Learn About Software-Defined Secure Networks (SDSN)

This *Learn About* introduces you to Software-Defined Secure Networks (SDSN), focusing on why they evolved and what security technology they deploy. Juniper Networks is a leading networking vendor in this space, offering a range of products and solutions that constitute SDSN today.

Evolving Threat Landscape

A recent, in-depth report by economic and cybersecurity experts at RAND (http://www.rand.org/pubs/research_reports/RR1024.html) found that chief information security officers are faced with a chaotic and confusing landscape when deciding how to manage the risks (and costs) associated with providing security to their business.

More troubling is the fact that the research indicated that while companies are increasingly spending on cybersecurity tools, they are not sure whether these investments are making their infrastructure more secure. Many do not know when, or whether they have invested enough in their security strategy. Even more concerning is the common belief that attackers are gaining quickly.

Cybercrime was second highest reported economic crime as per PwC Economic Crime Survey 2016. Year 2016 turned out to be a record year for cybercrime which included largest data breaches to date, an explosion of DDoS attacks, and number of ransomware variants.

Figure 1 shows some of the cybercrime statistics that explain how threat climate continues to expand (Source: Symantec Internet Security Threat Report 2017, Verizon 2016 Data Breach Investigations Report).

Figure 1 Eye-Opening Cybercrime Statistics

Figure 2 shows attack vector samples of what are the biggest threats in the 2016. (Source: 2016 Data Breach Investigations Report).

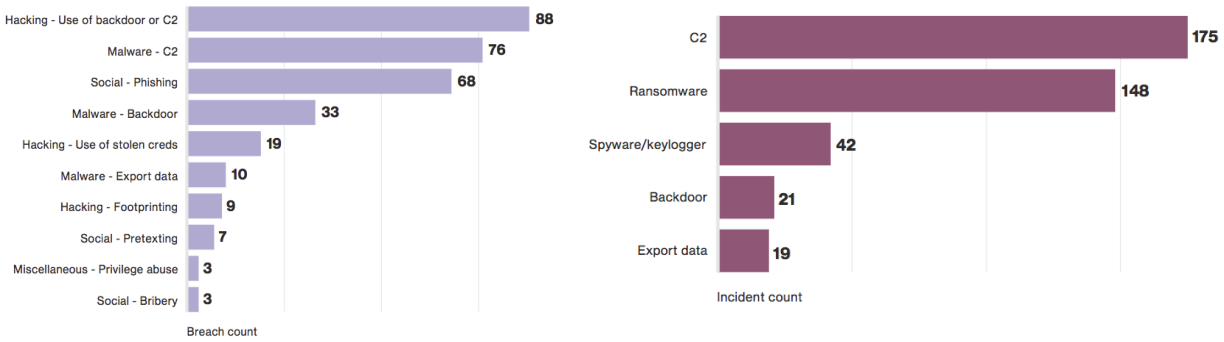

Figure 2 Top Threat Action Varieties within Cyber-Espionage and Top Five Malware Varieties

Managing risk is a misunderstood concept in cybersecurity, usually focused on risks posed by threats and vulnerabilities instead of risks specific to business outcomes and operations. Much of the emphasis is often on – and even the metrics used to demonstrate the value of security programs are based on – the ability of a particular tool or program to stop a certain number of attacks rather than those metrics that matter more to the business.

Instead of measuring the quantity of blocked attacks, the goal of a comprehensive security program must be to understand the return between managing where to invest and the risk of not adopting various security measures. Therefore, although stopping attacks is an imperative, it must also be balanced with reducing the risk to business if an attacker were to get through.

What made these seasoned security experts nervous? Unfortunately, it is the ability of advanced threats to bypass traditional perimeter security defenses, enter their trusted network, and move about undetected. The traditional network security posture of building a strong perimeter defense, where devices at the edge are the primary means of defense for all types of threats, is becoming less and less effective. Why? Because the perimeter defense that checks everything coming inside is based on the trust/no trust model – trust what's inside the network, don't trust what's outside coming in. This model is no longer pertinent nor sufficient. Advanced threats can bypass traditional perimeter security defenses, and they can enter the trusted areas and stay there undetected. That greatly increases the surface area of the attack because the perimeter has now been lost.

How and where one needs to deploy security has changed.

