Using SD-WAN to Enhance Your Security Posture

WHITE PAPER

Perhaps the single most important and overarching IT infrastructure strategy is the movement toward software-defined environments. A good definition of software-defined infrastructure is as follows:

A computing infrastructure entirely under the control of software with no operator or human intervention. It operates independently of any hardware-specific dependencies and is programmatically extensible.

These same benefits are driving the rapid adoption of software-defined wide area networks (SD-WANs). The WAN is a critical component of agile IT infrastructure and must deliver many of the same benefits as other aspects of the infrastructure: efficiency, simplicity, visibility, and scalability.

More importantly, new secure SD-WAN services can also provide a substantially improved platform for enhancing the security posture of the organization, in addition to the more typical benefits of these services. The right secure SD-WAN solution helps solve many of the thorny cybersecurity problems that all organizations face when they leverage public networks for sensitive workloads. These services provide new options to the network manager or administrator. In the past, MPLS was often the only technology that could be effectively used to provide secure network infrastructure. However, with new secure SD-WAN services, it is now possible to deploy highly secure hybrid networks. This fundamentally changes the game, providing far greater flexibility and more efficient options.

TechTarget | Custom Media

open systems

Improved SD-WAN security is an important enhancement. For example, the utilization of direct Internet access can thwart the effectiveness of current security solutions when the network becomes a "back door". With many SD-WAN offerings focusing solely on cost and offering little in the way of security enhancements, prescient organizations are now much more focused on ensuring that any SD-WAN deployment does not create vulnerabilities at branch locations that have direct Internet access. Additional protection is gained by using connectivity-as-a-service (CaaS) offerings that centrally manage all the ISP lines. This type of service ensures that security policies and cyberprotection products are consistently implemented on all ISP lines.

BEST-IN-CLASS SD-WAN SOLUTIONS MUST PROVIDE INTEGRATED SECURITY

One of the most fundamental problems of the legacy approach to network security is the process of building the network first and then adding security after the fact. This is not a problem resulting from bad decisions by security or network professionals, but rather the result of having to secure existing networks once they are already deployed. When deploying a new SD-WAN service, there is the opportunity to integrate security functionality into the network as it is deployed. This provides numerous benefits, including the ability to:

- Apply security policies and protection holistically across the network in a consistent manner
- Use a single point of management for the entire SD-WAN that will provide full visibility that enhances the security posture
- Ensure that patches and updates are applied more quickly and are fully deployed across the entire network

This approach also helps the SecOps team by reducing its workload when security is deployed consistently across the WAN utilizing secure SD-WAN solutions. Deploying a secure SD-WAN solution starts the process of NetOps and SecOps working more closely together. Integration of the SecOps and NetOps teams is an important advancement and will result in better communication and interaction, which improves overall security.

Another important benefit of secure SD-WAN is support for the digital worker. The modern workforce is not only highly mobile and agile, but also very dynamic as temp employees, contractors, and partners come and go frequently. Older approaches of securing network access that require substantial manual intervention by either network or security professionals are not a good way forward. Secure SD-WAN, in contrast, is a substantial improvement. Users will be delighted that they can use any network, ensuring that they get the application performance they deem necessary. In addition, this performance is available anywhere, and eliminating dependence on end users to ensure network security removes a major usage obstacle that often requires the user to get deep into the technology.

The cloud is another key driver for deploying next-generation secure SD-WANs. The clear majority of enterprise-class companies already have multiple cloud services under contract. A midsize enterprise will have many cloud services and a number of cloud suppliers. Research from RightScale1 shows that the average company is already using five different clouds, and a Logic Monitor survey2 estimates that 83% of workloads will be in the cloud by 2020. The use of multiple cloud services demands a network that can seamlessly provide high-performance access to each of these clouds and ensure that none of the clouds becomes a silo. A single logical SD-WAN managing and providing bandwidth to all clouds is the best approach to enable broad cloud use. This type of deployment also allows the organization to ensure that the bandwidth necessary to ensure performance is available across all clouds in the most efficient manner.

