Brought to you by

cisco SECURE

# Secure Access Service Edge (SASE)

for dummies®
A Wiley Brand

2nd Cisco Special Edition

Explore SASE networking

Extend cloud-native security everywhere

Reduce cost and complexity

Lawrence Miller

## About Cisco

Cisco has long established itself as the networking leader, while building an open, integrated portfolio of cybersecurity solutions along the way. Cisco Secure is built on the principle of better security, not more. We deliver a streamlined, customer-centric approach to security that ensures it's easy to deploy, easy to manage, and easy to use – and it all works together to increase your resilience. Because people and our customers are at the heart of what we do, Cisco Secure empowers the security community with the reliability and confidence that they're safe from threats now and in the future.

We help 100 percent of the Fortune 100 companies protect what's now and what's next with the most comprehensive, integrated cybersecurity platform on the planet. Learn more about how we simplify experiences, accelerate success, and protect futures at cisco.com/go/secure.

# Secure Access Service Edge (SASE)

2nd Cisco Special Edition

**by Lawrence Miller**

for dummies®
A Wiley Brand

# Secure Access Service Edge (SASE) For Dummies®, 2nd Cisco Special Edition

Published by
**John Wiley & Sons, Inc.**
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com



ISBN 978-1-394-19353-0 (pbk); ISBN 978-1-394-19354-7 (ebk)

## Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

**Project Manager:** Jen Bingham
**Acquisitions Editor:** Traci Martin
**Editorial Manager:** Rev Mengle
**Sales Manager:** Molly Daugherty
**Content Refinement Specialist:** Saikarthick Kumarasamy

# Introduction

Today's IT teams face a common challenge: how to securely connect and enable the growing universe of roaming users, devices, and software as a service (SaaS) apps without adding complexity or degrading end-user performance. Likewise, users in remote and branch offices expect the same user experience and level of network performance and security as users in central locations. IT must develop strategies to connect and protect users — wherever they work and on any device they use — from a variety of threats, including malware infections, command-and-control callbacks, phishing attacks, unauthorized access, and unacceptable use, among others.

This ebook delves into the dynamically changing network and security landscape. These changes are paving the way to a new solution category that delivers software-defined connectivity and multiple security functions from the cloud that are simple, scalable, and flexible to meet the unique needs of your business and its changing network architecture.

The goal of this ebook is to help you gain a deep understanding of the latest trends, the new challenges they bring, and how technologies have evolved to address them. Finally, the ebook introduces you to a new product category that has emerged to help solve these problems and shows how Cisco's approach can help your business today and in the future.

## About This Book

This book comprises six chapters that explore:

- Key networking and security trends and their associated challenges (Chapter 1)
- Different networking and security options and key considerations (Chapter 2)
- How an SD-WAN architecture addresses modern networking challenges (Chapter 3)

- How a multifunction, cloud-native security service complements SD-WAN security components and addresses today's security challenges (Chapter 4)
- The Cisco approach to SASE (Chapter 5)
- Key SD-WAN and cloud security takeaways (Chapter 6)

Each chapter is written to stand on its own, so if a topic piques your interest, feel free to jump ahead to that chapter. You can read this ebook in any order that suits you (though we don't recommend upside down or backwards).

## Icons Used in This eBook

Throughout this ebook, you will find special icons to call attention to important information. Here's what to expect:


REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays!


TECHNICAL STUFF

If you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon and is the stuff nerds are made of!


TIP

Tips are appreciated, never expected — hopefully, you'll appreciate these useful nuggets of information.


WARNING

These alerts point out the stuff your mother warned you about (well, probably not), but they do offer practical advice to help you avoid potentially costly or frustrating mistakes.

## Beyond the eBook

There's only so much information that can fit in 48 short pages, so if you find yourself at the end of this ebook thinking, "Gosh, this was an amazing ebook; where can I learn more?" check out `https://www.cisco.com/site/us/en/solutions/secure-access-service-edge-sase/index.html`.

IN THIS CHAPTER

- Considering how networking and security have changed
- Addressing modern network and security challenges

# Chapter 1
# Networking and Security: Evolution and Challenges

The enterprise network underwent a huge transformation over the past decade. As a result, security products are evolving, too. The market is moving from single-purpose, point products to multifunction security solutions tightly integrated in a cloud service offering. The goal is simple: to deploy security services how and where you choose with the capability to control and secure direct-to-Internet access, cloud applications, Internet of Things (IoT), and central, remote, and roaming users alike — without the need for additional hardware.

This chapter discusses modern trends and challenges that drive the need for a new approach to networking and security.

## The Way We Work Has Changed

Several key trends have reshaped the networking and security landscape.

## Cloud adoption

The transition to cloud and software as a service (SaaS) continues to accelerate as organizations seek to be more agile and resilient in the face of heightened disruption and uncertainty.

TIP

The growth of enterprise cloud adoption, particularly hybrid cloud and multicloud strategies, is highlighted in Cisco's 2023 *Global Networking Trends Report*. The study found that 67 percent of organizations already have more than 40 percent of their workloads in multiple clouds, with 92 percent using more than two cloud providers, and 69 percent using more than five SaaS providers.

## Remote offices

The days of employees working together in the same place — company headquarters — are long gone. As organizations expand into new markets, acquiring smaller companies and their office footprints, the number of remote and branch offices grows, too. Remote office employees need to be protected as well as their counterparts at main office locations, even if their network traffic is going directly to the Internet instead of backhauling it to the corporate data center.

REMEMBER

A remote or branch office is a dedicated business (non-home) site that has more than one employee. This location may be connected to a central data center via a wide-area network (WAN) or may connect directly to the Internet. Remote and branch offices typically receive some level of technology support from headquarters locations and most (although not all) typically have one or more on-site servers to provide users with file, print, and other IT services.

Some remote office locations may be connected to a main office over a multiprotocol label switching (MPLS) WAN link. However, it is common for remote offices to connect to the main office over a virtual private network (VPN), and a secondary direct Internet access (DIA) link may serve as a backup to the primary MPLS link. Additionally, remote offices may use DIA links — going directly to the Internet and bypassing the VPN — which can create security gaps if not properly managed with the right set of security functions.

TIP

As companies become more decentralized, the growing population of remote workers and branch offices needs a new approach to networking and security.

## Roaming users

Laptop computers have supplanted desktop computers to become the primary endpoint for many business users. Similarly, mobile computing has untethered workers as mobile devices have become more powerful than many desktop computers and their use has proliferated. Because of these technology trends, many forms of work can now be performed from practically anywhere, and organizations increasingly recognize that work is an activity, not a place. According to IDC's *Hybrid Work Maturity Study* conducted with Cisco, 45 percent of business and technology leaders view remote and hybrid work models as an embedded part of accepted work practices, with 93 percent planning to maintain or increase spending in this area. However, The Cybersecurity Insiders 2022 *Security Visibility Report* warns that the shift to remote work (and the associated risks) is the second-biggest security challenge cited by respondents (47 percent), surpassed only by ransomware (53 percent).

REMEMBER

A *roaming user* is any employee that works from a home office or from another noncorporate location (such as at a customer's office or on the road). Roaming users may use corporate-owned devices and/or personal devices, accessing the corporate network via a VPN or connecting directly to the Internet to access cloud applications in order to perform their job functions.

## More network traffic

New apps, including public cloud storage and video conferencing, are data-intensive and generate large amounts of network traffic to support the increasing demand from employees. This increased traffic load is putting an ever-greater strain on existing network infrastructure and centralized security processes. This increased strain can reduce performance, lower productivity, and hinder the overall user experience.

