WHAT TO CONSIDER WHEN EVALUATING YOUR SD-WAN OPTIONS

CONTENTS

INTRODUCTION

Enterprises currently face challenges regarding the price, performance, and flexibility of traditional wide area networks (WANs). Aggressive growth in the adoption of public cloud services (28.6% year-over-year growth in 2017)[1] is forcing organizations to look elsewhere for a more effective network solution to address distributed traffic across remote sites and branch offices.

Some of the specific issues organizations face with their traditional WANs include:

- High total cost of ownership (TCO)
- Lengthy provisioning cycles
- Performance degradation with the growth of cloud traffic
- Inadequate redundancy and resiliency
- Lack of application-aware connectivity

To better manage WAN investments, enterprises are adopting a new approach for their distributed branch office networks. **Software-defined WAN (SD-WAN)** offers improved performance, agility, and operational flexibility plus significant cost savings. But not all SD-WAN solutions are created equal.

[1] "Worldwide Public Cloud Services Revenue Growth Remains Strong in the First Half of 2017," IDC, November 6, 2017.

01 PROBLEMS WITH TRADITIONAL WAN SOLUTIONS

Traditional WAN performance comes at a premium because it is almost entirely limited to expensive circuits like multiprotocol label switching (MPLS). At the same time, the rapid increase of cloud applications being used across distributed organizations has caused a sharp uptick in network bandwidth demands. As these performance needs increase, traditional WAN infrastructures become dramatically more expensive, complex to deploy, and difficult to manage. As evidence of this problem, **according to a poll conducted at Gartner's 2016 data center conference, "a 6:1 ratio of respondents described their WAN as either 'brittle and slow, prone to outage, or too expensive,' versus 'cost-effective and agile'."**[2]

[2] Gartner, Market Guide for WAN Edge Infrastructure, Andrew Lerner, Neil Rickard, March 2017.

High TCO

- Traditional WAN solutions have **expensive bandwidth**. They maintain intersite connectivity and quality of service by relying on costly MPLS circuits. MPLS also requires long deployment times, which inhibits company growth and overall productivity.
- There's also **greater complexity**. Disparate security and network functions means that there are more pieces to keep track of. Management through a command-line interface (CLI) compounds this problem. CLI requires a lot of time dedicated to log management tracking, increases the chance of human error, and decreases overall staff productivity.

Cloud Visibility and Adoption

- Traditional WANs have **inferior cloud visibility** because they can only offer a packet- and routing-level view, rather than application visibility.
- Traditional WANs can also create **performance bottlenecks** that impact user performance and productivity across the business, and especially so with increasing cloud-based demands. Because traffic gets routed through the data center, it travels further and increases latency. Also, **traditional WAN traffic is not intelligent** and cannot be assigned by policy to the right broadband channel.

Security at the Data Center

- The private MPLS connections that most traditional WANs utilize enable centralized security. Traffic is funneled into the data center (a process known as backhauling) in a typical "hub-and-spoke" network architecture where everything passing through the network can be checked and filtered. While traffic is secure, it comes with a **performance penalty.**
- By design, traditional WANs have **no direct internet access** via public links—which in turn limits the performance available for the ever-expanding use of cloud services such as Software-as-a-Service (SaaS) applications.
- Some organizations elect to purchase their network and security solutions separately, resulting in **siloed devices with separate management consoles** that **limit transparent visibility.** This makes operations more complex and time-consuming.

Resiliency/Business Continuity

- The WAN connectivity failover options for MPLS (4G/3G networks) are **not reliable** and organizations lack the **resiliency** their business requires. This, in turn, can disrupt regular business operations with downtime and incur lost productivity.

02 SIX THINGS TO CONSIDER WHEN EVALUATING SD-WAN OPTIONS

With all the above issues associated with traditional WANs, enterprises need a replacement infrastructure with significant simplification, an improved cost advantage, and better support for cloud adoption.

Unlike traditional WAN architectures, **software-defined wide area networks (SD-WANs)** can dynamically distribute traffic across multiple locations while automatically responding to changing application policies for better performance. This, in turn, enables better agility and cost-effectiveness versus traditional networking solutions.

Gartner anticipates that "25% of enterprises will adopt SD-WAN in the next two years."[3] But there are many differences between the various vendor products on the market—from functionality, to deployment and management, to the visibility they provide, to price-performance and cost.

