paloalto NETWORKS | STRATA

Consistent Security with SD-WAN

Four Ways to Optimize Security from HQ to the Branch

Table of Contents

Executive Summary

Enterprise networks are experiencing an explosion of traffic due to data moving to the cloud. Heavy traffic increases the need for bandwidth and impacts costs as well as the user experience. As a result, more and more IT executives are turning to software-defined wide area networking (SD-WAN) for a fast, reliable way to connect their branch offices to the cloud. In fact, Gartner predicts that spending on SD-WAN will surpass spending on traditional branch routers by 2022.[1]

SD-WAN is a newer approach to wide area connectivity that marries software-defined networking (SDN) to WAN technology. SD-WAN separates network control and management processes from the underlying hardware, and then makes these processes available as services that enterprises can easily configure and deploy.

However, when adopting SD-WAN, decisionmakers often focus on the networking benefits, prioritizing connectivity and cost over security. This can put the network at risk. It's not simple to integrate security to an existing design if it wasn't set up to accommodate security in the first place. SD-WAN architectures incorporate direct-to-internet connections and therefore create more opportunities for attacks if traffic inspection is not in place.

This e-book serves as a guide to CIOs, CTOs, VPs of infrastructure, and network teams. We recommend four best practices when selecting and deploying SD-WAN security:

1. Ensure Consistent Security

With SD-WAN, each branch and location will access the internet directly and need security policies in place. In all cases, you need consistent security at your data center and branch offices regardless of their size or location.

2. Consolidate Connectivity and Security

Without a natively integrated solution, your IT staff needs to manage multiple solutions, which translates to more time lost and higher operating expenses.

3. Choose a Flexible Solution to Help Your Company Scale as You Embrace Digital Transformation

Select a vendor that offers a variety of SD-WAN deployment options: on the firewall, in the cloud, or through partners. The right vendor will also offer a variety of security deployment options: a physical, virtual, or hybrid approach.

4. Own Your End-to-End SD-WAN Infrastructure, Including the Middle Mile

Having a global backbone improves reliability and network performance while giving you more complete visibility and precise control.

1. "6 Critical Questions to Ask on SD-WAN," Gartner, June 6, 2018, https://www.gartner.com/en/documents/3877766/6-critical-questions-to-ask-on-sd-wan.

First Things First: WAN and SD-WAN

A wide area network connects multiple local area networks (LANs). An enterprise WAN may extend over several branch offices, cloud services, and facilities across cities or countries. A WAN based on traditional multiprotocol label switching (MPLS) uses a model in which traffic from the branch is "backhauled" to the cloud through the headquarters or a centralized data center.

There are several disadvantages to MPLS:

1. Internet is slower due to the latency added by distance and the limited bandwidth available over MPLS.
2. MPLS is expensive, especially if traffic is being backhauled.

These disadvantages impact employee productivity and user experience. With more applications moving to the cloud, it puts more strain on the bandwidth. Poor user experience can lead to frustration and low motivation.

SD-WAN is a newer approach to wide area connectivity that marries SDN to WAN technology. SD-WAN separates the network control and management processes from the underlying hardware, and then makes these processes available as software that enterprises can easily configure and deploy. SD-WAN networks manage multiple types of connections, including MPLS, broadband, and long-term evolution (LTE); support applications hosted in data centers, public clouds, private clouds, and software-as-a-service (SaaS) offerings; and route traffic over the optimal path in real time.

Which features should you consider when evaluating SD-WAN solutions?

