Definitive Guide™

to

Secure Access Service Edge (SASE)

Unifying Security and Networking for a Work-from-Anywhere World

Karen Scarfone

Compliments of:

SONICWALL®

FOREWORD BY:

Atul Dhablania

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era in a work reality where everyone is remote, mobile and unsecure. SonicWall safeguards organizations mobilizing for their new business normal with seamless protection that stops the most evasive cyberattacks across boundless exposure points and increasingly remote, mobile and cloud-enabled workforces.

The cost of conventional security is more prohibitive than ever, and the shortage of trained personnel makes the problem exceptionally acute. Constrained budgets and staffing resources simply can't keep up. This creates a growing cybersecurity business gap, which is unbridgeable with conventional security approaches.

By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide.

Boundless Cybersecurity empowers organizations to break free from untenable economic, technical and staffing constraints of traditional or outdated approaches — all with less cost and human intervention than conventional security.

For more information, visit www.sonicwall.com.

Definitive Guide™

to

Secure Access Service Edge (SASE)

Unifying Security and Networking for a Work-from-Anywhere World

Karen Scarfone

Foreword by Atul Dhablania

CYBEREDGE PRESS

Definitive Guide™ to Secure Access Service Edge (SASE)

Published by:
CyberEdge Group, LLC
1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
(800) 327-8711
www.cyber-edge.com

ISBN: 978-1-948939-19-5 (Paperback); ISBN: 978-1-948939-18-8 (eBook)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Graphic Design: Debbi Stocco
Special Help from SonicWall: Sony Kogin, Anusha Vaidyanathan, Kayvon Sadeghi

Table of Contents

Foreword

Like it or not, perimeter security is being redefined. Work-from-anywhere, BYOD, and mobile technologies have radically changed user behavior, while cloud technology adoption has changed how users are served. Most organizations still have a perimeter that needs to be secured, but they also have many assets outside that perimeter that need to be protected no matter where they are.

At the same time, networking is also evolving as remote workers need direct access to public cloud-based services. Such direct access eliminates the bottlenecks that arise from forcing all employee traffic through the organization's perimeter and then out to its final destination, otherwise known as backhauling or hairpinning. The same applies to branch sites that use MPLS to send all traffic through the centralized perimeter security instead of directly to its destination. MPLS-based WANs are also expensive compared to direct internet access.

What's important is that your organization's security perimeter should follow your employees regardless of where they work, and it should extend to wherever your assets reside. This is where secure access service edge (SASE) solutions can help.

SASE brings together security and network technologies in a cloud-delivered, secure, network-as-a-service solution. With SASE, security and network services are easy and quick to deploy, manage, and use. SASE enables secure access to your organization's technologies, regardless of their location, e.g., your branch sites, your individual users, and your business partners.

Your organization can gain a lot of advantages by using SASE. It empowers your workforce by enabling them to work from anywhere using the devices and client software they choose. It cuts through the complexity of security and network infrastructure administration, allowing you to focus on core innovative projects.

Another major benefit of SASE is flexibility in obtaining a secure network-as-a-service that organizations never had before. Using SASE, new branch sites that previously required long lead times can now be connected to your enterprise on demand. Workers can utilize self-service features to get up and running in just a few minutes.

In this guide, you'll learn the basics of SASE. It's a relatively new concept that's still evolving, so this guide provides a high-level picture. As the finer details of SASE emerge, you'll be ready to add them to the picture you already have. This guide will help you to understand why SASE is important and how your organization can start adopting it.

We at SonicWall hope that you will find this book illuminating and practical. If you have any questions about this book, or if you want more information on how other organizations are starting their SASE transformations, feel free to contact us.

Atul Dhablania

Senior Vice President and Chief Operating Officer
at SonicWall

Introduction

In the past few years, there's been a huge shift toward work-from-anywhere technologies and increased adoption of cloud-based services and applications. With the exodus of technology from organizations' headquarters and data centers, the old network perimeter-based security models have largely degraded and crumbled.

This has left a void that must be filled swiftly. Organizations need to regain control over their technology, but not at the expense of halting progress or preventing employees from making the best possible use of technology assets.

The answer to this dilemma is secure access service edge (SASE), a holistic portfolio of cloud-based security and networking capabilities. SASE uses a set of components, including zero-trust network access (ZTNA), firewall-as-a-service (FWaaS), and software-defined wide area network-as-a-service (SD-WANaaS). Together, the SASE components offer a unified solution that provides numerous benefits for any organization.

This book is meant for anyone with a role in security or networking, whether an administrator, manager, or executive.

Chapters at a Glance

Chapter 1, "Losing Control and Trust in the Cloud Era," explains how recent changes in technology needs, networking, and security have changed the landscape.

Chapter 2, "Regaining Control Through SASE," explores how SASE merges security and network services, and recommends a modular approach to implementation.

Chapter 3, "Making the Business Case for SASE Adoption," describes how SASE can provide agility and flexibility for your business, empower your employees, simplify your operations, and evolve your security.

Chapter 4, "Securing Access with Zero-Trust Network Access (ZTNA)," explains zero trust, ZTNA, and software-defined perimeters (SDPs), and also reviews real-world case studies of ZTNA deployments.

Chapter 5, "Inspecting Traffic with Firewall-as-a-Service (FWaaS)," discusses the benefits of using FWaaS instead of on-premises firewalls.

Chapter 6, "Improving Connectivity and User Experience with Software-Defined WAN-as-a-Service (SD-WANaaS)," explains why SD-WANaaS is a major improvement over existing WANs and how it can serve as an on-ramp to a full SASE implementation.

Chapter 7, "Selecting a SASE Solution," looks at several factors to keep in mind when evaluating potential SASE solutions for your organization.

Helpful Icons

Tips provide practical advice that you can apply in your own organization.

When you see this icon, take note as the related content contains key information that you won't want to forget.

Proceed with caution because if you don't it may prove costly to you and your organization.

Content associated with this icon is more technical in nature and is intended for IT practitioners.

Want to learn more? Follow the corresponding URL to discover additional content available on the Web.

Chapter 1

Losing Control and Trust in the Cloud Era

In this chapter

- Understand what's recently changed in organizations' technology needs
- Examine how security and networking have swiftly evolved in just the past few years
- Look at the path forward for using untrusted technology

"We cannot change the cards we are dealt, just how we play the hand."

— Randy Pausch

The Old Security Model

For decades, the network perimeter was a core principle of security. Organizations housed their servers at their headquarters, and employees at HQ accessed those servers from organization-controlled desktop computers over organization-controlled networks. Firewalls and other network security controls at the perimeter protected all of the systems and networks inside.

Remote sites, like branch offices or retail locations, used multi-protocol label switching (MPLS) architectures to provide wide area network (WAN) connectivity to HQ, where all their traffic was routed. This is known as *backhauling*.

Similarly, if individual employees needed remote access, their organization-controlled laptops could connect to virtual

private networking (VPN) appliances on the network perimeter. The laptops' configuration forced all of their network traffic through the VPN so that the organization could monitor it and enforce policies on it.

In short, the organizations were responsible for everything and in control of everything to the extent possible. And then…

Changes in Organizations' Technology Needs

In the last decade, organizations' technology needs have changed – gradually at first, then accelerating more and more, and finally undergoing a sudden transformation because of the COVID-19 pandemic. Whew. Let's recap the most important changes.

Decentralization

For most organizations, the technologies they use are no longer concentrated within their own data centers and offices. They're **everywhere**.

Organizations have migrated their apps, services, and data to numerous cloud service providers. Software-as-a-service (SaaS) versions have replaced many of those apps. Additionally, users often adopt other cloud-based apps and services without the organization's knowledge, better known as *shadow IT*.

