LEARNING MADE EASY

Versa Networks Special Edition

SASE

for dummies®
A Wiley Brand

Future-proof your enterprise

Optimize security and application performance

Protect an expanding network perimeter

Brought to you by

VERSA NETWORKS

Kumar Mehta, MSE
Apurva Mehta, MSCS

About Versa Networks

Versa Networks, the leader in SASE, combines extensive security, advanced networking, full-featured SD-WAN, genuine multitenancy, and sophisticated analytics via the cloud, on-premises, or as a blended combination of both to meet SASE requirements for small to extremely large enterprises and service providers. Versa SASE delivers secure, scalable, and reliable enterprise-wide networking and security while increasing multi-cloud application performance and dramatically driving down costs. Thousands of customers globally with hundreds of thousands of sites trust Versa with their networks, security, and clouds. Versa Networks is privately held and funded by Sequoia Capital, Mayfield Capital, Artis Ventures, Princeville Global Fund, RPS Ventures, Triangle Peak Partners, Verizon Ventures, Comcast Ventures, and Liberty Global Ventures.

For more information, visit www.versa-networks.com or follow Versa Networks on Twitter at @versanetworks.

SASE

Versa Networks Special Edition

by Kumar Mehta, MSE, and Apurva Mehta, MSCS

for dummies®
A Wiley Brand

SASE For Dummies®, Versa Networks Special Edition

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

ISBN 978-1-119-80629-5 (pbk); ISBN 978-1-119-80630-1 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Publisher's Acknowledgments

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

Project Editor: Elizabeth Kuball

Acquisitions Editor: Ashley Coffey

Editorial Manager: Rev Mengle

Business Development Representative: William Hull

Production Editor: Tamilmani Varadharaj

Special Help: Kelly Ahuja, Monnia Deng, Aviva Garrett, Christina Hattingh, Sunil Ravi, Rohan Ravindranath, Faithe Wempen, Michael Wood, Chitresh Yadav

Table of Contents

Introduction

It's a scary world out there. Cybersecurity threats are more sophisticated, pervasive, distributed, and multidimensional than at any other time in history. At the same time, digital initiatives, technological modernization, and cloud innovations are enabling applications, users, and devices to be more physically distributed than ever before in history, making it harder for companies to control what comes into and goes out of their networks.

This unprecedented expansion of applications and users combined with deepening security vulnerabilities calls for an innovative method of connecting and protecting with cloud economies of scale. Micro-segmentation of network, security, applications, and users is no longer acceptable alone for ensuring data, asset, and application security.

To meet these challenges, enterprises must be able to provide network services that are as diverse and as spread out geographically as the applications and users who rely on them. Fortunately, comprehensive and integrated security, networking, and visibility via the cloud is possible today with the same scale and performance that were once available only in on-premises solutions.

Because you've picked up this book, we're betting that you're interested in making that happen for your company. So, let's get started.

About This Book

Secure access service edge (SASE) offers a way to bring trustworthy security to the peril-fraught modern enterprise networking landscape. Its capabilities extend far beyond legacy security architectures, incorporating identity, trust, and context regardless of the connection, user, device, or application. SASE also enables policies to be delivered pervasively, consistently, and ubiquitously, as well as meet security, networking, application, user, and business requirements.

This book covers everything you need to know about SASE. You discover what it includes, how enterprises and organizations benefit, how it supports security, how to best implement it, and how to take advantage of its best features.

Foolish Assumptions

In writing this book, we've gone out on a limb and made some assumptions about you. We assume that:

- You're an IT, networking, or information security (InfoSec) practitioner.
- You have a basic familiarity with IT, networking, and security issues.
- You're acutely aware of the pain points pervading the networking and network security landscape.
- You're not content with the status quo — you want a new approach to contain the costs and complexity of legacy solutions and products.

Icons Used in This Book

To make it easy to navigate to the most useful information, these icons highlight key text:

REMEMBER

The Remember icon marks key takeaway points.

TECHNICAL STUFF

Read these optional passages if you crave a more technical explanation.

TIP

The Tip icon highlights information that can save you time and effort.

WARNING

Watch out for these potential pitfalls on the road ahead.

Where to Go from Here

The book is written as a reference guide, so you can read it from cover to cover or jump straight to the parts you're most interested in. Whichever way you choose, you can't go wrong. Both paths lead to the same outcome — a better understanding of SASE and the steps and technologies you need to move forward.

IN THIS CHAPTER

- Explaining SASE features
- Understanding SASE requirements
- Deploying SASE

Chapter 1
Defining SASE

Enterprises today are transforming how they deliver business and productivity services to internal and external employees, partners, and customers. Organizations everywhere are adopting new technologies such as cloud, software as a service (SaaS), a work-from-anywhere (WFA) solutions, and the Internet of Things (IoT).

Organizations can find themselves caught in a bind, though, between enabling new capabilities and ensuring security. The cloud migration and mobility that employees and customers demand for ever-greater flexibility, agility, and reliability also substantially increase a network's attack surface. Legacy architectures no longer adequately meet either performance or security demands. It's time to reevaluate enterprise systems and tools.

Organizations must adopt a new IT model to eliminate the inefficiencies of traditional wide area network (WAN) architectures, enable a WFA workforce, and protect against a weak security posture. SASE can help them do that.

Secure access services edge (SASE) is an architectural framework and implementation introduced by Gartner to address security solutions for the client-to-cloud era. This chapter explains SASE's features and helps you understand what a SASE solution must offer.

Introducing SASE

SASE is not just one technology but an entire package of technologies, including:

- Software-defined WANs (SD-WANs)
- Secure web gateways (SWGs)
- Cloud access security brokers (CASBs)
- Zero-trust network access (ZTNA)
- Firewall as a service (FWaaS)

Deployed together, SASE technologies can help your networks meet the demand for robust security without compromising on technology, flexibility, or features. Let's look at each of them individually.

Moving from WAN to SD-WAN

Traditional IT infrastructure was like a walled garden. Employees connected to the corporate network at a company office and accessed applications in a private data center using a private, secure site-to-site WAN. Internet connectivity was centrally provided and secured from headquarters or data center locations.

The next generation of networking introduced SD-WANs. An SD-WAN is a network where the network hardware is separate from its software-based controls. First-generation SD-WANs identified applications, used policy to steer traffic, and achieved cost arbitrage. Second-generation SD-WANs delivered full networking with integrated security and allowed secure Internet breakout via Direct Internet Access (DIA) at every location to connect users directly to the cloud and SaaS applications.

Today's WFA workforce accesses applications from anywhere at any time. Enterprises are embracing SaaS for business-critical applications and migrating their workloads from private to multicloud architectures to meet speed, agility, and economic needs.

REMEMBER

In the current client-to-cloud era, the old fixed-network perimeter has dissolved into a fluid, amorphous edge. IT must deliver a secure, reliable, and dynamic user, customer, and application experience that can be enhanced, measured, monitored, and diagnosed.

Protecting web gateways and a work-from-anywhere workforce

A SWG guards a WFA workforce against Internet-sourced threats by protecting a web-surfing user device from being infected by unwanted software or malware and by enforcing corporate and regulatory policy compliance. A SWG includes

- Uniform Resource Locator (URL) filtering
- Anti-malware and antivirus protection
- Application identification and control capabilities
- Data loss prevention capabilities

SWGs can be implemented as on-premises hardware, virtual appliances, cloud-based services, or in hybrid mode as combined on-premises and cloud.

WARNING

Cloud-based SWG features and services vary significantly in sophistication among market offerings.

Securing cloud access

A CASB offers products and services to address security deficits in an organization's use of cloud services. This technology fills the need to secure the cloud services that users are increasingly adopting (both inside and outside the traditional fixed perimeter) and the growing deployment of direct cloud-to-cloud access. CASBs can be either on-premises or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to inject enterprise security policies as the cloud-based data or applications are accessed. A CASB can

- Inspect data, application, and user behavior in cloud services via provider application programming interfaces (APIs)
- Operate inline between users and cloud services or optionally offer Remote Browser Isolation (RBI) as an alternative
- Support the ability to provide visibility and perform access control of any user, device, or location
- Integrate with an enterprise's existing identity provider, security information and event management (SIEM) tool, and unified endpoint management (UEM) product

- Apply a variety of analytics when monitoring behavior of users, third-party applications, and data
- Identify and respond to malicious and/or unwanted sessions using multiple methods
- Distinguish between corporate and personal instances of cloud services and provide the ability to limit or block the exchange of data between them

REMEMBER

CASB vendors understand that, for cloud services, the protection target is different: It's still your data, but it's processed and stored in systems that belong to someone else.

CASBs provide concurrent central policy governance across multiple cloud services for both users and devices. They facilitate granular visibility into, and control over, user activities and sensitive data.

Trusting nothing

ZTNA asserts that no user or device is trusted by default, as with legacy local area network (LAN) segments and Internet Protocol (IP) addresses inside the perimeter. Traditional trust boundaries have dissolved in a world with ubiquitous Internet access.

ZTNA creates an identity- and context-based logical access boundary around an application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a set of named entities. The broker verifies the identity, context, and policy adherence of the specified participants before allowing access and prohibits lateral movement to elsewhere in the network. ZTNA significantly reduces the attack surface by hiding assets from public visibility. A zero-trust architecture is key to a SASE strategy, because it grants access only to traffic between authenticated users, devices, and applications.

TIP

Organizations can implement a zero-trust model by defining the protection surface, determining where sensitive information resides and who needs access, and establishing a variety of preventive measures such as unified policy, multifactor authentication (MFA), micro-segmentation, and least privilege access.

Providing threat protection

Next-generation firewalls (NGFWs) are deep packet inspection engines that move beyond port/protocol inspection and blocking to add application-level inspection. Leading-edge NGFWs integrate

- Traditional stateful firewall features
- Application-aware, deep packet content inspection
- Unified threat management (UTM), including intrusion detection and prevention systems (IDPSs)
- Advanced visibility across the entire attack surface
- Flexibility to address the evolving threat landscape

WARNING

As the threat landscape rapidly expands with DIA and multicloud adoption, traditional firewalls are unable to protect at scale, causing a weak security posture. NGFWs and UTM are necessary to ensure good security hygiene.

Protecting sensitive data from malware

Data leakage occurs when personal or other sensitive data such as financial account numbers, healthcare data, or usernames/passwords are inadvertently exposed. A *data breach* occurs when an attacker actively penetrates a system to access, steal, or damage information.

TIP

To protect sensitive data, an organization must install and use a security software suite that includes malware and virus protection, and always keep it updated.

SASE enables sensitive applications and data to be accessed only by those who have a need-to-know per the corporate policy, regardless of the user's or application's location or the transport technology between them.

Operating at line rate with advanced routing

Advanced routing provides a unique set of integrated functions, such as path optimization, rapid convergence, traffic remediation, per-application quality of experience (QoE), and encryption.

Executing SASE properly requires an understanding and visibility of line-rate traffic at the edge of the network. A distributed-services edge architecture leverages the same scale-out model used for compute scalability: As demand grows, additional servers or virtual machines (VMs) are added to handle the overall volume of traffic while continuing to operate at line rate.

Understanding What SASE Requires

SASE embraces dynamic, contextual security based on identity, and delivers it primarily as a cloud service. A leading SASE solution must meet a certain minimum set of requirements. Here's a summary of what's needed.

Hardware neutrality

Traditional branch and site-to-site hardware architectures have served enterprises well, but they have resulted in stacks of single-purpose appliances at each corporate office. This appliance sprawl lacks agility, requires multiple touch points for changes, needs staff skilled on various vendors' products, and uses excessive space and power. It also ties the enterprise to a proprietary architecture and reduces the ability to easily change technologies.

In contrast, a single-stack software solution deployed on a bare-metal appliance — as a VM or as a container — saves space, power, time, and effort while providing much improved scalability, performance, and manageability. The solution integrates:

- Application awareness
- Full-security stack
- SWG
- SD-WAN and application-based traffic steering

- Routing
- Quality of service (QoS)
- Compression
- Encryption
- WAN optimization

Single-pass execution

An environment with discrete single-service appliances hands off packets from one product to the next. Each one copies the packet into memory, unpacks the content, analyzes the data and context, applies a decision or policy, repacks the packet, and transmits it to the next device in the chain. Each device must decompress/decrypt the packet if necessary and redo these actions before transmission. This process is time-intensive and significantly impairs performance.

A single-pass, flow-based architecture with internal service chaining like the one shown in Figure 1-1 optimizes performance by executing each action only once:

- It unpacks (and decrypts) the packet into memory.
- It makes content and context available to all security, routing, policies, filtering, and other functions.
- It repacks (and encrypts) the packet for transmission.

