LEARNING MADE EASY

VMware Special Edition

SASE & ZTNA

for dummies®
A Wiley Brand

Make your network more safe and secure

Improve the speed and reliability of your apps

Tackle the new needs of remote workers

Brought to you by

vmware®

Roopa Honnachari
Lee Doyle
Keith Townsend
Zeus Kerravala
Craig Connors
Pere Monclus

About VMware

VMware software powers the world's complex digital infrastructure. The company's cloud, app modernization, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact. For more information, please visit **https://sdwan.vmware.com**.

SASE & ZTNA

for dummies®
A Wiley Brand

SASE & ZTNA

VMware Special Edition

by Roopa Honnachari, Lee Doyle, Keith Townsend, Zeus Kerravala, Craig Connors, and Pere Monclus

for dummies®
A Wiley Brand

SASE & ZTNA For Dummies®, VMware Special Edition

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

ISBN 978-1-119-76643-8 (pbk); ISBN 978-1-119-76645-2 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

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: Mohammed Zafar

Special Help: Ryan Williams, Chris Le, Vivian Clark, Nitin Kumar Ananda, Vinod Kumar Balasubramanyam, Ferdinand Sales, Rohan Naggi, Aamer Akhter, Karl Brown

Contents at a Glance

Table of Contents

Introduction

Enterprise networking isn't what it used to be, and businesses are struggling to adapt. Not long ago, most users worked from a corporate office. Today, they could be working from anywhere: a coffee shop, a customer site, or, for millions of new home-based workers, a home office. The applications they're using look different, too — most now live in the cloud. This new normal calls for a different approach to networking and security — one built for today's distributed, cloud-first businesses and increased security threats rather than the data center–centric IT models of the past.

Fortunately, the industry has answered with secure access service edge (SASE). SASE combines the flexibility of a software-defined wide-area network (SD-WAN) with a full suite of security services, all delivered from the cloud. SASE reinvents remote access for millions of mobile and home-based users with zero-trust network access (ZTNA). Together, SASE and ZTNA provide the more flexible, context-driven approach to networking and security that today's dynamic businesses need.

What's wrong with legacy networking and security models, and why are modern enterprises stretching them to the breaking point? How do SASE and ZTNA do things differently, and what do you need to know to successfully use them in your business? In this book, VMware, along with some of the industry's premier analysts, provide some answers. We explore how we got here and how SASE and ZTNA meet today's toughest connectivity challenges. We examine how these technologies address the most common enterprise use cases. Finally, we go inside a typical solution to see how SASE and ZTNA make smarter access and policy decisions.

It's a new world out there for the modern distributed enterprise. Keep reading to find out how SASE and ZTNA can help your business navigate it successfully.

Foolish Assumptions

In writing this book, we made some assumptions about you, the reader:

- You're likely an IT professional with some power over how your company implements networking solutions.
- You may not be a security expert, but you probably have some basic experience with the concepts, and you know why you need to make sure only the right people get access to only the right data.
- You don't want to spend a huge amount of time considering theoretical concepts, and you do want to get right to a solution that can help you make your team members' lives easier.

Icons Used in This Book

As you page through this book, you'll notice some icons in the margin designed to attract your attention. Here's a guide to what those icons mean:

TIP

Anything marked with this icon offers some info to make your life easier (at least when it comes to IT security — we can't do anything to solve your relationship problems).

REMEMBER

Some information is so important it bears committing to memory. When we tell you something you'll want to remember, we flag it with this icon.

WARNING

You can't insert a flashing light in a print book, and it's bad form to use a <blink> tag on the web (this isn't 1997, after all). Still, if you don't pay attention to this icon, you may encounter a lot of trouble later. Pay attention!

Where to Go from Here

Check out the following resources from VMware to learn more:

- ***Software-Defined WAN For Dummies:*** `https://sdwan.vmware.com/sd-wan-resources/ebooks/software-defined-wan-for-dummies`
- **VMware Secure Access:** `https://sdwan.vmware.com/vmware-secure-access`
- **VMware SASE Platform:** `https://sdwan.vmware.com/secure-access-service-edge`

IN THIS CHAPTER

- Seeing how we got where we are today
- Looking at current connectivity models
- Understanding the weakness of the old WAN
- Using SD-WAN to address the problems of yore
- Securing every last bit of your network
- Appreciating the power of SASE and ZTNA

Chapter 1
Introducing SASE and ZTNA

Modern enterprises demand access to the latest and greatest business applications anywhere, anytime. Problem is, you may still use those tools over private, leased-line architectures built in the early '90s. Why drive your newest high-powered sports car down a gravel road? In this chapter, we take a look at the older models and discover a better way to make sure work from anywhere actually works.

Understanding How We Got Here

Routing every network connection through a central data center made sense when that data center actually hosted all your business applications. Today, most of them live in the cloud. So, branch traffic often takes the scenic route from data center, to cloud, back to data center, and finally back to the user. Performance suffers.

In the mid-2010s, software-defined wide-area network (SD-WAN) technology came to the rescue. Acting as a kind of cloud-based traffic cop for applications, SD-WAN introduced a much smarter, more efficient WAN model. As great as SD-WAN is, though, it's optimized for connecting branches and certain home workers. When it comes to the growing number of remote users (and devices and services) outside the branch, businesses once again must route everything through the data center.

Today, the industry is taking SD-WAN to the next level with secure access service edge (SASE, pronounced "sassy") and zero-trust network access (ZTNA) solutions. SASE and ZTNA combine SD-WAN efficiencies with a much more flexible, user-centric approach to securing remote workers and cloud applications. We're finally building a secure connectivity model suited to the world we live in today, instead of the world of 30 years ago.

Identifying What's Wrong with Current Connectivity Models

To understand the urgent problems SASE and ZTNA solve, we need to review how we got here and why. Let's take a trip down memory lane.

The '90s called, and they want their network architectures back

Back in the early days of the Internet, businesses used "heavy" branches, hosting most applications and security on-site. This wasn't exactly by choice — public Internet connections hadn't yet reached every market, and the connections that existed weren't very reliable. You could get a time-division multiplexing (TDM) leased-line circuit, but they were expensive and restrictive in terms of bandwidth. (You could either aggregate multiple 1.5-Mbps T1 links or bump up to a 45-Mbps T3.) Businesses had little choice but to build out branch software stacks like miniature, standalone versions of the company headquarters.

In the 2000s, Multiprotocol Label Switching (MPLS) hit the scene to offer a lot more WAN circuit flexibility and control. Branches got "lighter" as businesses moved everything they could to centralized data centers. Users connected back to the data center to

access most of their applications and data. Enterprises outfitted branches with dual WAN uplinks, so those applications could remain available even if the primary circuit failed.

MPLS links were still expensive, but this basic WAN model served businesses well for years. And if it sounds familiar, it's because many businesses still use it. Today, though, the world has changed. The assumptions underlying legacy WAN architectures — that most users work from branches and that almost everything lives in a central data center — no longer apply.

Welcome to the cloud

Hosting applications (buying servers, installing and maintaining software, scaling with demand) can be an expensive, time-consuming job for IT. One 2018 study conducted by Rackspace found that for every dollar companies spend on capital expenses to upgrade data center infrastructure, they can expect to pay roughly $2 for managing, maintaining, and securing that infrastructure. So, when cloud computing came around in the mid-2000s, and businesses could offload that effort to someone else, many jumped at the chance.

First, tech giants provided software-as-a-service (SaaS) options like Salesforce and Microsoft Office 365. Suddenly, it didn't matter where an application technically lived, employees could get to it from any web browser. Businesses no longer had to worry about maintaining apps either. SaaS providers could deal with software updates, resiliency, and scalability. And businesses could treat key applications like a utility: Turn them on when you need them, pay for only what you use.

Many companies found this IT model to be much simpler and more flexible. They could launch new applications and services more quickly, with a fraction of the effort. And they could focus their IT resources on things that really mattered to their businesses, instead of the care and feeding of server farms.

Over the last decade, companies have been moving several IT workloads to the cloud:

- Computing
- Storage

- Test and developments environments
- Enterprise applications such as web hosting, telephony, conferencing, email, and customer relationship management (CRM) tools

In a recent Frost & Sullivan cloud survey, 84 percent of respondents said they now use or plan to implement public cloud infrastructure-as-a-service (IaaS) in the next two years, and 77 percent use or plan to implement SaaS.

The rise of the remote workforce

Applications aren't the only things to move out of the branch. As broadband became ubiquitous in the early 2000s, work started moving out of the office. Using virtual private networks (VPNs), employees could now securely connect to data center applications even when they were outside the corporate firewall, from anywhere. And they do. According to one 2019 survey, remote work has grown by 400 percent over the past decade. And that was *before* COVID-19 forced millions to spend months working from home.

