In co-operation with

Executive Briefing

# ENTERPRISE NETWORKING CHALLENGES: HOW CAN SD-WAN HELP?

We highlight the main networking challenges that SD-WAN is designed to address. Part 1 of a three-part mini-series exploring SD-WAN technology from an enterprise perspective.

David Martin, Associate Senior Analyst | Matt Pooley, Virtualisation Lead
matt.pooley@stlpartners.com | May 2019

# Preface

This document is the first in a mini-series of three reports which seek to explore SD-WAN technology from an enterprise perspective, covering the challenges that SD-WAN is designed to address, the differing types of SD-WAN product on the market today, and how we envisage SD-WAN-type services evolving in future.

The document has been prepared by independent research firm STL Partners and commissioned by Juniper Networks. It is based on STL Partners' continuous research program into the future telecoms operator and how to get there.

Mentions or allusions to companies or products in this document are intended as illustrations of market evolution and are not intended as endorsements or product/service recommendations.

# Table of Contents

# Table of Figures

# Introduction: What networking challenges are faced by today's digital enterprises?

Enterprises throughout the world are rapidly digitizing their operations. Increasingly, the digital strategies they are adopting include the transition of business tools, applications and processes to a 'multicloud' environment: involving a hybrid combination of applications and data hosted in one or more public clouds alongside the company's own private data centers.

Digital enterprises require secure access to their applications and data from any location, at any time, via any device and over any network. At the same time, they need to ensure that their end users – both employees and customers – have the same application quality of experience as they did when the tools, applications and processes were hosted in the company's own private data center.

Unfortunately, existing WAN architecture models often do not provide the scale, flexibility or agility required to support this transition. These legacy WAN architectures typically leverage a hub and spoke network topology, where the hub is in the corporate data center and static, point-to-point circuits that often require manual provisioning for deployment, moves, adds and changes connect the hub site to the branch offices. As these organizations transition to multicloud, the corporate data center, hub site, becomes a bottle neck. Additionally, their static, manually provisioned circuits can't keep pace with the dynamic nature of multicloud traffic flows.

Consequently, these businesses need to look for a new, simplified and automated approach to managing and transforming their WAN. Additionally, as enterprises look to leverage broadband internet to simplify and manage the cost of the WAN, they need to maintain the same SLA levels, ensure application quality of experience (QoE), and to be mindful of the security implications and risks in doing so.

SD-WAN platforms and services represent a response to these networking challenges that is being adopted more and more by enterprises of all sizes – from SMBs through to the largest multi-nationals – across all regions worldwide.

In this report, we highlight the main networking challenges that SD-WAN is designed to address, and outline in brief some of the ways it does so.

