCP header parsing, session table maintenance and network address translation.

Implementing policy lookup in the ASIC is key to achieving better performance without sacrificing security. Juniper Networks policies are stored in SDRAM and can be updated without system reset. The ASIC uses limited on-board memory and a high-speed bus to access policies. As a result, when the ASIC is invoked to classify a packet, its policy engine takes just four cycles to examine each policy (25 million per second). Compare this to a software policy search that requires 100 cycles per policy. Because denied packets usually require every policy to be examined, the ability to complete this search quickly is of paramount importance. Without this, denial-of-service attacks can be accomplished rather easily by flooding the firewall with unauthorized packets. Because policies can be searched quickly, Juniper Networks devices have a very high session ramp rate. The NetScreen-500 and NetScreen-5200 can create up to 17,000 and 25,000 new sessions per second, respectively.

Protecting Against Denial-of-Service Attacks

Juniper Networks provides accurate, high-speed packet inspection, but it doesn't stop there. By scanning for attack signatures and selectively applying proxy technology, ScreenOS offers exceptional defense against common Denial-of-Service (DOS) attacks. For example, consider the notorious DOS attack that crippled major eCommerce sites in early 2000: the SYN Flood.

How SYN Floods Work

When any host wants to establish a TCP connection, it goes through a "three-way handshake" process (Figure 4). The initiator sends a TCP packet carrying a starting sequence number and a SYN flag (an enabled bit in the TCP header Code field). The responder returns a packet that carries its own starting sequence number and acknowledges the initiator's packet (both SYN and ACK bits are enabled). To complete connection establishment, the initiator acknowledges the responder's packet (returns a packet with the ACK bit enabled). Most TCP implementations wait 60 seconds for an ACK before aborting a "half open" connection.

If an attacker floods a server with SYN packets, that server may reach its TCP connection limit and begin refusing legitimate connections. The attacker simply sends SYN packets, but never acknowledges the server's SYN-ACK packets. Because the server waits for up to 60 seconds, the attacker is able to send SYNs much faster than the server can time them out.

When a Juniper Networks device sees this three-way handshake, it creates a new entry in its Session Table. Juniper Networks SYN protection algorithm kicks in whenever the ScreenOS detects more SYN packets per second to a single destination than the predefined threshold (200 SYN packets per second by default). When this configurable threshold is reached, the firewall proxies any additional SYN packets -- that is, it acknowledges each SYN on behalf of the responder, returning a random sequence number in a SYN-ACK packet. The proxy slows the attacker down and lets the responder continue to do its job. As a result, Juniper Networks devices are able to withstand much larger SYN floods.

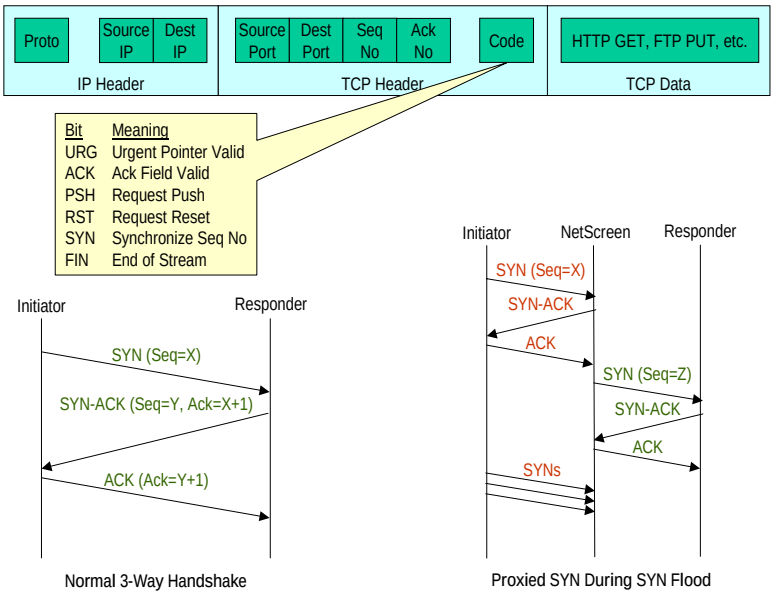

Figure 4: Protection Against SYN Attacks

Common DOS Attacks

ScreenOS is designed to withstand many other common DOS attacks. Examples include:

ICMP Flood: Attackers can flood a system with so many ICMP echo requests that it can no longer process valid traffic. Juniper Networks firewalls can ignore ICMP echo requests that exceed a configurable threshold (by default, 1,000 per second). Similar protection is provided against UDP Flood Attacks.

Ping of Death: A grossly oversized ICMP packet can create a series of fragmented packets with overlapping offset values in the packet header, triggering a range of adverse destination system reactions, including crashing, freezing, and rebooting. Juniper Networks firewalls can be configured to detect and reject such oversized and irregular ICMP packets.

IP Spoofing: Juniper Networks firewalls guard against spoofing (attackers that imitate a valid sender) by analyzing each packet's source IP address. If the IP address is not in the firewall's route table, traffic from that source is dropped.

