# THOUGHT LEADERSHIP

## Securing SD-WAN- Beyond the base level

Digital transformation has enabled businesses of all sizes to create new ways of achieving operational efficiencies. But just as technology has enabled business strategy to evolve, so too have the risks to security. With data breaches and ransomware attacks now a daily occurrence for businesses of all sizes across the world, security is a critical component for businesses to address from the start.

According to research from Global Market Insights, the SD-WAN market will grow at a 60 per cent compound annual growth rate from 2018 to 2025 – demonstrating how the adoption of the technology is rapidly increasing. However, as with the implementation of any new technology, the risks to security must be considered. High levels of security are essential for SD-WAN in particular as in many cases the network is built across public infrastructure, which could potentially leave data exposed and vulnerable to threats.

The first design of SD-WAN was a building block approach, comprising of a router, adding a firewall and further equipment to ensure security. With the advent of a software approach to SD-WAN, sophisticated security features are built in from the start, ensuring that at a base level, it includes industrial-grade encryption and a set of tools to manage the end to end security over a public access network. With firewalls built in at the edge of the network at each site, there is not necessarily a need to proliferate hardware, which provides an operational efficiency.

It's important to note that depending on how a business is structured and where the users are located, there may be further security protocols within an SD-WAN infrastructure that need to be considered, beyond the base level security. There are several ways to enhance SD-WAN security further, but vendors must educate customers to the options that are relevant to their business setup to ensure a considered approach to security.

### Local Breakout

One example of how additional security layers can be applied to improve the security of SD-WAN is local breakout. If an organisation has a head office in the UK and another in France, SD-WAN can be used to establish the connection between sites to connect privately and exchange internal corporate traffic. Should the French office want to connect to localised sites, such as search engines etc. there could be a delay, considering the traffic has to be routed through back through the UK. Therefore, the SD-WAN must be augmented to incorporate local breakout and firewall technology must also be implemented; either within the SD-WAN appliance, or an extra layer of security must be added.

Depending on how the network is designed, it is essential to implement strong security at the Edge. Furthermore, with an increasingly mobile workforce, software must be able to scale not just to local sites, but also mobile assets, devices and people. The SD-WAN setup can affect how you apply security to users and the sites, which is something that must be factored into the initial design.

SD-WAN technology is second to none when it comes to replacing legacy models such as MPLS in terms of operational efficiencies and being cost effective, but there is an additional responsibility to ensure the security is pervasive, particularly when it comes to mobile users or local breakout. The standard SD-WAN security is a strong base level, but depending on the organisational setup – such as if there is a need for local breakout – further security protocols may be required.

## Unified Threat Management

Whilst SD-WAN has strong encryption built in from the start, this is designed to be at site level rather than on a per-user basis. In basic terms, the firewall provides the capabilities to keep threats away from the site, but it cannot provide more advanced functionalities and policies that provide a granular way of looking at how to secure devices and people in the organisation.

This additional layer of security is provided through Unified Threat Management (UTM). These devices, either virtual or physical, are more comprehensive in how they are able to apply rules and security on traffic and policies down to the user level. So, in order to enhance the base level of security of SD-WAN, companies can route all traffic back to a central point, where an advanced UTM firewall can manage the security on a per-user basis. This could be via a next generation firewall service in the data centre, or alternatively there are vendors that can provide a cloud based service where the traffic can be routed to and security policies are then applied.

## Conclusion

The evolution of SD-WAN security technology continues to advance rapidly in order to keep up with increasingly sophisticated methods that cyber criminals are using. Advancements are already becoming reality with security mechanisms such as advanced cryptographic cyphers. With this technology, in order to hack into each SD-WAN appliance, the hacker would need to get past a node key that applies only to that site. To take this even further, rotating cyphers can be added which changes the key every hour – meaning that hacking into the system is almost impossible.

At the basic level, SD-WAN already has sophisticated security features but it must be used correctly to ensure the appropriate level of security is matched to how the organisation is structured. There are already a number of options to enhance the security of SD-WAN further, the key for vendors is to ensure that customers have all the facts to hand that are applicable to their business setup, so that the appropriate additional layers of security can be applied where relevant.

**Nick Sacke**
Head of IoT and Products, Comms365 Ltd
07757 007569 | nick.sacke@comms365.com
www.comms365.com