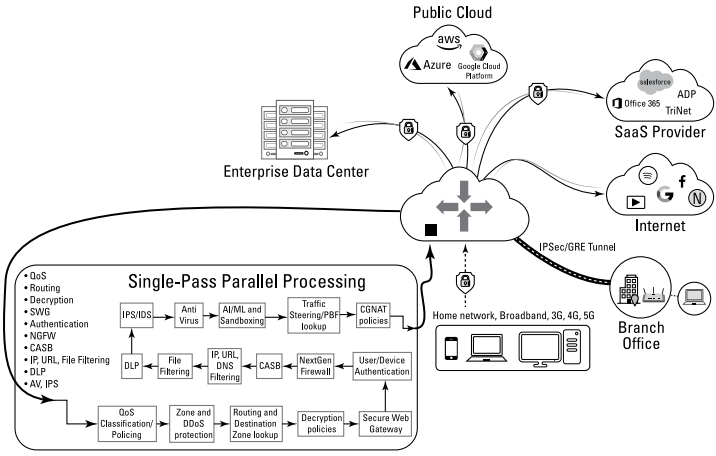

FIGURE 1-1: Single-pass processing flow.

Elastic scale-out

A single-pass processing architecture dramatically lowers latency, significantly improves performance, mitigates security exposure, and saves space, power, and specially skilled IT staffing. It is efficient and scales horizontally by leveraging multiple underlying cores or memory.

The ability to run the integrated software-only solution on a bare-metal server, VM, or container makes it deployable as a cloud-based service that provides additional flexibility and agility.


TECHNICAL STUFF

Using fully automated, single-pane-of-glass orchestration capabilities, a *branch* can be instantiated temporarily in the cloud and then as easily be decommissioned. For example, a home office can be defined as a *branch.*

Containers and microservices

A *microservice* is a service-oriented application, strongly encapsulated, loosely coupled, independently deployable, and independently scalable. Each service is responsible for a discrete task and communicates with other services through simple APIs to solve a larger, complex business problem.

A cloud-native SASE solution based on a microservices design has a fluid architecture that can run on public or private clouds, making horizontal scaling both easy and flexible.


REMEMBER

The benefits of a microservices architecture are its isolation, resilience, and scalability.

Global distribution

Globally distributed SASE-capable points of presence (POPs) offered through colocation facilities, service provider POPs, and infrastructure as a service (IaaS) should be used to reduce latency and improve performance for network security services. A SASE solution must offer distributed POPs that align with the digital enterprise's access latency and data residency requirements. This is also critical for maximizing localized end-user experiences.

Inline encryption

Encryption is paramount to protect transactions and data in transit. SASE providers must be able to terminate and inspect encrypted sessions, where required, based on policy with a scalable (ideally, software-based) architecture. SASE offerings must be able to deliver inline encrypted traffic inspection (decryption and subsequent re-encryption) at scale, ideally delivered from the cloud and without the use of proprietary hardware.

TIP

SASE solutions must include line-rate encryption capabilities (hardware or software) to provide acceptable user QoE.

Segmentation with multitenancy

SASE delivers security by isolating and segmenting traffic. Cloud-native SASE architectures are multitenant with multiple customers sharing the underlying data plane compared to single tenancy, which results in lower densities and potentially higher costs.

A multitenant architecture completely separates each tenant's operating environment, configurations, profiles, privileges, policies, and traffic handling, thereby ensuring complete security between each tenant's partition of a shared resource. Multitenant partitioning enables reliability, availability, and scalability, while enabling cost savings, flexibility, and security to IT organizations. A multitenant platform scales easily to handle increasing demand.

REMEMBER

It is imperative that the multitenant architecture encompasses *all* of each tenant's environments — the management, control, and data planes.

TIP

Multitenancy support is required on any shared SASE or cloud resource, such as gateways, controllers, and orchestration platforms.

Deploying a SASE Solution

A leading SASE solution must support flexible models for on-premises, in the cloud, and combined premises-and-cloud deployments. It must also deliver consistent security, networking, and business policies on-premises and in the cloud for users and traffic anywhere in the world.

A truly flexible SASE solution offers a global cloud-native architecture, deploying cloud instances with a simple point and click, regardless of whether it's a public, hybrid, or on-premises cloud, or a combination thereof.

A SASE solution attaches and anchors a SASE client to the most optimal SASE gateway by taking into consideration the distance between the SASE client and SASE gateway, as well as the service load on the SASE gateways.


TIP

SASE infrastructure eliminates multicloud interconnectivity challenges by seamlessly establishing dynamic secure overlay connectivity for both the data and control planes to each cloud.

IN THIS CHAPTER

- Transforming the network perimeter
- Consolidating complexity and cost
- Optimizing security and performance
- Driving digital transformation

Chapter 2
Becoming a Modern Enterprise

Modern enterprises conduct business in the client-to-cloud era. According to Gartner, "Network and network security architectures were designed for an era that is waning, and they are unable to effectively serve the dynamic secure access requirements of digital business." Gone is the time when employees all worked in a physical building and all your corporate resources were held in private data centers that were both physically and digitally secured.

The enterprise data center is no longer the focal point for applications, and the fixed network perimeter no longer exists. Digital transformation initiatives and the adoption of software as a service (SaaS) applications and cloud-based services have completely changed the enterprise network. In today's IT world:

- More user work is performed outside the traditional enterprise network perimeter than inside it.
- More workloads are running in the cloud than in the enterprise data center.
- SaaS applications are used more frequently than locally installed ones.

- More sensitive data is located outside the enterprise data center than inside it.
- More traffic is destined for public cloud services than the enterprise data center.
- More traffic from branch offices is heading to public clouds than to the enterprise data center.

In this chapter, you learn about securing the new software-defined network perimeter, maintaining and improving quality of experience (QoE) and application performance, the digital transformation trends in modern enterprises, and how to reduce hardware and network complexity while simplifying your network and streamlining its management.

Expanding the Network Perimeter

For decades, enterprises relied on different wide area network (WAN) technologies such as leased lines, Frame Relay, and asynchronous transfer mode (ATM) to securely connect physical sites. More recently, Multiprotocol Label Switching (MPLS) became the widely adopted WAN technology of choice for secure connections between corporate locations, creating a walled garden.

The perimeter is evolving and amorphous

MPLS is excellent at securely connecting corporate offices to each other. However, it's expensive, inflexible, fixed-bandwidth, slow to provision, and inappropriate to connect homes, mobile devices, or temporary locations.

Yesterday's fixed network perimeter connected static branch sites via dedicated MPLS circuits to a hub site and/or a headquarters or data center location. Everything was private. It was secure because it was private. Today's client-to-cloud networks connect work-from-anywhere (WFA) clients in homes and mobile locations over the Internet to globally distributed cloud assets where workloads may dynamically change location based on cost, performance requirements, or demand volume. In a cloud-centric enterprise, users and devices are omnipresent, as are the network

capabilities to which they require secure access. This means secure access services must be everywhere as well.

The fixed building perimeter of yesterday has expanded and evolved into a software-defined client-to-cloud perimeter that exists transiently between a WFA user device connected via the Internet to a dynamic cloud location. This client-to-cloud perimeter is profoundly in need of precise and dynamic security measures based on identity and context.

Working with legacy WANs

Traditional WAN architectures secured the enterprise perimeter by funneling all access to resources outside the enterprise (including the cloud) through a centralized Internet connection managed and firewalled by the security team, as shown in Figure 2-1. Imagine the complexity, congestion, and delays if all passengers flying internationally were funneled through a single international airport. Imagine the client experience!

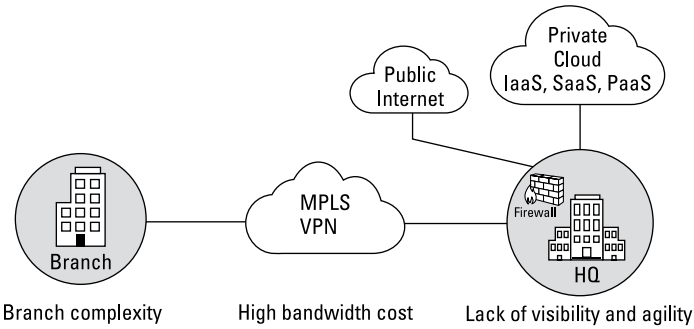

FIGURE 2-1: Traditional WAN architecture.

Although legacy architectures worked well enough in a past era when all employees and corporate assets were in fixed, private corporate locations and Internet access for business purposes was minimal, there were nevertheless serious drawbacks:

- Significant branch complexity
- Expensive bandwidth costs
- Lack of visibility and agility

Working with modern WANs

SD-WAN 1.0 solutions integrated the Internet as an alternative transport option to MPLS while maintaining the old network topology, as shown in Figure 2-2. This reduced MPLS costs but addressed neither security nor poor QoE for cloud and SaaS applications. It did not connect the user directly to the cloud.

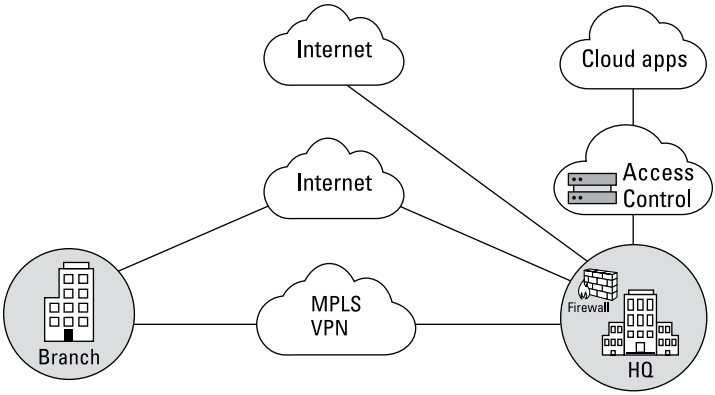

FIGURE 2-2: SD-WAN 1.0 architecture.

Bolt-on security approaches filled the gap but resulted in added cost and complexity with multiple single-purpose appliances at each location — a considerable burden in a network with many small sites such as retail stores.

TECHNICAL STUFF

A bolt-on security approach solved cloud security only for outbound traffic, but sites were still exposed to Internet threats on traffic inbound from the cloud. The branch perimeter still required on-premises security to control and segment traffic, to protect against ingress denial-of-service (DOS) attacks, and to stop the lateral movement of malware and attackers. For example, a bank might want to segment retail and ATM traffic from investment services for compliance reasons, or a company may choose to segment guest Wi-Fi traffic based on security policies. Some organizations might inspect outbound Hypertext Transfer Protocol (HTTP) traffic through a cloud-security service but deploy on-premises security to protect non-HTTP traffic. The critical component in each scenario is to simply and cost-effectively have security embedded in the SD-WAN across the entire enterprise edge.

REMEMBER

A second-generation solution — secure SD-WAN — incorporates full networking and integrated security in a single software stack. This solution, shown in Figure 2-3, finally enables enterprises to deploy secure, direct Internet breakout at every site and build an express on-ramp to cloud and SaaS applications. This architecture additionally provides

- Simplification, with a single device at each location
- Lower bandwidth costs
- Increased agility and visibility
- Co-existence with augmented cloud security

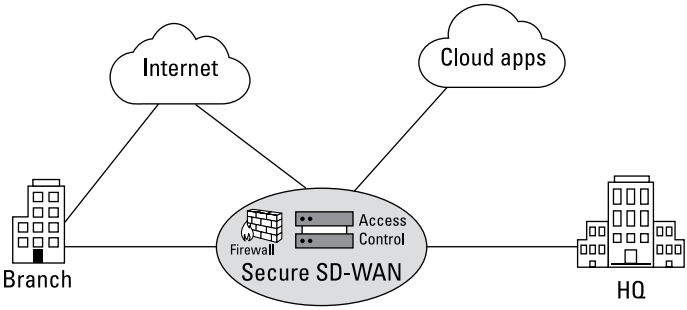

FIGURE 2-3: Secure SD-WAN architecture.

Reducing Hardware Complexity and Cost

The stack of proprietary appliances deployed at each site of an enterprise network quickly adds up in cost and complexity. Typically, these are point products from a plethora of vendors that

- Require IT staff to be skilled in many different vendor-specific interfaces and technical product details
- Require manual and error-prone coordination of configurations and policies
- Have widely varying troubleshooting capabilities
- Lack "dashboard" visibility across the entire network
- Are not automated

- Require tracking many software versions and security patches

Appliance sprawl is a key contributor to the lack of agility in an enterprise. Every little change requires multiple touch points and multiple maintenance windows.

Second-generation secure SD-WAN solutions, like the one illustrated in Figure 2-4, solve this challenge by incorporating full networking and security in a single software stack. This is the preferred approach for modern enterprises and is anticipated to remain the primary approach for secure site-to-site and direct client-to-cloud connectivity between users and cloud resources. Additionally, a secure SD-WAN "branch" can be deployed on a virtual platform in the cloud, providing more deployment flexibility and agility to handle traffic that does not originate in a physical building site. This approach also provides automation and single-pane-of-glass dashboard visibility to everything in the network, including Internet and cloud network segments.

