Brought to you by:

netskope

Modern SD-WAN for SASE

for dummies®
A Wiley Brand

Connect, optimize, and secure anything

Provide consistent policy and experience everywhere

Monitor networks in real time with AIOps

Netskope Special Edition

Muhammad Abid
Parag Thakore

About Netskope

Netskope, a global SASE leader, helps organizations integrate networking and security seamlessly, leverage AIOps, apply zero trust principles and AI/ML innovations to secure data with high performance connectivity and comprehensive threat protection. Fast and easy to use, the Netskope platform provides optimized access and real-time security for people, devices, and data anywhere they go. Netskope helps customers reduce risk, accelerate performance, and get unrivaled visibility into any cloud, web, and private application activity. Thousands of customers trust Netskope and its powerful NewEdge network to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements. To learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.

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

From Netskope: Amanda Anderson, Robert Arandjelovic, Madhavan Arunachalam, Chad Berndtson, Jason Clark, Fan Gu, Kathy Jacobsen, Jessica Jostes, Naveen Palavalli, Gerry Plaza, Carolyn Robinson, James Yokota

From Evolved Media: Shay Ben-Dov, Theresa Ingles, David Penick, Karen Queen, Vincent Rossmeier, Evan Sirof, Lauren Wagner, Dan Woods

Table of Contents

Introduction

For decades, computer networking has powered our businesses, our communities, and our lives as a whole. As computing and the digital world have evolved, enterprise networking has struggled to keep up. Networking is a dynamic and living practice driven by business need, available technological innovation, and human ingenuity. Sometimes networks surge ahead of practical applications, and in other cases, a once-dazzling technology outlives its useful life and new technologies emerge to fill nascent needs.

This book examines both the history and the future of enterprise networking. It explains how enterprise networks can catch up to and keep pace with the cloud-centric, internet of things (IoT)–driven, mobile-first world. There are many positives about the networking practices of the past. But those models and the technology they employed are no longer optimal for today's enterprises that operate in an increasingly borderless world.

We need a new kind of networking and a new way of thinking. Technology capabilities will not, by themselves, interconnect people using a multitude of devices to a vastly distributed collection of destinations and applications. We need a vision for networks without borders to support our borderless and hyperconnected world.

About This Book

Borderless software-defined wide-area network (SD-WAN) is a way to create a safer, more reliable, and higher-performance networking architecture that fits today's highly diffuse and cloud-based technological environment. This book can help you understand how to develop a plan to implement this networking solution geared for the modern world. And because it's "software-defined," it can also evolve as business requirements change. Even better, it'll also help you work more productively and save money.

Foolish Assumptions

You're not a stranger to the fundamentals of enterprise networking and how the internet has become central to networking. You can easily see why companies moved from a traditional Multiprotocol Label Switching (MPLS) WAN to a more modern SD-WAN. But you're likely wondering what comes next. You can see how the assumptions about where people will work have permanently changed and how mobile devices and IoT infrastructure, along with the continuously expanding world of Software-as-a-Service (SaaS) applications and cloud services, are driving still more change. You want to stop playing catch-up with your network architecture and take advantage of Borderless SD-WAN to support this continuously evolving world.

Icons Used in This Book

Throughout this book, icons appear in the margins to call attention to important information.


TIP

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


REMEMBER

The Remember icon calls out facts that are especially important to know.


TECHNICAL STUFF

Highly technical info that you can safely skip is marked with 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 thinking, "Where can I learn more?," just go to www.netskope.com.

IN THIS CHAPTER

- Tracking the evolution of the wide-area network (WAN)
- Exploring how the software-defined WAN (SD-WAN) improved on WAN
- Understanding the remote-first challenge to traditional SD-WANs
- Seeing why SD-WANs can't be as effective as we need them to be

Chapter 1
Why Networking Is Playing Catch-Up to Modern Computing

The history of computer networking has included many inflection points: Out with the old, in with the new. Local-area networks (LANs) gave way to WANs, WANs gave way to SD-WANs, and now the sun is setting on that era of SD-WANs. In its place, borderless SD-WANs are emerging as the next big thing in enterprise networking. This evolution is enabling seamless delivery of secure, context-aware connectivity from anywhere to anywhere, in a way that is purpose-built for the era of cloud-first, hybrid-centric working. Organizations that embark on this upgrade journey sooner rather than later stand to get out ahead of their competitors with a more flexible, secure, and performant IT infrastructure.

The World of One-to-One

Long ago, in a universe very much like our own, galaxies of businesses all had to survive in a static, hardware-oriented world. Networking began with LANs that connected users and devices within a building — generally a company's headquarters or branch offices. Every employee came into the office every day. LANs enabled anyone within the same physical location to work together on the same network. Any applications that served those users had to be connected to a central data center in a central location, and every action that occurred on the network had to be routed through that data center. This worked well . . . until it didn't.

REMEMBER

LANs had their limitations — most notably the fact that they required all users to be in the same place.

When we moved from LANs to WANs, we were able to put more devices in more locations and connect them to data centers connected to the internet and protected by a firewall. Each device was in a physical perimeter that performed networking functions.

With WANs, branch employees who wanted to connect to the company's applications had to traverse the company's private network — typically through Multiprotocol Label Switching (MPLS) links — back to the central data center. (MPLS is a widely used networking technology for private networks.) Putting applications in each remote facility was simply too difficult and impractical. The centralized location allowed for uniform control and security of applications and the network. This forced all branch offices to connect across the WAN to the data center or corporate headquarters.

If access to the internet was required, the users were routed out to and from any internet-hosted business applications from the central office. This arrangement, known as *backhauling* or *hairpinning,* was cumbersome.

This was true even for companies with global footprints, including international financial institutions, multi-hospital health-care systems, and chain restaurants with point-of-sale (PoS) equipment like Taco Bell or McDonald's.

In the 2000s, MPLS connections enabled carriers to converge voice, video, and data on the same network. Even today, MPLS provides dependable network connections backed by service-level

agreements (SLAs), but it's expensive, and it can take months to plan and provision (see Figure 1-1).

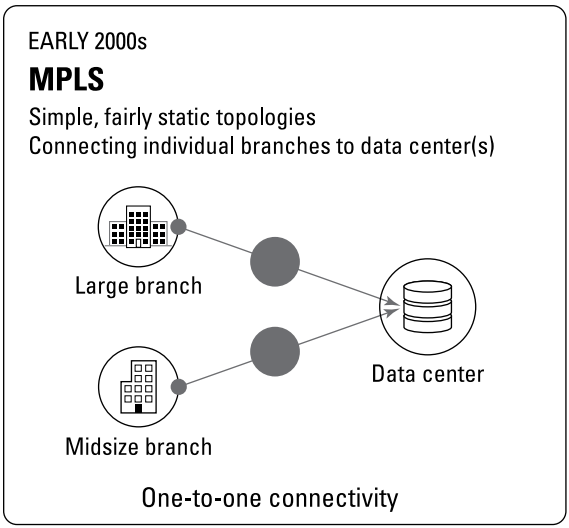

FIGURE 1-1: In the one-to-one world, branch offices use MPLS to connect to a centralized location called the data center, where all the applications are hosted.

However, as companies began to use more immersive applications like video, MPLS simply couldn't provide sufficient bandwidth in a branch location. Furthermore, MPLS was expensive to deploy and maintain, and using it to support the high-bandwidth needs of video consumption was cost-prohibitive. So, the companies were looking for an alternative, cost-effective transport. They found that, and it's well known to us as *internet transport.*

Supporting the One-to-Many World

The expense of MPLS bandwidth and the slowing of a WAN's provisioning were the first signs that the networking structures of the past weren't keeping up with present demands. But there were many other signs as well.

Companies faced a new challenge in a world where software and storage shifted online, a model known as cloud computing and Software-as-a-Service (SaaS). They needed to ensure that they

could deliver and maintain applications — like Microsoft 365 for productivity, Amazon Web Services (AWS) for computing power and data storage, and Google Cloud for Google Docs and other cloud services — securely and with reliable performance. As reliance on the number of immersive video-based, cloud-based, and SaaS applications increased, and as the type of applications changed, simply adding more MPLS bandwidth became onerously expensive. What were companies to do? They needed a hero in shining, digital armor to arrive — and quickly.

Fortunately, SD-WAN showed up just in time, providing the logical next evolution in WAN architecture. SD-WAN was a modern technology that enabled centralized control within a distributed infrastructure, resolving many of the pressures that cloud applications put on traditional WAN.

SD-WAN promised to leverage a variety of different transports (MPLS, internet, cellular) and deliver enterprise-grade performance over one or more links. By abstracting the network layer and routing traffic based upon centrally defined and managed policies, SD-WAN optimized the routing and prioritization of application traffic. SD-WAN promised connectivity between users at the branch to the data center and cloud applications (see Figure 1-2).

Specifically, SD-WAN

- Allowed for a secure and encrypted connection over the public internet, cellular, and MPLS to applications/data both on-premises and in the cloud
- Made it possible to connect one central location such as a data center to many distributed locations such as branch offices
- Allowed companies to route and prioritize traffic based on the type of application that was being used and the data the traffic contained

SD-WAN gave companies more choice and control. It enabled them to use internet transport in a dynamic and efficient way, while still providing the option to use MPLS when necessary. Because using internet connections was much cheaper than using MPLS, this led to much lower costs.

There were also performance benefits from using SD-WAN. Although the public internet could sometimes be less reliable than MPLS, SD-WAN has features that improve the user

experience and maintain high reliability. For example, it could provide quality of service (QoS) functions, which prioritize data. It also has link remediation capabilities, such as a forward error connection, which can help fix problems and improve the connection.

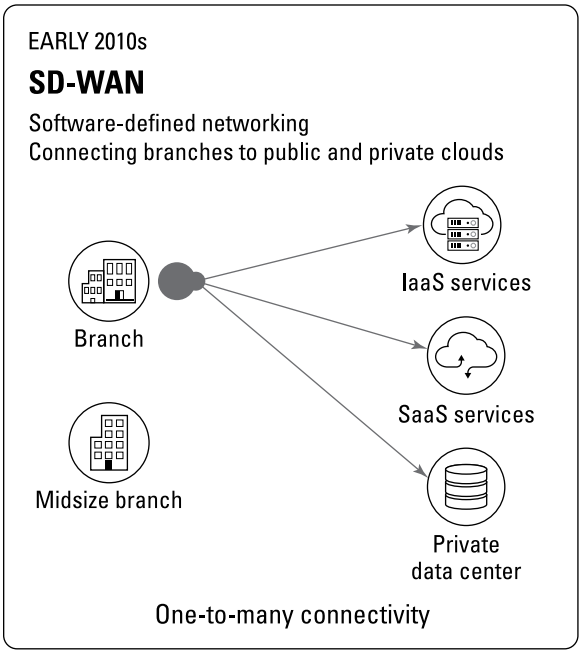

FIGURE 1-2: In the one-to-many world, the branch offices route traffic not just to the centralized data center using MPLS, but also to multiple clouds using MPLS and low-cost internet leveraging SD-WAN.

The result? As soon as companies could experience the power and ease of internet-based SaaS applications (rather than applications that resided in the data center), there was no going back.

You'd think this would have led to a utopian world in which every company was able to fully utilize the power of the cloud through a flexible and affordable network, right?

Well, that *would* have been the case . . . but the world changed again.

The Challenge of Many-to-Many: SD-WAN at a Major Inflection Point

Today, we've entered a new era of borderless enterprise (see Figure 1-3), in which users, devices, sites, and clouds are all connected in numerous ways. We have a remote-first perspective and have moved beyond the four walls of the traditional corporate office. The growth of micro branches, multi-cloud, remote-work, telehealth, mobile fleet, and internet of things (IoT) assets are examples of how the enterprise's networking perimeter has expanded.