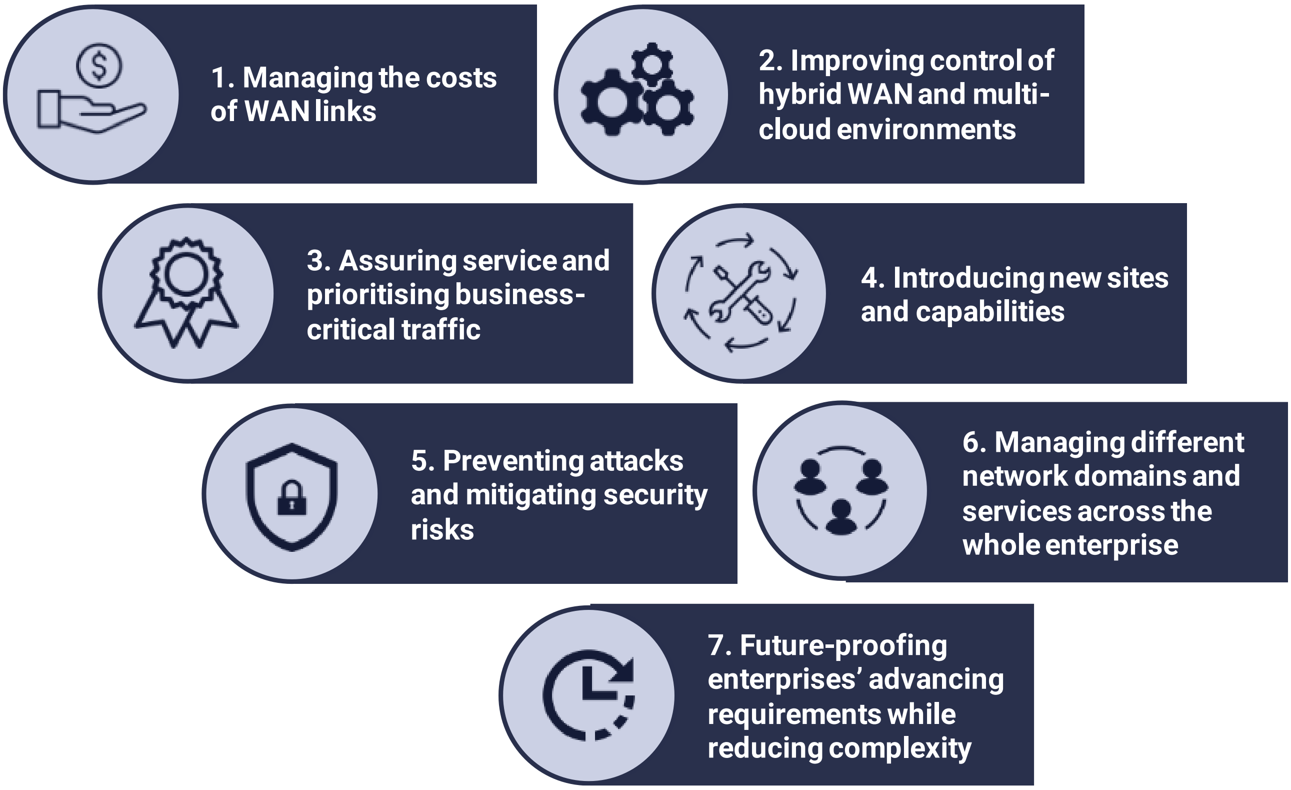
In a subsequent report, we will discuss the main types of SD-WAN platforms and services available on the market today, along with the leading vendors and communications service providers that provide them. And in a third report, we discuss some of the ways in which we expect SD-WAN technology and services to develop over the next few years as it expands to encompass more and more aspects of enterprise information and communications technology, and to meet the needs of new applications and automated processes.

# Which networking challenges does SD-WAN address?

In this section, we discuss the main problems faced by network engineers and operations personnel managing the WAN, and evolving its architecture and functionality, in response to the rapidly changing, digital requirements of their enterprise. At the same time, network operations are under increasing pressure to reduce costs while maintaining, and indeed improving, quality of service and experience.

With these pressures in mind, we have identified seven key networking challenges faced by enterprises:

**Figure 1: 7 key enterprise networking challenges**



1. Managing the costs of WAN links

2. Improving control of hybrid WAN and multi-cloud environments

3. Assuring service and prioritising business-critical traffic

4. Introducing new sites and capabilities

5. Preventing attacks and mitigating security risks

6. Managing different network domains and services across the whole enterprise

7. Future-proofing enterprises' advancing requirements while reducing complexity

Source: STL Partners

In the sections below, we explore each of these challenges in detail, and how SD-WAN helps to address them.

## Challenge 1: managing the costs of WAN links

SD-WAN provides a means for enterprises to manage the relationship of networking costs to benefits more efficiently than under service provider contracts which are sometimes perceived as inflexible, longer-term and fixed-value, because capacity is effectively over-provisioned most of the time. One of the ways it does this is by enabling enterprises to use broadband Internet services (i.e. Internet breakout) as a cheaper alternative to the IP-MPLS and Ethernet circuits offered by service providers. to carry some or even all of their WAN traffic – with cloud-hosted software-defined networking (SDN) control replacing and improving on much of the traffic prioritization and management functionality previously provided by IP-MPLS and IP-VPNs.

