Building a Software-Defined Secure Network for Financial Services

Detect, adapt, and enforce security policies faster with network-wide visibility, orchestration, and control

Challenge

Enable digital transformation at financial services firms by eliminating threats inside and out.

Solution

Juniper's Software-Defined Secure Network, which includes SRX Series Services Gateways for branch and data center, vSRX virtual firewall, Spotlight Secure cloud service, Sky Advanced Threat Prevention, and Junos Space Security Director, provides an open, scalable way to block threats at every step of the cyber kill chain.

Benefits

- Expand threat visibility and enforcement capabilities across the entire network infrastructure
- Provide flexibility and agility in responding to threats
- Reduce time between threat detection and enforcement
- Simplify management with a platform for creation, deployment, and replication of common security policies across a global enterprise

The digital economy is transforming the financial services sector. The pace of innovation is accelerating, customers have higher expectations than ever, and new competitors are emerging from nontraditional markets. At the same time, financial services has long been a favorite target of cyber attackers, and despite firms' best efforts, cybersecurity threats are rising and attacks are more successful than ever. Financial services firms need a more effective, adaptable approach to detecting and stopping cyberthreats.

The Challenge

Traditionally, network security has meant a strong perimeter defense. Firewalls sat at the boundary of the network, checking everything coming inside, while everything on the inside of the network was trusted. That's no longer enough. Advanced threats can bypass traditional perimeter security defenses, enter the trusted network, and move about undetected. Employees' and contractors' mobile devices can be infected when used on public or home networks, and that malware can be inadvertently unleashed inside the corporate network. The risk increases exponentially with the rise of the Internet of Things. In the data center, virtualization and cloud have brought new agility, but modern security technologies have failed to keep pace with evolving threats. As a result, threats can persist unseen inside the network, giving criminals time to carefully plan the theft of high-value information, commit fraud, destroy brands, and disrupt global markets.

Employees and contractors rely on regional and branch networks to access applications and other resources to do their jobs. Customers count on websites and mobile apps to interact with their banks, insurance companies, and other financial providers. Attackers commonly target branch resources and mobile devices because these systems have access to business-critical applications, but it can be very difficult for security administrators to control and monitor today's highly distributed environments for suspicious activities. Security pros need greater visibility into business applications, whether they are in the data center or in the cloud. Data privacy is critical to maintain competitive advantage and regulatory compliance, but data sent to and from data centers over service provider networks or the public Internet is at a great risk for eavesdropping, even if appropriately encrypted.

Data center networks are also prime targets for attackers, as they run the core operations for financial services firms and are home to the organization's most valuable information and applications. In addition to data theft and destruction, a denial-of-service (DoS) attack can overwhelm the data center network and prevent workers and customers from accessing critical resources and financial accounts. A DoS attack can be just as damaging to business viability as the exfiltration of high-value data.

To thrive, security professionals can no longer view internal networks as trusted and external networks as untrusted. *In today's cybersecurity threat landscape, all network traffic must be viewed as untrusted*.

The Juniper Networks Software-Defined Secure Network

Juniper's Software-Defined Secure Network (SDSN) creates a holistic security ecosystem that enables financial services firms to react in near real time to current and evolving intelligence to protect against unknown threats. SDSN delivers a zero trust model for information security.

With SDSN, financial services firms can make the shift from a traditional, siloed approach to security to viewing the network as a single enforcement domain. Network policy, detection, and enforcement become more adaptable, and firms can stop threats with greater accuracy. Security administrators can create and manage policies that are tightly aligned with business policies, rather than micromanaging security for different VLANs and security zones.

Software-Defined Secure Networks

Policy	Create and centrally manage security through a user intent-based system
Detection	Unify and rate intelligence from multiple sources
Enforcement	Enforce policy in near real time across the network, and have the ability to adapt to network changes

With an SDSN approach, threats can be detected faster, even as they evolve, by leveraging threat intelligence from multiple sources (including third-party feeds) and tapping into the power of the cloud. Network security can adapt dynamically to real-time threat information so that security policies are enforced consistently, even in a global enterprise. The building blocks of a Software-Defined Secure Network include advanced firewalls for the branch and data center, threat intelligence, orchestration, and cloud-based protection.