# Understanding Networking and Security Challenges

This past decade has also presented many new networking and security challenges requiring innovative solutions to address them effectively.

## Rising costs of traditional networking architecture

The traditional function of a WAN was to connect users at the branch or campus to applications hosted on servers in a centralized data center. Typically, dedicated MPLS circuits helped ensure security and reliable connectivity. However, these dedicated circuits are costly to provision and maintain, especially when compared to the widespread availability of other, less costly transport options available to businesses today.


MPLS is a routing transport that provides high-availability and performance, reduces load on routers, and speeds up traffic delivery. MPLS provides more reliable quality-of-service (QoS) for bandwidth-heavy or latency-sensitive applications. MPLS technologies are applicable to any network layer protocol (hence the name, "multiprotocol") and are often used by enterprises, for example, to backhaul business-critical network traffic from branch offices to the data center.

## Inefficiencies in the centralized network model

A centralized network model made sense when the enterprise data center was the primary destination for users to access applications and data across the network. Internet traffic was relatively insignificant and could easily be handled over the existing MPLS circuits. Network traffic could be routed and prioritized as necessary to ensure efficient, reliable performance — while limited and expensive IT staff resources such as networking and security teams could centrally manage the network for all locations.

Traditionally, an organization would backhaul (that is, reroute) network traffic from branch offices to headquarters to apply security policies, often using MPLS links. But in the digital era,

this approach just isn't efficient. As businesses increasingly adopt SaaS applications, as well as platform as a service (PaaS) and IaaS resources and workloads delivered from multiple clouds, the user application experience has suffered. Backhauling Internet-bound traffic to apply security policies at the data center can be slow and isn't an efficient or effective way to handle the unprecedented explosion of Internet traffic that cloud adoption brings.


Traffic destined for the Internet is effectively backhauled across the MPLS network to a headend (such as a corporate headquarters or data center) that directs it through a set of security checks and then provides Internet access — but unfortunately, it also acts as a bottleneck.


Existing WAN links that backhaul traffic to a security stack in a central location using MPLS are unable to handle increasing bandwidth demands from users who need fast, reliable access to the Internet. To address the growing need for DIA to cloud-based apps, many organizations are either investigating, or already using, broadband DIA at branch locations instead of backhauling this traffic over MPLS. TeleGeography, a global telecommunications market research and consulting firm, reported in its 2021 *WAN Manager* survey that DIA is gaining ground on MPLS, with 42 percent of sites using DIA in 2021. Although these DIA links address performance issues associated with backhauling traffic to a headend location, they're often provided by local Internet service providers (ISPs) as broadband links. It's important to check into resiliency, quality of service (QoS) prioritization, and service level agreement (SLA) guarantees.

## Performance issues with "run-the-business" SaaS apps

Many SaaS apps today, like Salesforce, Microsoft 365, and Workday (to name a few) have become core "run-the-business" enterprise apps. Backhauling SaaS traffic to a corporate headend creates network congestion and latency. This, in turn, causes performance issues that result in lost productivity and user frustration. Complexity in the WAN may cause additional performance issues due to less-than-optimal routing decisions, improper traffic classification and prioritization, and inefficient policy enforcement.

TECHNICAL STUFF

Modern SaaS applications are often built on a microservices architecture that can be comprised of hundreds, or even thousands, of microservices spanning multiple cloud locations. Each of these microservices has the potential to add latency as data travels back and forth between them and the application.

When users experience performance issues with corporate-approved apps, they often turn to unauthorized and potentially risky apps to get their jobs done. This shadow IT culture in which the IT department — and security controls — are circumvented is a big problem. According to a survey conducted by Beezy.net, 32 percent of employees use shadow IT such as unapproved communication and collaboration tools to perform work. More than 1,200 cloud services are used in the average large enterprise today, and the Enterprise Strategy Group reports that as much as 98 percent of those services are unsanctioned and unvetted SaaS apps.

## Too many siloed IT tools and integration challenges

IT teams are frequently inundated by mountains of data from stand-alone, point connectivity, and security products that don't integrate with other products and require different knowledge levels and skill sets to operate and maintain. The Panaseer 2022 *Security Leaders Peer Report* found that enterprise security teams use an average of 76 different security tools, and Cisco research indicates that the majority of them find it challenging to orchestrate alerts from these different tools. This lack of integration and interoperability makes it difficult, if not impossible, for IT personnel to manage the network and monitor and correlate security and threat information in realtime.

REMEMBER

These challenges have grown exponentially as connected branch and remote offices have proliferated. Each location typically requires a router and firewall at minimum. In remote and branch locations these are often purchased as commodity components that provide limited functionality and remote management capabilities. When implementing DIA at remote locations, there is a need to deliver the right level of security to users — web security, firewalls, data loss prevention, and so on. However, it may not be practical and cost-effective to buy a separate stack of security appliances for each location. Even if some of these components in

branch locations do include security tools, there are usually no IT personnel in these locations to maintain them. To improve security of these dynamic environments, security measures will need to be shifted to the cloud where they can be applied and managed centrally.

## Security talent shortage and increasing personnel costs

The worldwide shortage of security professionals and the high ongoing investment necessary to train and retain qualified security staff is a very real problem for organizations everywhere. Forbes.com reported that at the end of the first quarter of 2022, 3.5 million cybersecurity positions remained open worldwide.

## New cyberthreats taking advantage of security gaps

Advanced cyberthreats, including ransomware, remote access trojans (RATs), and advanced persistent threats (APTs), have evolved to take advantage of the lack of visibility and control in the modern hyper-distributed network. Remote and branch users are particularly susceptible to many of these threats because organizations have moved away from a centralized security model and are often unable to enforce consistent security policies across the network. Limited security capabilities and IT staff in remote locations make these users even more susceptible to a successful breach or attack. Cybercriminals understand that remote workers are typically more vulnerable and thus target remote locations and roaming users.

WARNING

According to the Enterprise Strategy Group, 68 percent of organizations experienced attacks in the last 12 months in which a branch location or roaming user was the source of compromise.

TIP

Modern organizations need to consider innovative networking and security options to successfully address the challenges in today's enterprise network. You can find more information on this in Chapter 2.

IN THIS CHAPTER

- Using MPLS where needed
- Getting innovative with SD-WAN
- Addressing security threats with SWGs and SIGs
- Introducing the secure access service edge (SASE)

# Chapter 2
# The Evolution of Networking and Security Solutions

The networking and security landscape is evolving from numerous, disparate point solutions to fully integrated, multifunction, cloud-delivered networking and security platforms. This shift is happening because businesses increasingly need the flexibility and power to deploy networking and security services how and where they choose. They need to control and secure Internet access, manage the use of cloud applications, and provide protection for roaming users while reducing strain on resources and eliminating the need for hardware.

In this chapter, you learn how networking and security evolved from traditional wide area networks (WAN) to software-defined WAN (SD-WAN) and from secure web gateway (SWG) appliances to cloud-based SWGs or multifunction cloud-native security services. There is also information about the new, combined concept of the secure access service edge (SASE).

# Looking at Traditional WAN Technologies

For nearly two decades, the go-to WAN technology for IT, voice, and data networking infrastructure has been multiprotocol label switching (MPLS) network architectures. MPLS networks provide a resilient network backbone for connecting enterprise headquarters and remote branch locations. MPLS provides the capability to prioritize voice, video, and data traffic on your network to meet unique business requirements, and packets can be sent over a private MPLS network.