When offered as part of a managed platform service, SD-WAN can also integrate other SDN features, such as the ability to add, scale or remove network connections and links on demand. This allows networking services to be consumed closer to a pay-as-you-use business model ('Network as a Service', or NaaS), on a similar basis to cloud-based Software-, Infrastructure- or Platform-as-a-Service business models. Consequently, enterprises can manage the relationship of networking costs to benefits more efficiently than under inflexible, longer-term and fixed-value service provider contracts in which capacity is effectively over-provisioned for much of the time.

## Challenge 2: improving control of hybrid WAN and multicloud environments

WAN routing and security is traditionally intricate to configure, and as the number of sites connected to the WAN grows, so too does the complexity. Adding multiple, new capabilities at each site becomes unmanageable. As enterprises adopt multicloud and hybrid WAN, this complexity will only intensify.

Many SD-WAN solutions use a single customer premises equipment (CPE) appliance to replace the multiple edge devices at each site, all with dedicated functions such as routing, firewall, load balancing, etc. The SD-WAN appliance hosts the SD-WAN capabilities, which are either dedicated to the SD-WAN vendor's appliance or can be implemented as a virtual network function (VNF) on a vendor-neutral, open hardware appliance universal CPE (uCPE) that can also run other VNFs.

Unifying networking and security in one device is on the rise and assists simplicity. Furthermore, to cope with a sprawling site footprint and to simplify management of remote sites without expert network engineers, SD-WAN solutions streamline the deployment and ongoing management of remote sites. Their support for zero-touch provisioning of WAN edge devices eliminates the need for on-site technicians to bring new sites online and to carry out further site visits to make configuration changes or corrections. Their ability to collect network data from the SD-WAN CPE device and provide metrics, analytics and reports provides network administrators with visibility into not just the remote WAN connections, but for some solutions they can also get visibility into the remote branch site LANs as well.

In addition, replacing multiple hardware appliances with a single edge device reduces capex alongside opex: it lowers the total cost of ownership of network assets while increasing the long-term return enterprises can earn from their network investments. This is because it is easier and cheaper to upgrade VNFs on a COTS hardware device – or even swap them out altogether for another vendor's SD-WAN or VNFs – than it is to upgrade or replace multiple dedicated appliances.

Finally, enterprises are increasingly adopting cloud-hosted solutions for SD-WAN management – either as a software service, or an end-to-end managed service which includes connectivity and CPE.

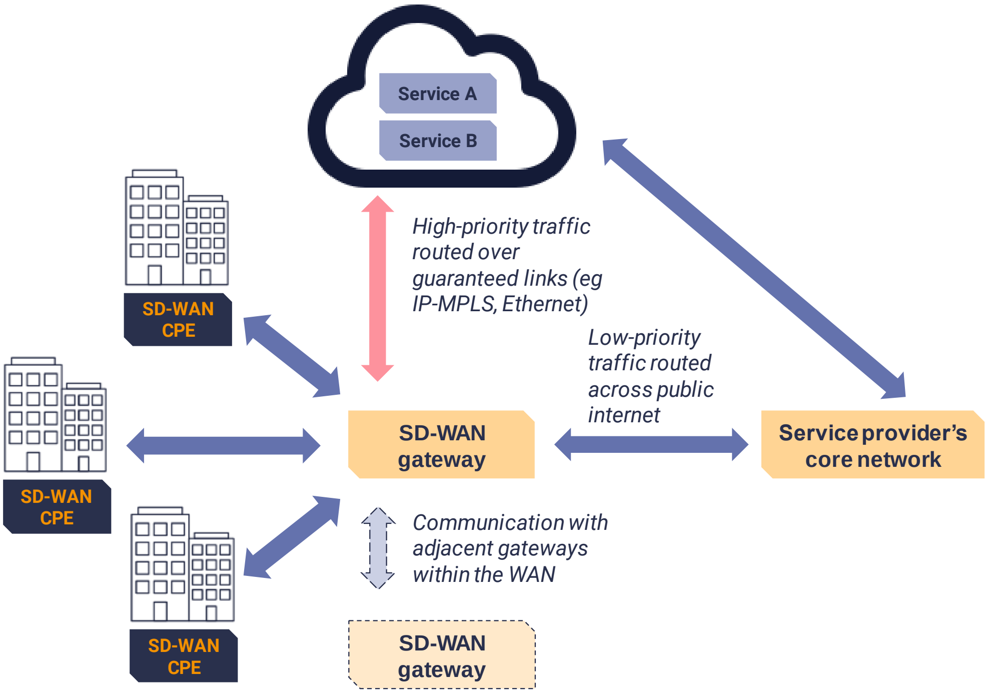
These solutions further aid with the simplification of tools, as they eliminate the need for enterprises to maintain centralized control software. Cloud-hosted network functions, if they can be easily tied into the WAN service path, can further reduce the need to manage functions in each site, although cloud is not always the best option - some services will always benefit from the proximity of sitting on site.