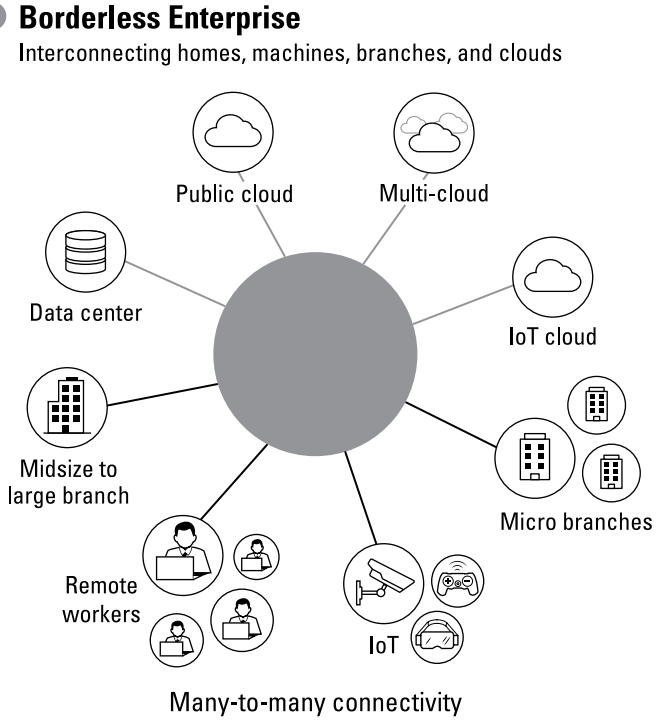

FIGURE 1-3: In the many-to-many world, the borderless enterprise requires simple, flexible, secure, and high-performance connectivity anywhere, from all types of branch offices, remote workers, and IoT devices to data centers and multiple clouds.

The beauty of SD-WAN was that it allowed a company to control the flow of traffic from users in branch offices to the destinations

they wanted to connect to. But the whole system was bound up in a set of assumptions that started to come apart as multiple waves of innovation changed the world. The following sections offer a brief overview of the key trends that have reduced the effectiveness of SD-WAN.

Apps and IoT device proliferation

Traditional SD-WAN was able to support a few thousand applications, which was sufficient at its inception. But with the explosion in volume of cloud applications and IoT devices, its capabilities were challenged. SD-WAN wasn't built to recognize and categorize these new applications and devices based on a rich context, or to set reasonable policies for them. It's impossible to prioritize or secure what can't be understood and sorted into meaningful categories.

IoT device proliferation matters now more than ever. Current network architectures aren't built for the convergence of IoT, operational technology (OT), and information technology (IT). The lack of detailed visibility and granular control of IoT devices poses risks to the network. For this, fine-grained artificial intelligence (AI)/machine learning (ML)-driven segmentation is required, as opposed to traditional Internet Protocol (IP)–based segmentation.

Hybrid work

Today's workers aren't confined to branch offices and can't be protected by SD-WAN networks that were designed with office-based workers in mind. Now, each user and each device is a branch of one. In addition, the number of staff working outside of branches, especially after the COVID-19 pandemic, has increased dramatically to a scale that SD-WAN was never built to handle. Workers expect and deserve a high-quality, secure user experience comparable to that in the central office no matter where they're working.

When employees were initially sent home during the pandemic, IT architects were largely focused on securing remote-access connectivity. Often, little thought was put into long-term architecture planning. Because of this, many companies are now struggling to manage multiple point-based remote connectivity solutions like remote access virtual private networks (VPNs), Security Service Edge (SSE), Zero Trust Network Access (ZTNA), secure web gateway (SWG), cloud access security broker (CASB), data loss prevention (DLP), and SD-WAN appliances.

Connecting users to multiple clouds and networking clouds together

Establishing connections between users, devices, and sites to one or more clouds is an intricate endeavor. This process often proves immensely vexing, encompassing aspects like security, speed, and network efficiency that must be inherently integrated rather than retroactively added. This necessitates the progressive evolution of architectural design.

Use cases include, among others:

- Allowing users to realize secure, optimized access to on-premises or cloud apps over the unreliable internet
- Enabling businesses to facilitate secure, policy-driven application-to-application communication across multiple clouds
- Empowering branches that are globally distributed to access apps across unreliable mid-mile network connections

The common thread among these use cases is the necessity for a dispersed network of cloud points of presence (PoPs), strategically positioned to provide security and optimization in closer proximity to users, devices, sites, and various cloud environments. This strategic arrangement ensures a superior user experience. For example, a PoP located in San Francisco wouldn't deliver a satisfactory experience to users in Bangalore.

Wireless first (4G/5G)

A many-to-many world where people need to be able to work anywhere at any time needs more built-in wireless/cellular capability than what SD-WAN has provided. Fast and reliable connectivity is required at every location, whether it's a constantly moving field vehicle or a construction or exploration site, especially where broadband isn't available or takes a long time to set up. Thus, wireless-first connections are needed for a variety of scenarios, and expanded support for 4G/5G wireless should be a priority, not an afterthought.

Micro branch

The meaning of the word *branch* has changed since it was first introduced. At first, branches were almost always large collections of users. In our massively distributed world, a branch can be five or ten people at a small office, in a bank branch, or working from a construction site. Traditional SD-WAN is too clunky and fat to quickly handle large numbers of micro branches.

What's needed is a small "all-in-one" mobile gateway that has integrated SD-WAN, security, edge compute, cellular, access point, and switch. Micro-branch or branch offices should support home-grown or partner-built lightweight edge-compute applications, thus eliminating the need for extra servers and reducing hardware capital expenditures (CapEx) and operational expenditures (OpEx). Think of this like an application store that allows you to run your own custom applications or one of the applications from a partner catalog.

IT/OT convergence

Proliferation of IoT devices, building smart manufacturing devices, and high-value assets have completely transformed the branch in the borderless world. It's no longer the situation where we envision humans accessing applications with optimal user experience enabled by SD-WAN. The new branch is composed of high-value assets that need to access applications in a similar fashion. These machines could be an automated teller machine (ATM), a crane, a robot on a factory floor, or any other IoT sensor that collects data that must be transported efficiently and analyzed automatically using AI techniques to unlock business value and predict any failures.

Running efficient operations requires compute capabilities at the network edge, to power any lightweight containerized application, specifically customized for an intended use. For example, in an oil field, a fiber-optic cable only reports temperature based on a predefined threshold to the cloud-based analytics service. Running Day 1 operations effectively is equally important; think of a smart manufacturing factory floor with a computer numerical control (CNC) machine, continuously reporting its health-check values to an AI-powered tool that can anticipate a problem before it happens. The network operations staff can remotely connect to the device, troubleshoot any problem, and perform any predictive maintenance, saving costs associated with truck rolls. These innovative capabilities allow convergence of IT with OT.

Limitations of Traditional SD-WAN in Facing the Modern World

Today, traditional network architectures lag behind business requirements and weigh down companies. The enterprise network was never designed for the contemporary, remote-work landscape. We need to rethink how we build modern networks to allow networking and security to tightly integrate and deliver security from the cloud based on Zero Trust principles. These principles state that instead of assuming that everything behind the corporate firewall is safe, security should never trust but always verify. Existing networking and security technologies are like old bricks in a modern glass building — they've been shoehorned into enterprise infrastructures, disrupting the design rather than enhancing it. They either create or simply aren't built to overcome today's challenges. And that's a problem.

All the aforementioned challenges put stress on SD-WAN. Just as SD-WAN developed because WAN couldn't handle a branch-based world, now SD-WAN has reached a major turning point (some might even say breaking point) because it can't handle a many-to-many world.

The following sections outline the reasons SD-WAN has reached its limits.

You can't patch your way to a better network

SD-WAN wasn't built for the modern world, and no minor upgrade will change that. Imagine having a "fat" SD-WAN appliance for every remote worker, IoT asset, or edge application. It's the equivalent of every passenger on a flight trying to board with an old-fashioned, oversized suitcase that's too large and unwieldy for a modern overhead compartment. It's unworkable. Networking teams have traditionally addressed emerging business needs by adding new individual, custom-tailored solutions. Once, every new idea would get a new black box; now each idea gets a new virtual machine (VM). SD-WAN appliances, cellular gateways in branch offices for connectivity, additional products for multi-cloud app-to-app connectivity, and traditional VPN clients — they

all fit this pattern. This approach has created technological silos, built with point solutions that are loosely integrated and separately managed.

Ultimately, IT needs to provide consistent performance and robust security for all global business resources, and it needs to do so in a cost-effective way for every connection. This is an architectural challenge, not a functional problem, that requires the elimination of IT silos and point solution "Band-Aids" to address new business requirements. The "add another box or VM" paradigm won't support the new ways businesses run.

SD-WAN can't scale

SD-WAN can't scale to handle the volume of users, apps, and devices. Branch offices vary in size, from a branch of a few to a few hundred to a couple of thousand people. At the higher end of this range, SD-WAN solutions must be run in a large, load-balancing cluster to work effectively. Imagine a company with tens of thousands of remote workers spread across the globe, or a manufacturing environment with more than 100,000 IoT-enabled machines to manage. In such scenarios, SD-WAN struggles to handle the massive volume of traffic, the multitude of connections, or the complexity of policies and QoS rules that must be defined and enforced.

SD-WAN is missing key functionality

If we look at the way the world works now, it's clear that the control point no longer resides at the boundary of a branch. The ability to define and manage a network can't be connected to a physical perimeter. And we must know much more about each connection to be able to manage networking and QoS.

SD-WAN is missing context awareness. It can't understand which applications users are trying to access and the potential risks they may pose, as well as the range of devices in use and their potential compromise. Companies need this comprehensive knowledge to make informed decisions about application prioritization. Practically, this means that a much richer set of information is required about users, apps, and devices. This understanding enables administrators to make specific rules not only about specific users and devices, but also that allow risks to be managed across broad categories using Zero Trust principles.

In traditional SD-WAN, security was bolted on and not integrated. Traditional SD-WAN allowed branches to communicate directly over the internet to multiple clouds, opening a gaping security hole in the process. Some enterprises opted for distributed security at each branch, which was complex to manage and scale. Plus, it doesn't enable security to follow mobile users and apps wherever they may be. SD-WAN vendors even started throwing around the term *good-enough security* when referring to the branch level. "Good-enough" network security is no substitute for the best-in-breed security provided by secure access service edge (SASE; pronounced "sassy"), a cloud-based architecture that delivers network and security services meant to protect users, applications, and data irrespective of their location. Time has proven that cloud-delivered security is the right approach. Single-vendor SASE enables a unified architecture with simplification and context sharing between SD-WAN and cloud-delivered security. (We cover SASE in more detail in Chapter 5.)

SD-WAN doesn't leverage AI/ML

Traditional SD-WAN failed to leverage ML and advanced predictive analytics that could result in effective and automated operations providing ease and efficiency to the network teams looking to solve problems before they occur and deliver an unmatched experience from any user to any application. The modern SD-WAN is expected to collect all the required data throughout the entire network — per remote user, per branch office, and per cloud workload — and leverage AI/ML to deliver enterprise-wide predictive insights that make it easier for network engineers to ensure higher network performance while end users gain higher productivity.

SD-WAN can't deliver a quality experience for 60,000+ applications

A typical SD-WAN implementation may have understood the characteristics of 3,000 or 4,000 applications, but the modern landscape has 60,000 or more applications. Knowing the characteristics and mission-criticality of these applications allows for prioritization of user experience remedies. For instance, a person using Zoom for business should be optimized, while someone using YouTube or gaming apps from work doesn't need to be optimized.

SD-WAN doesn't make the control plane simple to use

SD-WAN has made strides in separating the data plane from the control plane, but having the control plane as a do-it-yourself (DIY) on-premises has fallen short of making the control plane simple to use. What organizations should look for is a 100 percent SaaS-based controller that has the ability to support advanced routing such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF). Organizations should also look for the infrastructure that powers SSE capabilities and explore if this provides global-coverage, full-stack security at every location; extensive peering with cloud providers; and lowest possible latency so that the customers don't have to make a trade-off between security efficacy and performance — a very hard problem to solve. A single-click configuration of SSE-type capabilities for an SD-WAN box at a branch automatically finds the nearest PoP.

