Brought to you by:

netskope

Designing a SASE Architecture

for dummies®
A Wiley Brand

Master cloud security

Address key changes to apps, data, security, and networks

Improve and maintain the user experience

Netskope Special Edition

Jason Clark
Lamont Orange
Steve Riley

About Netskope

Netskope, the SASE leader, safely and quickly connects users directly to the Internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, Netskope is fast everywhere, data centric, and cloud smart, all while enabling good digital citizenship and providing a lower total-cost-of-ownership. Go to www.netskope.com to learn more.

We would like to thank a number of individuals that made publication of this book possible:

From Netskope: Amanda Anderson, Mike Anderson, Chad Berndtson, James Christiansen, Tom Clare, Mark Day, David Fairman, Maxwell Havey, Scott Hogrefe, Kathy Jacobsen, Greg Mayfield, Mariesa Milan, Sasi Murthy, Krishna Narayanaswamy, Lauren Polito, Kate Reid, Zoe Revis, Brian Tokuyoshi

From Evolved Media: Karen Queen, Evan Sirof, Lauren Wagner, Dan Woods

Designing a SASE Architecture

Netskope Special Edition

by Jason Clark, Lamont Orange, and Steve Riley

for dummies®
A Wiley Brand

Designing a SASE Architecture For Dummies®, Netskope Special Edition

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

ISBN 978-1-119-80073-6 (pbk); ISBN 978-1-119-80074-3 (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: Vivek Lakshmikanth
Special Help: Nicole Sholly

Introduction

Your employees, partners, and customers increasingly use the cloud instead of private networks and data centers. Security can't inhibit how they do things. Meanwhile, you and fellow business leaders are struggling to realign security for an environment that, if you're using traditional security tools, is outside your control. This balance of security and user experience is difficult to achieve in "normal" times, but no catalyst has challenged organizations like the COVID-19 pandemic, which drove millions of workers home.

The complexity of the security landscape has challenged even the best security teams and increased the chance of misconfigurations and breaches. Conflicting products, services, and industry messaging make it challenging for security decision-makers to embrace opportunities while refactoring security to suit their needs.

An emerging networking and security architecture called secure access service edge (SASE; pronounced "sassy") points the way forward. Next-generation secure web gateways (NG-SWGs), cloud access security brokers (CASBs), and Zero Trust principles represent critical building blocks for SASE architecture that combines key network services and network security services into a unified system to protect business interests in, and the usability of, the cloud. But how to architect it all the right way and in the right sequence? That's where this book comes in.

About This Book

This book can help you develop a road map for implementing networking and security projects that will deliver positive, incremental results in the near term while paving the way for a resilient, secure future that's cloud-first. It cuts through the marketing blather you receive from purported SASE vendors, giving you a practical understanding of what SASE is — and isn't — and enabling you to future-proof your investments in security and networking to ensure adapting to inevitable changes is as easy and cost-effective as possible.

Foolish Assumptions

You aren't a stranger to the Internet. You know it's home to a wide variety of cloud-based digital tools that people use for both work and personal needs — tools that are in use without the involvement, let alone the approval, of security and IT teams. You're also aware that the cloud can be a dangerous place where the credentials and data of both individuals and companies have been attacked. Lastly, you have an interest in fixing that challenge for your company, employees, shareholders, customers, and business partners.

Icons Used in This Book

We use icons in the margin to call attention to important information. Here's what you can expect:


TIP

Anything marked with the Tip icon is a shortcut to make a specific task easier.


REMEMBER

The Remember icon flags facts that are especially important to know.


TECHNICAL STUFF

When we offer up highly technical info that you can safely skip, we use the Technical Stuff icon.


WARNING

Heed anything marked with the Warning icon to save yourself some headaches.

Beyond the Book

Although this book is chock-full of information, if you find yourself at the end of it thinking, "Where can I learn more?," just go to `www.netskope.com`.

IN THIS CHAPTER

- Recognizing how the nature of security has changed in the cloud era
- Identifying how pre-cloud security practices create new problems
- Getting to know SASE and how it enables the cloud for business
- Creating lasting business value with a SASE architecture that works
- Separating SASE value from marketing noise

Chapter 1
Seeing the SASE Vision for Securing Cloud-First Enterprises

The term *cloud* is tossed around so frequently, it can be hard to figure out just what it means. In terms of applications — and in greatly simplified terms — the term *cloud* may refer to:

- **Private cloud:** Applications in your data center.
- **Public cloud:** There's a lot that's sometimes meant here, including infrastructure as a service (IaaS) and platform as a service (PaaS), but for simplicity's sake, just think of the public cloud as applications that are available over the public Internet.

- **Virtual private cloud:** Private applications accessible from the public cloud.
- **Software as a service (SaaS):** Applications hosted by a third-party vendor and accessed over the Internet.

That casual application of the word *cloud* can make it hard to evaluate options and their relationship to your specific needs. Start by understanding what you need security to do. That information will help clarify the issues, because you need these capabilities across every cloud interaction.

In this chapter, you discover how the cloud has changed security, why pre-cloud security no longer works in the era of cloud, why traditional network approaches like hairpinning don't work, how secure access service edge (SASE) can enable your workers to work securely and productively in the cloud, and the defining factors of best-in-class SASE.

NICHE NO MORE

Cloud-centric vulnerabilities can no longer be thought of as "niche." As of 2021:

- The number of cloud apps in use per organization increased 20 percent over the previous year. Organizations with 500 to 2,000 employees now use, on average, 664 distinct cloud apps per month, according to a February 2021 report by Netskope.
- Sixty-one percent of malware downloads can be traced to cloud storage and collaborative apps as of December 2020, up from 48 percent in January 2020, according to the Netskope report.
- Fifty-five percent of sessions are app- and cloud service- related in web traffic, according to the Netskope report.
- Eighty-three percent of users access personal apps on company-managed devices, according to the Netskope report. This is the urgent security issue you must address: how to enable your organization to make the most of everything the cloud can offer in terms of flexibility, cost management, and new approaches to business opportunity, while keeping your business users, customers, data, and other precious assets safe at all times.

How the Cloud Changed Security and Networking

Once upon a time, corporate data centers were the mighty fortresses of the business world. Companies erected these digital citadels and then built and deployed business applications within their walls. Inside the fortress, companies established private networks that connected people to data, including staff at headquarters, employees in far-flung branch offices, and road warriors traveling the globe.

Like all great castles, there was an obvious perimeter: a wall with a guarded gate. Access to and from the wilds of the Internet beyond the gate was strictly regulated. Gatekeepers could keep a vigilant eye over traffic along their few protected network roads, letting in the righteous, keeping out anything suspicious, and leaping into action at the first sign of trouble. Every exchange with that outside world was forced to travel back and forth along the narrow confines of the private network.

First a trickle, then a torrent, of business users gravitated to apps based in the cloud. Cloud-based apps — for social media and communication, for collaboration, and for crunching the details of sales, finance, marketing, and customer relationships — were simply better than anything offered in-house. Then enterprises and even slow-to-evolve government agencies got onboard. Today's organizations favor SaaS applications and have adopted sweeping cloud-first policies that mandate solving business challenges with cloud solutions and moving critical enterprise systems to the cloud.

Things changed when new, powerful applications became available in the cloud. People, devices, and applications are mobile on and off your network. SaaS products provide fantastic capabilities to companies, faster and better than previous approaches that required long development times and acquisition of hardware and software.

As the last decade ended, the growth of spending on cloud activities increased significantly to far outstrip the pace of all other parts of IT budgets, according to Synergy Research Group. By 2024, more than 45 percent of IT spending on system infrastructure, infrastructure software, application software, and business

process outsourcing will shift from traditional solutions to cloud, making cloud computing one of the most continually disruptive forces in IT markets since the early days of the digital age, according to Gartner.

Yet, many of these cloud-based tools remain outside the visibility and control of IT departments. From a security perspective, that's troubling. But security isn't just about protecting cloud apps.

Security is also about providing all the protection needed when your entire workforce has gone remote. Wherever they are, your users need to be protected from attacks and provided guardrails to keep data and applications safe. And from a networking point of view, the experience needs to be not only safe, but also functional. Security can't be a bottleneck to the undeniable productivity users realize when they can use the cloud to get more stuff done, faster, from wherever they are.

Then there's information. Data (everything from intellectual property and sales figures to customer credit card numbers) is valuable treasure possessed by your business — perhaps more valuable than the products you sell. The fact that IT security is the stuff of front-page headlines is not surprising; when it is, the news is rarely good. With data, applications, and people mostly operating in the cloud, old security techniques developed for primarily on-premises data centers and other traditional infrastructure have struggled to keep up. The world has seen a rising wave of attacks from a variety of hackers using sophisticated techniques to wreak havoc and exploit vulnerabilities in cloud applications and how they're accessed.

The transition to cloud hasn't been easy or seamless. The old roads running through the data center network are littered with obstacles, annoyances, and inefficiencies that slow productivity, frustrate users, and compromise security. Applications based in the data center pale in comparison to SaaS apps in terms of productivity, user experience, and convenience. The much-needed improvements brought by SaaS have empowered salespeople to sell more, marketers to amplify their messages, HR departments to find the best job candidates, and product developers to work faster. Giving up SaaS would mean letting go of unprecedented productivity. No business wants that.

The catch was that these SaaS applications required data from inside the walls to be useful, and yet the applications were outside the walls, so they weren't controlled or protected by security. Corporate security, knowing it had very little control over things "out there" in the cloud, had two choices: Say no or pretend not to notice. This is what's now described as *shadow IT,* where users and even whole departments circumvent IT and security to use SaaS tools like Salesforce and Google Docs as well as large file-sharing tools like Dropbox that are convenient but not approved for business use. Shadow IT has existed for many years, but its use (and danger) accelerated thanks to cloud adoption. Security professionals, with their toolkits built for enterprise data centers and the old style of how to keep track of and control applications, find themselves in a real bind.

REMEMBER

Old security always forces compromises: Choices that raise some standards, such as speed or flexibility, come at the cost of others, namely security. SASE, done right, is *enabling.* It enables the people closest to the problem to innovate and solve problems with technology in a secure and governed way — all while helping IT leaders have a better understanding of their business.

The Problems of Pre–Cloud Era Security

Pre–cloud era security tools, techniques, and technologies are still in use everywhere. Very likely that includes your own company's IT infrastructure. This creates a situation in which a lot of security "stuff" is out there, but the result is anything but secure, or efficient. The lingering problems usually fall into one of two categories: the wrong approach or no strategic approach at all.

The wrong approach

One of the perceived benefits of an enterprise data center and the efficacy of its security was that it kept a company's digital assets in a single, safe location. A company could then build its own private network to connect workers at headquarters, as well as those at branch offices, and control their access to the bits that they needed within the data center.

REMEMBER

Companies still need data centers. But today, the data center is just one of many places users and data go. It's no longer at the center of anything, either for business needs or as a single security control point.

