LEARNING MADE EASY

Zero Trust Branch with SD-WAN

for dummies®
A Wiley Brand

Palo Alto Networks Edition

As enterprises expand globally, the resources required to set up and manage branch networks can be a drain on staffing, operations and budget. This new reality needs a software-defined wide area network (SD-WAN) — a revolutionary architecture that provides connectivity at the branch without the hassle and cost of point products and multiple site visits.

In this brief, you discover how SD-WAN provides a foundational component of secure access service edge (SASE) and securely enables the branch of the future.

Modern Challenges for Branch Locations

For more than two decades, organizations have relied on legacy WAN architectures to connect branch locations to a centralized corporate data center to form a single interconnected enterprise. More recently, three important trends have fundamentally changed how we work, creating new challenges for enterprise network and security teams:

- **SaaS adoption has accelerated.** Organizations are struggling to deliver the best user experience for these applications, which are increasingly used for productivity and collaboration. SaaS applications have more dynamic content with application protocols, ports, and server Internet Protocol (IP) addresses constantly evolving, making it challenging to optimize

application brownouts and degradation with traditional techniques. They're distributed and increasingly hosted across multiple cloud platforms, making it difficult to provide connectivity based on availability, performance, and geolocations. Palo Alto Networks research shows that 90 percent of end-to-end latency occurs at the application server level for Software as a Service (SaaS) applications [source: Palo Alto Networks].

- **Security threats have increased in speed, sophistication, and scale while the threat surface has expanded with artificial intelligence (AI) and device proliferation.** The number of devices and the usage of AI applications has exploded at branch locations. Internet of Things (IoT) devices have been added to enable tracking and monitoring, and now branch operations have been open to inherent vulnerabilities. A research study by Palo Alto Networks with Starfleet found that 81 percent of organizations have experienced an IoT-focused attack in the last 12 months. The rapid usage of unsanctioned generative AI (GenAI) applications by branch users has led to more sophisticated threats.
- **Organizations are increasingly experiencing outages and the number-one cause is the complexity of their networks.** Deploying point products has increased the hardware footprint, user interfaces (UIs), and fragmented data in the branch. This has resulted in operational complexity, longer troubleshooting and resolution times, and more outages. This complexity particularly creates more challenges for branches when mergers and acquisitions (M&As) take place, which many enterprises widely use to grow their businesses. In fact, according to Gartner, 70 percent of M&As fail due to integration issues.

The implications of these three trends for legacy WAN architectures are profound. Backhauling (or hairpinning) branch office traffic bound for the internet or the cloud through a headend router and perimeter firewall in a centralized, on-premises data center

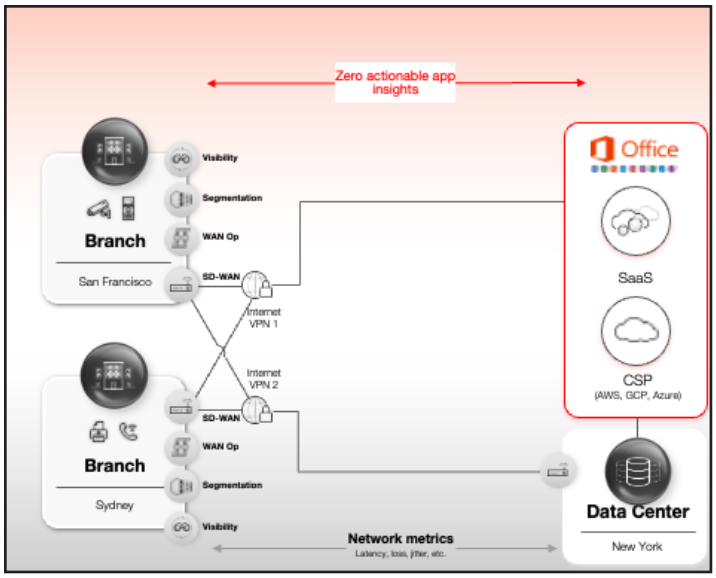

Figure 1: Backhauling branch office traffic through a data center is costly and inefficient and creates a poor user experience.

(see Figure 1) is costly and inefficient and creates a poor user experience due to latency and congestion.