The neat and tidy world of organization-issued standard desktops and BlackBerry devices has also disappeared. In its place are an incredible variety and number of client devices, from desktop and laptop computers (mostly laptops) to smartphones and tablets. Some of the client devices are issued and controlled by the organization, but many are bring-your-own-device (BYOD). There's also all sorts of Internet of Things (IoT) devices used in addition to or instead of conventional client devices.

Today's users expect flexibility. They want to be able to work from any of their client devices no matter where they are, not just at the office or at home. The demand for work-from-anywhere capabilities means that organizations must rethink their entire approach to technology.

Expectations

At the same time that technology has become so decentralized, the network bandwidth it consumes has greatly increased. Some of this increase is because the technologies no longer use the same internal network, but usage has changed too. For example, users expect to be able to watch training videos and participate in videoconferences without performance and other quality issues.

Organizations are also recognizing the growing need to improve technology usability. With devices and apps proliferating, users have too many credentials to manage, too many places where their data is stored, etc. They want seamless experiences. Efforts to improve usability often boost performance as well by removing obstacles that slow down and frustrate users and increase the organization's support costs.

Finally, organizations need better agility and scalability to rapidly address emerging needs. They don't have the luxury of waiting for new servers to be delivered or new dedicated circuits to become available, and they can't afford the downtime needed to replace their network security appliances. Adding physical servers, appliances, and circuits to meet transient needs, like seasonal surges, isn't practical either. Fast deployment – in minutes or hours, not weeks or months – is now a must-have.

Changes in Security and Networking

Generally, a change in technology tends to be followed by changes in security and networking to support that technology. Let's look at some of the ways that security and networking have evolved recently in response to increased work-from-anywhere and cloud technology usage.

One thing never seems to change: security threats continue to worsen. Malware, phishing attacks, ransomware, and other types of threats are increasing in response to the growing number of online assets to attack.

The aftermath of data breaches

It seems like every day there's a new story in the media about another data breach. The sheer number of data breaches means that while they're certainly not being ignored, individual breaches tend not to get the attention they used to.

Some breaches, however, are over the top and highlight how little concern some organizations seemingly have for protecting sensitive data. These breaches can tarnish corporate brands and even cause drops in market value. Here are a few examples:

Equifax: In 2017, Equifax revealed a huge data breach that affected roughly 150 million Americans. Five days after the announcement, its stock value had plummeted by 30%. (https://money.cnn.com/2017/09/13/investing/equifax-stock-mark-warner-ftc-probe/index.html)

Capital One Financial: A massive 2019 data breach affecting over 100 million people led to an immediate drop of almost 6% in share price. (https://www.wsj.com/articles/capital-one-shares-plummet-after-breach-11564500956)

Data breaches can have long-term effects on companies. A recent study showed that the stocks of these companies usually underperform the market for years after the breach becomes public. (https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/)

Loss of the perimeter

Today the network perimeter is largely gone. Users, devices, apps, and services are dispersed all over the world. For most organizations, trying to sustain a perimeter-based security architecture for the entire enterprise is no longer feasible.

Forcing remote workers to have all of their network traffic routed to HQ and then immediately back out to reach a cloud-based resource slows things down. Potentially this backhauling could cause major bottlenecks and some outages because too much traffic is trying to enter and exit HQ at times. But not forcing remote workers' traffic through HQ means that the organization's network security controls wouldn't be applied to it. That's a big problem.

Branch sites could face the same problem as remote workers. They would be forced to send all their traffic through their MPLS-based WAN to HQ so that network security controls could be applied. This is both slow and costly. Or branch sites

could have direct internet access (DIA) connections and many of the same network security controls on site as HQ has. This would only be feasible for large branch sites, though, because of the high hardware and software costs for the network security controls.

Losing most of the perimeter means losing the ability to enforce security policies through the network for many or most users and devices.

Loss of control and trust

Organizations are also losing control of devices, networks, apps, and other aspects of the technologies they rely upon. Examples of this loss of control include:

- ☑ The migration of devices from enterprise networks to home networks and other third-party networks
- ☑ The shift from organization-issued devices to personally owned devices
- ☑ The transition from on-premises apps to cloud-based apps
- ☑ The decrease in dedicated circuits between offices

Sometimes the loss of control is partial, like adopting cloud-based apps. In those cases, there's a new shared responsibility model between the organization and the third party providing the technology or technology service. This is yet another change for organizations to accommodate.

Organizations already feel that they shouldn't trust the technologies they **don't** control, but they're also learning they shouldn't trust the ones they **do** control, either. We'll take a much closer look at that in Chapter 4, "Securing Access with Zero-Trust Network Access (ZTNA)."

Increased complexity

The complexity of security seems to know no bounds. There are constantly more devices, apps, data, and environments – which all equal higher complexity and larger attack surfaces. The more complex things are, the harder they are to secure, manage, and monitor.

Correspondingly, organizations need more types of security products and services to try to keep up with increasingly complex security needs. Meanwhile, there's a severe personnel shortage, and staff must learn a different management console for each product and service. On top of that, most of these products and services don't integrate with each other. Their complexity makes integration more and more difficult.

Finally, regulatory requirements continue to increase as technology plays an even more important role in many sectors and industries. More requirements mean implementing more complex security policies.

The Path Forward

Technology has changed, so security and networking need to change in response. The old model of routing all communications through HQ no longer works. Users need direct access to the internet to use cloud-based apps from whatever client device they choose. Trust in networks and devices has been lost. So where do we go from here?

Organizations need to regain control over technology. Since they can't trust client devices, they need to examine their users' network traffic, enforce policies on it, and look for threats. The only way to do that while achieving reasonable performance is to force client devices to send their traffic through cloud-based security services. This is a key principle of secure access service edge (SASE), but SASE is much more than that, as you will see in the next chapter.

Chapter 2

Regaining Control Through SASE

In this chapter

- Explore how SASE merges security and network services into a new type of cloud-based solution
- Study the high-level composition of SASE, and understand its security and networking benefits
- Learn why a modular approach to SASE implementation is recommended

"Start where you stand, and work whatever tools you may have at your command and better tools will be found as you go along."

— Napoleon Hill

Merging Security and Network Services

Most organizations have separate security and network services. Network teams handle routing, quality of service, and other elements of network communications, while security teams take care of all the security functionality for communications, devices, etc.

SASE, pronounced like "sassy," merges security and network services into a single service. The idea is to have an agile and highly scalable solution for regaining control of security while also integrating networking functionality. SASE greatly simplifies what security and network teams have to do. It also provides a better user experience!

SASE isn't a single service or application. It's a holistic solution with many moving parts. Think of SASE as a portfolio of functionality that addresses security and networking in an integrated manner.

Gartner published the first depiction of SASE in 2019. It showed SASE as the convergence of 17 aspects of security and networking. Figure 2-1 shows the components in our current vision of SASE, which builds on the original concept and makes it easier to understand. SASE is still evolving and maturing. Its composition continues to morph, and vendors are in the process of building their SASE offerings and SASE component portfolios.

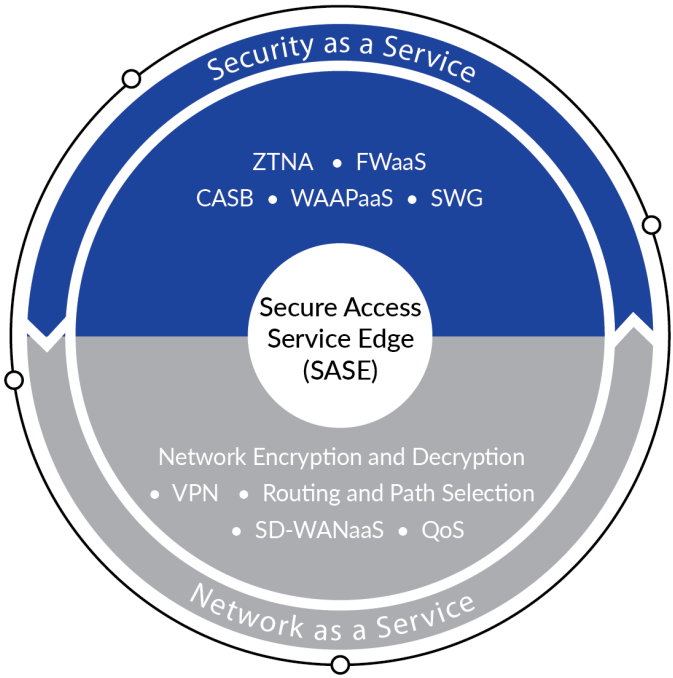


Figure 2-1: Current vision of SASE's components

In this book we don't attempt to comprehensively explore every possible SASE component. SASE is meant to be flexible so that every organization using the basic SASE architecture can incorporate the combination of security and networking services that meets its requirements.