4G/5G wireless was an afterthought

Expanded support for 4G/5G wireless must not be an afterthought. Instead, it must be supported in many different ways — as an integrated transport option in the SD-WAN device and as a wireless WAN solution extending the reach of the SD-WAN gateway running in the closet. Branch offices may need wireless access, but so will mobile equipment like trucks or robots. Wireless plays a different role in each of these contexts.

The architecture wasn't born in the cloud

The overwhelming complexity of cloud networking leads organizations to experience immense frustration when it comes to connecting users, devices, and sites to the cloud or multiple clouds. Architecture needs to evolve so that security, speed, and network optimization are built in as essential parts of connectivity, not bolted-on afterthoughts. Use cases could range from a user getting secure, optimized access to on-premises or cloud apps over unreliable internet or branches that are globally distributed and are trying to access apps across unreliable mid-mile or multi-cloud app-to-app connectivity with security. But connecting to the cloud also requires moving the network's PoP closer to the user to ensure performance and a high-quality user experience.

SD-WAN isn't extensible

Today, networking is moving to the cloud and compute is occurring closer to the edge. Initially, many SD-WAN vendors started on the path of service chaining SD-WAN VMs with on-premises partner security VMs housed on a large appliance. However, a lot of these security and networking functions have since moved to the cloud. Consequently, there's an increasing need to have lightweight compute functions closer to the data source. Imagine a retailer that wants a PoS system to be available 100 percent of the time; it would move the PoS system as an edge compute application to maintain high availability or, in the IoT world, run Azure IoT Edge runtime on the edge. Other examples may include your own custom applications.

SD-WAN is rigid and irrelevant

The success of any technology depends on its relevance within the current tech landscape. It's all about context. Despite its one-time strengths, SD-WAN just doesn't support "any-to-any" or "many-to-many" connections in the way that today's organizations require. It also doesn't scale well, a must for any industry.

REMEMBER

SD-WAN had its day in the sun. But it has now become too rigid and inflexible to support transformation in our hyperconnected world. It will fade into the background and be overtaken by the next generation of technology. And so the cycle of innovation goes.

WARNING

At some point, the lack of assured application experience or uniform security, visibility, or application management becomes like a dam with growing cracks, heading toward a catastrophic breakdown. Users and devices find themselves caught in a downstream deluge, unable to access remote resources with the proper level of performance or cybersecurity policy. So, in the face of this flood of new requirements, what's an IT architect supposed to do to stem the tide? Organizations of all shapes and sizes now need an SD-WAN built for the many-to-many, any-to-any world. Fortunately for those of us with a stake in technology, such a form of SD-WAN has arrived. Netskope calls it *Borderless SD-WAN,* and it goes beyond what traditional SD-WAN offers.

IN THIS CHAPTER

- Understanding the benefits of Netskope Borderless SD-WAN
- Securing a software-defined wide-area network (SD-WAN)
- Serving the needs of the micro branch
- Supporting end users, wherever they are
- Achieving fast and reliable connectivity with 4G/5G
- Taking full advantage of internet of things (IoT) capabilities
- Seeing what borderless SD-WAN can do for you

Chapter 2
A Vision for Fully Realized SD-WAN: The Borderless Future

SD-WAN succeeded as a technology because users in branch offices needed to have much better support for routing their traffic and quality of service (QoS) over a combination of low-cost internet links and Multiprotocol Label Switching (MPLS). But as Chapter 1 summarizes, the world kept expanding in ways that SD-WAN wasn't equipped to handle. Each of the areas we mention in Chapter 1 — exploding mobility, proliferation of apps and IoT devices, and multi-cloud networking — must

have wireless networking, edge computing, and cloud-delivered security. These requirements stress traditional SD-WAN, and the products that have risen to help it, to the breaking point.

In this chapter, we dive into these problems in more detail and specifically address how Netskope Borderless SD-WAN will fix them.

Borderless SD-WAN: Networking for a Many-to-Many World

Right now, when users or devices are cast adrift in the digital sea, interacting with numerous clouds and a vast array of applications, they can feel like sailors navigating the vast expanse without a compass or a map — protection and optimization may be as elusive as a lighthouse in a storm. Even when they're thrown a lifeline, it turns out to be a hodgepodge of solutions that are an administrative nightmare to hold together. That isn't what organizations want.

The goal of Borderless SD-WAN is to allow any person or any device to have secure, optimized connectivity from wherever they are. It sounds great, doesn't it? But how does it work? How can this promise come to life?

To fully explain Borderless SD-WAN (see Figure 2-1), we need to explore how six current scenarios within computing, networking, and security are breaking traditional SD-WAN:

- Secure SD-WAN
- Micro branch
- Endpoint SD-WAN
- Wireless WAN gateway
- IoT intelligent access
- Multi-cloud networking

As we move through each of these, we explain what's needed in the many-to-many world, how SD-WAN and current solutions fall short, and how Borderless SD-WAN will help.

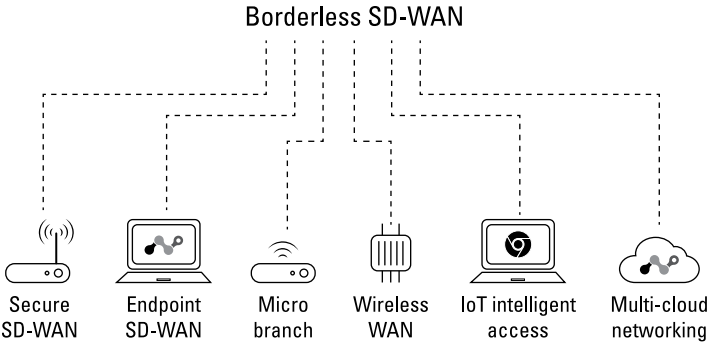

FIGURE 2-1: Borderless SD-WAN supports software on laptops, cellular gateways, and micro to large branch or data center appliances, and acts as a virtual gateway for multi-cloud networking.

Secure SD-WAN

Security and networking have always been intertwined. As we discuss earlier, MPLS links were expensive and static, and they lacked application-level visibility and control. In response to the high cost of MPLS, SD-WAN was born. SD-WAN augmented MPLS with high-bandwidth, inexpensive internet links, allowing users in branches to connect directly to distributed on-premises and Software-as-a-Service (SaaS) applications. SD-WAN's goal was to deliver the same level of performance and security over commodity broadband links, which it efficiently achieved with application-aware visibility and control. This allowed administrators to define policies that ensured that Zoom was a higher priority than Netflix.

REMEMBER

We're at another inflection point where it's time to look beyond traditional SD-WAN. The sheer volume of cloud applications and IoT devices has exploded, and traditional SD-WAN solutions with controls based on application-centric policies are not enough, especially if the specific SD-WAN solution lacks Zero Trust principles.

The evolving enterprise now needs Zero Trust–enabled, context-aware SD-WAN to provide fast, reliable, and secure access to any application and any device at any location with full visibility and the right set of controls. This is possible using contextual policies that include understanding applications, application risks, users, user risks, devices, and device risks, all of which make network operations more intelligent and more secure.

SD-WAN solutions usually allowed administrators to set policies for a few thousand apps, but this is now only a fraction of the number of applications that exist on the web and in the cloud, which exceed multiple tens of thousands. If you can't discover applications, how can you control them? Some of these apps may be enterprise ready, while others are not. Automatically assigning traffic priorities to all supported applications remains a big challenge. Network operations teams need to configure these applications manually one at a time. That process is extremely slow and error-prone, and it doesn't scale for tens of thousands of applications.

The Borderless SD-WAN solution supports a database of 60,000+ applications. Information technology (IT) administrators aren't going to configure QoS policies for these applications one at a time, so rating every application with a Cloud Confidence Index (CCI) is important. The CCI offers the enterprise-readiness score of an application; this score is used to produce out-of-the-box smart defaults for QoS-driven traffic prioritization. This takes all the manual labor away from the network operations team and results in much more efficient operations. (For example, Zoom has a CCI of 82; that's marked as a high priority by default. SureVoIP has a CCI of 38; it's treated as low priority out of the box.)

Companies aspire to have continuous monitoring of the health of their links to applications and the flexibility to switch the application from a bad link to a good link in a sub-second fashion. They also seek on-demand remediation and Transmission Control Protocol (TCP) optimization.

SD-WAN used static Internet Protocol (IP) address/subnet-based segmentation. Security was derived from knowledge and control of the network. This worked in yesterday's world. What about micro-segmenting IoT devices at the edge as they become compromised and provide a path into the enterprise network? Traditional SD-WAN doesn't provide visibility into IoT devices, and with IoT proliferation, this has become more important than ever. Context-aware capabilities leverage artificial intelligence/machine learning (AI/ML) to automatically detect all IoT devices, managed and unmanaged, and micro-segment to manage risks that may be associated with a compromised device. For example, an IoT device like a camera could be sending video to an unsanctioned application. This camera can easily be blocked through micro-segmentation to reduce the blast radius if the IoT device is compromised and can easily be remediated.

Borderless SD-WAN addresses these needs because it collects a much larger set of data about users, devices, applications, and networks. The richer context allows granular policies to be applied in a precise manner.

Micro branch

The term *micro branch* refers to a small office, a cafe, or a retail store, which in today's remote work culture might be a location where a person is working. In these scenarios, there may be only a few users or devices; however, their needs for connectivity, QoS, and security remain as crucial as they would be in a conventional branch office. They need a thin gateway that is cost-effective and offers quality connectivity and security.

Borderless WAN supports the micro-branch use case by providing lightweight software that resides on a compact secure access service edge (SASE) gateway, a hardware device located in a branch or a micro branch. In Borderless SD-WAN, network and security services are converged. A consolidated SASE gateway is the most suitable way of delivering Borderless SD-WAN. It can converge capabilities such as cellular connectivity, SD-WAN, Wi-Fi, security, and edge compute in an all-in-one fashion, all operated from one console and governed by one policy. The ideal setup is one-click integration through a single console with an intelligent Security Service Edge (SSE) to provide comprehensive security. (By the way, Netskope's single-vendor SASE delivers just this combination.)

REMEMBER

Distributed Borderless SD-WAN means being able to offer a branch-quality experience in any location, from a small office to a fleet vehicle in a harsh environment like a Texas oil field. This requires being able to support multiple services from a single device in a thin, lightweight form factor. Most SD-WAN vendors can't offer this; they can provide SD-WAN only for traditional branch offices.

Endpoint SD-WAN

In today's world, secure and high-performance remote access is often achieved through an SD-WAN device combined with virtual private network (VPN) software clients. However, this setup can be inconvenient for remote users who don't enjoy the same smooth connectivity experience as their office-based counterparts. The dual dependence on SD-WAN and VPNs also means

companies must juggle multiple vendors, devices, and cost centers, making this approach unscalable.

Relying solely on a VPN software client without an SD-WAN device leads to many issues. VPNs, for instance, suffer from a lack of visibility, static point-to-point connections, latency from backhauling, and an inability to optimize voice/video traffic. The failure to recognize who is accessing what and from where, combined with unnoticed network performance variations, can directly impact user productivity.

Traditional VPNs are designed to backhaul traffic to VPN concentrators, resulting in added latency due to suboptimal path selection. SD-WAN solutions can overcome some of these issues, but they're hardware-dependent and lack Zero Trust security. They can't be scaled to the needs of every remote user.

Today's workforce expects Zero Trust security and reliable connectivity, regardless of location. IT organizations, in turn, need simplicity and extended visibility to support remote users adequately. Despite its "software-defined" moniker, SD-WAN relies on specialized hardware or dedicated servers, primarily in branch offices.

Installing SD-WAN on a laptop can significantly improve the user's experience, regardless of where they're accessing the network. Network operators gain full visibility into all applications and links being used, aiding in troubleshooting. No matter where users are, even in places where the internet is weak, SD-WAN installed on a laptop will improve the experience by optimizing and creating QoS policies to prioritize traffic for those latency-sensitive applications.

The hardware-based nature of SD-WAN becomes problematic as the volume of remote access connections continues to grow. Consider a large insurance company that had to ship physical SD-WAN devices to 25,000+ remote contact center agents. When the employee turnover spiked, more than 500 devices per month weren't returned, causing security risks, increased costs, and logistical headaches. This scenario highlights the need for a solution like Borderless SD-WAN that can be run directly on an employee's laptop.