Early (Gen 1) SD-WAN products tried to overcome some of these challenges by adding dedicated internet access (DIA) links at branch locations to offload

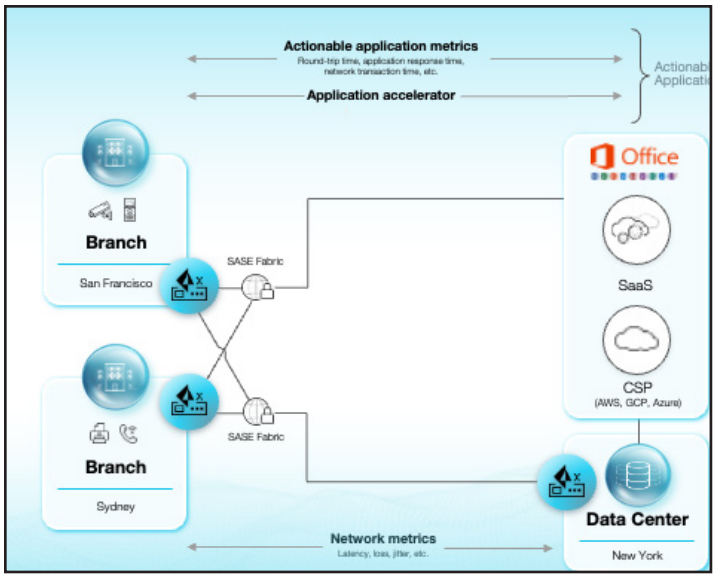

Figure 2: Gen 1 SD-WAN solutions provided direct access to Internet, cloud, and SaaS apps.

internet- and cloud-bound traffic from the private Multiprotocol Label Switching (MPLS) WAN (see Figure 2).

However, these Gen 1 SD-WAN products created new challenges for branch office users directly accessing apps, including the following:

- **Most SD-WAN solutions mandate an SD-WAN appliance at their branches, data centers and cloud to intelligently steer traffic based on service-level agreements (SLAs).** Unfortunately, they can't implement a similar architecture for SaaS applications that are distributed and hosted across multi-cloud, making them unsuitable for delivering performance for SaaS applications. Additionally, SaaS applications' dynamic content can't be optimized by traditional caching mechanisms, which don't consider the context of users' application access.
- **Most SD-WAN solutions fail to provide real-time detection and protection from sophisticated threats that come with adopting AI apps that significantly increase the attack surface.** They fail to provide real-time visibility into AI apps to learn exactly which AI apps

are being used, by whom, and for what purpose to ensure there are no blind spots. They can't provide complete visibility of devices including IoT limiting the ability to segment, isolate, and protect devices regardless of the vendor or operating system.

- **Most SD-WAN solutions offer fragmented products for their SD-WAN, segmentation, application optimization and visibility.** They leverage disparate UIs with fragmented visibility, forcing IT teams to correlate events across notifications to root cause analysis, increasing troubleshooting time significantly. They offer separate data for these tools, limiting the ability to use AI/machine learning (ML) to automate remediation, resulting in longer resolution cycles.

For SD-WAN, organizations need a networking solution that delivers the foundational capabilities for all applications by providing a direct-to-app access, while also ensuring application assurance. Additionally, organizations need integrated and cloud-delivered security services that are delivered to branch offices to enforce true least-privilege access. This ensures only the right people get access to the right information and assets and also provides visibility to all your assets. These solutions should leverage the latest innovations in observability and telemetry with the power of AI/ML to help customers automate complex IT operations and reduce mean time to resolution (MTTR).

REMEMBER

SD-WAN is a foundational component of SASE, which integrates networking and security services into a unified, cloud-delivered solution that reliably and securely connects branch users to the internet, public cloud, SaaS apps, and corporate data center resources.

What Is SASE?

SASE is built on a modular platform that allows organizations to quickly modernize their branch locations with core SD-WAN services and incrementally add new networking and security functionality (see Figure 3) over time, such as:

- Networking
  - **Virtual private networks (VPNs)**
  - **Quality of service (QoS)**
  - **SaaS acceleration**
  - **Application acceleration**

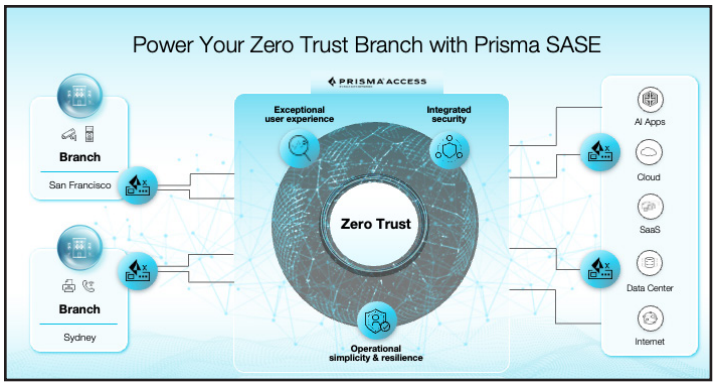

Figure 3: SASE delivers advanced network and security capabilities in a converged cloud-delivered solution.