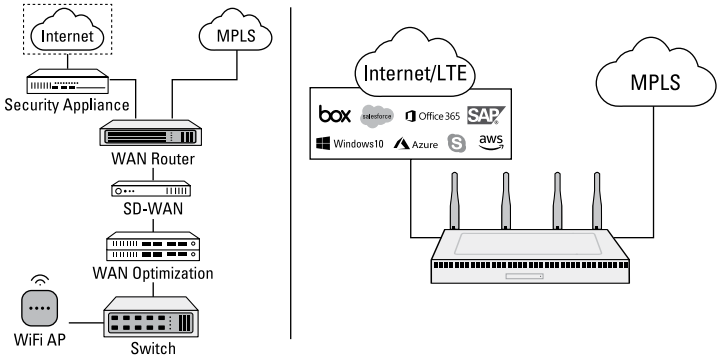

FIGURE 2-4: Secure SD-WAN appliance consolidation.

Enhancing Security and Increasing Performance

Enterprises face significant challenges to deliver secure client-to-cloud connectivity in legacy network and security architectures. The modern network's expanded amorphous perimeter and

ubiquitous Internet connectivity significantly magnify the attack surface of a company's workforce and assets — the types, volume, and sophistication of the threats your users and assets are exposed to.

Key IT challenges include

- **User experience:** IT must deliver a consistent, reliable, and secure user experience through an automated, comprehensive policy based on user identity, context, enterprise security/compliance policies, and continuous assessment of trust.
- **Security:** To meet compliance standards and protect network environments with amorphous perimeters, the enterprise must guard itself against attacks along all Internet touch points. This is the new perimeter.
- **Visibility:** IT must have real-time and historical visibility into users, devices, applications, and sessions regardless of location, private or public. The network must have the ability to reduce the mean time to identify the root cause of an issue.
- **Automated control:** The environment must offer unified policy automation for user, network, and security that is dynamically and automatically enforced.
- **Save to invest:** IT must do all of the above with no increase in staffing or budget. Finding ways to modernize and transform the organization and its network, while also saving money, is key for the modern enterprise.

Understanding the Trends Driving Digital Transformation

The trends toward cloud computing and cloud storage, SaaS, infrastructure as a service (IaaS), mobility, ubiquitous Internet connectivity, and a WFA workforce renders traditional WAN architectures obsolete. These trends require advanced security solutions to protect your users and assets.

Cloud and mobility adoption

A legacy WAN architecture — a single Internet entry point at a central secure headquarters location with a beefy firewall — might still be stretched to serve an enterprise that uses a single cloud, albeit with deficits in QoE and application performance because of suboptimal connectivity and traffic routing.

REMEMBER

Multicloud migration is rapidly becoming the norm, but legacy WAN architectures entirely lack the ability to serve a multicloud environment. Traditional hub-and-spoke connectivity to connect branch users via static MPLS circuits to a data center firewall just doesn't work in modern multicloud environments where the Internet perimeter has become a distributed model in which every branch location and user must have direct and optimized cloud access.

A combination of SD-WAN and multilayered security is required to make multicloud work. When a corporate office connects to multiple clouds, you need cloud-intelligent, dynamic multipath connectivity and robust networking and security functions such as routing, SD-WAN, carrier-grade network address translation (CGNAT), DOS prevention, stateful firewall, next-generation firewall (NGFW), Uniform Resource Locator (URL) filtering, data loss prevention (DLP), intrusion prevention system (IPS), antivirus, Internet Protocol (IP) filtering, file filtering, anti-malware, lateral movement detection, and Secure Sockets Layer (SSL) proxy.

TIP

The key to enabling a smooth multicloud migration is an integrated, versatile, and multiservice cloud-native platform with embedded security.

Widespread acceptance of work-from-anywhere

The COVID-19 pandemic instantly made a majority-WFA workforce a practical reality. Government stay-at-home orders caused a dramatic surge in a previously slow-ramping trend. A large percentage of enterprises today accepts that WFA is the "new

normal" and expects real-estate assets to become significantly more shared in the future, replacing the old norm of company-owned buildings dedicated to a single use or activity.

Enterprise users include employees, customers, and partners who consume multicloud-hosted applications from anywhere — home, branch office, campus, or on the road. This client-to-cloud era calls for dynamic, secure, and reliable user and application experiences. A digital enterprise must

- Be accessible by customers from anywhere
- Provide a digital storefront available from anywhere

IN THIS CHAPTER

- Leveraging an SD-WAN foundation
- Defining what is genuine SD-WAN
- Delivering a consistent experience

Chapter 3
Starting with Networking

The goal of secure access service edge (SASE) is to provide secure work-from-anywhere (WFA) user access to all applications and data, whether resident in a data center, cloud platform, or at a software as a service (SaaS) provider. That's what today's enterprises want and need.

In this chapter, you learn about how software-defined wide area network (SD-WAN) technology forms the foundation of SASE by providing those features. SD-WAN is the key to SASE and the technology of choice for enterprise WAN on-ramp to SASE and multicloud connectivity. SASE encompasses hosted SD-WAN, security, and routing in the cloud.

Building on SD-WAN

Trends in cloud computing and services, distributed workloads, a burgeoning WFA workforce, and Direct Internet Access (DIA) have obsoleted traditional WAN architectures.

SD-WAN technology enables a client-to-cloud architecture: Internet-based backbones, traffic routing from anywhere, direct cloud access, and path selection to optimize quality of experience

(QoE). Figure 3-1 compares the networks of the past to the networks we're seeing in today's enterprises.

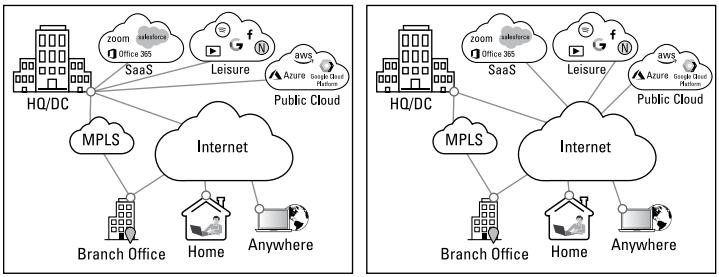

FIGURE 3-1: Modernization of network paths.

Using on-ramps and off-ramps

The *service edge* is the point of presence (POP) where traffic from WFA endpoints and cloud applications is secured and forwarded directly — or via the best alternate path — to the destination without being forced through a static focal point.

TIP

SASE technology must be deployed at every on-ramp and off-ramp point to secure traffic between users, devices, and cloud resources — regardless of location.

Ramping up with SD-WAN technology

SD-WAN technology offers several key capabilities to enable optimal performance in a client-to-cloud environment:

- Application-awareness and traffic classification
- DIA and intelligent traffic steering
- Global gateways to secure on-ramping from any location

Routing traffic from WFA employees requires application traffic to be classified accurately and immediately. When a home broadband link is shared among the kids' online learning, the spouse's work at a competing enterprise, and your employee's traffic, application classification, security, traffic prioritization, and traffic steering are paramount all the way to the endpoint device.

Application classification is done with deep packet inspection (DPI) based on application signatures and heuristic analysis that are dynamically and regularly updated. Using application classification, the application category is identified. Application categories can include application families and subfamilies, risk tags, productivity tags, and a tag to mark the traffic as business-centric or not.

TECHNICAL STUFF

If the DPI engine can dynamically query the fully qualified domain names (FQDN) and Internet Protocol (IP) addresses of SaaS providers, SaaS application identification starts with the first packet in the flow. This ensures that all flows are immediately associated with the appropriate policies and treated accordingly.

SD-WANs deliver much greater agility and lower transport costs across your network than traditional architectures. Using local DIA breakout at branch locations or for mobile workers enables traffic to use the most efficient and optimal path to access cloud applications.

WARNING

These newly opened Internet routes substantially enlarge your network's attack surface — exposure to malware and attacks — compared with the traditional private Multiprotocol Label Switching (MPLS) network.

Securing DIA traffic is a primary SASE responsibility. SASE must protect every session and every location, so its security functions include, at a minimum:

- A fully functional next-generation firewall (NGFW)
- Uniform Resource Locator (URL) filtering
- Secure Sockets Layer (SSL) encryption/decryption
- Intrusion detection and prevention system (IDPS)
- Antivirus
- Anti-malware
- Secure web gateways (SWGs)
- Zero-trust network access (ZTNA)
- Cloud access security broker (CASB)
- Data loss prevention (DLP)

SD-WAN gateways are globally available and provide distributed secure, reliable, and high-performance access to cloud

applications, services, and resources in addition to providing cloud-delivered SASE. Enterprises may have their own gateways (their own SASE service) or use provider gateways (a provider's SASE service).

As shown in Figure 3-2, gateways authenticate users, authorize application access protected with ZTNA, and secure the enterprise network from external threats, while optimizing QoE and direct access to cloud applications. SD-WAN cloud gateways with integrated SASE functions provide comprehensive security and QoE for business applications, as well as enable direct, optimal cloud/SaaS traffic steering.

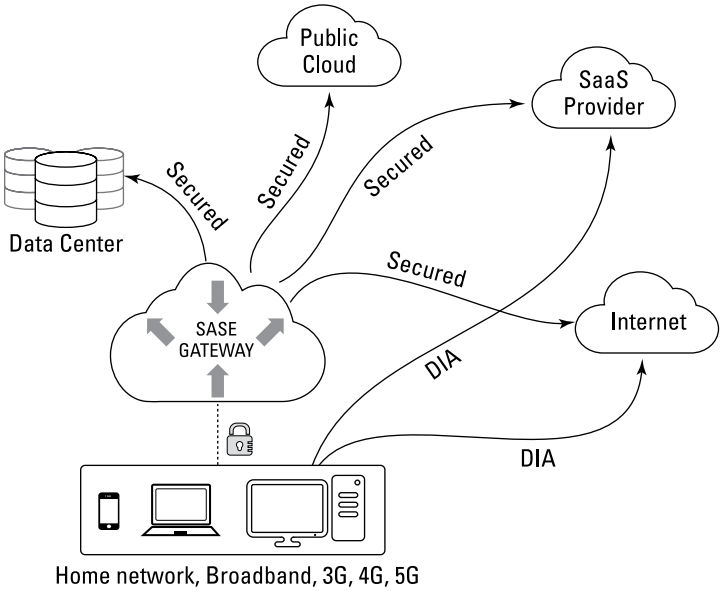

FIGURE 3-2: SASE gateway for users and devices.

Embedded security: The foundation of SD-WAN

Contextual security grants access based on multiple factors, including the identity of the entity, real-time context, enterprise security and compliance policies, and continuous assessment of trust throughout the sessions.

REMEMBER

Secure SD-WAN is a single-software-stack architecture with embedded security features, offering seamless contextual security based on user, group, location, device, posture, application, and content. Its embedded capabilities include

- **Protecting your users, locations, and devices:** Security must reside where traffic enters and leaves the network regardless of location: home, mobile site, branch, or a cloud software workload. Traffic may be headed for any Internet destination. Security must be dynamically applied inline to all flows based on the risk associated with the flow.
- **Special security considerations for cloud services:** An SD-WAN provides SaaS optimization, DIA security, and cloud gateways. The SD-WAN's SASE function ensures that all traffic on every path is secure. In a virtual private cloud (VPC) deployment, a virtual SD-WAN location with SASE can exist to bring the equivalent of "branch" security to the VPC.
- **Stopping threats before they become major problems:** Cloud migration, hybrid computing environments, and WFA realities — and ever more sophisticated attacks — pose a threat that demands a disciplined and dynamic approach to security that moves beyond defense and perimeter strategies. Enterprises today require an active, broad cybersecurity posture that encompasses continuous monitoring, rapid incident response, and proactive threat assessment. All this while also optimizing application performance and QoE.
- **Integrating security for all traffic and securing access for all endpoints:** SD-WAN security today must be distributed, augmented with cloud-based presence, flexible, simple, and available everywhere.

Understanding Genuine SD-WAN

All SD-WAN architectures do not innately provide the fluid edge security required for today's threat landscape. Different SD-WAN architectures, designs, and deployment approaches yield varying results.

SASE is an expansion of SD-WAN capabilities to provide a cloud-delivered networking and security solution. This is done

via a distributed system of edge software and cloud gateways to enforce consistent, unified, and global policies across cloud, home, mobile, and on-premises locations. SD-WAN is the on-ramp to SASE and is the technology of choice for enterprise WAN and multicloud connectivity. SASE encompasses hosted SD-WAN, security, and routing in the cloud. Because SD-WAN is the foundation for SASE, organizations must consider the key attributes required for a genuine SD-WAN solution.

Cloud gateways extend an organization's SD-WAN backbone from their premises (branch offices, regional sites, campuses, data centers, and home offices) to the front doorstep of SaaS and other cloud resources around the world. SASE converges network and security services in the cloud, on-premises, or as a combination of both, as shown in Figure 3-3.