## Challenge 3: assuring service and prioritizing business-critical traffic

Critical services like business communications and customer-relations management (e.g. Salesforce) must not suffer because of relatively unimportant traffic (e.g. social media use by staff, or public and guest Wi-Fi). This extends to cloud applications too – enterprises want to give priority to more important apps, as appropriate. SD-WAN enables traffic prioritization with policies and monitoring to configure and detect service levels per application or even per user. More critical application traffic can be directed over links with guaranteed service levels, such as service provider IP-MPLS or Ethernet; meanwhile, less critical traffic is routed across fixed or mobile broadband access and public Internet connections.

By providing breakouts and gateways from the private WAN to the public Internet, SD-WAN can also enable direct connections from WAN sites to the public clouds hosting their applications and data. Such internet breakouts or gateways may be directly on the CPE devices or in SD-WAN routing hubs. These hubs may be managed by the enterprise or the SD-WAN provider. This improves efficiency, lowers costs and reduces latency from having to backhaul all cloud-directed traffic to the private data center and then on to the cloud services employed.

### Figure 2: SD-WAN enables traffic prioritization


Service A
Service B
High-priority traffic routed over guaranteed links (eg IP-MPLS, Ethernet)
Low-priority traffic routed across public internet
SD-WAN CPE
SD-WAN CPE
SD-WAN CPE
SD-WAN gateway
Service provider's core network
Communication with adjacent gateways within the WAN
SD-WAN gateway

Source: STL Partners

In addition to monitoring application quality of experience, most SD-WAN platforms now provide dynamic, automatic adjustment of per-application routing and capacity across multiple, redundant hybrid WAN links and different connection types to ensure that sufficient bandwidth is always available for the higher-priority applications. Many SD-WAN solutions also provide failover links or link aggregation to assure service continuity in the event of network outages or capacity overloads.

## Challenge 4: introducing new sites and capabilities

The typical process of adding new or temporary sites to the WAN, usually one site at a time, is often too cumbersome and slow to keep up with the speed of business needs and continual barrage of threats and vulnerabilities. At the same time, introducing a new policy, feature, patch or upgrade across multiple locations requires automation in the control and management plane of the solution.

The centralized and simplified management features of SD-WAN discussed above vastly accelerate the process of adding new or temporary sites to the WAN by consolidating diverse branch appliances and hybrid WAN connections. SD-WAN gives engineers a holistic view of the network, so that they can ensure compliance with existing policies, security, service levels and application prioritization.

SDN-based control and automated workflows across many devices are core to SD-WAN. Going beyond a central point of management or cloud-based management, software-defined management truly means that new sites, connections can be provisioned and observed across the aggregation of WAN sites and devices. Thus, changes are possible within a few days or hours, where there is no need for uneven or device-by-device changes.

Similarly, network functions virtualization (NFV) characteristics of SD-WAN platforms allow new VNFs or arbitrary virtual machines (VMs) to be added or upgraded into sites' universal CPEs.