However, MPLS circuits come with a higher cost than other transports, and enterprises today need to evaluate where these more expensive circuits should be utilized when needed. MPLS networks are typically provided by Internet service providers (ISPs) and other service providers — both the well-known telecoms and the not so well-known smaller companies. For many companies, lower cost Internet circuits will be sufficient for the majority of network traffic.

Many organizations inevitably install a secondary direct Internet access (DIA) link at their branch locations to offload some of this Internet traffic. Such a solution increases recurring costs and introduces still more complexity. Network traffic may not necessarily be routed across the best link at a given time, and bandwidth on one link or the other may be underutilized.

On the security side, Internet-bound traffic needs to be minimally secured by DNS-layer security or a firewall, but it may also require web content filtering, data loss prevention, real-time malware detection, and other security services. The lack of visibility and a centralized policy enforcement point make it difficult, if not impossible, for security teams to ensure a secure and compliant operating environment (see Figure 2-1).

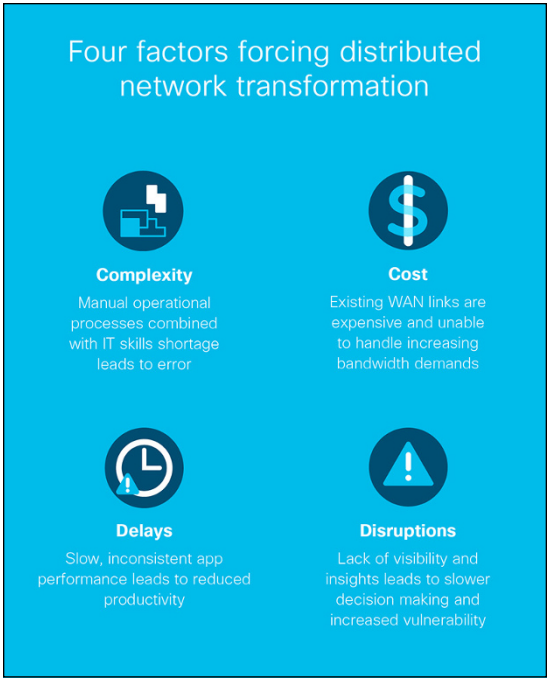



**FIGURE 2-1:** Challenges with current WAN architectures include complexity, cost, delays, and disruptions.

# Exploring SD-WAN Solutions

In a traditional WAN, an organization would need to provision an MPLS uplink from a carrier. Since configuration is done at the physical router, this means a networking team needs to "roll the truck" to the site in order to configure policies on the device itself. The ongoing life-cycle management for these devices is also cumbersome due to the need to physically go to the site for troubleshooting and maintenance.

With the speed of business today and the increasingly distributed enterprise, this inflexibility of a traditional WAN to scale up and down has led to a surge in the adoption of SD-WAN. Simply put, SD-WAN uses software to manage the WAN. The software allows networking teams to manage and automate the connectivity,

configurations, and policies across all users, transports, devices, applications, clouds, and data centers in multiple locations from a centralized dashboard. In addition, it empowers networking and security teams with advanced intelligence and analytics that help resolve or prevent issues before they impact the user experience.

In many WAN architectures using simple load balancing, available bandwidth capacity may go unused during periods of congestion. For example, your broadband Internet connection may be running slowly during a given period of time, while your MPLS link is relatively uncongested and may actually be able to provide faster Internet connectivity despite backhauling Internet-bound traffic to a centralized security control point. The inability to aggregate disparate links means wasted bandwidth capacity and lower employee satisfaction.


TIP

An SD-WAN solution can address these scenarios and provide other advanced routing capabilities to optimize your network traffic as needed. Additional considerations and capabilities include:

- Routing traffic across different links based on destination and/or cost
- Addressing the explosion of remote workers (the "branch of one") with flexible routing and traffic management options
- Meeting rapidly changing business needs with the capability to quickly build up and tear down branch locations
- Aggregating multiple links to provide greater total bandwidth
- Rerouting traffic across an alternate link when a link is congested, unstable, or down
- Prioritizing certain application traffic, such as voice and video, to ensure quality of service

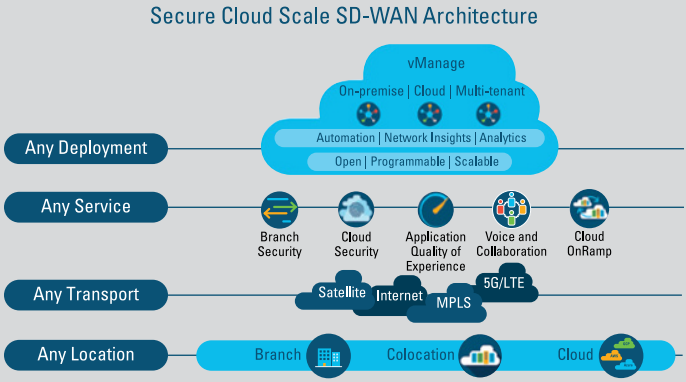
SD-WAN combines and optimizes WAN technologies such as MPLS and broadband Internet connections. This allows organizations to efficiently route network traffic to multiple remote branch locations while providing enhanced monitoring and management capabilities. SD-WAN monitors network traffic across all available links in real time and dynamically selects the best route for each data packet traversing the network.

In addition to its routing capabilities, SD-WAN also provides several other benefits such as improved security, reduced costs, and greater flexibility.

## CISCO SD-WAN EXAMPLE

Cisco SD-WAN connects any user to any application with integrated capabilities for multicloud, security, predictive operations, and enhanced network visibility — all on a SASE-enabled architecture (see the figure below). Cisco SD-WAN supports

- **Any deployment:** Flexible WAN management for on-premises, cloud, and multitenant environments.
- **Any service:** A full suite of services including branch security, cloud security, application quality of experience, voice and collaboration, and cloud on-ramp.
- **Any transport:** Deploy your WAN over any type of connection including satellite, Internet, MPLS, and 5G/Long-Term Evolution (LTE).
- **Any location:** Physical or virtual platforms are available for branch, colocation, and cloud.




*Source: Cisco.*

## Tackling Internet Security Threats

For most of the past 25 years, network security has focused on detecting and preventing malware threats (such as viruses, ransomware, spam, and phishing), identifying and blocking unauthorized Internet use (such as browsing inappropriate content and downloading pirated content), and assuring network performance (with caching proxy and anti-distributed denial-of-service (DDoS) products).

REMEMBER

Back in 2017, several vendors and analysts in the industry defined a new concept — the secure Internet gateway (SIG). While the SWG is designed mainly for web traffic, this new type of cloud-native solution would offer multiple functions across more traffic types — such as domain name system (DNS) security, SWG, firewall as a service (FWaaS), and cloud access security broker (CASB) — to improve security and performance while reducing costs and maintenance tasks. The term *SIG* is less commonly used now, but the concept of providing a broad set of security from the cloud so organizations can protect users no matter where they work has consistently gained traction. It can easily scale to cover additional traffic and users more efficiently than the older on-premises SWG appliance approach.

## SASE: Combining Network Connectivity with Cloud Security

In 2019, Gartner published a report called *The Future of Network Security Is in the Cloud*. In this report, Gartner introduced the secure access service edge (SASE) concept. The SASE concept extends the notion of multiple security capabilities, unified and delivered in the cloud, by adding SD-WAN capability. A SASE solution can secure users from any location or device as they access the Internet, SaaS apps, and private apps, while delivering a secure SD-WAN fabric across disparate connections and simplified, centralized management (see Figure 2-2).