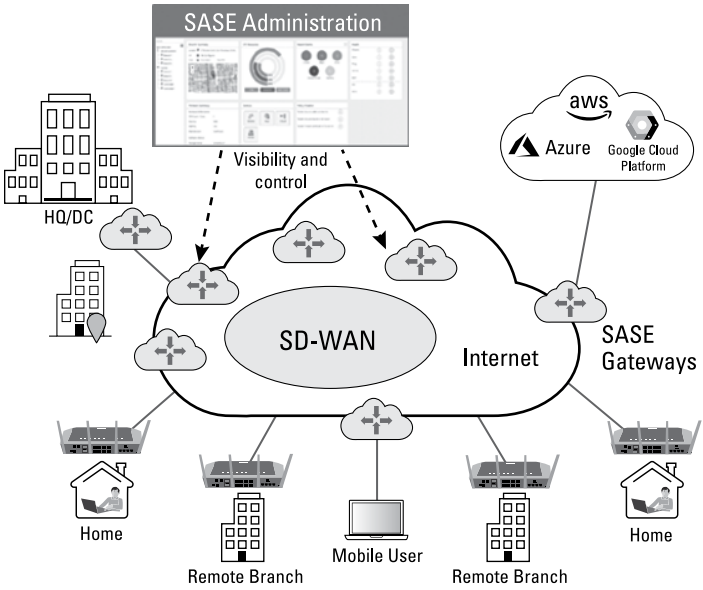

FIGURE 3-3: SD-WAN is the foundation for SASE.

In the next several sections you learn about some of the necessary attributes of a genuine SD-WAN.

Advanced routing capabilities

Several SD-WAN environments necessitate advanced routing capabilities to maintain well-behaved traffic and QoE. These environment attributes include

- The presence of underlay and overlay networks
- Individual, dynamic Internet Protocol Security (IPsec) tunnels for secure access to gateways and other cloud resources
- A middle-mile network to connect the cloud gateways that run a traffic engineering protocol to guarantee the best QoE by choosing the optimal path to SaaS, cloud service providers, and remote sites based on the offered end-to-end service-level agreement (SLA)

SD-WAN networks provide scalability, adaptability, and fast failure convergence regardless of deployment on-premises, in the cloud, or on a hybrid. SD-WANs deliver high-performance, application-aware intelligent routing to guarantee QoE at scale by optimizing routing protocols, including

- Internet Protocol version 4 (IPv4) static routing
- Internet Protocol version 6 (IPv6) static routing
- Open Shortest Path First version 2 (OSPFv2)
- Open Shortest Path First version 3 (OSPFv3)
- Border Gateway Protocol (BGP)
- Multiprotocol Extensions for BGP (MP-BGP)
  - MPLS-based Layer 3 virtual private networks (VPNs)
  - MPLS-based Ethernet VPNs (EVPNs)
  - Virtual Extensible LAN (VXLAN)–based EVPN
- Routing Information Protocol (RIP)
- Internet Group Management Protocol version 2 (IGMPv2)
- Internet Group Management Protocol version 3 (IGMPv3)
- Protocol Independent Multicast Sparse Mode (PIM-SM)
- Protocol Independent Multicast Source-Specific Multicast (PIM-SSM)
- Virtual Router Redundancy Protocol (VRRP)
- Policy-based routing (PBR)

Bidirectional forwarding (BFD) is used with routing protocols to monitor control plane health and provide rapid failure convergence.

An SD-WAN provides per-packet traffic steering, per-application policies, forward error correction (FEC), replication, first packet identification of SaaS applications, active probes, passive inline monitoring, and composite score calculations used for path selection.

SD-WAN supports numerous advanced capabilities, including

- **Enhanced voice and video:** The industry has recognized that a mean opinion score (MOS) is the best measure of voice and video QoE. Based on configuration and underlay performance, voice and video flows are dynamically switched to the path that provides the required MOS score.
- **Traffic conditioning and restoration:** When all available paths are impaired, remedial techniques such as FEC and packet cloning can restore flows that experience packet drops.
- **SaaS application optimization:** Measurements and historical reporting of SaaS application performance leverage passive inline analysis of Transmission Control Protocol (TCP) traffic and active TCP and Hypertext Transfer Protocol (HTTP) probes for each SaaS application. Active and passive performance metrics are used to select the best path for each SaaS application.
- **Advanced routing decisions based on end-to-end SLA:** Next-hop SLA monitoring lacks the end-to-end path awareness necessary to provide satisfactory QoE results. Traffic steering decisions must be made on the path's end-to-end SLA to achieve excellent QoE.
- **Application visibility:** SD-WAN auto-recognizes thousands of applications using a built-in DPI engine that employs various mechanisms such as:
  - Network-based identification (source address, destination address, port, protocol)
  - Signature/pattern-based identification
  - Protocol parsers (such as DPI)
  - Transport layer security handshake

- Heuristics
- IPS signature-based identification
- URL categorization and filtering

An SD-WAN must also identify encrypted applications, and the identification must be unaffected by the presence of a web proxy.

Quality of service

An SD-WAN edge device should support traffic prioritization (for example, high, low, strict high), weighted round robin (WRR), hierarchical queuing, random early detection (RED), weighted RED, tail drops, traffic shapers, hierarchical shapers, traffic policing, and traffic classification based on a comprehensive set of parameters. Additionally, it should also be capable of traffic marking, remarking, honoring type of service (ToS) and differentiated services code point (DSCP), and 802.1p priority bits. Remarking and shaping can be configured based on Layer 4 to Layer 7 policies.

An SD-WAN also supports multiple ingress queues to ensure packets are processed per configured scheduling priorities to avoid starvation and latency. In the case of over-subscription, lesser priority packets (including SD-WAN traffic) are tail-dropped at the time a packet enters the system.

Traffic optimization

As enterprise applications are increasingly consumed from the cloud, ensuring consistently high performance for these applications requires that various traffic optimization capabilities must be employed for Internet-bound traffic, as well as traditional private-network traffic.

The SD-WAN capabilities leveraged to provide optimal performance for SaaS applications include

- First-packet application identification
- Intelligent path selection mechanisms
- Passive performance monitoring via inline analysis of TCP traffic to all SaaS applications to create a near-term history of application performance per path

- Active TCP and HTTP probes for each SaaS application to create a near-term history of application performance per path
- Active and passive performance metrics to select the best egress or path for each SaaS application
- Combining local, direct egress with SaaS gateway egress

Guaranteeing QoE requires knowing when a particular path is congested and then smart-rerouting traffic. An SD-WAN continuously measures SLA characteristics for all paths to determine the optimal path that meets application performance requirements.

End-to-end QoS of the network is measured with active/passive probes between branches/nodes over different access circuits, across various transport paths, and for each specific traffic class.


TECHNICAL STUFF

Connectivity fault management/Y.1731 is used to monitor all possible paths to other branches deployed in your network. Each direction of every path is monitored independently. A database of SLA information is built (latency, jitter, packet loss, round-trip delay) to other VPN sites over various access circuits. SLA measurements are done per forwarding class. Two-Way Active Measurement Protocol (TWAMP) and ICMP-based probes measure SLA characteristics to non-SD-WAN endpoints, while HTTP-based probes more accurately measure response time for SaaS applications.


TIP

A mature SD-WAN solution uses both active traffic and synthetic probes to assess the SLA for a given path.

SD-WAN traffic-steering actions are crucial SASE functions to secure traffic and preserve QoE. Wherever the user is, and whatever paths are available to the application, the SD-WAN path selection logic must determine the optimal path.

WAN optimization

WAN optimization is needed to achieve high throughput for any TCP application, as well as for traffic traversing high-latency links such as transcontinental or satellite links.

An SD-WAN employs the following WAN optimization techniques:

- **TCP optimization:** TCP proxy-based optimizations are used that help maintain high throughput in challenging network conditions including high latency and loss.
- **Enhanced congestion control, loss detection, and loss recovery:** Mechanisms for these include congestion control based on bottleneck bandwidth and round-trip propagation time (BBR), recent acknowledgment (RACK) loss detection, tail loss probing (TLP), and rate pacing.
- **Intelligent buffer management:** This prevents data transfers from being buffer limited in high bandwidth-delay-product (BDP) networks.
- **Enabling high-performance options:** These include selective ACK (SACK), window scaling, and timestamp options.
- **Deduplication:** This method is a dual-ended — deployed at two nodes, one close to the client and one close to the server — optimization that involves representing large chunks or blocks of data by a shorter signature.
- **Compression:** Stateless, lossless compression methods such as zip are often used to further compress a deduplicated data stream when sent across the network, but they can be used by themselves as well.
- **Caching:** Single-ended optimization for applications such as HTTP or Server Message Block (SMB). Content (files) can be cached on the edge device so that subsequent requests for the same file are locally answered, avoiding duplicate WAN data transfers.

Global distribution

SASE offers distributed points of presence and a portfolio of traffic-peering relationships that align with the enterprise's access latency and data residency requirements. This is also critical for end-user QoE.

The Internet is used as a short hop to a SASE cloud gateway where the traffic is then inspected based on policy and optimized for best performance using fast-path routing and peering arrangements.

Multitenancy and segmentation

A multitenant architecture completely separates each tenant's operating environment, profiles, privileges, policies, and traffic handling, thereby ensuring complete security for each tenant's partition of a shared resource.

SD-WAN and SASE solutions should support native segmentation with a true multitenant implementation that separates the data plane, control plane, management plane, and analytics of each tenant. Each tenant can have multiple virtual routing and forwarding (VRF) systems, virtual LANs (VLANs), and service chains. Each segment can have

- A unique topology across the WAN
- Integrated network security per segment
- A set of configured internal or external services (such as security and WAN optimization) and service chains
- Service profiles
- Access control based on roles and responsibilities

WARNING

It is imperative that a multitenant architecture encompasses all of each tenant's environment — the management, control, and data planes. There must be separate per-tenant overlay tunnels for the traffic — management, control, and data — of each tenant.

Any shared SASE or cloud resource requires multitenancy support. Cloud-native SASE architectures are almost always multitenant with multiple customers sharing the underlying data plane.

5G architecture

Tight integration of SD-WAN, security, cloud, and 5G results in a more seamless deployment experience. The SD-WAN is the bearer (data) plane for the 5G/edge cloud and is the method by which 5G network slicing is implemented.

Edge-to-edge integration of SD-WAN and edge compute architecture accelerates 5G deployments and enables better device-to-cloud experiences. SASE offloads security functions for better 5G packet core utilization and reduces costs by sharing mobile infrastructure using multitenancy. SD-WAN is an enabler for 5G network slicing while SASE provides the security for 5G DIA. SASE and SD-WAN enable thousands of 5G cell sites to be easily deployed at scale.

Reducing Complexity

SD-WAN and SASE solutions are becoming the connectivity choice for the enterprise. SASE simplicity starts with a single cloud-native system — cloud-native SD-WAN networks are specifically designed for cloud-based applications and services.

Cloud-native systems exhibit a fluid architecture that is easily placed and moved through different environments. The architecture readily scales up or down during fluctuations in traffic so that users are much less likely to experience interruptions during peak demand times.

By being flexible, scalable, and dynamic, SASE simplifies the complexity that is associated with managing both on-premises and hybrid cloud components. The cloud-native SASE architecture gives consistent policy enforcement to reduce IT burden and assures end-user experience to reduce adoption friction.

IN THIS CHAPTER

- Evolving network security
- Protecting against intrusions
- Dealing with security threats
- Implementing cloud security
- Controlling user access

Chapter 4
Extending Security to Client and Cloud

The fixed perimeter of enterprise networks was softened by increasingly popular cloud applications and storage offerings. It then dissolved almost completely with users and devices from remote branch offices and a work-from-anywhere (WFA) workforce accessing corporate resources over the Internet. This trend creates individualized "virtual perimeters" that encompass only the user, the device, and the application, thereby removing the access distinctions that exist between being on or off the corporate network.

In this environment, security must be bound to and enforced by the identity and context of the user and device, the transport, the type of access, the accessed resource, and the access policy applicable to the transaction.

Security must be flexible, agile, and dynamic to serve every combination of users and resources. Security services must also scale and perform well to ensure quality of experience (QoE); they must tightly secure the transaction, as well as optimize user productivity.

In this chapter, you see how security methods and services have evolved to protect the amorphous, software-defined Internet perimeter of the modern enterprise.

Understanding the Evolution of Network Security

The traditional enterprise network security approach separated internal resources from the outside world with a fixed, well-defined border. Perimeter firewalls protected internal infrastructure from the outside: They inspected and disallowed unwanted traffic and blocked visibility and accessibility from outside.

Digital transformation trends and threats — such as unmanaged user devices, Internet of Things (IoT) devices, phishing, perimeter extension into the cloud by software as a service (SaaS)/infrastructure as a service (IaaS), Direct Internet Access (DIA), Long-Term Evolution (LTE) transport at home and at business locations, and a WFA workforce — have eroded the perimeter into a virtual and dynamic concept, rather than fixed infrastructure at specific locations.

