KORIS365 FORTINET

A GUIDE TO SD-WAN:

HOW SD-WAN CAN GIVE YOU BETTER NETWORK SECURITY

01 Introduction

If you're a large, multi-location organisation, and particularly if you're spread over vast geographical regions, your networking procurement needs are no trivial matter. Networking is fundamental to such businesses, which, as they grow, are almost always seeking more efficient and cost-effective sources for their networking needs while improving network connectivity. To fulfil this brief, IT managers must adopt networks that are high speed, agile and secure.

Like many markets, IT infrastructure has evolved quickly, and traditional products no longer necessarily meet growth requirements. However, a networking solution known as an SD-WAN is being touted as one of the leading solutions to allow businesses to keep their edge. As a result, SD-WAN technology is predicted to be worth approximately $5.25 billion by 2023.

The evolution to an SD-WAN is a natural consequence of digitally transforming industries relying increasingly on the cloud.
WAN – wide-area network – solutions have long been driving networks for companies, but those typically used in the past, like multiprotocol label switching (MPLS), have been outpaced by individual business productivity.

An SD-WAN is quicker, more cost-effective, more secure and simpler than MPLS or broadband, and for those wanting a robust business case, there are technical benefits to choosing SD-WAN over other network solutions. These six benefits should provide IT professionals and executives with an informed understanding of why SD-WAN is the primary option for your networking needs compared to older solutions like MPLS.

The e-book will cover:

- What Is an SD-WAN?
- Encrypted Traffic and Firewalls
- Application-Level Segmentation
- Secure Zero-Touch Provisioning
- Secure Cloud Connectivity
- Efficient Connectivity While Secure
- Security For Growing Businesses
- SD-WAN vs MPLS

02 What is SD-WAN?

What is an SD-WAN, exactly?

Wide-area networks have traditionally taken care of the business needs of international organisations, and the concept remains the same for an SD-WAN.

A WAN is a large network of information that is not centred to a particular location but can share information between devices around the world through a WAN provider. To understand how much we rely on WANs, consider that the internet is an example of a WAN. These types of networks are, however, typically established by service providers utilising lots of different local area networks that lease their WAN to entities like schools or businesses.

Software-defined wide-area networks (SD-WANs) are a type of application of software-defined networks that carry out a WAN's function. So, they use software to connect network users over vast geographic distances. Whereas a WAN involves fixed infrastructure — servers and other hardware — an SD-WAN involves virtualised routers and firewalls with central coordination.

In effect, an SD-WAN manages connectivity through commercially available internet access rather than replacing an internet connection or other WAN networks, and it overlays these existing technologies.

However, you may hear about "SD-WAN solutions," and what these encompass can be broad and varied depending on what the vendor or carrier wants to offer. SD-WAN solutions can, therefore, include the underlying connectivity as well as the modems, terminals or adapters, otherwise known as customer premise equipment (CPE). Some vendors will only offer the overlay, however.

Why change to SD-WAN at all?

The reason for this development and its broad take-up is that there are many more software-based applications that WANs can no longer manage – Software as a Service (SaaS) and cloud-based networks. Therefore, a rethink was needed around connectivity. SD-WANs addressed the challenge by being more dynamic in directing internet traffic between different branches, data centres and clouds.

Management of an SD-WAN is more flexible and simpler than traditional WAN networks, with traffic offloaded to the internet, making its deployment more cost-effective as well as efficient. This efficiency and economising are crucial with the digital transformation sweeping the corporate world where there will be more reliance on applications run over the internet. WANs just weren't designed with this explosion of traffic online in mind.

Now, there must be better monitoring of the IP path. Businesses have more exposure to security threats now there are more net-based business applications, which may be accessed by actors beyond immediate staff, including contractors, vendors, partners and guests. An SD-WAN encompasses a lot of features that overcome security and high-volume traffic concerns. The overriding benefit of these features is that it allows enterprises to perform at a level that keeps them competitive, reliable and more profitable.

03 Encrypted Traffic and Firewalls

Increasing need for encryption

An uptick in remote working has also made the need for secure connectivity more urgent, particularly as working from home has normalised after the COVID-19 pandemic and will likely become a permanent feature of some sort.

More users in a greater variety of locations mean security is more vulnerable but SD-WANs encompass specific features to deal with this vulnerability, including strong encryption along the tunnels it creates carrying traffic.