As for alternative pathways to remote access, like Zero Trust/Zero Trust Network Access (ZTNA) systems, they also have their

drawbacks. Most Zero Trust/ZTNA clients can't offer the benefits of SD-WAN optimization, and most SD-WAN vendors fail to deliver the Zero Trust elements and require hardware. A solution that unifies Zero Trust capabilities and SD-WAN's application optimization benefits in software form could offer the best of both worlds without hardware. Today's modern work landscape demands a 100 percent software-based unified SASE client (see Figure 2-2).

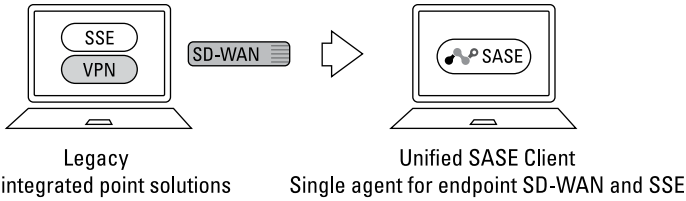

FIGURE 2-2: Borderless SD-WAN supports a unified SASE client that unifies SD-WAN optimization with SSE security to meet the demands of today's hybrid workforce.

REMEMBER

Remote access is only effective when it provides a high-quality user experience and Zero Trust security everywhere the user works. Some specialized solutions can also offer this, but the problem then becomes having to manage a plethora of products instead of a single Borderless SD-WAN solution.

Wireless WAN

To be able to work anywhere at any time in a many-to-many world, there is a need for more than what SD-WAN provides on the wireless front. What's required is fast and reliable connectivity in every location, whether it's in a perpetually mobile field vehicle or a stationary enterprise access point on a wall that provides a strong signal from within IT closets.

Traditional SD-WAN can't do this. Borderless SD-WAN can. From the customer's perspective, two scenarios or use cases emerge.

The first use case involves an organization looking for a device that consolidates multiple functions like SD-WAN, security, edge compute, and wireless gateway into a single all-in-one device, easing pains that are associated with managing complex networks and cost centers. The wireless gateway should support global carriers and offer quality of experience (QoE) capabilities to dynamically adjust the application bandwidth to save cost on expensive

cellular links. For example, it may be acceptable to have Netflix as a medium-priority application when a broadband link is available along with the cellular link, but if the broadband link fails, a dynamic QoS policy can block Netflix over cellular links.

The second use case incorporates Borderless SD-WAN as a wireless WAN gateway device. The Netskope cellular gateway can be mounted on a wall/ceiling and powered by a Power over Ethernet (PoE) cable. It provides strong signal strength to the Borderless SD-WAN SASE gateway located in the IT closet. This setup helps organizations manage all devices from a single console, bypassing the need for multiple vendors and consoles. This capability saves costs and helps to overcome the limitations of external antennae, which lose signal strength as a function of distance, making them almost unusable if the distance between the closet router and the rooftop is too long.

Multi-cloud networking

Traditional SD-WAN fails to properly handle multi-cloud networking and automated operations. Companies may access dozens of distinct clouds, each hosting different workloads. They're looking for a networking solution that provides secure connectivity to all these clouds while enabling policy-driven application-to-application communication. Some emerging vendors provide a cloud networking solution that supports visibility and control of intercloud connections through a set of policies and automated configuration of connections. These multi-cloud networking vendors solve an important problem: They enable companies to migrate their workloads to these clouds from a unified dashboard that provides the insights needed for effective orchestration, which is great — for as far as it goes. But Borderless SD-WAN goes further, providing integrated security and optimization for every user, device, site, and cloud. With Borderless SD-WAN, customers get one-click access to SSE, ensuring full-stack security to any cloud.

Imagine running thousands of servers across multiple clouds, where these servers need to fetch updates from the internet. Given that the servers are exposed to cyber threats, how can their protection be assured? Borderless SD-WAN uses its rich contextual awareness and its ability to integrate with cloud automation systems like Terraform to apply policies controlling intercloud connectivity, network optimization, and security. This multi-cloud networking is managed from a single unified console, which can

easily instantiate Borderless SD-WAN's lightweight software across all clouds. From this single unified console, automated cloud operations allow these instances of Borderless SD-WAN software to interoperate and exchange routes with major cloud providers like Amazon Web Services (AWS) Transit Gateway, Azure Virtual Router, and Google Cloud Platform (GCP) Cloud Router. With one-click access to Netskope Intelligent SSE, companies also have integrated full-stack security to protect from all cyberattacks.

Borderless SD-WAN also extends the enterprise WAN, allowing users to connect to multiple clouds and integrate public cloud infrastructure into the Borderless SD-WAN fabric. This allows applications running on user devices to consume cloud-delivered services like Infrastructure-as-a-Service (IaaS) in a secure and performant manner.

The result: Borderless SD-WAN converges networking and security uniformly at every edge.


TIP

With integrated security and optimization, companies can set policies uniformly across the entire network, encompassing all devices and all users on all clouds. This means that the policies will be consistent no matter which cloud a user is tapping into. What's optimized, allowed, and restricted won't change depending on the cloud in use. Not only can each cloud talk to one another (AWS needs to talk to GCP, which needs to talk to Azure, and so on — who knew that clouds were so chatty?), but connections can be routed securely though multi-cloud environments. That's how multi-cloud networking needs to be done in this day and age in order to follow best practices.

IoT intelligent access

Companies today require intelligent access to IoT from their SD-WAN. Organizations want their IoT/operational technology (OT)–enabled assets to connect to the cloud so that edge computing can run on these assets, forwarding to the cloud only the data necessary to analyze a problem and proactively determine a solution. They also need to be able to take advantage of the IoT capabilities for remote monitoring, troubleshooting, data collection, and predictive maintenance, while reducing unnecessary truck rolls — the in-person service calls that drive up labor, gas, and other expenses. Without these features, achieving the

desired return on investment (ROI) from their ecosystem of IoT assets will be challenging.

The goal is to provide an IoT asset with high-quality, secure connectivity with wireless and edge compute.

For example, for a computer numerical control (CNC) machine in a factory, ruggedized Borderless SD-WAN devices not only provide Wi-Fi for sensors but also support edge compute capabilities to collect information such as temperature and vibration data from sensors. They also selectively gather useful data based on predefined thresholds, thus offering enhanced operational efficiency at dramatically reduced cost.

Netskope SASE gateway supports zero-touch provisioning and integrated edge compute, bringing the compute closer to the data source. It can collect and extract data from IoT sensors and deliver only data exceeding preset thresholds to the IoT cloud, using cellular or other transport connections of choice. Offering scalable application life-cycle management (ALM), it provides out-of-the-box container services like Azure IoT Edge runtime, as well as the ability to run other services from a catalog of services for mobile devices. Customers can run their own custom applications as well. Netskope SASE gateway, with its developer-friendly software development kit (SDK) and application programming interfaces (APIs), provides choice and flexibility and allows enterprises to bring their own applications.

To provide Day 2 support and ongoing maintenance, the Borderless SD-WAN gateway supports outside-in access through the natively built IoT manager to high-value assets, thereby accelerating time-to-incident resolution. This feature helps avoid the need for a truck roll, enabling the IT person to troubleshoot and diagnose remotely. By anticipating a malfunctioning device, they can promptly send the right part to fix the issue, thus avoiding or minimizing business disruptions.

What to Expect from These New Capabilities

Companies should have high expectations of what new capabilities Borderless SD-WAN can provide to them. Here is a list of what Borderless SD-WAN must do to support security and

performance, including elements we've already covered and a few additional items:

- **Provide visibility for contextual awareness.** Monitoring, prioritizing, or defending what's unseen is impossible. A Borderless SD-WAN solution should offer as much visibility as possible about users, devices, applications, and networks throughout the traffic flow. When possible, this information should be monitored and updated in real time.
- **Provide intelligent access and routing that eliminates complex administration.** Aim for a solution that enables single-click configuration of SSE and SD-WAN capabilities for an SD-WAN device at a branch, remote users, IoT devices, and multi-cloud environments. This solution should locate the nearest point of presence (PoP) automatically. Additionally, seek a scalable cloud controller that has the ability to interoperate with advanced routing such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF).
- **Offer cloud-delivered security built on Zero Trust principles.** Security must now follow the connectivity wherever it goes and react in real time to changing conditions. Traditional SD-WAN systems started to address this issue with bundled firewalls, but this doesn't allow security to follow mobile users and apps wherever they may be. A Borderless SD-WAN solution, tightly integrated with intelligent SSE, delivers single-vendor SASE. It enables unified architecture with hybrid network security, delivering on-premises security like east–west firewall, intrusion prevention system/intrusion detection system (IPS/IDS) and segmentation at the branch, and 360-degree protection with cloud-delivered security.
- **Offer scalable, AI-driven operations.** Borderless SD-WAN leverages AI-driven operations to monitor the network at all levels — including activity at the level of users, branches, and clouds — to enable proactive troubleshooting and comprehensive analytics. Identifying anomalies and warning signs early using AI and ML helps reduce the number of support tickets and mean time to resolution, which in turn allows customers to run large-scale networks. AI and ML also help to automatically rectify any poor network conditions to deliver the highest network performance.

- **Provide assured application experience and security for tens of thousands of applications and IoT devices.** A typical SD-WAN implementation may understand the characteristics of 3,000 or 4,000 applications, but the explosion of cloud applications and IoT demands a Borderless SD-WAN solution that can detect and automatically prioritize 60,000 or more applications and automatically micro-segment risky IoT devices.
- **Offer expanded support for 4G/5G wireless that is not an afterthought and is supported in many different ways.** With Borderless SD-WAN, users can access 4G and 5G networks securely where a broadband connection is unavailable or time-consuming to establish. This capability is crucial not only for branch offices but also for mobile fleets or machines and robots.
- **Provide a cloud on-ramp that brings cloud, network, and security together.** Organizations experience immense frustration when it comes to connecting users, devices, and sites to the cloud or multiple clouds, due to the overwhelming complexity of cloud networking. Architecture needs to evolve so security, speed, and network optimization are integral parts of connectivity, rather than a bolted-on afterthought. To deliver a Borderless SD-WAN solution and integrated security, high-quality connectivity must be close to users and devices, wherever they are. A global cloud with PoPs everywhere allows the functionality to run at the edge and deliver high-quality connectivity and performance for the cloud on-ramp.
- **Provision edge compute applications to enable new services.** More containerized applications are being deployed at the network edge. This shift creates significant application management challenges that current SD-WAN architectures aren't built to handle. Examples include an IT admin who wants to run a digital experience monitoring application of their choice in a branch.

IN THIS CHAPTER

- Understanding the importance of cloud-first architecture
- Creating more sophisticated management, control, and data planes
- Using machine learning (ML) and artificial intelligence (AI) to monitor networks in real time

Chapter 3
How Borderless SD-WAN Works

There's an old saying in the tech world, attributed to Thomas Edison, that vision without execution is hallucination. Or as they might say in Texas, without execution "that thar' tech is all hat and no cattle." Well, Netskope's version of borderless software-defined wide-area network (SD-WAN) has been engineered from top to bottom to deliver a great experience for the people who use the tech and the people who configure, run, optimize, and debug it. In other words, Netskope has the execution. They've got the cattle.

Execution for Netskope Borderless SD-WAN has to break new ground because the technology expands both the scope and the reach of traditional SD-WAN and has created a set of requirements that break the architecture and administrative functions used for SD-WAN. As a result, network architecture must also change to allow users operating from anywhere around the globe to have a pleasant experience.

The large scope of services being delivered to a huge population of users, branches, internet of things (IoT) devices, and the cloud demands a shift in how the management, control, and data planes

work. Older configurations that were built only to address branch offices are replaced by policies that express the desired outcome based on a much richer context about the user, device, application, data, and network. For these reasons, Borderless SD-WAN works in a completely new way using a cloud-native architecture. This chapter looks at what this means in practice.

