

White Paper

Architecture for High Performance Financial Services Networks



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408.745.2000
1.888 JUNIPER
www.juniper.net

Table of Contents

Executive Summary	3
Introduction	3
Overview of Juniper's Solutions	3
Routers	4
Firewalls	4
Virtual Private Networks	4
Unified Access Control	4
AAA/802.1X	4
Intrusion Detection and Prevention	5
Application Security Gateways	5
Anti-virus	5
WAN Optimization	5
Application Acceleration	5
Overview of the Financial Services Network Architecture.	6
Enterprise Internal Network.	6
Secure Server Area	8
Access Network	11
Remote Access via Application Security Gateways	12
Internet Access Subnet.	13
Market Data Feeds Subnet	13
Remote Office/Branch Office Solutions.	14
Global Security Policy Management	16
Conclusion	16
About Juniper Networks.	16

Executive Summary

In recent years, the global financial services market has been very dynamic, and this has set high expectations for financial services institution (FSI) IT departments. FSI management requires IT to contribute strongly to enable customer acquisition and retention, consolidate disparate and dispersed networks, implement regulatory compliance controls and control operational costs. Emerging application technologies like voice over IP (VoIP) and service-oriented architecture (SOA) can be leveraged to deploy applications that meet these needs, but existing network infrastructures may no longer perform adequately to support these new applications.

This paper will look at Juniper Networks overall networking strategy, followed by specific examples of the ways Juniper's architecture can be applied to the typical network segments in FSI networks.

Introduction

Financial services institutions derive strategic value from their networks. FSIs constantly face trade-offs in their efforts to deliver a secure and resilient experience for their users:

- Protecting their infrastructure in the face of increasingly sophisticated and frequent security attacks, versus providing open and flexible network services to users
- Sophisticated intelligence at scale, versus superior performance
- The flexibility and economics of the Internet, versus the security and reliability of private networks

These trade-offs can be eliminated by a high-performance infrastructure that enables security and networking to work together. With this type of infrastructure, Juniper Networks customers understand not only who their users are, but also what they are allowed to do on the network. The delivery and performance of communications based on the needs of the application and the user are ensured.

Juniper Networks delivers this secure, dependable infrastructure for customers with strategic networking requirements through intelligent network solutions that operate as a service layer on top of existing infrastructures. This allows financial institutions to deliver secure and reliable applications over advanced networks while protecting their infrastructure investments. A leader in innovation, Juniper has a solid track record of delivering best-in-class networking and security products that solve the industry's most difficult problems. Hundreds of FSIs—including the top 10 commercial banks and 9 of the top 10 investment services firms—rely on Juniper Networks innovations and highly scalable, reliable networking and security platforms to deliver the best user experience at the lowest total cost of operation.

Overview of Juniper's Solutions

Juniper Networks offers a range of technologies that can be categorized into the following functional groups:

- Routers
- Firewalls
- VPNs
- Unified Access Control (UAC)
- AAA/802.1X
- Intrusion Detection and Prevention (IDP)
- Application Security Gateways (ASGs)
- Anti-virus Solutions
- WAN Optimization
- Application Acceleration

The current industry trend is the consolidation of many of these functions into a single device. Juniper, for example, offers numerous products, which incorporate LAN/WAN connectivity, firewall, VPN and Deep Inspection. Juniper also offers standalone devices, enabling the enterprise to select the right level of functionality for any given application.

Routers

Routers are the cornerstone of effective and efficient delivery of information in enterprise networks. Juniper offers a wide range of routing products from carrier-class core routers to streamlined 1U routers for smaller offices and branches. All Juniper routers run the modular JUNOS™ software, which manages many functions independently to deliver high levels of security, uptime and performance with reduced operational effort. By running multiple functions in parallel on assigned processing resources, JUNOS software delivers high stability with the flexibility to enable advanced routing, quality of service (QoS), security, and management policies with predictable performance. Once a user is trained to operate one Juniper router, he/she is able to operate any other Juniper router equally well, thus minimizing operational and training costs. Juniper maintains one code train for JUNOS, ensuring that every release is identical and simultaneously available for all routers, thus shortening training and testing times.

Firewalls

Firewalls are the cornerstone of policy enforcement in the enterprise network. Again, Juniper offers a wide range of products from the multi-gigabit NetScreen-5400 to the compact Secure Services Gateway 5 (SSG 5), with all products offering virtually the same functionality and user interface. Once again, when a user is trained to operate a Juniper NetScreen firewall, he/she is able to operate any other product in the family equally well.

Virtual Private Networks

Currently, there are two varieties of VPNs that provide data confidentiality (encryption). IPSec VPN functionality is a standard component of all Juniper Networks NetScreen firewalls. SSL VPN functionality is provided by Juniper's Secure Access line of products, which is considered to be an Application Security Gateway technology, discussed later in this document. It is important to note that other VPN technologies such as MPLS and Institute of Electrical and Electronics Engineers (IEEE) 802.1Q VLANs, while important, merely provide granular traffic separation. Only IPSec and SSL provide data confidentiality, authentication and data integrity using cryptographically secure methods.