Today, practically every business appreciates how important remote work can be to business continuity, but the benefits don't end there. By giving employees the option to work where they choose, businesses say they can

- Better attract and retain talent
- Improve employee morale and job satisfaction
- Increase productivity
- Reduce environmental impact
- Lower operating costs

Recognizing That Yesterday's WAN Can't Keep Up

These cloud and remote work trends are stretching early-'90s-era WAN architectures to the breaking point. Under the new status quo, applications may be hosted from a cloud point of presence

(PoP) practically anywhere. But to minimize the risks of connecting over the Internet, many enterprises still see a need to route all cloud application traffic through a central data center. This creates many challenges for businesses and their IT and security teams.

Driving costs higher and hurting user experience

In yesterday's WAN, most application traffic traveled back and forth from branches to the data center. Very little traffic went between branches or out to the Internet. Today, employees use multiple cloud-based applications running in many public and private clouds. Branch traffic may be going anywhere. This creates big inefficiencies for the following:

- **Branch employees:** A user joining a Microsoft Teams videoconference may have a Microsoft cloud PoP available just a few miles from her location, but the WAN still routes all her traffic through the company's central data center — even if it's hundreds of miles away.
- **Remote workers:** Imagine an employee traveling overseas, trying to download the latest sales presentation from an international colleague's Box folder. Box may host a PoP in that country, but the employee must connect to SaaS applications through a VPN gateway back in the central data center. His download request travels all the way to the company headquarters and back. That's a *long* detour for that big file.

WARNING

This connectivity model creates big bottlenecks in the data center. Worse, it leads to major inefficiencies, as traffic gets "hairpinned" or "tromboned" back and forth, sometimes over vast distances. Those extra round trips can introduce latency, producing a poor user experience, especially for delay-sensitive voice and video applications. They also rack up much higher costs for WAN capacity than businesses would otherwise need.

Wasting resources

Even if businesses didn't have to hairpin traffic, legacy WAN architectures would still waste resources. Remember those dual WAN uplinks that branches used in case one circuit were to fail? Well, by default, that means the business is typically paying for a backup link that sees minimal usage.

REMEMBER

In traditional WAN architectures, the backup link only activates if the primary fails, so it almost never gets used. These architectures also tend to be very static. You can't reroute traffic without extensive manual reprogramming.

Relying on old security models in a world of new threats

Habit and momentum aren't the only things keeping antiquated WAN architectures in place. Enterprises still keep firewalls, intrusion prevention systems (IPSs), VPN concentrators, and more in the data center. They don't want to deal with dozens or hundreds of instances of those security tools at every branch. So, they just make application traffic pass through centralized defenses.

REMEMBER

Relying on centralized security solutions worked fine when the traditional concept of the network perimeter still applied — when trust was based on whether a user (or device or application) was "inside" or "outside" the business. Today, those lines have disappeared. A branch employee using a cloud application may be using multiple services running in multiple public and private clouds, all in the same session.

The risks are even higher for remote workers. Even when enterprises try to force remote workers to access cloud applications through the data center, employees find ways around it. To avoid the performance hit, some just disable the VPN client and try to access the application directly over the Internet — bypassing data center defenses entirely.

Adding complexity

An inside-versus-outside trust model may seem simple on its surface, but in practice it adds a lot of complexity for IT security teams. IT must maintain separate sets of security policies for users, depending on where and how they connect. IT also must manage a patchwork of disparate security tools for all the different possible access scenarios.

WARNING

In security, complexity equals risk. If you're dealing with tens of thousands of firewall rules, for example, it's much easier for a misconfiguration somewhere to leave something important exposed. But when you're forced to think about security in terms of "inside" versus "outside" the network perimeter (even if that

bears little resemblance to reality), you don't have much choice. There's no good way to implement a single, consistent policy based on the user, rather than the IP address.

Solving Many (But Not All) of These Problems with SD-WAN

Enterprises understand the inefficiencies of outdated connectivity models better than anyone. In fact, that's the rationale for one of today's fastest-growing technology trends: SD-WAN. According to Frost & Sullivan, the global SD-WAN market exceeded $1 billion in 2019, more than doubling 2018 revenues. During that same period, the number of sites using SD-WAN also grew by more than 100 percent.

REMEMBER

SD-WAN adds a layer of software intelligence on top of the WAN infrastructure. Instead of using a static topology that mostly routes traffic through the data center, SD-WAN technology can route traffic on a packet-by-packet basis. SD-WAN can change those routing decisions on the fly, automatically, in response to real-time conditions in the network.

Unlike yesterday's static WAN, which wastes capacity and costs on backup links that rarely get used, SD-WAN technology uses all available links, all the time, in an active–active configuration. It continuously tracks the health and status of all connections, sending traffic down the best path available at that moment.

SD-WAN technology gives users a much more efficient, higher-performing connection to cloud-based applications. Modern SD-WANs can recognize traffic for more than 3,000 applications. Based on each application's business policy, the SD-WAN can route that traffic to the enterprise data center, a nearby cloud PoP, or directly over the Internet.

SD-WAN capabilities like these produce much better application experiences for users, while reducing WAN bandwidth consumption and costs. They enable a more flexible approach to WAN connectivity, aligned to the cloud-centric world in which we live today.

SD-WAN solutions solve most of the performance and efficiency problems associated with antiquated WAN architectures, and most include a built-in stateful firewall. But when it comes to remote workers and cloud-based application traffic, they just weren't designed to provide the full-featured security stack available in the enterprise data center. Until now.

Welcome to the Secure Connectivity of SASE and Zero Trust

What if you could take everything that's great about SD-WAN and combine it with more dynamic, user-centric security? What if your core security capabilities — encryption, firewall, access control, and more — could run from any of hundreds or thousands of cloud PoPs around the world, like any other cloud service?

You don't have to wonder anymore. A new generation of SASE solutions now delivers that. These solutions also free businesses from perimeter-based trust models that haven't reflected reality for years. Using ZTNA, they grant trusted access based on the identity of the user (or application or other entity), instead of the user's location or IP address.

Together, SASE and ZTNA finally bring branch and remote connectivity out of a model that dates to the turn of the millennium. They create a foundation for much more secure and intelligent connectivity from anywhere.

A smarter, more secure edge

As originally defined by Gartner, SASE brings together network and cloud security services to provide flexibility, agility, and scale. SASE offers a much simpler secure connectivity model for cloud-first enterprises, bringing security functions wherever they're needed, like with other cloud services.

SASE providers (often, companies that already offer SD-WAN) build a national or global fabric of PoPs and peering relationships with cloud providers. These PoPs serve as an onramp to SaaS applications and other cloud services. When users (or devices or applications) connect, either in a branch or via remote access,

each PoP can apply the full suite of enterprise security functions. Typically, that includes

- ZTNA
- Secure web gateways
- Cloud access security broker (CASB) solutions to apply security policy to cloud applications and data
- Cloud-based firewalls
- Identity services to establish the user's context and security posture

Just as important, SASE delivers many of these cloud-based security functions "as a service." Businesses can apply the full suite of state-of-the-art security protections anywhere, without having to maintain hundreds of point products distributed around the globe. Who's got the time and frequent-flyer miles for that anyway?

Reimagining trust

Inside SASE solutions — in many ways, making them possible — there's a revolution in the way businesses think about secure connectivity and trust. With ZTNA, they can eliminate yesterday's inflexible inside-versus-outside approach to granting access to corporate resources. Instead, they can implement a dynamic, user-centric, software-defined perimeter (SDP).

Businesses don't have to build the entire IT security stack around physical locations or IP addresses. Instead, SASE platforms grant access based on the identity of the user, device, and application.

ZTNA replaces VPN remote access models, but it does much more than that. It also creates a virtual gatehouse guarding all corporate applications and resources, no matter where they're physically located. As "zero trust" implies, ZTNA denies access to those resources by default. In fact, it hides them entirely, so they're not even discoverable except to the users, applications, or other entities that the enterprise specifically allows.

Whenever a user, device, or application tries to access a corporate resource, ZTNA verifies that they're a trusted entity. It does this based on the user's identity, not his IP address. It can examine context (such as device type, geolocation, security posture, and

specific resources being accessed) to apply the right policy. And it applies that policy automatically, without security teams having to manually spell out what should happen for every possible access scenario.

A powerful combination

SASE and ZTNA represent different technologies. But, like many of the classics — peanut butter and jelly, burgers and fries, bacon and eggs — they just go better together.

Used in concert, ZTNA can provide the user's contextual identity (such as her location and the security posture of her device) to all the different SASE security services. That contextual identity can then dictate policy. For example, if the system identifies that a user is connecting with a jailbroken iPhone, it can send that traffic to the CASB service for further threat protection and scanning.