Encrypted tunnels

In an SD-WAN, encryption keys are shared by the hosts sharing the data. Encryption usually comes via an algorithm and different connection types might provide this.

Some systems opt for Datagram Transport Layer Security (DTLS), which is a session layer communications protocol based on the TLS protocol, originally meant for applications with unreliable transport layers, as is the case with the Internet of Things and online gaming.

DTLS is a security protocol for web real-time communication technology, including web browsing or online communication. It works fast, even on low-power devices, making it cost-effective for businesses.

Internet Protocol Security or IPsec is another way of securing connections developed from the most common internet protocol, IPv4, which didn't have inherent security provisions and could be breached easily. IPsec can be used to secure traffic passing over IPv4. IPsec can also authenticate data and deploy encryption algorithms using hashing algorithms and other mechanics to ensure secure connections.

DTLS and IPsec aren't the only options, and many available security protocols perform identical functions and create the secure tunnels required between the two endpoints. DTLS and IPsec also, for instance, employ confidentiality, integrity, and authentication to further ensure no one is accessing the data where they don't have the appropriate authorisation. However, the choice of the algorithm within each of these protocols may make one more secure than the other.

Virtual firewalls

SD-WANs also allow the deployment of virtual firewalls to deal with a potential threat or malware in real-time. These can then be turned off once the threat is gone. The same firewalls can also be implemented to restrict access between, for example, staff and other users of a network.

Virtual firewalls are needed where hardware firewalls can't be deployed, including cloud-based applications — a key motivating factor for the development of SD-WANs. Virtual firewalls are cloud firewalls and can be used in public and private cloud environments and an SD-WAN.

These firewalls work in much the same way as hardware firewalls in that they restrict or allow traffic to flow between zones. They can also be deployed as virtualised instances of next-generation firewalls, which can facilitate segmentation. More on that later.

04 Application-Level Segmentation

What is segmentation?

Micro-segmentation is used in network security to allow security architects to separate data centres into segments that can drill down to granular levels, including individual workloads. Each segment can then receive individual security policies using network virtualisation technology. Micro-segmentation is thus another security feature that negates the need for hardware firewalls, perfect for cloud-based applications.

Why micro-segmentation bolsters security

Free of the burden of needing physical firewalls, the possibilities include being able to protect all virtual machines within a network, according to application-level security controls.

Having every workload securitised is a boon for an enterprise's defence against cyber-attacks and can be done in a variety of ways, from tagging workloads or using virtual local area networks (VLANs), which allow hosts to be grouped together with communication managed by access control lists, as examples.

Micro-segmentation in an SD-WAN

Even if an attack on your network infiltrates the perimeter of your network's defences, it cannot then penetrate the entire network because of the individual security policies, so the threat can be isolated rapidly. In addition, threats from other servers and from within data centres are also prevented.

Micro-segmentation within an SD-WAN means there are no threats from other servers or within the data centre and a minimal threat to your network is maintained. This security technique is complex for an attacker but is simple for network controllers as the segmentation in an SD-WAN is visible through centralised management. Adding to the simplicity, security policies in an SD-WAN can automatically adapt as infrastructure develops.

Best practice

Segmenting traffic at an application level, according to performance needs and security policies, is thought of as best practice in security, even though it has been difficult to apply in traditional WAN environments. SD-WANs have reversed those challenges, allowing a granular segmented approach stretching from data centres to the entire WAN, ensuring zero trust and complete validation of each digital interaction.

There's also nonporous security between the cloud infrastructures, containers and on-premises data centres. The individual security policies should be applied to a small workload like the utilisation of particular software by a named branch, cloud-based apps, or the use of VoIP, for example.

The most manageable micro-segmentation in an SD-WAN is where the segmentation happens according to business intent — application characteristics or service-level agreements — and then applied to a group. This approach also means there are fewer policies to manage than there are in, say, network segmentation.

It should also incorporate a firewall and strong encryption, another feature of SD-WANs, as discussed.

05 Secure Zero-Touch Provisioning

What is zero-touch provisioning?

Zero-touch provisioning is almost what it says on the tin: You can provision your router with zero need for manual, even minimal, configuration when it's located anywhere on the network.

There are numerous benefits to ZTP, including security, better network control, lower installation costs, simplicity and efficiency. It also eliminates the likelihood of errors that can occur with manual configuration.