Following are six key benefits that decision-makers should look for when considering SD-WAN for their organization:

[3] Gartner, Market Guide for WAN Edge Infrastructure, Andrew Lerner, Neil Rickard, March 2017.

1. CLOUD APPLICATION ADOPTION

According to IDC, adoption of public cloud services is growing at a 28.6% year-over-year clip.[4] This growth results in a proliferation of clouds across the enterprise. At present, the average enterprise already uses around 30 different SaaS applications across their organization.[5]

Complicating matters is the fact that a rising percentage of those who purchase and manage SaaS apps are non-IT managers. In 2017, line-of-business buyers will spend more on software applications ($150.7 billion) than IT buyers ($64.7 billion).[6]

With the number of active cloud apps expected to continue growing, SD-WAN can help businesses adopt more SaaS apps without bottlenecking network performance or impacting the productivity of end-users. Specifically, SD-WAN eliminates backhauling cloud application traffic through the data center by enabling direct internet access to remote networks. This dramatically reduces latency and packet loss.

[4] "Worldwide Public Cloud Services Revenue Growth Remains Strong in the First Half of 2017," IDC, November 6, 2017.
[5] Nirav Shah and Bill McGee, "Empowering Distributed Enterprises with Secured SD-WAN," Fortinet, accessed December 16, 2017.
[6] "Technology Purchases from Line of Business Budgets Forecast to Grow Faster Than Purchases Funded by the IT Organization," IDC, March 23, 2017.

Any number of industries can benefit from SD-WAN, though the potential outcomes are greater for certain ones such as:

- **Healthcare.** Healthcare organizations typically have numerous remote sites consisting of users that need access to SaaS services used for electronic medical records (EMR), patient care, accounting, and finance, among other functions. As each of these requires substantial bandwidth, traditional WANs simply cannot keep up with expanding cloud-based performance needs across an extended healthcare infrastructure. A secure SD-WAN solution provides flexible, affordable bandwidth to better address the growing cloud application needs of healthcare professionals, while better serving patient outcomes and keeping private medical information safe.
- **Retail.** Combining brick-and-mortar and web-based sales, today's retail chains increasingly rely on a converged suite of cloud-based ecommerce tools to coordinate all aspects of their business—from inventory management to payment processing to customer data analytics. With remote outlets that can tally in the hundreds or even thousands, retail organizations can rely on SD-WAN for better high-volume network application performance across widely distributed geographies, even at peak sales times.
- **Manufacturing.** Like retail, modern manufacturing and industrial organizations are tapping an assortment of coordinated SaaS applications to better run many different job functions across diverse territories and even international boundaries. The rigorous conditions and critical nature of some of these operations means that networked applications cannot be constrained by performance limits without serious consequences. A secure SD-WAN solution offers affordable and agile bandwidth to support functions such as automated supply chain management, international sales, and industrial controls that maintain both worker safety and optimal productivity.

2. APPLICATION AWARE

The static nature of a traditional WAN infrastructure can put a serious damper on application performance across a distributed operation. Your SD-WAN solution should support the increasingly urgent need for **complete visibility into applications** to help administrators monitor and manage traffic patterns, balance bandwidth needs, and scale performance across the entire distributed enterprise. In this scenario, the SD-WAN maintains current information on all applications and optimizes their function by intelligently routing and prioritizing applications based on network bandwidth and which users need access to each. Information on each application includes application state and resource requirements.

3. PATH AWARENESS INTELLIGENCE

Path awareness intelligence means that your solution should **automatically prioritize the routing of applications** across network bandwidth based on the specific application and user. Offering a per-application-level SLA, path awareness intelligence dynamically selects the best WAN link/connection for the situation. This enables organizations to prioritize

applications based on their criticality, time of the day, and other factors.

Unlike the traditional MPLS-based WAN service (with limited and expensive connectivity), SD-WANs provide a lightweight replacement for traditional WAN routers and are agnostic to WAN transport (MPLS, internet, LTE, etc.). SD-WAN solutions allow for intelligent load sharing of traffic across multiple broadband connections for greater network efficiency and dynamic operation across a distributed enterprise. Path awareness intelligence helps maximize the benefits of SD-WAN's connectivity advantage.

