Understanding SD-WAN

The growth of internet users and the shift to the cloud makes the potential for SD-WAN huge

EXCLUSIVE NETWORKS

FORTINET

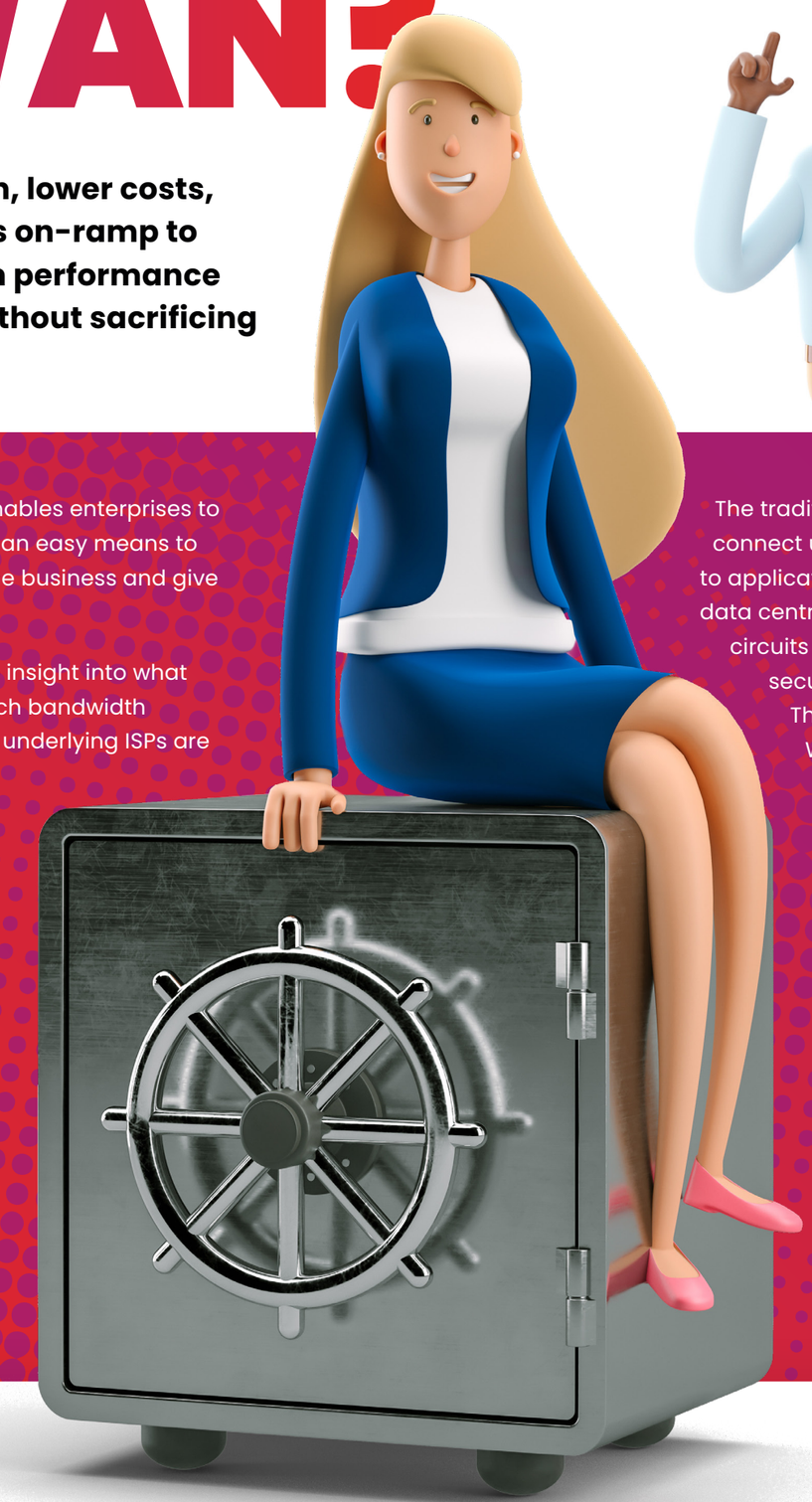
What is SD-WAN?

SD-WAN provides WAN simplification, lower costs, bandwidth efficiency and a seamless on-ramp to the cloud with significant application performance especially for critical applications without sacrificing security and data privacy.

Software Defined Wide Area Networking (SD-WAN) enables enterprises to connect multiple offices together while also allowing an easy means to prioritize which applications are most important to the business and give them priority over the network.