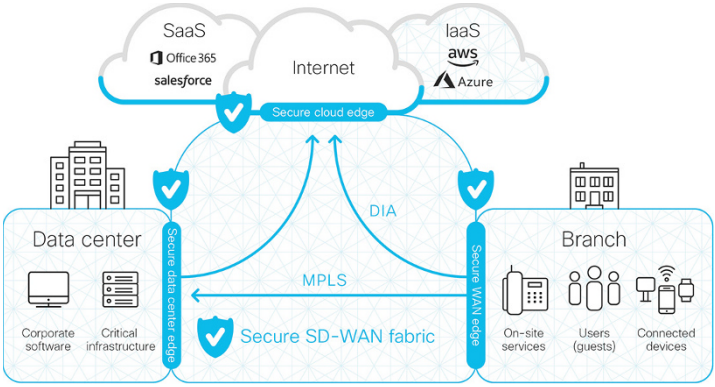



**FIGURE 2-2:** SD-WAN is a critical networking element in SASE solutions that can direct traffic for the protection of cloud, data center, and branch edge networks.

IN THIS CHAPTER

- Looking at secure connectivity challenges in the cloud era
- Recognizing key characteristics and benefits of SASE
- Getting started with SASE

# Chapter 3
# SASE: Combining Networking and Security Functionality

This chapter covers the challenges created in the new network architecture model, what functionality you need for secure connectivity, what issues you need to consider when deploying your solution, and how a secure access service edge (SASE) solution can help.

## Recognizing Secure Connectivity Challenges

Network security is no longer confined to the data center — it's shifting to the cloud. As work moves outside the office and applications move to the cloud, the tried-and-true perimeter-based security model just can't keep up. To be successful, IT teams need to identify a new approach to control and secure users, apps, devices, and data — anywhere and everywhere.

Today, the wide-scale use of cloud applications has become fundamental to business operations at all locations. Gartner predicted worldwide end-user spending on public cloud services would near the $600 billion mark in 2023. The centralized security approach has become impractical because of the high cost of backhauling traffic and the resulting performance issues for branch locations.

To overcome these cost and performance issues, many organizations are adopting a more decentralized networking approach to optimize performance at remote locations. This enables a more efficient direct Internet access (DIA) path for these offices but also highlights a set of new security challenges, including:

- **Gaps in visibility and coverage:** Centralized security policies can't be effectively managed and enforced in a decentralized network. This is because most traffic from branch locations to the cloud and Internet doesn't cross a centralized policy enforcement point. This results in visibility and coverage gaps, which increase the risk of a successful breach or a compliance violation.
- **Volume and complexity of security tools:** Security teams already struggle to keep up with cybersecurity threats. Many of them have a large number of point solutions that are difficult to integrate and manage. These point products generate thousands of alerts, making it very difficult, if not impossible, for analysts to keep up. As a result, many alerts go untouched.
- **Limited budgets and security resources:** IT and security budgets are already constrained. Deploying multiple, costly point security solutions — such as firewalls, secure web gateways (SWGs), intrusion detection and prevention systems (IDS and IPS), and data loss prevention (DLP) — to multiple locations and remotely managing these solutions with limited security resources is both impractical and ineffective.

# Key Characteristics and Benefits of SASE

The SASE concept consolidates numerous networking and security capabilities and functions — traditionally delivered in multiple, siloed point solutions — in a single, fully-integrated cloud-native platform (see Table 3-1).

**TABLE 3-1** SASE Combines Core Capabilities Provided by SD-WAN and Cloud Security

| SD-WAN | Cloud Security |
|---|---|
| **Centralized management.** A centralized, highly visual dashboard that facilitates device configuration, network management, monitoring, and automation. Includes zero-touch provisioning at the network edge. | **Zero-trust network access (ZTNA).** A security framework that mitigates unauthorized access, contains breaches, and reduces attackers' lateral movement across the network. ZTNA should be coupled with strong identity and access management to verify users' identity and establish device trust before granting access to authorized applications. |
| **Cloud network extension and middle-mile optimization.** Extensive cloud on-ramp integrations to enable seamless, automated connectivity with any site-to-cloud and site-to-site configuration. Includes optimized middle-mile connectivity through software-defined cloud interconnect (SDCI) and colocation integrations. | **Secure web gateway (SWG).** A gateway that logs and inspects web traffic to provide full visibility, URL filtering, and application control and protection against malware. |
| **Application experience.** The ability to monitor and validate the usability and performance of web applications. The detailed metrics and waterfalls show the sequential fetching and loading of web components to identify errors and bottlenecks and understand the impact on application performance. | **Cloud-delivered firewall with intrusion prevention system (IPS).** Software-based, cloud-deployed services that help manage and inspect network traffic. |
| **Flexible and scalable infrastructure.** A wide range of physical and virtual platforms that deliver high availability and throughput, multigigabit port options, 5G cellular links, and powerful encryption capabilities. Optimizes WAN traffic by dynamically selecting the most efficient WAN links that meet the service-level requirements. | **Cloud access security broker (CASB).** Software that detects and reports on cloud applications in use across a network, exposing shadow IT and enabling risky SaaS apps and specific actions, such as posts and uploads, to be blocked. |

*(continued)*

**TABLE 3-1** *(continued)*

| SD-WAN | Cloud Security |
|---|---|
| **Artificial intelligence (AI) enhanced troubleshooting.** Robust AI and machine learning (ML) for optimizing network performance, automating routine manual tasks, and accelerating troubleshooting. Provides intelligent alerting, self-healing, and predictive Internet rerouting capabilities. | **Data loss prevention (DLP).** Software that analyzes data inline or in cloud apps to provide visibility and control over sensitive data being pushed or pulled beyond the organization's network or cloud. |
| **Integrated security.** Robust security capabilities that work hand in hand with cloud security to protect branches, home users, and cloud-based applications from infiltration. | **Remote browser isolation (RBI).** Software that isolates web traffic from user devices to mitigate the risk of browser-delivered threats. |
| **Identity-based policy management.** Microsegmentation and identity-based policy management across multiple locations and domains. | **DNS-layer security.** Software that acts as the first line of defense against threats on the Internet, blocking malicious DNS requests before a connection to an IP address is even established. Strong DNS security can greatly reduce the number of threats a security team has to triage on a daily basis. |
| **Advanced insights.** Enhanced visibility into application, Internet, cloud, and SaaS environments with comprehensive, hop-by-hop analysis. Enables the isolation of fault domains and provides actionable insights to accelerate troubleshooting and minimize or eliminate the impact on users. | **Threat intelligence.** Threat researchers, engineers, and data scientists who use telemetry and sophisticated systems to create accurate, rapid, and actionable threat intelligence to identify emerging threats, discover new vulnerabilities, and interdict threats in the wild before they spread, with rule sets that support the tooling in your security stack. |

Potential business benefits of the SASE concept include the following:

- Reduce cost and complexity
- Enable secure remote and mobile access to private and SaaS apps plus other Internet services
- Provide latency-optimized, policy-based routing

- Improve security with consistent policy
- Update threat protection and policies without hardware and software upgrades

## HOW AVRIL EXTENDS PROTECTION TO BRANCH OFFICES WITH CISCO UMBRELLA

Today, DI allows branch offices to significantly improve network performance — eliminating latency by removing the need to backhaul traffic to the data center. But as a result, Internet traffic from these locations isn't seen or protected by the centralized security stack, which can leave users and sensitive data exposed.