In Chapters 4, 5, and 6, you'll learn more technical details about several of the most commonly used SASE components. For now, we'll keep the discussion at a high level so you understand the big picture before we go deeper.

The birth of SASE

Gartner's 2019 report, "The Future of Network Security Is in the Cloud," explained the research firm's vision for network security. In the report, Gartner coined the term "secure access service edge" and explained SASE this way: "Instead of the security perimeter being entombed in a box at the data center edge, the perimeter is now everywhere an enterprise needs it to be – a dynamically created, policy-based secure access service edge."

The report makes it clear that Gartner expects SASE to become widely adopted in the coming years: "SASE will be as disruptive to network and network security architectures as IaaS was to the architecture for data center design." Core components of SASE are already being adopted by many organizations, and all indications are that SASE will be the next-generation solution for enterprise security and networking services.

High-Level SASE Composition

Every SASE solution involves a cloud-based SASE provider that offers and manages the SASE solution for its customers. SASE solutions are global services with points of presence (POPs) in locations around the world. The POPs provide direct connections to the cloud-based SASE services for individual end users. The POPs can also connect an organization's sites to each other through encrypted tunnels.

SASE architecture

Figure 2-2 shows a notional high-level SASE architecture. In the old perimeter architecture, HQ was at the center. In the SASE architecture, the SASE POPs and services are at the center. HQ and other on-prem resources are outside the center in SASE, just like branch offices, client devices, and public cloud-based resources. The resources communicate with each other through the SASE POPs and services.

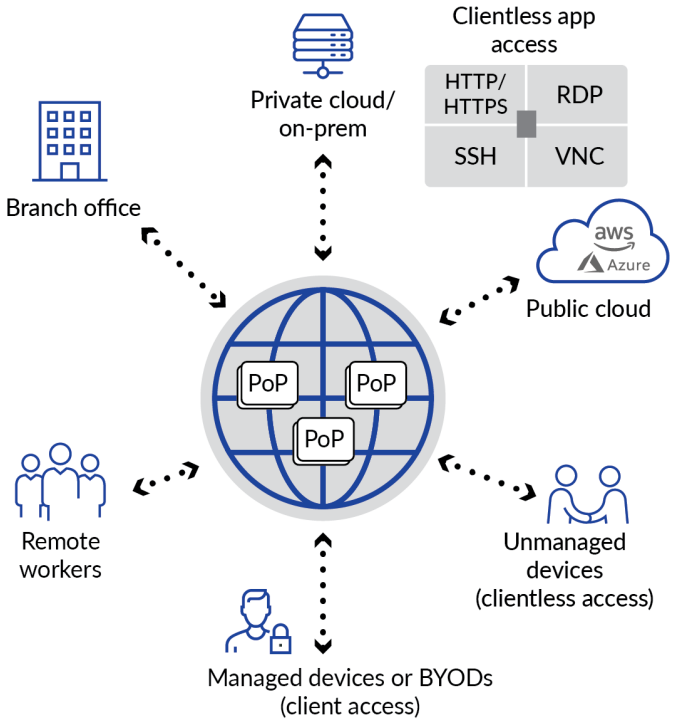


Figure 2-2: Notional high-level SASE architecture diagram

Major SASE functions

Major functions of the SASE services include the following:

- ☑ Deciding which apps and other resources each user should be allowed to access based on authenticating the user and evaluating their client device's characteristics
- ☑ Enforcing security policies for all network traffic between client devices and apps or services
- ☑ Optimizing network connectivity and bandwidth based on the organization's policies
- ☑ Delivering security functions such as distributed denial of service (DDoS) protection

SASE clients

SASE solutions typically offer different levels of support based on the type of client device. Organization-managed client devices usually run SASE client software as an agent. It automatically and transparently connects each device to the cloud-based SASE service, with no user action needed. The SASE service facilitates access for each user to all apps they use for their work (other than any locally installed apps, of course).

Client devices that aren't organization-managed but are controlled by the user, like BYOD, usually run the same SASE client software as the organization-managed devices, and it works the same way.

Finally, for devices used by the public, such as desktop computers in libraries and hotels, organizations may allow clientless access to the SASE service. In this case, the SASE service can be configured to allow access only to particular low-risk apps, and not the full range of apps that can be accessed through SASE client software.

Benefits

Organizations that implement SASE can gain numerous benefits. The following are expected benefits for security, network, and operations teams. Chapter 3 goes into detail on the business case for adopting SASE.

Hardware, software, and staffing reductions

Moving security and networking services to the cloud eliminates many hardware and software costs, such as purchasing network security appliances and security applications from several vendors. The subscription model used by SASE means that services can be scaled up or down on demand without waiting weeks or months for equipment to arrive and dedicated circuits to be installed.

Security and networking teams can efficiently monitor and manage all of the SASE components from a single pane of glass management console, as compared to switching among several consoles without SASE. Greater efficiency, in turn, reduces the hours needed from those employees and can free up skilled experts to work on more strategically valuable projects.

SASE vendors may offer additional services, like continuous monitoring. These can be valuable for smaller organizations that can't afford their own 24-hour staffing.

Improved security and networking performance

SASE allows you to keep many security and networking controls in the cloud instead of having client devices perform them. This avoids having to send potentially large security updates to each client device several times a day. Also, cloud-based controls provide stronger security for BYOD and mobile devices that can't run all the controls that organization-managed devices can.

Because SASE solutions and their components are fully integrated and cloud based, they typically offer stronger security, better reliability, and less latency than their traditional counterparts. SASE architectures have redundancy and DDoS protection built in.

SASE Implementation Approach

Implementing SASE isn't just a matter of subscribing to a solution. SASE requires changes to people, processes, and technology throughout your organization. It's worth the effort. We recommend a phased, modular approach to SASE. Think of it like installing a modular chassis and over time adding service blades, some with capabilities that weren't yet available when you got the chassis.

You'll want to start by adopting ZTNA, then FWaaS, and finally SD-WANaaS. Progress to the next one only when your organization is truly ready. Chapters 4, 5, and 6 provide more information on them.

Chapter 3

Making the Business Case for SASE Adoption

In this chapter

- Learn about the business agility and flexibility that SASE will bring to your organization
- Understand how SASE empowers your employees to do their jobs the way they want to while keeping everything secure
- Explore how SASE can simplify operations, evolve your security, and help ensure compliance with requirements

"They always say time changes things, but you actually have to change them yourself."

— Andy Warhol

Business Agility and Flexibility

To succeed and thrive in today's business climate, organizations need a high degree of agility and flexibility in their technology implementations. This allows them to take advantage of unexpected opportunities and to minimize the impact of negative events, such as the COVID-19 pandemic.

Business agility and flexibility also allow organizations to handle more-routine technology changes rapidly and easily, like moving a branch site from one location to another.