Organizations also end up with a single access infrastructure for both "inside" and "outside" users, as well as both data center– and cloud-hosted applications, which means they can now use a single, consistent security policy everywhere.

REMEMBER

You *could* use SASE or ZTNA in isolation — but you really shouldn't.

If you use ZTNA without SASE, you may leave users exposed to certain types of web-based attacks. You also must handle malware and threat detection on a per-device basis, making it more expensive, harder to manage, and (for employee-owned endpoints) sometimes not applicable at all.

If you use SASE without ZTNA, any user accessing an application could see all other applications hosted on that network, increasing the potential attack surface. You're also now relying on each application to handle user access individually — a big operational problem.

Identifying the SASE and ZTNA Advantage

When businesses move to a SASE plus ZTNA model, they get secure, reliable, performance-optimized access for both traditional and cloud-based applications. They can securely connect

anything and everything — branches, campuses, remote workers, Internet of Things (IoT) devices — with a single, holistic solution.

This result is obviously better for users. Drawing on SD-WAN innovations, SASE makes WAN architectures and security models align with the way enterprises actually work. Employees can work from anywhere, using any traditional or cloud-based application, and automatically get the right security protection — without compromising performance.

The model also makes life better for IT operations. SASE and ZTNA make it much easier to manage security and access. Most deployment, monitoring, and troubleshooting tasks now happen automatically. And enterprises can use a single security policy and infrastructure everywhere.

Finally, you'll see better results for enterprise security. Enterprises can now protect themselves with contextual intelligence, automatically granting or denying access based on a user's identity and security posture. They can combine all the layers of defense used in the data center — plus new ones for the cloud — and apply them anywhere from local PoPs around the globe.

IN THIS CHAPTER

- Finding out about different services that SASE and ZTNA offer
- Understanding different SASE and ZTNA components
- Transforming secure connectivity in your enterprise

Chapter 2
Identifying the Key Components of SASE

For modern enterprises, the edge is not what it used to be. A growing reliance on remote workers, guest networks, and extranets blurs the lines of the traditional network perimeter. Meanwhile, businesses are adopting a software-first approach to networking and security and moving more intelligence to the cloud.

In this chapter, we take a look at the components involved in a secure access service edge (SASE) and zero-trust network access (ZTNA) implementation and explain how you can dramatically improve how your users connect to your network (while preventing others from joining the party).

Living (And Working) on the Edge

The traditional network edge is overdue for an extreme makeover, as employees and applications now connect in more ways, from more places and devices. All of a sudden, it's a lot harder to define where "inside" the enterprise ends and "outside" begins, which means you need to rethink these concepts.

Edge networking

Cloud and software-as-a-service (SaaS) applications now dominate enterprise software, with most traffic flowing from branch to cloud and not to the centralized data center. These shifting traffic patterns, along with a need to position more intelligence at the edge for Internet of Things (IoT) and other applications, require a more distributed IT model.

Edge security

The erosion of the traditional security perimeter is pushing security services away from the central data center and toward the edge of the network. Cloud-based solutions can address the many new threats that come with a distributed workforce and the growing reliance on the cloud. Each new layer of cloud security adds new complexity to the system, though.

IT operations

To operate safely as part of this new model, you need to better integrate your network and security intelligence, and you need the ability to deploy that intelligence in more flexible ways. Ideally, you should apply all the networking and security functions you need as scalable cloud services. Today though, networking and security remain highly specialized, with core capabilities distributed across multiple technology categories and solutions. IT also typically controls networking and security functions in silos, making them complex and harder to manage.

The network, no matter what form it takes, must protect the usability and integrity of network resources. Many new solutions, including the following, have emerged in the past few years to help you do it:

- Software-defined wide-area networks (SD-WANs)
- Secure web gateways (SWGs)
- Cloud-based next-generation firewalls (NGFWs)

Until recently though, most of these solutions functioned as independent entities. Enterprises were left to patch them together into a cohesive edge architecture themselves — at significant complexity and cost.

Today, you can implement a simpler, more capable model for building and securing edge networks: SASE. As defined by Gartner, SASE converges networking and security intelligence in the cloud. This solution combines the full stack of modern security services with advanced networking intelligence in a single platform, delivered as a service.

In the rest of this chapter, we take a closer look at the different networking and security services SASE brings together to make this possible.

SASE Networking-as-a-Service

The networking-as-a-service component of SASE uses the increasingly popular SD-WAN networking model. SD-WAN uses software and cloud-based technologies to simplify the delivery of WAN services. Networking intelligence moves to the cloud, where it's delivered as a service through a cloud-based orchestrator and cloud gateways, which communicate with simplified hardware appliances in branches.

With SD-WAN networking intelligence, a SASE solution can treat edge traffic differently depending on where that traffic is going. For instance, the solution can route cloud application traffic to nearby cloud exchanges, while sending other traffic to the corporate data center or the Internet. SASE can also extend that intelligence from the application all the way to each user's device — whether on an enterprise campus, in a branch, in a home office, or on the go.

SASE also abstracts network functions via software-based virtualization — uncoupling network intelligence from physical infrastructure. Run your network as a flexible cloud service to simplify your IT operations. You gain the flexibility to optimize your WAN for cloud-centric traffic patterns and ditch your old models. You can use Internet-grade transport (with its benefits of ubiquity, high bandwidth, and low cost). And you can apply traffic-handling intelligence to provide a better user experience. Everybody wins!

Moving edge intelligence to cloud gateways

As more branch traffic and applications move to the cloud, you can create a more flexible and efficient edge by moving your network intelligence there, too. The more branch software and infrastructure live in the cloud, the less you need to take care of at each branch.

VMware SD-WAN, for example, positions most network intelligence in cloud-hosted gateways, which connect to "thin" edge devices in the branch via secure Internet Protocol Security (IPSec) tunnels. These cloud gateways are hosted in points of presence (PoPs) around the globe, typically collocated with cloud exchanges. Those exchanges then act as hubs for connecting with diverse cloud-based services and applications. Cloud-based SASE PoPs provide several different benefits:

- **A cloud on-ramp:** By connecting to cloud gateways in PoPs collocated with cloud exchanges, you can extend the network edge right to the doorstep of the cloud. The network can then hand off SaaS, infrastructure as a service (IaaS), and other public cloud traffic with minimal latency, providing a better application experience.
- **Increased control over application performance:** SASE includes intelligence at both the branch or user device and the cloud gateway. This way, the network can monitor and optimize applications all the way from the user device to the data center or cloud where they're hosted. It can track live statistics for every WAN link to make better traffic routing decisions, especially for delay-sensitive voice and video traffic. It can also perform remediation techniques for jitter, latency, and packet loss that wouldn't be possible otherwise.
- **Simpler deployment:** To protect against a shifting threat landscape, businesses use more cloud-hosted security services. This practice often means routing traffic through multiple third-party clouds for processing. If you're not using cloud gateways, you must manually build IPSec tunnels to each of those services from each and every branch appliance. With a gateway model, the branch device just needs one tunnel to the gateway in which all the diverse security services can connect in the same cloud PoP.

TIP

Cloud gateways make adding new branches a lot easier. The edge appliance only needs to locate the closest cloud gateway and build an IPSec tunnel to it. Traffic for that branch is automatically routed to the right cloud networking and security services, with no additional configuration needed. Sounds dreamy, doesn't it?

- **On-demand scalability:** When your networking intelligence lives in the cloud, you can easily scale up as needed. This ability becomes especially valuable with SASE. As you add more cloud security services, such as NGFW or SWG, you'll need more processing power. Those compute requirements increase linearly as traffic grows. If your edge intelligence lives in cloud gateways instead of branch appliances, you can add more gateways or cluster services to improve performance from anywhere, in seconds.

TIP

Not all cloud gateways are created equal. To realize the full benefits of this approach, gateways should be fully integrated with your SASE solution. You should also be able to use cloud gateways as a service, without having to take on a complex implementation effort (finding the closest gateway for each branch or manually building tunnels) yourself.

SASE Security-as-a-Service

Ideally, security should be automatic for every connection to every application, without users (or even IT) having to think about it. As the nature of work changes and the threat landscape evolves, though, the number of security services that are "intrinsic" keeps getting smaller.

Today, to safeguard all the different ways and places people work, businesses use cloud-based security services, such as these examples:

- Cloud web security
- Cloud access security broker (CASB)
- Data loss prevention (DLP)

Typically, these services are delivered by different vendors and processed in each vendor's cloud. That means that each service requires special attention to implement and manage.

With SASE, many of those cloud security layers become intrinsic. You no longer have to deal with different vendors and clouds. Everything is pre-integrated into the SASE solution, and you can monitor and control it all from one place. By expanding the scope of your intrinsic protection, SASE makes security much simpler to manage — even as it becomes more powerful and comprehensive.