To embrace the increasing use of DIA, IT teams need a simplified, cloud-delivered service that unifies the power of multiple point security solutions in a single console. That solution is Cisco Umbrella.

Avril, a French agro-industrial group, needed to provide their branch offices with a reliable security solution that could continue to expand as Avril acquired new businesses and divisions. To secure these locations while still providing them with fast DIA, they needed a cloud-delivered security service that could work at the outer edges of the network, providing a front line of protection.

Using Cisco Umbrella's integrated network and security architecture, Avril can protect branch users, connected devices, and app usage at tens of thousands of DIA breakouts. By leveraging Umbrella security to extend protection everywhere, Avril has been able to substantially reduce the risk of data exfiltration and malware across all ports and protocols. Simple to deploy and easy to manage from the cloud, Umbrella also allows Avril to keep expanding protection to keep up with new needs and new growth.

With Cisco Umbrella, the Avril Group was able to reduce ransomware by 100 percent, secure mobile users working off-network, and reduce security management time over previous solutions.

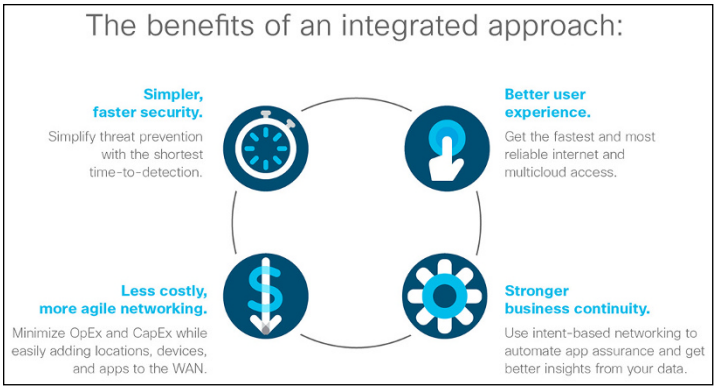
Marc Tournier, Information Security and Compliance Manager (CISO) at Avril, was impressed with the quick time-to-value. "Umbrella secured the whole company network in 10 minutes."

- Restrict access based on user, device, and application identity
- Increase network and security staff effectiveness with centralized policy management
- Deliver a consistently seamless user experience anywhere

These benefits are critical for organizations that need to address the modern networking and security challenges of an increasingly cloud-first, distributed, mobile, and global workforce.

## Starting Your SASE Journey

SASE is a broad concept. To keep things simple, you should look for options that are flexible, allowing you to iteratively make changes at your pace and progress toward your organization's goals. That being said, two major SASE concepts are consolidation and simplification, so it makes sense to chart a course that includes both networking and security elements from a single vendor. There are many technical, cost, and end-user performance advantages to this type of combined approach (see Figure 3-1).




*Source: Cisco*

**FIGURE 3-1:** The benefits of an integrated networking and security approach.

With these combined benefits in mind, it makes sense to look at the logical first step in both networking and security.

## Networking first step

Begin by looking at the many benefits of software-defined wide area networking (SD-WAN) and start a trial to show the impact it could have on your networking service costs, performance, and management tasks. As you develop a plan for SD-WAN, you should also decide the best way to secure the new traffic flows, especially from the increasing number of remote branches and roaming users. Look for a vendor with a strong portfolio of network technology that will deliver a broad range of network as-a-service capabilities in the future.

## Security first step

Look for a cloud-native solution that can flexibly improve or even replace your current security stack capabilities. Look for a solution that can handle a broad set of security tasks and present data in a single console to help simplify deployment, investigations, and ongoing maintenance tasks. In 2021 Gartner defined the term Security Service Edge (SSE) to describe the combined security elements of SASE.

WARNING

Don't re-create the challenges that resulted from on-premises security stacks with a large number of separate point solutions.

IN THIS CHAPTER

- Exploring key components in the security service edge (SSE)
- Integrating networking in a SASE solution with SD-WAN

# Chapter 4
# Knowing What to Look for in a SASE Solution

This chapter explores the two sides of the SASE coin: the security service edge (SSE) and software-defined wide-area network (SD-WAN).

## Security Service Edge (SSE)

An SSE solution secures access to the web, cloud services, and private applications. Some key capabilities include access control, threat protection, data security, security monitoring, and acceptable-use control enforced by network-based and application programming interface (API) based integration. SSE is primarily delivered as a cloud-based service and may include on-premises or agent-based components.

An SSE includes the following components:

- **Secure web gateway (SWG):** A cloud-based web proxy or secure web gateway (SWG) provides security functions such as malware detection, file sandboxing and dynamic threat

intelligence, Secure Sockets Layer (SSL) decryption, application and content filtering, and data loss prevention (DLP).

- **Cloud access security broker (CASB):** A CASB helps control and secure the use of cloud-based, software as-a-service (SaaS) applications, enabling organizations to enforce their security policies and compliance regulations. CASBs provide insight into cloud application use across cloud platforms and identify unsanctioned use within an organization. CASBs use auto-discovery to detect the cloud applications in use and identify high-risk applications and users, as well as other key risk factors. CASBs typically include DLP functionality and the capability to detect and provide alerts when abnormal user activity occurs, to help stop both internal and external threats.
- **Firewall as a service (FWaaS):** FWaaS is the cloud-based delivery of firewall functionality to protect non-web Internet traffic. This typically includes Layer 3 and Layer 4 (IP, port, and protocol) visibility and control, along with Layer 7 (application control) rules and IP anonymization.
- **Zero trust network access (ZTNA):** The zero-trust security framework takes a "never trust, always verify" approach to security. ZTNA verifies user identities and establishes device trust before granting access to authorized applications, helping organizations prevent unauthorized access, contain breaches, and limit an attacker's lateral movement on your network. ZTNA requires a strong, cloud-based, multifactor authentication (MFA) approach to security.
- **Domain name system (DNS) layer security:** Domain name system (DNS) resolution is the first step when a user attempts to access a website or other service on the Internet. Thus, enforcing security at the DNS and Internet Protocol (IP) layers is the first line of defense against threats and is a great way to stop attacks before users connect to bad destinations. DNS layer security is often, but not always, referenced when analysts discuss an SSE solution. However, because it's a highly effective first layer of security, it's wise to consider it as part of your overall SASE solution.


DNS is the system that maps Internet hostnames to IP addresses. For example, when a user enters `www.cisco.com` in a web browser, DNS translates cisco.com to the IP address associated with that website (96.7.212.119).

## Software-Defined Wide Area Network

An SD-WAN is a virtual WAN that allows companies to use any combination of transport services, including multiprotocol label switching (MPLS), cellular Long-Term Evolution (LTE) and 5G, and broadband, to securely connect users to network locations. It can select the most efficient routing method while reducing costs and simplifying management.

You can learn more about SD-WAN in Chapter 2.

IN THIS CHAPTER

- Getting a turnkey experience with Cisco+ Secure Connect
- Taking an incremental approach with Cisco SD-WAN and Cisco Umbrella
- Simplifying security with Cisco SecureX

# Chapter 5
# Exploring How Cisco Delivers SASE

Understanding that customers will be at different stages of their SASE journey, Cisco provides a variety of options. Cisco offers a unified SASE solution for a simplified experience, as well as an integrated solution — a converged security service edge (SSE) solution and separate SASE components — for those organizations that prefer greater customization flexibility. In this chapter, you discover how Cisco delivers secure access service edge (SASE) solutions.