Security systems for data centers are usually appliances — physical boxes plugged into the data center to serve specific, narrow functions. Over the years, enterprises may have purchased security systems from hundreds of vendors; as of 2021, the average enterprise has bought and deployed scores of security products. In the majority of cases, those products were not designed to work together. It's all but impossible for security staff to integrate all these systems into an orchestrated, adaptive security solution that can enforce policies that support cloud applications and remote workers.

WARNING

Having diverse systems often results in console chaos (and perhaps arguments over who gets to sit at which consoles). Your security and network personnel may face dozens of different management windows, each with its own priorities and all competing for attention. Making sense of the big picture or a single situation may be impossible when you're in the crunch of diagnosing an issue. Security processes like these are also reactive, often relying on logs to replay and diagnose what happened. Worse, this spaghetti bowl of systems defies establishing the kind of order that would make everything more secure. You can achieve that order and security only by creating a system of detailed rules with the nuances to automatically maintain security across the endless variety of digital interactions taking place.

REMEMBER

The role of security isn't just to shout "no." You want to say "yes" to things that enable your business to work more quickly and effectively, especially with a distributed workforce. Security must prioritize protecting users and data, but it also must adapt in real time to keep pace with fast-changing requirements. That means providing users with a smooth, productive work experience wherever they happen to be by letting them access the data they need using whatever tools enable them to be the most productive and successful.

No approach at all

Your users are everywhere, and today's network needs to be designed with that in mind. Trying to repeatedly force all of a user's traffic through the data center's numerous security services

stifles productivity. (Sometimes security and network professionals call this tactic *hairpinning*, which means forcing users to constantly slow down and change course instead of heading directly where they need to go.) Hairpinning results in business systems that are less usable, performance that is dramatically reduced, and users who become frustrated.

How big is the challenge of controlling this new environment? Here's one example: The National Institute of Standards and Technology (NIST) is mandated by the U.S. Congress to provide organizations with cybersecurity guidance. NIST published a Cybersecurity Framework that identified 400 points of control to be considered for securing any application in your organization. That number is likely low because it assumes that everything — the user, the data, the application, and the network — resides on-premises. And that's no longer the case.

The huge range of controls you have for people and services within your network isn't available to your security systems when it comes to SaaS applications. Your strategy must be to secure a far broader landscape, in real time, and do it all using just three control points:

- The data, which you own, that flows in and out of the SaaS applications
- The identity of each user who's accessing those apps
- Approval based on whether your business conducts business with the outside entity

REMEMBER

The key to successful cloud security lies in readjusting your focus. Past security systems were largely based on controlling access. They were the walls and gatekeepers of the castle. That castle-and-gate approach no longer works. For cloud security to succeed, you should focus not on access but on activity: who's doing what, how applications are being used, what data is going where. If you're tired of thinking about castles, consider a basketball metaphor: It's time to switch your security from a perimeter-based zone defense to an activity-based man-to-man defense.

TECHNICAL STUFF

Older security systems typically know where on the Internet a user is headed. But the SaaS application they're using may itself rely on tens, hundreds, or even thousands of additional resources to populate the web page your user sees. To secure the cloud, you need to know those details. Your legacy tools don't do things

like decrypting Transport Layer Security (TLS), which would let them see what's happening inside the traffic of the user's communication with that application. Those tools also can't spot certain application programming interface (API) connections that the SaaS application uses to exchange information with other, unknown resources to build a rich environment for the user. Without that type of detail, you can never be certain that your data is safe or that what your user is seeing has been legitimately sourced.

Defining SASE

On one level, SASE means moving the network security perimeter controls to the cloud, while at the same time making those controls faster, more application- and user-aware, and data-centric.

On another level, SASE means a new architectural strategy for security and networking that your organization will work to achieve. It addresses the fact that a cloud-centric world needs an updated model for security and networking — and addresses fundamental ways in which security, networks, applications, and data protection have all transformed.

Functionally, SASE comprises a body of integrated, interlocking security and networking services built and delivered not only to grant users access to the cloud, but also to continuously monitor their activities, their devices, and applications they use so that data can be secured at all times, at every point it's accessed, all without sacrificing user experience. The good news is that the foundation of your SASE security architecture can be deployed today, and in deliberate, incremental steps (see Chapter 5).

WARNING

One of the defining characteristics of SASE is that every aspect of this security architecture is purpose-built for use in and with the cloud. It doesn't repurpose devices or code intended for data centers. You already know the reason why: Security services for the data centers primarily seek to control access. They don't speak the native language of the cloud, which is rich with nuance and information describing connections between points and describing the data contained in the flow of traffic between points. Keep this in mind as you evaluate security and networking options.

Context is crucial and an informative guide to just how deep and rich this new security architecture intends to be. SASE contextual factors include the following:

- The identity of the user
- The device being used to request access
- The location from which access is being attempted
- The identity of the applications being accessed in the cloud
- The data being requested — what it is and where it's stored
- The user's behavioral patterns
- The application interaction — what the user is specifically trying to do

Then, while continuously reevaluating that dynamic stream of information, the SASE security system applies security based on policies that determine the following:

- The service level and type of network services to apply
- The use of appropriate types of data encryption
- The level of data protection to be applied to prevent misuse of data
- The level of authentication to apply
- Whether the application requires the use of specific, specialized security services such as a cloud access security broker (CASB) to further intermediate in the activity

REMEMBER

Yes, a lot's going on in a SASE architecture. But when it's truly functional and properly implemented, SASE dramatically simplifies and improves the quality of your security and your network connectivity. When SASE is done right, all these things happen in real time, including continuous risk management. By moving security services out of your data center and into the cloud, closer to both your points of vulnerability and your users, you gain greater visibility and firmer control over what's going on, with whom, at all times. SASE helps network and security teams transition to enable the new applications and way of doing business while at the same time protecting the older, on-premises applications' access.

Seeing the Business Benefits of SASE

The reasons for adopting a SASE model for security closely align with the value that business has broadly recognized in the embrace of the cloud. The cloud makes it possible for people and businesses to work more effectively, collaboratively, quickly, flexibly, and cost-effectively. SASE makes that progress safe.

Enabling the growth of the business as it embraces digital transformation

Security needs to be like brakes on a fast car. It's there to enable going fast (because you know you can stop if needed) so you can manage the risks more quickly. It's not there to slow the business down and not let it go fast. It's not there to prevent speed in the first place.

You can't do digital transformation in a secure way without transforming your security controls. As every business is adopting new technologies to accelerate growth and be closer to the customer, the IT organization can significantly assist the business by moving the security controls to follow the user and the data, removing a lot of friction out of the process. Give your users the apps and access they need with just-in-time coaching on how to be safe with their use.

Keeping up with change

The cloud delivers crucial services across all aspects of your business, and new use cases emerge daily. Your company has certainly approved some cloud services for its users. And if there is an unapproved cloud service that does things better, faster, and cheaper for individuals or whole organizations, there's a high probability that someone in your organization is using that, too. They've sidestepped security, paid the subscription fee, and downloaded the app, and they're using it every day.

Reducing costs

REMEMBER

There's an oft-repeated truism regarding security that says, "If you think security is expensive, try a security breach." According to research published by IBM and Ponemon, the average total cost of a data breach is $3.86 million. Most companies realize they need security, but they rarely appreciate how much they need it until they experience a problem.

Security is often perceived as a cost center that is at its least visible when it's working its best. Security is actually a business enabler, but even putting that true role aside, the security budget, whether ample or thin, needs to be spent judiciously. Sadly, judicious, efficient spending on security is something many organizations still struggle with.

SASE brings important cost-efficiency advantages. With its highly integrated approach to security services, SASE can help reduce capital spending, consolidating the capabilities of many data center security appliances. With fewer systems to monitor and maintain, SASE also reduces operating expenses. There are further savings in vendor consolidation, improved network design, and efficient interaction with cloud providers.

SASE also helps overcome the much-mentioned global shortfall in skilled cybersecurity workers. By automating much of the detection and response activity, you can reassign skilled staff to higher-value activities, such as developing security policies that enable new, accelerated business activities or building artificial intelligence (AI) models that expand the automation and flexibility of the security infrastructure. The SASE architecture makes better and more adaptable use of individual team members than any other enterprise security framework.

Maintaining simplicity

Human error is one of the leading contributors to the increasing frequency of security incidents. That's partially a reflection of the unwieldy complexity human security analysts confront, the direct result of legacy security and network systems being used to do jobs for which they were never intended. These systems wrestle daily with a modern Frankenstein's monster brought to life in the form of dozens of monitoring applications that don't speak a common language with each other or with the people administering them. SASE provides a clear game plan so that many security services can work together in an understandable way.

Busting SASE Myths

WARNING

This probably isn't the first *For Dummies* book you've read on SASE, and it probably won't be the last, though it's our job to make it the best! Joking aside, as with any emerging technology or trend, SASE is ripe for misinformation. Just as slapping an *i* before

a product name doesn't automatically confer design elegance, and adding an *e* doesn't translate into power and efficiency, the SASE moniker is already being co-opted, over-marketed, and misinterpreted. Here are several common myths.

Myth: SASE can be supported by legacy technology

Today's network security infrastructure is the product of years (in some cases, decades) of development and sales efforts. But no amount of patching, tweaking, and upselling magically turns legacy appliances into cloud-native security solutions. The cloud demands a fresh approach.

Myth: SASE can be built using a regular SWG as a foundation

Previously, secure web gateways (SWGs) were dedicated to controlling access and defending against web threats. SASE has a much wider mandate that also includes applications, cloud services, data protection, and data loss prevention. (Chapter 2 looks in detail at how next-generation SWG [NG-SWG] services meet those broader needs.)

Myth: SASE lets you keep your network architecture

SASE can be effective only when its policies and enforcement are out at the edge, close to where your users, devices, and applications meet. This proximity is what gives SASE its dynamic security characteristics and provides the performance and reliability users require to be their most productive (and least frustrated!).

Myth: SASE doesn't need to see all your network traffic

SASE is effective precisely because it's an all-in approach to security. Its power, simplicity, and impact are powered by its ability to develop context about users, data, and applications, including underlying APIs. SASE thrives on visibility. That rich context is precisely what makes SASE so effective in a landscape that offers far fewer control points than the old data center ever had.

Myth: SASE adds to complexity

Complexity is the bane of your and every security or networking person's existence, and it's the common denominator among the majority of headline-grabbing failures of security. SASE demands that every piece of your network security work together in harmony. Network security cobbled together piecemeal can never deliver on the SASE vision of a single, integrated cloud security architecture in which policy and enforcement are perfectly orchestrated and adaptable to rapidly changing requirements.