Support for applications hosted across data centers, private and public clouds, and SaaS

A global backbone for reliable, high-performance connectivity

Reduced manual effort for network and security management

Improved user experience

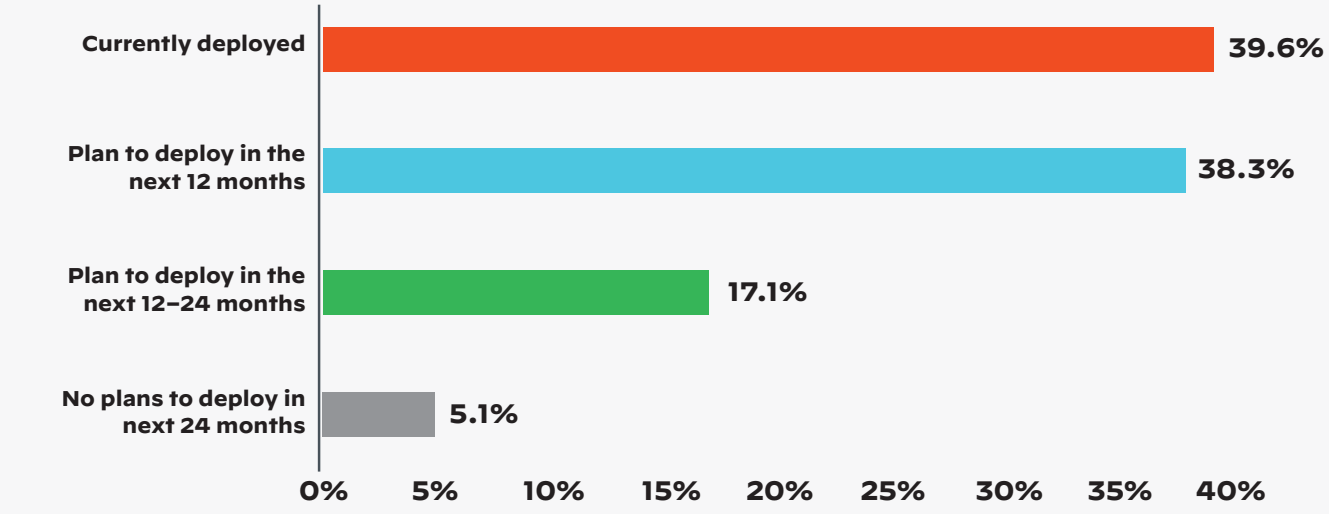
Consistent security delivered across all locations

Cost savings

Market Forces

Enterprise networks are experiencing an explosion of traffic and complexity due to data moving to the cloud. Heavy network traffic increases the need for bandwidth and impacts both costs and the user experience. IT executives are turning to SD-WAN for fast, reliable connectivity to multiple clouds and branch offices. According to IDC, nearly 95% of enterprises either currently use SD-WAN or plan to begin using it within 24 months (see figure 1).[2] Gartner predicts that "SD-WAN technology will be included in up to 75% of infrastructure refreshes by 2020" and that spend on SD-WAN products will surpass the spend on traditional routing by 2022.[3]

Q: Does your organization currently use or plan to use SD-WAN technology solutions?



n = 1,202

Source: IDC's Software-Defined WAN Survey, August 2018

Figure 1: SD-WAN usage

2. "SD-WAN: Security, Application Experience and Operational Simplicity Drive Market Growth," IDC, April 2019, https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/intelligent-wan/idc-tangible-benefits.pdf.
3. "6 Critical Questions to Ask on SD-WAN," Gartner, June 6, 2018, https://www.gartner.com/en/documents/3877766/6-critical-questions-to-ask-on-sd-wan.

The Benefits of SD-WAN

SD-WAN offers geographically distributed organizations and companies with multiple branches a number of benefits:

- **Increased flexibility and agility:** With SD-WAN, organizations have more connectivity options, such as broadband internet, which is faster to provision than MPLS. Configuring, deploying, and managing MPLS is time-consuming for most organizations. SD-WAN remediates this challenge because it separates control of the network services from transport, letting organizations use any broadband internet available in a given region without being limited to the coverage provided by the MPLS carrier.
- **Improved user experience:** Without SD-WAN, connecting branch offices to cloud applications is expensive. Traditional WANs have to "backhaul" traffic to the headquarters or corporate data center, usually over MPLS. This can lead to poor user experience. SD-WAN provides efficient access to cloud-based resources, which leads to better user collaboration, less frustration, and a better overall user experience (see figure 2).
- **Reduced cost:** SD-WAN can lead to substantial cost savings in:
  - » Acquisition of hardware, software, and support. According to Gartner, companies can save up to 40% over five years.[4]
  - » Personnel to manage, troubleshoot, and provision WAN equipment.
  - » Network expenses. Because SD-WAN supplements or substitutes expensive MPLS with broadband connectivity, traffic can be routed based on the best option for cost versus performance.