Organizations that adopt SASE can take advantage of the agility and flexibility its cloud-based technologies offer without sacrificing security. Examples of how SASE enables this include the following:

- ☑ SASE eliminates most of the hardware acquisitions and implementations associated with traditional solutions. Adding a new branch site to your organization takes almost no time at all, compared to months of waiting for dedicated circuits and new hardware and software to arrive and be installed.
- ☑ SASE services are easy to consume and lightweight. Self-service options enable new users to get themselves up and running in minutes. Making a new resource available to users involves a single policy change, which immediately enables access to the resource for authorized users only.
- ☑ SASE solutions are subscription-based services. This makes it easy to increase or decrease SASE services as needed.
- ☑ A SASE solution is already supported by points of presence around the world. It can provide immediate, reliable access to your organization's resources from new geographic locations.
- ☑ SASE requires significantly fewer staffing resources than older approaches, so it frees up skilled security staff to support strategically valuable projects.

SASE can be particularly helpful for organizations that are reluctant to migrate their on-premises assets to the cloud. SASE offers a clear plan for taking a journey into cloud computing technologies without sacrificing security.

Employee Empowerment

Employees are increasingly demanding the ability to work from anywhere. They don't want to be restricted to working only from particular locations. They don't want to be forced to use a certain brand or model of client device or an operating system that they don't like. They want the flexibility to work the way that best suits them.

Supporting employees' ability to work from anywhere and to use personally owned devices also provides better resiliency for organizations. During adverse situations, like natural disasters and pandemics, employees may not be able to reach the organization's facilities, potentially for extended periods of

time. Ensuring they can be just as productive regardless of their location can make a huge difference in the bottom line.

By adopting SASE, you can stop saying "no" to your employees and start saying "yes." At the same time you're empowering your employees, you're strengthening your organization's business continuity and disaster recovery practices. You're ensuring that your employees can do their jobs from anywhere at any time.

You're also giving your employees a better user experience. They will have better performance than traditional solutions can provide, and seamless and consistent access to their applications and other resources. SASE is SaaS based, so it's simple and lightweight, and it provides self-service options so users can be up and running in minutes.

Simple, Fast Administration

Organizations typically use a staggering number of security and networking technologies. These technologies also continue to become more complex. In fact, staffing shortages can result when employees are forced to spend so much time learning and using many distinct and complicated management consoles, each one completely different from the others.

SASE brings security and networking functions together in a single pane of glass management console through which security and networking administrators alike can manage, monitor, and maintain all of those functions throughout the organization. This unified console greatly simplifies training and helps alleviate staffing shortages through greater efficiency. In many organizations, transitioning to SASE will eliminate most network administration tasks, allowing scarce resources to be shifted to more strategically valuable purposes.

Administrators will find that SASE gives them agility. When there's a problem, they can find it quickly and respond to it right away. They don't have to waste time trying to figure out which console to check – everything is in one place. Also, when something needs to be updated, like making a new app available to users, it's easy and fast. So is scaling SASE resources up or down as needed.

Security Evolution and Maturity

Security continues to become more and more important to organizations. Businesses need to avoid data breaches, ransomware attacks, and other major security incidents that can damage their reputations and lower their market value. Many organizations must also comply with increasingly stringent security laws and regulations. (This topic is discussed in more detail below in "Compliance Requirements.")

Security challenges also continue to intensify. Threats keep evolving, and it's harder to keep them out of organizations and stop them from causing damage. Also, the number of users keeps increasing at many organizations, as does the number and complexity of the devices and apps each person uses. That means there are always more targets for attackers.

As we've already discussed in Chapter 1, "Losing Control and Trust in the Cloud Era," organizations are also losing their network perimeters and their visibility and control over the technology their users rely upon.

In short, most organizations would benefit from improving and evolving their security practices – making security stronger in spite of many factors trying to weaken it. Adopting SASE is the ideal way to increase the maturity of your security.

Examples of ways that SASE can benefit your organization by improving your security include:

- ☑ Enabling faster responses when security problems happen, which can reduce negative impacts to the business and prevent minor incidents from becoming major ones
- ☑ Restricting access so each user can only access the resources they're explicitly authorized to; this can help reduce data breaches and other incidents
- ☑ Regaining visibility into network traffic by gathering data on network traffic that other security technologies can utilize for attack detection purposes
- ☑ Identifying use of *shadow IT* – unofficial or unauthorized use of applications – and either blocking or protecting each shadow IT instance, as appropriate

- ☑ Being able to continuously monitor the security of client devices, including BYOD, and taking automatic action immediately to prevent compromised devices from negatively impacting the rest of the organization

Effectiveness at stopping common cyberthreats

It's important to consider the effectiveness of any proposed security solution against the threats it will face. Here's a brief description of how SASE solutions could potentially thwart several common types of threats.

Email-borne threats: SASE could provide security services for popular SaaS email applications. These services could include checking each email for known malware, phishing, and other attacks, and executing unknown file attachments in a sandbox and stopping them from being delivered if they appear to be malicious.

DDoS attacks: Since SASE is cloud based with a high degree of redundancy, and it conceals resources from view, it is naturally resilient against DDoS attacks.

Data exfiltration: With SASE, data could remain at rest, effectively preventing exfiltration. For example, policies could be enforced on external users that give them access to a rendered copy of resources, instead of direct access to the resources themselves. In this environment, there's no way a user could gain access to sensitive data and transfer it elsewhere.

Data breaches: SASE could prevent the lateral jumps from system to system that usually lead to a data breach.

Compliance Requirements

There's been some lingering reluctance to adopt cloud and work-from-anywhere technologies, especially in more highly regulated industries where organizations must provide evidence of compliance with numerous security and privacy requirements. Examples include healthcare (the Health Insurance Portability and Accountability Act of 1996, or HIPAA) and retail (the General Data Protection Regulation, or GDPR).

SASE can help jump-start cloud and work-from-anywhere adoption while also supporting compliance efforts. SASE solutions give organizations the visibility, logging, and auditing capabilities they need to demonstrate that their security controls meet requirements, no matter where their devices or apps are located.

In addition, SASE supports a wide range of security controls that protect sensitive, regulated data like personally identifiable information (PII). Here are some examples:

- ☑ SASE encrypts sensitive data being transmitted. With ZTNA there's also an option to keep all data at rest centrally and only send data as graphics.
- ☑ SASE's ZTNA component implements the principle of least privilege to minimize the possibility of unauthorized access to sensitive data.
- ☑ SASE's ZTNA component uses micro-segmentation to protect access to valuable resources and to prevent the compromise of one resource from readily spreading to other resources.

Summary

SASE brings together security and networking technologies. SASE increases your business agility and flexibility. It empowers your employees to work from anywhere, on demand, using the devices they prefer. It also makes technology administration faster and easier, improves your organization's overall security capabilities, thwarts common threats, and helps protect sensitive, regulated data.

The sooner you start working on SASE adoption, the sooner you'll be reaping its benefits.

Chapter 4

Securing Access with Zero-Trust Network Access (ZTNA)

In this chapter

- Understand what zero-trust principles are and why organizations need to adopt them
- Learn the basics of zero-trust network access (ZTNA), how it utilizes software-defined perimeters (SDPs), and why it should be compatible with endpoint security solutions
- Review real-world case studies that demonstrate how ZTNA is already benefiting organizations

"For there to be betrayal, there would have to have been trust first."

— Suzanne Collins, The Hunger Games

The Shift to Zero Trust

In Chapter 1, we examined the loss of the perimeter and the loss of control and trust. Organizations are finding that the best way to address these challenges is embracing the principle called zero trust. Zero trust isn't new, but it's become better developed in recent years. Adopting zero trust means that you start by assuming nothing should be trusted. You build on that by verifying the identity of users, devices, services, and every other entity in the environment, tightly restricting what each can do, and monitoring them to determine if they should still be trusted.

