TechTarget Custom Media
A TECHTARGET IMPACT REPORT

4 Strategies for Keeping Critical Networks Secure

Simplify the Network

Setting directions for your cybersecurity programs is like starting to assemble a thousand-piece jigsaw puzzle: You need to fit together a central cluster of pieces now, while making sure you can build toward a complete picture in the future.

Selecting the right technology providers is an essential part of this process. You need to find partners that can address today's security needs, and also have the vision, resources and track record to offer you new options in the future. Those partners must help you take advantage of innovative technologies while leveraging your existing investments. Finding partners with "the right stuff" can be particularly challenging if you have mission-critical requirements for high performance, high reliability and comprehensive security against evolving threats.

This short paper highlights four criteria for selecting the right security partner for the long term. It concludes by discussing how Juniper Networks is meeting those criteria.

Criterion #1: Breadth and Depth of Capabilities in One Solution

Enterprises today are challenged by the continuing proliferation of threat actors and new attack methods. In addition, enterprise "attack surfaces" are expanding as cloud computing, mobile devices, and mobile applications increase the number of vulnerabilities cybercriminals and hackers can target.

To address these challenges, you have to deploy a comprehensive set of defenses, including next-generation firewalls (NGFWs), antimalware packages, intrusion prevention systems (IPSs), application firewalls, monitoring and visibility products, and security management tools. These defenses need to complement each other and share information.

When security services are comprehensive and integrated they:

- Simplify operations and lower management costs
- Increase performance and reliability
- Reduce the inconsistencies and errors that lead to data breaches
- Provide visibility into threat events and data across the network, so you can identify attacks faster
- Generate automated responses, so you can block advanced attacks sooner

What do these issues imply for cybersecurity planning and vendor selection? They mean that deploying "point products" opportunistically is no longer a viable strategy. You need to look for a long-term security partner that can provide a broad range of key security offerings, integrate them, support them together, and enhance and expand capabilities as new security technologies become available.

Expectations of reliability have also gone up. Corporate executives expect security solutions to be working effectively with "four nines" or "five nines" availability

Criterion #2: Mission-Critical Scalability, Performance and Reliability

Breadth and depth of functionality is certainly critical, but so too is the performance and reliability of security solutions.

Distributed users, cloud computing and new bandwidth-intensive applications are generating unprecedented volumes of network traffic. To be effective today, security solutions need to scale up and be able to scan these data flows at "wire speed." The alternatives—holding back application traffic at peak times until scanning catches up, or allowing traffic to pass through unexamined—are unacceptable.

Expectations of reliability have also gone up. Corporate executives expect security solutions to be working effectively with "four nines" or "five nines" availability. Anything less gives attackers too many opportunities to penetrate the network undetected.

Yet many vendors focus entirely on security features and treat scalability, performance and reliability as afterthoughts. Look for security partners who have a track record of successfully supporting high-volume mission-critical environments with excellent performance and reliability.

Criterion #3: Threat Intelligence: Open Source and the Backing of an Expert Team

Cybercriminals are continuously developing new forms of malware. Hackers are constantly setting up new botnets and command and control (C&C) servers to disguise their attacks. You need the best possible threat intelligence to alert you to new attacks and suspicious IP addresses as soon as they are identified anywhere on the Internet.

In fact, you should look for security solutions that integrate two types of threat intelligence: feeds from open (publicly available) sources such as malware clearinghouses and security industry associations, and information from an established cybersecurity research lab that can validate and prioritize threat indicators.

If you are developing your own internal threat intelligence capability, you also want it to be easy to integrate your partner's threat feeds with your security tools and organization.

You also need a mechanism to distribute threat indicators to all of the enforcement points across your enterprise, quickly and reliably. That prevents zero-day attacks and new targeted attacks from finding vulnerable points in obscure corners of your network.

Look for a security partner who gives you a mechanism to aggregate multiple types of threat feeds, and to automate the process of distributing them to enforcement points.

Criterion #4:
A Vision for Software-Defined Networking

Security today is all about fast response:

- Updating defenses to detect new threats
- Shutting down ongoing attacks as soon as the first indicators are discovered
- Deploying new security services when and where they are needed to protect data and new business applications and data

Software-defined networking (SDN) is going to be a critical enabler for providing fast response and agility in mission-critical environments.

