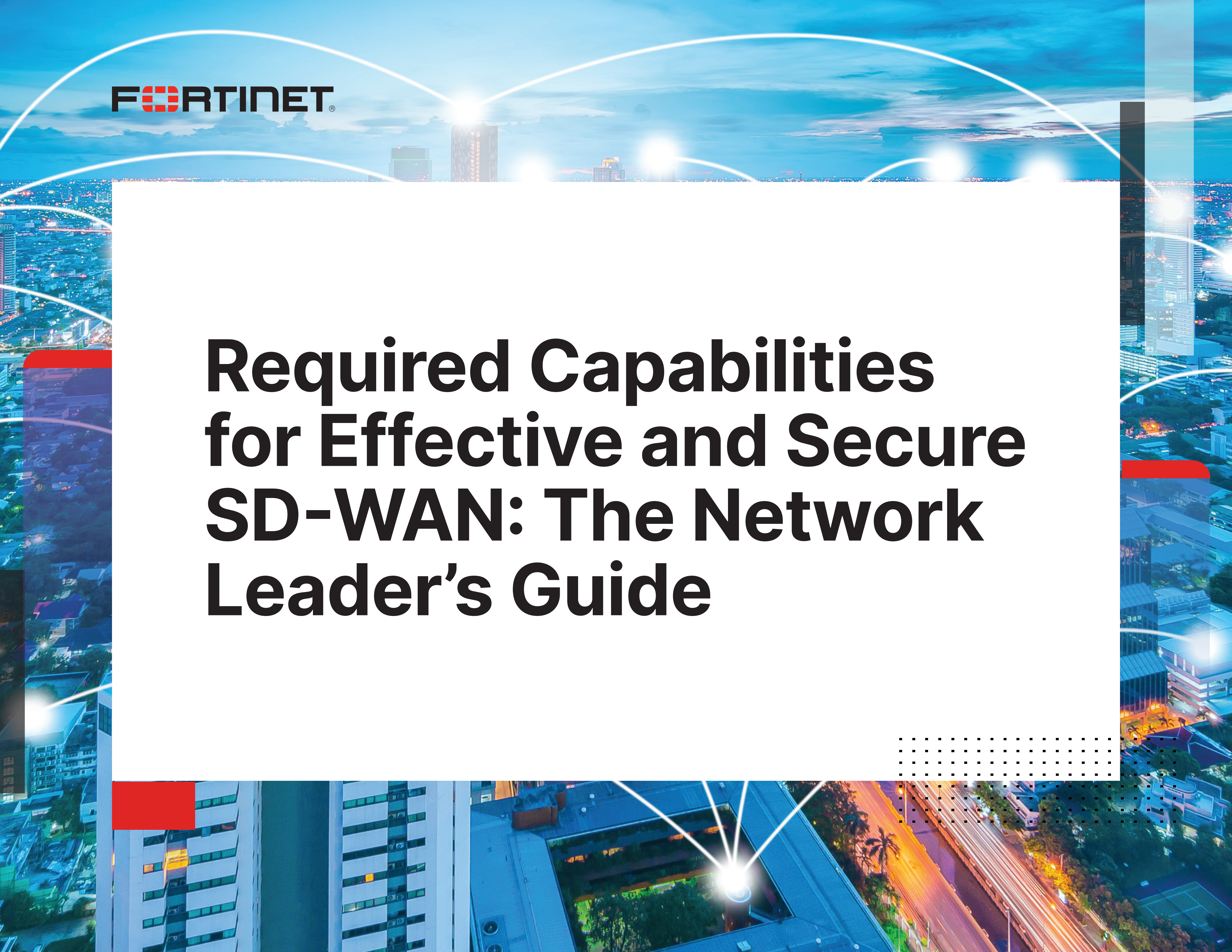

FORTINET

Required Capabilities for Effective and Secure SD-WAN: The Network Leader’s Guide

Table of Contents

Executive Overview

There are three main trends driving organizations to replace outdated wide-area networking (WAN) infrastructures with a secure software-defined WAN (SD-WAN) solution.