Zero trust is a major departure from the perimeter security model, where it was normally assumed that all users, devices, servers, and networks inside the perimeter should be trusted. A device inside the perimeter could access all sorts of resources inside the perimeter by default. Now not only is the perimeter largely gone, but there's recognition that malicious activity may come from your organization's own users and devices, as well as mistakes that can be detrimental. Where a device is located is irrelevant, and a device that's OK one minute may not be OK the next.

The terms "zero trust" and "zero-trust network access" have different meanings. Essentially, zero-trust network access is one way of implementing zero-trust principles.

The basic tenets of zero trust

NIST Special Publication 800-207, Zero Trust Architecture, defines seven basic tenets that zero-trust architectures should follow:

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.

See the NIST publication (https://doi.org/10.6028/NIST.SP.800-207) for a more technical and academic deep dive into zero-trust principles.

ZTNA Basics

ZTNA is a model for implementing zero-trust principles for networks, specifically for individual users and their client devices. ZTNA is the first fundamental component of SASE. Like SASE, ZTNA is a convergence of security and networking, but ZTNA entails a smaller set of security and networking functionality. As a cloud-based service, ZTNA can be adopted by an organization in mere minutes. ZTNA can also be appliance based. In this guide, we focus on cloud-based ZTNA as part of larger SASE solutions.

With ZTNA, all of the client device's network traffic must pass through the ZTNA solution in the cloud. This traffic is carried through a secure tunnel that protects it from eavesdropping and tampering. The ZTNA solution continuously monitors all of the traffic flows involving each client device for reporting and auditing purposes. Also, if at any time the ZTNA solution detects or is notified that malicious activity is occurring, it can immediately terminate access for the client devices involved.

Before accessing any network-based resources on behalf of the organization, the ZTNA user and their client device must each authenticate successfully. The user and device will only be able to access the resources they are authorized to access – the principle of *least privilege*.

It's also important for the ZTNA solution to be compatible with endpoint security solutions, like endpoint control (EPC) or anti-virus software. Endpoint security can evaluate the current security posture of an endpoint, and ZTNA policies can check that evaluation and allow or deny access to network-based resources based on the risk.

Software-defined perimeters

ZTNA is a model for implementing zero-trust principles. Software-defined perimeters (SDPs) are one way of implementing ZTNA to protect cloud-based resources that remote client devices are attempting to access. When we talk about SASE, we're including SDP-based ZTNA. Many consider the terms "SDP" and "ZTNA" to be equivalent, especially within the context of SASE, but that's not quite right. ZTNA can be implemented through mechanisms other than SDP. It's just not common to do so at this time.

First defined by the Cloud Security Alliance (CSA), a *software-defined perimeter* is a logical perimeter established behind an SDP gateway. Within each logical perimeter are one or more resources that the organization's users may want to access. Each SDP gateway effectively hides and protects the resources within its perimeter.

SDP architecture for ZTNA

Figure 4-1 depicts an example of the logical architecture of an SDP-based ZTNA. The top layer of the diagram depicts the ZTNA users and client devices. The middle layer shows the SDP controller and gateways, which establish and enforce the perimeter. Finally, the bottom layer includes the resources behind the SDP perimeter that ZTNA users and devices may want to utilize.

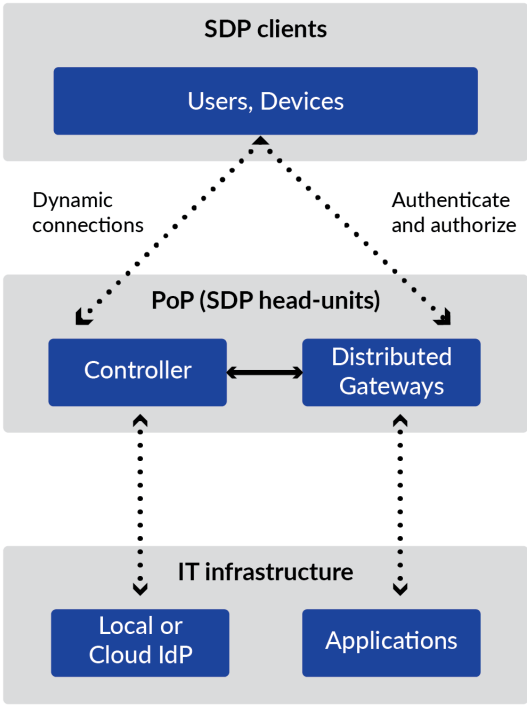


Figure 4-1: SDP-based ZTNA architecture example

When a user and their client device need to use one of the hidden protected resources, the ZTNA solution must first determine if they should be trusted. The SDP controller, which is shown in the middle layer of Figure 4-1, handles the trust verification process. Only after trust is established can the user and client device see and connect to the resource they're trying to use.

This is an important distinction. In traditional perimeter-based architectures, the client establishes a network connection to a server, and then the server attempts to verify the identity of the client. With ZTNA, things work the other way around, which reduces the protected resources' exposure to potentially malicious activity.

Micro-segmentation

With ZTNA the organization can establish many logical perimeters, each behind its own SDP gateway, to achieve micro-segmentation. The resources within each perimeter are logically grouped and don't need to be in physical proximity to the gateway or each other. They could be located anywhere. In any case, the user would have no idea where the resources were or how to access them without going through the SDP gateway.

The ZTNA solution knows which users are connected and which target applications and other resources they are authorized to access. This can greatly reduce the risk that unauthorized users could gain access to resources and attackers could jump laterally between resources.

Read this excerpt from Gartner's 2020 publication, "Market Guide for Zero Trust Network Access," with SDP in mind. Gartner defines ZTNA as "products and services that create an identity- and context-based, logical-access boundary encompassing a user and an application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a collection of named entities. The broker verifies the identity, context and policy adherence of the specified participants before allowing access [...]." SDP is what's hiding the applications and providing the trust broker functionality.

ZTNA and Traditional VPNs

ZTNA and traditional VPN technology provide some of the same functionality. Where they differ most is in deployment and management. With cloud-based ZTNA, there's no need to ship appliances to branch sites, provision each user's client devices, or manage applications.

ZTNA doesn't eliminate the need for VPNs. For example, an organization may already have a dedicated circuit in place to connect two of its sites. Those sites share a set of applications and data that are only accessed onsite. In cases like this, it makes sense to continue using a traditional VPN instead of transitioning that particular link to ZTNA.

In other cases, organizations will benefit from replacing some existing VPN technology with ZTNA or by acquiring ZTNA for certain new use cases. Examples of ZTNA functionality that traditional VPNs might not supply include:

- ☑ Supporting mobile devices and other devices besides desktops and laptops
- ☑ Continuously monitoring the user's behavior and the client device's actions and security health for signs of malicious activity
- ☑ Stopping common forms of DDoS attacks, such as Slowloris and synfloods
- ☑ Automatically establishing network segments for resources, known as *auto-segmentation*, to help stop lateral threats. ZTNA can perform auto-segmentation without needing traditional firewall policies, access control lists, or other configurations manually specified for it.

A final important difference between ZTNA and traditional VPNs is the protocol they use for secure tunneling. Traditional VPNs use protocols like IPsec. Some ZTNA solutions use a new generation of tunneling protocols, like WireGuard (https://www.wireguard.com), which use established cryptographic protocols but implement them in ways that minimize source code. This makes code auditing easier and gives the solution a smaller attack surface with fewer vulnerabilities.

Using ZTNA as an all-in-one solution

SonicWall's website features real-world case studies that explain how their customers have used SonicWall products to meet their needs. One of the case studies showcases an integrated security and networking solutions provider. This company wanted a cloud-native, zero-trust security solution to better safeguard its operations. Its lean IT department needed a solution that would save their staff time.

Business challenges this customer needed to address included:

- Protecting users' network traffic and authenticating those users through the company's identity provider
- Preventing users from having excessive privileges, with the ideal state being least privileged access as the default
- Eliminating delays in onboarding new office sites and remote users
- Empowering the remote workforce
- Ensuring that data remains at rest to comply with regulations
- Stopping several types of DDoS attacks

To address these challenges, the company piloted SonicWall Cloud Edge Secure Access (https://www.sonicwall.com/products/cloud-edge-secure-access). This product uses SDPs to provide ZTNA.