Unified Access Control

As access to network resources has grown ubiquitous, the challenge of making resources available and preserving a high level of security has increased. Mobile laptops and non-compliant desktops are susceptible to a myriad of threats, yet must still be allowed to access the corporate network and internal resources. But providing such access without sufficient security controls opens the FSI to a number of risks and regulatory compliance challenges. Juniper's UAC solution solves the problem of balancing access and security controls by binding user endpoint, identity and network information for dynamic policy management that is enforced in real time throughout the network.

AAA/802.1X

The Juniper Networks complete family of AAA and 802.1X network access security products are suitable for wired or wireless networks of any size. This comprehensive suite of products is an important component to uniform security policy enforcement across all network access methods, including WLAN, remote/VPN, dial up and identity-based (wired 802.1X).

Intrusion Detection and Prevention

Juniper Networks IDP product line offers full layer 7 application-aware processing of packets in real time. These products employ multiple detection methods in parallel, to identify and stop intrusions. Deep Inspection functionality is also offered on the NetScreen firewall product line, providing a subset of the full IDP product. Deep Inspection is designed to focus on the most common sources of attacks, namely Web, email, FTP, Domain Name System (DNS) and Internet Control Message Protocol (ICMP).

Finally, the Integrated Security Gateway (ISG) platform provides complete integration of the IDP product line with the firewall/VPN capabilities of the NetScreen firewall products into a single chassis. The Secure Services Gateway (SSG) platform includes LAN/WAN connectivity along with firewall and IDP functionality.

Application Security Gateways

Implemented in the Juniper Secure Access product family and commonly called SSL VPNs, Application Security Gateways are typically used to provide remote access to corporate resources. The ASG is application-aware and provides very granular access policy, even down to the specific file or URL. Since the ASG relies on the SSL protocol for data confidentiality, no client-side software is required except for a standard Web browser that supports SSL. This ability to offer vendors, partners and employees secure access to user-specific resources from anywhere, without requiring special software, is unprecedented.

Anti-virus

Juniper Networks has partnered with a proven industry leader for antivirus solutions. Integrated fully in the SSG 5, anti-virus is a key security technology. For the higher performance solutions, the NetScreen firewalls can be configured to offload anti-virus to a standalone virus scanning server.

WAN Optimization

The Juniper Networks WX platforms provide distributed enterprises with a cost-effective solution for accelerating applications over the WAN. WX platforms help businesses improve application response times, maximize their WAN investments, and control and prioritize key applications by improving application performance over the WAN. This is accomplished by eliminating redundant transmissions, accelerating TCP and application-specific protocols, prioritizing and allocating access to bandwidth, and ensuring High Availability (HA) at sites with multiple WAN links.

Application Acceleration

The Juniper Networks DX Application Acceleration platform delivers a complete data center acceleration solution for Web-enabled and IP-based business applications. The DX platform improves the end user experience by delivering content quicker, and it solves IT budget, HA and security requirements through a combination of centralized services like server load balancing, global server load balancing, SSL encryption and termination, HTTP compression and application security—all on a single device. The DX platform has scaling options in both functionality and performance to accommodate different business environments.

Overview of the Financial Services Network Architecture

Experience has shown that most financial services organizations follow similar network architectures, implementing functionally distinct networking and security silos. This enables the enterprise to divide and conquer the massive challenges of securing data and maintaining High Availability. The network has become a critical infrastructure for every financial services organization, and Juniper Networks has responded to customer needs with tailored products to address key challenges.

The major network silos in most financial services networks are defined as:

- Enterprise Internal Network—where most employee computers reside (until recently viewed as a safe zone)
- Secure Servers Area (SSA)—where the most critical databases and servers reside
- Access Network—where remote employees, partners and customers access services
- Internet Access Subnet—where internal resources securely access the public Internet
- Market Data Feeds—where external news, information and trade information enters the organization

Within each silo, there are typically independent security and routing functions as well as full redundancy. Common to global financial services firms, each of these silos is duplicated for each of the geographies in which the firm operates, or at each of the firm's major data centers. Often the geographically dispersed silos are directly connected to each other; for example, the Secure Server Area in Tokyo may have a direct connection to the SSA in New York. Due to the complex nature and significant demands placed on the network, it is not uncommon for a financial services firm to have hundreds of routers, firewalls and other networking devices deployed. Thus the ability to securely and remotely manage the organization's security policy is imperative.

Connectivity to other key network components must also be ensured. For example, there may be one or more connections to remote backup data centers from the SSA. These critical links carry some of the firm's most sensitive data.

Subsequent sections of this paper detail the major network silos common to the financial services industry, the unique networking challenges associated with each, and the ways that Juniper Networks products can provide High Availability and robust security without compromising performance.

Enterprise Internal Network

The Enterprise Internal Network is where most of the access, distribution and core LAN switches are located, connecting PC users as well as trading terminals to the applications and services they require. The Internal Network is the LAN that the typical employee will use to access records and perform transactions from within a corporate controlled location. Remote access from non-corporate sites such as homes, vendors, partners and clients is discussed in the Access Network section later in this document. However, it should be noted that the objective of the Access Network is to provide secure, remote entry into the Enterprise Internal Network.

While a major portion of the firm's data is warehoused in the Secure Server Area, the majority of the transactions upon that data will take place on the Enterprise Internal Network, and a majority of the firm's employees will operate devices attached to that network. Thus, it is particularly important to enforce access policies in this network and protect applications from malicious or unwitting internal attacks.