Myth: SASE needs to start with the network using SD-WAN

As an advance in networking technology, software-defined wide area networking (SD-WAN) can greatly simplify the management and operation of a wide-area network (WAN) and be a useful — and more cost-effective — option against legacy connectivity technologies such as Multiprotocol Label Switching (MPLS). The usefulness of SD-WAN shouldn't be dismissed; nor should its relevance as a SASE building block be ignored. However, many vendors that are focused on SD-WAN have already made a marketing leap to "SD-WAN is the right way to get to SASE" — one that's intellectually dishonest at best. SD-WAN — and firewalls, for that matter — aren't the only way into SASE, nor are they the most critical building blocks.

Myth: SASE doesn't need a new ecosystem of vendors

It is all but impossible for companies to fully unburden themselves of their past — old products, biases, beliefs, and investments. Companies with a history of acquiring other companies and technologies, and that have built deep wells of institutional knowledge that they perceive as significant assets, struggle to shake free of those burdens. SASE is a new approach to networking and security. You won't build for the future if you (or your vendors) try to shoehorn yesterday's solutions into tomorrow's needs.

IN THIS CHAPTER

- Understanding what your security needs to become cloud-native
- Identifying how SASE creates security fit for the cloud
- Understanding why NG-SWG is an important building block for true SASE
- Looking at NG-SWG in action

Chapter 2
Recognizing the Importance of the Next-Generation Secure Web Gateway

Until recently, much of security strategy focused on web threats. That makes sense. Before cloud services were embraced, web traffic and web links in emails were the primary source of digital threats. The tactics of security departments — along with widely used appliances such as traditional secure web gateways (SWGs), web filters, and proxy devices commonly found on enterprise networks — were all tuned to the frequency of the web.

That approach also made sense in the era when most employees worked in corporate buildings and connected to resources and the Internet using company networks. Today, however, when your users are "at work," they're often remote, mobile, moving among different networks, and getting things done using the cloud. People use a wide range of devices as they work from home, spend productive time in their favorite coffee shop, visit customers, and

travel. All this adds up to a dynamic workforce that connects to networks, apps, and data distributed everywhere, all the time.

The cloud era clearly requires enhanced security. But if you've ever stood in line at an airport, you know increasing security doesn't always mean better security, and it doesn't guarantee a great user experience. At the airport, TSA PreCheck and trusted traveler programs help speed passengers to their flights. Significant aspects of security procedures shifted away from security officers and other bottlenecks at the airport toward a vetting process that begins before a passenger arrives at the airport. The intent is to enhance the experience for passengers and ensure reliable security and greater efficiency to the entire system.

A next-generation SWG (NG-SWG) is an important step toward secure access service edge (SASE) and is increasingly more often embraced as the first step because it moves you the most amount of distance and maturity on the SASE journey in a very quick fashion.

Moving Out the Old

Following the same pattern the travel industry adopted for frequent travelers, the security industry had to reconsider how and where to deliver enhanced security. The hardware appliances of previous generations of security were designed to protect networks and data centers, not cloud applications. Nor were they designed to offer the flexibility and responsiveness users expect in a cloud experience.

This mismatch — attempting to use old appliances for new outcomes — has led to painful, overly complex security configurations that result in frustrated users, lost productivity, painful errors, and slow responses to security breaches. Previous-generation tools don't adapt to the shifting nature of work in the cloud.

Here's an example of how that mismatch affects security and illustrates why SASE is critical today: Under the old approach, security systems check when a user's browser makes connections to web servers. Security analysis doesn't extend beyond checking a list to determine whether a URL is good or bad. (Chapter 1 describes this as a zone defense.)

That's a big problem for anyone securing the cloud for their enterprise. One of the fastest-growing security challenges is breaches taking place *inside* those approved connections (that is, *after* you say okay to a URL). Attackers present seemingly legitimate forms to collect information within a compromised software as a service (SaaS) app or cloud service to trick your users into giving away precious data and login credentials. Sometimes employees, in an understandable hurry to do things quickly, cut, copy, paste, share, and shift sensitive data to places where your organization doesn't want it. A zone defense no longer provides adequate protection in this environment.

The rapid rise in the importance of cloud services to businesses and the growing number of remote workers means you must develop and adopt new approaches, including SASE. Your cloud-reliant enterprise requires security that can keep up with nearly infinite permutations of location, device, and user identity. The purpose is to safely speed users on the way to highly productive interactions with the applications they use to do their jobs.

The need for expansive visibility

Let's leave the airport and get on the highway. That web-modulated approach acts like a traffic officer standing at an intersection where your network meets the outside world. The vigilant officer keeps a watchful eye on vehicles streaming by, stopping drivers from making wrong turns and looking out for suspicious vehicles.

But in a cloud-dominated world, the officer faces two significant problems:

- Unless the officer has been told to look out for a specific vehicle or a driver misbehaves conspicuously, they don't have much information to act on.
- Pre-cloud cybersecurity systems look at only one lane of traffic: web traffic. These systems can't see the new lanes for SaaS, cloud-based services, and custom apps — the very lanes being used by cybercriminals who know those lanes are probably not being inspected. The officer can't see the cars and trucks streaming by in those new lanes, vehicles that could be hiding a horde of stolen diamonds or, more precisely, your precious data.

REMEMBER

True visibility means having the ability to see down to fine layers of activity and interaction between the user, data, and apps. You need to know what your users are doing inside those applications — continuously. Is your user trying to paste sensitive data into the SaaS application? Are they about to expose your payroll file to a public-facing cloud service? Your security systems need to know.

Beyond visibility: Vast data collection powers rich context

In the era of cloud, visibility alone isn't enough. You could have the highest-resolution picture of something and still miss the fine details of what's in that picture if you don't know how and where to look or what you're actually looking at. Security teams need that detail to answer questions such as the following:

- Who is the user?
- What device are they using?
- What network is the user on?
- What applications are they accessing?
- What can be known about each app and its behavior?
- What data is the user accessing?
- Are their current and past behaviors consistent?

We refer to details inside the picture as *context*, which is one of the most critical concepts in cloud access. That context is what makes it possible to define and enforce security policies that can limit what happens as needed within actions and applications in real time. (See Chapter 4 for more on context and policies.)

REMEMBER

The requirements of effective security in the cloud era are as follows:

- To minimize the complexity of your security architecture to make work easier for both users and the security team
- To provide users — no matter where they are — with fast, responsive interactions with their apps so they can get the full benefits of the cloud

- To manage risks to your business continuously by being able to easily see and quickly address potentially risky activity involving company data and users

A properly implemented SASE architecture does all of this.

SASE: Built for the cloud

You can't just rename or repurpose yesterday's technology and think it's ready for today's job of cloud security, let alone tomorrow's. Legacy appliances aren't held back only by being stuck in your data center. The cloud also works at an entirely different scale and speed. Security services need to be designed to operate at that same speed and scale.

What makes SASE such an appealing security framework is that, just like the cloud, it makes work easier and more flexible.

Being built for the cloud means all critical SASE requirements must be baked into the design of the architecture. To get the job done fast and at scale, true SASE requires every service involved in security to do its work in coordination as one continuous, rapid action. All your verification and inspection has to happen "out there," wherever "there" happens to be. A user's traffic doesn't have to return to a security bottleneck (your data center!) for every interaction. By bringing security close to the user and points of access, every interaction is made both more secure and more efficient. Your security aligns with everything the cloud is supposed to be. Returning to the highway metaphor, with SASE, the officer now finally sees all lanes of traffic.

Enabling True Cloud Security

SASE, done well, has two key jobs:

- **To provide a *global edge network* that grants your users access to cloud services, no matter where those users are:** This global edge network authenticates users and then optimizes their connections to SaaS applications, your data center, and other services.

- **To deliver security services throughout the global edge network so that they're close to users:** This ensures that users and organizations can always rely on this security network to get work done safely. This configuration also makes it feasible to apply security policies and dictate users' online interactions based on who the person is and where they are, and to do so while optimizing the security, reliability, and performance of those activities.

REMEMBER

Properly implemented SASE is effective because it acknowledges that applications and workloads have moved to the cloud, and therefore, security services must follow. For your users, that means they don't have to worry about jumping through hoops to use an application. When they go to a coffee shop, getting access to what they need is as easy as getting a latte. For you, the security pro, having context and shared, integrated security services makes it possible to create sophisticated policies that can be applied automatically and appropriately based on who needs access, what they're trying to access, and where all the pieces of the interaction are located. In a digital world that has left the restrictive confines of the data center for the wide-open possibilities of the cloud, SASE is the *only* security and networking architecture that makes sense.

What about the data center?

The data center still has a role to play in enterprise IT for the foreseeable future. Large applications like enterprise resource planning (ERP) were built to last for decades, so such applications in the private cloud will likely coexist with SaaS and the public cloud for a long time. More broadly, organizations have invested a lot over many years to create and nurture their enterprise data centers. Letting go of that momentum may be hard. Be patient.

REMEMBER

When you accept the data center as just one of many places your users go to do their jobs, routing all your cloud-bound traffic through it starts to make less sense. Forcing a user's traffic to constantly detour back through your organization's private network to then be crunched through a succession of separate security black boxes — a process known to security people as *hairpinning* or *backhauling* — is cumbersome and inefficient. After all, you wouldn't plan to drive from Los Angeles to San Francisco by way of Cairo unless you had a lot of spare time (and a ship). The same logic applies to linking your users to their SaaS applications.

TIP

SASE isn't just about SaaS applications. It can and should be used to provide access and to protect all your applications, including the ones in the data center, regardless of whether a user is on- or off-premises.

The right services for every scenario

Flexibility is one of the great advantages of cloud services. But just slapping words like *cloud* or *SASE* onto a product doesn't get you there. Flexibility must be designed by intent into a true SASE implementation. Because context in the cloud changes constantly, different technologies and services will be required to work together on an ad hoc basis and applied as scenarios change and evolve. Done right, SASE applies all the security services needed to enforce security policy for any connection, while always prioritizing these goals:

- Accommodating a distributed workforce
- Optimizing levels of service based on changing context
- Keeping the security services as close to the user as possible at all times
- Providing security services needed to operate at hyperscale with the performance needed by modern business workflows

So, the question now is: How do you shift your organization to effective SASE? In the following sections, we take a look at some key requirements — including a big one, NG-SWG.

Needing a Global Edge Network

When looked at through the lens of old security architectures, the very idea of securing the cloud for business seems to contain a contradiction. On one side, you have users who count on you to provide them with fast access to their apps and data, from anywhere, with minimal disruption from security roadblocks. This stands in near-perfect opposition to the expectation that you'll also provide your users and business with the utmost security and data protection.

Hairpinning traffic through your data center wasn't a significant problem when 85 percent of users were working in corporate offices. In the world created by the COVID-19 pandemic, more workers got a taste of working from home and 74 percent of workers would now like to work from home at least two days a week, according to a survey by PwC. For remote users, hairpinning introduces latency and hurdles that get in the way of a productive user experience. Because remote working is likely the new normal, it's imperative that security move to the cloud where it can best follow those users and provide data protection without degrading the user experience.

That last bit is important because frustrated users who want fast access will avoid connecting to your virtual private network (VPN), something they've been doing already for years. When that happens, your users and your data aren't protected at all, and your security team is flying blind. A global edge network makes it possible for users to connect to the cloud from anywhere without having to hairpin back to the data center for protection and data security.

