BIZCOMMUNITY

Do not underestimate the challenge of securing SD-WAN

By Doros Hadjizenonos

21 Feb 2019

Historically, the branch office of an organisation was the red-headed stepchild of the network, but digital transformation has changed all of that.

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet

Today, transactions, workflows, applications, and data requests at the branch need to be just as fast as those being processed at the network core.

Even more challenging, the number and types of end users and the increasing volume of voice and video traffic and business applications connected to the branch network have multiplied dramatically, including cloud-based networks (IaaS) and services (SaaS).SD-WAN solutions were developed to overcome the networking challenges that traditional MPLS-based branch network strategies couldn't address.

They provide branch users with flexible access to resources located anywhere across the distributed network and allow end users to use advanced applications, generate complex workflows, and utilise cloud-based services from a variety of devices, including their BYOD solutions.

Core SD-WAN Benefits - Automation and Application Steering

One of the challenges with traditional WAN connections is that routers generally don’t provide any visibility into today’s traffic and applications. SD-WAN enables deep application visibility and first packet classification so that the network can better support business-critical applications. Because poor application performance can seriously impact the business, SD-WAN automatically identifies traffic by type, user, source, and destination to steer critical applications down pathways with adequate bandwidth and minimal latency.

Combined with simplified connection failover, branch users experience better visibility, higher performance, and greater availability for business applications.

Securing SD-WAN is harder than it looks

However, many IT teams who have been quick to adopt SD-WAN due to its clear benefits significantly underestimated the challenge of implementing an effective and comprehensive security strategy to go along with it due to the challenge of direct Internet access from devices running at the branch.

Any branch security solution needs to address the SD-WAN connection as well as split-tunnel challenges resulting from also running cloud services, mobile devices, IoT, BYOD, and mobile users remotely connecting to branch resources. Organisations need to wrap that all together into a single, integrated security and network solution for consistent performance and security.

Resources are limited

And to complicate matters further, organisations are also experiencing a global shortage of trained and experienced cybersecurity professionals. The last thing that they need is to build, deploy, manage, and monitor yet another suite of security tools designed to protect their branch offices.

Unfortunately, of the over sixty SD-WAN vendors on the market today, only a handful provide anything beyond the most basic security. Instead, they rely on organisations to figure out how to leverage their existing security solutions into their SD-WAN tools.

Traditional security solutions don’t scale

Unfortunately, the majority of security devices and solutions deployed on the main campus of an organisation were never designed to support the unique and highly dynamic requirements of today's branch offices. They can't see far enough, can't track data that moves between network domains, and can't share and correlate threat intelligence to identify and stop today's advanced attacks. The best they can usually do is encrypt traffic and then apply a security filter at the edge of the network to shut down a connection if it detects malware or unusual behaviour.

Organisations require a secure SD-WAN solution

To address this challenge, SD-WAN needs to have a sophisticated suite of security tools embedded directly into the solution, including NGFW, IPS, web filtering, antivirus/antimalware, encryption, sandbox, and high-speed inspection of encrypted data.

Further, those security tools need to seamlessly integrate with the security tools deployed elsewhere in the distributed network, whether on the main campus, or remote and mobile devices, and across each of the different cloud solutions that have been adopted.

Any SD-WAN security solution MUST include the following three characteristics:

- They must provide a comprehensive suite of essential security tools. The security concerns at the branch are identical to those in any other part of the network.
- Security must be natively embedded in the SD-WAN solution itself to reduce the device footprint needed to protect the branch office.
- Finally, those security solutions deployed as part of the SD-WAN solution must also seamlessly integrate with other security solutions deployed elsewhere.

Secure SD-WAN supports digital transformation without compromising on security

Business-critical applications are the lifeblood of today's digital enterprise. As a result, ensuring the consistent availability and performance of those applications - especially over traditionally unreliable public networks - is essential for ensuring the productivity and integrity of today's branch offices. SD-WAN also supports centralised control, policy-based management, hybrid gateways that use a variety of connections and transport services, and things like service chaining that allow different network services to work together.

What most SD-WAN solutions don't provide is security. Because Secure SD-WAN natively includes a suite of fully integrated security solutions, it not only provides the essential functionality that SD-WAN provides, but it also secures the entire range of critical branch applications and services, while seamlessly tying that security back into the organisation's larger security framework.

This, in turn, reduces security overhead, ensures consistent protection and policy enforcement, and reduces total cost of ownership - without compromising on SD-WAN performance or functionality.

ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet
- Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- How to have strong cyber hygiene - 26 May 2020
- How to approach data breaches - 11 May 2020
- Employees must be educated about mobile cyber threats - 13 Feb 2020
- Stay ahead of emerging cyber threats - 8 Jul 2019

View my profile and articles...