SD-WAN solutions also allow network admins to have insight into what types of traffic are traversing their networks, how much bandwidth individual applications are consuming and how their underlying ISPs are performing. Additionally, many SD-WAN providers have their own cloud networks which incorporate peering arrangements with other cloud and SaaS providers. This improves access and performance, and can ultimately rival the quality of traditional private WAN solutions like MPLS and point-to-point circuits.

SD-WAN is used for better security. The areas needing improvement are generally associated with proprietary backhaul connectivity services, poor network performance, and inconsistent security posture and policy management. All of which inhibit low risk adoption of cloud-based applications and other digital transformation initiatives.



The traditional WAN function was to connect users at the branch or campus to applications hosted on servers in the data centre. Typically, dedicated MPLS circuits were used to help ensure security and reliable connectivity. This has driven Software-defined WAN (SD-WAN) solutions to become increasingly popular as organizations request fast, scalable, and flexible connectivity among different network environments. They also want to lower the overall total cost of ownership (TCO) while delivering enhanced application performance. But a subpar SD-WAN approach can significantly inhibit an organization's ability to quickly adapt to changing business demands, especially if it does not offer integrated security.

What are the benefits of SD-WAN?

- **Deliver superior quality of experience at any scale**
- **Accelerate network and security convergence and simplify WAN architecture**
- **Orchestrate consistent network and security policies**
- **Achieve operational efficiencies through automation, deep analytics, and self-healing**

What is the difference between

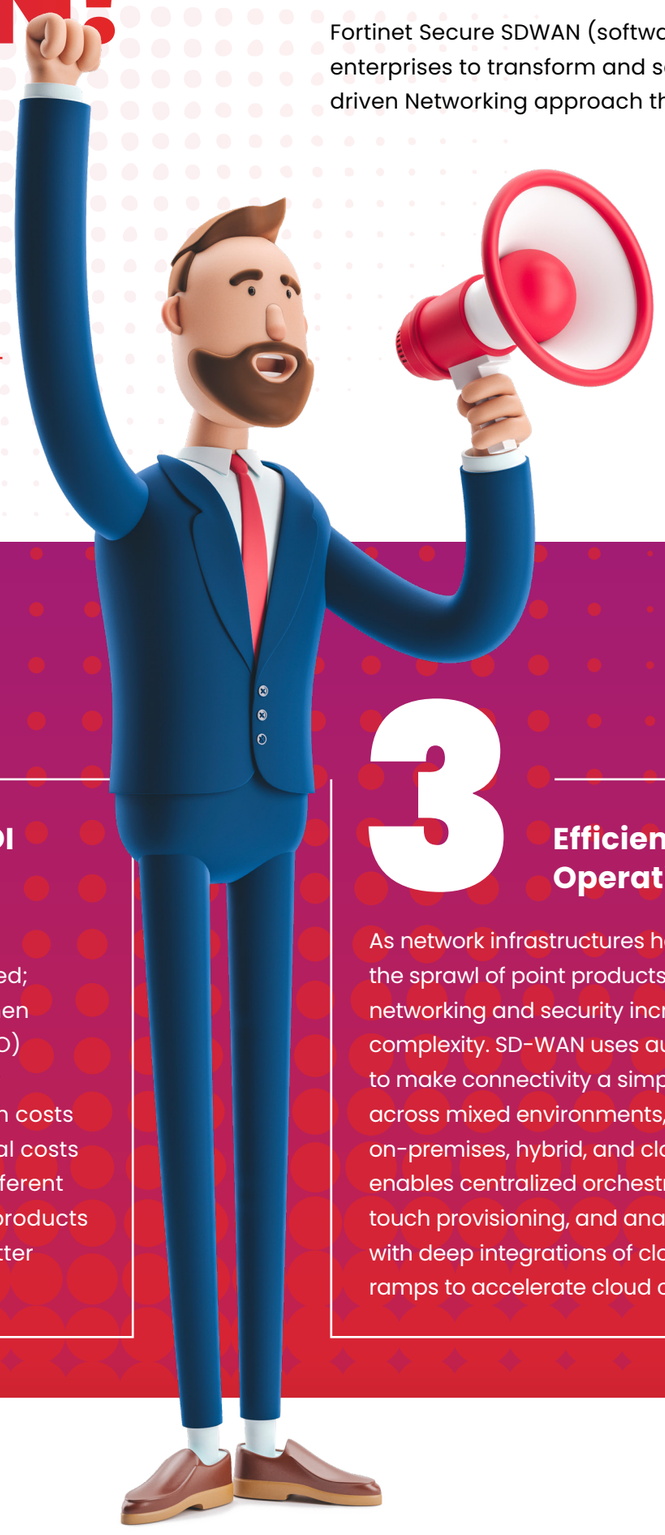
WAN & SD-WAN?