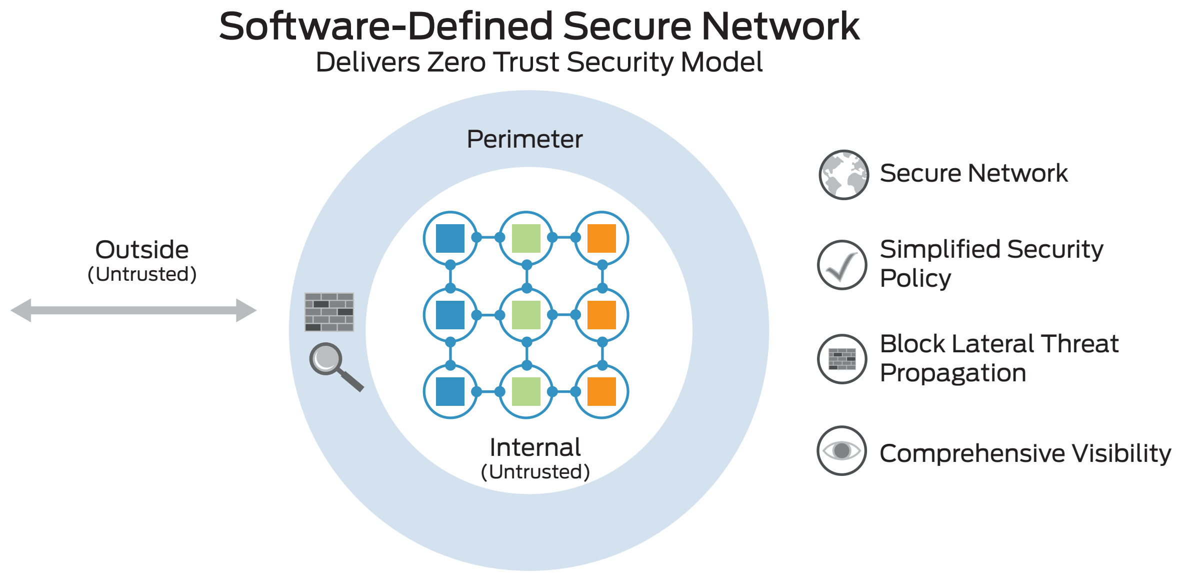
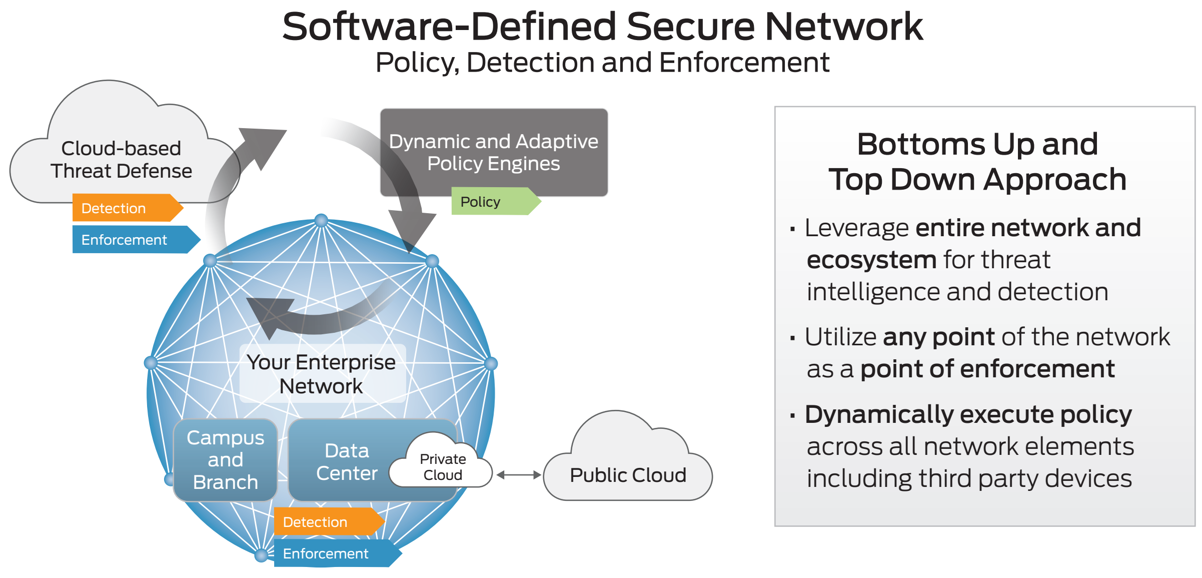

Software-Defined Secure Network
Delivers Zero Trust Security Model
Perimeter
Outside
(Untrusted)
Internal
(Untrusted)
Secure Network
Simplified Security Policy
Block Lateral Threat Propagation
Comprehensive Visibility

Figure 1: Juniper's SDSN is based on a zero trust security model.