Why Borderless SD-WAN Must Have Cloud-First Architecture

The many-to-many world we now live in radically changes the numbers of users, devices, sites, and clouds that need secure, optimized connectivity with Borderless SD-WAN. For example, if a company moves thousands of call-center workers to a work-at-home model, the SD-WAN function must scale massively. To provide high-quality service to those staff, a reliable point of presence (PoP) near each individual is necessary. The only way to achieve this involves moving the implementation to the cloud and adopting a new connectivity strategy. That's exactly what Borderless SD-WAN does.

Many vendors claim to offer Borderless SD-WAN's cloud-native architecture, but few actually do. Vendors will state, "Our management plane, control plane, and data plane are cloud delivered." But the fact is, they actually run the software as active-backup servers in the cloud. The problem with this strategy is that every time you run out of capacity, vendors need to continuously spin up active-backup servers in the cloud to address varying customer needs. With so many devices, sites, and users to connect, this architecture and approach won't scale. Simply moving a software implementation to run in the cloud doesn't mean that the system takes advantage of the scaling potential of cloud technology.

To take advantage of the cloud, Borderless SD-WAN uses software containers and microservices, each of which can be scaled separately using the elastic resources of the cloud. This architecture allows Borderless SD-WAN to deploy and manage thousands of sites, IoT devices, and end-user endpoints.

More specifically, Netskope Borderless SD-WAN operates on top of a highly redundant distributed cloud platform with multiple layers of redundancy, backup snapshots, and auto-failover. All components within the Borderless SD-WAN architecture are deployed in a fault-tolerant and redundant cluster, with services deployed as active–active, which allows load balancing in addition to high availability.

This allows Borderless SD-WAN not only to maintain high uptime independently but also to auto-scale each service. Each service is deployed behind a cluster of load balancers configured for high availability (HA), and every such pool is monitored for load using various metrics.

If machines in a pool are overloaded, additional machines are added to distribute load. Borderless SD-WAN's services are also designed to be stateless and can, therefore, scale out elastically, across server instances within each data center, as well as between data centers without downtime or performance impact.

Reshaping the Management, Control, and Data Planes

Borderless SD-WAN architecture enables the management plane, control plane, and data plane to be much smarter and more sophisticated. In this section, we describe the new approaches to each plane and their new capabilities.

The management plane

The *management plane* in SD-WAN emerged from a central service, which was usually on a virtual machine (VM) in a data center or possibly in the cloud. The main task of the management plane was to manage SD-WAN branch devices across the network and ensure they were updated, provisioned, and controlled so that the SD-WAN software was running properly on the company's hardware. That worked until it didn't, when new challenges emerged.

Now, companies must account for a plethora of IoT and personal devices, as well as laptops that are connecting to the network and multi-cloud environments. Borderless SD-WAN has to manage all

these diverse use cases, as well as all the data they produce and application configuration. That's why, in Borderless SD-WAN, the management plane has undergone a radical transformation. It's cloud-native, highly redundant, multitenant, and easy to use with an intuitive, web-based interface. This evolution was critical because Borderless SD-WAN has to perform several vital functions:

- **Software management on distributed use cases:** High performance and secure connectivity need to be extended to every user, every device, every branch, and multi-cloud environments. Borderless SD-WAN must manage the software on these distributed use cases, a much larger task than managing the software on the smaller number of SD-WAN boxes that companies previously had.
- **Data and telemetry management:** It must manage all the data and telemetry that the network receives. This can happen only with the scalability provided by Borderless SD-WAN.
- **New remote work model management:** It must be able to handle the new remote work model at scale, when organizations no longer are trying to run 400 remote offices and are instead trying to remotely manage and consume data from thousands of remote users efficiently and securely.


TIP

With Borderless SD-WAN, companies receive complete configuration and visibility into all their network devices through the management plane. The Borderless SD-WAN management plane can also supply information on application health, as well as automated and secure software updates to all network devices at the same time. Traditional SD-WAN products can't provide such a comprehensive management view of a company's entire network and all its devices.

The control plane

The *control plane* is how companies can build and control the network topology; this is how a branch discovers another branch. In the SD-WAN of the past, this control plane typically operated on a physical hardware device on which the SD-WAN data plane also resided. If the data plane failed, the control plane failed with it, offering no resilience whatsoever. In other situations, when the

control plane ran out of adjacency capacity (to technical gurus, if the control plane is using a Border Gateway Protocol [BGP], it's the BGP running out of adjacency capacity), more SD-WAN devices would need to be installed because the control plane and data plane were running on the same router/hardware. Furthermore, the SD-WAN control plane simply was not designed to handle the sheer volume of users, devices, branch offices, and multi-cloud environments that it would need to manage.

With Borderless SD-WAN, the control plane is moved to the cloud and delivered via Software-as-a-Service (SaaS). It interoperates with an on-premises control plane like BGP and Open Shortest Path First (OSPF). As a result, a controller no longer physically lives in a company's environment. It's a service that organizations use, just like Salesforce, Workday, or any other SaaS. The main reason this was needed is that, by having the control plane operate as a SaaS, Borderless SD-WAN now has the ability to scale on demand. Another benefit is that companies no longer have to worry about adding more hardware to increase control plane capacity in order to add new branches due to a company's growth.


TIP

This move of the control plane to the cloud enables Borderless SD-WAN to manage the topology of a network in a more detailed and sophisticated manner than before. This is necessary as networks expand and there are more personal and IoT devices, as well as connections to wireless gateways, to handle than ever before.

Borderless SD-WAN moves controllers completely to the cloud, offering levels of control, simplicity, and scale that simply weren't possible with SD-WAN.

The data plane

With a 100 percent SaaS-based controller providing visibility into the entire network and all the devices connected to it, companies gain unprecedented insight about the data moving through their network and eliminate DIY and complex on-premises controllers.

The *data plane* also has changed significantly under the Borderless SD-WAN paradigm. MPLS was about packet routing; traditional SD-WAN heralded a major step forward by making routing

decisions and policies based on applications without accounting for any context associated with applications, users, and devices. In other words, traditional SD-WAN couldn't accommodate policies based on application risks, user-to-user risk, or device-to-device risk. Security was bolted on in SD-WAN, as shown in Figure 3-1, and it was either "good enough" or loosely integrated, making it operationally complex and unable to share context between network and security.

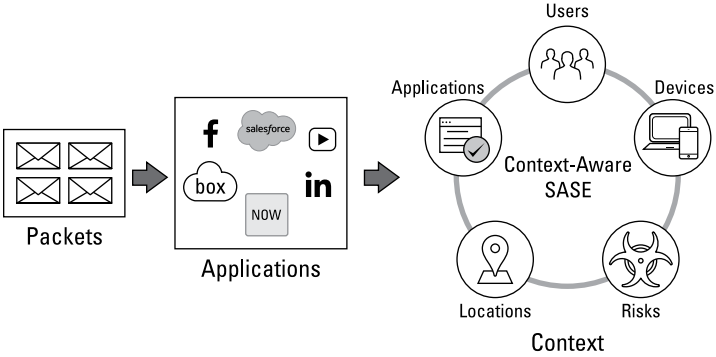

FIGURE 3-1: Borderless SD-WAN contextual policies include understanding applications and application risks, users and user risks, devices and device risks, all of which make NetOps intelligent and secure.

In today's environment, also shown in Figure 3-1, companies need to uniformly set policies around application performance, Zero Trust access, and security for every remote user, site, device, and cloud.

Borderless SD-WAN takes these capabilities to entirely new levels:

- **The one click to Security Service Edge (SSE) automates connectivity from Borderless SD-WAN to SSE.** And it gives you ease of service consumption without the need to create traffic routing configurations or the use of Proxy Auto-Configuration (PAC) files.
- **Borderless SD-WAN expands the context about the user, device, data, and application, which enables far more effective and sophisticated policies to be defined and enforced.** By scoring solutions to make contextually relevant security and traffic routing decisions in the cloud, it's possible

to better manage user risk and detect and address device risk with segmented policies in real time. Imagine detecting and automatically prioritizing and optimizing 60,000+ applications or detecting IoT device risk based on AI/ML.

- **Borderless SD-WAN also keeps remote users, sites, devices, and multi-cloud environments close to a global network of PoPs.** Borderless SD-WAN combined with SSE inserts itself between the users and applications at these PoPs. That's how it performs its magic and provides the services needed to apply policies and improve quality of service (QoS) with integrated security. But to make this work, the network connection and the Borderless SD-WAN services must be close to the user in network terms. If all the Borderless SD-WAN and SSE functionality is in a data center in Seattle, and your users or branch offices are in Mumbai or Berlin, the experience will be slow and inconsistent.

And that's why Netskope created a global network of PoPs all over the world called NewEdge.

Netskope NewEdge is a purpose-built private cloud that combines network and security services on a large scale, providing low-latency traffic on-ramps in more than 70 regions around the world. The NewEdge network enables seamless integration of Borderless SD-WAN and SSE services, ensuring that users, branches, sites, devices, and multi-cloud environments globally have close proximity to these converged services. SSE at NewEdge offers various services, including next-generation secure web gateway (NG-SWG), cloud access security broker (CASB), Zero Trust Network Access (ZTNA), SaaS security posture management (SSPM), cloud security posture management (CSPM), Firewall-as-a-Service (FWaaS), and data loss prevention (DLP). Borderless SD-WAN at NewEdge provides an optimized pathway for SaaS applications and mid-mile services in the cloud. Overall, NewEdge with SSE and Borderless SD-WAN guarantees secure and high-performance connectivity for cloud, web, SaaS, and private applications.

Making Room for Artificial Intelligence

In the management planes of Borderless SD-WAN, more AI-driven operations can be implemented compared to traditional SD-WAN. Companies achieve a full view of their network, and AI can monitor in real time what a good, safe link for external devices connecting to the network should look like. The AI can identify a bad link, and it can also use historical data and context to predict when a link might become faulty. ML and AI can also provide an automated solution when these types of problems arise, such as forward error corrections or *automated link remediation* (a correction that allows users to be automatically switched to a better, currently available link to get a more reliable connection). ML/AI can also automatically detect IoT devices and their behavior and quarantine problematic devices.

Borderless SD-WAN also includes valuable flow analytics on application performance throughout the entire network. In these flows, companies can see each device using an application and that device's experience. It uses this data to automatically determine baselines. Essentially, it defines what is "normal" network performance for packet loss or application flow statistics. Baselines also need to consider time and network activity because network activity varies based on the normal business hours for different branch sites and remote users.

Borderless SD-WAN also includes a built-in flight tracker view that monitors every user and branch, over every minute. This seeks out service-level experience issues and flags service provider service-level agreement (SLA) violations. The flight tracker simplifies management with insights into traffic flows (including where the fault is occurring), flags policy violations, and performs anomaly detection.

Additionally, Borderless SD-WAN goes beyond actionable ML-based fault insights to actually troubleshoot devices behind a branch. For example, its auto-discovery features can identify the actual devices accessing applications from inside the branch or home. Remote IT can use the integrated IoT manager to remotely troubleshoot these devices, significantly reducing the mean time to resolution.

IN THIS CHAPTER

- Looking at the business benefits of Borderless SD-WAN
- Exploring the end user's benefits
- Checking out the benefits for networking experts
- Saving money with Borderless SD-WAN

Chapter 4
The Benefits of Borderless SD-WAN for Enterprises

Netskope Borderless SD-WAN offers a set of network capabilities that address the needs of the modern world. It's a software-defined wide-area network (SD-WAN) made to meet today's needs for mobility, flexibility, integrated security, and constant availability from anywhere, at any time, and on any device. Just as SD-WAN brought WAN into the one-to-many world, Borderless SD-WAN evolves the network into the many-to-many era.

The benefits of this transformation are not only available to network experts. They're tangible and experienced enterprise-wide every single day. If that doesn't make the networking geek in you happy, what will?