## Cisco+ Secure Connect: A Turnkey Experience in a Unified SASE Solution

Cisco+ Secure Connect is a unified, turnkey solution with a blueprint for SASE made easy. It helps organizations build greater network resiliency, enables secure hybrid work, delivers a unified IT management experience, and provides an easy and seamless path to SASE that extends across premises to the cloud. Cisco+ Secure Connect is ideal for organizations looking to simplify networking and security operations while moving toward a cloud-first approach.

Powered within a single platform, Cisco+ Secure Connect securely connects users anywhere to any application with a single subscription. The solution integrates client-based and clientless remote worker access, native Cisco SD-WAN connectivity through either Cisco Meraki or Viptela technology, and comprehensive cloud-based security capabilities with Zero Trust Network Access (ZTNA).

# Integrated Solution for Greater Customization Flexibility

For organizations that prefer an incremental approach to their SASE deployments, Cisco offers a complete ecosystem of modular networking and security solutions, as well as individual SASE components, providing maximum customization flexibility.

## Cisco Umbrella: Multifunction, cloud-native security service edge (SSE)

Cisco Umbrella is a cloud security service that delivers a secure, reliable, and fast Internet experience. By unifying multiple security functions into a single service, Umbrella helps businesses of all sizes embrace direct Internet access (DIA), secure cloud applications, and extend protection to roaming users and branch offices.

REMEMBER

By enabling these functions together instead of through point solutions, Umbrella significantly reduces the time, money, and resources typically required for deployment, configuration, integration, and management of a stack of stand-alone security products.

Cisco Umbrella provides a core set of security functions in one cloud-based console (see Figure 5-1):

- **Secure web gateway (SWG).** Cisco Umbrella includes a cloud-based proxy that can log and inspect all your web traffic for greater transparency, control, and protection. This includes:

- Real-time inspection of inbound files for malware and other threats using Cisco Secure Endpoint (formerly Cisco Advanced Malware Protection (AMP) for Endpoints) and third-party resources
- Advanced file sandboxing provided by Cisco Secure Malware Analytics (formerly Cisco Threat Grid)
- Full or selective SSL decryption to further protect against hidden attacks
- Blocking of specific user activities in select apps (for example, file uploads, attachments, and posts/shares)
- Content filtering by category or specific uniform resource locators (URLs) to block destinations that violate policies or compliance rules

» **Cloud access security broker (CASB) functionality.** Umbrella helps expose shadow IT by detecting and reporting on cloud applications in use across your environment. Insights can help manage cloud adoption, reduce risk, and block the use of offensive or inappropriate cloud applications. Other highlights include:

- Data loss prevention (DLP) can prevent sensitive data from leaving the organization and being stored the cloud.
- Cloud malware detection can detect and remove malware from cloud-based file storage applications and ensure that applications remain free of malware.
- Tenant restrictions can control the software-as-a-service (SaaS) application instance(s) that all users or specific groups/individuals can access.
- Granular app controls allow you to control usage of capabilities within cloud apps.

» **DNS-layer security.** Cisco Umbrella blocks requests to malicious and unwanted destinations before a connection is even established — stopping threats over any port or protocol before they reach your network or endpoints. As a cloud-delivered service, Umbrella:

- Provides the visibility needed to protect Internet access across all network devices, office locations, and roaming users

- Logs and categorizes DNS activity by type of security threat or web content and the action taken, whether it was blocked or allowed
- Can be implemented quickly to cover thousands of locations and users in minutes to provide immediate return on investment

- **Firewall as a Service (FWaaS).** With Cisco Umbrella's firewall, all activity is logged, and unwanted traffic is blocked using IP, port, and application rules via its Layer 3/4 protection plus Layer 7 application visibility and control. To forward traffic, you simply configure an IPsec tunnel from any network device. Management is handled through the Umbrella dashboard, and as new tunnels are created, security policies can automatically be applied for easy setup and consistent enforcement throughout your environment. Cisco Umbrella's cloud-delivered firewall provides:
  - Visibility and control for Internet traffic across all ports and protocols
  - Customizable IP, port, and protocol policies in the Umbrella dashboard
  - Layer 7 application visibility and control
  - Intrusion prevention services (IPS)
- **Interactive threat intelligence.** Cisco Umbrella, supported by Cisco Talos, resolves approximately 625 billion web requests per day and discovers over 200 new vulnerabilities per year. With over 400 full-time threat researchers and data scientists, Cisco Talos creates and manages dozens of models to continuously analyze millions of live events per second. Further, Cisco Talos develops learning models that automatically classify and score domains and IPs. Umbrella is powered by this threat intelligence, and Cisco gives you access to that data to accelerate your threat response and detection. Your security analysts can leverage Umbrella Investigate for rich intelligence about domains, IPs, and malware across the Internet. Investigate provides the following:
  - Deep visibility into current and future threats
  - Better prioritization of incident investigations
  - Faster incident investigations and response

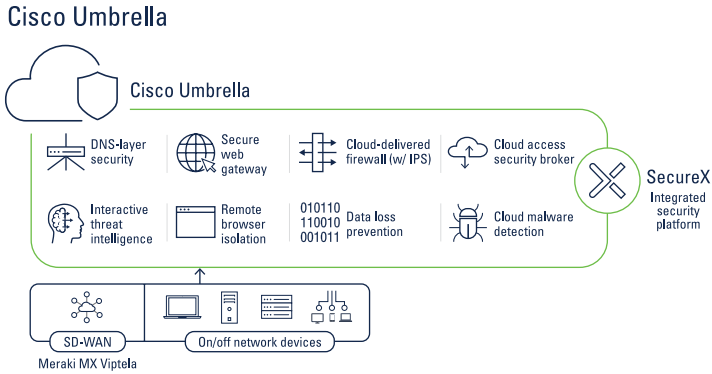



**FIGURE 5-1:** Cisco Umbrella delivers SASE security capabilities and more.

## Cisco Umbrella and SD-WAN integration

Cisco provides extensive integration between Cisco Umbrella and Cisco SD-WAN (Viptela and Meraki), as well as third-party SD-WAN providers such as VMware VeloCloud, HPE (Aruba) Silver Peak, and Palo Alto Networks Prisma. For organizations that prefer the flexibility of their own customization of SASE (as opposed to using a singular, unified SASE solution), the Umbrella and SD-WAN integrations provide automation that enables security administrators to infuse effective cloud security simply and rapidly throughout the SD-WAN fabric to protect branch offices and roaming users.

TIP

For a complete list of supported third-party SD-WAN providers, go to `https://docs.umbrella.com/umbrella-user-guide/docs/tunnels`.

TIP

For DNS-layer security, Umbrella can be deployed across hundreds of devices with a single configuration using the Cisco SD-WAN dashboard. For additional security and more granular controls, Umbrella's SWG and cloud-delivered firewall capabilities can be deployed through a single IPsec tunnel. Cisco has broken new ground in the automation, connection, and deployment of the tunnels, which connect SD-WAN traffic to cloud-based

security services. This integrated approach efficiently protects your branch users, connected devices, and application usage from all DIA breakouts.