The notion of a *software-defined perimeter* (SDP) draws on the Defense Information Systems Agency (DISA) idea of restricting connections to those with a need to know rather than trusting everything inside the fixed perimeter of the enterprise network. The Cloud Security Alliance (CSA) SDP Working Group popularized SDP to create highly secure, trusted, end-to-end networks for broad enterprise use.

REMEMBER

By default, SDP trusts nothing — the zero-trust model — and permits per-session access based on authentication and policy. There are commercial, open-source implementations of SDP as published by CSA, such as Google's BeyondCorp.

Software-defined networking (SDN) transformed all aspects of networking — including the perimeter and the wide area network (WAN) — into a software-only model. Fundamental to SDN architecture are the separate, isolated control and data planes. This separation allows for control of both the software-defined

WAN (SD-WAN) and the SDP control plane in a network, which in turn enables enterprises to implement both SD-WAN and SD-security in the same software control component. Being software-only, it can be deployed on bare-metal appliances (white box or branded appliances) and virtual machines, or VMs (in private or public clouds). All network and security functions are deeply integrated into a single software stack, resulting in operational simplicity and flexibility at the network edge and in the cloud.


TIP

To achieve SASE, a solution must be able to broker safe client-to-cloud security with an integrated software-defined architecture. Figure 4-1 shows how organizations need to integrate advanced SD-WAN capabilities and security functions together to achieve SASE.

Advanced SD-WAN Functions				
ZTP	Application ID	Probes, Inline Measurements	FEC	Packet Striping
Dynamic IPSec Overlays	Application PBF	SD-WAN Fabric Traffic Mgmt	Packet Cloning	DIA Traffic Optimizations
NAT Traversal	Application QoS	Application TE, App SLA	Multi-tenant	Built-in Security
Security Functions (all software-defined)				
NG Firewall	DoS Prevention	Device Authentication	IPsec	User and Group Authentication
CGNAT	HTTP/SSL Proxy	DNS Security	URL Filtering	Web and IP Feeds
Malware Sandboxing	IPS/IDS	Antivirus	File Filtering	Visibility and Analytics
CASB	ZTNA/SDP	UEBA	Device Identification	DLP

FIGURE 4-1: SD-WAN and security functions.

Detecting and Preventing Intrusions

There are multiple ways of detecting and preventing threats and vulnerabilities. The following sections outline the popular solutions on the market.

Next-generation firewalls

Next-generation firewalls (NGFWs) are essential for today's networks. They include traditional stateful inspection, but additionally go beyond those capabilities with identity-based and

application-level visibility and control using deep packet inspection (DPI). NGFWs remain key network security controls, and they continue to evolve to cover expanded use cases, such as the public cloud and distributed edge security.

Leading-edge NGFWs integrate traditionally free-standing capabilities such as intrusion and malware detection and protection.

Intrusion detection and prevention systems

An *intrusion detection and prevention system* (IDPS) is a standalone physical and/or virtual appliance that inspects network traffic, either on-premises or in virtualized/public cloud environments. It combines the function of two different systems: an intrusion detection system (IDS) and an intrusion prevention system (IPS).

Traditionally, an enterprise deploys an IDPS to inspect network traffic that has passed through perimeter security devices, such as firewalls and secure web and email gateways. While many companies still use detection only (IDS), many others additionally deploy appliances inline (IPS) to block detected threats.

Current deployment models integrate IPS functionality within the NGFW instead of deploying them as separate entities. An IDPS provides detection via several methods — such as signatures, protocol anomaly detection, various methods of analytics, behavioral monitoring and heuristics, sandboxing, and threat intelligence (TI) — to uncover unwanted and/or malicious traffic and report or take various actions on it.

All the aforementioned methods augment IDPS capabilities with more context to reduce analyst time processing alerts and help reduce or confirm false positives.

When deployed inline, an IDPS can use various techniques to detect and block attacks that are identified with high confidence.

Two increasingly popular trends are the use of Transport Layer Security (TLS) to encrypt traffic and the use of HTTP for various applications. TLS decryption must be integrated with the NGFW and IPS to enforce effective security policies and threat prevention.

Overall solution performance improves when unpacking and analyzing a packet occurs only once, and all security functions are applied to the packet content at the same time.

TIP

The best performance results when TLS decryption, IDS, IPS, and firewalls are combined into a single software stack.

DNS security

The Domain Name System (DNS) was created in the 1980s as a way to simplify the Internet, long before anyone gave serious thought to security best practices or security-by-design approaches. The DNS protocol has no built-in security precautions, so attackers can compromise the DNS system and redirect traffic to fake or bogus websites. Cache poisoning and man-in-the-middle are two well-known DNS attacks, the hacker's objective being to redirect web traffic by modifying the mapping of domain names to Internet Protocol (IP) addresses.

REMEMBER

Because it has no implicit security of its own, DNS traffic must be secured with various DNS security mechanisms like DNS security (DNSSEC), DNS proxy, DNS filtering, and IPS/IDS.

DNSSEC is an extension to DNS that uses public key infrastructure (PKI) that makes it more difficult to launch DNS attacks. DNSSEC uses a standardized method to add authentication to DNS transactions, verifying the sender and the integrity of the message.

DNSSEC is a broader concept that includes a variety of technical solutions for handling security exposure and preventing attacks on DNS servers and transactions. In addition to DNSSEC, security functions such as DNS proxy and DNS filtering can be used to address DNS attacks like DNS hijacking, DNS snooping, and DNS tunneling.

The DNS proxy mechanism forces DNS queries to always be forwarded to the corporate DNS server or a trusted DNS server.

DNS filtering evaluates and blocks access to unallowed and/or malicious websites, web pages, and IP addresses. DNS maps domain names to IP addresses to enable computers to find network resources, and DNS filtering enables an enterprise to control access to Internet resources from within the enterprise network. Using techniques such as allow/deny-listing and threat intelligence, DNS filtering can be used for devices on and off

the corporate network to help control what hosts are able to be resolved with DNS requests.

Managing and Controlling Security Threats

All traditional security mechanisms — firewalls, IPS/IDS, malware, antivirus, employee privileges, user and resource authentication, and URL/website filtering — now apply dynamically to every transaction on the network, whether on-premises or in the cloud.

Unified threat management

Unified threat management (UTM) is a blanket term for comprehensive security coverage of application access, consisting of various threat prevention features including NGFW, data loss prevention (DLP), IPS, IDS, malware detection, antivirus, antispam, TLS decryption, IP/URL/DNS filtering, file filtering, remote access for mobile employees (virtual private networks [VPNs]), and centralized management console.

Malware protection

Leading-edge UTM malware detection inspects traffic as it traverses the security point and extracts files for malware analysis, as shown in Figure 4-2. Malware detection targets two categories:

- **Known malware inspection:** This uses reputation (file filtering) and signatures (antivirus).
- **Unknown malware detection:** This requires more sophisticated predictive methods, such as algorithmic analysis and prediction (artificial intelligence [AI]–based scoring/prediction) and sandboxing with behavioral analysis, to determine whether content is potentially malicious.

Although some solutions send everything to the sandbox, most use triage methods. The triage process filters known bad (signature-style) files and passes known good files on to the next step in the process. This limits the number of files that must be deeply inspected — the so-called "gray list."

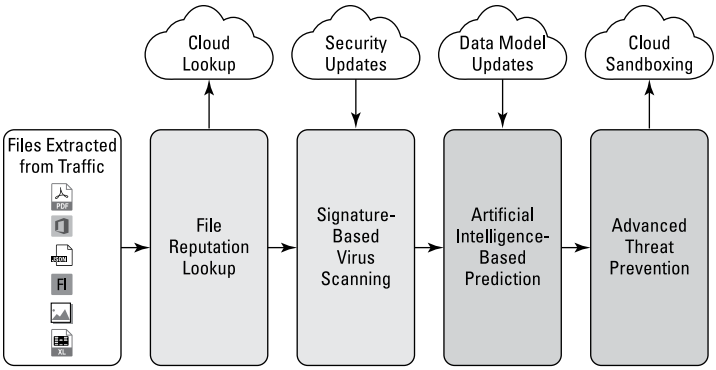

FIGURE 4-2: Identifying known and unknown malware.

TECHNICAL STUFF

A malware protection system (MPS) may rely on its physical placement for triage. For example, by placing an MPS behind a secure web gateway (SWG) or by integrating it with an IPS that performs malware scanning, the more trivial malware doesn't end up in the expensive MPS. Some MPSs perform their own content and/or network traffic heuristics or quick emulation before deciding that a file requires more in-depth inspection.

Most MPS solutions consult reputation lists (allow and deny lists) to narrow down gray lists. During triage, MPSs typically compute risk scores based on various characteristics and the configurable policy settings to pass or further inspect files.

Malware detection employs a combination of static and dynamic analysis techniques to determine if a certain file is malicious. Static analysis techniques include detection methods such as file reputation, signature/rule-based inspection, heuristics, emulation, machine learning (ML), and AI.

If the static analysis detection methods do not conclusively identify the file as either benign or malicious, the system dynamically analyzes the file by launching it in a sandboxed environment. Using a combination of static and dynamic analysis, systems can prevent harm from both known malware and zero-day malware.

Dynamic secure web gateway

A secure web gateway (SWG) protects enterprises and users from being accessed and infected by malicious web traffic and from being contaminated by hijacked websites that contain malware or viruses.

SWGs have evolved from their historical task of preventing enterprise end users from accessing time-wasting or otherwise unacceptable websites. SWG now has a broader security focus compared with its previous strictly operational role. Some features commonly supported by today's SWG include the following:

- URL filtering
- Anti-malware protection where the SWG inspects traffic that flows through it from the web using known malware signatures, as well as behavioral characteristics of malware that has not been encountered before
- IPS/IDS
- Application identification and control capabilities
- Native or integrated DLP capabilities
- Centralized management and logging

Based on the user, device, and location context, the SWG evaluates application policy and grants access only if the policy allows the request based on identity context. If the system allows access, the SWG informs the client which gateway to use and informs the gateway that governs access to the application of the user/device/location identity context.

Deployment architectures for SWG include

- Explicit mode forward proxy
- Inline mode
- Transparent mode
- DNS-based
- Cloud-based


TIP

Cloud-based SWGs protect users wherever they are, regardless of whether they're currently working in a company office, traveling, or WFA.

ZTNA and the new perimeter of users and devices

A *zero-trust network access* (ZTNA) solution creates an identity- and context-based logical access boundary around an application or set of applications.

REMEMBER

ZTNA provides controlled identity- and context-aware access to resources, reducing the surface area for attack.

When a user attempts to access an application in a zero-trust environment, the security software enforces authentication and evaluates the application access policy based on the user, device, and location. It verifies identity using an enterprise-specific authentication system such as Active Directory or Single Sign-On (SSO) using Security Assertion Markup Language (SAML). Depending on the context and security requirements, it may also enforce multifactor authentication (MFA) in addition to the enterprise-specific authentication system.

As a result of digital transformation, many enterprises have more applications, services, and data residing outside their traditional borders than inside. Cloud-based ZTNA services place the security controls where the users and applications are: in the cloud.

Adopting a zero-trust model focuses all security on identity: users, applications, devices, services, and systems. By normalizing the user experience for application access, ZTNA eliminates the distinction between being on and off the corporate network.

REMEMBER

A SASE solution proxies authentication into the infrastructure and directly monitors network traffic, integrating with SSO and federated services to ensure an authoritative view of "who is using what" across the entire enterprise.

A wide range of potential policy-based responses aligns with an observed level of risk, including blocking, MFA, reducing user privileges, forcing a password change, requiring an authorizer, or isolating the user from the Internet. All responses can be triggered based on identity, behavior, risk level, and other event contexts.

Securing the Cloud

In addition to the traditional security services, new cloud-focused services were established after organizations began to move to the cloud, such as cloud access security broker (CASB), Remote Browser Isolation (RBI), and user and entity behavioral analytics (UEBA). These services are critical to every transaction — merging old and new security protections.


TIP

Only by bringing together traditional security mechanisms with new cloud-native security approaches can organizations achieve secure client-to-cloud for their SASE implementation.

Cloud access security broker

CASB products and services deployed on-premises or in the cloud address security gaps in an organization's use of cloud services. This technology is the result of the need to secure cloud services, enable secure access to them from users both within and outside the traditional enterprise perimeter, and support secure cloud-to-cloud access.

For CASB products and cloud services, the protection target is different from that of an on-premises security system. It's still enterprise data, but the data is processed and stored in systems that belong to someone else. CASB provides a central location for policy and governance concurrently across multiple cloud services for both users and devices along with granular visibility into and control over user activities and sensitive data.

Some vendors and service/cloud providers offer cloud-hosted security as a service as part of their portfolios in both on-premises and provider-based models. These products and services provide a global footprint of locations where the CASB software nodes are deployed (see Figure 4-3). Enterprises use the nearest or most convenient point of presence as an on-ramp to high-speed and secure network and application access to the cloud infrastructure.


REMEMBER

CASB delivers five critical security capabilities: cloud application discovery, data security, adaptive access control, malware detection, and user and entity behavior analytics.