## Challenge 5: preventing attacks and mitigating security risks

Security is important in all networking, but it is particularly essential for an Internet-connected, hybrid SD-WAN. Carrying more WAN traffic over the public Internet inherently creates potential vulnerabilities, while the multiplication of endpoints and Internet gateways expands the attack surface.

So, in parallel to the deployment of the SD-WAN, there is a need to ensure an integrated, unified and comprehensive approach to security. When deep security measures, such as next-generation firewalling (NGFW) and unified threat management (UTM), are provided as an integral part of an SD-WAN solution, this eliminates the complexity, network load and risks of adding a separate security layer on top of SD-WAN networking.

In addition, adopting security measures such as these helps to simplify and enhance the security of branch sites' LAN too when integrating LAN security into the SD-WAN management tools, analytics and reporting capabilities.

## Challenge 6: managing different network domains and services across the whole enterprise

Network and security policy management is not limited to the hybrid WAN overlay and private WAN underlays; it extends to the enterprise campus and branch LANs, WLAN or Wi-Fi networks, private clouds and data centers, and public clouds. The scope of some SD-WAN platforms is also being expanded to incorporate integrated management of the whole of the enterprise's networking operations, including 'SD-Branch' and 'SD-LAN' alongside SD-WAN. The centralized capabilities of SD-WAN can provide a single pane of glass that enables comprehensive visibility and monitoring of application and network performance across the different network domains and technologies employed.

In addition, many enterprises need to run multiple SD-WAN platforms serving different geographies, network domains, application usage or security requirements. Increasingly, SD-WAN platforms and management consoles can support the smooth interworking and performance monitoring of multiple SD-WAN deployments, and their associated routing and control platforms, across different parts of the enterprise.

## Challenge 7: future-proofing enterprises' advancing requirements while reducing complexity

While meeting the networking challenges of today's enterprises, network managers need to ensure that the SD-WAN and other networking platforms and services being deployed have evolvable capabilities and capacity to support further digitization and automation of enterprise processes. In addition, they need to support the introduction and management of new technologies such as Internet of things (IoT) networks and artificial intelligence (AI).

The advent of these technologies, together with the drive towards automation and ever greater operational efficiency, create additional complexities across all network domains: access, edge and cloud; LAN and WAN. At the same time, the whole purpose of introducing these technologies is ultimately to reduce operational complexity and business costs.

It is the networking function that carries the burden of reconciling these two seemingly conflicting directions. SD-WAN platforms and architectures can play a major role in supporting these goals. First, automated SD-WAN tools, systems and technologies can help remove and abstract complexity, and increase productivity with faster (dynamically driven) and smarter (AI-driven) workflows. Second, infrastructure such as VNFs and SDN control software must become more openly extensible and programmable. The use of standard APIs will support infrastructure and operations engineers to integrate and automate more agility, reliability and flexibility into the network and their own operational processes.

# Conclusion: is SD-WAN really a one-stop shop solution?

In this report, we have discussed seven major enterprise networking challenges for which SD-WAN can be a major part of the solution. These are:

1. Managing the costs of WAN links
2. Improving control of hybrid WAN and multicloud environments
3. Assuring service and prioritizing business-critical traffic
4. Introducing new sites and capabilities
5. Preventing attacks and mitigating security risks
6. Managing different network domains and services across the whole enterprise
7. Future-proofing enterprises' advancing requirements while reducing complexity.

However, it would be wrong to assume that SD-WAN represents a simple, one-stop-shop solution and panacea to all these networking challenges. In practice, there is a growing array of SD-WAN solutions and delivery models in the market. These include CPE appliance or cloud-hosted SD-WAN capabilities; managed SD-WAN platforms provided by vendors and service providers; SD-WAN solutions with integrated, value-added capabilities such as security; and comprehensive managed services offerings.

In the next report in this SD-WAN mini-series, we discuss some of the different options that are available to enterprises as they navigate the complicated SD-WAN landscape to find the optimal solution to meet their business needs.

STL PARTNERS

Research

Consulting

Events

www.stlpartners.com