The Perimeter Collapses

How has this happened? Here are some recent developments that have weakened the perimeter approach to network security:

- *Failing to deploy at all endpoints* – Any smartphone or tablet that connects to a corporate network is an endpoint, and must be secured. If employees in an organization use VPN to connect from remote locations, their devices become endpoints, too. And with the proliferation of BYOD and the Internet of Things (IoT), trying to secure endpoints is nearly impossible.
- *Increasing threat sophistication* – Threats have changed from phishing, malware, and morphing executables to security hackers who infiltrate enterprises to retrieve data for financial gain. The attacks are targeted and focused, and use advanced persistent threat (APT) processes. The attackers have the advantage of time on their side, while their victims have the disadvantage of organizational and network complexity working against them. It is crucial to control botnets' attack vector before it can be used as an APT and migrated into mobile devices.
- *Insider threats* – You now need to secure every point of access in your network, because it is not just the intruder trying to break in. The threat can be your employee who has walked through your front door with malware on their device, or an employee who was developing software in a container and accidentally copied malware into the code. The security posture is quickly evolving into *zero trust* of anything entering or leaving the network.
- *Virtualization and cloud infrastructure* – The burgeoning growth of cloud services adds new layers of infrastructure complexity. Security issues can include data breaches, handling security incidents, sensitive data access, exploited system vulnerabilities, malicious insiders, management console security, account control, and multitenancy issues. Failure to ensure appropriate security protection when using the cloud can ultimately result in higher costs and loss of business.
- *Managing security across multiple environments operating in an incoherent and unorchestrated manner* – The use of different public/private cloud offerings by organizations can make network security operations extremely complex. The daily proliferation of security devices and policy enforcement points further adds to the complexity of new application deployments. With the advent of cloud, custom applications can be now be hosted in legacy data centers, or in private clouds or in public cloud. In addition, usage of SAAS applications are becoming more prevalent. If your management solutions are slow, unintuitive, or restricted in their level of granularity and control, your network security management becomes overly time-consuming and prone to error. The result? Your unorchestrated security management can actually make your network vulnerable to cyberthreats.

Coping with This Threat Landscape

To cope with today's broad threat landscape, you need threat intelligence and immediate threat enforcement. And that means a comprehensive security platform that can tie together and coordinate various threat analytics platforms. You also need a method of providing a simpler policy mechanism. Above all, you must be able to leverage the entire network, not just the perimeter, as a threat detection and enforcement solution.

The paradigm is changing to security solutions that can deliver comprehensive yet coordinated protection by:

- Integrating and deploying advanced security features to protect systems and data from spyware, viruses, malicious code, denial-of-service attacks, and more.
- Building a network flexible enough to deliver new services without causing a security gap and with improved performance and resilience (high availability).
- Using policy automation to adapt and enforce policy in real time and improve both compliance and business agility.
- Providing an automated, end-to-end network with endpoint security across the Web, e-mail, files, and applications.
- Creating comprehensive visibility into the entire network so that you can identify and address threats wherever they are detected, inside or outside the network perimeter.

The paradigm is also changing to solutions that can combat the new breed of hackers, by treating the internal network just like the Internet or an untrusted network, and by:

- Treating every port in the network as untrusted, including ports outside your network, inside your network, and between endpoints and cloud applications.
- Encrypting *all* communications with advanced encryption techniques to secure network communications.
- Understanding the new threat landscape and quarantining infected endpoints in real time, and making the network adaptable, to automatically detect aberrant behavior and immediately respond.

And finally, the paradigm is morphing into using the network itself as a detection and enforcement ecosystem by:

- Enabling every part of the network to be a detection as well as an enforcement point to respond to suspicious activity anywhere in the network, which is the most effective way to deal with threats and intruders.
- Centralizing the security policy engine so that it can determine trust levels between network segments by collecting real-time threat information.
- Closing the gap between threat intelligence and enforcement because threat intelligence loses most of its value if it is distributed too slowly, or if it does not reach all of the enterprise's enforcement points.
- Creating a unified security policy, with distributed new policies implemented in real time from a central location.

SDSN – The Path Forward

Software-Defined Secure Networks (SDSN) is Juniper's vision of applied threat intelligence and immediate threat enforcement. It is the future of network security because by leveraging the cloud, it can more effectively and dynamically solve the litany of current network security issues cited earlier in this *Learn About*.

SDSN works on the following principles:

- Leverage the entire network as points of threat detection and enforcement.

- Leverage the economy of the cloud to share threat intelligence at scale and to accelerate threat detection and make it adaptable in real time.
- And implement a centralized controller/policy engine that dynamically adapts policy and so stays ahead of constantly evolving threats and attacks.

Figure 3 illustrates the building blocks of a Software-Defined Secure Network that includes advanced firewalls for the branch and the data center, threat intelligence, orchestration, and cloud-based protection. You can see in Figure 3 that SDSN is the industry's only inside-out security model because it leverages the network as a sensor for delivery of context-aware threat alerts and then dynamically enforces security policy with software-defined segmentation designed to reduce the overall attack surface. SDSN promotes a *zero trust* model for information security that is fundamentally more secure, because even if one application on the network is compromised, you can isolate that infection or threat. You can protect the more critical assets inside your network.