REMEMBER

You can still use a specific third-party security service if you want. SASE solutions should provide the flexibility to do that, too. But if you want to make your life simple, stick with the basics.

Locking down access with ZTNA

As one of its core components, SASE includes a more flexible way to handle secure access for remote and mobile users: ZTNA. ZTNA moves access control from a perimeter-based model, where everything is dictated by the source and destination IP address, to one based on context-aware identity.

As the name implies, ZTNA implements a zero-trust model to tightly control access. Applications are not accessible or even visible by default, reducing the surface area for attack. Today, enterprises can use ZTNA solutions in a variety of ways.

- Use ZTNA as a hardware-based, software-based, or as-a-service solution.
- Make your solution work with managed or unmanaged user devices.
- Interface with access control intelligence deployed on the user device, edge, data center, or cloud.

In all cases, ZTNA inserts a trust broker between the user and application to mediate all connections. This broker provides a proxy connection to the desired resource. In this way, ZTNA provides several important benefits for enterprises and their remote users:

- **Securing the air gap between resource and user:** ZTNA treats the Internet as an inherently untrusted transport. By inserting a proxy between users and applications, the device initiating the connection never sees an actual address or location for that application.

- **Identity-based policy:** With ZTNA, the network can make access decisions based on user identity and context. These attributes include role, location, device type, and security posture. No longer does the system just look at an IP address. This change provides more granular access control and lets you fine-tune per-client application policies. It's like giving each user a finely tailored uniform!
- **Unified security policy:** ZTNA's biggest benefit is that it brings all users together in one place. Enterprise campus, branch, home office, or mobile users interact with a single security perimeter that doesn't end at the enterprise data center or branch edge network. This wall of safety extends from application containers to each individual user. Each user is mapped to a per-application policy that applies no matter where that application is hosted. No matter where users are or how they connect, IT can maintain a single set of policies for every user.


TIP

As part of a SASE solution, ZTNA can draw on a variety of contextual sources to make access decisions, including mobile device management (MDM). MDM provides a framework to monitor the security posture of employee devices, including bring-your-own-device (BYOD) endpoints. Although not officially part of SASE, MDM can play a crucial role in providing information about device security posture (such as whether a device is jailbroken and whether it's running up-to-date software and security patches) to support ZTNA services.

Cloud-based web security

SASE solutions also typically include cloud-based web security services, such as SWGs. SWGs monitor and control the flow of incoming and outgoing Internet traffic, evaluating that traffic based on state, port, and protocol. These gateways also filter based on policy. To do this, SWGs provide comprehensive cloud-based NGFW capabilities, all delivered as a service.

SWGs can apply a number of security services to network and cloud traffic, including the following:

- Application-level inspection
- Intrusion detection and intrusion prevention services (IDS/IPS) to monitor the network for policy violations or malicious activity

- Secure Sockets Layer (SSL) proxy, which can decrypt SSL traffic to find malware lurking in encrypted sessions

Additionally, SWGs provide a single point of security management to configure and update policies in the cloud. Instead of managing thousands of individual branch firewalls, IT can keep it simple.

Other SASE security components

Beyond ZTNA and SWG, SASE can include several other cloud-based security services:

- **Data loss prevention:** DLP services monitor network and cloud traffic to identify sensitive data, whether at motion or at rest, and prevent it from leaving the enterprise.
- **Cloud access security broker:** CASBs empower businesses to extend the same security policies they use for internal applications to public cloud applications and resources. CASB includes these capabilities:
  - Authentication
  - Auditing
  - Malware prevention
  - DLP
  - Encryption
  - Logging

  These features also provide intelligence on how employees and services are using cloud applications to protect against unsanctioned use.
- **Remote browser isolation (RBI):** RBI provides a safer web browsing experience by moving fetch and execute functions out of the business network to a cloud-based platform. Only sanitized, nonexecutable content renders in users' devices. This feature provides a safe, seamless user experience. Suspicious web forms (a common target for hackers) are rendered in read-only mode, preventing employees from entering their credentials by accident or on purpose.

IN THIS CHAPTER

- Eliminating problems with remote connections
- Expanding your access options
- Creating as-needed secure work locations

Chapter 3
Looking at SASE and ZTNA Use Cases

Secure access service edge (SASE) and zero-trust network access (ZTNA) give enterprises powerful new tools to provide secure connectivity anywhere, for all kinds of users accessing any type of application. And if there's one thing we've learned recently, it's that people may need to connect to anything, anywhere, at any time, for a variety of reasons. In this chapter, we explore how SASE and ZTNA work in real-world scenarios.

Solving Complex Connectivity Problems with SASE and ZTNA

For modern enterprises, work is no longer something that just happens in an office. Users may be working from home, on the road, at airports or in coffee shops over public Internet connections, and more. Enterprises have been adjusting to these trends for years, but the huge numbers of people working from home in the wake of COVID-19 have dramatically accelerated the rate of change (and maybe the sales of comfortable-yet-still-presentable clothing).

As businesses try to adapt to this new normal, they're finding that the network and security models they've relied on for years are too complex, clunky, and inefficient to keep up with changing needs. Businesses have to contend with the following concerns.

An expanded threat surface

As more users work from more locations — often using their own devices, connecting over the public Internet — enterprises face a higher risk of breaches, malware, and other Internet threats. The problem only grows as more enterprise data moves to software-as-a-service (SaaS) and cloud applications, where businesses face elevated risk of data loss or users failing to comply with corporate security policy due to poor data-handling practices.

Poor application performance

No matter how users connect — from a branch or home office, or remotely via virtual private network (VPN) — most of their traffic gets routed through the centralized data center for security inspection. This need to funnel all traffic through the data center, even when it's destined for the cloud or Internet, adds latency that can significantly degrade the user experience.

Complex access experience

Today, employees use different access methods depending on where and how they work. In the branch, they typically access all applications through the branch's edge gateway. When using a mobile device, though, they have to do things differently. Typically, working outside the branch means establishing a connection with a VPN concentrator (again, routing all traffic through the data center) or using specialized remote access web pages. These disparate experiences make access more complex and confusing, diminishing productivity and leading to more calls to the help desk.

Long, complicated setup for new services

The need to connect users in more ways, from more places, gets complex and expensive. For home offices and remote users, setting up the right networking and security often requires extensive

IT assistance. This process can become a huge burden, especially in circumstances like COVID-19, when businesses need to connect hundreds or thousands of users under tight timelines. Even in traditional branches, expensive private line circuits such as Multiprotocol Label Switching (MPLS) take a long time to provision and can be expensive to operate and scale.

REMEMBER

Put simply, you're dealing with long timelines, extremely complex solutions, and an ever-expanding budget.

Reimagining Access with SASE and ZTNA

SASE and ZTNA provide a framework to make connectivity simpler, more consistent, and more secure — even as the ways and places people work evolve. A SASE/ZTNA framework provides the following benefits:

- **Simpler cloud-based security:** SASE points of presence (PoPs) include a number of security services that help inspect traffic and centrally enforce security policy, no matter where people work or where applications are hosted. SASE PoPs are also typically collocated with cloud exchanges, providing a natural control point to apply additional cloud-based security. Ultimately, businesses can apply the full security stack from the cloud, including the following:
  - Next-generation firewalls (NGFWs)
  - URL filtering
  - Anti-malware
  - Secure web gateways (SWGs)
  - Data loss prevention (DLP)
  - Cloud access security brokers (CASBs)

  Unlike today's security stack, which relies on siloed solutions that are deployed and managed separately, SASE pre-integrates diverse security services into a single control point and management interface. This solution automatically applies the right protection to every connection, based on

policy, expanding the "intrinsic" security built into every network connection.

- **More flexible remote access:** ZTNA eliminates the need to use VPN concentrators or specialized remote access portals. Instead, a ZTNA agent installed on the user's device automatically establishes a secure Internet Protocol Security (IPSec) tunnel to the nearest SASE PoP.

  Hosted in any of hundreds of PoPs around the world, these gateways act as a broker between users and the resources they want to access, providing an application-specific VPN tunnel directly to the resource — and only that resource. Enterprises can now enforce security policy on a per-application basis, with access based on the user's identity and real-time context (such as location or device type), instead of just IP addresses. All of a sudden, the security perimeter no longer ends at the data center or branch edge network. It extends all the way from the individual application, no matter where it's hosted, to the individual user. The world just got a little smaller.

  In VMware's SASE solution, this ZTNA agent is integrated with VMware Workspace ONE.