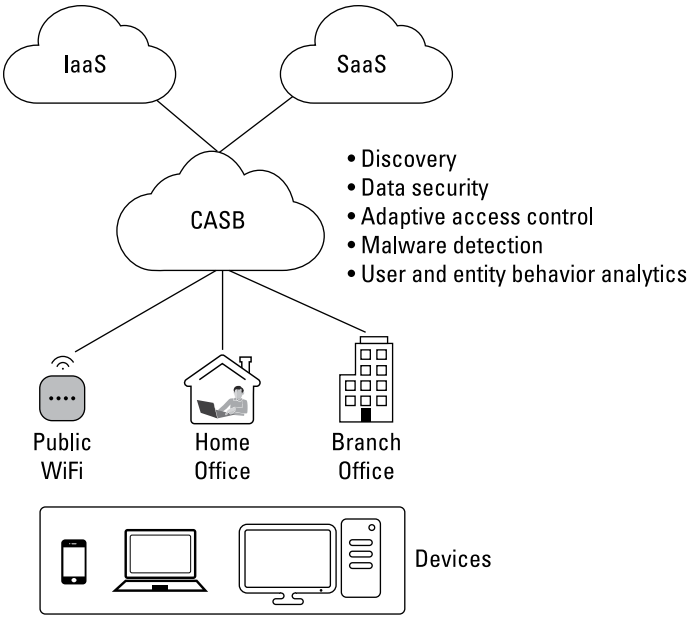

FIGURE 4-3: CASB architecture.

CASB helps organizations to

- Identify and evaluate all cloud applications in use (sanctioned applications as well as shadow and rogue IT)
- Enforce cloud application management policies
- Create and enforce granular policies to govern the handling of sensitive information, including compliance-related content
- Encrypt or tokenize sensitive content to enforce privacy
- Detect and block unusual behavior indicative of malicious activity
- Integrate cloud visibility and controls with existing security solutions

DLP in the cloud

Data loss prevention technology (also known as *data leakage prevention* technology) is designed to stop data being used or located where it shouldn't be. The technology has been available for a

long time and used with varying degrees of success. DLP vendors use the concepts of data at rest, data in motion, and data in use to structure DLP architectures.

TECHNICAL STUFF

DLP uses a "content + context" approach to managing data. DLP systems analyze the data within a document (DLP works almost exclusively on unstructured data) to determine its content, analyze the context (location, user, system, and process, among other attributes), and then apply controls determined by policies implemented by the security team.

TIP

DLP can be found in a wide variety of products, so it can help to think of DLP as a capability rather than a market. DLP capabilities of increasing competence can be found not only in enterprise DLP suites, but also within SaaS and IaaS environments as native controls, and in secure web and email gateways, CASBs, and firewalls.

With organizations increasingly adopting distributed managed cloud applications, it becomes ever more difficult to gain visibility and control over data in the cloud, whether at rest (stored data), in use (data open by a user), or in motion (data moving between locations). The ability to protect all three data states is essential to prevent data breaches — especially when data is moving in third-party clouds.

In the modern environment, DLP must now also become a cloud function in addition to on-premises to provide visibility and protection for sensitive data in SaaS/IaaS applications. This is also necessary to protect an organization's sensitive and critical information from cyberattacks, insider threats, and deliberate or accidental exposure.

REMEMBER

Cloud-native DLP can be highly effective because the cloud service providers (CSPs) themselves have the best access to, and ability to perform operations on, the data they're storing. Third parties are limited by the application programming interfaces (APIs) that the CSP provides, and some provide nothing.

Cloud-native DLP provides a subset of functionality to CASB solutions that can work in lockstep to protect data in the cloud. Any cloud use must be protected by a combination of CASB's inherent functionality and support for APIs to multicloud-native DLPs.

TIP

Cloud-based DLP is a primary CASB function. Business rules classify and protect confidential and critical information, and they deploy the required security controls so that users can't accidentally or maliciously share data.

Remote Browser Isolation

RBI moves the execution of a user's browser activity from the client device to a remote server — hosted on-premises or in the cloud. This protects against browser-based security exploits and provides a means of anonymous browsing and risk-free open Internet access.

As the user browses the public Internet, the remote browser is isolated from the user's physical endpoint and enterprise network. Therefore, any attacks on the remote browser session are constrained to the virtual environment. Every browser session runs in an isolated environment that prevents any compromise from infecting the user's working environment. Attacks at the browser level are expected, but when using a remote browser, attacks can't reach other systems and can't persist. This removes the threat because sessions are reset after each use.

RBI also helps in DLP, especially in the case of unmanaged/untrusted devices being used to access confidential or sensitive information. Instead of allowing the unmanaged devices to download the information/files, the system downloads the sensitive information to the remote/isolated browser instance. The unmanaged/untrusted devices only see a visual rendering of the data.

RBI can be implemented in two ways. One is as a primary means of protection, where it renders all sites using RBI, with other filtering (mainly site categorization) applied as needed. The other is as a feature of a traditional web proxy, where it renders sites selectively using RBI based on the site's reputation. Here's how that works:

- User sessions are scanned for risk based on URL filtering and categorization.
- Risky websites are rendered on a remote browser.
- Sanitized pages (primarily image files) are rendered on the user's browser.

As shown in Figure 4-4, RBI takes a selective content disarm and reconstruction (CDR) approach to web browser sessions. An RBI feature typically operates in one of two ways:

- By rendering an image of a web page in the user's browser using a plug-in or an HTML5 rendering
- By extracting readable information from a web page's HTML and reconstructing it in the user's browser

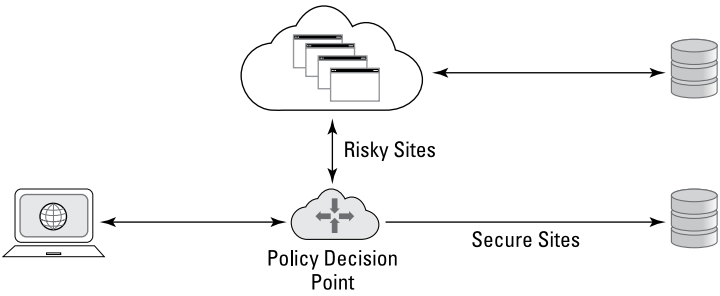

FIGURE 4-4: RBI in action.

User and entity behavior analytics

UEBA uses packaged analytics to evaluate the activity of users and other entities (such as hosts, applications, network traffic, and data repositories). UEBA discovers threats and potential incidents, commonly presented as activity anomalous to the standard profiles and behaviors of users and entities across time and peer group horizons.

REMEMBER

The most common use cases that enterprises seek are threat detection/response and insider threat detection/response (mainly compromised insiders but sometimes malicious insiders as well). Other use cases could include monitoring for unauthorized data access and movement, suspect privileged user activities, and malicious or unauthorized employee activities. UEBA also monitors unusual cloud resource access and usage and supports better detection from existing security technology investments — for example, CASB and identity and access management (IAM).

UEBA solutions are also sometimes used for non-cybersecurity-centric use cases such as fraud or employee monitoring. However, these often require non-IT and non-security data sources, or specific analytics models derived from deep domain expertise.

Where SWG systems use identity to apply point policies, a UEBA system expands the policy scope to apply context-based policy (see Figure 4-5). The determination of whether a user may legitimately access data depends not only on the user's access permissions, but also on the user's historical behavior.

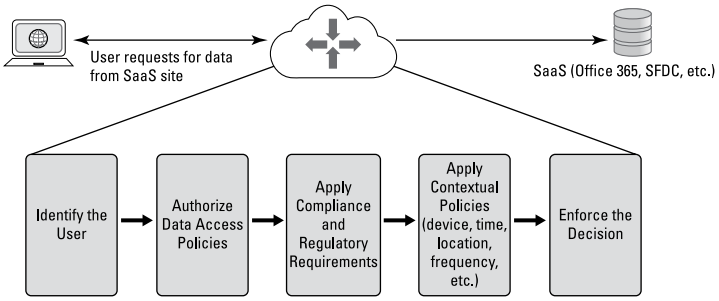

FIGURE 4-5: UEBA enables context-based policy.

UEBA systems detect anomalous behavior based on past history, and this detection enables intelligent access decisions. For example, if a user frequently tries to access files containing sensitive information, the system may block the user and notify administrators, whereas the system may permit a user to access a single file one time.

Fine-Tuning Access Management

When a user is redirected to a SASE gateway for application access, the SDP gateway again performs device and user authentication and verifies the location of the request.

After authentication, the SASE gateway receives authentication tokens for the user on behalf of the application. Token examples include SAML assertions, NT LAN Manager (NTLM) tokens, Kerberos tokens, and the basic username/password fields of the application request. The SASE gateway may provide an SSO user experience for any application by acting as an identity broker for the user.

Sensitive data protection

A SASE solution should understand the context of the data/applications being accessed and be able to take adaptive actions such as blocking sensitive data upload/download when detecting excessive risk.

TIP

A critical evaluation criterion is the richness in how sensitive data policies are defined. It's necessary to inspect data using APIs in order to understand the data context and apply useful policies (such as encryption or watermarking) as data leaves the cloud.

SASE enables security teams to deliver a rich set of secure network security services in a consistent and integrated manner to support digital transformation and workforce mobility.

Mitigating malware

Adopting SASE improves soft-perimeter security to users, devices, and applications regardless of location. In SASE solutions that support content inspection (identification of sensitive data and malware), they can inspect any access session and apply the same set of policies. For example, a SASE system could scan for sensitive data in Salesforce, Facebook, and cloud-hosted applications using a single policy that is applied consistently regardless of where the user/device is located. Ideally the SASE system should be able to inspect content for both sensitive data and malware in a single pass.

Further, where applied by policy, the inspection capabilities applied are consistent regardless of what the entity is accessing. For example, the SASE system can inspect content across all connections for sensitive data and malware.

REMEMBER

SASE solutions should understand the context of the data — whether the content is sensitive or malicious. Data context is critical to setting policies on access, understanding and prioritizing risk, and adapting access policies accordingly. Solutions that don't have this context are limited in their capability to make rich context-aware adaptive SASE decisions.

IN THIS CHAPTER

- Enabling digital transformation
- Centralizing management and control
- Delivering consistent corporate policies
- Saving time and money
- Evaluating a real-life SASE enterprise

Chapter 5
Capitalizing on SASE

Chief information officers (CIOs) of modern enterprises need exemplary client-to-cloud experiences that are secure, reliable, scalable, and simple. That's exactly what SASE delivers.

In this chapter, you learn about how to draw out the best advantages from your secure access service edge (SASE) solution, how SASE helps you through the digital transformation of your organization, how you manage it, how to protect your assets, and how to drive down costs.

Understanding How SASE Enables Digital Transformation

SASE enables enterprise-wide digital transformation with client-to-cloud security, a cloud-native approach, and horizontal elasticity, as shown in Figure 5-1.

Gone is the time when employees all worked in a physical building and all corporate resources were held in a private data center — both physically and digitally secured. Traditional IT infrastructure is unsuitable to support and secure cloud-hosted applications, Direct Internet Access (DIA), non-IT-managed user

devices, work-from-anywhere (WFA)/mobile users, bandwidth-intensive and delay-sensitive voice and video applications, and unsecured Internet of Things (IoT) devices. Organizations seeking to employ these technologies and architectures must make the leap into digital transformation.

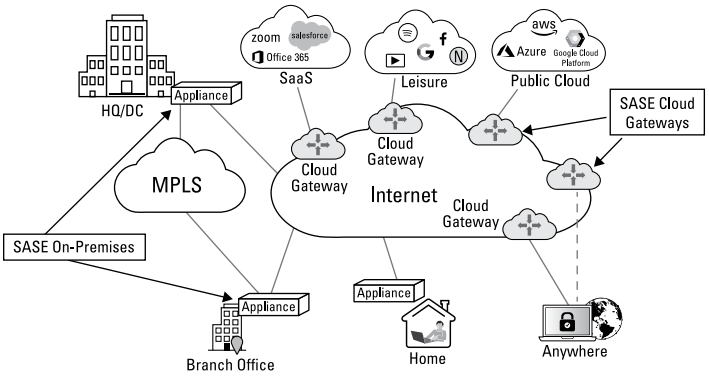

FIGURE 5-1: An integrated SASE enterprise.

Transforming networks and the business environment demands modern-day capabilities such as multicloud readiness, comprehensive embedded security, scalable advanced routing, traffic-steering optimization and remediation, and sophisticated visibility and analytics.

REMEMBER

Software-defined wide area network (SD-WAN)/SASE architectures that integrate all these functions are the only viable approach to support the trends and technologies inherent in the modern era of digital transformation.

Multicloud implementation

Multicloud environments have become increasingly common by encompassing multiple software as a service (SaaS), infrastructure as a service (IaaS), public clouds, and on-premises clouds. This network model provides benefits such as avoiding vendor lock-in, minimizing costs, and enhancing disaster recovery options. But it comes with challenges of security and data protection.