This chapter covers these daily benefits for all users, as well as some of the more advanced benefits for network experts tasked with maintaining technology and networking infrastructure. After reading this chapter, you'll understand that Borderless

SD-WAN is not just a networking capability; it also provides high-performance connectivity and seamlessly integrates security. This makes it an essential function for businesses, delivering the same experience to every user, no matter where they want to go.

A Unique One-Platform, One-Software, One-Policy Approach

Before proceeding, let's look at the broader philosophical change Borderless SD-WAN brings about for the business. This context helps shape the rest of the analysis in this chapter. There's an old adage from countless TV shows that says that every person needs a code, a personal philosophy to live by (this seems to be the case for every depiction of criminal gangs and noble clans of space aliens). The same is true for connectivity. Borderless SD-WAN's mantra is all about the Power of One (see Figure 4-1) and how this approach helps organizations streamline operations.

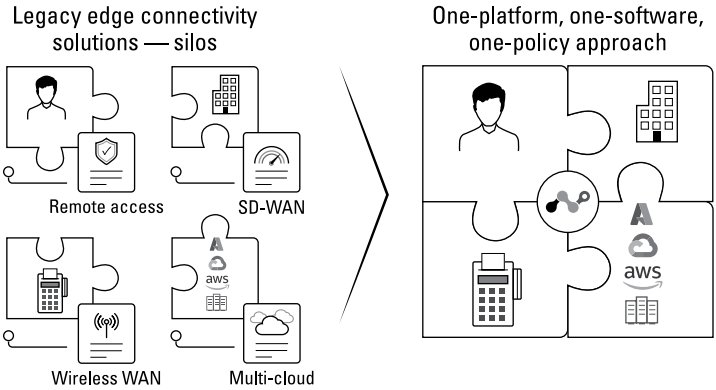

FIGURE 4-1: Power of One architecture can serve multiple use cases, seamlessly integrate networking with security, reduce costs, and simplify operations.

This Power of One manifests in a variety of ways:

- **It means creating a consistent user experience governed by policies that follow users regardless of their location.** This consistency is delivered by lightweight software that delivers the same set of SD-WAN capabilities everywhere, from a branch of any size to a laptop on the move. The same

software also enables wireless WAN capabilities, allows multi-cloud networking to facilitate application-to-application connectivity across multiple clouds, provides internet of things (IoT) intelligent access to unlock business value from a multitude of data sources, and remotely monitors and troubleshoots smart assets.

- **All Borderless SD-WAN solutions are managed through a single console.**
- **It encapsulates a single platform that seamlessly integrates networking with security, delivering secure optimized access and a unified experience that reduces costs and simplifies operations.**

One user experience delivered by one comprehensive platform that shares a common Zero Trust engine, digital experience management, and context between networking and security — this is how the Power of One ultimately delivers a true single-vendor secure access service edge (SASE) framework (more details coming in this chapter).

Sounds great, right? That's only the beginning. Let's start with the benefits to end users and then discuss the broader benefits of Borderless SD-WAN solutions to the network operations teams and the businesses.

Making Life Easier for End Users with Borderless SD-WAN

Borderless SD-WAN benefits every user, working from anywhere, whether they're an employee inside a branch, an analyst at home on their laptop trying to access corporate applications located across the globe, or a contact center agent who wants to provide an optimal service to a customer. It even extends to a field engineer on a rig in an oil field, working from a truck. The advantages of Borderless SD-WAN for everyday business users include the following:

- **Flexibility and choice:** Users can work from anywhere (whether a branch or a remote location, like their home, a cafe, an RV, or a hotel) and have the same SASE (SD-WAN and Security Service Edge [SSE]) capabilities everywhere.

- **Optimized connectivity:** Each user can enjoy high-performance access to multiple clouds and data centers. Performance and quality of service (QoS) glitches become a thing of the past. Even demanding applications like Zoom and Microsoft Teams perform well over spotty connections.
- **Business continuity:** Full-stack security protection delivered from a SASE gateway and a unified SASE client avoids any disruptions resulting from cyberattacks. Security follows the users on-premises in branches and at remote locations.
- **Zero Trust access:** The same context-aware Zero Trust access is available at any location, allowing users to stay compliant with corporate policies. The system ensures that policies follow the users and adapt to their context.
- **Easy resolution of problems:** Artificial intelligence (AI)–driven operations with machine learning (ML) insights enable information technology (IT) administrators to remotely diagnose end-user issues and reduce mean time to resolving support tickets and higher end-user productivity.

The user experience improves dramatically with Borderless SD-WAN. For mobile users, such as those in fleet trucks, the SASE gateway converges SD-WAN, switching, routing, Wi-Fi, and wireless with seamless integration with SSE, allowing secure, optimized access to any enterprise application, no matter where the users are.

Users working from remote locations enjoy improved productivity with reliable connectivity, even from iffy connections. Borderless SD-WAN provides this by constantly optimizing the user connection to any application, including more demanding time-sensitive voice/video applications like Zoom and RingCentral. For instance, while using these applications, if connections experience latency, jitter, and packet loss, Borderless SD-WAN remedies the situation so smoothly that the user doesn't even know there's a problem. That consistent, high-quality experience and secure connectivity occurs between the user and any cloud or data center, no matter which device the user is working on and from any location.

Additionally, users receive consistent security and network optimization policies with endpoint SD-WAN and SSE, all integrated as a part of a unified SASE client running on a user laptop, delivering the same branch experience to remote locations. Their access and productivity won't be constrained if they're

working in the office, at home, in an RV, or at the beach. They experience the same security and high-performance connectivity wherever they are (notice a theme?). The application experience is always the same.

The user now has greater flexibility and choice in how and where they work. They don't have to think about where they are and what device they're on — they can access applications and work the same way they would if they were physically in an office. That's a powerful capability! If you're working from a hotel room with an internet connection and you want to lead a Zoom meeting, your laptop can become the SD-WAN device that performs the last-mile optimization to deliver a great video experience automatically.

SSE Software-as-a-Service (SaaS) security posture management (SSPM) continuously monitors Zoom environments to discover and remediate any misconfigurations that weaken security to maintain compliance with industry benchmarks and regulatory frameworks.

The best part is that the user doesn't even know that optimization and security work is being performed — they just know their connection is stable, secure, and optimized. They achieve unprecedented reach with connectivity everywhere. Borderless SD-WAN is made for today's many-to-many world.

What Networking Experts Get from Borderless SD-WAN

Now let's turn to the more sophisticated and technical networking experts (that would be you!), who obtain eight main benefits with Borderless SD-WAN.

Boosting operational confidence with AIOps

Network architects and operations teams benefit from administrative capabilities that unify and future-proof network optimization, security, and visibility. One pane of glass (or, in other words, one console) defines the policies, monitors, and supports the resolution of problems for all locations, users, and devices on the network. The branch offices and users get the same

experience and are managed in the same way. The same branch office Borderless SD-WAN and SSE orchestration — including the context-aware Zero Trust policies enforced and managed by network teams today — can now be applied for individual users running the unified SASE client. The same support from a single pane of glass extends to multi-cloud networking, wireless WAN, and IoT intelligent access solutions.

With zero-touch provisioning, you can bring your entire network — including users, devices, sites, and cloud — online in minutes. Policies can be set for the entire network and then pushed out through all Borderless SD-WAN gateways and endpoints running the same SD-WAN and SSE capabilities. When it comes to monitoring and optimizing the network, AI and ML put smiles on the faces of network experts by detecting anomalies in bandwidth utilizations, enabling automated troubleshooting, providing proactive support, and offering insights into traffic flows and policies.

The results are tangible. Having a consolidated view of your key networking solutions under one console allows network operation teams to streamline all aspects of network monitoring, reporting, and management and to efficiently utilize their time by focusing on more strategic long-term projects that will add value to the company's overall growth.

Driving efficiency and agility with context-aware SD-WAN

Borderless SD-WAN provides complete visibility into data and apps that are part of a hybrid network, connecting every site, remote user, IoT device, and multi-cloud environment. This application visibility is crucial when supporting users who consume a variety of applications, including SaaS and various personal- and work-related cloud or on-premises applications. The evolving enterprise now needs Zero Trust–enabled, context-aware SD-WAN to provide fast, reliable, and secure access to any application and device at any location with full visibility and the right set of controls.

Borderless SD-WAN can classify traffic by application on all ports by default. The trick is to provide the best QoS for mission-critical applications and to avoid spending resources, bandwidth, and operations time on less important apps. Given

that there are tens of thousands of SaaS apps out there, network operations teams can't possibly configure QoS policies for every one of them. The Netskope SASE supports a database of more than 60,000 applications (as we discuss in Chapter 1 and elsewhere) categorized by a Cloud Confidence Index (CCI) that determines the enterprise-readiness score of the application. The CCI helps to automatically map the applications to the right level of QoS policies. We discuss this further in the context of SASE adoption in Chapter 5.

Netskope has a database of QoS policies that are assigned to apps based on the CCI and other criteria. This automatic mapping dramatically reduces manual labor for the network operations team, resulting in much more efficient operations.

Netskope's context-aware capabilities can extend to automatically detect all IoT devices, managed and unmanaged, and micro-segments to manage risks associated with a compromised device.

Increasing productivity and enhancing user experience with assured application performance

Borderless SD-WAN leads to higher productivity and better collaboration by providing highly reliable, optimized access to all applications, including any Unified-Communication-as-a-Service (UCaaS) capability. With little effort, network experts can deliver a better experience for users working from home, a branch office, or a non-office location such as a home, a hotel, or a coffee shop, with SD-WAN capabilities running in a branch office, in the cloud, and on user laptops. Borderless SD-WAN can improve network performance with a sub-second failover in multiple link scenarios or on-demand remediation, even over a single, unstable broadband internet connection.

Future-proofing your investment with a 100 percent SaaS-based controller

SD-WAN controllers were manually deployed on-premises by IT administrators. This do-it-yourself (DIY) approach is complex to roll out and scale. With Borderless SD-WAN 100 percent SaaS-based controllers that support advanced routing, such as Border Gateway Protocol (BGP) and Open Shortest Path First

(OSPF), organizations can quickly roll out new locations and connect remote sites. This cloud controller capability means network experts can easily scale from one to thousands of sites and hundreds of thousands of users and IoT assets, all with hassle-free configuration, management, and visibility across sites globally.

Networking experts can let their networks grow as large as necessary. They don't have to predict the capacity (measured in the number of sites supported in the SD-WAN network) in advance. A SASE gateway or client can be added any time a new branch or remote user must be brought online. Infinite scaling will be available because the controller runs as a SaaS service. The network can now expand on demand. Boom! Future-proof.

Expanding reach and flexibility with wireless WAN

The world of business extends far beyond the reach of traditional wired networking. But just because wireless connectivity is available, that doesn't mean that you'll get the connectivity, QoS, and security needed to run a modern business. With Borderless SD-WAN's cloud-managed wireless gateways, you can turn wireless connectivity into a rock-solid, secure, optimized network, whether you're setting up an ad hoc network at a remote site or temporary office or you're providing fast, reliable, and effortless wireless connectivity.

The Borderless SD-WAN wireless gateway can integrate into your existing infrastructure and be paired with any SD-WAN solution for primary or backup cellular support. This facilitates the rapid creation of network services, increasing productivity and business agility.

Transforming your business with cloud-delivered SASE

Traditional SD-WAN struggles to provide full visibility and optimized on-ramps from any user or site to any cloud, SaaS, or private applications. Even getting "creative" with a combination of DIY SD-WAN hub installations means that provider environments will be mired with latencies and not deliver high-performance connectivity. That's where the quality of the network infrastructure really counts.