Only authorized users should be allowed to access the Enterprise Internal Network. Juniper Networks offers a complete family of RADIUS/AAA and policy management servers for FSIs, available in a variety of form factors. The Steel-Belted Radius® Family (SBR) provides centralized user authentication and access policy management. SBR gives enterprises control over how users access and use their networks—preventing unauthorized access, ensuring that users comply with security policies before they connect, and granting the appropriate level of access to each user.

Juniper's UAC enables the FSI to bind user identity in SBR or other AAA solutions to endpoint assessment, ensuring that authorized users access the Enterprise Internal Network using only devices compliant with the FSI's security policy. For example, UAC can ensure that the network is accessed by an authorized user whose device is properly secured against viruses, trojan horses and worms. UAC endpoint assessment is performed dynamically, and any change to the endpoint device is automatically registered by UAC, so that the appropriate policy is enforced.

Once on the Enterprise Internal Network, users' access should be limited to the servers of the functional group in which they work, and should be limited to using protocols that are necessary for their business unit's mission. For example, it is unlikely that a retail banking manager should be performing SQL queries to the mutual fund manager's databases. Juniper Networks firewalls enforce the policies configured on UAC, ensuring that access is controlled throughout the network. For organizations without UAC, judicious use of firewalls will prevent access to resources through the concept of *security zones*, whereby each user group and each resource group are contained in separate zones. Policy is enforced by Juniper firewalls when traffic crosses zones, and this provides the opportunity to provide stateful traffic filtering based on IP addresses, port numbers and protocols.

Furthermore, Juniper's IDP technology enables the firewall to provide protection from layer 7 attacks like the malicious use of Internet protocol ambiguities. For example, a Simple Mail Transfer Protocol (SMTP) message may be purposely formed incorrectly with the intent of causing a buffer overflow in the target server. The buffer overflow could cause the server to hang or worse open a trapdoor for an attacker to exploit. By utilizing IDP, protocol compliance can be guaranteed and the risk of this type of exploit from within the firm can be greatly reduced.

The Enterprise Internal Network may contain a significant amount of multicast traffic as a result of conference calls, Web-casts and ticker data. It is imperative that the firewall selected provides linear performance under load. Performance is not simply a measure of best-case throughput with a single firewall rule and 1500 byte packets. Today's networks demand near line-rate throughput with 64 byte packets, driven mainly by the increase in VoIP traffic. In addition, the ability for the firewall to perform a stateful session setup without introducing latency is important as more traffic becomes interactive in nature.

Most traffic on the Enterprise Internal Network will be IP, consisting heavily of HTTP/HTTPS and Network File System (NFS) as well as some NetBIOS over IP. Typical applications seen in this network silo include Web-based transactions, streaming media, email, Remote Procedure Call (RPC), as well as legacy "green-screen" IBM mainframe access. Database protocols like DB2 and SQL, which have been exploited at large scale in the past, will also appear on the Enterprise Internal Network. Protocol compliance checking through Deep Inspection or Intrusion Detection and Prevention may greatly reduce the risk from these exploits.

Support protocols like those used for antivirus updates, Microsoft product updates, and remote desktop for helpdesk support will be present on the network also, so it is important to restrict the way these protocols are used to prevent virus and trojan activity from remotely exploiting systems. Internet access from the Enterprise Internal Network should be closely controlled and routed through the Internet Access silo, which will be discussed in detail later.

To appropriately protect the Enterprise Internal Network traffic, IT managers need an adaptive and flexible security safeguard that is able to identify and protect against issues arising from the various Internet Engineering Taskforce (IETF) standard protocols, as well as proprietary, custom-built protocols.

Each functional group (for example traders, personal money managers, retail banking, human resources, facility operations) should be confined to the minimum subset of resources required to complete their mission. By using a firewall to provide compartmentalization based on job duty, the likelihood of unauthorized insider access is greatly reduced and a barrier to worm proliferation during attack is also created. This network compartmentalization supports three common best practices, namely: Need to Know, Least Privilege and Separation of Duties.

The Juniper Networks NetScreen-5000 Series provides high port density and a multi-gigabit firewall that is capable of providing the segmentation necessary to secure different functional groups within the Enterprise Internal Network. The NetScreen-5000 family can be populated with as many as 72 Fast Ethernet or 24 Gigabit Ethernet ports and is the industry's only multi-gigabit firewall with sub-second *stateful failover*.

NSRP (NetScreen Redundancy Protocol) is the cornerstone of Juniper's HA security systems. This protocol enables various configuration options between the firewall and adjacent switches and routers. The protocol has been proven in the field, in the most demanding of environments, and works seamlessly with products from other vendors such as Cisco, Extreme Networks and Foundry Networks. When configured for stateful failover, sessions and VPN tunnels running through an active system that has a component or link failure are automatically transferred to the standby firewall in as little as 50 milliseconds¹.

To further support the separation of duties, in some situations *virtual systems* may be configured in the NetScreen firewall. This feature divides the physical system into numerous logical partitions for management and policy configuration. Each administrator has visibility only to the interfaces that have been designated as part of their virtual firewall.