TIP

- **More efficient, better-performing connectivity:** SASE solutions use software-defined wide-area network (SD-WAN) technology to provide an intelligent software overlay across all branches and home offices. This feature automatically routes traffic over the best available path and connection. Think of it like your maps app helpfully rerouting you to avoid a traffic jam. Application traffic gets routed to a gateway in a nearby cloud PoP — instead of getting back-hauled through the data center — eliminating delays and bottlenecks. The SD-WAN steers traffic on a per-packet basis to account for real-time network conditions such as delay, jitter, or packet loss, and automatically remediates problems detected over a given link.

In the following sections, we take a closer look at how these capabilities change the game for different enterprise use cases.

Extending the Branch Experience to Remote and Mobile Users

With SASE and ZTNA, businesses can extend the same business-class network and application experience that they'd get in a branch to remote and mobile users. At the same time, they can bring the complete enterprise security stack to all users, no matter where or how they connect. Remote and mobile users now get the following benefits:

- **A consistent, unified experience:** Network and application access looks and acts the same whether users are working remotely or in a branch.
- **Granular access control:** ZTNA provides a stronger security footing for remote users than conventional VPN connections. Internet transport is treated as inherently untrusted. And with per-application IPSec tunnels, users can only access the specific resources they're authorized to use, based on policy. This feature is just like a virtual ID badge for certain doors in the office.
- **Enhanced security:** With SASE, the business can apply a full security stack to remote and mobile users' traffic. For example, when remote users are accessing sensitive data from an unmanaged device, the business can automatically apply CASB services to ensure that SaaS and infrastructure-as-a-service (IaaS) application usage complies with corporate policy, and DLP to guard against data leakage.
- **Business-quality performance:** SASE SD-WAN intelligence automatically routes traffic over the best available path and connection, based on real-time network conditions. By reducing the need to backhaul traffic through the central data center, latency and bottlenecks are eliminated, and you have a more consistent, better-performing application experience.

Transforming a Home Office into a Branch Office

As working from home becomes the new normal, enterprises need to provide scalable business-class networking and security services for multiple types of home-based users. For example, a home-based radiologist who needs to securely access large diagnostic imaging files requires different considerations than an office worker who needs access to a subset of business applications with basic bandwidth requirements.

Businesses also need to protect against brownouts. During the COVID crisis, brownout rates increased dramatically as millions of workers shifted to home offices. From pixelated Zoom video calls to voice glitches, these issues severely degrade user experience (and inspire a million YouTube parodies).

Additionally, businesses need to make sure that the home office doesn't become an entry point for malicious websites or other threats. This possibility is a real risk when users rely on their broadband Internet service provider (ISP) to provide connectivity and Domain Name System (DNS) services.

Within a SASE framework, home offices act like any other branch office, with users connecting to a nearby SASE cloud PoP via a simple edge appliance. The edge appliance and connection can vary for different types of users. "Light" or "standard" users can do fine without top-tier connectivity, while power users (like that home-based radiologist) get high-capacity, low-latency connections that are basically indistinguishable from what they'd have at the office.

As in the branch, home edge devices connect to a nearby cloud PoP, which provides a direct on-ramp to the diverse public cloud applications and IaaS resources the enterprise uses. Home users get better network and application performance, while the enterprise can use the SWG services in the SASE PoP to apply anti-malware and other cloud-based security to their traffic, based on policy. What kind of results should you expect? Have a look:

- **Simpler IT operations:** By providing intelligent WAN connectivity and traffic handling as a service, enterprises benefit from zero-touch deployment; centralized policy-based

management; and end-to-end visibility, troubleshooting, and reporting. Home offices become much quicker to enable and easier to manage.

- **Improved performance:** The cloud-based networking intelligence of SASE monitors applications continuously. The result is improved application performance for both data center–hosted and cloud-based applications, even under brownout conditions.
- **Stronger intrinsic security:** Home users get the same strong protection they'd get working in a branch, with a full security stack inspecting their traffic, filtering out bad URLs, and applying anti-malware protection automatically in the cloud. They won't get a security guard or receptionist, but that's really the only difference. The combination of ZTNA for secure access and SWG for Internet applications protects the business, even when home users work over Wi-Fi or public Internet connections.

Connecting, Securing, and Optimizing the Branch

Today's "branch" can include a wide range of corporate sites, from small-footprint retail stores to large regional and national corporate offices. Historically, branches relied on inefficient legacy WAN architectures, where most traffic gets backhauled through the central data center.

Today, enterprises can make branch connectivity simpler and more efficient with SASE SD-WAN intelligence. Like home office users, branches connect via an SD-WAN edge appliance that provides software-defined traffic handling for all applications. The edge appliance connects to a nearby SASE PoP in the cloud, where it can apply cloud-based security services to public cloud and SaaS traffic, even as it improves their performance. In cases where additional local security functions are needed (such as advanced intrusion prevention and intrusion detection services [IPS/IDS] or unified threat management), branches can also integrate virtualized network functions (VNFs) from third-party solution providers into the branch stack.

Branches ultimately benefit from these outcomes:

- **Simpler operations:** SASE and ZTNA use a dynamic SD-WAN connectivity model, where much of the effort of bringing up new sites is fully automated via zero-touch provisioning. The branch network can now be managed from the cloud, as a service. IT can stand up sites and provision services much more quickly and easily, without needing expert staff on-site.
- **Reduced capital and operational expenses:** Businesses reduce their capital investments by replacing expensive routers and security and WAN acceleration devices at every branch with simpler SASE edge appliances. And, with the ability to use broadband instead of MPLS circuits — without sacrificing performance or security — they lower operational expenses as well.
- **Improved performance:** Moving to an SD-WAN model for branch connectivity eliminates the delays and performance issues that come with backhauling traffic through the data center. SASE also introduces a cloud-based control point to monitor and inspect all application traffic and, in many cases, automatically remediate issues.
- **More comprehensive security:** SASE makes it easy for branch employees to securely access cloud applications and the Internet, whether they're working on-site or remotely. Enterprises can apply security roles, enforce security policy, and apply services like ZTNA, NGFW, and SWG entirely from cloud. IT can now manage access for both branch and remote users with a single set of policies and enforce security based on each user's identity and context.

Setting Up Temporary or Seasonal Sites

There are many scenarios in which enterprises may need to set up temporary or seasonal sites. In the wake of COVID-19, for example, health-care providers rapidly set up mobile clinics, field hospitals, and testing sites. Each location had to adhere to the same data security and privacy requirements as primary care offices. These and other temporary implementations need secure, reliable network connectivity — even when they're in remote locations where the traditional WAN doesn't reach.

SASE and ZTNA make it easier to quickly bring up temporary sites, without compromising security. Enterprises can deploy SD-WAN edge devices wherever they're needed. They connect to a nearby SASE PoP, where they can apply a full stack of cloud-based security services, based on policy, to protect users, applications, and the network against Internet and cloud threats. The results may sound familiar at this point, but here's a review:

- **Improved performance:** SASE provides an intelligent SD-WAN overlay for any kind of remote site link (broadband Internet, satellite, or wireless connection). The solution monitors real-time link conditions and can steer traffic to the optimal path, based on policy. With the SASE PoP providing an on-ramp to cloud and SaaS applications, users also get a more consistent application experience.
- **Simpler setup and operations:** Businesses can set up temporary sites much more quickly using simplified edge appliances. These devices use zero-touch provisioning to automatically configure themselves, minimizing the need for on-site IT or network engineering personnel.
- **Comprehensive security:** Instead of having to route everything back through the central data center, SASE allows businesses to apply SWG, CASB, DLP, anti-malware, and the rest of the security stack at any location from the cloud. And with ZTNA, users have the same access experience, regardless of how they connect.

Inviting Everybody to the Party

Non-employee workers — contractors, partners, contingent workers, and others — are playing an increasingly important role in many enterprises. Like employees, these workers also need access to corporate resources and applications. Today, they often have to use specialized web and application portals, increasing complexity for both users and IT.

With SASE and ZTNA, bringing these workers securely into the business is much easier. ZTNA provides a seamless, automated

access experience, while protecting business applications and resources. Take a look at these advantages:

- **Simplified operations:** A SASE and ZTNA framework makes connecting non-employee workers just as simple as it is for branch users and remote employees, making your IT department's job a lot easier.
- **Improved security:** ZTNA-based services authenticate non-employee users and grant secure access based on their identity and context, such as, location, time, and device type and security posture. With ZTNA, these users can't even see, much less access, network resources they aren't explicitly authorized to use. The SASE framework also protects these users, and the applications they access, by using cloud-based security services like CASB and DLP to automatically enforce consistent, corporate-wide policy.

REMEMBER

All of these solutions point toward some common outcomes: increased security, simpler operations, more granular control, and reduced costs. See a problem there? Neither do we.