SASE infrastructure eliminates these multicloud interconnectivity challenges by automatically discovering — and seamlessly establishing — dynamic overlay connectivity for both the data and control planes to each cloud. The connectivity

topology is automated and ready in minutes — fully secured with encryption — and the control plane across the disparate clouds is normalized by the tunnel mesh to provide complete global visibility of the network.

Cloud-native and flexible

A SASE solution is cloud-native, built on cloud principles for flexibility and automation. Cloud elasticity allows users to enjoy highly consistent, predictable quality of experience (QoE) without the risk of services slowing down, failing, or becoming unavailable.

Resources are automatically provisioned — with the end user unaware of the process. This significantly simplifies IT tasks to allow staff more time to focus on their core business.

Managing with Confidence

SASE operates from the cloud to deliver all network and security capabilities in a single unified framework.

An SD-WAN with SASE removes the administrative burden of procuring, installing, configuring, and managing individual appliances, enabling security teams to streamline management of all network and security operations through a single solution and a cohesive policy. In the following sections, we outline some of the management benefits SASE provides.

Faster administration and deployment time

With the right SD-WAN-with-SASE architecture, most of the deployment and monitoring is automated. After comprehensive policies are set, the network's configuration and deployment activities happen automatically.

A true SASE solution also improves network reliability and performance in conjunction with SD-WAN features. It does this by being application-aware, monitoring traffic patterns, dynamically steering traffic, and optimizing transport path selection. These capabilities ensure all applications — especially voice and

video — run seamlessly and reliably to deliver uninterrupted services and maximize user QoE.

The globally distributed system of SASE-capable cloud gateways extends enterprise deployments to seamless cloud access, whether they're enterprise, service provider, or vendor provided. Cloud gateways are available in many global locations at the doorstep of nearly every cloud service. Leading-edge cloud gateways interconnect with one another using traffic-engineered middle-mile technologies or public cloud backbones such as Azure or Amazon Web Services (AWS).

Single-pane visibility

Managing your network with confidence requires full operational visibility. A SASE architecture offers user, application, and device views across the entire enterprise: on-premises, in private and public clouds, or Internet-connected, as shown in Figure 5-2.

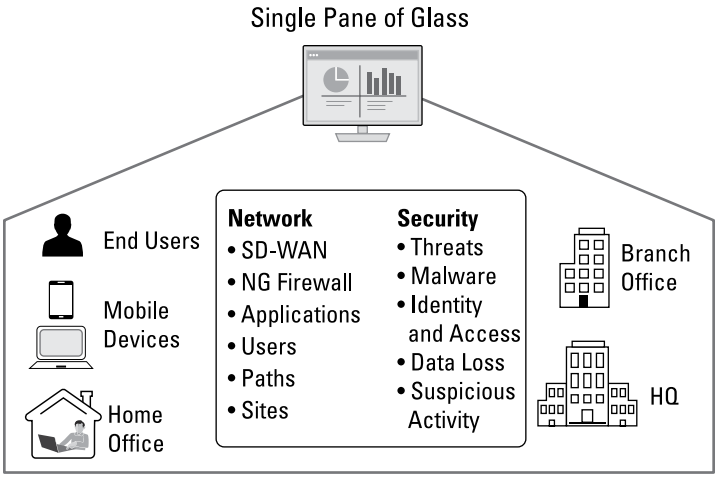

FIGURE 5-2: One console for visibility and control.

REMEMBER

Legacy network views focused on IT-managed devices and data center and branch sites, whereas digitally transformed SASE architectures focus on devices, users, and applications.

Complete control over users, applications, and devices

An SD-WAN/SASE architecture provides visibility into application performance, application connectivity issues, control plane issues such as denial-of-service (DOS) attacks or protocol storms, rogue traffic flows, and underlay or overlay issues.

The system automatically classifies application traffic to provide QoE and filters out unsanctioned applications. This readily available application security information helps IT staff make appropriate policy changes, minimize security risks, derive critical insights, troubleshoot faster, and make better-informed decisions, as shown in Figure 5-3.

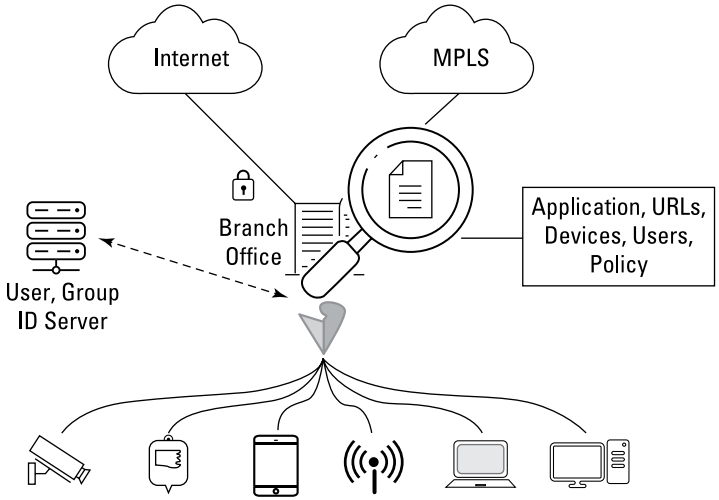

FIGURE 5-3: Managing users and devices.

Protecting Your Assets

SASE enables security teams to bring cloud platforms, data centers, branches, and WFA/mobile users under one umbrella and protect them with a coherent security policy pushed to every user on any device, anywhere. SASE security policy focuses on the dynamic identity-and-access context rather than old fixed trusted/untrusted network boundaries.

TIP

Central control of security policies helps eliminate fragmentation, blind spots, and policy misconfigurations.

Here are some of the ways that SASE can help protect your assets.

Better security and compliance

For many enterprises, maintaining security hygiene and regulatory compliance with data privacy and security standards starts with keeping track of what sensitive information is held about customers and then developing rules to guard access to that information.

SASE enforces compliance by ensuring that only individuals with the right credentials can access secure systems and databases with sensitive customer data. Role-based access control (RBAC) policies are consistently applied and user and entity behavior analytics (UEBA) systems track access and actions within the system with logs and audit trails.

The visibility and control of a SASE framework lowers the likelihood of a data breach by shrinking the attack surface and limiting lateral movement. Data breaches harm a company's reputation, undermine customer trust in an organization, and imply perceived negligence in protecting customers' privacy and security.

REMEMBER

A SASE solution offers a simple way to protect data and meet compliance requirements with identity-controlled access.

Inline encryption

Encryption is vital in modern networks to guard data in transit. Virtual private networks (VPNs) have long been used for this purpose, but encryption/decryption is compute-intensive and may impair application performance. Statically defined VPN tunnels in legacy networks may result in poor traffic-steering choices.

Leading SASE solutions include options for software and hardware-accelerated encryption that provide faster processing and tamper-resistant key storage.

REMEMBER

In a dynamic software encryption architecture, the system must protect keys by never sending them in the traffic path.

To ensure both security and good QoE, encrypted tunnels in the SD-WAN overlay network must be automated, dynamic, and flexible in how they're set up and torn down.

Isolation and segmentation

A SASE solution delivers security through network isolation, segmentation, and multitenancy. Segmentation slows a data breach, because the attacker must break out of one network segment to access resources in other segments. A layer of separation between different servers with sensitive data reduces the risk of data loss/theft and the scope of corporate damage.

Driving Down Costs

Installing disparate, proprietary point products in branch locations is costly, results in sprawl, is complex to manage, and neither enables WFA nor optimizes cloud access. A SASE architecture — with all network and security capabilities embedded in a single software stack — reduces capital investment, allows IT staff to focus on strategic work, and enables a coherent security policy deployment.

Cost savings delivered with a SASE architecture include

- **Bandwidth cost savings:** DIA along with SASE-capable cloud gateways significantly reduce traffic congestion via hubs, data centers, and VPN aggregators in legacy networks. SASE removes centralized security inspection and distributes policy enforcement across the global network.
- **Network management and IT staff cost savings:** A legacy network service-chains several security and routing appliances at each site. SASE consolidates all networking and security in an automated, multitenant, cloud-native software stack with single-pane-of-glass orchestration, eliminating cost, complexity, and the coordination of configurations among vendors.
- **Security cost savings:** Multicloud environments and a WFA workforce using DIA have enlarged the enterprise's attack surface. Breaches are damaging and expensive. SASE uses a zero-trust network access (ZTNA) approach to clouds, DIA,

unmanaged client devices, IoT, data centers, branches, and WFA users, and protects it all with a dynamic, unified security policy for every communications session. ZTNA provides adaptive, identity-aware, precision access. ZTNA improves the flexibility, agility, and scalability of application access, enabling businesses to thrive without exposing internal applications directly to the Internet, reducing the risk of attack.

- **Scalability cost savings:** Extending networking and security to new locations in a legacy network is costly. Common tasks include provisioning commodity products, setting up VPNs for remote employees, upgrading VPN aggregators, and ensuring (often manually) that disparate security configurations don't conflict or have loopholes. A SASE architecture offers easily scalable networking and security capabilities directly in the cloud, implements a central cohesive security policy, and distributes it automatically.

Considering a Real-Life Enterprise Use Case

Acme Bank's traditional wide area network (WAN) architecture, shown in Figure 5-4, no longer reflects how their customers interact with bank services. Cafes are becoming financial hubs. Customers cash checks and make deposits using mobile devices. Bank associates interact with customers on tablets when consulting on financial needs and accounts. Some of the applications have moved to the public cloud, and the bank has started using SaaS for customer relationship management (CRM) and enterprise resource planning (ERP) systems. The bank must also

- Reduce dependence on carriers
- Shorten provisioning time for new locations by using broadband, Long Term Evolution (LTE), and 5G
- Ensure secure access for customers and employees
- Improve application performance
- Provide ZTNA to applications in the public cloud and to SaaS applications

- Allow secure WFA access to applications in the public cloud, SaaS, and some "approved" Internet-based services
- Improve failover of all applications and phone systems
- Gain visibility and control over users and devices

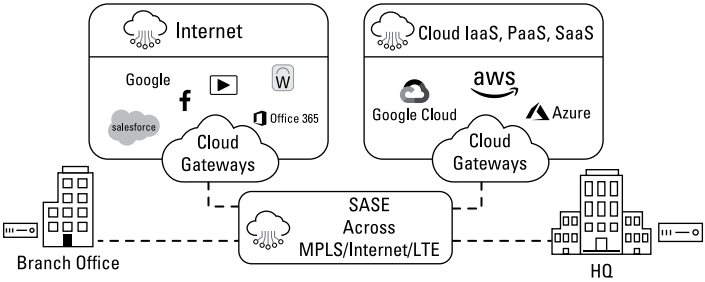

FIGURE 5-4: Acme Bank architecture.

Acme Bank chose a SASE architecture deployed on a single, multifunction platform with cloud-native service, routing, SD-WAN, multilayered security, and UEBA — simplifying its infrastructure footprint for both on-premises and cloud, lowering its costs, and automating management.

The bank is also rolling out — in record time — connections to home offices, conference locations, and road shows, with fast, reliable, and secure SASE services. All the core SASE functions such as WAN edge, secure web gateway (SWG), next-generation firewall (NGFW), stateful firewall, Uniform Resource Locator (URL) filtering, data loss prevention (DLP), intrusion prevention system (IPS), intrusion detection system (IDS), antivirus, Internet Protocol (IP) filtering, file filtering, cloud access security broker (CASB), Remote Browser Isolation (RBI), anti-malware, lateral movement detection, and Secure Sockets Layer (SSL) proxy are thoroughly integrated in the cloud-native SASE service augmented by on-premises customer premises equipment (CPE)–based services.

IN THIS CHAPTER

- Understanding SASE architecture
- Reaping the benefits of single pass
- Future-proofing your enterprise

Chapter 6
Evaluating SASE Best Practices

Secure access service edge (SASE) is both an architecture and an implementation. It's crucial to evaluate different implementations to ensure you select an architecture that can deliver the security benefits you expect while at the same time providing the scale and performance you require.

In this chapter, you find out about SASE architectural attributes; the benefits of having a single-pass, multitenant software implementation; and how to plan a SASE implementation to satisfy today's and tomorrow's requirements.

Comparing Architectures

A good SASE architecture requires several key attributes, including the following:

- It must coexist in any existing network and infrastructure, which means it should be deployable in any *brownfield* (mixture of new and existing/legacy systems) environment.

- It must be built with a solid, secure architecture with the flexibility and scalability required to be deployed in any cloud environment — Equinix, Amazon Web Services (AWS), Azure, Google Cloud, Alibaba, and many others.
- It must support running in containers/microservices or bare-metal devices with the ability to scale out for maximum performance.
- It must be cloud-native, multiservice, and multitenant capable.
- It must have centralized management with distributed security enforcement, providing policy enforcement via strategically placed globally available points of presence (PoPs).
- It must use the security policy enforcement point that is closest to the user/device from which the application access is being made.
- It must have a battle-tested, effective, and intrusion-resistant security stack that provides a multitude of classification and detection capabilities and policy enforcement mechanisms.
- It must combine software-defined wide area network (SD-WAN), routing, and encryption with security capabilities to deliver the best user/application experience while also enforcing all aspects of security.