- Digital innovation that leverages Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS) increases traffic demands, cost, and performance bottlenecks of multiprotocol label switching (MPLS) connectivity over traditional WAN infrastructures.
- The work-from-anywhere model, meant to be a short-term fix at the start of the pandemic, has become the new normal. Organizations need to ensure remote workers have secure, reliable access to all corporate resources.
- Cyber criminals are busier than ever, and innovations in Cybercrime-as-a-Service make it fast and easy for unsophisticated attackers to launch very sophisticated attacks.

When considering SD-WAN solutions, there are three key requirements to look for to address these trends. An effective solution will offer integrated capabilities needed to enable efficient management and operations, excellent quality of experience (QoE) for both end-users and IT staff, and comprehensive security.

Introduction

With digital innovation, work-from-anywhere, and increasingly sophisticated cyberattacks placing increased demands on bandwidth requirements to securely deliver the experience users demand, SD-WAN requirements are maturing. However, many solutions on the market today are incomplete. Issues like limited scalability, the lack of automation to simplify operations, and lackluster cloud on-ramp and cloud and SaaS integrations can result in a poor user experience that can undermine the value of an SD-WAN deployment. Further, enabling a direct internet connection via SD-WAN means traffic is no longer backhauled through the data center to apply security controls. Therefore, to be effective, an SD-WAN solution must include a robust set of networking, connectivity, and security tools that can meet and adapt to the dynamic nature of today's networks. The solution must be able to keep up with rapid cloud adoption, transition from regional to global deployments, office or branch expansion, and the remote workforce.

“The global Software-Defined Wide Area Network (SD-WAN) market size is expected to grow ... to USD 8.4 billion by 2025, at a Compound Annual Growth Rate (CAGR) of 34.5% during the forecast period.”[1]

Addressing Business Demands With SD-WAN

SD-WAN offers the ability to use available WAN services more effectively and economically—giving users across distributed organizations the freedom to better engage customers, optimize business processes, and innovate. WAN innovation with additional carrier links can be leveraged to provide redundancy, load balancing, and optimization of application traffic. It also makes WAN management more cost-effective, which is why SD-WAN solutions will continue to be a robust growth market for the foreseeable future.

To answer this demand, there have been many SD-WAN solutions introduced in the last few years. But not all of them include the necessary capabilities.

The optimal SD-WAN for an enterprise depends on the organization's requirements regarding:

- Security
- Application performance
- Cloud on-ramp to multi-cloud deployments
- Simplified operations with centralized management at any scale

To address these business requirements, organizations need a comprehensive SD-WAN offering with built-in security and the performance capabilities to scale across any size enterprise. This solution should also enable centralized visibility and management.

As branch offices are directly exposed to the internet via broadband connections with SD-WAN, an ideal solution integrates SD-WAN and a next-generation firewall in a single appliance or virtual machine (VM).

Instead of separate WAN routers and security devices such as firewalls and secure web gateways (SWGs), a single NGFW should perform all these functions.

Application Awareness for Improved Service Levels

Performance is critical so an effective SD-WAN solution will deliver fast, dynamic application steering and application identification performance. This includes deep secure sockets layer (SSL)/transport layer security (TLS) inspection with no performance degradation. Encryption inspection capabilities also must include the ability to inspect the packet for the SD-WAN solution to correctly route the traffic.

Technically, SD-WAN works by routing applications over the most efficient WAN connection at any point in time. To ensure optimal application performance, SD-WAN solutions must be able to identify a broad range of applications and apply routing policies at a very granular level. Without these capabilities, SaaS applications, video, and voice can slow and impede end-user productivity.

Advanced SD-WAN solutions can recognize applications by business criticality. Business-critical applications (e.g., Office 365, Salesforce, SAP), general productivity applications (e.g., Dropbox), and social media (e.g., Twitter, Instagram) can be given different routing priorities. Unique policies can be applied at a deeper level for sub-applications (e.g., Word or OneNote within Office 365).

This deep and broad application-level visibility into traffic patterns and utilization offers a better position to allocate WAN resources according to business needs.