# Cisco SD-WAN: Flexible Cloud-Managed Networking

Cisco's approach to SASE leverages a cloud-scale SD-WAN architecture (see Figure 5-2) designed to meet the complex needs of modern WANs in three key areas:

- Advanced application optimization that delivers a predictable application experience as the business application strategy evolves
- Multilayered security that provides the flexibility to deploy the right security in the right place, either on-premises or cloud-delivered
- Simplicity at enterprise scale, which enables end-to-end policy from the user to the application over thousands of sites

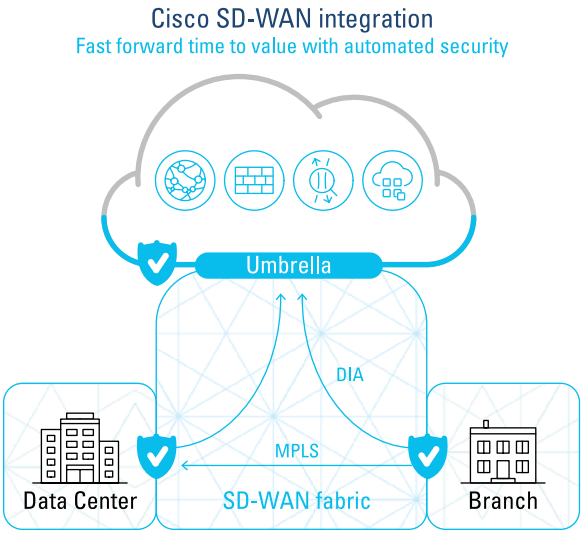



**FIGURE 5-2:** Cisco SD-WAN cloud-scale architecture.

The Cisco SD-WAN solution contains the following four key components that work together to form the Cisco SD-WAN fabric (see Figure 5-3):

- **Cisco vManage (management plane).** A centralized network management system that lets you configure and manage the entire overlay network from a simple, yet highly customizable, graphical dashboard. Cisco vManage simplifies and automates the deployment, configuration, management, and operation of Cisco SD-WAN.
- **Cisco vBond (orchestration plane).** The Cisco vBond Orchestrator automatically orchestrates connectivity between edge routers and Cisco vSmart Controllers. If any edge router or Cisco vSmart Controller is behind a network address translation (NAT) gateway, the Cisco vBond Orchestrator also serves as an initial NAT-traversal orchestrator.
- **Cisco vSmart (control plane).** The Cisco vSmart Controller is the centralized brain of the Cisco SD-WAN solution, controlling the flow of data traffic throughout the network. The Cisco vSmart Controller works with the Cisco vBond Orchestrator to authenticate Cisco vEdge devices as they join the network and orchestrates connectivity among edge routers.

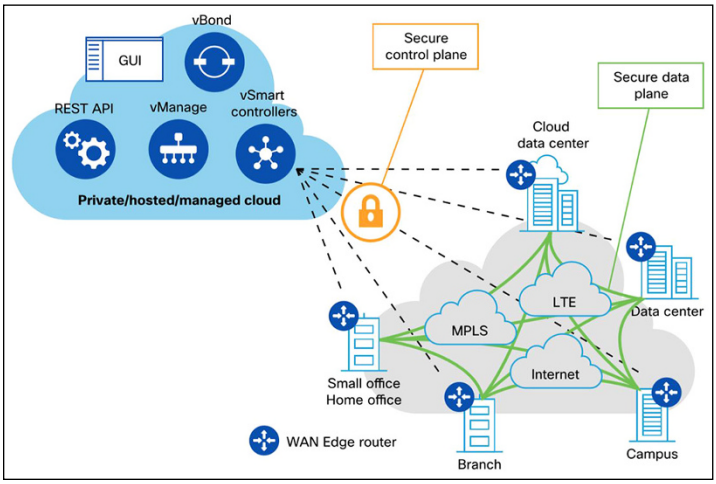



**FIGURE 5-3:** Cisco SD-WAN integration.

- **Cisco WAN Edge routers (network fabric).** Cisco IOS XE SD-WAN and Cisco vEdge Devices sit at the perimeter of a site (such as remote offices, branches, campuses, and data centers) and provide connectivity among the sites. They are either hardware devices or software (cloud router) that runs as a virtual machine. The edge routers handle the transmission of data traffic.

## Cisco SecureX: Simplified Security for a More Resilient Business

The Cisco SecureX platform connects the breadth of Cisco's integrated security portfolio and additional third-party tools for a consistent, simplified experience that unifies visibility, enables automation, and strengthens your security posture. It is a cloud-native, built-in platform experience within the Cisco Secure portfolio (thus no additional cost) that is connected to your infrastructure. SecureX aggregates data from all your security solutions for improved intelligence and faster response times.

With SecureX, you can immediately visualize threats and their organizational impact, and get an at-a-glance verdict for the observables you are investigating through a visually intuitive relations graph. It enables you to triage, prioritize, track, and respond to high-fidelity alerts through the built-in Incident Manager. Then you can take rapid response actions across multiple security products: isolate hosts, block files and domains, and block IPs — all from one convenient interface (see Figure 5-4).

SecureX empowers your security operations center (SOC) teams with a single console for direct remediation, access to threat intelligence, and tools like casebook and incident manager. It overcomes many challenges by making threat investigations faster, simpler, and more effective.

**FIGURE 5-4:** Cisco SecureX simplifies security with better visibility and automation.

## ZERO TRUST WITH CISCO DUO

For organizations of all sizes that need to protect sensitive data at scale, Cisco Duo's trusted access solution is a user-centric Zero Trust security platform for all users, all devices, and all applications. Duo's multifactor authentication (MFA) lets you verify the identity of all users — before granting access to corporate applications. You can also ensure devices meet security standards, develop and manage access policies, and streamline remote access and single-sign-on (SSO) for enterprise applications.

Today, many organizations combine the Cisco Umbrella SSE capabilities for robust cloud-delivered security with Cisco Duo for trusted access. Going forward, Cisco is further integrating zero trust network access (ZTNA) into its expanding Cisco SSE solution for seamless, secure access to cloud-based and private applications.

IN THIS CHAPTER

- Recognizing the changing nature of work and networking
- Dealing with cloud-delivered apps and services
- Addressing modern threats and attracting and retaining top security talent
- Getting started with SASE

# Chapter 6
# Ten Key Takeaways

Here are ten key takeaways about software-defined wide area networking (SD-WAN) and cloud security to keep in mind.

## More Remote Offices and Roaming Users

The number of remote office, mobile, and roaming users is growing — and these users are often some of your most susceptible targets for an attacker. The opportunity for mistakes — such as clicking on a malicious email link or visiting a malicious website — is growing, too. Because these remote and roaming users may not have access to a local IT resource, they may be less inclined to contact the help desk or security team when an issue arises.

Similarly, mobile and roaming users often don't think twice about connecting to a public Wi-Fi hotspot. Cybercriminals take every opportunity to exploit Wi-Fi vulnerabilities and the inherent trust that a coffee shop patron or hotel guest places in a "secure" Wi-Fi connection.

## DIA Is the New Normal

With the advent of the cloud era, network architectures designed to provide robust connectivity to a corporate data center are now obsolete and must evolve. The majority of network traffic today occurs either within the data center itself (east-west traffic) or from an organization's various locations to the cloud via the Internet (north-south traffic). As a result, backhauling network traffic from remote or branch locations over multiprotocol label switching (MPLS) wide-area network (WAN) links, or roaming user traffic over virtual private network (VPN) connections, is no longer an efficient or viable option. Organizations are increasingly providing direct Internet access (DIA) broadband links for their remote, branch, and roaming users to access their software as a service (SaaS) applications without the slow performance and latency associated with backhauling traffic to a corporate office with a single security stack.