REMEMBER

Having access to a global edge network is a distinct advantage for your mobile workforce. Netskope's global edge network provides access points in more than 40 regions around the world where security functions are hosted and executed. This is what makes it possible to keep security close to the user at all times and deliver single-pass inspection of traffic (see "Single-pass inspection," later in this chapter, for more — for now, just think "fast"). Together, these help provide a smooth, fast, secure user experience.

One of the fundamental differences between SASE and traditional security is how and where security is applied. Within a SASE security architecture, when a user wants to connect to the Internet — whether to use a SaaS application, browse the web, or post to a social media site — they first connect to an access point on the global edge network. Each access point includes the computational capabilities needed to power security services. Because of that distribution, users don't encounter the performance tradeoffs or the complex, multistep security headaches they encountered when everything flowed through the enterprise data center.

Understanding How NG-SWG Relates to SASE

The ideal, complete form of SASE is a new security architecture in which all your security services work together in perfect coordination. If that sounds like a big undertaking, it is. But you don't have to arrive immediately. By taking the right first steps, you'll create a strong foundation for everything that comes later. A key early step is to implement NG-SWG. It's a critical difference-maker between "pretend SASE" and a properly executed SASE. NG-SWG is the catalyst for creating the security cloud that makes SASE possible.

SASE is best implemented using a microservices architecture. Simply put, *microservices* are a way to build a system out of many small, discrete services modules. When done right, those modules share a common code base and all work together to understand the native language of the cloud.

All those services must be orchestrated to work together to enforce your security policies based on content and context. NG-SWG acts as the air traffic control of a SASE implementation. Whenever and wherever a user accesses data, NG-SWG coordinates services so they act in concert to enforce security policies throughout the IT environment.

In one fast sequence, NG-SWG applies all the shared security services needed for the policy-based application of security to each connection based on a super-rich understanding of the users, data, apps, and traffic on your network.

NG-SWG also enables you to retire less capable appliances, reducing the complexity of your security infrastructure without giving up the characteristics of their best and most useful services. Now part of NG-SWG, those services are applied in coordination with the many new services that work together to inspect deep inside your SaaS and web traffic, gain that super-rich understanding, and enforce context-based security policies.

WARNING

A generic public cloud platform like Amazon Web Services (AWS) or Google Cloud isn't SASE, or even SASE-ready, on its own. Public cloud solutions are optimized to deliver applications — the public cloud architecture is designed as a destination rather than as a hub for security services that traffic flows through on its way somewhere else. SASE has unique computing and performance requirements that make it possible to support a microservices-based architecture designed for security workloads.

SWG versus NG-SWG

SWGs are sometimes called secure Internet gateways or web proxies or web filters (or other names). They've been around in some form since at least the '90s and were originally built in an era very different from today.

What makes NG-SWG different from traditional SWG and other, similar products you may be familiar with? The simplest answer is that traditional SWG addresses only web traffic and provides only allow/deny controls. It was built for an era when the Internet was about websites and Hypertext Transfer Protocol/Secure (HTTP/S) communication — as in, "Yes, you can go to this website" or "No, you definitely cannot go to, ahem, *that* website."

NG-SWG, however, is the organizing umbrella under which all web and other services reside, while also creating an expansive security cloud with control points near the user (that global edge network from earlier) where a wide range of security services are orchestrated. NG-SWG executes and enhances all the basic web traffic functions in legacy SWGs and similar appliances and adds significant new security functions. In particular, NG-SWG performs a deep inspection of cloud and web traffic, looking to see what's happening inside interactions, applying data and threat protection, and building understanding of the content and context to enforce granular policy controls.

With NG-SWG in your SASE, the traffic officer or controller can see all the lanes of traffic, know what's happening inside the vehicles, and enforce the rules (see Table 2-1).

TABLE 2-1 How Netskope Fulfills SASE Requirements

SASE Requirement	Netskope NG-SWG
Cloud-native with single pass architecture for encrypted traffic inspection	Resides entirely in the cloud using cloud-native architecture with the ability to decode and understand apps and cloud services for data context. The Netskope single-pass architecture provides advanced data and threat inspection of encrypted traffic (support for TLS1.3 without down-negotiating connection) at line speed at every NewEdge data center for all services (SWG, cloud access security broker [CASB], advanced data loss prevention [DLP], sandboxing, machine learning [ML] analysis, firewall as a service [FWaaS], remote browser isolation [RBI], and so on).
Points of presence, with service-level agreements (SLAs) for low latency and high availability	Netskope NewEdge Network, a high-performance security private cloud hosts security services and provides abundant access points worldwide. With low single-digit millisecond latency for the best experience, NewEdge is backed by five nines (99.999%) availability inline services SLA plus Trust Portal for real-time service/data center status (`https://trust.netskope.com`).
Security as services via a single policy control plane	Single-cloud platform and policy engine run on management planes, separate from traffic processing data planes. A single console is used for ease of administration to manage and add any SASE security services, which are deployed via a single agent for simplified access and user experience across all locations.
Traffic inspection with NG-SWG forward proxy of five types of user traffic	Analyzes all lanes of user traffic for web, managed SaaS, shadow IT apps, public cloud services, and custom apps in the public cloud or data center, unlike legacy SWGs that analyze only web traffic. Consistent security inspection policies are applied across all access methods.
Sensitive data visibility and control and cloud DLP	Unmatched visibility across web, SaaS, shadow IT, public cloud services, and custom apps in public cloud for sensitive data movement. Protects data in motion for five types of user traffic plus email DLP for outbound Microsoft Office 365 (M365) and Gmail Simple Mail Transfer Protocol (SMTP) traffic; key to this capability is analyzing data movement between company and personal apps and app instances, as well as data movement anomalies.

(continued)

TABLE 2-1 *(continued)*

SASE Requirement	Netskope NG-SWG
Advanced threat protection (ATP) and user and entity behavior analytics (UEBA)	Offers protection from web- and cloud-enabled malware, cloud phishing, and malicious documents with inline anti-malware, pre-execution analysis, sandboxing, machine-learning analysis, and UEBA for behavior anomalies and user-risk scoring with real-time analytics and dashboard visualization across all users/applications for data, threat, and activity.
Cloud firewall	Provides outbound cloud firewall controls for remote users and branch offices across all ports and protocols.
RBI	Targeted RBI pixel renders uncategorized and risky websites to provide safe access to users, in addition to blocking file downloads and uploads, form inputs seen with phishing attacks, and clipboard copy/paste.
Zero trust networking security posture	Zero trust security controls applied starting with user access (zero trust network access [ZTNA], identity access management [IAM]) to capture risk info and context for user, device type, app, app instance, app risk rating, category, activity, content and action to apply risk based conditional and contextual policy controls. As user behavior and anomalies are monitored, adaptive policy actions are dynamically enforced per Zero Trust principles, including step-up auth challenges, limiting activity access, data movement, or terminating user application access altogether.
Adaptive context-driven policy creation and consistent enforcement	Provides real-time coaching, step-up authentication, and adaptive policies based on app risk, user risk, and data context. Real time enforcement is consistent across all users, branch offices and other edge locations.
IAM	Integrates with IAM and identity provider systems that manage and verify the digital identity of users and groups.
Endpoint protection	Enables bidirectional automated indicator of compromise (IOC) sharing, as well as conditional access with endpoint protection enablement and the ability to share rich metadata for investigations.

SASE Requirement	Netskope NG-SWG
Security information and event management (SIEM) and security operations center (SOC)	Provides IOC sharing and rich metadata to work seamlessly with the management points and dashboards used by security personnel to investigate alerts and incidents.
Real-time analytics and visualization	Provides cloud metadata for real time visualization and analytics on data movement, threats, users, and applications in dynamic customizable dashboards for C-level, board-level, and security and risk teams.

A little bit SASE versus properly implemented SASE

With NG-SWG, you no longer have to configure hundreds or thousands of tiny, detailed, but complicated, rules separately for every one of your security solutions and appliances, each of which handles only a small portion of traffic in your data center. In best-in-class SASE solutions using NG-SWG, you focus on creating high-level policies that describe your desired outcomes for *all* traffic. NG-SWG then tells the different security services what to do to deliver those results across your web traffic, managed SaaS apps, unmanaged SaaS apps (shadow IT), public cloud services, and custom apps hosted in the public cloud. Enforcement can even include rich features such as user coaching and risk-based actions to enable nuanced and appropriate responses. You define the things you want to happen throughout the architecture, and NG-SWG coordinates services to make it happen.

How does NG-SWG create the context-based foundation for properly implementing SASE? Table 2-1 (earlier in this chapter) shows which services and features of a SASE architecture NG-SWG provides. It also lays out the other services that help complete the SASE picture when connected to Netskope NG-SWG.

Examining How NG-SWG Works

The previous section describes what NG-SWGs deliver within the broader SASE architecture. This section digs into how NG-SWG puts it in action.

REMEMBER

Although the following description is organized into sections, remember that security with NG-SWG isn't a chain of separate appliances or a linear sequence of operations as you'd have in a data center.

Single-pass inspection

When a user's device is connected to an access point on the global edge network, all of a user's traffic undergoes a single-pass inspection. *Single-pass* means exactly what it sounds like: All the security services needed to enforce policy form one continuous funnel through which traffic flows. The traffic between user and destination goes through this single funnel once, in real time. This process is different from legacy, web-only SWG appliances and inline cloud traffic solutions, which were like having a series of independent funnels that everything had to pass through.

NG-SWG single-pass inspection applies to web content, SaaS apps managed by your organization, any shadow IT or unmanaged SaaS apps a user attempts to use, public cloud services, and any custom apps in the public cloud that your organization deploys. Web and cloud traffic flow through this single system, which aggregates and coordinates all security services as a single coherent platform, and then improves on them to bring properly implemented SASE to life.

Traffic is filtered, in a single pass, in stages. The most obvious problems are removed first, leaving an ever-smaller amount of traffic to be subjected to more detailed analysis (see Chapter 4 for more on these stages).

The richer the context, the stronger the security

Context is the key to the active, deeply inspective, nimble security offered by properly implemented SASE. The instant a user connects to an access point, NG-SWG services within the security cloud develop a contextual picture available to all the services. That picture is used to dictate how policy is enforced. This context is a massive conglomeration of *metadata* (data that describes other data or adds context), including a wealth of information that identifies and recognizes the following:

- The user or the organizational group to which the user belongs
- The user's device, its location, and whether that device is managed by your organization
- The website, app, or app suite the user is working with
- Netskope's Cloud Confidence Index — a risk rating derived from multiple, independent security assessment services and assigned to the particular website, app, or app suite being accessed
- The data being requested, generated, and/or used by the user and the application

In addition, this context is enhanced with many new and varied sources of information that NG-SWG can leverage to add further detail based on the following:

- Awareness of the user's behavior and any anomalies in that behavior
- Inspection of the content and the data contained within the traffic
- Activities performed by the application, web content, and services being accessed, and the nature of those activities
- Knowledge of the data within the application environment
- Stored information collected from past interactions

Context is constantly changing the entire time the user has access. You want a system that's nimble, responsive, and appropriate to the subtle variations in risk presented by different combinations of contextual detail. Policy may describe the desired security outcome, but context determines the optimal combination of services and security actions that deliver that outcome based on the particulars of the moment. For example, a user who's suddenly acting strangely and accessing files they shouldn't becomes subject to *step-up authentication*, a request for more information to establish their identity. Having a huge dynamic context makes it possible to apply granular security policies and enable policy actions in real time as the context changes. Artificial intelligence (AI) and ML play a major role in helping your security sift through those nuanced contextual details (see Chapter 4).