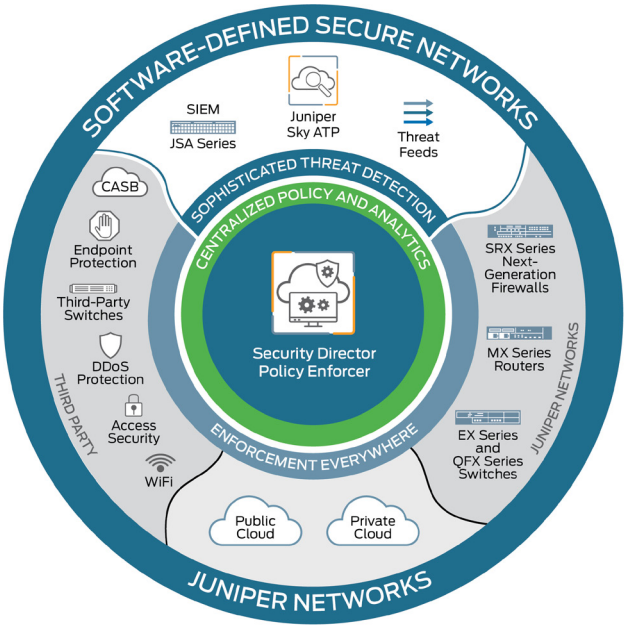

Figure 3 *SDSN Building Blocks*

Juniper Networks SDSN has the following salient features:

- *Visibility into network*. With SDSN, you get full visibility of all the traffic, whether it is North–South or East–West. The entire network infrastructure is operationalized and managed as a single enforcement domain (unified enforcement domain), providing enforce- ment point including third-party switches across the wired and wireless network where policy can be deployed dynamically, and in unison, to block threats anywhere.
- *Comprehensive security.* With SDSN, the firewalls, virtual or physical, are right-sized for their application in the network – for example, to provide consistent, automated defense across diverse environments with advanced firewall and unified threat management (UTM) capabilities whenever needed. These capabilities are consistent across both physical and virtual platforms; therefore, with SDSN the device not only meets the security requirement but is also configured

with the same policy as other devices, thereby simplifying the operation of the whole network.

- *Streamlining policy enforcement across the network*. In an SDSN network, cloud-based security services provide the foundation for an open policy engine especially when you have security controllers that can push those policies into the network. By providing real-time feedback between firewalls, the controller plus the cloud can deploy policy across network devices the instant it is needed.
- *Third-party integration*. SDSN is grounded in integrating third-party capabilities, in an effort to unite the good guys against the bad guys. Open architecture and suite of APIs enables SDSN networks to choose their preferred threat intelligence information sources and remediate across multivendor network infrastructure.

Threats can be detected faster with an SDSN approach because SDSN detects threats as they evolve, by leveraging threat intelligence from multiple sources (including third-party feeds) and tapping into the power of the cloud. When security policies are enforced consistently, be it in global networks or private clouds, network security can adapt dynamically to respond to real-time threat information.

Resources and References

Resources for learning more about SDSN, including product information, solution briefs, and press releases:

- http://www.juniper.net/us/en/solutions/software-defined-secure-networks/
- https://www.juniper.net/assets/us/en/local/pdf/solutionbriefs/3510569-en.pdf
- https://www.juniper.net/assets/us/en/local/pdf/solutionbriefs/3510608-en.pdf
- http://www.juniper.net/assets/us/en/local/pdf/infographics/sdsn-in-action.pdf
- http://investor.juniper.net/investor-relations/press-releases/press-release-details/2015/The-New-Economics-of-Defense-First-of-Its-Kind-Heuristic-Model-Empowers-Companies-to-Make-Smart-Security-Investments/default.aspx

YouTube SDSN Video with an overview of the solution, features, and benefits:
https://youtu.be/dTMGw5Byi8E

A recent, in-depth report by economic and cybersecurity experts at RAND:
http://www.rand.org/pubs/research_reports/RR1024.html

ZDNet Special Feature about the cybersecurity industry's 2015 predictions:
http://www.zdnet.com/article/cybersecurity-in-2015-what-to-expect/

Learn About Software-Defined Secure Networks (SDSN)

by Madhavi Katti

You need threat intelligence and immediate threat enforcement to cope with today's threat landscape. You also need a comprehensive security platform that can coordinate various threat analytics platforms. Most importantly, you need to leverage the entire network, not just the perimeter, as a threat detection and enforcement solution. You need to learn about SDSN.

About the Author:
Madhavi Katti is an Information Development Engineer at Juniper Networks with over 10 years of experience in writing and developing documentation for networking and telecommunications.

Version History: Second Edition, July 2017 3 4 5 6 7 8 9

For more information go to the TechLibrary at: www.juniper.net/documentation