TechTarget

E-Guide

Evaluating the Security of Software Defined Networking

Contents

This expert e-guide explores the latest challenges in network security. Get tips for evaluating network security virtualization products and explore the security pros and cons of software-defined networking.

Evaluating network security virtualization products

Dave Shackleford, SearchSecurity.com Contributor

Along with business units' and IT operations' steady push to virtualize data center servers and components comes a new conundrum for security professionals: how best to maintain adequate controls inside the virtual environment.

Fortunately, there is now a new breed of mature network security options that encompass virtualization, with enhanced features that rival those of their physical counterparts. In this tip, we'll review key factors to consider when evaluating network security virtualization products.

The first step (and arguably the most important one) in the evaluation process is to determine which security virtualization products would be a good fit for you and your organization. The following specific points can help to determine this:

- Cost. Cost is primarily a factor when weighing whether to replace existing network security technology that likely has limited or no virtualization security capabilities or augment or replace it with new virtual technology. Many vendors have pricing models for virtual platforms that license per hypervisor, per a certain number of virtual machines or per CPU. This may not only result in applying a totally different formula for evaluating the cost of the product, but also the incurrence of additional costs as virtualization use increases over time.

- Vendor viability. As with any vendor, make sure you do your homework. Some suppliers are more viable than others, and you should talk to their existing customers to see what they think of both the product and their relationship with the vendor. It's wise to scan the recent headlines for any news pertaining to vendors' executive leadership changes, funding announcements or acquisition rumors.
- Native integration with hypervisor platforms. In looking at more technical considerations, most virtual security vendors focus on VMware as the market leader, but more technology companies support Microsoft Hyper-V, Citrix, KVM, and other platforms as well. If your organization has chosen a single virtualization platform vendor, then the security vendor evaluation process becomes easier; if several different virtualization platforms exist, then multiplatform support is a must.
- Management capabilities. Consider whether the virtual network appliance is easy to manage, whether it integrates into existing security consoles, what type of remote access is available (SSH, for example) and whether the system provides granular role-based access.
- Performance impact and scalability. How much RAM and other resources does the virtual network appliance require? What are the average peak usage scenarios? Vendors should be able to supply some of this information.
- Architecture flexibility. How many virtual NICs/ports can the virtual firewall support? What kinds of rules are supported and at which protocol stack layers?
- Virtualization-specific features. What features are available to help control and protect virtual assets, ranging from the hypervisors to VMs?

Speaking of features, there are a number that are good to look for, depending on the type of virtual firewall, switch or gateway you are interested in. One of the most important is API extensibility, allowing integration with orchestration platforms, automation environments and other vendors' products. Many virtual firewalls today offer stateful inspection, intrusion detection capabilities, anti-malware features, and configuration and patch

Contents

assessment and monitoring for the virtual infrastructure. Ensure the platform can perform both intra-VM (internal flows on the hypervisor) and inter-VM (between virtual machines and external networks) monitoring and filtering. Deep integration with the hypervisor environment, preferably at the kernel level, will improve performance and reduce overhead, as well. The ability to identify, monitor and control virtualization-specific traffic and dynamic VM migration operations like vMotion should also be a priority when choosing one of these solutions.

Many security virtualization options exist today, from both well-known vendors and startups. Juniper Networks offers its vGW (vGateway) series of virtual appliances, Cisco Systems has the Nexus 1000v virtual switch and ASA 1000v virtual firewall, and 5Nine Security Manager for Hyper-V offers anti-malware and traffic access controls for Microsoft environments. Most IDS/IPS vendors have virtual models, as well, including Sourcefire, McAfee, TippingPoint and others.

Software-defined networking: Exploring SDN security pros and cons

Matthew Pascucci

In the technology industry, hype is a constant. This is no different with the up-and-coming technology of software-defined networks. In this case, however, the hype is justified: SDN could change the network security landscape as we know it.

Over the past couple of years, software-defined networking (SDN) has developed from merely an idea to a paradigm that large networking vendors are not only embracing, but also talking up as their model for future enterprise network management. This technology adds greater granularity, dynamics and manageability to networking, but brings up other concerns that should be seen from a security perspective.