REMEMBER

Legacy web security was basically a "yes or no" proposition. NG-SWG is a dynamic, ongoing approach to security that continuously observes behavior and what's happening inside all web and cloud traffic. This gives NG-SWG the power to adjust decisions about security on the fly, a capability that's critical for securing user interaction with apps and websites.

TECHNICAL STUFF

Table 2-2 describes some of the security services that are expanded and enhanced by NG-SWG and that lay the foundation for a full-blown SASE architecture.

TABLE 2-2 Key Security Services Delivered by NG-SWG

Security Service	What the Service Did in a Traditional Setup	How NG-SWG Supercharges the Service
SWG	Protected users against web threats and objectionable content.	Adds app and data context (who's using the app or data, where they're using it, and why). Adds data protection (preventing its modification or theft). Stops inappropriate use of data (preventing data from being used or sent where it's not intended).
DLP	Protected only the data stored in the data center and being moved beyond the data center's firewall via the web.	Protects all data in motion, including data distributed on the web, in SaaS apps, in the cloud, in cloud services, and in custom apps on the public cloud.
CASB	Monitored and protected managed apps that provided visible application programming interfaces (APIs) that could be monitored and protected through those APIs and also inline; its focus was on data at rest and data in motion — data stored either within the app environment or the data center, as well as passing between the two; not all solutions support all modes.	Monitors unmanaged apps that don't offer obvious management APIs, allowing large numbers of unmanaged apps to be monitored and protected. Monitors data in motion; data actively being used by and conveyed to apps and websites can be protected. Offers strong app risk insights to inform SaaS selection and deployment.

Security Service	What the Service Did in a Traditional Setup	How NG-SWG Supercharges the Service
Advanced threat protection (ATP)	Protected against web-based threats using advanced methods such as *sandboxing* (detonating executables safely to detect malicious intent and hyperlinks) and threat intelligence (shared IOCs from public and paid sources).	Protects against cloud-enabled threats, including malware delivery and phishing attacks using apps and cloud services such as Microsoft Office 365 and Google Docs. Isolates unknown apps and websites to safely interact and protect against potential threats.

Single-pass policy enforcement

Of course, even the most detailed context isn't much help unless both your users and your security services know what they are and aren't supposed to do. You need ground rules to which the context can be compared.

You may have written a set of rules that would dictate the behavior of the firewall, checking the URL input by a user against lists of websites that you decided to block. But traditional security always forces compromises between speed and flexibility on the one hand and security on the other. Between the steady flood of new sites and personnel changes over time, your rule list may become massive — and brittle. You may be wary of changing your rules — perhaps to allow access to a useful sales tool — for fear of unwittingly opening a new vulnerability.

SASE, done right, does away with such tradeoffs by offering a new paradigm for delivering world-class security. Single-pass policy enforcement is the power, or superpower, of SASE to enforce data policy or activity controls across all apps, app categories, and web services. Think of it as the power of context in action. For example, if single-pass inspection sees a sensitive data type in a web form or within a file or a field in an app or in a Slack channel, single-pass policy enforcement can block the content on the web and/or control the activity in the app (upload) while still allowing view.

With a consistent, granular, and centralized policy framework that extends across all your security services, you can take control and declare your intent clearly — without worrying about the details of how to implement a specific policy. This dramatically reduces complexity.

TIP

SASE with NG-SWG changes your security team's job. Instead of inefficiently writing separate code to manage each separate appliance, your team focuses on writing effective, high-level rules to deliver services that make sense for the business.

NG-SWG in Action

Figure 2-1 shows what NG-SWG looks like in action from the perspective of a single user.

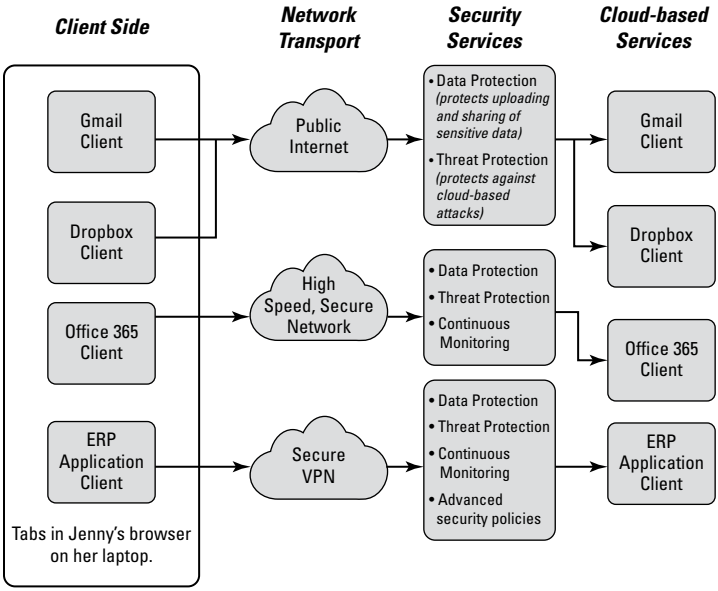

FIGURE 2-1: NG-SWG in action for a single user named Jenny.

In Figure 2-1, Jenny represents a typical user working from home who might initiate four connections from her laptop to

- Her personal Gmail account
- Her company Microsoft Office 365 email
- A cloud storage app like Dropbox
- Critical enterprise-managed apps such as Salesforce, ServiceNow, or Workday

In this case, NG-SWG handles these discrete interactions as follows:

- **Jenny's personal Gmail app is routed to the public Internet.** NG-SWG secures and analyzes the connection, providing threat protection and data protection and resulting in a high-performance user experience.
- **Jenny's company Microsoft Office 365 email is routed over a high-speed, secure network.** The traffic in this connection is continuously monitored to make sure crucial data isn't shared.
- **The connection to the unmanaged Dropbox cloud storage app is routed via the public Internet.** NG-SWG secures and analyzes this connection continuously and enforces security policy, enabling Jenny to view shared files from third-party sources. However, NG-SWG blocks uploads and applies threat prevention to file downloads when a justification has been provided by Jenny for the file download.
- **Jenny's connection to the mission-critical enterprise app is routed over a special, encrypted VPN.** The connection is monitored by several different security services that provide layers of protection to ensure that data isn't improperly shared or used. It also enforces policies to make sure the app is used properly.

In this example, using just one worker, you can see how four different connections are protected. Each connection has a distinct context that dictates the application of specific, relevant policies. The resulting user experience is excellent, and the level of security is high. Jenny can check her personal Gmail and do her job without risking the company's data. That's the difference NG-SWG can make.

At this juncture, it's important to note that NG-SWG isn't the *only* difference-maker when it comes to properly implemented SASE architecture. NG-SWG isn't magic beans; the CASB functionality (found not in SWG, but in true NG-SWG), and the judicious application of zero trust principles, are other key pieces of the puzzle.

NG-SWG is a big one, however. It can dramatically accelerate your journey to SASE and help you leave behind old technology like legacy SWG that will only hamper your successful SASE architecture.

IN THIS CHAPTER

- Improving security by knowing your people better
- Exploring which combination of services makes security more robust
- Understanding how trust changes when people work outside the network you traditionally control
- Discovering how security is supercharged to protect people in the cloud

Chapter 3
Protecting People

So much of security is about people — protecting the people who matter to you and protecting the things that matter to you from people with bad intentions. For enterprise security and networking teams, the obvious, practical scenarios are those concerned with protecting your organization's personnel and digital assets from those who would cause harm, all while ensuring your employees and customers have good and reliable experiences.

But security is also about protecting your staff from themselves — the mistakes, temptations, negligence, and errors of judgment that can do irreparable harm to them or your business. (You may be surprised to know that more than 90 percent of cybersecurity incidents are attributable to human error, according to Kaspersky Lab.)

Secure access service edge (SASE), when correctly designed, provides your security people with the insights and tools to effectively and intelligently take on those broad challenges by helping your organization along two fronts:

- **Protecting your systems from people who aren't authorized to access them:** Whether those systems are in your data center or the cloud, the same standard must be applied at all times.

- **When people are authorized to enter your systems, preventing them from intentionally or unintentionally doing unsafe things**

SASE shifts security to an edge-based cloud environment, creating a structure that is rich in security services, provides full visibility and control, and can reach everywhere.

This chapter looks at how a well-designed SASE, built using next-generation secure web gateway (NG-SWG), cloud access security broker (CASB) capabilities, and zero trust principles, makes life safer and easier when your users are in the cloud.

Context: Changing the Game for Security

Effective SASE is driven by context, and the generator for that rich background resides within the Netskope platform. From Netskope, Cloud XD (short for *extreme definition*) is the context service that transforms your web traffic, cloud services, and software as a service (SaaS) app activity into intelligible, actionable insight. Cloud XD captures and decodes details inside the traffic that makes it possible to identify users, their devices, applications being used, and specific activities within those applications. This decoded information is shared with all the security services, making it possible to enforce detailed security policies based on cues provided by Cloud XD.

Answering basic questions

The detail Cloud XD provides is wide and varied, itself dependent on the specific activity underway. That detail may include information such as the following:

- Is the user uploading or downloading something?
- If so, does that "something" include sensitive data?
- How many bytes is the user uploading or downloading?
- What application is being used?
- Is the person using a corporate or personal instance of an application?

Those examples are simple, but it may surprise you to learn that, until recently, such basic, high-level data wasn't effectively available to security teams, and not anywhere close to an aggregated, coherent presentation that could be applied across the entire security landscape.

These newly available details make it possible to construct a narrative about a user's activity that may sound something like this:

> Lauren is using her corporate instance of Gmail and has been granted access using her business login credentials: a username that you know, her password that was accepted, and a two-factor authentication (2FA) code that was accepted. You know that Lauren may have a personal Gmail account, so you'll keep track of what instance she's working with because Gmail allows her to readily switch accounts within her browser window.

WARNING

Context, in the sense of modern, sophisticated security, requires that your security services have their eyes open for change and anomalies at *all* times. These days, attackers have become very skilled at capturing credentials by phishing through SaaS applications and launching other cloud-oriented attacks, making it easier for them to evade legacy web defenses. When access is granted to a user, security's job is just getting started!