Manual configuration is by and large a hassle and can involve two lots of shipping as devices go back and forth. When this happens, there's a risk a device with a different IP address gets sent back. With ZTP, the device makes one trip directly to its intended location and can be installed immediately, reducing lead times and hugely facilitating the ability to plug and play.

From a business sense, that's hugely beneficial because you may have many sites with no IT staff or have lots of sites frequently opening, like pop-up stores if you're in retail.

How does it work?

The customer is assigned an IP address, after which an SD-WAN router automatically searches for the ZTP server.

The ZTP feature conducts the configuration and connects to the central management system. This type of provisioning is becoming more supported as vendors understand that their equipment could be installed anywhere across a huge geographic area and installation infrastructure. For example, a technical team is expensive, impacting potentially the bottom lines of the supplier or the cost would be passed on to the customer and their margins.

Things to consider

ZTP is an increasingly important feature that home offices are using. Zero-touch also requires no manual interception, so any configuration work, even minimal, would still not be considered ZTP. Rather, it would be called minimal touch provisioning (MTP) or one-touch provisioning (OTP).

An IP address is the first step to ZTP, so it needs to be the right one to be truly secure. Possible obstacles include when the WAN connection is via the internet and authentication requires manual intervention or if a firewall prevents a connection. When that happens, the firewall's parameters must be adjusted, although this can be performed remotely, so no work has to be done at the customer end.

There may also be some prerequisites. For example, when the IP address is being assigned, remote setup is often facilitated by DHCP. Therefore, even though DHCP is fairly ubiquitous now, ZTP could fail at the first stage if you don't have it.

DHCP also provides the gateway address, DNS server location and local domain name.

Any good SD-WAN solution will have pre-managed these potential obstacles and ensure security at each step, including authenticating the device and connecting it to the appropriate management system.

06 Secure Cloud Connectivity

Connection to the cloud makes security more important than ever, and the fail-safe capability of an SD-WAN to deliver this is woven into its design. Here are four security features to ensure secure cloud connectivity.

Embedded quality of service

SD-WANs encompass a variety of different modules, all likely with their own service-level agreements (SLAs), and when one service provider is coming up short, it could impact the entire network.

However, SD-WANs can include quality of service, which sets the parameters that all SLAs must meet, which means they are operating at a minimum threshold at all times. From a business point of view, that gives you leverage to encourage providers to increase their offer.

Service chaining compounds security

Service chaining with an SD-WAN is much easier than with traditional WANs. A service chain is a set of features related to the network such as firewalls, WAN optimisation or virtual private networks connected to each other via the network to support an application.

An SD-WAN simplifies service chaining by grouping these features into a single interface, which then uses the intelligence within the SD-WAN processed packets associated with each application processed while supporting high encryption algorithms.

Prioritising business-critical traffic

As cloud applications aren't the same — they have different importance to the business and will differ regarding bandwidth requirements, ensuring seamless operation, as well as security, is vital to cloud connectivity.

An SD-WAN facilitates this by creating path liquidity with QoS built into these pathways. Further, edge appliances on the SD-WAN can pick up bandwidth requirements and restrict or allow bandwidth access on any given application while preserving QoS. Each application's packet characteristic data is bundled in packets before it’s transmitted and can also be monitored to ensure the right WAN path is selected as they reach the edge devices (where the SD-WAN endpoints are).

Also, what's smart about an SD-WAN is that the traffic flowing through your network does not impact connectivity as the SD-WAN matches the network resources to enterprise needs

Fail-safe security for cloud connectivity

Integrating an SD-WAN with the cloud is of prime benefit to businesses and answers many user questions around security and reliability regarding cloud connectivity.

The network can be integrated seamlessly, intelligently navigating traffic through secure tunnels. Many vendors will also provide a security stack that will evolve security policies with developing threats like malware.

Having security and access controls in the cloud rather than the data centres means that security is distributed across all users evenly and continuously, and it becomes easier to scale up as businesses and user bases grow in number and diversity.

07 Efficient Connectivity While Secure

Better performance

Traditional circuits typically use one backup circuit for connectivity at important sites. These tend to remain dormant until the main circuit fails but only having one circuit actively working is inefficient and SD-WANs have already levelled up in this regard.