Software-Defined Secure Network
Policy, Detection and Enforcement
Cloud-based Threat Defense
Detection
Enforcement
Dynamic and Adaptive Policy Engines
Policy
Your Enterprise Network
Campus and Branch
Data Center
Private Cloud
Public Cloud
Detection
Enforcement

Bottoms Up and Top Down Approach

- Leverage **entire network and ecosystem** for threat intelligence and detection
- Utilize **any point** of the network as a **point of enforcement**
- **Dynamically execute policy** across all network elements including third party devices

Figure 2: SDSN simplifies creating security policies, detecting threats, and enforcing policies.

Securing Branch Office Networks in Financial Services

Juniper Networks® SRX Series Services Gateways for the branch combine next-generation firewall and unified threat management (UTM) services with routing and switching in a single, high-performance, cost-effective network device. SRX Series gateways provide network connectivity to regional or branch locations using standards-based routing protocols. A small branch SRX Series gateway also provides switching to connect a small number of endpoints, while a large SRX Series gateway can provide WAN connectivity and switching for a regional office.

SRX Series gateways also support full, standards-based IPsec encryption to ensure the secure transport of business data across networks that are not managed, controlled, or secured by the firm's security administrators, whether the organization uses a shared service provider network or the public Internet.

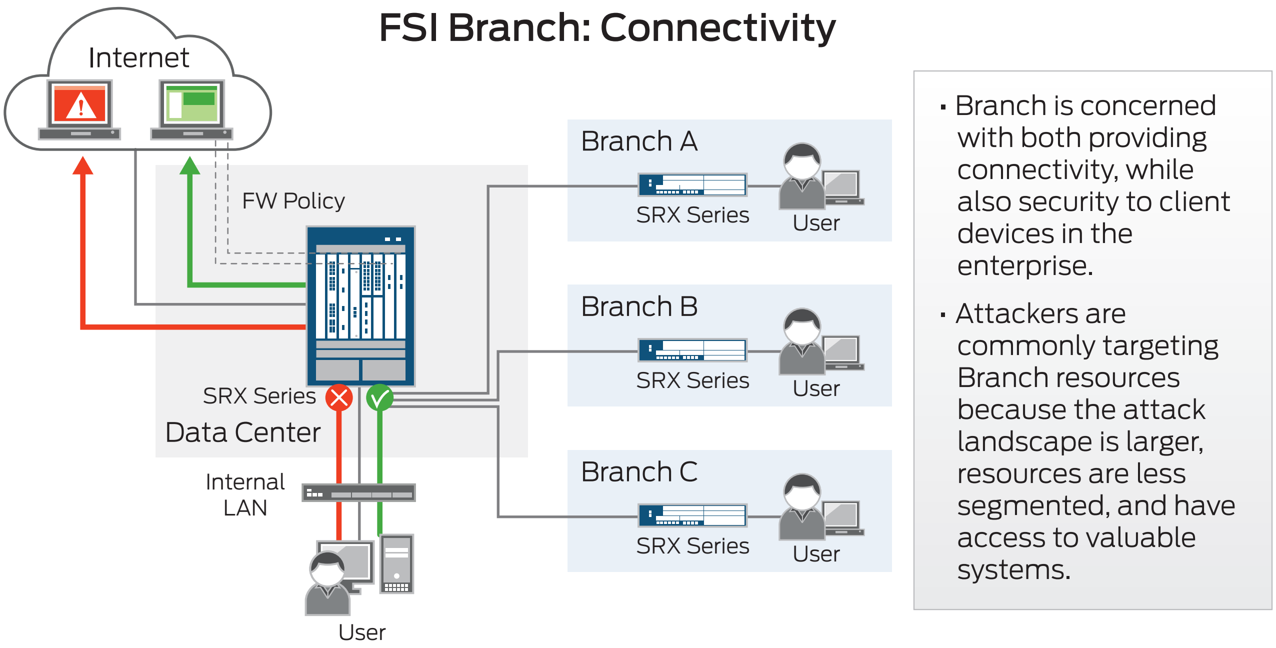

FSI Branch: Connectivity
Internet
FW Policy
SRX Series
Data Center
Internal LAN
User
Branch A
SRX Series
User
Branch B
SRX Series
User
Branch C
SRX Series
User
▪ Branch is concerned with both providing connectivity, while also security to client devices in the enterprise.
▪ Attackers are commonly targeting Branch resources because the attack landscape is larger, resources are less segmented, and have access to valuable systems.

Figure 3: Secure network services architecture supports financial services branches.

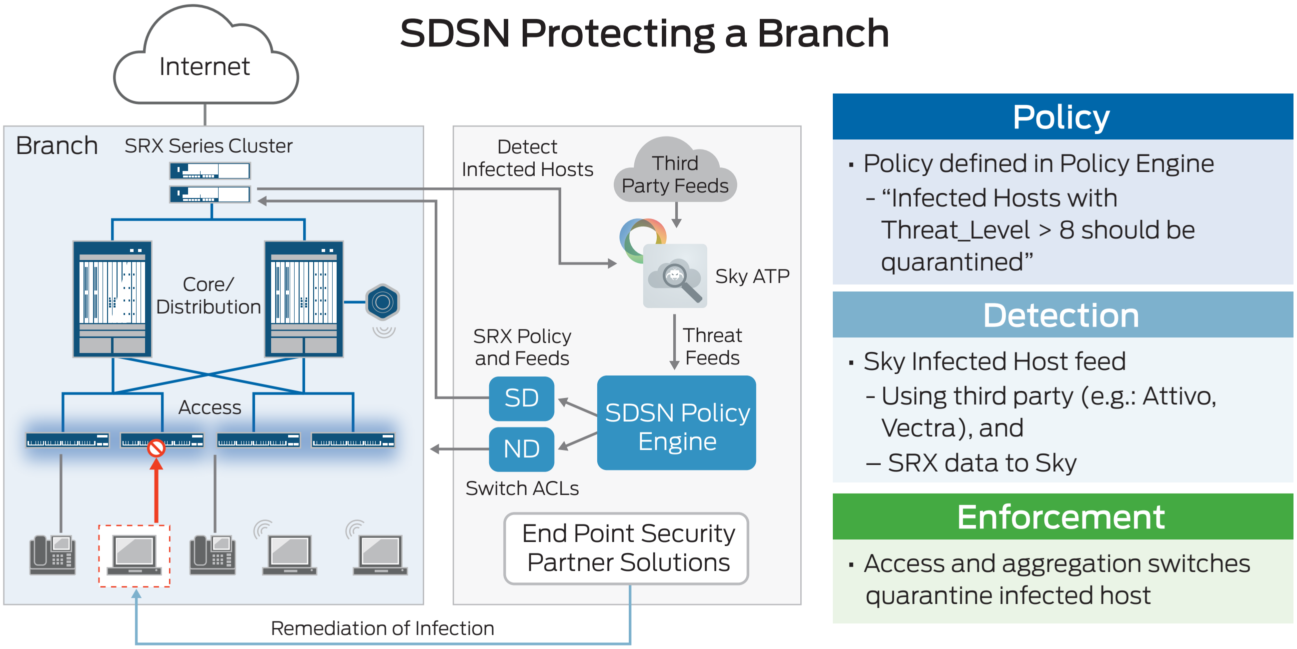


Figure 4: SDSN makes it easier to protect branches with consistent security policies, threat detection, and enforcement.

Securing Data Center Networks in Financial Services Through Micro-Segmentation

Financial services firms of all sizes can defend their data centers with Juniper's portfolio of enterprise security solutions. SRX Series Services Gateways are a next-generation, anti-threat firewall with advanced, integrated threat intelligence, delivered on the industry's most scalable and resilient platform.