SD-WAN SERVICES WITH INTEGRATED SECURITY ELIMINATE VULNERABILITIES

When it comes to cybersecurity, unmanaged use of public network services may add new vulnerabilities. This makes the job of both the network administrators and security engineers more difficult. Secure SD-WAN services can mitigate many of these vulnerabilities and potential entry points. SD-WAN services that do not have integrated security look dated or are useful only for a specific and well-defined set of workloads that can absorb the risks.

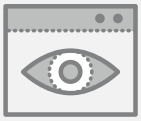
1 "Cloud Computing Trends: 2018 State of the Cloud Survey," RightScale, Feb. 13, 2018

2 "83% Of Enterprise Workloads Will Be in the Cloud By 2020," Louis Columbus, Forbes, Jan. 7, 2018

For this reason, organizations should focus their buying interest on SD-WAN services that have integrated security functionality. To be useful, security should be intrinsic to the offering, not merely a third-party security product that is bolted on. The most important reason for focusing on secure SD-WAN services is that dynamic network utilization can create vulnerabilities without warning when unsecured new or different networks are used. Security must be deployed across all networks to eliminate this problem.

Some network and security teams have used the fear of public network security threats as a reason to focus only on MPLS or private networks, but when security is correctly integrated into IP networks, the problems are mitigated. The key to remaining secure is to ensure that critical security capabilities are consistently deployed across the SD-WAN. These include:

Firewall



Traffic monitoring

Encryption

OPEN SYSTEMS DELIVERS SECURE SD-WAN DEPLOYMENTS

Open Systems is an SD-WAN industry leader. As part of this leadership, the company provides SD-WAN services that include integrated security functionality, ensuring consistent protection across all of your ISPs. This delivers dramatic operational simplicity. It is no longer necessary to manage and secure every IP network individually or create specific routing rules to avoid less secure networks.

The secure SD-WAN service leverages Open Systems' CaaS offering. The customer can manage all ISP lines with one service, optimize provider selection, utilize dynamic line sizing, and leverage a faster ordering process while ensuring that security is in place for those different lines. This is highly beneficial, since Open Systems' CaaS service is carrier- and transport-agnostic, providing more options for the customer.

The company's Secure SD-WAN solution provides an important bridge between NetOps staff and the security team. Security professionals can be assured that critical security capabilities such as firewall, traffic monitoring and encryption are being used on ISP lines in the same way they

are for other networks and carriers. This dramatically reduces the operational complexity of the network. Many network breaches can be traced to inconsistent deployment of security policies or products that were the result of too much network complexity, making it impossible to be sure all lines are protected.

KEY TAKEAWAYS

The use of SD-WAN is increasing dramatically, and in many cases, it is a means of reducing network complexity that can create vulnerabilities. However, SD-WAN is just the starting point for reducing risk. Utilizing a secure SD-WAN offering that includes the most important security technologies will improve the defensive posture of the organization and offer far greater protection. It is likely that deploying SD-WAN services without security may increase the threat, rather than reduce it.

Using a secure SD-WAN provides most of the security benefits that are derived from "software-defining" other aspects of the infrastructure: consistent application of policies, consistent deployment of specific security technologies and tools, and comprehensive visibility across the infrastructure. This thinking, coupled with the implementation of other unique security capabilities, infuses Open Systems' Secure SD-WAN offering. **This service provides a huge step forward in delivering secure, agile, and cost-efficient networks. For more information, please go to https://www.open.ch/en/index.php**

About Open Systems

Open Systems was founded in 1990 and is today a leading provider of Managed Secure SD-WAN. With its Mission Control Security Services, Open Systems protects secure operations and ensures availability of business-critical applications and ICT infrastructures of global companies, institutions and NGOs in more than 180 countries around the clock, 365 days a year. The company's excellent service and operations earned the trust of renowned companies such as gategroup, Mammut, Sulzer and UBS.

Open Systems AG, Raeffelstrasse 29, 8045 Zurich, t +41 58 100 10 10, f +41 58 100 10 11, www.open.ch