When adopting SD-WAN, however, decision-makers often prioritize connectivity and cost benefits over security. This can put your network at risk.

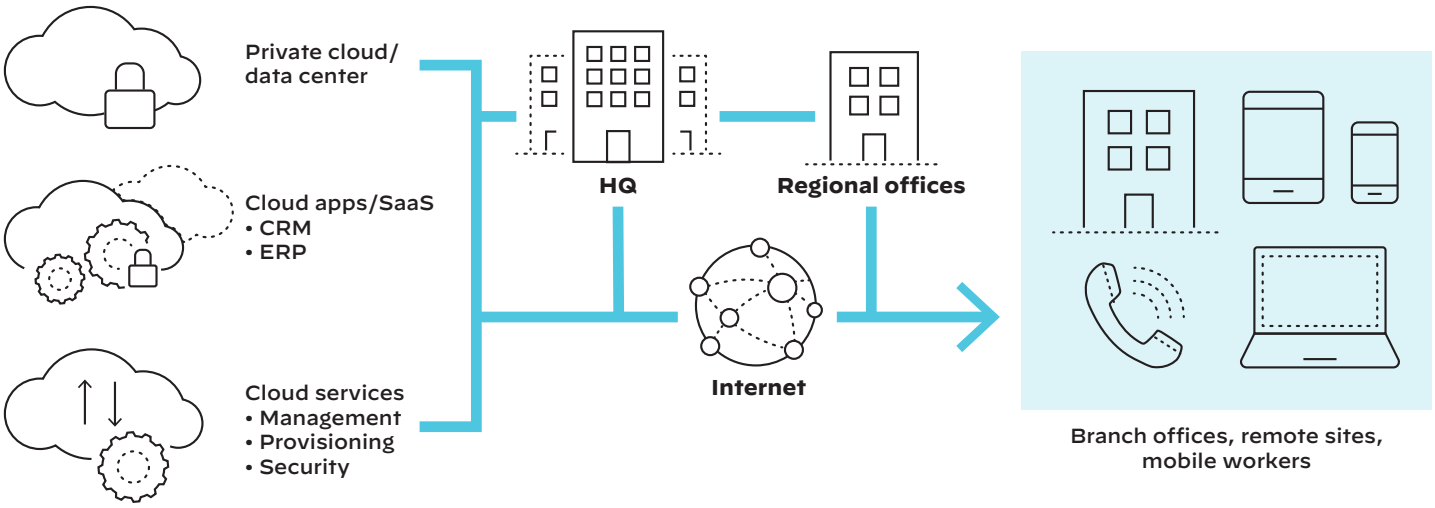


Figure 2: Efficient SD-WAN traffic routing[5]

4. Ibid.
5. "SD-WAN: Security, Application Experience and Operational Simplicity Drive Market Growth," IDC, April 2019, https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/intelligent-wan/idc-tangible-benefits.pdf.