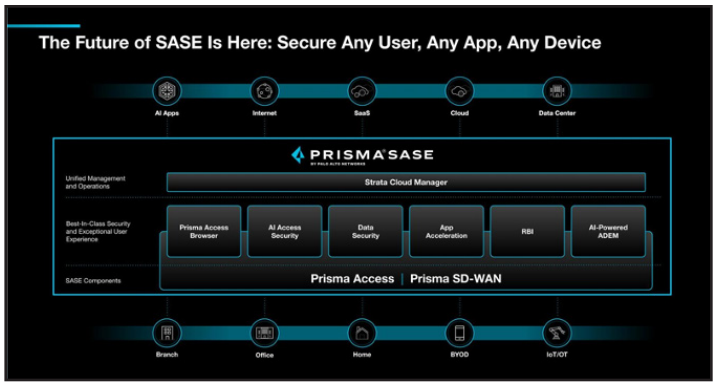

Figure 4: The four tenets of SD-WAN.

- **Security**
  - **Firewall as a service (FWaaS)**
  - **Zero Trust network access (ZTNA)**
  - **Cloud access security broker (CASB)**
  - **Cloud secure web gateway (Cloud SWG)**
  - **Data loss prevention (DLP)**
  - **Domain Name System (DNS) security**
  - **Threat prevention**
  - **Enterprise browser**
- **Autonomous digital experience management (ADEM)**
  - **Deep observability**
  - **AI-powered operations**

SD-WAN for Zero Trust Branch

To address the inherent limitations of Gen 1 SD-WAN products, a SD-WAN, combined with SASE, should adhere to the following three design tenets (see Figure 4):

- **Exceptional user experience:** SD-WAN should deliver an application assurance framework that measures, enforces, and alerts IT administrators about application performance. The foundational SD-WAN capabilities such as measuring SLAs, traffic failover, and load balancing should extend to security service edge (SSE) and leverage SSEs' distributed and global hyperscale architecture to optimize application performance at the middle mile.

TIP

Prisma SD-WAN natively delivers application acceleration to improve application performance by up to 5x. Unlike traditional caching mechanisms, application acceleration uses a context-based approach to application traffic per user to optimize performance better.

- **Integrated Security:** SD-WAN must deliver Zero Trust security with accurate user, applications, and device visibility, including IoT and precision AI. By connecting seamlessly with a globally distributed cloud-delivered SSE with low-latency connections, organizations have access to capabilities including FWaaS, CASB, SWG, and IoT security to ensure Zero Trust at all times. This provide visibility to all your assets, including the rapidly growing IoT devices to ensure you can apply the proper controls and policies to the entire network.
- **Operational resiliency and simplicity:** Lastly, a SD-WAN requires branch simplicity with easy onboarding, comprehensive visibility and segment-wise insights that provide ease of troubleshooting, resolution, and zero routing complexity. Gain visibility into traffic forwarding and remediation decisions to help IT administrators understand and troubleshoot performance issues. With digital experience management, IT admins have end-to-end visibility and segment-wise insights into user experience from user to branches to WAN circuits to SSE nodes to applications for easy troubleshooting and root cause analysis.

Prisma SD-WAN with SASE powers the Zero Trust branch by providing exceptional user experience, simplifying IT operations, and improving security outcomes.

TIP

Check out the following resources from Palo Alto Networks to help you transform your branch locations with SD-WAN:

- E-book: Download *SASE For Dummies*, Palo Alto Networks 2nd Special Edition.
- Web page: Visit the Prisma SD-WAN web page.
- Test drive: Take the SD-WAN Ultimate Test Drive.
- E-book: Read the Palo Alto ebook *The Power of Zero Trust Branch* to learn why branch evolution demands SD-WAN innovation.
- Contact Palo Alto Networks: Connect with the Palo Alto team of SASE and SD-WAN experts today.

paloalto® NETWORKS

 ISBN: 9781394352838