> Juniper Networks is a clear leader in designing security solutions that provide the very highest levels of performance and reliability.

Traditionally, network configurations and services, including security services, are embedded in specific hardware devices. That makes the configurations and services static and rigid. Changes in networks and security policies must be made manually on each system, using laborious, error-prone processes.

SDN implements configurations and policies in software so they can be created and distributed programmatically across diverse hardware devices and environments, including virtual and cloud-based environments. SDN also automates processes for making changes, so adjustments can be made with minimal manual effort and fewer errors. It promotes business agility and makes security more reliable, while reducing administrative costs. You should look for a security partner who is already delivering SDN and has a vision of how it can reach its full potential in the future.

How Juniper Networks is Addressing These Criteria

Juniper Networks has a proven track record of providing world-class networking and security solutions for the most demanding mission-critical environments in the world. Let's look at how it is addressing the problems and challenges discussed in this paper.

Criterion #1: Breadth and Depth of Capabilities in One Solution

Juniper Networks SRX Series Services Gateways provide a wide variety of critical security services, including:

- Stateful firewall capabilities
- Unified threat management (UTM) technologies such as antivirus, antispam, Web filtering and content filtering
- Intrusion prevention system (IPS) capabilities
- Protection against denial of service (DoS) and distributed denial of service (DDoS) attacks
- Application firewall and application quality of service (QoS) features
- SSL encryption and decryption and support for IPSec VPN tunnels

The Sky Advanced Threat Prevention service adds an additional layer of security. Sky Advanced Threat Prevention is a cloud-based service that uses static analysis, dynamic analysis (sandboxing), and unique deception techniques to detect new forms of malware and zero-day threats.

The breadth of security technologies included in the SRX Series Services Gateways and Sky Advanced Threat Prevention allow you to defend against malware, phishing and social engineering attacks, DDoS attacks, malicious URLs and many other threats with one integrated solution.

Criterion #2: Mission-Critical Performance and Reliability

Juniper Networks is a clear leader in designing security solutions that provide the very highest levels of performance and reliability. For example, SRX5800 Services Gateways have been

documented handling network traffic up to 2 terabits per second, and SRX Series Services Gateways can provide 99.9999% availability.

Recently the independent analyst firm Enterprise Strategy Group (ESG) ran simulations of two business computing environments with Juniper SRX5400 devices. The simulation of a financial services company found that two of these devices could handle 900,000 concurrent sessions with a throughput of almost 20 Gbps. A simulation of a scientific research institution performing high-volume downloads and data transfers yielded a line rate throughput of 197 Gbps.[1]

Criterion #3: Threat Intelligence from Open Sources and Juniper Source Feeds

Juniper's Spotlight Secure threat intelligence platform gathers a wide range of threat intelligence from Juniper's own threat intelligence organization, from third party threat feeds, and from threat detection devices you have already installed on your network.

Junos Space Security Director can take threat intelligence from Spotlight Secure and use it to update thousands of firewalls simultaneously, without the need for manual changes to firewall policies.

Together, Spotlight Secure and Junos Space Security Director allow you to distribute an extensive set of threat indicators to all of the enforcement points across your enterprise, quickly and reliably. That helps you neutralize zero-day attacks and advanced attacks in progress before they can do serious damage.

Criterion #4: A Dynamic Vision for SDN

Juniper Networks is leading the industry in turning the concepts of software-defined networking into working products. Juniper has built SDN into its security offerings, including the SRX Series Services Gateways, as well as into its networking and network management solutions.

For details on Juniper's approach to SDN, please see Agility Without Compromise with Juniper SDN and Customer Benefits Through Automation with SDN and NFV.

Summary: Selecting the Right Security Partner for the Long Term

Where can you look for a long-term security partner that can address today's needs and has the vision, resources and track record to anticipate and address tomorrow's challenges?

Juniper Networks is a great place to start. Today the company is satisfying the networking and security needs of many of the largest and most demanding enterprises and service providers in the world. Juniper has integrated a wide range of leading-edge security technologies and simplified management, visibility and the continuous delivery of threat intelligence to enforcement points. Juniper is also on the leading edge of implementing the concepts of software-defined networking in order to increase business agility and security.

For more information, please visit www.juniper.net/unite.

1 "ESG Lab Review: Performance and Scalability with the Juniper SRX5400," Enterprise Strategy Group, March 2015