IN THIS CHAPTER

- Simplifying access to your services securely
- Basing access on identity and context
- Bringing all your users together

Chapter 4
Considering Context to Determine Services

Secure access service edge (SASE) and zero-trust network access (ZTNA) give businesses a more flexible, agile framework for secure network access. In this chapter, we show you how businesses can use identity and context to securely connect today's dynamic and mobile workforce.

Recognizing the Trouble with Traditional Access

Modern workforces are much more dynamic and distributed than they used to be. Companies are using more cloud-based applications, and user mobility has become the norm rather than the exception. In this new normal, traditional wide-area network (WAN) models, where everything revolves around the central data center, no longer make sense. Now, SASE and ZTNA offer a more comprehensive approach to secure connectivity that's easier for IT to manage, while providing a more consistent application experience for users.

In legacy models, where trust is based on whether users are "inside" or "outside" the network perimeter, security gets complicated. First, IT has to patch together multiple solutions — network and cloud firewalls, virtual private network (VPN) concentrators, secure web gateways (SWGs), and others — to protect against the different types of threats. And patching things together is a bad idea for both Frankenstein's monster and IT. Then, because security policy is dictated by the IP address of the user and network resource, IT has to configure multiple policies for every possible way in which users may connect. This process is typically done manually, so updating these policies can be laborious and require long lead times.

This model isn't great for users either, because they end up with inconsistent, sometimes confusing access methods depending on where or how they connect. Users often wind up being the integration point for the enterprise's disparate security tools — and they may even look for ways to work around them. Security is hard enough without your own users looking to circumvent them to make their lives easier.

Simplifying Access with SASE and ZTNA

With SASE and ZTNA, connectivity is tied to a user's identity and context, not an IP address. The network grants access on a per-application basis. And it can draw on a comprehensive networking and security stack in the cloud to automatically apply the right services for every scenario. Note also that, unlike traditional networks, with SASE and ZTNA, the user can be anywhere — even at home or in a coffee shop. The network applies consistent security regardless of location.

REMEMBER

SASE makes it easy to manage access and security, no matter where or when a user logs in.

Using contextual identity in this way requires a different approach to access. Instead of focusing on abstract or indirect concepts like source and destination IP address, the network makes decisions based on direct measures of security, such as user group membership and device state. Now, security can be enforced based on real-world concepts that are easy to understand and describe:

- Who the user is
- Where and how the user connects
- Which network and security services should be applied to the user's connection

The following sections examine these concepts in detail. Then we explore how a network using SASE and ZTNA can use contextual identity to enable secure, high-performing connectivity for all access scenarios.

REMEMBER

Using smarter, more agile access models has become even more important as the number of remote users explodes. The 2020 ZK Research Work-from-Anywhere Study found that the percentage of users working remotely nearly doubled, growing from 22 percent in 2019 to 42 percent in 2020. This represents a paradigm shift in the way people work, and it demands a comparable shift in how businesses secure those users.

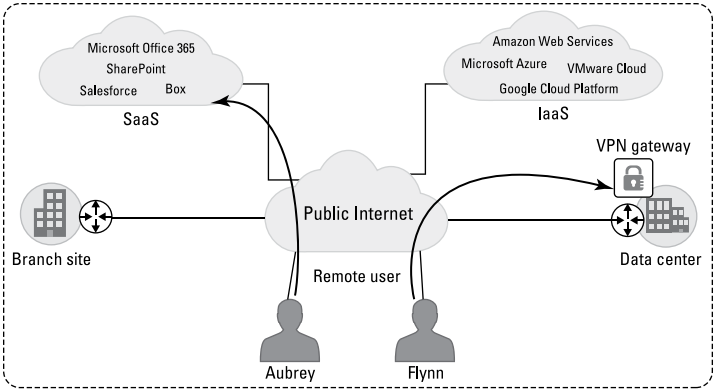
Looking at Identity and Context

To build a framework for secure access that's as dynamic and flexible as today's workforce, we need to define three basic elements:

- Identity types
- Context
- Services

Identity types

Businesses must be able to uniquely identify any user attempting to access business resources, whether hosted within the enterprise data center or in the cloud. Consider two remote users, Aubrey and Flynn (see Figure 4-1). Aubrey is an enterprise employee accessing a software-as-a-service (SaaS) application, such as Office 365, from a coffee shop over a public Internet connection. Flynn is a contractor accessing a controlled enterprise application hosted in the data center. Aubrey and Flynn are both remote users, but their unique identities matter a great deal in determining how and what they can access.



Aubrey is accessing Microsoft Office 365 over the public Internet.

Flynn is a contractor accessing a controlled enterprise application in the data center.

FIGURE 4-1: Identities make a difference for remote users.

Identity types can be grouped into broad categories, such as the following:

- **Enterprise users:** An enterprise user is typically a traditional employee, connecting to business applications from a branch location or corporate office, over the corporate network.
- **Remote users:** A remote user is someone accessing business resources, hosted in a private or public cloud, from outside an enterprise location or branch.
  - *Internal remote users* are part of the enterprise and need to access critical business applications from outside the office. Think of a sales manager accessing Salesforce while visiting a customer on-site, or an HR employee accessing Workday from home.
  - *External remote users* could be contractors, partners, or customers who need to access a specific business resource for a specific purpose. Examples include a contractor accessing an engineering portal to check in code or a partner accessing technical documents hosted in the private cloud.
- **Internet of Things (IoT) devices:** Human beings aren't the only types of users needing secure access. IoT devices also connect to the network and require special security

considerations. IoT endpoints used to be limited to specific verticals, but they've exploded in recent years. ZK Research predicts the number of IoT endpoints to grow from 25 billion in 2017 to a whopping 80 billion in 2025.

IoT devices can encompass a wide range of technologies. You need to secure everything from basic enterprise devices (printers, phones, videoconferencing equipment) to more innovative connected applications. For example, businesses can build safer workplaces by introducing connected cameras, thermal scanners, voice-activated devices, and other endpoints. In many cases, these devices connect over the public Internet, which means they need a higher level of security. Without adequate security, cybercriminals can easily intercept or alter data transferred between IoT devices and corporate servers hosted on-premises or in the cloud, or even hijack them to host new attacks.

WARNING

There is typically no way to load security tools onto IoT endpoints, so they must be secured via the network. That means everything, right down to the smart refrigerator reminding you to put more orange juice in the breakroom.

Context

After the network has established who the user is (identity), it analyzes the context for the access request. Context is about granting access to the right resources and applying the right services, based on a detailed picture of the user and what the user is trying to do.

The system needs some basic information to help determine context:

- How is the user connecting? What kind of device is she using and what's that device's security posture?
- Which resources is she trying to access and how sensitive are those resources?
- Which location is she accessing the network from and over what kind of connection?

The answers to those questions can dictate policy, allowing the network to apply the right network and security services automatically. In the example from Figure 4-1, we see Aubrey attempting to connect via a laptop running Windows 10, accessing an Internet application from her home Wi-Fi.

Services

The third component of contextual identity entails defining the services that the network will apply to that connection. In SASE, this includes both networking and security services, all of which can be delivered as a service from the cloud.

SASE networking uses software-defined wide-area network (SD-WAN) technology. An intelligent software network overlay selects the best path for each packet, based on real-time network conditions. To assure a consistent application experience no matter where or how users connect, SD-WAN can prioritize applications, monitor links, and automatically remediate issues. Within a SASE framework, this networking intelligence can even extend to "off-net" connections such as users' homes and remote endpoints.

On the security side, the network can apply services from the full security stack, such as the following:

- Access control lists (ACLs)
- Authentication and authorization
- Key management (Secure Sockets Layer [SSL]/Transport Layer Security [TLS])
- VPN

The network can also apply the many intrinsic security functions aggregated within SASE (ZTNA, cloud-based firewall, SWG, and others) to protect users, data, and applications in the cloud from internal and external threats.

Putting It All Together

Now, let's look at how identity, context, and services come together within a SASE and ZTNA framework. First, let's review how secure access works today.

As shown in Figure 4-2, a remote user seeking to access a business application must connect to the centralized data center via a VPN tunnel or some form of proxy device. Even if he's accessing a cloud application — even if there's a nearby cloud point of presence (PoP) for that application close to his remote location — all his traffic still gets routed through the data center, because that's where the security services live.