When it comes to WAN efficiencies, key capabilities of SD-WAN include:

Automated path intelligence. Application awareness enables prioritized application routing across network bandwidth based on the specific application and user. SD-WAN service-level agreements (SLAs) should be able to be easily defined by dynamically selecting the best WAN connection for the specific business circumstances. For low- to medium-priority applications, organizations can specify the quality criteria, and the solution will select the corresponding link. For high-priority and business-critical applications, organizations can define strict SLAs based on a combination of jitter, packet loss, and latency metrics.

Automatic failover. Multi-path technology can automatically fail over in a sub-second to the best primary WAN path. This automation should be built into the solution, and occur immediately, which reduces complexity for end-users while improving their experience and productivity.

WAN path remediation. WAN path remediation utilizes forward error correction (FEC) and packet duplication to overcome adverse WAN conditions such as poor or noisy links. This enhances data reliability and delivers a better user experience for applications like voice and video services. FEC adds error correction data to the outbound traffic, allowing the receiving end to recover from packet loss and other errors that occur during transmission. Packet duplication sends copies of packets on alternate available paths. This improves the quality of real-time applications.

Application prioritization. With the ability to define application-specific business policies, the best possible utilization of bandwidth can be ensured by adding precise quality of service (QoS) prioritization for critical applications, while rate-limiting non-critical applications that can impact performance and end-user experience.

Tunnel bandwidth aggregation. For applications that require greater bandwidth, SD-WAN should enable per-packet load balancing and delivery by combining two overlay tunnels to maximize network capacity.

"A common misconception about software-defined wide area networking (SD-WAN) is that all solutions are essentially the same."[2]

Simplified Management and Increased TCO

Network engineering and operations leaders are often in a quandary when it comes to deploying SD-WAN devices in numerous remote sites and branch offices. Truck rolls are expensive, and technical staff is often limited. On the other hand, shipping fully configured devices is not secure. Also, once edge devices are deployed, staff must manage both the WAN and security functions from separate consoles.

Secure SD-WAN solves both deployment and the management problems to reduce total cost of ownership (TCO).

Zero-touch deployment. Simplified deployment capabilities let enterprises ship unconfigured SD-WAN appliances to each remote site. When plugged in, they should automatically connect to a service that authenticates the remote devices and connects them to a centralized management system.

Single-pane-of-glass management. Centralized visibility of all deployed secure SD-WAN devices across the distributed organization is key. A simplified workflow to deploy and update policies with few easy clicks/steps should be included.

An SD-WAN solution should be able to automatically build and manage full mesh overlay links for secure connectivity between sites.

With guided workflows, automated overlay, and simplified business policies, IT staff hours spent on infrastructure deployment and changes are reduced from months to minutes.

SD-WAN reporting and analytics. Enhanced analytics for WAN link availability, performance SLAs, and application traffic should enable the infrastructure team to troubleshoot and quickly resolve network issues.

These features would include:

- SD-WAN bandwidth monitoring reports and datasets
- SLA logging and history monitoring via datasets, charts, and reports
- Customizable SLA alerting
- Application usage reports and dashboards
- Adaptive response handlers for SD-WAN events as well as event logging and archiving SLAs across applications and interfaces

Access proxy capabilities. The ideal SD-WAN solution will integrate access proxy capabilities, such as zero-trust network access (ZTNA). This allows organizations to host applications anywhere with consistent policy controls to enable and secure hybrid workforce models with seamless and superior user experience.

“With the right secure SD-WAN solution in place, organizations can enjoy the combined benefits of NGFW, ZTNA access proxy, automation, and traffic shaping, among others.”[3]

Controlling Multi-cloud Complexity

Low-latency access to distributed cloud. An ideal secure SD-WAN solution provides instant multi-cloud access such as Office 365. Plus, built-in security adds another layer of secure access to these applications, while providing a low-latency connection through public internet links so they can become part of the trusted and reliable WAN infrastructure.

This is especially critical as remote workers use advanced, feature-rich, cloud-hosted applications for voice and video conferencing. While these applications provide enhanced voice and video capabilities, they also demand more bandwidth availability. And in most cases, that traffic can also be encrypted, which adds strain due to traffic inspection. The intelligence to detect sub-applications and provide encrypted applications with SSL inspection capability at line rates ensures these applications are steered to the best-performing WAN link to provide optimal performance.