The traditional WAN (wide-area network) function was to connect users at the branch or campus to applications hosted on servers in the data centre.

SD-WAN allows remote sites to connect more easily to networks, data centers, and/or multiple-clouds with lower latency, better performance, and more reliable connectivity.

What is SD-WAN's purpose?

In a nutshell, SD-WAN is used for security.



Fortinet Secure SD-WAN Transforms and Secures WAN

Fortinet Secure SDWAN (software-defined wide-area network) solution enables enterprises to transform and secure all WAN edges. Leveraging the Security-driven Networking approach that uses one operating system and one centralized management console, enterprises realize superior user experience, enhanced security posture effectiveness with converged networking and security, and achieve operational continuity and efficiency.

WATCH THE VIDEO

But what is SD-WAN's purpose when working towards specific business outcomes?

1 Improved User Experience

SD-WAN allows remote sites to connect more easily to networks, data centers, and/or multiple-clouds with lower latency, better performance, and more reliable connectivity. When users demand more of their applications and infrastructure at unprecedented agility and scale, an appealing user experience can be make-or-break.

2 Instant ROI Benefits

MPLS and other connectivity technologies aren't just outdated; they're also more expensive when the total cost of ownership (TCO) is considered. SD-WAN not only significantly reduces bandwidth costs but can also help reduce capital costs by allowing consolidation of different point networking and security products at the edge while delivering better control and performance.

3 Efficient Operations

As network infrastructures have evolved, the sprawl of point products used for networking and security increases complexity. SD-WAN uses automation to make connectivity a simpler process across mixed environments, including on-premises, hybrid, and cloud. SD-WAN enables centralized orchestration, zero-touch provisioning, and analytics along with deep integrations of cloud on-ramps to accelerate cloud connectivity.

4 Enhanced Security Posture

An SD-WAN solution needs to have integrated security. Otherwise, it's just another connectivity option that unfortunately becomes an attack vector. When properly implemented, secure SD-WAN enables private, secure and direct internet access. It's critical that an SD-WAN solution can ensure consistent security at all edges, from flexible WAN edges to the cloud edge.

History and evolution of SD-WAN

Modern SD networking and SD-WAN technology evolved from earlier networking solutions like point-to-point (PPP) leased lines, frame relay, and MPLS. PPP was the original mode for connecting multiple local area networks (LANs) before frame relay removed the need to buy and manage individual connecting links between various corporate locations. MPLS connection made more improvements by bringing previously separate functions such as voice, video, and data networking onto the same network using Internet Protocol (IP)-based technology.

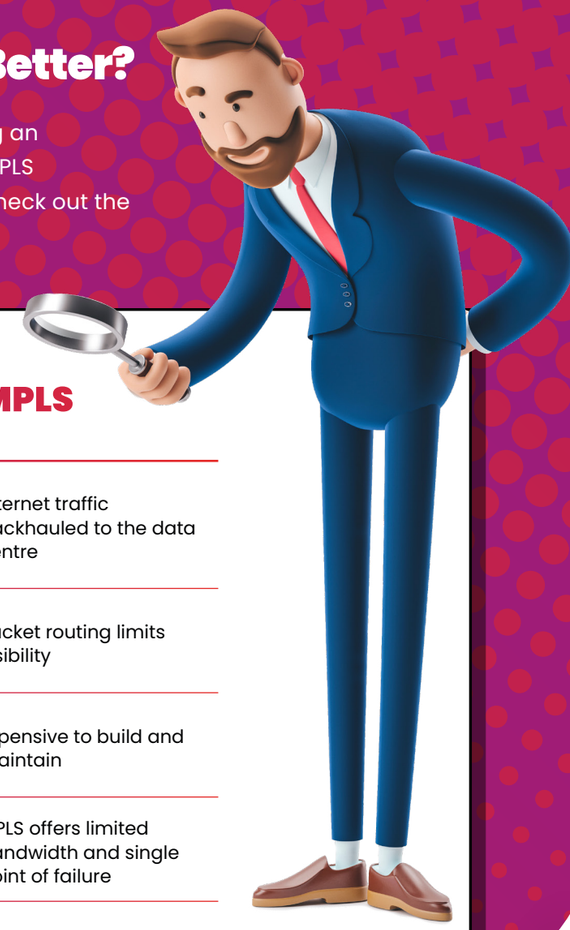
Fast-forward to the 2000s, and multiprotocol label switching (MPLS) came to popularity. MPLS soon overtook frame relay in popularity because of how it leverages Internet Protocol (IP)-based technology to bring previously separate functions such as voice, video, and data networking onto the same network. MPLS today is the most common technology in use for enterprise WANs, and is still held up for the reduced latency and quality of service (QoS) benefits it provides.