SRX Series gateways set new benchmarks with 100GbE interfaces, and also provide connectivity options for 1GbE, 10GbE, and 40GbE. Express Path technology enables up to 2 Tbps performance for the data center and with less than 7 microseconds of throughput latency. All SRX Series gateways can encrypt and decrypt traffic across shared and public WANs using IPSec VPN, and can simultaneously support thousands of VPN tunnels. In cloud and virtual environments, vSRX virtual firewall can be deployed to provide east-west separation for traffic to meet requirements of micro-perimeterization and micro-segmentation addressing today's virtual workloads. The vSRX is the industry's fastest virtual security platform, providing scalable, secure protection for data centers and cloud. This level of advanced security is extended to Docker Containers with Juniper

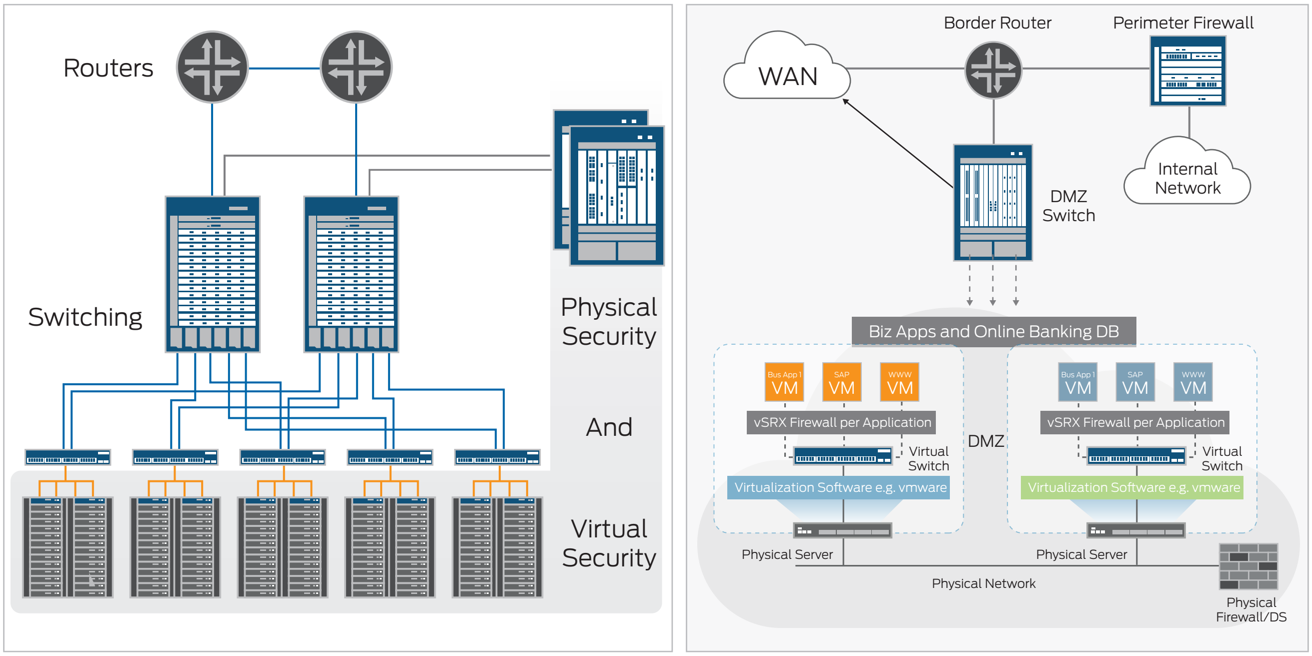
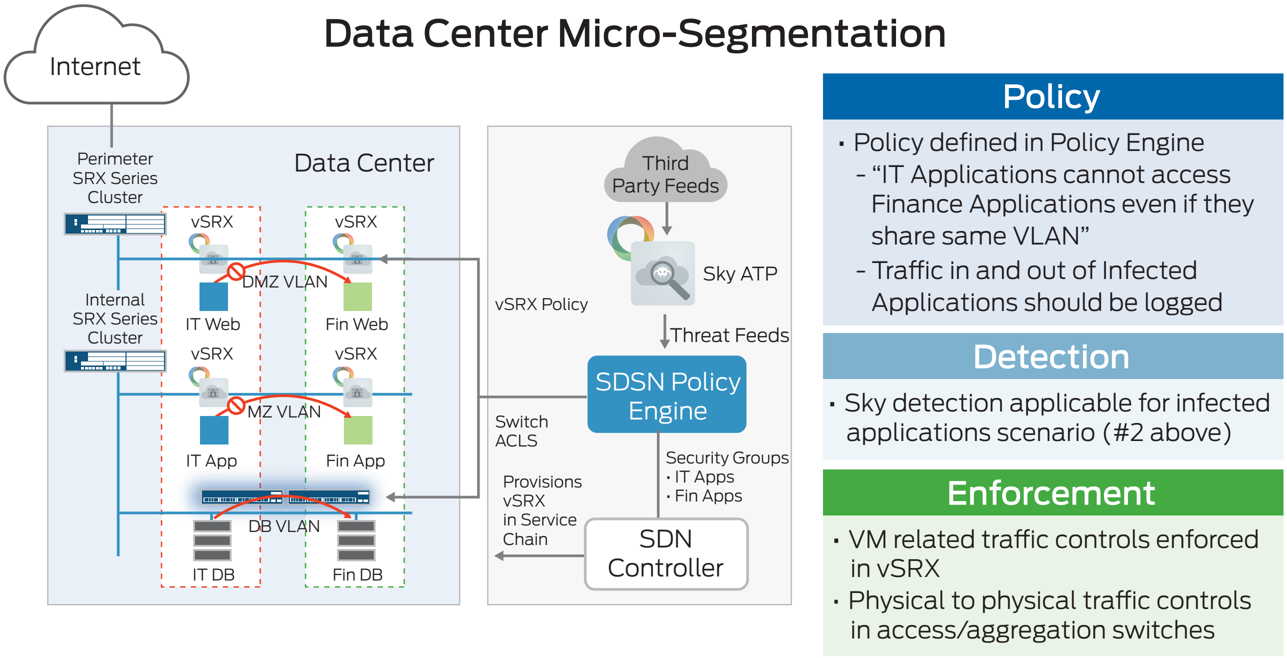