In this tip, we'll explain what SDN is and explore the network security pros and cons that enterprise networking and security pros need to know.

A definition of software-defined networking

To understand a few of the security benefits and downfalls of software-defined networking, let's take a quick tour of the technology. Software-defined networking is the ability to split the data plane from the control plane in routers and switches. The control plane, which has historically been proprietary and known only to the vendors that developed them, would be open and controlled centrally with SDN while having commands and logic sent back down to the data planes of the hardware (routers or switches).

This provides a view of the entire network and affords the ability to make changes centrally without a device-centric configuration on each router or switch. The ability to manage the control planes through open protocols such as the OpenFlow standard allows for precise changes to networks or devices that will increase the speed and security of the network.

SDN security benefits

Like everything else, there will be both benefits and concerns when implementing new technology. Let's review some of the benefits of software-defined networking:

- By having the free-moving network of SDN, engineers are able to change the rules by having a quick, high-level view into all areas of the network and being able to modify the network.
- This freedom and control also allows for better security of your systems. By having the ability to quickly limit and see inside the network from a centralized viewpoint, managers can make changes with efficiency. For example, if there were a malware outbreak within your network, with SDN and OpenFlow you'd be able to quickly limit the outbreak from one centralized control plane that would stop the traffic without having to access multiple routers or switches.
- Being able to quickly change things in the network enables managers to perform traffic shaping and QoS of packets in a more secure matter. This ability exists now, but the speed and efficiency

doesn't exist and will limit the manager's ability when attempting to secure the network.

SDN security concerns

With innovative new technology come security concerns that could easily go overlooked. Let's take a look at a few security-related issues to be aware of when implementing SDN. The majority of software-defined networking security concerns are going to evolve around the controller itself. The controller can be considered the brains of the switching/routing, which allows the control panel from each system to be centrally managed.

The largest SDN challenge for security managers is securing the controller at all costs. Now that the brains have been taken out of the routers or switches and replaced with the new controller, this device needs to be hardened and secured through the following steps:

- Knowing and auditing who has access to the controller and where it resides on the network is a big security concern. It's important to remember that access to the controller could potentially give complete control to an attacker, so it's vital that it is secured.
- Verify the security between the controller and end nodes (routers or switches) -- specifically that they're communicating over SSL to prevent any malicious intent from accessing the controller. As with anything else, if security isn't baked in from the start, it must be added later on, and it's always more difficult and expensive to do it that way. Make sure the security between the node and controller is configured properly.
- Verify that there is high availability in the controllers. Creating a business continuity effort for controllers is important because if they are lost, the ability to manage the network is also lost -- and consequently, so are all the benefits of SDN and OpenFlow.
- Verify that everything that comes out of the system is logged. Since managers have control over the network centrally, log every change made and send it to the company's log management solution.
- When implementing SDN, verify that the organization's SIEM, IPS and any other filtering technology that might block or log changes is updated accordingly. Correlate the logs from the SIEM to alert the

manager of changes. Tracking custom events with the SIEM on the control, like login failures and policy changes, will assist with the security of the system.

- Verify that the IPS isn't identifying any of this traffic as malicious. Configure the appropriate rules in the filtering systems to allow the controller to speak with the nodes when needed.

In conclusion, software-defined networking is an emerging technology that can allow for granular security by giving an administrator a complete view of the enterprise network. However, by giving the SDN controller centralized management over network nodes to push down changes to these systems, it becomes imperative that the security around this system is locked down. This system is the brains of SDN, and without proper security wrapped around it, the network becomes completely vulnerable to malicious attacks or accidental changes, both of which can take a network down. Now is the time for organizations to ensure that security is a primary consideration in the design, deployment and management of SDNs.

About the author

Matthew Pascucci is senior information security engineer at a large retail company where he leads the threat and vulnerability management program. He has written for various information security publications and spoken for many industry companies, and is heavily involved with his local InfraGard chapter. You can follow him on Twitter @matthewpascucci or check out his blog at www.frontlinesentinel.com.

TechTarget

Contents

Free resources for technology professionals

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.

Related TechTarget Websites

- SearchFinancialSecurity
- SearchCloudSecurity
- SearchMidmarketSecurity