Examining behavior

Valuable context further expands beyond the basic questions (which we reference in the previous section) by detecting and evaluating behavior patterns after a user has access. Cloud XD applies sophisticated analytics looking for clues that an account has been compromised, revealing when an "authorized user" (or what looks like one) engages in activity outside their usual behavior or assigned role. Cloud XD looks for signs of suspicious behavior to answer questions such as the following:

- Is this user doing things they don't normally do, such as moving data?
- Is the user accessing applications or content that are different from usual?

- How much data is the user uploading or downloading, and is that activity or amount of data unusual?
- Is the user interacting with their device in an atypical manner?

REMEMBER

People may seem unpredictable, but their routines and patterns of work are recognizable. NG-SWG develops a user profile over time and uses that profile to detect actions outside the norm, such as unusual data movement, attempts to misuse credentials, and many other anomalies.

Digging into rich external context

This overall, context-driven approach makes security smart about the cloud — very smart. You know more not only about internal context — the user, device, network, and applications that are all "inside" the company network — but also about what's outside the company network. Netskope makes it possible for a SASE architecture to better understand all of what makes the cloud go, such as application programming interfaces (APIs), which are how applications talk to each other, and JavaScript Object Notation (JSON), which allows data to have a flexible structure. Additional services provide contextual information about specific websites, cloud services, and data repositories to paint a complete picture of the cloud environment in which the user is working.

Taken together, this context makes security services more effective. Because the security services now know more, they can act more intelligently. Services can be controlled by policies that define exactly what's allowed and what isn't — down to very specific details and ever-changing context.

Seeing how services are greater than the sum of their parts

In the past, security appliances often functioned separately from each other, performing their individual jobs in sequence and isolation. In contrast, the architecture enabled by Netskope and required for effective SASE means that services can help each other as needed, making the entire architecture smarter. Data loss prevention (DLP) services can work together with user and entity behavior analytics (UEBA) services to apply extra levels of data

protection when a user exhibits behavior that indicates risk. For example, optical character recognition (OCR), an advanced DLP service, can be used to detect what's contained in a document a user is uploading and then determine if the document is safe to share. A team approach for the win!

The user profile further informs the process, permitting, for example, your chief financial officer (CFO) to share information with the company's accountant but preventing a business line manager with access from sharing a subset of the same information with a stockbroker pal.

Seeing How Security Works When Users Are the Perimeter

Before SASE, user security primarily meant one thing: knowing who the person is. After you identified the user, access was granted past the perimeter to the so-called *castle* (the data, applications, and services the individual was allowed to use). Beyond that, the person may have had specific permissions and restrictions dictating what things they were allowed to work with, with no deeper granular understanding and certainly no protections for errant behaviors inside those permitted engagements.

WARNING

SASE still begins with identity and access management — the usual username, password, and multifactor authentication processes we all encounter daily in our digital lives. But in a SASE architecture, that's just the beginning of verifying a user's identity. Your security services now have a rich, detailed, and continuously updated user profile on which they can rely. All that other "stuff" — including what device they're using, the time of day, where they're located, applications they're using, and how quickly they type — provide a lot more information to confirm that the user is who they say they are. Even if a user's basic credentials are compromised, your SASE security services are still working to protect your enterprise and its data. (In Netskope's architecture, this intelligence also rolls up into a user risk score. More on that in Chapter 4.)

A widely endorsed idea in security circles is *zero trust:* When users or devices try to work with applications and data in your systems, the assumption is that they can't be trusted — at all — until they can prove that they are who they say they are. Even then, the user is confined to only the set resources for which they were just approved. If they try to do something else, they must be verified again.

Zero trust principles can be more powerfully applied across SASE architectures and are another key to properly implemented SASE. It's the idea that with all network traffic, regardless of whether you recognize the user, their device, and so on, you always assume the user may be up to no good.

Zero trust, and one of its better-known implementations, zero trust network access (ZTNA), aren't new in enterprise security circles, but SASE expands the scope of how the principles of zero trust can be applied. Before zero trust, after a user was allowed inside the data center's services, they might be further limited to a specific set of allowable activities; within those confines, they were essentially free to do whatever they wanted.

SASE makes the principles of zero trust both stronger and more flexible, even permissive, across all users globally. (***Remember:*** Your users are now the perimeter! And that's more like "perimeters," if we're being honest.) The SASE architecture applies the context the users have across all traffic toward more informed and granular decisions on what users can and should be permitted to do. At no point does the SASE architecture *ever* assume that a user's traffic is okay. Even though your known employee is using a SaaS application that you want them to use and they're working with a data set that makes sense for their job role, you don't simply assume that what they're doing with those two things is okay.

REMEMBER

If you can't see what's happening inside your traffic — the interactions and transactions inside the connections that have been allowed — your security is weak. By moving the protection *close to* the users wherever those users are accessing data and distributing services to those edge access points, your security can see inside the flow of traffic without forcing users to hairpin back to your data center. People can work from anywhere, and security policy can be enforced everywhere.

Recognizing That Advanced Threat Protection Is Better in the Cloud

Advanced threat protection (ATP) is another existing security activity whose scope and effectiveness are dramatically increased within a properly implemented SASE. Until recently, ATP referred only to approaches taken to protect users from incoming threats, typically in the form of malicious files.

But to be effective in cloud workflows, ATP must also focus on cloud-based threats, which include not only bad files but also applications and systems that may present dangers. In the cloud, you have new angles of attack to consider, including the following:

- Endpoints or edges such as laptops, tablets, phones, and Internet of Things (IoT) sensors and devices feeding information from the outside world to your internal systems using a cloud connection
- The cloud, including SaaS applications and websites — good ones, bad ones, and every variation in between, such as legitimate services co-opted by bad actors
- Users, mainly the assessment and verification of the people acting in the name of your company

Effective ATP in the cloud requires a proactive approach. It must prevent threats from starting when possible and detect threats that do manifest as quickly as possible. (Netskope further deploys artificial intelligence [AI]/machine learning [ML] analysis services to amplify its ability to recognize trouble.)

NG-SWG is at the forefront of helping overcome this large-scale challenge with the Netskope Cloud Threat Exchange, which feeds your SASE services with a continuous river of up-to-date threat intelligence developed by *all* the vendors who contribute to your SASE platform. In addition to the intelligence derived from NG-SWG, that includes the specific expertise from identity management, endpoint protection, security information, event management, and other integrated services.

TIP

The variety of possible threat vectors in the cloud is daunting. No single organization can keep pace on its own, so effective SASE is the result of teamwork by your security service providers.

Evolving SWG for the Cloud

When you were defending only against basic web threats, your security infrastructure probably featured an appliance used to block users from accessing bad websites and to prevent them from downloading malware and other bad stuff from the web. Referred to mainly as an *SWG* and by several other names such as *web proxy* or *content filtering,* these systems actively scan URLs requested by users, keep an eye on what's happening when people use communications apps, and watch inbound traffic for known malware and viruses.

Of course, you still need that functionality, so NG-SWG (see Chapter 2) provides those basic SWG services. But thanks to its deeper suite of inspection services and access to extensive context resources, NG-SWG makes a much stronger stand against the newer threats made possible by the cloud. For example, although NG-SWG still prevents malware from being downloaded, it also looks inside and monitors the traffic when someone is using Dropbox, Google Workspace, Microsoft Office 365, and any other SaaS- or cloud-based service. This makes it possible to protect the user's work environment even when it's entirely in the cloud and not being downloaded to a local corporate system.

When you get all these things right, your users are safer and more empowered to be effective at their jobs. Your people are protected, and the organization benefits when its employees are free to be productive without compromising valuable assets or running afoul of compliance and governance concerns.

IN THIS CHAPTER

- Changing the security game by setting high-level policies
- Using NG-SWG superpowers to control data wherever it's accessed
- Overcoming the challenge of unmanaged cloud apps and services
- Getting a look at single-pass inspection in action
- Understanding why zero trust is essential for effective data protection

Chapter 4
Protecting Data and Applications

In the past, protection meant keeping everything safely inside the perimeter of your data center. Today, data and applications are outside your data center fortress and in the cloud. It's time to leave some outdated concepts of data protection permanently behind.

This chapter examines how data protection must evolve to be successful and how Netskope SASE technology helps you ensure your organization's sensitive data isn't misused or vulnerable.

Conquering Complexity with the Power of Policies

In the past, security teams have been limited not only by their skill, but also in their reach. Their primary defenses were stacks of disparate security appliances — firewalls, secure web gateways

(SWGs), cloud access security brokers (CASBs), and so on. Disjointed security environments and specialized appliances are inherently limited. Worst, after enduring the micromanagement needed to tell each of those specialized boxes how to do its job, these systems don't have the visibility, reach, or power to properly secure the cloud or to work together to prevent and respond to threats. The only choice is to block access (see Figure 4-1), even when that policy doesn't make sense because the user context is available.

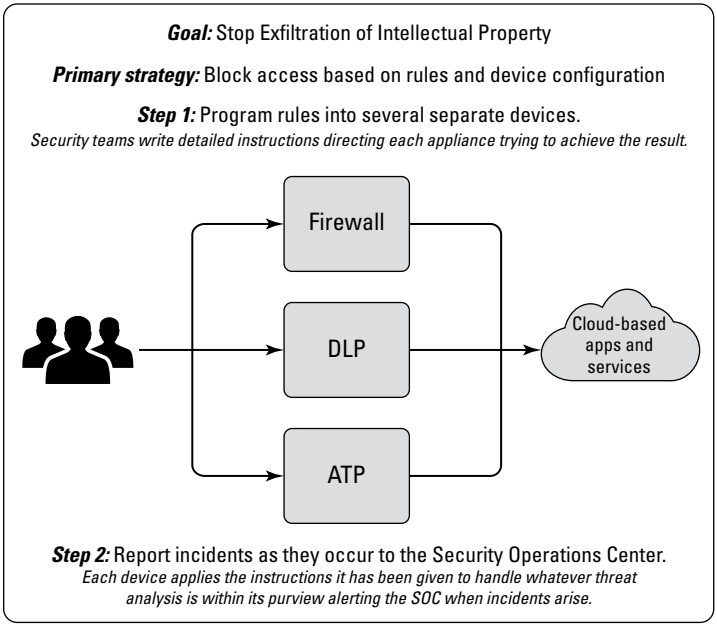

FIGURE 4-1: Blocking access no matter the context.

Netskope fixes the problem by replacing that disjointed mess (see Figure 4-2). It enables your security team to set broad macro-level policies — a consistent set of instructions that describe the outcome you want. Next-generation SWG (NG-SWG) helps turn those instructions into action, coordinating and directing security services to achieve your desired results.