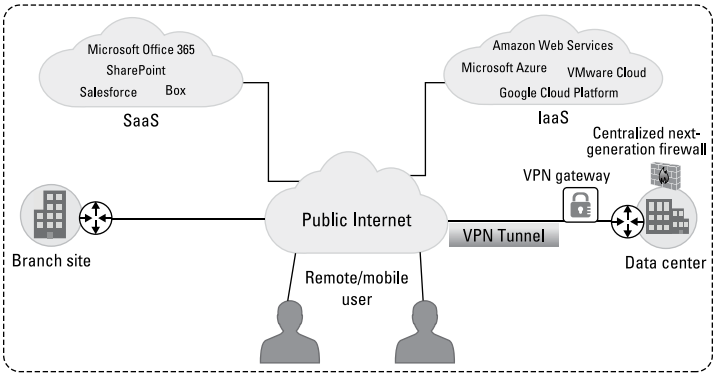


FIGURE 4-2: No matter where you are, the data has to make the same long journey.

Backhauling traffic in this way is inherently inefficient, adding latency that can deteriorate application performance. When large numbers of people are working remotely via public Internet connections, such as during the COVID-19 crisis, the problem gets even worse. Imagine a Los Angeles freeway at rush hour, but everybody is driving Big Wheels. This system also adds unnecessary bandwidth (and costs) as traffic "trombones" back and forth, effectively doubling the traffic volume. Finally, cloud applications often have issues with proxy security gateways, causing applications to time out and users to be frustrated.

To address these issues, enterprises want a more flexible secure connectivity model, one that's application-centric rather than network-centric and that lets users access cloud applications directly over the Internet, without performance penalties. Enter SASE and ZTNA.

WARNING

Traditional remote connectivity models based on VPNs aren't as secure as they could be, because they rely on an antiquated "inside-versus-outside" approach to trust. After a remote user is granted access to the network, she can access any resource there, including cloud applications. VPNs are also expensive and hardware-dependent, leading to high total cost of ownership. Ultimately, VPNs were designed for an earlier time, when just a small percentage of employees worked remotely. VPNs were never meant to handle today's large remote workforces.

Identity + context + services = ZTNA

ZTNA changes the game for secure remote connectivity. It implements a zero-trust model, where users can't even see corporate resources, much less access them, without explicit permission. Users access each individual application — not the full enterprise network — via a secure, encrypted connection. The network automatically applies the right security (services), allowing only trusted devices (context) and users (identity) to access the application. The network does this for both on-premises and cloud-hosted applications.

ZTNA maps each user to the policy defined for that specific application, regardless of whether the user is inside or outside the office. This allows IT personnel to maintain a single set of policies per user, reducing operational complexity and costs. It also ensures a consistent application experience, no matter where users connect from (remote or branch) or where the application resides (branch, data center, cloud, or Internet).

In the following sections, we explore what this means for different kinds of users and access scenarios.

Remote users

Bob is a remote user working on his corporate laptop from home, accessing applications hosted in the corporate data center as well as SaaS applications over the public Internet. This common scenario actually encompasses three different access models:

- **Bob accesses the Internet.** Bob types `www.yahoo.com` in his browser. The traffic from his home network gets redirected to a nearby SASE cloud PoP. SASE uses ZTNA to identify the user (Bob) and traffic type (Internet). As per

corporate policy for Internet access, it enables URL filtering, blocking access to web content that's inappropriate or potentially dangerous.

- **Bob accesses an enterprise application.** Bob, who works in sales, logs onto an internal sales application hosted in the corporate data center. The ZTNA framework verifies that Bob is authorized to access the application, and an application-layer firewall continues to inspect all traffic over that connection. Through his zero-trust connection, Bob can't even see, much less access, any application he's not specifically authorized to use. For example, if Bob were to click a link in an email for an HR SharePoint folder, ZTNA would block that connection, because Bob's identity as a sales employee doesn't allow him access.
- **Bob accesses a SaaS application.** Bob wants to use the company's cloud-based Salesforce application to access a bill of materials for a customer. Here, the cloud-based SASE solution provides seamless, secure connectivity to a nearby Salesforce cloud PoP, without ever routing Bob's application traffic through the corporate network or exposing it to the public Internet. The SASE solution also applies the right security based on Bob's identity and the application he's accessing. Finally, the SASE solution automatically adds cloud-based anti-malware protection, guarding against viruses, spyware, and other harmful or malicious programs.

Enterprise users at a branch

Vanessa is working from an enterprise branch office, accessing corporate applications hosted in the central data center, as well as SaaS applications and infrastructure-as-a-service (IaaS) resources in the cloud, over the enterprise network.

All traffic leaving Vanessa's workstation is inspected by the lightweight firewall at the branch to apply stateful application-aware policy.

REMEMBER

This policy can be applied per user, just as in the remote access case.

Traffic destined for cloud and SaaS applications gets redirected to a nearby SASE cloud PoP for more granular inspection and analysis. As Figure 4-3 shows, this analysis can include a variety of cloud-based security services:

- Intrusion detection service/intrusion prevention service (IDS/IPS)
- URL filtering
- Anti-malware protection
- Cloud access security broker (CASB)
- Data loss prevention (DLP)

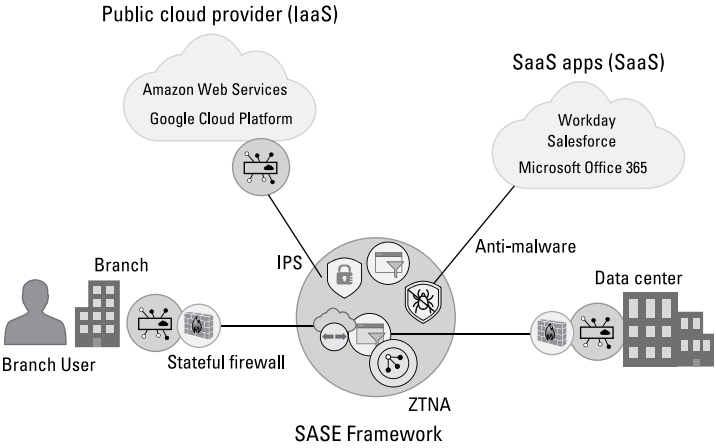


FIGURE 4-3: A typical SASE framework

Now, the enterprise can automatically apply additional layers of cloud security to Vanessa's SaaS and IaaS traffic, even when she's working in the branch. It uses cloud-based security like CASB and DLP to protect against data leakage and ensure that corporate security policy is always enforced — even when Vanessa is using cloud applications that don't get routed through the data center.

Internet of Things devices

A large regional grocery store chain wants to connect sensors in refrigerators at its retail stores and send temperature data to an application running in the corporate data center. The company

also wants to communicate with local temperature control devices at the stores, which connect over each store's Wi-Fi network. The devices upload historical data, logs, and statistics to a cloud-based management station over the public Internet.

For both of these IoT scenarios, the framework invokes SASE components such as cloud-based firewall, IDS/IPS, and anti-malware. It automatically applies the right protection for privacy, security, and data loss. The stores stay safe, and the milk stays cold.

IN THIS CHAPTER

- Building a smarter, more secure enterprise network
- Improving your business agility
- Making life easier for all your users

Chapter 5
Ten (Or So) Benefits of SASE and ZTNA

Secure access service edge (SASE) and zero-trust network access (ZTNA) change the game for securely connecting users — no matter where or how those users work. Here are the top benefits you can expect after you implement your SASE and ZTNA solution.

Building a Smarter, More Secure Enterprise Network

Enterprise wide-area networks (WANs) continue to play a crucial role in connecting enterprise users. However, the traditional hub-and-spoke topologies that many enterprise wide-area networks (WANs) still use no longer align with the way businesses actually work.

In these traditional WAN topologies, all branches and remote users revolve around the central data center, and all network traffic gets routed through it to apply security policy. This model made sense when most applications lived in that data center, too. Today, though, they don't. With the rise of cloud and software as

a service (SaaS), applications may be hosted anywhere. Users can be working from anywhere, too — in a branch, on the road, or in a home office. Routing all traffic through the data center can add latency, reducing application performance.

We need a different topology optimized for today's distributed applications and users — and SASE can provide it. SASE uses software-defined wide-area network (SD-WAN) technology to optimize routing for distributed, cloud-first businesses, but it doesn't stop there. SASE merges SD-WAN with cloud-scale remote access (ZTNA), secure web gateway (SWG), and next-generation firewall (NGFW) services, all delivered from any of hundreds of regionalized cloud points of presence (PoPs).

Reimagining the WAN with SASE and ZTNA can offer a long list of advantages:

- You can move network and security services closer to your users and workloads and establish a more direct path for Internet, software-as-a-service (SaaS), and cloud traffic.
- You eliminate the need to hairpin traffic through the central data center — and the latency and costs that come with such anchoring.
- You can provide inline security everywhere, no matter where users work or where the applications they're using are hosted.
- You can flexibly enforce security policy based on user identity, regardless of where users or applications reside.
- You can manage hundreds of sites and thousands of distributed remote users centrally in the cloud, through a single pane of glass.