Netskope NewEdge is the world's most well-connected security private cloud, covering 70+ regions and converging network and security services at scale. It provides globally distributed low-latency traffic on-ramps, is extensively peered, and has full compute in every region for traffic processing. It's backed by five nines of availability and delivers the industry's best service-level agreements (SLAs). The NewEdge network means that every user, branch, site, device, and multi-cloud environment around the globe will be close to converged Borderless SD-WAN with SSE services. Borderless WAN cloud hubs and SSE at globally distributed NewEdge infrastructure provides several levels of benefits:

- **Netskope Borderless SD-WAN in NewEdge expands SD-WAN fabric from on-premises locations to all SaaS and cloud resources.** For instance, by utilizing endpoint SD-WAN with a unified SASE client, Zoom traffic can be optimized for a user operating from a remote location, just as it would be for a user working at a corporate branch utilizing the Netskope SASE gateway. Another example is leveraging a middle-mile service connecting geographically dispersed branches to an application located at the headquarters in a different continent.
- **Through seamless integration with SSE, Borderless SD-WAN provides comprehensive protection against all cybersecurity threats and high-performance networking, ensuring uninterrupted business operations.**
- **Borderless SD-WAN can be leveraged to connect enterprise resources distributed across multiple cloud environments, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), into a unified network fabric.** Through advanced routing and native integration within cloud providers, Borderless SD-WAN enables the interconnection of different regions within these cloud providers and facilitates one-click integration with Netskope Intelligent SSE for cloud workloads.

By providing these capabilities, Borderless SD-WAN allows companies to accelerate their cloud adoption with both high-performance connectivity and the right security posture. Hosting some assets on-premises while others are in the cloud is no longer a worry. The journey to gradually migrate more infrastructure to

the cloud is fully supported without having to consider the limitations of the existing SD-WAN landscape. The limited support for multiple clouds by traditional SD-WAN often leads to massive logistical headaches — something we don't want networking experts to endure.

REMEMBER

With Borderless SD-WAN, companies are able to govern how each cloud talks and interacts with every other cloud, which is a great company cloud strategy.

Securing your enterprise with 360-degree SASE protection

Borderless SD-WAN provides a complete bouquet of integrated security capabilities. From a network perspective, Borderless SD-WAN provides hybrid network security at the edge by inserting services like a firewall and intrusion prevention system (IPS) for east–west segmentation. Through integration with Netskope Intelligent SSE, you get 360-degree protection with capabilities for secure web gateway (SWG), cloud access security broker (CASB), Zero Trust Network Access (ZTNA), data loss prevention (DLP), SSPM, cloud security posture management (CSPM), cloud firewall, and other security services.

Both the network and security services that comprise Netskope's SASE are built on NewEdge, a fast, reliable, and converged cloud-native platform that offers the broadest geographic coverage in the industry (70+ regions). This means single-digit millisecond latency for the vast majority of the world's knowledge workers. Businesses are protected from all types of cyberattacks and data exfiltration, preventing disruptions and protecting brand reputation. SASE gateways and clients automatically pick the most optimal SSE point of presence (PoP) for security and optimization. Networking experts are thrilled by the ability to deploy SSE with one click both for branch offices and remote users. The result is a new way forward for connectivity — built in the cloud — that delivers incredible business agility.

Unlocking the business value of the data with edge compute

Borderless SD-WAN natively supports edge compute capabilities and the ability to run out-of-the-box container services like

Azure IoT Edge runtime, digital experience management, and so on. IT admins can pick a service from a catalog or bring their own custom applications. With application life-cycle management (ALM) capabilities, businesses can roll out these services on a large scale and provision these applications on thousands of SASE gateway devices with a single click.

Reducing Overall IT Costs

In the meantime, the benefits provided by Borderless SD-WAN result in a consolidated networking footprint. A single, centralized solution replaces the multiple-vendor setup of SD-WAN with one product from one vendor. It should come as no surprise that fewer vendors equate to significantly reduced networking support costs. The cost to train operational staff on a multitude of point products can quickly exceed the organization's capital and operational expenditures for these products.

Borderless SD-WAN paves the way to eliminate siloed, nonintegrated solutions to reduce cost and achieve a higher return on investment. Borderless SD-WAN reduces complexity by replacing multiple products and consoles with a single lightweight software that addresses key customer needs. Networking experts gain new control with Borderless SD-WAN. (We're not saying we're control freaks, but okay, yeah, we are. It's sort of the job, right?) Borderless SD-WAN reduces the administrative burden by providing centralized cloud-native management for the entire network.

With Borderless SD-WAN, companies can save on capital expenditures (CapEx) and overall IT operations. With one console, one automation, and one software governing the entire network, enterprises spend less and increase their return on investment (ROI). For example, Netskope Borderless SD-WAN has delivered at least ten times total cost of ownership (TCO) savings for its customers that have built converged architecture with its technologies.

IN THIS CHAPTER

- Overcoming the security challenges of the software-defined wide-area network (SD-WAN)
- Using secure access service edge (SASE) to combine networking and security
- Navigating the SASE journey

Chapter 5
Accelerating SASE Adoption

Now we need to talk about how security integrates with the larger Netskope Borderless SD-WAN as part of a broader SASE architecture. The path to SASE was accelerated by enterprises looking for digital innovations to differentiate themselves. This created the need for new digital capabilities like cloud computing and the convergence of networking and security at the product, architectural, and organizational levels.

SASE combines concepts such as Zero Trust, SD-WAN, and Security Service Edge (SSE) to guide us to a security and networking posture that protects and governs the cloud and the new work-from-anywhere environment. To achieve SASE, both networking and security must be software-defined and cloud-delivered. Part of achieving SASE is the consolidation and integration of security capabilities — the very essence of SSE.

SSE relocates critical control and inspection points to the cloud(s) where your business runs. That shift places security adjacent to where data, applications, and people operate — and where the potential danger lies. SSE works well with Borderless SD-WAN because it's software-defined and its critical services are natively

delivered from the cloud. This optimizes connectivity for every user, device, site, application, and piece of the corporate infrastructure without slowing down the business.

So, coupling SD-WAN with SSE enables companies to achieve a SASE, which is needed to truly secure Borderless SD-WAN. In this chapter, we cover the problems of security in a traditional SD-WAN environment and how new technologies emerged to enable companies to have security in a cloud architecture.

The Problem of Security with SD-WAN in the Pre-SASE World

Borderless SD-WAN is focused on empowering the modern workforce to work anywhere on any device. Users must be able to access any application — which, in turn, may be located anywhere. To do so, users need confidence that no matter where they are, no matter what applications they access, their key enterprise capabilities are available to them with a consistent experience. But those users, devices, sites, and applications also need to be secured completely. Therefore, Borderless SD-WAN must be integrated with an appropriate security stack protecting every user, device, site, application, and piece of the corporate infrastructure.

To understand the challenges involved with seamlessly integrating security with Borderless SD-WAN, it helps first to have a picture in mind of where we were and where we are today with traditional SD-WAN and security.

With traditional SD-WAN, all connections originate from within the physical confines of a brick-and-mortar branch, to one or more Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), or Software-as-a-Service (SaaS) providers, and any Unified-Communication-as-a-Service (UCaaS) provider. All these connections are predicated on the needs of users and the applications they want to access. One of the main issues that emerged with traditional SD-WAN was maintaining security. Security became the proverbial Achilles heel for traditional SD-WAN. A point worth noting here: When it comes to applications, traditional SD-WAN is designed to detect, prioritize, and secure only a few thousand applications. This is very limiting in an age of application proliferation.

And this all worked well . . . until it didn't!

As the enterprise became borderless, the perimeter transformed and expanded beyond branches to include micro branches, users' remote locations, and internet of things (IoT) devices, across all multi-cloud edges. The common requirement here is that all these things need to be secured. Network architects started deploying multiple point products for security and connectivity to address these newly emerged edges or perimeters. This approach led to a network full of disparate and disjointed technologies that were forced to work together. The result often proved overly complicated from both an end-user and ITOps perspective. A fragmented architecture can't consistently apply security or quality of experience (QoE) policies across all users, devices, sites, and clouds. Further, tens of thousands of new applications now reside in the cloud, a model that traditional SD-WAN was not designed to support. As the saying goes, "You can't prioritize or secure what you can't detect." And traditional SD-WAN struggled with all the new applications it couldn't detect.

Plus, the lack of visibility and granular control of IoT poses risks to the enterprise. Traditional SD-WAN couldn't mitigate the impact of compromised devices. So, bringing additional context into the model with Zero Trust security became essential to delivering SD-WAN services that could meet today's enterprise needs at the edge and across the WAN.

To achieve comprehensive security adequate to prevent cyberattacks with SD-WAN, some organizations had to backhaul all the traffic to a centralized location like a data center. From there, they would connect to the internet and multiple clouds to consume IaaS, PaaS, and SaaS services. Although security was in place, the user experience was again compromised due to latency performance issues inherent in that backhauling. To avoid backhaul and resultant latency, some enterprises opted for distributed security at each site. Some went for bolting on separate security devices to the existing SD-WAN solutions. Although others employed complex services, chaining approaches within the same devices dubbed as "fat" SD-WAN solutions, they were all costly and complex to manage and scale. Some SD-WAN vendors with basic firewall capabilities started throwing around the term *good-enough security* at the branch level. But "good-enough" network security was no substitute for the best-in-breed security enterprise required.

To say converging network and security for every remote user, branch, IoT, and multi-cloud environment was the ultimate juggling act is a severe understatement. It was more like trying to clear a beach of sand by removing one grain at a time — a truly Sisyphean task. (We set a challenge for ourselves to try to fit as many metaphors as possible into two sentences, and we think we succeeded.)

Cloud-Delivered Security Paved the Way for SASE

The emergence and rapid gain in popularity of cloud-delivered security marked a shift in SD-WAN vendors' strategy. They started to partner with the cloud security providers in an effort to mitigate the risks posed by allowing direct internet access via the cloud. This was in contrast to the previous practice of routing the SD-WAN traffic through the company's data centers for security inspection, which created the network traffic "hairpin" that led to high latency or the distribution of a full security stack in every single branch.

Time has proven that cloud-delivered security is the right approach and it has paved the way for SASE. Enterprises are looking to unify their network and security architectures to simplify operations and to enable context sharing between SD-WAN and cloud-delivered security for more effective and granular controls.

SASE: Born to Unite Networking and Security

SASE and SSE are the way security moves to the cloud and becomes more effective than anything we've had before. SSE is how all the security services necessary for SASE — which were previously separate applications, products, or services, often from different vendors — come together in a unified, integrated form that provides greater capability, enhances efficiency, and reduces complexity and cost. SASE is an overall vision for transitioning networking and security capabilities to the cloud. SSE consolidates

all the required security capabilities, while Borderless SD-WAN consolidates all the required networking capabilities — and then SASE converges both networking and security.

SASE offers a set of integrated network and security services that become the primary inspection point for all traffic, ensuring consistent security for all users, data, devices, sites, and applications. SASE connects all your network and security "senses" to a single brain that connects, optimizes, interprets the data, comprehends the breadth of risks presented, and negotiates the right level of access at any given moment, in any scenario.

Netskope Intelligent SSE harnesses the full value of the cloud by integrating enterprise critical security capabilities like cloud access security broker (CASB), secure web gateway (SWG), Zero Trust Network Access (ZTNA), data loss prevention (DLP), cloud security posture management (CSPM), SaaS security posture management (SSPM), digital experience management (DEM), Firewall-as-a-Service (FWaaS), and so on, making sure that they work together. Using one-click integration and Netskope NewEdge, Borderless SD-WAN can help deliver these SSE services as near as possible to the point of access with people, data, and applications. In addition, NewEdge's globally distributed points of presence (PoPs) ensure the lowest possible latency for users to access any application from anywhere to deliver high performance and high-quality connectivity to accelerate SASE adoption. Netskope NewEdge also provides security with SSE and on-ramp to any cloud with Borderless SD-WAN, including optimizing business-critical UCaaS applications.

So, what about the enterprise edge, where the SASE gateway is located and where users and devices operate from? The SASE gateway, powered by Borderless SD-WAN software, natively offers advanced Layer 7 firewalling and an intrusion prevention system (IPS).

The following expands on the integrated, security capabilities of Netskope SASE:

- **Classification:** Identifies and labels sensitive information, ideally when it's created, but also through periodic scans of data stores.