## SaaS Apps Are Taking Over

Once limited to personal apps that employees downloaded to their smartphones, SaaS apps have now become core business apps supporting critical business functions in the modern digital workplace. Salesforce enables customer relationship management (CRM), Workday delivers payroll services, and Concur provides expense management. Other apps such as Office 365 provide email and collaboration, and still other apps such as Box, Dropbox, Google Drive, and OneDrive provide file storage and management.

Of course, part of the allure of SaaS apps is ease of use. To deliver this convenient user experience, many SaaS apps provide only weak access control and security mechanisms — or none at all. Others have robust access control and security but at the cost of convenience.

A multifunction, cloud-native security solution can provide cloud access security broker (CASB) services to ensure robust and consistent security, and access control policies are applied to all apps — for example by enabling single sign-on (SSO) and integrated threat intelligence.

REMEMBER

When you're considering SASE solutions, it's important to evaluate not only solutions that are just delivered by the cloud, but also solutions that were "born" in the clou (that is, cloud native).

## SD-WAN Is a Foundational Component of SASE

A SASE architecture can only be achieved through the combination of SD-WAN with cloud security. In other words, you can't have SASE without SD-WAN!

SD-WAN provides:

- Automated traffic routing and tunnel creation between SD-WAN devices and cloud security points of presence (POPs)
- Automated deployment of resilient connections and associated dynamic failover
- Cross visibility between platforms to provide awareness into cloud security via the SD-WAN console and vice versa
- Capability to share and consume security policies (such as segmentation) between SD-WAN and cloud security vendors
- Integration such that consoles are automatically opened with single sign-on (SSO)

## Network Architecture Is Meeting New Demands

SD-WAN as a stand-alone networking solution is great for solving enterprise networking challenges, particularly in remote and branch locations. SD-WAN enables organizations to set up new sites quickly without having to wait weeks or months to provision new MPLS WAN links. Instead, a local Internet service provider (ISP) can provide a DIA link, often within just a couple of days.

But agility and simplicity introduce new challenges for enterprise security teams. In the rush to get connected, security may be an afterthought to the business. Once the Internet connection is live,

the business is ready to go — with or without security. And if the SD-WAN solution doesn't have built-in security capabilities, the security team may need to ship a separate firewall and/or other security appliances to the remote office. Plugging in one appliance is fine but two or three — well, that's just asking for too much!

## Look for a Solution That Reduces Cost and Complexity

In the not too distant past, enterprise security teams routinely deployed best-of-breed point security solutions from different vendors to address single purpose needs — firewalls, secure web gateways (SWGs), intrusion detection and intrusion prevention systems (IDS and IPS), web content filtering, domain name system (DNS) security, data loss prevention (DLP), distributed denial-of-service (DDoS) prevention, and malware protection, to name just a few. These stand-alone products all have different operating systems and management consoles and typically provide only limited, if any, integration with other security products.

Unfortunately, in the pursuit of a "defense in depth" strategy, many organizations end up with "defense ad nauseam" as these various siloed security tools add complexity and often create performance issues in the network.


TIP

Avoid patchwork at all costs. A true SASE solution integrates networking (SD-WAN) and cloud security capabilities. Simply looking to add multiple best-of-breed point products that make up a SASE architecture may lead to more complexity than your original architecture.

## Don't Compromise on Network Performance

A key consideration for organizations implementing a SASE architecture is addressing the requirement for a better user and application experience. SD-WAN, a core component of this architecture, enables the quality of experience by intelligent network

selection. Ultimately, the user experience is what drives successful adoption of digital transformation initiatives in an organization. Poor network performance guarantees a poor user experience and drives frustrated employees to turn to potentially risky shadow IT apps and solutions.

SD-WAN enhances the quality of the application and user experience by enabling traffic steering and dynamic failover, resulting in greater enterprise productivity and agility within a SASE architecture.

In the hybrid workforce world, a key focus for many enterprises is application performance as it drives employee and ecosystem productivity, as well as customer satisfaction. With the increase in cloud adoption, the first thing users want is easy and reliable access to their SaaS cloud business applications — which is all about using the most optimized path to those applications. This is where SD-WAN plays a big role. While security inspection is important, before you even send the traffic out, you need to make sure that users utilize a thin or lightweight edge SD-WAN appliance to identify their application, prioritize that application, and then steer the traffic to the most optimized path.


TIP

Ensure that your network and security platform can deliver the performance (and security) your users require to stay productive — whether they are in the headquarters location, a remote or branch office, or roaming on a mobile device.

## Always Keep Security Top-of-Mind

Cyberthreats are becoming more advanced and attackers are employing new techniques to exploit vulnerabilities and breach targeted networks. Phishing emails that were once easily identifiable by their spelling and grammatical errors have become much more difficult to spot. Ransomware has become far more prevalent as well, with ransomware as a service (RaaS) making it easy for practically anyone to launch an attack. And these are among some of the less sophisticated threats today. Organized crime and nation-states launch far more advanced attacks with vast resources that can take years to detect and eradicate.

TIP

In a SASE architecture, the SD-WAN collects and transports vital telemetry (such as data about user, device, application, cloud, security, and so on) to apply and enforce cohesive, real-time, intelligent networking and security policies across all domains.

## Make Life Easier for Your Operations Team

The worldwide shortage of qualified security professionals is a trend that will continue for the foreseeable future. The good news for security professionals is that there will be well-paying security jobs for years to come. The bad news is that the already difficult job of securing an enterprise network is only getting harder as threats are getting more advanced, and the proliferation of siloed security tools requires specialized knowledge and experience that must constantly be updated and refreshed.

Attract and retain top talent by implementing innovative networking and security solutions that integrate functionality in a single, cloud-delivered platform and make life easier for your entire operations team.

## Every Journey Starts with a Single Step

With Cisco Umbrella, you can start small with DNS-layer security and build up with additional capabilities from there as your organization is ready.

A fully integrated SD-WAN and cloud-native security solution can help organizations address the networking and security challenges of the cloud and mobile computing era. Secure access service edge (SASE) provides advanced networking and security functionality in a single pane of glass, enabling enterprise networking and security teams to confidently build out their networks with the agility that modern businesses require.

TIP

Learn more about Cisco's approach to SASE at `https://umbrella.cisco.com/sase`.

# Discover multi-function cloud-native security

Enterprise networks are undergoing a significant transformation. Internet traffic from branch offices has traditionally been routed back to a central location where security functions are performed. Today, business-critical cloud applications make it impractical to backhaul traffic from branch offices due to cost and performance issues. Enterprises need a fully integrated networking and security solution built for the cloud. In this book, you'll learn how SASE addresses modern networking and security challenges.

## Inside...

- Leverage SD-WAN capabilities
- Optimize edge network performance
- Secure remote and mobile access
- Simplify network and security management
- Consume security functions as a service
- Access interactive threat intelligence
- Implement zero trust network access

cisco SECURE

**Lawrence Miller** served as a Chief Petty Officer in the U.S. Navy and has worked in information technology in various industries for more than 25 years. He is the co-author of *CISSP For Dummies* and has written more than 150 *For Dummies* books on numerous technology and security topics.

**Go to Dummies.com™**
**for videos, step-by-step photos, how-to articles, or to shop!**

ISBN: 978-1-394-19353-0
Not For Resale


for dummies®
A Wiley Brand

# WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.