4. INTEGRATED SECURITY AND COMPLIANCE

Without the centralized protection provided by backhauling traffic through the data center, moving from MPLS to direct internet broadband connections requires additional security within the enterprise infrastructure—especially considering that cyber attacks continue to grow in volume and sophistication.

Distributed network and security capabilities in WANs have proven inefficient and ineffective. Today, according to Gartner, "Software-defined WAN (SD-WAN) products now incorporate internet perimeter security, but more than 90% of SD-WAN vendors are not traditional security vendors, which causes clients to question whether they can rely on embedded security alone."[7] This offers the potential for higher setup costs and increased TCO, not to mention greater risk from potential gaps between the disparate technologies for network and security. And as SSL-encrypted enterprise traffic grows beyond 50% in the coming years, encrypted traffic must be thoroughly checked for hidden malware without bottlenecking network performance.[8]

[7] Gartner, Four Architectures to Secure SD-WAN, Bjarne Munch, Greg Young, October 2017.
[8] Nirav Shah and Bill McGee, "Empowering Distributed Enterprises with Secured SD-WAN," Fortinet, accessed December 16, 2017.

Next-generation firewall (NGFW) security is a key requirement for enabling direct internet access in an SD-WAN architecture. NGFW protection is critical for reducing risk exposure across an extended network. Its SD-WAN-ready security features should include:

- **A single-box solution** that combines both network and security functions in one device can strengthen protection across the distributed environment while simplifying controls and reducing investment costs.
- **SSL inspection** to protect your distributed network against malware and other threats hidden in encrypted web traffic. SSL inspection can unlock sessions, look into encrypted packets, find threats, and block them.
- **Web filtering** to offer a first line of defense against web-based attacks. It protects organizations by blocking access to malicious, hacked, or inappropriate websites.
- **High-throughput IPsec VPN** is critical for secure SD-WAN deployments. Internet protocol security (IPsec) allows two or more hosts to communicate in a secure manner by authenticating and encrypting each IP packet of a virtual private network (VPN) communication session.
- **Compliance tracking and reporting functions** help ensure adherence to industry standards and regulations while reducing collateral risks of fines and legal costs in the event of a breach. Your NGFW should include reporting features that track real-time threat activity to facilitate risk assessment, detect potential issues, and mitigate problems. It should also monitor firewall rules and policies and automate compliance audits.

5. MULTI-BROADBAND SUPPORT

As previously mentioned in reference to path awareness intelligence, your SD-WAN controller should be able to mix and match multiple broadband connections (internet, MPLS, LTE, etc.) to support direct use of public internet connections. Because SD-WAN is transport and carrier agnostic, its connectivity is no longer dependent on just MPLS and unreliable 4G/3G network failovers, which can put business operations at risk of downtime. By leveraging the public internet as a failover option, SD-WAN offers **greater resiliency and redundancy** to prevent performance degradation and outages.

6. TCO

The move to public broadband means that expensive MPLS connections can be replaced with more cost-effective options such as the public internet or long-term evolution (LTE). This can deliver measurable operational cost savings versus traditional WAN.

In addition, with security and network control functions integrated into **a single pane of glass**, SD-WAN reduces complexity and simplifies management. Security staff can spend less time managing the various aspects of network and security operations and correlating events.

Your SD-WAN solution should also support **zero-touch deployment** for greater efficiency when bringing new branches online. These features help businesses grow through fast provisioning, streamlined configuration, and automatic authentication—as well as centralized monitoring and support. Zero-touch deployment saves tons of time when compared to the more involved processes of adding branches in a traditional WAN environment.

SUMMARY

The traditional WAN is no longer an effective solution for today's distributed enterprise. Organizations are overcoming the significant security and network issues by moving to SD-WAN. Gartner indicates that "by 2018, more than 40% of WAN edge infrastructure refresh initiatives will be based on vCPE or SD-WAN appliances versus traditional routers."[9]

[9] Gartner, Market Guide for WAN Edge Infrastructure, Andrew Lerner, Neil Rickard, March 2017.

There are many different SD-WANs on the market today, and VPs of IT should carefully review each of them. This is where the above "Six Things to Consider" can help. In that regard, Fortinet Secure SD-WAN integrates enhanced SD-WAN features into proven security capabilities, providing next-generation protection and networking capabilities that improve network efficiency without compromising security.

FORTINET®

www.fortinet.com

154319-A-0-EN