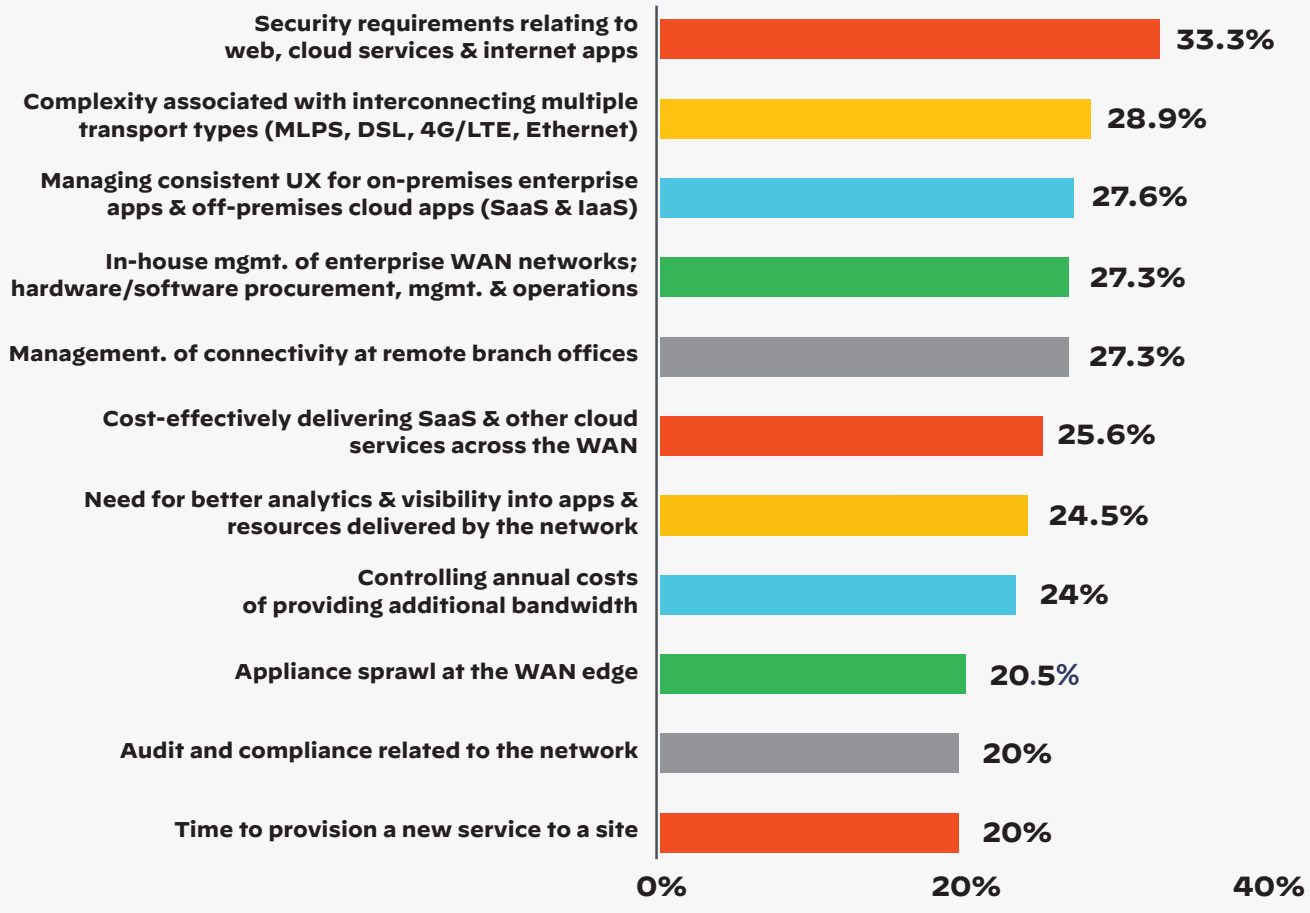
The Imperative for SD-WAN Security

According to IDC, security for web, cloud services, and internet applications are the top challenges for enterprise WAN administrators (see figure 3).[6]

In a traditional WAN that uses MPLS links, traffic from branch offices gets routed through the corporate office or data center. One of the advantages of a hub-and-spoke network is that it centralizes egress to the internet at the corporate firewall, ensuring that security policies can be defined centrally and deployed across the network.