SonicWall Cloud Edge Secure Access exceeded the company's needs. Aspects the company considered particularly noteworthy are:

- **Ease of deployment**: "It worked out of the box." They loved the management portal interface and how well it worked. The company also noted how scalable the solution was, how quickly IT managers could configure it, and how fast onboarding new offices and users was.
- **Ease of use**: The company ran SonicWall apps on its client devices to give users access to a variety of resources. The apps worked "seamlessly" on both desktop and mobile platforms.
- **Security capabilities**. Compared to traditional VPNs, the company felt that SonicWall's solution was better at protecting high-value assets. It offered users in their remote workforce instant secure access to sites and resources. Its micro-segmentation capabilities prevented unauthorized lateral movements that attackers often use to reach additional targets.
- **Integration with existing resources**. SonicWall's solution integrated with the company's existing cloud identity provider, as well as its single sign-on and multi-factor authentication solutions.

Secure access for distributed offices and the remote workforce

Another SonicWall case study is on Chalkline Solutions, a solutions integrator. Chalkline Solutions has relied on SonicWall firewalls for several years. The company chose to deploy the beta version of SonicWall Cloud Edge Secure Access (https://www.sonicwall.com/products/cloud-edge-secure-access) in part of its production environment focused on the remote workforce to judge how well it would meet these needs:

- Cloud-native zero-trust security for distributed, multi-regional offices and the remote workforce
- Support for both company-issued client devices and BYODs
- User access via the solution to both cloud-based and on-premises resources
- Compliance with security regulations and the ability to demonstrate that compliance
- Integration with existing security solutions, including a SIEM and multiple identity providers

Chalkline Solutions personnel were impressed at how well the SonicWall Cloud Edge Secure Access solution worked and addressed their needs. Compared to traditional cloud-based or on-premises VPN solutions, the SonicWall solution had the following advantages:

- Easier and faster onboarding of new users and new office locations
- Better protection of the company's high-value assets
- Faster performance
- Easy-to-use management console

Personnel managing the SonicWall solution were also impressed with its ability to enforce zero-trust policies by network, application, user, and device profiles, while simultaneously providing users in any location with instant, secure access to sites and resources regardless of location.

You can learn more about the Chalkline Solutions case study at https://www.sonicwall.com/medialibrary/en/case-study/chalkline-solutions.pdf. To read more real-world case studies about SonicWall customers, visit https://www.sonicwall.com/resources/ and look for the "Case Studies" heading.

Chapter 5

Inspecting Traffic with Firewall-as-a-Service (FWaaS)

In this chapter

- Review common limitations of on-premises firewalls
- Learn about the security and networking capabilities of FWaaS solutions
- Compare FWaaS and secure web gateway (SWG) offerings

"I am the watcher on the walls. I am the fire that burns against the cold, the light that brings the dawn, the horn that wakes the sleepers, the shield that guards the realms of men."

— George R. R. Martin, A Clash of Kings

Limitations of On-Premises Firewalls

In Chapter 1, we discussed the loss of the network perimeter. This loss has obvious implications for on-premises firewalls, which typically help define the perimeter and enforce policies on incoming and outgoing network traffic at the perimeter. Network traffic that doesn't pass through on-premises firewalls, such as communications between work-from-anywhere employees and cloud-based applications, won't have firewall policies applied to or enforced on it.

With bandwidth usage continuing to increase, on-premises firewalls are more likely than ever to become bottlenecks, unable to keep up with the demands imposed on them.

Bottlenecks caused by on-premises firewalls can't easily be resolved. Adding capacity means upgrading or replacing the firewalls' hardware and software, or purchasing extra firewalls. This is expensive, and it can take months to rip out and replace existing firewall hardware.

Another result of the loss of the perimeter is that the whole notion of a trusted side and an untrusted side of each firewall interface has evaporated. If anything, both sides are considered untrusted. Resources on each side of an on-premises firewall are less likely to be physically grouped together.

The locations of client devices, applications, services, and other technology elements are increasingly irrelevant. Having a unique set of firewall policies for each on-premises firewall, such as those at headquarters and branch sites, no longer makes sense. Organizations need uniform policy enforcement everywhere.

Secure Web Gateway (SWG) Capabilities

Before the emergence of FWaaS, there was the rise of the secure web gateway (SWG). These solutions are web proxies. They can only handle web traffic – they don't support any other type of network traffic. SWGs offer combinations of security capabilities such as:

- ☑ Content filtering, such as blocking connections to known malicious and undesirable websites, and preventing certain file types from being transferred
- ☑ Threat prevention/detection (including malware)
- ☑ Data loss prevention (DLP)
- ☑ File and application sandboxing

An SWG offers a subset of what FWaaS can provide, both in terms of protocols (web only versus everything) and security capabilities. SWG is often mentioned as a component of SASE, but SASE should include full FWaaS functionality, not just the SWG parts of FWaaS.

There's a noteworthy difference between SWG and FWaaS technology. An SWG is a web proxy, so network traffic doesn't pass through the SWG device. Instead, each network connection terminates at the SWG, and after examining the traffic contents, the SWG initiates a second connection to the destination for that traffic. FWaaS solutions don't generally proxy traffic; they perform inline inspection.

FWaaS Technology

FWaaS solutions are highly scalable, cloud-based services that provide next-generation firewall capabilities for all types of network traffic. They can perform all of the advanced security functions that on-premises physical firewalls would previously have been expected to perform. With FWaaS doing the heavy lifting, on-premises firewalls only need to provide connectivity and basic security.

An FWaaS solution is often deployed in conjunction with a ZTNA solution, especially as part of SASE. The FWaaS can apply all its firewall policies to the network traffic that is passing through the ZTNA solution. ZTNA also gives the FWaaS full visibility into the contents of the network traffic.

An organization can define its policies once and the FWaaS solution will dynamically apply them to all network traffic based on user, device, and application, no matter where they are located.

Networking capabilities

FWaaS solutions can provide segmentation and micro-segmentation capabilities. While ZTNA's micro-segmentation applies to private enterprise applications, an FWaaS solution's micro-segmentation involves internet-bound network traffic and public SaaS applications.

Security capabilities

FWaaS solutions provide many advanced inline security capabilities, including:

- ☑ All the capabilities that SWG solutions offer, such as DLP, threat prevention/detection, content filtering, and file sandboxing
- ☑ Deep packet inspection of both unencrypted and encrypted network traffic
- ☑ Deep memory inspection (of files executing in the sandbox) to identify unknown threats and malware
- ☑ Intrusion prevention system (IPS) functions
- ☑ Application control (access control for network traffic on an application-specific basis)
- ☑ Domain Name System (DNS) security

Scalability

FWaaS technology offers a fundamentally different type of scalability than on-premises firewalls. When you need on-premises firewalls to handle more capacity, you typically must rip them out and replace them. This doesn't scale easily or quickly because of its costs and delays.

With FWaaS, scalability is horizontal, not vertical. You can simply adjust your subscription to immediately add the capacity you need.

FWaaS and DNS security

An interesting security capability that some FWaaS solutions support is checking client devices' DNS queries and responses for signs of threats. One way that FWaaS may do this is by looking for attacks that use DNS to coordinate their actions. For example, malware often uses DNS to transfer commands or other malware from a centralized command and control (C2) site. Some FWaaS solutions recognize and block C2 DNS communications.

Also, certain DNS domains are considered suspicious. A domain may be a known malware distribution site, or threat intelligence may indicate that a particular domain is probably compromised. An FWaaS solution with access to up-to-date information on domains could identify suspicious DNS activity and either block it or alert a human analyst to take a closer look.

