How an SD-WAN can cure those security blues

By Zeus Kerravala, for Silver Peak*

Cyber security remains a hot topic with nearly every IT and business leader we meet. In particular, there seems to be an intensified focus on network security. Typically security is deployed in layers (network, compute and application), and that model is likely to continue in the short-term, but given the fact that many of the building blocks of digitisation, such as IoT and the cloud, are network-centric, there should be a stronger focus on leveraging the network and network-based security to protect the organisation. Nowhere in the network has there been more change than in the wide area network (WAN), so it stands to reason that as legacy WANs evolve into software-defined WANs, they must play an increasingly critical role in securing the enterprise. Below are my top five recommendations to better secure your organization with an SD-WAN.

1. Encrypt WAN transport
   In the past, companies had to choose a compromise from three, less than ideal, options. Use high-cost MPLS networks to move corporate traffic on a private IP network, use lower-cost broadband unencrypted circuits or use some sort of broadband with point-to-point encrypted tunnels. The first option is expensive (and is not guaranteed to be secure), the second puts the organisation at risk and the third is too complicated to do at scale. An SD-WAN eliminates the trade-offs for organisations to provide the best of all worlds. With an SD-WAN, businesses can leverage low cost broadband and encrypt all traffic to every site without requiring the network administrator to go make a bunch of manual configuration changes to every router every time a change is made to the network. It’s worth noting that an SD-WAN is actually more secure than the majority of private IP services since the data can’t be breached even if the carrier network is compromised.

2. Secure cloud connectivity
   Ask any IT leader or CISO about the cloud or look at any survey on cloud computing. What’s their top concern? It doesn’t matter how secure Amazon, Salesforce or Microsoft make their cloud services, business and technology leaders get the heebie jeebies when sensitive data must traverse the Internet to get to the cloud service. Many of the leading SD-WAN vendors offer granular internet breakout and steer applications traffic in alignment with security mandates through secure gateways and next-generation firewalls located in the branch, cloud or data centre. An SD-WAN mitigates the traditional risks associated with using the cloud and SaaS or IaaS services.

3. Improved branch security
   Most branch offices require some level of local security, particularly those with direct Internet access. Often the IT team doesn’t deploy all the services that are necessary because of the cost of buying and deploying physical appliances, which can often require an engineer to travel to each site. Leading SD-WAN solutions include the ability to deploy services such as VPNs, firewalls and WAN optimisation virtually by leveraging network functions virtualisation (NFV), so making it simple to deploy any service to any location.

4. Adhering to compliance mandates
   Highly regulated verticals such as healthcare, retail and financial services need to comply with some stiff rules such as PCI data security or Sarbanes-Oxley. An SD-WAN should be ideal for these verticals as the technology enables the business to create virtual overlays to segment different types of applications traffic. For example, a hospital could create a separate virtual network specifically for patient information making it much easier to comply with regulatory requirements across a distributed environment.

5. Implement secure segmentation
   The concept of segmenting a network into several secure zones has always had high appeal. Segmenting enables applications traffic to be isolated for security purposes or to address unique performance requirements. However, with legacy networks, the only way to accomplish this was with VLANs and ACLs that can be difficult and time-consuming to set up and even harder to maintain as the environment changes. An SD-WAN integrates this capability as a software feature, making it much easier to create both coarse and fine grained segments that can be defined and enforced through business intent policies. Also, because the policies aren’t tied to the underlying hardware, the policies become agile and can follow a device. For example, a hospital may have a clinician segment and as an individual goes from location to location, they will be placed in the correct zone. Segmentation can be managed centrally to ensure consistency of configurations and best practices, making it a powerful tool and SD-WANs can scale in line with changing requirements. This ability helps organisations to comply with a raft of regulatory requirements.

* Zeus Kerravala is the founder and principal analyst with ZK Research.

Contacts

David Frost
(02) 7903 9567
mailto: davidf@prdeadlines.com.au