Secure and Consistent Access for Branch and Remote Access Users

Yesterday's security models, where everything is based on whether access is "inside" or "outside" the enterprise, no longer work. To address the complex threat landscape that comes with

distributed users and applications, businesses need to rethink trust. That includes the following:

- Increasing focus on data classification and risk, and enforcing access on a more granular basis
- Taking into account the security posture of the device requesting data
- Factoring in the security posture of users themselves — verifying their identities, ensuring that they haven't been compromised, and analyzing their behavior for anomalies that could indicate a threat

The ZTNA component of SASE provides a "least privilege" framework to reduce that threat and provide greater depth and consistency in security policy enforcement. It grants access on a per-application basis and ties that access to a more comprehensive analysis of the user's identity, context, and risk.

Now, users can't even see, much less access, resources unless they're explicitly authorized. And, you can establish a user's identity with confidence across multiple access methods:

- ZTNA authentication
- SASE-based authentication methods via SWG
- 802.1x network access control

SASE also makes access more consistent by eliminating the need to use different methods inside and outside the branch.

With ZTNA, the user experience looks similar. Instead of having to log on via a virtual private network (VPN) concentrator or specialized portal, zero-trust clients on users' devices make connectivity seamless. When users connect through a branch or campus network, the zero-trust tunnel is automatically disabled. As soon as they connect from a non-enterprise network, though, enterprise traffic gets securely, automatically tunneled — without the user having to do anything different at all.

Simplified Security Policy Configuration and Enforcement

Many enterprise WANs still work as if everything revolves around the data center. Modern applications, though, are far more likely to be a mix of on-premises and multi-cloud. Users are also more distributed across campuses, branches, homes, and remote access — especially in the wake of COVID-19.

Network and security designs need to adapt to this distributed landscape and address the challenges that this distributed architecture creates in your ability to consistently apply and enforce policy. These challenges include the following:

- Dependencies between networking and security policy, where network policy may route traffic away from where security policy is traditionally enforced
- Configuring and maintaining policy across multiple sites and regions, which requires significant effort and can be a source of errors and inconsistencies
- Configuring and maintaining multiple standalone security solutions, even within the same site, also increasing errors
- High costs and risks in keeping track of the business's security state, because so many different systems and locations need to be analyzed (especially true if you have to undergo Payment Card Industry [PCI] audits or you have European sites subject to General Data Protection Regulation [GDPR])

SASE and ZTNA allow you to define and configure security policies centrally. The system automatically enforces those policies across all distributed regions, branches, and access methods. And because you can control everything from one place, it's easier to manage dependencies between networking and security policies.

REMEMBER

The SASE platform handles the complexities of distributed policy enforcement, using the security solutions and traffic paths that provide the best application experience for each user. SASE also provides a single, cloud-based control point to audit the environment holistically and better understand security risk.

Improved Security Posture Visibility

As users and applications get more distributed, the threat landscape becomes much more complex. To protect your business and users, you need not just a wider net but deeper analysis. You also need to understand more context — answering *who*, *what*, *when*, *where*, and *how* questions for every access attempt. Think of it like a really conscientious receptionist or bouncer.

A SASE solution consolidates metadata and threat intelligence across multiple sources, giving you a more comprehensive, context-driven view of security posture. The system analyzes:

- Security posture of the end device
- Risk profile based on SASE intrusion detection system (IDS) services and user behavior
- Network traffic patterns to identify anomalies

As a result, the larger SASE system now has much more information at its disposal, including users' group memberships and behavior patterns, as well as visibility into the workloads and applications being accessed. So, your security policies can be simpler, even as their effects are much more granular. You can also enforce policies through a single, cloud-based control point and give users flexibility in how much visibility you have into their data. And you have a single vendor integrating metadata from all the different SASE security services into meaningful, actionable information.

That integration alone is a huge benefit. It eliminates the need for your internal teams to manage and constantly monitor a long list of security point products across many distributed sites — as well as the errors that often come with that kind of heavy manual effort. Instead, a SASE solution consolidates multiple security point products and services into a unified, holistic framework. The SASE provider pre-integrates everything, eliminating the complexity of having to configure and monitor everything separately. You gain broader, deeper visibility into the security posture of distributed users and devices. And, you get unified monitoring and reporting across everything.

Improved Business Agility

SASE and ZTNA eliminate a huge amount of operational effort from your internal teams, allowing you to make changes to your business more easily. By pre-integrating multiple network and security point products, your SD-WAN appliances, SWGs, firewalls, and other solutions all work together as part of a unified system across all sites and regions. This reduces deployment timelines and complexity to bring up new branches, temporary sites, and home offices.


TIP

It's also now easier to onboard users — no matter who they are or how they connect. For remote access, ZTNA uses a smaller, simpler footprint on client devices. Users get better performance on those devices, while the enterprise gets faster certification and deployment. In the same way, it's now much easier to share resources with third parties and contractors and extend secure access to them.

All the Benefits of SD-WAN, Baked Right into SASE

SASE includes SD-WAN as one of its core components. So, when you use a SASE solution, you not only get more flexible security and access, you get all the benefits of SD-WAN:

- **Improved application performance:** With integrated SD-WAN technology, SASE solutions reduce latency for cloud and Internet traffic. This "optimized flight path" for WAN traffic inherently improves application performance. SASE SD-WAN solutions can also use advanced packet loss recovery mechanisms to deal with "lossy" connections (such as backup wireless links), without having to retransmit packets, which can make delay-sensitive voice and video applications downright unusable. SASE SD-WAN technologies can also employ application-specific routing, such as routing all voice and video traffic over low-latency paths, to ensure a better user experience.

- **Reduced risk of bandwidth congestion:** SASE SD-WAN intelligence combines all WAN links in and out of a given branch to create a larger pool of bandwidth. More advanced implementations can fully use that combined capacity — instead of using statistical load sharing, which can sometimes cause individual links to get overloaded.
- **Better user experience for remote workers:** With a SASE networking and security model, remote users now connect with a horizontally scalable headend in the cloud that's geographically close to them. This implementation reduces latency and provides a better user experience, especially for voice and video applications. You also gain the flexibility to customize connectivity for different types of home-based users. For instance, a typical business user can use the standard ZTNA access method from home. Meanwhile, power users that require higher quality and reliability (for example, a home-based radiologist who needs to work with huge imaging files) can use a thin-client SASE appliance, bringing SD-WAN right into the home office.
- **Improved reliability and resiliency:** A multi-tenant SASE service uses economies of scale to amortize costs over many customers and sites and deliver built-in high availability. You also get the benefits of that SASE provider's expertise, because they have amassed extensive knowledge from building and maintaining network and security services at a global scale. Inside any SASE cloud PoP, you (or your SASE provider) can also build multiple layers of redundancy. And because the SASE service spans multiple regions, you have full backup PoPs by default.

Lower Costs

By consolidating networking and security products and vendors into a single, easy-to-manage solution, SASE reduces both capital and operational expenses. You now have seamless interconnectivity between remote access and SD-WAN technologies. You're also now consolidating on a single cloud-delivered solution for both (reducing capital investments), with the ability to manage everything from one place (reducing operational expenses).

Building out new branches and home offices also gets easier, because it requires less space, power, and on-site IT expertise. Integrating your SASE network and security services with other IT security and management systems also gets simpler and less expensive.


REMEMBER

SASE SD-WAN intelligence also reduces WAN costs by eliminating the need to hairpin all traffic through the data center. It allows branches to use lower-cost links, like broadband, without sacrificing performance or reliability.

As a managed service, SASE shifts the burden of software upgrades and security updates to your SASE provider. And because your networking and security is now an elastically scalable cloud service, you pay for only what you need, instead of over-allocating resources on premises.

All of these benefits reduce the overall costs of both deploying and delivering the services needed to connect your users securely to your applications.

Notes

Notes

vmware®

Conduct SASE at Scale

Strike the perfect chord with cloud networking and security.

Upgrade your network's speed, safety, and reliability!

Your employees can work from anywhere, so your network needs to provide office-like quality and security wherever work happens. SASE and ZTNA help you implement the tools you need to deliver access wherever and whenever that need exists. Don't rely on outmoded network concepts. Meet your remote workers where they are, safely and securely. Remote access isn't just an option — it's a necessity. Make the experience easy to use and hard to hack!

Inside...

- Connect your remote workforce
- Understand different SASE and ZTNA components
- Transform secure connectivity in your enterprise
- Expand your network access options
- Base access on identity and context

vmware®

Roopa Honnachari of Frost & Sullivan, **Lee Doyle** of Doyle Research, **Keith Townsend** of The CTO Advisor, **Zeus Kerravala** of ZK Research, and **Craig Connors** and **Pere Monclus** of VMware contributed to this book.

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

ISBN: 978-1-119-76643-8
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

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