This feature may be particularly useful when consolidating numerous software-based firewalls to a single NetScreen system. If each of the older firewalls were controlled by separate administrators, the NetScreen firewall can be logically divided into numerous virtual systems. For yet another added level of separation, the NetScreen firewalls support the concept of *virtual routers*, whereby multiple separate routing tables are maintained by the system. This feature is generally used to hide internal route announcements from external routing peers. Juniper Networks has implemented these features, as well as virtual LANs or IEEE 802.1Q *VLANs* to provide customers with as many virtualization techniques as possible, as well as unparalleled flexibility to firewall and network administrators.

The Enterprise Internal Network is one of the most demanding silos, since virtually all connections will be either 100 Mbps Ethernet or Gigabit Ethernet. The need to support near line-rate performance is most important here and in the Secure Server Area which is described below. Depending on the network configuration and the firm's requirement for compartmentalization, the NetScreen-5000 family can be considered as a secure replacement for aging distribution switches. This stems from the ability of some or all of the firewall interfaces to operate in *transparent mode*, whereby the interfaces appear to the network as layer 2 bridge ports instead of routed interfaces. This feature also facilitates the installation of the firewall in an established network that requires increased security, but where IP address changes would be costly or impractical to implement. Virtually no function is lost by operating in transparent mode.

Secure Server Area

The Secure Server Area houses the firm's most critical systems and data. The SSA is usually contained in a physically secure location with limited access. Each connection into the SSA should be highly scrutinized and multiple layers of security should be employed. This silo will typically contain a large number of servers and possibly mainframes.

The challenges of securing and assuring the SSA include:

- High Throughput/Large Number of Connections: Since so many users are accessing the SSA at any point in time, the need to support high throughput aggregated across potentially tens of thousands of users is imperative.
- Low Latency: – Just as throughput is important, so too is latency. Latency should not increase as the number of simultaneous connections increases.
- High Availability: Since so much critical information is centrally located in the SSA, just a few moments of downtime could result in a large amount of lost business.

¹Configuration dependent.

- Worm Containment: It is imperative that worms not infiltrate the SSA. The systems contained in the SSA must be the most secured and most resilient to attack since so many operations rely on these systems.
- Cost Control: Because of the proliferation of applications, servers, storage and networking devices in the SSA, controlling capital and operational expenditures can represent a significant challenge to the FSI and can directly impact organizational efficiency metrics.

The SSA is attached to all of the other network silos so there should be high-performance and highly available routers and firewalls at each connection to the SSA. Without this, the SSA represents a significant potential performance bottleneck and provides an attacker easy access to the firm's most critical records.

Juniper Networks M-series Multiservice Edge Routing Portfolio uniquely combines advanced IP/MPLS capabilities with a high degree of reliability, stability, security and service richness. The M-series has been constructed with scale and stability in mind, including the modular and fault-protected design of JUNOS software and a rigorous system testing process. All M-series routers offer redundant power and cooling. The M10i and larger routers offer fully redundant hardware, including redundant routing engines and switching/forwarding engine boards. JUNOS software features enhance this redundant architecture: nonstop forwarding is enabled in the event of a routing engine failure via a hitless switchover, and in-service software upgrades are supported when a minor software upgrade is required. Other HA capabilities include Graceful Protocol Routing Restart, MPLS fast reroute, Virtual Router Redundancy Protocol (VRRP), SONET Automatic Protection Switching (APS), SDH Multiplexer Switching Protection (MSP), Bidirectional Forwarding Detection (BFD) protocol, and Link Aggregation Control Protocol (LACP).

As noted above, because of the centrality of the SSA and its importance to the organization, an attacker might exploit the SSA as a means to attack any other network silo.

The Juniper Networks ISG 2000 with Deep Inspection features, or ideally with ***Integrated Security Module***, provides firewall as well as intrusion prevention for the most critical systems. The Integrated Security Module provides the intrusion prevention features of the NetScreen IDP product line as an add-in feature to the ISG platform.

In particular, firms that rely on Windows-based systems should utilize the protocol conformance and application-aware Deep Inspection technology available from Juniper. By ensuring that software on employees' computers are abiding by the rules of various IETF protocols (as defined in RFCs), Juniper's Deep Inspection technology can eliminate many attacks that leverage buffer overflows and invalid parameters not properly handled by operating system software in servers. Even if a vulnerability has not yet been discovered, many exploits can be prevented by ensuring protocol conformance even prior to the software vendor releasing information on the vulnerability or a patch for it.

If the ISG 2000 does not match the performance requirements of the SSA connections, then a firewall in series with a NetScreen IDP product can be used to provide application-level awareness and inspection of the traffic into the SSA. IDP devices can flag (log and report) or drop malicious traffic.

Business Continuity initiatives are often centered on providing near real-time backup of the SSA data center to a remote location. All data transferred to the remote backup location should be encrypted using IPSec with a strong algorithm such as triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES). This can easily be accomplished using the built-in IPSec VPN capabilities in the entire NetScreen firewall product line, particularly the NetScreen-500 or NetScreen-204, depending on throughput available on the WAN link used for backup.