Chapter 6

Improving Connectivity and User Experience with SD-WANaaS

In this chapter

- Review common shortcomings of existing wide area networks (WANs)
- Understand the capabilities that SD-WANaaS offers
- Learn how SD-WANaaS can be an on-ramp to SASE

"Eventually everything connects – people, ideas, objects. The quality of the connections is the key to quality per se."

— Charles Eames

Shortcomings of Existing WANs

We've already touched on some shortcomings of existing WANs. Many WANs use MPLS to connect branch sites to HQ. With most applications and other resources no longer located at HQ, the process of routing all the traffic to HQ and then sending it back out to its final destination in the cloud causes poor performance and introduces bottlenecks.

The dedicated circuits used by existing WANs are quite expensive compared to the costs of using public networks. It can take a long time to establish a new MPLS circuit, so adding another location to the WAN may take months. Also, not all branch sites may be located in places where telecom providers offer WAN services.

Finally, existing WANs are only used for an organization's own facilities. There are no WANs for individual remote workers on arbitrary networks, so their connections don't benefit from WAN features like quality of service.

SD-WANaaS Features

SD-WANaaS is a cloud-based service that provides WAN features and functionality over any type of network and internet connectivity. The goal for SD-WANaaS is to provide the best application performance, even over broadband internet connections, while also ensuring security and cutting costs. Let's look at the high-level features SD-WANaaS provides to accomplish this goal.

Connectivity

When implementing SD-WANaaS for a branch site, organizations can use commodity broadband services instead of or in addition to dedicated circuits like MPLS. SD-WANaaS can use multiple forms of connectivity together for greater bandwidth and load balancing. Similarly, SD-WANaaS for individual remote users will work over the broadband services those users have, such as cable or 5G. SD-WANaaS can work from any location with broadband connectivity, instead of only locations in a telecom provider's service area.

Using SD-WANaaS as part of a SASE deployment means an organization can reduce the equipment required at each site, with no "truck rolls" needed for each branch site or home office that rolls out SD-WANaaS. These deployments also reduce the labor required to configure, manage, and maintain connectivity for each location.

Zero-touch provisioning

Traditional WANs rely on IP and MPLS routers. When a new router is deployed to a branch site, it must be manually preconfigured, and specialized staff must participate in its installation and integration.

Things are far different for SD-WANaaS. Deploying a new router is a zero-touch experience. The router is shipped to the branch site, where it is plugged into power and given a

commodity internet connection. The router automatically contacts the SD-WANaaS service to authenticate itself and be configured as part of the existing SD-WAN. That's it. Instead of the months it takes to procure and deploy MPLS, adding a new router for SD-WANaaS takes only a few days.

Centralized WAN orchestration and management

Another important feature of SD-WANaaS is centralized WAN orchestration and management. This provides a single-pane-of-glass experience that's far simpler than existing WAN management consoles. You can manage, monitor, and generate reports on all your WANs within the SD-WAN from one place. With SD-WANaaS, administrators can define policies once for all WANs instead of having to manually configure policies router by router. This alone can be a huge time savings, plus eliminate many human errors.

Performance

SD-WANaaS eliminates the need to backhaul all of the network traffic from each branch site to HQ and then route it out of HQ to the final destinations. More broadly, SD-WANaaS can provide the highest-quality experience for branch site users who are connecting to both on-premises and cloud-based applications and services. With SD-WANaaS, organizations can achieve last-mile performance even over commodity internet connections.

Security

Security is paramount for SD-WANaaS because you're moving from dedicated circuits to public networks, where threats are greater and there are few security controls.

SD-WANaaS is a connectivity service, not a security service. It provides basic tunnel security to prevent traffic interception, and it offers basic network segmentation. We strongly recommend using SD-WANaaS in conjunction with other technologies and services like ZTNA and FWaaS, which offer cloud-based security capabilities. The optimal way to do this is to adopt SASE.

Quality of Service (QoS)

Use of public networks raises concerns about traffic from other users that can impede an organization's traffic. Fortunately, this can be addressed through QoS. The concept of QoS is allocating different amounts of bandwidth for each application or type of application. This helps ensure that the most important applications can function properly. For example, QoS could give more bandwidth to corporate videoconferencing services and less to recreational applications.

SD-WANaaS can apply QoS markings to network traffic for each branch site or client device. This enables SD-WANaaS to optimize performance for some applications or users, and to optimize cost for others by reducing bandwidth utilization. SD-WANaaS also improves communications reliability because if a problem occurs in one network path, SD-WANaaS can immediately route traffic to another path.

Because SD-WANaaS uses a network tunneling protocol, the QoS markings it applies to network traffic are maintained even when traffic crosses networks and service providers. Also, although QoS is usually not available for work-from-anywhere scenarios or for users with broadband internet connectivity, it can be provided with SD-WANaaS.

SD-WANaaS as On-Ramp to SASE

By using SD-WANaaS alongside ZTNA, FWaaS, and other SASE components, your organization can build a SASE implementation over time. SD-WANaaS is often the last major SASE component to be implemented because the others need to be in place first to provide security services. Also, in order to leverage SD-WANaaS, individual users must be running client software (like ZTNA or FWaaS) that directs their network traffic through the organization's cloud-based services.

Once all the components are in place, SASE will give users the best quality of experience and necessary security, no matter where they are connecting from.

Chapter 7

Selecting a SASE Solution

In this chapter

- Learn the importance of assessing the breadth, quality, and degree of integration of a SASE solution's portfolio
- Understand why it's so critical to consider the maturity of each SASE solution and its vendor
- See why security, agility, and flexibility are especially important considerations when evaluating prospective SASE solutions

"The measure of intelligence is the ability to change."
— Albert Einstein

Portfolio Breadth

A critical aspect of evaluating any prospective SASE solution is the breadth of its portfolio of functionality. The original Gartner concept of SASE included 17 types of functions. Unfortunately, comparing SASE solutions based on the functions each provides can be a headache, with a veritable alphabet soup of acronyms and vague terminology. Different functions may also overlap each other, further complicating the matter.

It's important to realize that some of these functions may not be relevant or even helpful for your particular organization and situation. Your best bet for evaluating portfolio breadth is to list the core capabilities you need SASE to provide, and then compare each prospective solution against that list. Examples of common core capabilities are ZTNA, FWaaS, and SD-WANaaS.

It's just as important to identify the source of each core capability. Are they all from the same vendor and specifically created to work together? In other words, are the capabilities fully integrated such that processing isn't duplicated by multiple capabilities? Or does each capability do all of its own processing and not share the work and information with the other capabilities? The answer can make a huge difference in how well the SASE solution works as a whole.

A final consideration for portfolio breadth is which functions are supported by each client device platform. For example, which desktop and laptop computer, smartphone, and tablet operating systems support the SASE client agent and all of its functions? Which functions are supported for clientless devices? A broad portfolio doesn't do much good if your clients can't take advantage of it.

Other components in a SASE portfolio

We've already discussed the ZTNA, FWaaS, and SD-WANaaS components of SASE portfolios. Here's an overview of some other common components:

- Cloud application security: Cloud application security encompasses a range of security capabilities for popular SaaS applications, like Microsoft Office 365, Teams, and Slack; Google Workspace; and Box and Dropbox. The capabilities safeguard the usage of these applications by stopping malware and other threats, preventing data leakage, and protecting user accounts from takeover and misuse. Some cloud application security capabilities can also help to discover shadow IT usage.
- Web application firewall (WAF): WAF technology blocks attacks it finds in web applications' network traffic.
- Web application and API protection-as-a-service (WAAPaaS): WAAPaaS is a broader capability than WAF. It includes WAF and also provides application programming interface (API) protection services, DoS protection, and other features for web applications.
- Endpoint security solutions: These solutions provide information on the current security posture of an endpoint. Examples include endpoint control (EPC) and anti-virus software.

