A Guide to SD-WAN Security

By: Ray Watson

Today nearly every IT decision maker wants to invest in innovation that will facilitate network performance and agility without compromising security.

For many, the answer to these challenges is SD-WAN, which helps simplify the management and operation of enterprise wide-area networks. One of the main challenges that persists in standing up SD-WAN networks, however, is that traditional security solutions are no longer enough. Legacy security solutions simply do not have the performance, flexibility or interconnectivity that SD-WAN connections require.

Striking a balance between security and SD-WAN performance is critical in keeping data not only accessible but also safe.

Here's a guide to the security benefits, precautions and other "need-to-know" basics of SD-WAN.

The Security of SD-WAN Appliances

At the risk of oversimplification, SD-WAN hardware is essentially a small computer, which means that the devices themselves are not necessarily built to be secure. In many cases, these devices may not have the most up-to-date operating system when they are shipped to the customer location, so checking for appliance security updates is critical. When updating security systems and patches, ensure your appliance is automatically updated by the service provider, or—at the very minimum—ensure there is a process in place to do so.

When it comes to hardware, off-the-shelf box servers and microservices should come only from well-known vendors with tested products, as it is often difficult to trace the lineage of off-brand hardware, which may contain rogue hacking or tracking devices.

SD-WAN's Bundled Security Features: Benefits and Challenges

Because SD-WAN secures traffic in transit, solutions—which include integrated firewalls and associated unified threat management—have an advantage over solutions that require separate threat management. Properly configured SD-WAN devices can simplify security and defend data from attackers.

These bundled solutions, however, can sometimes trigger challenges, blurring the line between network and security operations. Adding an unmanaged (and possibly unsecured) SD-WAN appliance to a corporate network can make roles and responsibilities confusing.

Tight alignment is critical to helping network teams address questions such as, “does that mean our internal IT security team is responsible for managing the SD-WAN devices on our corporate network?” The worst-case scenario is if the network team assumes the security team knows about the SD-WAN deployment and will take care of it. Then, critical security monitoring tasks can be disregarded. Ensuring that the network team is in close contact with the security team can mitigate an adverse security event during or after a deployment.

Overlooked Benefits: Segmentation and Zero Trust

Increased security is another advantage that comes from SD-WAN. Built on flexible, software-defined architectural models, SD-WAN facilitates the normally difficult task of WAN segmentation, helping businesses deal with issues such as security threats from within. Because of the dramatic uptick of threats from inside a network, segmentation is key—and it is a key enabler of many zero-trust security strategies.

SD-WAN makes segmenting and implementing zero-trust processes far easier, but it also plays a key role in first-line-of-defense capabilities. Approaches include SD-WAN solutions that whitelist online applications and websites for branch offices that may not have local firewalls.

SD-WAN and the Internet: Security Risks and Resource Impacts

Because SD-WAN paves the way for enterprises and their branch locations to leverage the Internet for connectivity, security must be at the top of the priority list. When SD-WAN is deployed over dedicated Internet connectivity or public broadband, it can introduce security risks that require next-generation firewalls, threat monitoring and management. Therefore, bundling security into SD-WAN isn’t just an option—it’s a requirement.

Closely monitored firewalls are key defense mechanisms when SD-WAN shifts the network architecture away from a small set of centrally managed Internet gateways and toward a highly distributed set of gateways. Because this dispersed architecture inherently increases the attack surface, the next move of any savvy network engineer is to implement next-generation firewalls with unified threat management. Built-in features make this step seamless.

SD-WAN Security: Must-Have Features and Capabilities

Enterprises must be prepared to defend against any increased vulnerabilities, which means leveraging:

- **A single on-premise or virtual client device** that can proficiently and cost-effectively serve multiple security functions, including embedded firewalls for secure Internet offloads and automatic encrypted tunneling to secure data across the Internet.

- **The ability to centrally drive policies and configurations** to reduce complexity and ease of security management; for example, centralized orchestration is a path to chaining WAN security services like firewalls and routers across locations around the globe.

- **The ability for SD-WAN network performance monitoring** as well as security monitoring to sort through alerts generated by SD-WAN firewalls.

CIOs and CISOs may start to feel overwhelmed at this point, because SD-WAN implementation and management can tax IT resources. This is where managed SD-WAN, 24/7 security monitoring services, and managed detection and response solutions can help take the workload off your internal team. Service-based approaches are also more scalable from both a resource and budgetary standpoint.

Demonstrated Success with Secure SD-WAN

Let's look at one example of how managed SD-WAN was implemented effectively with consulting firm Pearl Meyer. In its industry, Pearl Meyer's robust, secure IT infrastructure is one of its own competitive advantages. Pearl Meyer aimed to align a new network modernization plan with the company's digital innovation strategies to drive further improvements in cloud migration, cybersecurity and disaster recovery.

In this endeavor, Pearl Meyer's IT department faced a variety of pressing needs, including updating its WAN edge architecture, diversifying connectivity options for better network redundancy, improving application performance and security, and freeing IT resources to focus on strategic cloud migration.

After investigating a number of SD-WAN edge equipment vendors, Pearl Meyer's team chose an SD-WAN solution delivered as a fully managed service that also integrated SD-WAN devices with next-generation firewalls including unified threat capabilities. SD-WAN now provides back-up connectivity for all of Pearl Meyer's offices, leveraging public broadband access where appropriate while also benefiting from 24/7 network security monitoring.

A Buyer's Guide for Secure SD-WAN

Enterprise decision makers should consider these three questions before investing in a secure SD-WAN architecture:

1. Does your SD-WAN solution include an integrated, next-generation firewall with unified threat management capabilities?

2. Do you offer secure local Internet breakouts, and if so, how?

3. Does your SD-WAN include an integrated router and firewall, making it easy to directly and securely route traffic to the Internet without stacking multiple devices at a given location?

It's critical not to forget about analytics. Buyers should also take a hard look at security analytics, which are sometimes just bolted on as aftermarket components rather than being incorporated into the SD-WAN solution. Within the online portal, most providers will provide you with visibility at the box level onsite but not at the network level itself.

However, partners with security and analytics tools integrated into the solution—truly embedded into the fabric of the software defined network platform—offer the ability to view data from the actual network ports inside the SD-WAN portal. These are key differentiators for those seeking full transparency and the deepest levels of insight into their networks and its data security.

SD-WAN architectures provide enterprises with the ability to efficiently manage large networks, but no network is immune from potential security risks. Therefore, enterprise decision makers must keep security concerns top of mind when choosing partners to help establish and maintain their secure SD-WAN networks.