Some network administrators commonly use Access Control Lists (ACLs) to prevent users on particular subnets from accessing other subnets. But ACLs provide a false sense of protection since IP addresses can easily be spoofed. There are numerous attack methods available to completely and easily circumvent ACLs. Only a stateful packet filtering firewall can dynamically learn what packets are valid and which are spoofed, malicious or erroneous. Protecting the SSA with ACLs is a glaring mistake commonly found in networks.

In addition to ensuring the connectivity and security of the SSA, it is important to ensure the availability and performance of the applications and data that reside within. This is particularly important as FSIs adopt Web-enabled and IP-based technologies to deliver critical applications like business performance management, customer resource management, human resources management, and proprietary FSI applications to remote users, partners and customers.

Juniper Networks DX Application Acceleration Platforms increase server availability and performance, while protecting existing resource investment and helping control new capital expenditure requirements. This is accomplished by offloading core networking and I/O responsibilities from Web and application servers. The DX platforms also simplify and improve the data center architecture by incorporating the functionality of multiple point products, like server load balancers (SLBs), Web accelerators, SSL terminators, and cache and proxy servers into a single platform.

With Juniper DX Application Acceleration Platforms, time to access business-critical applications is typically cut in half, leading to a boost in application usability and acceptance. The DX platform optimizes and compresses all outgoing Web data in real time—without adding latency. Content fidelity is maintained, bandwidth use is dramatically reduced, and users experience faster page loads. The DX platform also increases the capacity of applications by serving as a transaction broker, managing all connections and requests between servers and users. The DX platform maximizes available server and network resources, freeing server CPU for other tasks and yielding up to a 10x increase in server/application capacity. Also, using full layer 4-7 server load balancing functionality, DX supports the deployment of multiple applications and server clusters behind a single DX platform, which performs non-synthetic network, server and application health checking to ensure that users are served by the best resource.

As FSIs develop and deploy new business applications or productivity applications like IP telephony that must be delivered to remote and branch offices, distributed employees, customers and partners, demands on WAN connections increase. Even when applications and servers are accelerated and optimized, FSIs encounter challenges delivering applications that were not designed to be accessed over networks. These challenges include inefficient bandwidth utilization and network latency. Additionally, the proliferation of even IP-based applications can lead to challenges associated with contention. Juniper Networks WX and WXC™ WAN acceleration platforms overcome bandwidth, latency and contention challenges by integrating several interdependent technologies, including next-generation compression, sequence caching, TCP and application-specific acceleration, bandwidth management and path optimization—all in one device.

By positioning WX platforms in the SSA and one in each remote or branch office, FSIs can deliver applications and data across the wide area at LAN-like speeds. This allows for the removal of application, database and file servers from remote locations, and helps control costs by limiting IT management requirements at remote locations. Furthermore, centralizing important files and data simplifies business continuity and disaster recovery planning, streamlines backup and restore processes, and helps FSIs better comply with regulatory compliance requirements. Used simultaneously, Juniper Networks WX and DX platforms enable FSIs to centralize and consolidate resources. The result is lowered capital and operational expenditures, investment protection, and better return on assets.

Access Network

The Access Network is the primary entrance to the enterprise. While the Internet Access silo is also attached to the global Internet, that silo is provided for internally initiated traffic only and will be discussed in the next section. The Access Network provides entry into the enterprise via a variety of physical connections that include leased lines to branches, partners and large customers, private and managed MPLS networks, as well as connections via the public Internet possibly utilizing VPN protocols.

The Access Network requires a diverse variety of access technologies to be aggregated, secured and delivered to the Secure Server Area and Enterprise Internal Network. High Availability, accomplished through the stateful failover of all devices in this silo, is imperative. The organization's Internet presence is dependent on this portion of the network remaining available.

The Access Network will likely require a variety of routers with interfaces varying from DS0 to OC-12 or greater. Juniper Networks M-series multiservice edge routing portfolio spans from 5 up to 320 Gbps of throughput. The same scalable and production-hardened JUNOS software runs on all IP/MPLS M-series platforms, making a consistent set of capabilities available at all network locations, regardless of customer connection or serving-area density.

With its broad interface portfolio, a single M-series multiservice edge routing platform can provide a single point of edge aggregation for thousands of users over any access type—including Asynchronous Transfer Mode (ATM), Frame Relay, Ethernet, and time-division multiplexing (TDM)—and at any speed from DS0 up to OC-192/STM-64 and 10 Gigabit Ethernet. The M-series leverages dense Ethernet and highly channelized interfaces to deliver high densities.

Rich packet processing enables the M-series to support multiple levels of granular QoS per port, per logical circuit (DLCI, VC/VP, VLAN), and per channel (to DS0) for traffic prioritization. These comprehensive QoS functions include classification, rate limiting, shaping, weighted round-robin scheduling, strict priority queuing, weighted random early detection, random early detection, and packet marking. To facilitate network convergence, layer 2 class of service (CoS) can be mapped to layer 3 CoS on a per data-link connection identifier (DLCI), per virtual path (VP)/virtual circuit (VC), or per VLAN basis. Simultaneously, extensive statistics can be collected and diagnostics performed at this same level of granularity, to enable traffic planning, rapid troubleshooting, and to support regulatory compliance efforts.