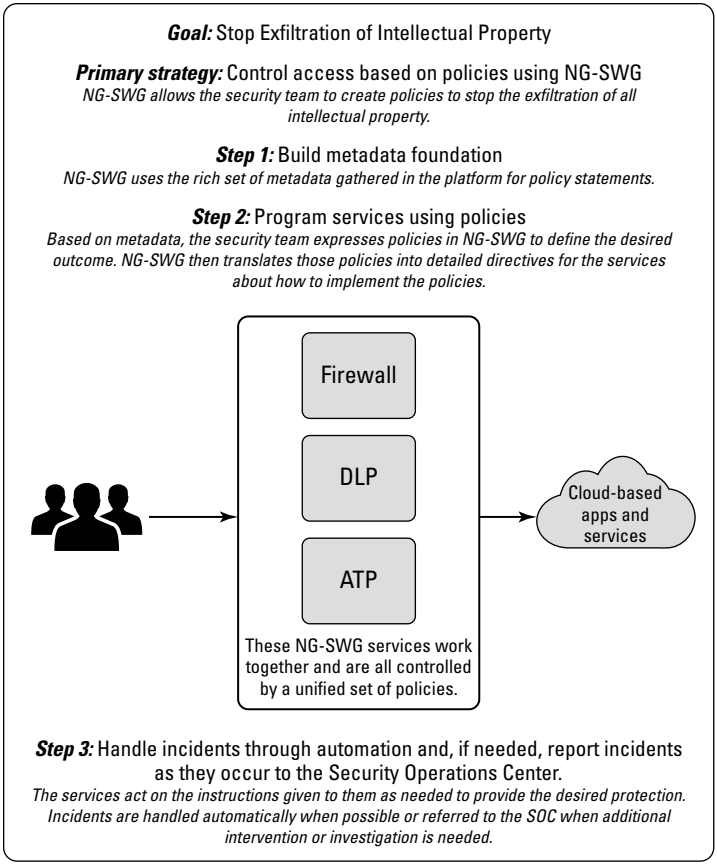

FIGURE 4-2: Broader policies direct security services to achieve desired outcomes.

As opposed to a rudimentary block-or-allow approach, specific policy controls that consider context and nuance result in fewer devices and rules to manage and allow more user engagement with apps and services that boost productivity. This approach simplifies life for your security team. Fewer devices to control and fewer rules to write means less potential for errors. Maintaining and modifying this system as needs change is easier. Even when underlying systems are updated and improved, policies stay the same. Services can evolve quickly to address new threats because changes don't disrupt the security framework.

Protecting Data

In the era before secure access service edge (SASE), data loss prevention (DLP) systems tracked data as it moved out of your enterprise network to prevent it from being used or shared in unauthorized ways and to meet compliance requirements. Now company data increasingly lives outside the enterprise among cloud services and applications; it also moves within and across cloud apps, sometimes without ever touching the endpoint.

Netskope watches both web traffic and cloud activity to secure all that data. NG-SWG remembers what it learns to enhance security services continuously. Specialized controls give it awareness no matter what managed or unmanaged cloud service is used and whether users are in your offices or remote. NG-SWG recognizes what users do within each service and what happens between services (for example, if an employee downloads sensitive data within a managed service and then tries to upload that data to their personal Gmail account).

NG-SWG implements your security policies automatically to protect data. When you set a policy to prohibit the sharing of confidential information, NG-SWG uses its DLP service and image classifiers to notice if a user captures a screenshot of a confidential Microsoft PowerPoint slide or whiteboard image with confidential text and prevents that user from emailing or uploading the screenshot to unmanaged or personal shared drives or sharing the data in a web form.

REMEMBER

Artificial intelligence (AI) and machine learning (ML) boost data protection. Netskope NG-SWG uses AI and ML as extra firepower to detect nuanced contextual details with greater accuracy. These technologies enable specialized capabilities, including the following:

- **Pattern and image detection:** Using algorithms that help categorize information to provide a dynamic web page risk rating or detect malicious documents and images of confidential information
- **Anomaly detection:** Recognizing occurrences in data or behavior that are rare, unusual, or otherwise out of place

Specialized AI/ML classifiers do things like determine what types of pictures are being moved around to recognize confidential content such as passports, whiteboard images, driver's licenses, and screenshots. Other classifiers analyze document types to detect source code, résumés, and other sources of protected data. This capability is a powerful enhancement to the accuracy and efficiency of data security, important to securing the volume of data being created today.

Protecting Applications

Today's organization relies on several categories of applications, including managed applications, unmanaged applications (what is known as *shadow IT*), public cloud services, and custom apps hosted in the public cloud.

Security teams were once able to protect applications from external threats just by keeping firewalls up to date. Later, web application firewalls added more protection. But that protection was limited to web applications running inside the data center.

When cloud applications first arrived, cloud application vendors were asked to provide management application programming interfaces (APIs) that allowed IT departments visibility into what users were doing with the applications and gave them a bit of control. These apps, such as Salesforce, ServiceNow, and Workday became known as *managed* or *approved apps* (see Chapter 2).

Netskope provided one of the first tools used for this management with its CASB, which utilizes the APIs provided by Google, Microsoft, Salesforce, and others to give access to whatever monitoring and control capabilities those app developers had included.

WARNING

The problem for security teams is that many valuable applications don't have published management APIs. Sometimes these unmanaged apps could be evaluated by IT staff for reliability, security, and safety. But as we discuss in earlier chapters, employees often use whatever app they want — resulting in that unauthorized, unmonitored shadow IT.

With NG-SWG, however — and unlike traditional SWG — CASB functionality expands dramatically. Deep inspection capabilities distributed throughout the Netskope Security Cloud monitor the Hypertext Transfer Protocol/Secure (HTTP/S) and API traffic of *all* web and cloud-based apps your employees use. That includes both your managed and unmanaged apps and services previously invisible to CASB. Shadow IT steps into the light!

Netskope can discover tens of thousands of cloud apps and services, assigning a risk rating to each. That risk rating is based on Netskope's Cloud Confidence Index, an objective measure of a cloud service's risk readiness derived from Netskope resources and a variety of industry threat intelligence services. NG-SWG uses that rating to inform users and security teams and to steer enforcement of your security policies. When a user is logged into your organization's cloud services, such as Microsoft Office 365, their activity is monitored so they can't download data in that instance and then upload it to an unmanaged, risky cloud app.

Seeing Netskope in Action

Chapter 2 describes the Netskope NG-SWG single-pass inspection approach. Here's a deeper look at how NG-SWG applies that approach to secure data and applications:

- **Stage 1:** NG-SWG identifies multiple instances of cloud services and applications to differentiate personal, third-party, and corporate instances of email and/or productivity applications. NG-SWG uses the Netskope Cloud Confidence Index rating system to block access to malicious websites, risky software as a service (SaaS) applications, and unsafe cloud services. It also actively works to stop malware and other sophisticated web threats from spreading.
- **Stage 2:** Using metadata about the user's identity, location, device, and network, NG-SWG adjusts the level of access for each session based on that context. For example, if NG-SWG determines that a fully authenticated employee is using a personal tablet on a public Wi-Fi hotspot, they can be prevented from accessing a critical, managed cloud application.

- **Stage 3:** NG-SWG enforces control over users' specific activities to reduce the risk of data being leaked and exposed. Rules about uploading and downloading documents, sharing screenshots, filling in web forms, and creating, posting, and publishing to services such as social media are enforced in each application and instance.
- **Stage 4:** NG-SWG continuously monitors all activities allowed by the previous steps, watching for anomalies and threats. It recognizes sensitive data moving around and reacts on the fly based on the sensitivity of data, type of action, and other relevant parameters. ML-enhanced image classifiers and pattern detection techniques kick in. NG-SWG might block certain specific actions, trigger an alert, query the user about their objectives, ask for step-up authentication, or quarantine data for further inspection by security teams. NG-SWG offers very detailed context, so false positives are rare.

NG-SWG expansively implements the guiding principles of properly implemented SASE so data and apps are protected, wherever they are and wherever or however they're accessed.

The Importance of Zero Trust Principles to Data Protection

The application of zero trust principles is one of the most important developments for security in the last decade (see Chapter 3), and no honest discussion of data protection is complete without it. The idea is that no users accessing data should be inherently trusted, and access to applications and data should be kept to as little as possible. Zero trust implementations such as zero trust network access (ZTNA) are well known in security and networking circles. But what does zero trust mean for data protection?

REMEMBER

Like other pre-cloud frameworks, DLP was founded on the idea that everything of importance is inside a data center, protected by a network perimeter. In the old days, the job of data protection was to prevent data from leaking out in unauthorized ways and to stop unauthorized individuals from getting inside the perimeter to access that data.

That approach doesn't work in the modern cloud era. Some crucial data is in the data center — behind the traditional perimeter — but at least as much (and increasingly more) data is in SaaS apps and in apps hosted in the public cloud. Organizations must rethink data protection in response to the way users work these days in order to protect a much wider, much more dynamic attack surface. You need a way to grant users access to just the data they need, at the time they need it, and nothing more.

In 2021, Netskope first described the term *zero trust data protection* as a security approach that provides continuous, real-time access and policy control based on risk and context. Context helps you understand what's happening between users and apps and informs how you allow and prevent data access based on a deep understanding of who the user is, what they're trying to do, and why. It's what allows security teams to define and enforce conditional controls based on data sensitivity, app risk, user behavior risk, and other factors — and to do all that in real time. The result is more effective security, thanks to continuous risk management.

A continuous risk management approach is the only effective way to manage risk dynamically across a mix of third-party applications when you have a remote-first workforce that needs always-on access to cloud apps and data to stay productive (see Chapter 2).

REMEMBER

Zero trust data protection isn't just a new way to think about DLP or to create yet another speculative marketing idea that hitches itself to the popularity of the *zero trust* term. Zero trust data protection gets to the heart of what best-in-class SASE is all about, which is to transform security and networking for the access-from-anywhere era of the cloud and ensure that data is protected everywhere. A unified, comprehensive approach to SASE and zero trust data protection separates true SASE technology providers from the pretenders.

IN THIS CHAPTER

- Developing a full understanding of your organization's cloud security posture
- Improving risk assessments by seeing activity outside your data center
- Gaining control over who's moving what data and where
- Fully enabling and securing your remote workforce at scale
- Refactoring your data center to work securely with the cloud

Chapter 5
Ten Steps (Or Fewer) to Get to SASE

This chapter provides a step-by-step approach to implementing secure access service edge (SASE), from knowing your starting point and where you're going to optimization and everything in between.

This chapter provides an overview of how to achieve success by deploying SASE in a series of seven steps. At each phase, you'll make big strides toward significantly increasing your organization's security posture, managing risks, and providing your employees and customers with the experience they require.

Step 1: Determine Where You're Going

When undertaking a new project, the need to deliver quantifiable results today (or at least very quickly!) is a significant challenge facing a chief information officer (CIO), chief information

security officer (CISO), or anyone with high-level responsibility for enterprise networking and security. Unlike typical IT projects where long development cycles may be tolerated, security must demonstrate value right away and deliver quick wins. Vulnerability is scary.