Figure 5: Micro-segmentation allows zoning and segmentation created by SRX Series gateways (both virtual and physical).



Policy

- Policy defined in Policy Engine
  - "IT Applications cannot access Finance Applications even if they share same VLAN"
  - Traffic in and out of Infected Applications should be logged

Detection

- Sky detection applicable for infected applications scenario (#2 above)

Enforcement

- VM related traffic controls enforced in vSRX
- Physical to physical traffic controls in access/aggregation switches

Figure 6: Juniper simplifies extending security to every segment in the data center using micro-segmentation.

Networks cSRX container firewall and brings greater agility and elasticity to virtual infrastructure. The cSRX has a microservices architecture that makes deployment throughout the network easier without compromising performance.

Unified Security Enforcement on a Common Platform

SRX Series security capabilities are consistent whether the SRX Series device is deployed as an appliance, a scalable chassis, or virtually—and whether it is protecting traditional physical architectures or virtual and cloud applications. Policies are enforced consistently to meet the needs of any financial organization of any shape or size.

Separation of Control and Data Planes

High volumes of traffic and processor overutilization can cause a firewall to become unmanageable and block user access to business resources if the firewall is designed with shared control and data planes. Juniper Networks Junos® operating system, the foundational operating system of the SRX Series gateway, is designed with the separation of control and data plane. When under a DoS attack, the SRX Series firewall provides strict policing protection of the control plane so administrators can maintain management connectivity with the platform, while screens and additional mechanisms can be put into place to minimize the impact that a DoS attack might have on the data plane.

Next-Generation Firewall Services and Application Inspection

SRX Series gateways provide security enforcement and deep inspection across all network layers and applications. Users can be permitted or prohibited from accessing specific business applications and Web applications, regardless of the network ports and protocols that are used to transmit the applications. Deep inspection can be applied via intrusion prevention policies for any traffic that is allowed to pass through the SRX Series, so security administrators can ensure that the desired traffic running across an organization's network is legitimate and is not being manipulated as an attack vector.