If the organization offers IEEE 802.11 wireless access throughout a large facility, the wireless access points are typically aggregated and backhauled to this silo for processing as untrusted connections, just as if the attaching devices were located outside the facility. This is done to remove the chance of unauthorized access by individuals in the facility parking lot or other locations. Unless the access points are equipped with the latest IEEE 802.11 encryption technology and security mechanisms, an external VPN approach is the only secure method for providing wireless access at a facility.

The Access Network is very demanding in terms of security, since this is the first network that Internet-based attackers will encounter. Similarly, if a partner or customer is compromised, an attacker may attempt to gain access through a leased line connection or through a VPN tunnel from a remote site. Therefore, tunnels should be terminated at this silo so that deep packet inspection or intrusion detection/prevention can be performed on the unencrypted traffic.

Because of the Access Network's high degree of connectivity and the importance of HA and high performance, the security products used here must be capable of interoperating with a variety of routers and *dynamic routing protocols* such as RIP, OSPF and BGP-4.

The first line of defense in the Access Network silo is the firewall, deployed in fully redundant pairs. At a minimum, these firewalls should provide integrated firewall, IPSec VPN capability and **Network Address Translation** (NAT) so that the connections from the Internet and leased lines can be filtered, and encrypted tunnels can be terminated prior to packet filtering. The NetScreen-5000 family or NetScreen-500 are excellent selections for firewalls in this silo. They provide as many as 25,000 IPSec VPN terminations, as well as stateful failover for those sessions in case of a power disruption or service provider link failure.

Intrusion detection and prevention solutions like the Juniper IDP-1000 should be used to augment the firewall in this silo. By providing application-aware intrusion prevention here, attackers that have successfully infiltrated partners or vendors are denied malicious access into the SSA. In recent years, these partner and vendor links have been successfully exploited by hackers in numerous high profile attacks.

To streamline security device deployment and simplify security management, Juniper Networks ISG platforms combine firewall, VPN and IDP functionality with multi-gigabit performance on a single device. The ISG Series provides the throughput and networking features that are required to protect high-speed perimeter and internal network deployments, where advanced applications such as VoIP and streaming media dictate network and application level protection with consistent, scalable performance.

Within the Access Network, a customized security posture which provides exactly the required security level for each application, including SYN thresholds, Distributed Denial of Service (DDoS) prevention customization and protocol conformance, can be developed using Juniper Networks firewalls and IDP products. Additionally, Secure Access products, discussed next, can provide superior remote access capabilities.

Remote Access via Application Security Gateways

For mobile employees, Juniper recommends the use of the Secure Access product line. The Juniper SA 5000 is a high-performance, application-aware remote access device which provides clientless access from anywhere that a standard Web browser is available to the employee. The SA 5000 supports two-factor authentication with seamless integration to LDAP and RADIUS servers, like Juniper Networks SBR RADIUS/AAA policy management servers.

While IPSec VPNs are ideal for providing remote sites a secure encrypted tunnel back to the data center, the SSL VPN technology used in the Secure Access products is intended to provide ubiquitous secure access based on user credentials and security analysis of the PC the employee is using. A security policy can even be designed such that employees utilizing a public PC at an Internet café or other kiosks have restricted access to specific applications, or possibly read-only access.

Another advantage of using SSL VPNs for remote employee access is the ability to specifically limit access based on application and user. Since IPSec VPNs provide an open pipe between two sites, they can create security holes for remote employees, especially those using home networks with children, who are all too often the source of malware and other security exploits.

IPSec VPNs and SSL VPNs both provide equally strong encryption algorithms; the difference between the two is the level of application awareness that is desired when permitting access into the enterprise. SSL VPNs are also ideal for vendors and contractors who require very limited access to the firm's resources. The audit log capabilities of the Secure Access products are also noteworthy, as they support compliance with various regulations.

Internet Access Subnet

The Internet perimeter provided by the Internet Access silo is primarily focused on filtering communications that originate from inside the Enterprise Internal Network and Secure Server Area. In order to filter outbound communications from the organization to the global Internet, the Internet Access silo is employed differently in financial services firms than in most other enterprises. While the Access Network silo is responsible for access into the firm, the Internet Access silo is responsible for connecting with and securing a fairly small number of protocols and servers.

Due to the sensitivity of data and directional restrictions of data flow, typical traffic in this silo is initiated by users inside the Enterprise Internal Network, mostly using IETF standard protocols such as HTTP, HTTPS or FTP. Another widely used protocol would be streaming media protocols such as real-audio, and Microsoft Streaming Media as a result of employees viewing Webcasts.

For many firms, the protection offered by the NetScreen-204 and NetScreen-500 with Deep Inspection capabilities enabled is sufficient. Deep Inspection provides application-aware firewall for the most common IP protocols, namely HTTP, FTP, ICMP, DNS and SMTP/point of presence (POP).

Of course, NAT and the ability to seamlessly integrate into the network, either via Transparent Mode or with a dynamic routing protocol such as BGP-4, is imperative. Depending on the number of employees accessing the Internet from within the enterprise, the session setup rate may be a factor in the firewall selection. The need for IPSec or other tunneling technology is minimized in this silo, since IPSec tunnel termination is a function of the Access Network.

For advanced security such as Instant Message logging, a NetScreen IDP product can augment the firewall and provide compliance with various government regulations and corporate policy.