Public cloud connectivity. SD-WAN technology can play a key role in cloud connectivity. SD-WAN gateways can steer applications over policy-defined links and automatically set up Internet Protocol security (IPsec) tunnels to and across cloud service providers—all from a centralized console.

This means that SD-WAN can be used as a cloud overlay network to connect branch offices to cloud services, virtual networks within a single public cloud, and even across multiple clouds with one another. Its ability to prioritize traffic by application enables the most critical traffic to receive priority, and its ability to steer traffic over multiple routes for the best performance makes it ideal as a multi-cloud overlay. Access and security policies are centralized, and administrators have full visibility into application traffic, performance, and security.

“The big three cloud providers have taken steps to make it easier to support SD-WAN gateways.”[4]

Proven, Comprehensive Security

Secure SD-WAN must have robust threat protection, including Layer 3 through Layer 7 security controls. These include:

- Complete threat protection, including firewall, antivirus, intrusion prevention system (IPS), and application control
- High-throughput decryption and deep packet inspection of SSL/TLS including TLS 1.3 with minimal performance degradation, ensuring that organizations do not sacrifice throughput for complete threat protection
- Web filtering to enforce internet security without requiring a separate SWG device
- High WAN performance for cloud applications, featuring exceptional virtual private network (VPN) overlay performance for superior user experience and low latency

Secure SD-WAN should also monitor firewall rules and policies and highlight best practices to improve the organization’s overall security posture. This helps to simplify compliance with security standards as well as privacy laws and industry regulations. Automated auditing and reporting workflows can save staff time while reducing the risk of omissions and errors.

Enabling the SD-Branch

Many enterprise branches are deciding to simultaneously replace both their WAN and local-area network (LAN) devices in favor of a solution with deeper integration and simplified branch operations management. Using separate WAN and LAN infrastructures increases branch complexity. There are more devices to deploy and update with multiple management consoles. It also reduces visibility and control of operations while increasing the opportunities for security gaps that hackers can exploit. The right SD-WAN solution will solve these issues and accelerate SD-Branch deployment.

Accurate application detection is essential to ensuring the proper prioritization of business-critical applications. However, most SD-WAN solutions are unable to handle encrypted traffic.[5]

Across Google, more than 90% of traffic is encrypted.[6]

In an Unequal SD-WAN Market, Choose Wisely

As cloud-based applications and tools like voice and video become increasingly critical to distributed businesses, organizations must be able to embrace the benefits of digital innovation without putting security at risk, bottlenecking application performance, or impacting end-user productivity.

To reap the benefits of SD-WAN, organizations should evaluate solutions carefully. Rarely do SD-WAN solutions employ one operating system for SD-WAN and security for true integration. Comprehensive, integrated SD-WAN and security managed by one console, at any scale, is essential, yet few vendors offer it. Further, an effective SD-WAN solution needs to have advanced capabilities to enable expected QoE for end-users and IT staff and improve operational efficiency across WAN and cloud edges.

[1] "Software-Defined Wide Area Network (SD-WAN) Market by Component (Solutions (Software and Appliances) and Services), Deployment Type (On-Premises and Cloud), End User (Service Providers and Verticals), and Region - Global Forecast to 2025," Markets and Markets, accessed August 22, 2021.

[2] Robert Herriage, "How to Choose the Right SD-WAN Solution," CDW, April 23. 2020.

[3] Renee Tarun, "Secure SD-WAN Has an Important Role to Play in Financial Services," Fortinet, April 15, 2021.

[4] "SD-WAN Enables a Multi-cloud Freeway," Fortinet, August 28, 2021.

[5] Nirav Shaw, "Enabling Self-Healing SD-WAN from the WAN Edge to the Cloud Edge," Fortinet, June 22, 2021.

[6] "Google Transparency Report," Google, accessed August 22, 2021.

FORTINET®

www.fortinet.com

December 17, 2021 1:08 PM

372656-A-0-EN