SASE addresses that vulnerability using an architecture that reflects the way security must be delivered *now* and the increasing (and favorable) convergence of security and networking. But true SASE is a long-term evolutionary process. Your organization will grow into SASE. The key to your success is to deliver a succession of tangible victories — deliberate leaps forward — that repeatedly expand and strengthen your organization's security in demonstrably meaningful ways.

But to do that, you must know where you're starting from and where you're going.

By approaching SASE as a series of informed investments and implementations, each game-changing in its own right, you can deliver continuous, dramatic results as you steer your enterprise away from its parochial data center–centric worldview to one able to fully and securely reap the many benefits of the cloud.

Step 2: Gain Awareness and Visibility

The first step in solving any problem is admitting there is one. This book explains how enterprise security hasn't kept up with the security and access needs of today but has remained rooted in the traditional data center.

More than half of enterprise app traffic and users are getting work done on networks the organization doesn't control — and that was before the COVID-19 pandemic made work-from-home the new norm (see Chapter 1).

You and your organization need to come to grips with the severity and breadth of what has escaped your control and the reality that the stuff outside your control is how your business does business today. Implementing NG-SWG in a basic way, even for just one service, will turn the lights on and show you what's happening and what's not protected.

TIP

At a minimum, you need thorough visibility into user activity in the cloud if you want to be confident in any solution you implement. You also need your organization's decision-makers onboard. You get buy-in when those decision-makers understand that SASE will protect critical things they value but don't realize are dangerously exposed. Millions, even billions, of dollars in value is derived from the work being done "out there."

Step 3: Place Core Inspection Points between Users and Apps

With next-generation secure web gateway (NG-SWG) firmly in place and your visibility into all your traffic dramatically increased, one thing is certain: You may not like what you see next.

Are your people using Microsoft Office 365? Salesforce? Workday? Box? The answer is almost certainly yes. But how big and how mature is that cloud environment beyond your security perimeter and outside of what you can easily see? Just how much of your organization's data is running around out there, unchecked?

For the first time, your organization will be aware of just how at risk it has been. You'll see the flow of data, some of which may be particularly sensitive, among unsecured sites, services, and apps.

Now you have a truthful, and likely worrying, picture of where your organization stands with respect to its dependence on the cloud environment. So many apps and services, so few effective security controls. Until now.

NG-SWG establishes a single-pass, funnel-like, core inspection point for all your traffic in the cloud and in the data center (see Chapter 2). That core inspection point is better than your old perimeter — way, way better.

REMEMBER

Whether it's the result of shadow IT that has been knowingly ignored or a more deliberate process of business digitalization, your old and outmoded security systems have been blind to the details. By replacing old SWG and similar appliances, you'll finally

have complete visibility into who's using non-enterprise-grade applications and services and what enterprise data is being sent "out there" beyond your control. As shown in Table 5-1, NG-SWG and its new inspection points in the cloud let you see what's going on inside all that traffic: web, managed software as a service (SaaS), shadow IT apps, public cloud services, and custom apps in the public cloud.

TABLE 5-1 Using Inspection Points to Monitor Traffic

Out with the Old	In with Netskope	Netskope integrates with . . .
Legacy SWG — only yes or no to web traffic.	Deep inspection of all traffic: web, managed SaaS, shadow IT apps, public cloud services, and custom apps in the public cloud.	Single sign-on (SSO) solution
Secure Sockets Layer (SSL) appliance.	SSL/Transport Layer Security (TLS) decryption is performed in the cloud at cloud-scale with no appliances required.	
Legacy cloud access security broker (CASB) monitors only managed apps that provided application programming interfaces (APIs).	Monitors managed apps plus the unmanaged apps that don't offer APIs; also sees what data is being used with apps, services, and websites.	

Step 4: Introduce Zero Trust Principles to Web, Cloud, and Activity Access

This is when you'll really begin to put your technology to work as you lay the foundation of your SASE. Fortunately, the capabilities needed to set things right are built into the Netskope platform. You have everything you need to reestablish control over your enterprise data, not only on your own network but also, ultimately, everywhere in the cloud.

In Step 3, as shown in Table 5-2, you'll leverage expanded security controls to apply context, going beyond the yes-or-no functions used by your old appliances. NG-SWG also performs deep inspections of both your web traffic *and* your cloud traffic. And now that you've established a new inspection point, its functionality is expanded to exert fine control over the movement of and access to data to manage risk according to policies that make sense for your business.

TABLE 5-2 Setting Policies to Manage Risk

Out with the Old	In with Netskope	Netskope integrates with . . .
Legacy data loss prevention (DLP) — protects only stuff in the data center.	Intelligent DLP protects all data being moved anywhere.	Security information and event management systems and endpoint protection systems
User and entity behavior analytics (UEBA)	Expanded behavior anomaly detection and user risk scoring.	
Various sandboxing solutions.	Advanced threat protection (ATP), including sandboxing and machine learning–based anomaly detection.	

Step 5: Extend Zero Trust to Data Protection and Private Access

Now that your organization is smarter about its traffic, able to see what's going on, and able to enforce policies to secure its data, you can realize the promise of a remote-first workforce. You're going to make it possible for people to work from anywhere and make it a great, fluid, productive experience that is highly protective of your data, your applications, and your employees.

The most noticeable change is to move away from your legacy virtual private network (VPN) — that long, inefficient hairpinning

route that forced all your remote users' traffic back to the data center on its way to the Internet. Using Netskope NewEdge, you can efficiently route that traffic to its destination while enforcing your security policies to protect data.


REMEMBER

Zero trust means enforcing the assumption that any user may be up to no good at all times and ensuring that data is always protected no matter where it needs to go. The Netskope platform's deep contextual knowledge about the user, device, network, behavior, and hundreds of other details, is used to limit activity to only what has been allowed by policy and to ensure that the user is who they say they are.

After it's in place, your security and networking will be transformed to suit the needs of cloud workers and data security (see Table 5-3).

TABLE 5-3 Security and Networking That Meet the Remote Workforce's Needs

Out with the Old	In with Netskope	Netskope integrates with . . .
Legacy VPN	Security cloud to route and protect traffic as dictated by policy	Software-defined wide-area networking (SD-WAN) providers
	Zero trust network access (ZTNA)	Identity management systems for managing and verifying the identities of users and groups
	Zero trust data protection	

Step 6: Refactor Internal Data Center Controls to Closed Loop Risk Management


REMEMBER

The data center is just one more place people and data have to go — it's no longer the center of attention. When you're far along in your SASE architecture, it's time to reconsider the data center.

Perhaps a few applications that are too unwieldy to move or too precious to let out of your sight remain in the data center. To

access these apps, you could use Netskope Private Access, which eliminates the VPN while providing secure access worldwide.

As for all those other boxes and bits that have been replaced by Netskope platform services in a SASE architecture? This is your opportunity to dramatically reduce the complexity and upkeep cost of your network, with those old systems depreciating out of existence and receding into the past while you and your enterprise look forward.

Table 5-4 indicates which older systems or technologies can be replaced using Netskope's platform.

TABLE 5-4 Providing Secure Access to the Data Center

Out with the Old	In with Netskope	Netskope integrates with . . .
Firewalls, intrusion prevention system (IPS), Domain Name System (DNS)	Provides firewall protections as one of many services	Legacy data center controls for ingress

True SASE yields ongoing operational cost savings. Table 5-5 shows a snapshot of what that can look like with a successful SASE architecture. Your finance people will be among the many stakeholders to thank you!

TABLE 5-5 Ongoing Operational Expenditure Savings

Domain	What Happens	Estimated Savings
Multi-cloud access	Enable multi-cloud strategy Improve user experience Streamline procurement and adoption Enable business unit–led apps	30% on connection and infrastructure 20% on future cloud costs
VPN replacement	Remove VPN appliances Direct-to-Net traffic for bandwidth-heavy apps Reduce virtual local area network (VLAN) and firewall policy changes	80% on hardware 50% on security changes and admin

(continued)

TABLE 5-5 *(continued)*

Domain	What Happens	Estimated Savings
Business partners	Manage third-party access Direct access to published apps Apply granular controls for activity Remove lateral movement opportunities	80% on hardware 20% on support time
Mergers & acquisitions (M&A)	Onboarding and integration become more efficient Consolidates current and future network and security costs Synchronizes policy	40% on hardware Onboarding is five times more efficient

Step 7: Monitor, Assess, and Optimize

The road to SASE will take time, but it offers huge, transformative benefits to your security teams and your organization at every step along the way. Security certainly improves throughout the journey, but the impact reaches much farther than that. You'll quickly begin to realize cost savings as legacy security appliances no longer need to be maintained, upgraded, and replaced. Even better, because you're fully optimized for cloud, you don't have to buy capital expenditure–intensive security appliances with excessive, unused capacity.

But the way SASE works at your company will be different from SASE at another company, even though the principles behind SASE are the same. To keep SASE alive and healthy, you must monitor how well it's working, assess where improvements are needed, and take steps to optimize your implementation.

Taking the time to continuously improve will protect your gains. It's difficult to overstate the benefits that NG-SWG, as part of a platform approach, brings to enterprise security. Where your security team had been overwhelmed, trying to make sense and

correlate what a dozen or more complex and independent security applications were trying to tell them in the heat of the moment, they'll now have a unified, automated platform working in real time. All the security services will deliver a shared, coherent message resulting in fewer errors and making it possible to act decisively — and immediately. Every person on your team will be able to get more done to further enhance security and enable your business to run smoothly.

Most important, however, properly architected SASE with NG-SWG will transform business operations and the relationship between employees and technology and among your networking and security teams. Shadow IT can emerge into the light, enabling true digital transformation where best-in-class applications and tools can quickly and securely be adopted to fuel efficiency and drive opportunity. User experience will be preserved, and your users will be happy and productive. This is possible only when security can confidently support digital innovation and the widespread adoption of cloud services and align with networking and all parts of the business on digital transformation priorities. That's what you get with true SASE.

Create a SASE architecture that protects data and drives lasting business value

In a digital world that has left the restrictive confines of the data center for the wide-open possibilities of the cloud, a secure access service edge (SASE) architecture is the only architecture that makes sense. Empower your users, protect your data, and grow your business with a well-designed SASE architecture that combines cloud access security broker (CASB), next-generation secure web gateway (NG-SWG), and Zero Trust principles as catalysts for success.

Inside...

- Learn about the evolution of data, applications, networks, and security
- Understand the roles of CASB, NG-SWG, and Zero Trust in SASE architecture
- Secure your remote workforce at scale and improve the overall experience for your users
- Build a confident plan for the future of your security and networking

Netskope leaders **Jason Clark** (CSO), **Lamont Orange** (CISO), and **Steve Riley** (Field CTO) are widely acknowledged authorities in cloud, security, and networking, with decades of experience from global organizations including Ernst & Young, Gartner, Optiv, Riverbed, and Websense.

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

ISBN: 978-1-119-80073-6
Not For Resale

WILEY END USER LICENSE AGREEMENT

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