Market Data Feeds Subnet

Unique to the financial services industry is the need for a Market Data Feeds network silo in the network architecture. A major challenge of this network segment is the need to securely aggregate streaming data feeds that carry latency-sensitive real-time market data for a multitude of sources. Market data is usually comprised of streaming, latency-sensitive real-time ticker data streams but may also include business wire news or other perishable data. Low latency and linear throughput under load are particularly important in this part of the network. And depending on the source, a large portion of the data can arrive in small packets.

Adding to the complexity, the institution, in certain situations, may be required to forward these feeds, in part, to partners or customers. As noted above, Juniper Networks M-series routers include a comprehensive suite of multicast capabilities that include multicast over MPLS VPNs to enable efficient distribution of multicast content.

Often the Market Data Feeds silo is comprised of numerous leased lines or other permanent circuits, but some feeds may arrive from the Internet via IPSec tunnel. Regardless of how the data arrives, the need to filter unwanted protocols as well as authenticate the source is imperative. History has shown that these links, if left unchecked, can be exploited by attackers and used by worms to propagate malicious code.

Typically, there is little control over the authenticity of the market data feeds, but wherever possible, financial services organizations should request cryptographic authentication of the streams using a protocol such as IPSec with the MD-5 or SHA-1 authentication algorithm applied to the data. When the market data is public in nature, there is no need to encrypt it, but when possible, the data should be authenticated to ensure that it is originating from a trusted source. An attack which generates false trade data could cause havoc in the market.

Another challenge in the Market Data Feeds silo is to ensure that only pertinent protocols traverse the links. For example, it is unlikely that RPC or telnet traffic should be entering through a market data feed link. It is imperative that the firewall filter extraneous or potentially malicious packets. An additional check that should be performed is source address validation.

Unlike the Access Network silo, the need for deep and intelligent application-level packet inspection is reduced, since only a limited number of protocols should be traversing these links. A better use of resources would be to employ anti-spoofing and DDoS prevention features available on Juniper's firewall products. The need to define protocol behaviors and alert on anomalies is still important in this silo, therefore an intrusion detection and prevention system such as Juniper's IDP 500, *used in detection mode*, may be appropriate in this portion of the network. The IDP products, when used in detection mode, will not drop traffic or increase latency as packets traverse the network, but these devices do provide a high degree of visibility into the network segment and can swiftly alert network administrators as to potential problems, such as worms, that may be attempting to access the network. Detection mode is used when the IDP product is **not** placed in-line with the firewall, but rather is attached in a look-aside configuration, using a span port or mirrored port on a switch.

Using the IDP in detection mode provides a tremendous amount of insight into the traffic flow, with zero risk of a trade being dropped. When used with the Enterprise Security Profiler (ESP), the IDP product provides unprecedented insight into the operation of the network. ESP allows the network or security manager to not only identify exploits quickly, but also to identify where the exploits are targeted and sourced.

Also unique to the financial services industry is the need to potentially support proprietary protocols from the market data feed providers. Juniper's firewalls are protocol-agnostic and can provide a high degree of stateful security for protocols without the firewall having to be configured with specifics of the protocols or applications.

Some firewall vendors do not support multicast and require unnatural encapsulation of multicast traffic into unicast packets for firewall processing. This results in increased latency and potential problems with packet maximum transmission unit (MTU) sizes, fragmentation, packet ordering and address translation. Juniper firewalls have support for multicast traffic and do not require special encapsulation, which is particularly important in the Market Data Feeds silo.

Since this portion of the network is aggregating numerous sources, port density and the ability to route or bridge (transparent mode) may also be an important consideration when selecting security products.

Remote Office/Branch Office Solutions

In recent years, a confluence of events has driven FSIs to revisit their approaches to remote office and branch office infrastructure. Customers have become used to accessing information and services from a variety of channels—telephone, Internet, ATM machines, and in person. Where branches were once dedicated facilities, they now appear within the confines of other businesses and locations like hospitals, and supermarkets. ATM machine functionality now includes support for broader services, and ATMs appear in locations outside of branches like airport kiosks or even as mobile branches. Roaming employees and telecommuters require access to network resources from locations both inside and outside the control of the organization.

In addition to the drive to create competitive advantage in acquiring and retaining customers, FSI IT managers must contend with increasing regulatory compliance and cost control expectations. For both compliance and cost control, successful strategies increasingly include significant resource consolidation. Managing and securing data for purposes of compliance is greatly simplified by removing resources from branches and centralizing them in the data center. The consolidation of servers, storage and other data infrastructure in the data center also reduces the capital expenditures of new branch development, as well as operational expenditures related to managing resources and data.

Technological innovations have also created opportunities for consolidating branch office resources. The development and adoption of IP telephony enables organizations to consolidate voice and data networks into one easier-to-manage and cheaper-to-own network. The flexibility to initiate, move and close branch offices while controlling costs and increasing productivity makes IP telephony an attractive solution for FSIs.

The result of business and environmental changes has been large-scale branch renewal projects with applications and data being centralized, and the infrastructure supporting them being consolidated. Existing applications are replaced or redesigned to leverage IP protocols and are centrally managed at the data center. Application, email and database servers are removed from the branch, also relocated to the data center. Voice applications like PBXs are similarly relocated. Voice and data networks are consolidated, simplifying network deployment and management, and enhancing disaster recovery/business continuity efforts.