TIP

Flexibility and choice are core considerations for a good SASE implementation.

Balancing technological and operational needs

Organizations must constantly balance technology needs against operational needs. The complex legacy branch office architecture shown in Figure 6-1 results from building one technology solution on top of another as new technology requirements pop up: wide area network (WAN) optimization, next-generation firewall (NGFW), unified threat management (UTM), SD-WAN, and Long Term Evolution (LTE) access solutions.

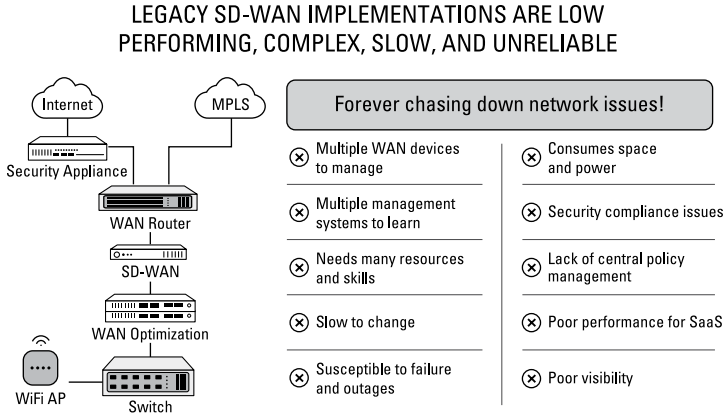

FIGURE 6-1: Legacy branch office hardware.

Over time, IT staff may become hesitant to change anything in the architecture, because it is somewhat working and would be difficult to fix if the prospective change broke some functionality. However, this somewhat-working status quo comes at an immense cost in complexity and inefficiency.

TIP

What is needed is a much simpler architecture that is efficient in both capital expenses (CapEx) and operating expenses (OpEx). Not having multiple devices to manage means you also don't have to learn multiple management systems or maintain skills on multiple products.

Depending on factors such as the size of the organization, the complexity of the infrastructure, security requirements, and the global footprint, organizations should consider a do-it-yourself SASE implementation, SASE services offered by a service provider, or a combination of both.

REMEMBER

Because of the inherent pervasiveness of SASE deployments, the SASE architecture must provide scalability not only for the data plane, but also for the control and management planes. This enables large network and security operations teams to effectively provide SASE services for a large number of tenants at scale, while also providing hybrid operational models where aspects of the services are comanaged by both the service provider and the organization.

The challenges of bolting on security

Bolting multiple solutions onto one another to craft a SASE solution means every individual solution's code base is different and each one has different attack surface characteristics. Such a haphazard architecture is nearly impossible to make highly secure or to demonstrate compliance with standards and regulations.

Additionally, this bolted-on architecture consumes more space and power and performs more poorly. A legacy security solution retrofitted for SASE results in unnecessary hops and steps, security gaps, and exposed vulnerabilities.

Realizing the Benefits of Single Pass

An ideal SASE implementation is a fully integrated single-software stack (like the one shown in Figure 6-2) that does not rely on service chaining or connecting multiple functions/services from different vendors together across multiple devices. SASE solutions from some vendors are functions stitched together from multiple acquisitions or other vendors.

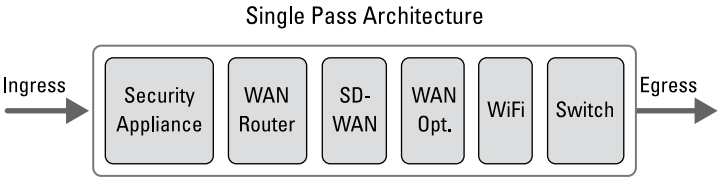

FIGURE 6-2: Data moving through a single pass.

WARNING

The industry has deployed combinations of single-purpose appliances (physical and/or virtual) for years, but this strategy is insufficient to carry you into the future because of processing latency, its unpredictable attack surface, and general complexity. To reduce latency, SASE should inspect traffic using a single-pass architecture where the traffic stream is opened (potentially decrypted) and scrutinized a single time only using multiple policy engines in parallel, ideally in-memory, without requiring chaining of inspection services.

Elastic scale-out


TIP

Top performance is delivered by using a multicore CPU with a single-pass parallel processing architecture. This model achieves an extremely elastic, scalable, and economical SASE implementation.

A high-performance SASE implementation has the following attributes:

- Is multicore and multithreaded
- Supports the Data Plane Development Kit (DPDK) interface
- Efficiently transmits packets without doing a lot of copying or context switching, and bypassing the kernel where possible
- Has a parallel processing and concurrency software architecture
- Does not duplicate functions. Any function is only done once, and its results are leveraged by other functions

Single-software efficiencies

SASE architecture relies on capabilities and features designed from the ground up into a single-software stack that embeds security: secure web gateway (SWG), NGFW, stateful firewall, Uniform Resource Locator (URL) filtering, data loss prevention (DLP), intrusion prevention system (IPS), antivirus, Internet Protocol (IP) filtering, file filtering, cloud access security broker (CASB), Remote Browser Isolation (RBI), anti-malware, lateral movement detection, and Secure Sockets Layer (SSL) proxy, advanced scalable routing, full-featured SD-WAN, WAN optimization, user and entity behavior analytics (UEBA), and more.

Converged SASE (see Figure 6-3) ensures that packets are not flowing separately and independently through each functional module, duplicating effort that results in inefficiency, poor performance, and potential security vulnerabilities.

Security functions must easily integrate with, or be part of, the single-software SASE architecture. Ideally, sophisticated security capabilities should be designed from the beginning into the single-software stack — architected in such a manner that they all operate together as a single entity.

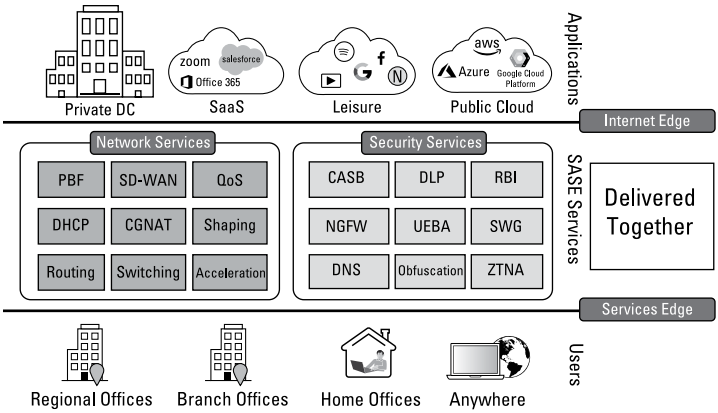

FIGURE 6-3: Converged networking and security services.

A true SASE architecture should

- Have a single, unified management system
- Be optimized for performance
- Be optimized for software as a service (SaaS)
- Contain a single software stack that embeds best-of-breed security
- Be software based and hardware neutral without requiring proprietary hardware
- Require minimum IT staff skills to manage
- Be adaptive and agile
- Be resilient to failure
- Provide full visibility and analytics

Contextual security and contextual access

You must be able to fully understand and segment your users and devices. Doing so requires a multitenancy architecture.

REMEMBER

Cloud-native SASE architectures are almost always multitenant, with multiple customers sharing the underlying data plane. Some providers instead use a dedicated instance per customer, but the architecture may affect the ability to scale. Single tenancy typically results in lower densities, with potentially higher costs that are passed on to the enterprise.

Multitenancy achieves security by keeping one tenant's policies, configurations, logs, and analytics segregated from those of the other tenants. With this architecture, one department's users, devices, and data are protected even if another department — hosted in another tenant — is compromised. This approach significantly limits the scope of damage when there is a breach.

Role-based access control (RBAC) is crucial to achieve contextual security. Within a multitenant environment, security policy configuration allows the right person on the right device to access the right application, and only that.

TIP

Multitenancy ensures isolation between different tenants' data, while RBAC ensures that user privileges govern which application data is accessed by which users within a tenant.

Single-pass and cloud-native advantages

To deliver maximum flexibility with the lowest latency and resource requirements, a cloud-native single-pass architecture is advantageous. A well-designed implementation performs the majority of services in parallel (single pass), ideally in the same cloud-service stack, at the same location, at the same time. The need to open, parse, and re-encrypt and forward traffic should happen only once. This avoids expensive, high-latency packet copying and service inconsistency.

WARNING

Disjointed solutions bolted onto each other provide neither the network visibility and control needed to protect users and devices, nor the administrative tools to comply with industry standards and government regulations/laws.

Planning for Scale, Performance, and the Future

Organizational planning must include not only today's business environment, but also a path to the future. A future-proof SASE architecture must support a new wave of technologies such as Internet of Things (IoT) devices, bring-your-own-device (BYOD) devices, smart manufacturing, augmented reality (AR), virtual reality (VR), and unified communications as a service (UCaaS) that come with their own security and connectivity challenges.


TIP

Any SASE solution you select today must be able to scale and perform for years to come, as well as provide security for new technological and business developments, such as 5G, that require exponentially more processing power.

IN THIS CHAPTER

- Benefitting from better security
- Finding the scale and performance you need
- Supporting the latest technologies and standards

Chapter 7
Ten Things to Look for in a SASE Solution

It is important to evaluate different secure access service edge (SASE) solutions to ensure that you select an offering that can deliver the security benefits you expect while simultaneously providing a single pane of glass and the scale and performance you require. Here are ten important things to look for in a SASE implementation:

- **Implementation delivery options** should include via the cloud, on-premises, or a combination of both, to any location or device for any application type. A cloud-based delivery model should be capable of dynamically adding new services or more compute power to the stack.
- **A low-latency, high-performance single-pass parallel processing architecture** within a single software stack that includes all or most of the core SASE functions such as wide area network (WAN) edge, secure web gateway (SWG), next-generation firewall (NGFW), stateful firewall, Uniform Resource Locator (URL) filtering, data loss prevention (DLP), intrusion prevention system (IPS), intrusion detection system (IDS), antivirus, Internet Protocol (IP) filtering, file filtering, anti-malware, lateral movement detection, and Secure Sockets Layer (SSL) proxy. There should be no requirement for service chaining to combine services.

- **A distributed system of cloud gateways** around the globe to cover existing or new users and applications. It should have cloud gateways that interconnect via a traffic engineering protocol. This guarantees the best application quality of experience (QoE) by choosing the optimal path to software as a service (SaaS), cloud providers, and remote sites based on end-to-end service-level agreements (SLAs).
- **A single management console** to configure, maintain, and monitor the system globally with visibility into sites, services, applications, users, and devices.
- **A future-proof design and architecture** that supports standard protocols, flexible application programming interfaces (APIs), and integration with existing infrastructure.
- **Scalable packaging, elastic pricing, and a growth model** (pay-as-you-grow/shrink) with a multitenant cloud and on-premises design.
- **Support for integrated DLP as a cloud function** in addition to an on-premises function to provide visibility and protection for sensitive data and APIs to multicloud environments. A cloud-native DLP can be highly effective because the CSPs themselves have the best access to, and operations on, the data they're storing.
- **Integrated user and entity behavior analytics (UEBA) functionality** that provides analytics to evaluate the activity of users and other entities such as hosts, applications, network traffic and data repositories. UEBA enables you to discover threats and potential incidents by identifying activities that are anomalous to standard profiles and user behaviors. UEBA should facilitate enterprises with threat detection and response, as well as insider threat detection and response (mainly compromised insiders; sometimes malicious insiders).
- **Support for Remote Browser Isolation (RBI)** with a selective content disarm and recovery approach to web browser sessions. Support for selective use of RBI can enable more restrictive URL reputation policies for high-sensitivity environments.
- **A cloud, hardware, and transport independent architecture** with support for the Internet of Things (IoT), 5G, artificial intelligence (AI), machine learning (ML), and adaptability to other emerging technologies.

Protect enterprise networks with cutting-edge solutions

Secure access service edge (SASE) brings trustworthy security to the peril-fraught modern enterprise network landscape. Its capabilities extend far beyond legacy security architectures, incorporating identity, trust, and context regardless of the connection, user, device, or application. In this book, you discover what SASE includes, how enterprises and organizations benefit, how it supports security, how to best implement it, and how to take advantage of its best features.

Inside...

- Understand SASE features and requirements
- Protect the network perimeter
- Optimize security and performance
- Decrease cost and complexity
- Deliver a consistent experience
- Centralize management and control

Kumar Mehta is a product visionary who has led multiple blockbuster networking and security products. **Apurva Mehta** is an engineering luminary who has developed industry-leading products in networking, security, and packet-core that have created billion-dollar revenue streams.

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

ISBN: 978-1-119-80629-5
Not For Resale

WILEY END USER LICENSE AGREEMENT

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