Portfolio Quality

Portfolio breadth is important, but so is the quality of each component and the portfolio as a whole. Here are some of the aspects of quality you should look for:

- ☑ Accurate, comprehensive, and uniform enforcement of policies
- ☑ Effective use of more-advanced and dynamic capabilities, like executable sandboxing and threat intelligence, while minimizing false positives
- ☑ Better performance and lower latency for all users, including those at branch sites and other locations, compared to legacy solutions

We strongly recommend that you review any available test and evaluation reports from independent third parties. There are highly respected laboratories that conduct extensive assessments of individual SASE components like FWaaS. They measure performance, alert accuracy, and other characteristics to give you an objective basis for comparing products. These reports give you quantifiable data that you can't get anywhere else.

Portfolio Integration

There are three important aspects of portfolio integration to consider. The first is how tightly the portfolio's components are integrated. The SASE solution should run as a single stack, with one management plane and orchestration layer.

The SASE solution should **not** be a series of separate applications that work consecutively without sharing information. That approach will degrade performance and the quality of policy enforcement measures.

The second aspect of integration is a single policy framework. An administrator should be able to define a policy once and have that policy enacted throughout the organization for all applicable components of the SASE portfolio.

A single administrative console and dashboard for all security and network services not only provides ease of use for administrators, but also improves accuracy and reduces human error. It can even reduce latency because network traffic only needs to be examined against a single unified policy, not numerous policies in series.

The final aspect of integration is ensuring that the SASE solution can work with your existing security and networking applications and services. For example, the SASE solution should use standards for any interfaces it makes available, like APIs or log management.

Solution Maturity

Because SASE is so new – a concept that Gartner introduced in August 2019 – no SASE vendor has a truly mature offering yet. It takes time to build all the pieces of the portfolio and ensure they are working together seamlessly and effectively in every real-world situation they will likely face.

Instead of evaluating the maturity of SASE solutions, focus on the vendor's security and networking experience and on the maturity of individual components of the SASE solution. In general, it is far preferable to use a proven on-premises component that a vendor has migrated to the cloud than a component that a vendor has just written from scratch.

Bringing a proven technology to the cloud essentially involves shifting its functions from one network location, the perimeter, to another, the cloud. Proven technologies have been used in an incredible variety of production environments for years. This long history has brought to light weaknesses and other issues that the technology vendors have long since been resolved. The vendors of proven components have already handled all the problems that users of new components will take years to uncover and vendors of new components will eventually address.

Security of the Solution

There's a potential disadvantage in using a SASE solution. Because it's the central point for so many security and networking services and has visibility into decrypted network traffic, it's a critically important resource. Its own security is paramount because a compromise of the SASE solution could be devastating.

Make sure any SASE solution you evaluate is as strongly secured as possible. Here are some things to be on the lookout for.

- ☑ The SASE solution should use standard cryptographic algorithms and modules wherever it uses encryption and other forms of cryptography. It should support cryptographic key lengths commensurate with current best practices, and it should ensure that all secret keys are well safeguarded against unauthorized access.
- ☑ The SASE solution should be resistant to common forms of DoS and DDoS attacks. Otherwise, attackers could readily make your SASE solution unavailable, causing outages for your users.
- ☑ Take a close look at the security of the SASE solution's own management. Make sure it requires administrators to be strongly authenticated before accessing any management functions and that all management communications are strongly encrypted.

In addition to evaluating each solution itself, you should also evaluate the solution's vendor. For example, ask vendors how they look for and address vulnerabilities in their SASE solution.

Also, look at each vendor's history with security and networking products. How have they fared, relative to others, in terms of delivering products with fewer serious vulnerabilities? Understanding how seriously a vendor takes security in its own software development practices can tell you a lot about the quality of an offering.

Business Agility and Flexibility

In Chapter 3, "Making the Business Case for SASE Adoption," we talked about how SASE solutions provide greater business agility and flexibility than the legacy security and networking solutions they replace. Taking advantage of SASE can provide huge agility and flexibility benefits for organizations, so it's well worth taking those attributes into account whenever you evaluate SASE solutions.

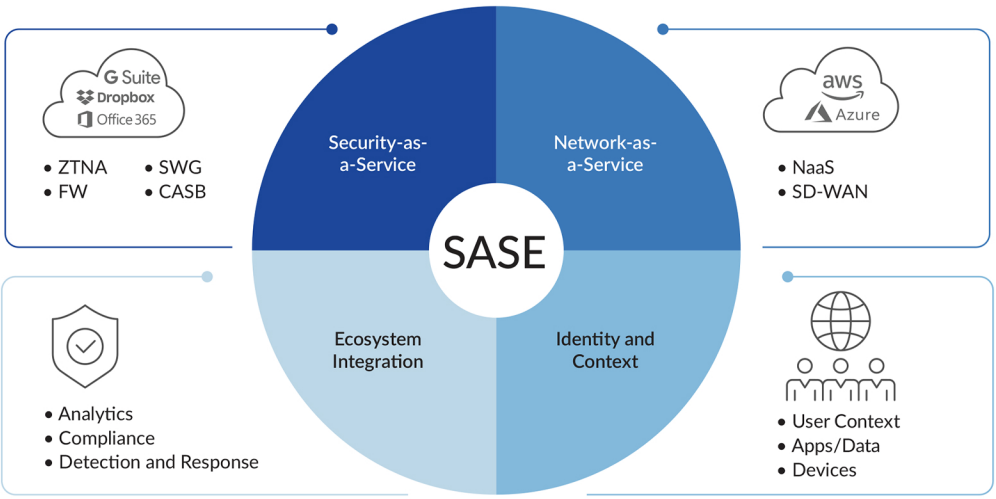
Here are some questions you may want to ask for each SASE solution you're considering. You can use the answers not only to compare SASE solutions to each other, but also to see examples of the agility and flexibility that SASE can provide and on-premises solutions can't.

Using the SASE solution, roughly how much effort and calendar time would it take for administrators to do each of the following?

- ☑ add a new branch office
- ☑ move a branch office's security and networking services from one facility to another
- ☑ double the number of users able to work from anywhere
- ☑ make a new resource available to authorized users only, where those users are:
  - all authenticated users at all locations
  - one small group at a single location
  - a cross-cutting subset (roughly 10 percent) of users who are authorized to work from anywhere

Finally, when thinking about agility and flexibility, start by looking at the benefits of each stage of SASE implementation. Adopting ZTNA alone can provide substantial improvements that justify using it as soon as feasible. For this reason, it may be easier to start with ZTNA as your immediate objective and add other components of SASE in the near future to further increase agility and flexibility.

SonicWall SASE Framework



Discover how SASE solutions bring together security and network services to empower your employees, provide business agility and flexibility, and evolve security.

Security and networking have both changed rapidly in recent years. Organizations are losing trust in the increasingly diverse technologies they rely on. SASE provides a new path forward: a single, highly scalable solution that greatly simplifies what security and network teams need to do, even in today's incredibly complex environments.

- Reviewing what's changed — see how organizations have lost control, visibility, and trust in the cloud era
- Regaining control through SASE — explore how SASE merges security and network services
- Gaining SASE's benefits — learn how SASE can benefit your organization, including simplifying operations and improving security and network performance
- Understanding major SASE components — know the roles of the largest SASE components: zero-trust network access (ZTNA), firewall-as-a-service (FWaaS), and software-defined WAN-as-a-service (SD-WANaaS)
- Selecting the right solution — know what to look for when evaluating potential solutions

About the Author

Karen Scarfone is an accomplished freelance writer and editor, and a recognized technical expert in the field of cybersecurity. She has contributed to hundreds of works from technical guidelines and reports to articles and books over the past 20 years. Learn more about her and her work at www.scarfonecybersecurity.com.

CYBEREDGE PRESS

Not for resale

ISBN 978-1-948939-19-5