However, implementing changes to network infrastructures to overcome the challenges of branch renewal has not been trivial. The centralization and consolidation of applications and resources pursued by many financial organizations require highly available and high-performance network infrastructures. Any network downtime or degradation of service can result in lost productivity, lost revenue generation and poor customer experience. Some examples of performance and availability challenges introduced by centralization include:

- HTTP Web traffic generates 10 times the traffic of existing applications
- Email and server centralization generate latency issues
- IP telephony signaling creates extra traffic
- Voice requires low latency to ensure high quality

Additionally, along with the widespread adoption of new technologies, there has been an increase in security threats to information and resources. These threats can incapacitate businesses, violate regulatory requirements, and significantly damage the FSI brand. Some examples of security challenges include:

- Intrusion attempts that target branches because they are perceived as weak points in the network
- Attacks that originate from within and from outside the network
- The proliferation of viruses and worms that enter via email, disks, or on computers that have been taken out of the branch environment

Whatever the size of the branch, Juniper Networks offers an array of solutions that help FSIs reduce the IT footprint of each location relative to other similarly sized locations. FSIs can increase the flexibility and productivity of their branches, while reducing total cost of ownership and simplifying regulatory compliance processes.

The performance of business applications at the renewed branch should provide FSI branch users the same experience they would enjoy if newly centralized applications and/or data were still local. Juniper Networks WAN application acceleration platforms significantly increase the performance of financial applications, email, document imaging transfers, file sharing and other business activities. WX delivers a combination of capabilities that include advanced compression, sequence caching, packet acceleration, bandwidth management and traffic shaping, path optimization, and Common Internet File System (CIFS) acceleration. These increase the effective throughput of existing WAN links several-fold, while at the same time overcoming network latency and contention. The result is the ability to effectively deploy new technologies like IP telephony, and remove resources from the branch like Exchange and file servers to increase effectiveness while reducing capital and operational expenditures. Regulatory requirements like Check 21 are also more easily met, thanks to higher performing and more intelligent network infrastructures.

The remote office or branch office should also be secured. Juniper Networks supplies a range of products that meet the needs of various sized branch offices. For smaller branch offices and branch-alternatives like ATMs, FSIs can deploy Juniper Networks NetScreen-5 Series integrated security solutions that combine firewall, IPSec VPN, antivirus, intrusion detection and prevention, denial of service mitigation, and Web filtering functionality—all in a single device. The 5 Series also supports a variety of routing protocols and optional wireless capabilities. Despite the small size of the device, the 5 Series consists of enterprise-class security solutions supporting full redundancy, sub-second firewall and VPN tunnel failover, and provides support critical for FSI security features like anti-spyware and anti-phishing.

For larger branches, Juniper Networks SSG provides the same advanced features as the 5 Series with increased throughput. Furthermore, all Juniper firewall devices support advanced virtual routing features that enable FSIs to consolidate security resources by increasing interface density without additional hardware expenditures. The result is lower policy creation costs, better containment of unauthorized users and attacks, and simplified VPN management.

Global Security Policy Management

No security policy is worth the investment unless it can be securely and reliably enforced. Juniper Networks has developed a centralized policy and device management tool, NetScreen-Security Manager (NSM), which is a fully integrated management solution for managing all aspects of the NetScreen firewalls.

Administrative access to specific devices can be limited by user, but more importantly, commands can be restricted to user sets. This enables a security organization to be segmented into various administrative groups based on job responsibilities. A network engineer can be provided access to commands that change the IP parameters of devices, but not any security policy. Likewise, an entry level helpdesk employee might be given limited read-only access to perform cursory problem determination, while the corporate security officer may be given global security policy control.

NSM has been deployed in some of the world's largest networks, with thousands of firewalls being efficiently managed. NSM allows the security officer to abstract the security policy to a simplified series of rules. Then the NSM software deploys the device-specific policy files to each firewall under control.

Conclusion

Juniper Networks networking and security products are deployed by many of the world's largest banking and financial networks. Juniper has evolved the functions provided in these products by listening to customers, and continually striving to provide technology that solves the real business problems that today's financial services institutions face. Juniper Networks has literally invested billions of dollars to ensure technical dominance with purpose-built, application-specific integrated circuit (ASIC)-based routing and security products, as well as application and network acceleration solutions—all with security and High Availability as paramount objectives.

Juniper's unique technology, coupled with complementary solutions from other best-of-breed vendors, provides unprecedented security, performance and resiliency so that FSI employees, customers and partners receive a secure and assured network experience.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS FOR
NORTH AND SOUTH AMERICA
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS
Juniper Networks (UK) Limited
Building 1
Aviator Park
Station Road
Aldrestone
Surrey, KT15 2PG, U.K.
Phone: 44.(0).1372.385500
Fax: 44.(0).1372.385501

EAST COAST OFFICE
Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978.589.5800
Fax: 978.589.0800

ASIA PACIFIC REGIONAL SALES HEADQUARTERS
Juniper Networks (Hong Kong) Ltd.
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

Copyright 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS 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.

To purchase Juniper Networks solutions, please contact your Juniper Networks sales representative at 1-866-298-6428 or authorized reseller.