Application- and user-based firewall policies can be combined to ensure that specific users within a financial organization's network can only access the specific business applications that they are authorized to access. Antivirus, content filtering, and antispam enforcements can be layered on top of these policies to round out the full spectrum of application-based services that can be applied to network traffic running through the firewall.

Enhanced Threat Intelligence and Spotlight Secure

To enhance traffic visibility and provide an additional layer of protection against advanced persistent threats, SRX Series gateways support IP address blocking via geo-IP and command-and-control botnet feeds. This additional threat intelligence is delivered via Juniper Networks Spotlight Secure cloud service, and is updated constantly to ensure that the threat data employed in the firewalls is accurate and fresh. IP address threat data is applied within security policies quickly and without requiring a commit of the configuration. This means that the new threat data within firewall policies can be applied in less than 60 seconds after being updated within the Spotlight Secure cloud service. A financial organization also can automatically enforce and block IP addresses on SRX Series firewalls from threat data that is created internally, or with data from a third-party threat feed. All of this threat data can be delivered and enforced on SRX Series firewalls within 60 seconds.

Sky Advanced Threat Prevention

As malware attacks evolve and grow more insidious, conventional anti-malware products have difficulty defending against them. Sky Advanced Threat Prevention keeps the network free of sophisticated zero-day attacks and other unknown threats by delivering superior cloud-based protection, scanning ingress and egress traffic for malware and indicators of compromise.

Sky Advanced Threat Prevention, which employs a pipeline of technologies in the cloud to identify varying levels of risk, provides a higher degree of accuracy in threat protection. It integrates with SRX Series gateways to deliver deep inspection, inline malware blocking, and actionable reporting.

Sky Advanced Threat Prevention's identification technology uses a variety of techniques to quickly identify a threat and prevent an impending attack. These methods include:

- Rapid cache lookups to identify known files
- Dynamic analysis that involves unique deception techniques applied in a sandbox to trick malware into activating and self-identifying

Additionally, machine-learning algorithms let Sky Advanced Threat Prevention adapt to and identify new malware in an ever-changing threat landscape.

Centralized and Orchestrated Policy Enforcement with Security Director

In today's complex environment, if management solutions are slow, unintuitive, or restricted in their level of granularity and control, network security management can become overly time-consuming and prone to error.

Junos Space Security Director provides centralized and orchestrated security policy management through an intuitive, web-based interface that offers enforcement across emerging and traditional risk vectors that financial organizations face every day. As an application on the Juniper Networks Junos Space platform, Security Director provides extensive security scale, granular policy control, and policy breadth across the network for every SRX Series physical and virtual device. Security administrators can use Security Director to quickly manage all phases of the security policy life cycle for stateful firewall, threat intelligence from Spotlight Secure, unified threat management (UTM), intrusion prevention system (IPS), application-based firewall, IPsec VPN, and Network Address Translation (NAT).

Summary—Stop Threats Faster with Juniper Security Solutions

Juniper's Software-Defined Secure Network can help security administrators in financial services organizations stop threats faster and more accurately. It can also help them gain greater control over the applications and traffic on their regional, branch office, and data center networks while protecting business assets against increasingly sophisticated—and successful—cyberthreats.

SRX Series Services Gateways deliver next-generation firewall protection with application awareness, IPS, and user role-based control options plus best-in-class UTM to help protect and control financial business assets. Financial services firms can choose from a broad range of models: from all-in-one security and networking appliances, to highly scalable, high-performance chassis options, to virtual and cloud-based enforcement platforms. Juniper's security intelligence for SRX Series gateways is designed to respond to a rapidly changing threat landscape, and as an open security intelligence solution, it is extensible based on business needs. Spotlight Secure delivers actionable security intelligence that can be used in policy immediately. Sky Advanced Threat Prevention integrates with SRX Series firewalls for detection and enforcement, and provides dynamic, automated protection against known malware and advanced zero-day threats, resulting in instant threat response. Administrators can centrally manage all SRX Series gateways using Junos Space Security Director, and other security services are easily added to existing SRX Series platforms for a cost-effective and easily managed solution.

Next Steps

To bring the power of Juniper's Software-Defined Secure Network to your firm, contact your Juniper representative, or go to www.juniper.net/us/en/solutions/software-defined-secure-networks/.

About Juniper Networks

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

3510569-001-EN May 2016