In the 2010s, specifically 2013, SD-WAN was born, and as more technologists examined SD-WAN for its benefits, they came to realize many of the same advantages SD-WAN has over MPLS, similar to how MPLS brought more advantages than frame relay. As a simple explanation, SD networks deliver MPLS-level QoS while being significantly less expensive and significantly easier to scale.

SD-WAN can handle a variety of connections and dynamically move traffic over the best transport available, and can provide both redundancy and much more capacity using lower-cost links. SD-WAN solutions are significantly cheaper than MPLS overall when time-to-installation and time-to-delivery are also considered. The best SD-WAN solutions offer zero-touch provisioning, allowing sites to be brought on quickly and not requiring networking or security experts to be on-site for installation.

SD-WAN vs. MPLS: Which is Better?

There are a handful of factors to consider before shifting an organization to an SD-WAN solution from a traditional MPLS configuration. So what is SD-WAN vs. MPLS useful for? Check out the table below to compare each option:



	SD-WAN	MPLS
Complexity	If security is not automatically built-in, teams need add-on options	Internet traffic backhauled to the data centre
Visibility	Broad application visibility	Packet routing limits visibility
Cost	Consolidated services greatly reduce TCO	Expensive to build and maintain
Performance & Availability	Enables MPLS, broadband, LTE for high-speed	MPLS offers limited bandwidth and single point of failure

Click here to explore all the benefits of SD-WAN vs.MPLS

Why is integrated SD-WAN security critical?

One of the critical requirements for SD-WAN success is fully integrated security. Without it, SD-WAN becomes just another attack vector.

A secure SD-WAN solution is explicitly designed to interoperate as a single offering, ideally with each element running on the same operating system and managed using a single-pane-of-glass interface. This ensures that transactions are all seen and inspected, and any threats or anomalous behaviors are shared between every solution for maximum protection. As part of such an integrated monitoring system, the networking and connectivity functionalities of an SD-WAN aren't just more closely associated with the security solutions installed on the platform. They're the same thing.

Deployment of security piecemeal is also unwise. Because of the dynamic nature and high scalability of SD-WAN, overlay security is not only very expensive to deploy and maintain, but often ends up with delays when reacting to connectivity changes, leaving critical connections and data vulnerable. An integrated system ensures that SD-WAN connectivity, traffic management functions, and advanced security function as a single, holistic solution.

An NGFW, whose key components include intrusion prevention (IPS), web filtering, secure sockets layer (SSL) inspection, and anti-malware, is an example of an integrated solution. Solutions that combine SD-WAN and NGFW capabilities into single offerings satisfy the key requirements for secure SD-WAN—and ensure the safety and reliability of connections and for the organization overall.

As enterprises adopt remote workforce policies, networks grow more distributed. A new networking and security strategy is required that combines network and security functions with WAN capabilities to support the dynamic, secure internet access for a "work from anywhere" global workforce. SD-WAN plays a critical role in the adoption of emerging solutions like Secure Access Service Edge (SASE) and enables flexible and consistent security across all edges.

Learn more about integrating security with SD-WAN to avoid common WAN security issues

Learn more about SD-WAN Pricing

How Fortinet can help

Fortinet's Secure SD-WAN solution delivers built-in security plus high-speed networking capabilities, ensuring organizations gain the cloud application access and performance they need along with industry-leading protection that does not compromise speed. The Fortinet Secure SD-WAN solution has been tested and validated by Gartner for high-performance, security, and low TCO. Fortinet's proven ability as a security and network leader makes it a clear choice for a complete SD-WAN solution.

- **Forrester Total Economic Impact (TEI) of Fortinet Secure SD-WAN**
- **The TEI study examines both the network and security impact on businesses.**
- **Download the report to understand the benefits of deploying Fortinet Secure SD-WAN**

Simplify Your Network and Security with Fortinet Secure SD-WAN | SD-WAN

Fortinet Secure SDWAN is foundational for seamless transition to SASE and SDBranch. It enables organizations to protect their investment and simplify operations along their journey to a Zero Trust Architecture.

WATCH THE VIDEO

2022 Gartner® Critical Capabilities for SD-WAN

Fortinet is the only vendor to rank #1 in 3 of 5 Use Cases two years in a row – "Remote Worker," "Security-sensitive WAN," and "WAN for Small Branches"

You can download the report here

EXCLUSIVE NETWORKS

FORTINET