If there's a backup, the SD-WAN will allow both circuits to be active instead of letting a passive circuit operate in the background. Using both circuits is more efficient because two circuits carry the connectivity load.

This rebalancing hasn't been possible in traditional WAN, which is unable to transfer the packets from an application to the second circuit should the first circuit become overloaded because it follows a fixed configuration. By contrast, an SD-WAN can perform more intelligently, and it can monitor bandwidth and decide which applications get access to traffic and determine capacity.

If an SD-WAN uses two circuits, it can also produce further cost savings.

Real-time application routing

Service-level agreements can be provided for each application with an SD-WAN, and they can contain conditions for routing. This capability means you can boost performance for most critical applications. Each application or group of applications can be set up with a "business intent," representing a set of rules reflecting protocols for different situations. These can include the SLA.

They can also be set up to use any bandwidth available in line with the SLA or to use a certain circuit. The business intent uses the underlying network to meet the SLAs in real-time.

An SD-WAN needs routing options to deploy the flexibility that partly makes an SD-WAN so efficient. Path conditioning lets the SD-WAN adopt dynamic routing and rerouting for application needs and can overcome various technological challenges associated with business applications like brownouts or microbursts so that business-critical applications like VoIP remain working.

Class of service

Class of service is a way of differentiating traffic for data and voice protocols. The types of payloads in data packets transmitted are differentiated in terms of priority. An SD-WAN creates end-to-end secure tunnels and knows what's on the SD-WAN's edge devices. That means if a phone call is happening between two sites, it won't be interrupted should a huge file transfer come through from a third site.

The business intent overlay in an SD-WAN maintains the application's performance in a way that was not possible with a traditional WAN.

08 Security for Growing Businesses

At-scale deployment

The SD-WAN market is growing and will result in $4.5 billion in revenue in 2022. The market is growing because businesses understand the need for secure, efficient and flexible connectivity that integrates seamlessly with the cloud. SD-WANs present an intelligent network solution that intuitively adapts as your business changes and grows.

In fact, this market forecast shows that SD-WANs are no longer only being taken up by early adopters, and enterprises are now deploying SD-WANs at scale. Therefore, it's a good thing the software-based network is scalable, and each SD-WAN can potentially support thousands of endpoints in one controller cluster.

Large or growing businesses can consider several capabilities when procuring SD-WAN solutions to make the most out of this potential.

Role-based access control

An SD-WAN has clear benefits for multi-site businesses and improves efficiency when you have one centralised controller. However, organisations can also consider setting up multiple tenants or role-based access control (RBAC), representing a hierarchy across the network with access to specific sub-groups.

Redundancy

Redundancy refers to the interconnecting of multiple WAN links onto an SDN device, which uses algorithms to distribute traffic along all the lines for load balancing and redundancy. Redundancy should be available across all aspects of the SDN solution.

Scaled-up CPE capacity

CPE devices enabling hardware acceleration can support tunnelling for traffic to flow through at scale across access links up to 10 Gbps. This at-scale provision must be included for medium to large-sized enterprises and avoids the need to get built-for-purpose SD-WAN hardware later down the line.

Integrating virtual network functions

Third-party virtual network functions (VNFs) are a requirement when incorporating external security solutions into an SD-WAN. Therefore, SD-WAN solutions should support integrating additional VNFs even if they're custom-designed products.

Multi-cloud scalability

As SD-WANs are picking up steam, so is multi-cloud deployment, which means firms may leverage more than one cloud provider to perform business functions. Therefore, SD-WAN solutions must be able to scale to the levels enterprises see them moving towards the multi-cloud, successfully simplifying their current networking before this transition is made.

09 SD-WAN Vs MPLS

Can a case still be made for MPLS?

If you've reached this chapter, it's clear that networking solutions are on a trajectory towards SD-WAN solutions.

However, despite clear benefits, some CIOs and technical officers ask, and not unreasonably, whether they should trade in multiprotocol label switching (MPLS) for an SD-WAN.

MPLS is a routing technique in networks and a type of WAN technology taking data from node to node according to short path labels rather than long network addresses. The result is faster traffic flows because complex lookups aren't being made.

However, stacked up against an SD-WAN, is it as secure, cost-efficient or better performing?