Unlike MPLS, SD-WAN takes advantage of direct-to-internet connections, creating more egress points. However, while direct access to the internet from the branch offices improves performance, lowers total costs, and improves branch user experience, it opens up more opportunities for attacks on the corporate infrastructure.

Q: Select the three most important WAN challenges (from the following) that best relate to your company?



n = 1,202

Source: IDC's Software-Defined WAN Survey, August 2018

Figure 3: Top WAN challenges

6. Ibid.

Four Ways to Secure SD-WAN

1. Consolidate Connectivity and Security

The ultimate goal of any IT organization is to simplify. When you consolidate connectivity and security, you can reduce the IT footprint. You no longer need both a next-generation firewall appliance and a router at the branch because connectivity and security are natively integrated.

The benefits of a consolidated approach are:

- **One management console for SD-WAN and security:** Deployment and management of SD-WAN are simplified. It's easier to get started with SD-WAN and manage both the network and security in one interface.
- **Quick, cost-effective branch deployment:** Deploying, configuring, and managing new branch offices is quicker, easier, and more cost-effective.

2. Choose a Flexible Solution

Flexibility is important on two fronts: deployment flexibility and secure digital transformation.

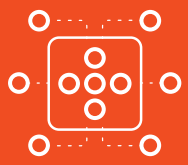
Flexibility of Deployment

Each company has its own SD-WAN security deployment requirements. Some prefer a cloud-first architecture; others prefer an on-premises deployment. More and more frequently, companies prefer a hybrid approach so that critical applications in the data center are accessible through MPLS while other data in SaaS applications can be accessed via broadband internet.

A flexible SD-WAN security solution can be deployed on the next-generation firewall, in the cloud, or on both, with one or more vendors. Managing one vendor, one appliance, and one management console is simpler, but having the option to choose is invaluable.

Best Practices for Secure SD-WAN Deployment

1 Consolidate connectivity and security



2 Choose a flexible solution

3 Control middle-mile connectivity

4 Ensure consistent security

Secure Digital Transformation

As businesses scale and begin to leverage the cloud more heavily, branch users will demand more bandwidth. With branches having the same access to your critical data and applications as your headquarters, it's important to have flexible security that can scale with your business growth. This means it's crucial to partner with the right vendor.

3. Control the Middle Mile

The "middle mile" is the path data travels from a cloud-based application to a user's device in a branch office. Many SD-WAN security vendors don't offer middle-mile connectivity, forcing you to either take your chances on the less secure and more congested public internet or hire a service provider.

When selecting security vendors, it is important to maintain control of the end-to-end infrastructure, including the middle mile, for three reasons:

- **Improved security:** You can arm your network with the same level of security as that of a private MPLS network.
- **Network performance:** Having your own private backbone ensures superior performance over that of the public internet.
- **Visibility and control of your own end-to-end infrastructure:** You can see who and which device is accessing your company's data, applications, and services.

4. Ensure Consistent Security

Palo Alto Networks offers secure SD-WAN for branches. Our native integration of SD-WAN and security simplifies operations and extends uniform protection from the data center and cloud all the way to the branches. Our global, cloud native backbone enables high-performance connectivity while providing superior visibility and precise control of your network.

Glossary

LAN: Local area network. A computer network that connects computers in a relatively small area, such as an office building, warehouse, or residence.

LTE: Long-term evolution. A type of 4G that provides fast connectivity for mobile internet use.

MPLS: Multiprotocol label switching. A technique developed in the late 1990s as an alternative to IP routing. MPLS speeds up traffic across a wide area network by allowing most data packets to be forwarded to the switching level rather than the routing level.

SDN: Software-defined network. An approach to network management that allows the network to be controlled intelligently through software.

SD-WAN: Software-defined wide area network. A newer approach to wide area networking that separates the network control and management processes from the underlying hardware, and makes them available as software.

WAN: Wide area network. A computer network that spans a wide geographic area and may connect multiple local area networks.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit **www.paloaltonetworks.com**.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com