Port Scans: By sending packets to many different destination ports, an attacker can often identify available services, then launch subsequent attacks. Juniper Networks firewalls log the ports scanned by each source IP. If a source scans 10 ports in 30 microseconds (configurable), Juniper Networks flags this as a probable attack and drops future traffic from that source. Similar protection is provided against Address Sweep Attacks.

Land Attack: If an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source address, the victim send SYN-ACK packets to itself, creating unused connections that occupy table space until they time out. By combining SYN Flood defense and IP Spoofing protection, Juniper Networks firewalls also block Land Attacks.

Tear Drop Attack: When the first and second parts of a fragmented TCP packet overlap, the server attempting to reassemble the packet can crash. If a Juniper Networks firewall sees this discrepancy in a fragmented packet, the packet is discarded.

IP Source Route: The standard IP Source Route Option can allow an attacker to enter a network with a false IP address and have data sent back to his real address. Juniper Networks firewalls can be configured to block all IP traffic that employs the Source Route Option.

Malicious Java, ActiveX, ZIP, and EXE Content: When downloaded, malicious applets and executables can install Trojan horses that compromise trusted network hosts. Juniper Networks firewalls can be configured to block all embedded Java and ActiveX applets and strip attached .zip, gzip, .tar and .exe files from Web pages.

WinNuke Attack: WinNuke is a malicious application that sends out-of-band (OOB) data — usually to NetBIOS port 139 — to a host with an established connection, introducing NetBIOS fragment overlaps that cause Windows hosts to crash. Juniper Networks firewalls can scan and correct invalid offsets in packets sent to port 139, preventing and logging the attempted attack.

Summary

A strong perimeter defense is essential for any online business. By offering a scalable family of products, Juniper Networks provides cost-effective solutions for networks of any size, with a clearly defined upgrade path. Security policies can be administered and applied uniformly across small/remote offices and central sites, with single-point definition and enforcement of firewall, VPN, and traffic management functions.

As this paper illustrates, Juniper Networks ASIC-based approach offers very high performance without sacrificing security. And ScreenOS, hardened out-of-the-box, offers ready protection against DOS attacks. By complementing silicon-based packet inspection with software-based DOS protection, Juniper Networks has created a platform that is flexible enough to withstand new attacks, yet robust enough to satisfy the availability, throughput, burst, and connection demands of even the largest enterprises and service providers.

Glossary

Access Control List (ACL) — A set of filters used to permit or deny access. Packet filters used with firewalls typically include protocol type, IP address, and/or port number.

Application Proxy — A technique used by firewalls to control access by specified applications. Application proxy firewalls intercept arriving packets on behalf of the destination, examine application payload, then relay permitted packets to the destination application.

Application Specific Integrated Circuit (ASIC) — Specially designed chips that accelerate computationally intensive tasks like firewall, encryption, authentication, and PKI processing.

Denial-of-Service (DoS) — A category of attacks intended to prevent a computer from providing service to legitimate users. Example DoS attacks include SYN Flood and "ping of death".

File Transfer Protocol (FTP) — An IETF standard application protocol for transferring files between network nodes.

Firewall — A device that filters the traffic exchanged between networks, enforcing each network's access control policy. Firewalls ensure that only authorized traffic passes into and out of each connected network, often referred to as "Trusted" and "Untrusted".

H.323 — An ITU standard that defines how multi-media conferencing data is transmitted across packet-based networks.

GigaScreen — The second generation ASIC used in Juniper Networks appliances and systems.

Hybrids — Firewalls that combine stateful inspection and application proxy techniques to optimize performance and security.

Medium Access Control (MAC) — The data link sublayer that ensures transmissions occur in an orderly and fair way over a physical interface.

MAC Address — Link layer addresses that uniquely identify network interface cards (e.g., Ethernet station addresses on an 802.3 CSMA/CD LAN).

Network Address Translation (NAT) — An Internet standard for translating IP addresses, enabling private address hiding and public address reuse.

NAT Mode — A Juniper Networks deployment option that allows a network of privately addressed hosts to share the firewall's public IP address.

Packet Filtering — A basic "stateless" technique used by routers to evaluate and permit or deny packets at the network layer. See also access control lists (ACLs).

Reduced Instruction Set Computing (RISC) — A processor architecture in which instructions are pared down to improve computing efficiency.

Route Mode — A Juniper Networks deployment option in which the firewall is inserted between separately numbered subnets that do not require address translation.

ScreenOS — The security-hardened, real-time operating system employed by all Juniper Networks devices.

Stateful Inspection — A technique used by firewalls to control access by TCP sessions and UDP "pseudo" sessions. A stateful inspection firewall maintains a session table. Entries are created for TCP connections or UDP streams that satisfy a defined security policy; packets associated with these sessions are permitted to pass through the firewall.

Transparent Mode — A Juniper Networks deployment option in which the firewall can be dropped seamlessly into an existing LAN and bridge segments of the same subnet.