On cost

SD-WAN is a cheaper solution than MPLS; the latter can have high bandwidth costs. It's also the case that before SD-WANs, many organisations connected other sites via a central data centre through a WAN using different MPLS connections. This setup necessitated all data, workflows, and interactions, including access to cloud-based services, to go back through the data centre for processing and redistribution, which is cost-inefficient.

An SD-WAN doesn't require this backhauling of data and can direct traffic straight to the cloud.

On performance

SD-WAN is also thought to be better performing. For one, it has better visibility of the different components of the network: its needs and capabilities across packs, traffic flows, security and prioritisation.

It's also more flexible. MPLS connections are fixed and unadaptable, which doesn't fulfil the need of businesses when they are faced with increasing interconnectivity between sites requiring more agile networks to facilitate this.

The kind of intelligent rerouting, application recognition and bandwidth recognition are also lacking from MPLS.

On protection

One advantage MPLS has over some SD-WANs is security. MPLS is basically a secured tunnel going through a secured private network. It's a dedicated circuit and can effectively prevent packet loss. An SD-WAN is a virtual overlay separated from physical links and the same assurances couldn't be made about packet loss if its security is not as robust as it could be.

An SD-WAN, after all, does allow connections like MPLS to be leveraged. It can also intelligently analyse the data flows. For MPLS, which doesn't have this capability, the client would have to do a lot of the heavy lifting to detect malware or other threats and deploy firewalls and other security mechanisms at either end of the connection.

Some SD-WAN solutions may need security overlays and deploying security as an afterthought will not allow an SD-WAN to provide superior protection to MPLS. However, an SD-WAN can integrate security that can resist intrusions, packet sniffing and other direct attacks.

10 Summary

The world is fast moving towards SD-WAN deployment to serve evolving networking needs, facilitating digital transformation strategies that increasingly rely on the cloud. So, there's no real disadvantage for all businesses to get on the bandwagon.

In summary, an SD-WAN is a software-defined wide-area network that does what traditional WAN does in that it connects various locations on a network across vast geographic areas. An SD-WAN is also an overlay to the underlying connection, so it uses various MPLS connections and manages them centrally.

An SD-WAN carries many benefits over MPLS in that it is more cost-efficient, performs better, and offers better protection if security integration is done from the outset. It can securely connect to the cloud through its various features, and it can be scaled, helping business growth.

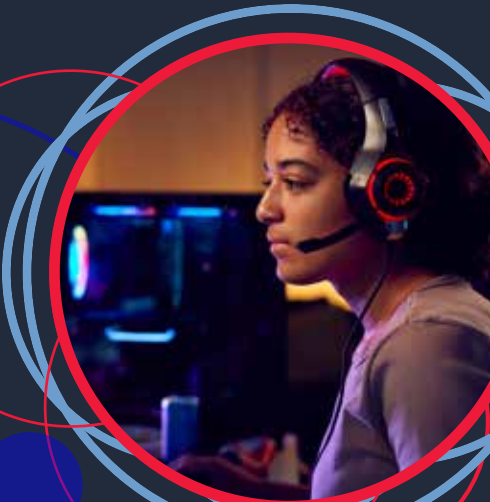
Handling of an SD-WAN also appears to be light-touch through zero-touch provisioning and security, including encryption and firewalls, enabling the security features to rise and compete against secure MPLS connections. This protection is further enhanced through micro-level segmentation, offering a granular level of security with security levels that can intelligently adapt as the infrastructure does.

In light of these clear benefits to using an SD-WAN for organisational networks, the key thing to remember is to make the most of the SD-WAN deployment, particularly enhanced and adequate security. Choosing the right SD-WAN solution from the right vendor thus becomes key.

Koris365 staff are experts on emerging technologies with a team who hold a variety of business and technical skills intuitive to the needs of its customers. That's why many of our clients have chosen us to provide, implement, upgrade and adapt technologies and implement new technologies.

We do this while focusing on customer service, always striving to enhance the client experience to serve our reputation and ensure they are satisfied and remain with us through the organisational life cycle.

That's why we can provide SD-WAN solutions that leverage a full spectrum of benefits that are in line with your business requirements. Get in touch today to find out how we can work together.



At Koris365, we have a wealth of expertise in network design, installation and configuration. Contact us today to discuss your network requirements.

SPEAK TO OUR TEAM

info@koris365.com

0345 230 0365

koris365.com