- **CASB:** Serves as a security policy enforcement point placed between cloud service consumers and cloud service providers to enforce enterprise security policies as cloud-based resources are accessed.
- **SWG:** Controls access and defends against web threats only. Netskope's next-gen SWG addresses cloud-enabled threats and data risks for personal instances of managed applications, thousands of shadow information technology (IT) applications, and cloud services.
- **ZTNA:** Enforces the premise that no one is blindly trusted and allowed to access company assets until they've been validated as legitimate and authorized. Least-privilege access grants access only to resources that users require, nothing more.
- **Remote browser isolation (RBI):** Separates worker devices from the act of web browsing by hosting and running all browsing activity in a remote, cloud-based container. Such sandboxing protects data, devices, and networks from all kinds of threats originating from malicious websites.
- **FWaaS:** Provides security for all outbound ports and protocols for safe, direct-to-internet access via an agent on a managed device or via Generic Routing Encapsulation (GRE) and Internet Protocol Security (IPsec) for offices.
- **DLP:** DLP prevents intentional and accidental data exfiltration by intentional and unintentional misuse. Netskope DLP delivers accurate detection of all sensitive data in any form with the lowest degree of error possible.
- **Threat awareness and neutralization (also known as advanced threat protection [ATP]):** Identifies indications that an environment has been compromised and performs actions to reduce or eliminate the likelihood of future attacks.
- **CSPM:** Identify and correct misconfiguration issues between organizations and cloud service provider (CSP) IaaS cloud environments like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).
- **SSPM:** Evaluates the configuration of SaaS applications and eliminates misconfigurations that might allow exfiltration, impersonation, or other kinds of attacks.
- **On-premises security:** Security services can also be inserted on-premises. East–west traffic can also leverage on-premises next-generation firewall (NGFW), IPS/intrusion detection system (IDS), and so on with Borderless SD-WAN SASE gateway.

SASE Is a Journey: Navigating the Landscape

A robust SASE architecture that integrates Borderless SD-WAN can take many forms, depending on the needs of an individual business. By definition, successful SASE implies fewer vendors; simpler operations; reduced complexity; lower costs; and faster, smoother network performance with full-stack security. Such comprehensive improvement doesn't take place in a single stroke.

REMEMBER

SASE is a journey and not a rip-and-replace; vendor consolidation will, in most cases, occur over time.

Many companies already utilize cloud-delivered security from SSE providers, and they could select an SD-WAN that best integrates with their existing security solutions. On the other hand, if the organization already has a Borderless SD-WAN product, they could integrate that with their choice of cloud-delivered security solution. There is no right or wrong approach. What matters most are the organization's unique needs and what will work best for them to achieve their business goals.

The following sections describe the distinct advantages of a single-vendor SASE. We suggest keeping these in mind before starting on the journey and deciding on a path forward. Sometimes 1 + 1 can equal more than 2.

Zero Trust, context-aware SASE

In the cloud era, visibility alone isn't sufficient. Even with the highest-resolution picture, it's still possible to miss fine details if you don't know how and where to look, or what you're actually looking for. A rich context focused on users, devices, applications, and the associated risks is a necessary ingredient to enable the definition of granular SASE policies. Such a context is also crucial for implementing Zero Trust.

For both the networking and security capabilities of Netskope's SASE, the context comes from Netskope Cloud XD (Xtreme Definition) that runs the Zero Trust Engine. Netskope's SSE, as part of Netskope SASE architecture, shares the same Zero Trust Engine with Borderless SD-WAN. This enables context sharing between converged security and network services and includes granular

policies based on detecting applications and identifying application risks, detecting devices and identifying device risks, and detecting users and identifying user risks.

As an example, Netskope SSE and Borderless SD-WAN share a common application database engine that identifies more than 60,000 applications. Netskope rates every application with a Cloud Confidence Index (CCI), which provides an enterprise-readiness score of an application. With Netskope SSE, IT administrators can use CCI to identify and assess the risk associated with various cloud services and make informed decisions about allowing or blocking specific applications within their environment. This enables fine-grained control over the usage of cloud services, ensuring compliance with security and governance requirements. Borderless SD-WAN leverages contextual insights provided by the CCI to establish out-of-the-box QoE smart defaults for Netskope SASE gateway. This eliminates the intricate and time-intensive task of manually configuring QoE rules for tens of thousands of applications. By leveraging the CCI information, Borderless SD-WAN can dynamically allocate network resources like bandwidth and priority, ensuring optimal performance for essential applications (see Figure 5-1).

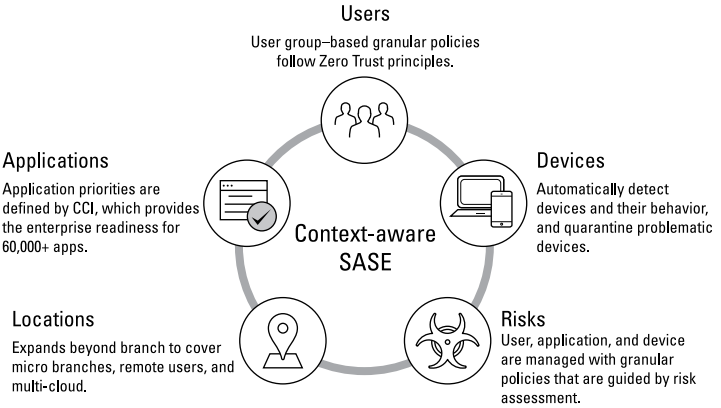

FIGURE 5-1: A rich context focused on users, devices, applications, and the associated risks is a necessary ingredient to enable the definition of granular SASE policies.

Unified policy and consistent experience at any location

In the current world that most companies live in, branches and remote users aren't handled in a unified manner. Traditional SD-WAN support for branch users lacks context awareness and Zero Trust security, while Netskope Borderless SD-WAN SASE gateway enables SD-WAN with granular Zero Trust context-aware policies. Virtual private networks (VPNs) typically used to support remote users lack visibility and optimization, while Netskope Endpoint SD-WAN addresses both of these needs. In this way, with Borderless SD-WAN and SSE integration capabilities, a modern enterprise can deliver high-performance, context-aware SD-WAN for both branch users and remote users (see Figure 5-2).

The result is a unified policy framework, one that delivers consistent experience and security that follows the users. Network architects and operations teams benefit from the Borderless SD-WAN's One Platform, One Console, and One Policy to configure and manage branch policies and can now be applied for individual users at remote locations. No matter where your users, apps, and services reside, from a single unified platform, enterprise IT departments can now manage branch offices and individual remote users using a uniform Zero Trust and network performance policy across the entire corporate infrastructure. This unified approach delivers scalable architecture, streamlined operations, high-performance connectivity, and steadfast security based on context-aware Zero Trust principles.

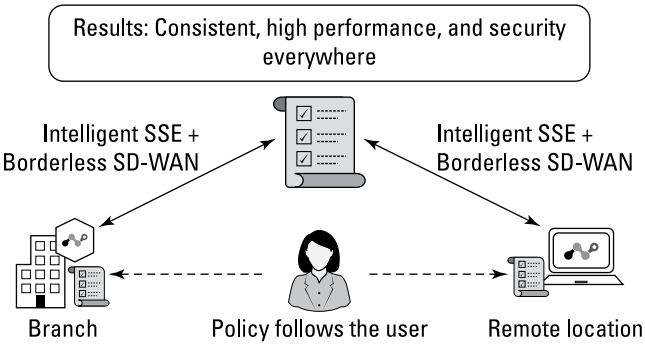

FIGURE 5-2: From a single unified platform, IT teams can now manage branch offices and individual remote users using a uniform security and network performance policy that follows the user.

Cloud-delivered SASE with unrivaled global reach

Historically, security and network engineers have always faced a familiar balancing act: more security versus better performance. The unwritten law of network security is that you can't have it all: There's always a trade-off among performance, availability, and security. Netskope's NewEdge platform breaks the rule and delivers on all three requirements without demanding trade-offs.

As we initially discuss in Chapter 3, Netskope NewEdge is today the preeminent private cloud for security, boasting an extensive global coverage across 70+ regions. It successfully combines network and security services on a large scale, offering low-latency traffic on-ramps that span the globe. With its extensive peering arrangements and comprehensive compute infrastructure in each region, NewEdge efficiently processes traffic. Additionally, it guarantees exceptional availability with a five nines uptime, and it upholds the industry's leading service-level agreements (SLAs) for optimal performance and reliability.

With the NewEdge network in place (see Figure 5-3), every user, branch, site, device, and multi-cloud environment across the globe can seamlessly access the integrated Borderless SD-WAN with SSE services. The SSE services available in NewEdge encompass a wide range of offerings, including next-generation secure web gateway (NG-SWG), CASB, ZTNA, SSPM, CSPM, FWaaS, and DLP. Netskope Borderless SD-WAN services in the NewEdge network effectively expands the reach of SD-WAN to encompass SaaS and cloud resources. It facilitates the optimization of cloud traffic for remote users and branch offices. It also offers a mid-mile service that delivers reliable connectivity between geographically distributed branches and centralized applications on a different continent.

This combination of NewEdge network, SSE services, and Borderless SD-WAN guarantees secure and high-performance connectivity for cloud, web, SaaS, and private applications. It empowers organizations with a robust infrastructure that enables high performance and protected access to critical resources across various environments.

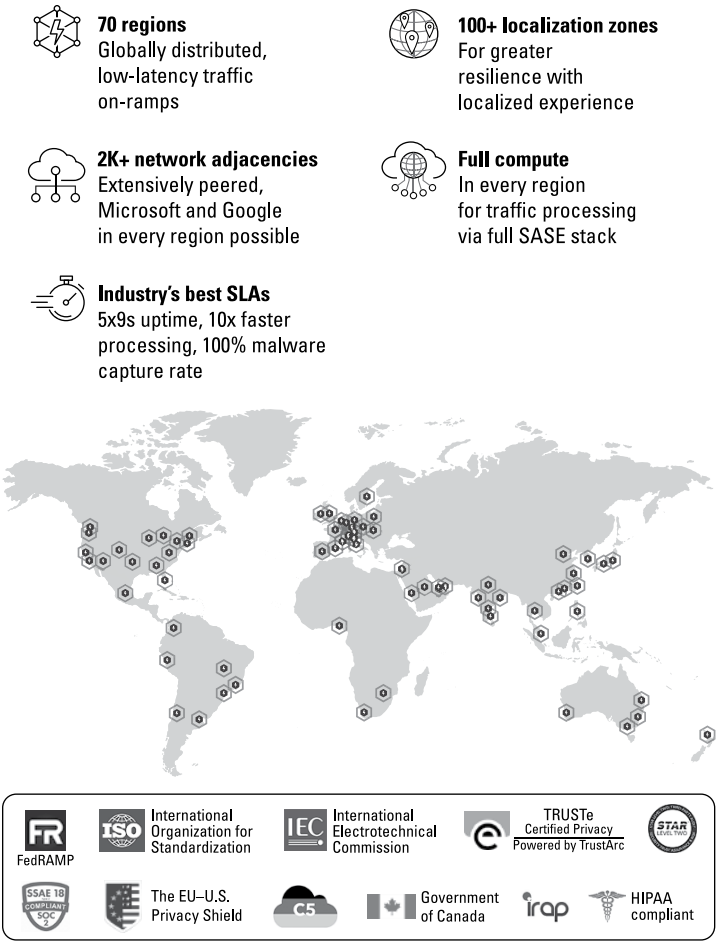

FIGURE 5-3: NewEdge combines network and security services at scale, offering low-latency traffic on-ramps that span the globe.

Unify and simplify ITOps

Users, devices, sites, and clouds demand high performance and secure any-to-any connections. Existing approaches result in multiple, disparate point products increasing cost and complexity. With its highly integrated approach to security and networking services, SASE brings important cost-efficiency advantages.

From the networking perspective, a single lightweight Borderless SD-WAN software can help eliminate multiple point products (for example, branch SD-WAN, remote access VPN, wireless gateways, multi-cloud edge, and so on), thereby reducing complexity (see Figure 5-4). The SSE integrates multiple security capabilities in a single whole, further eliminating the needs of various products that don't share threat intelligence with one another and weaken the security posture. Plus, as discussed earlier, Borderless SD-WAN and SSE seamlessly integrate with each other and share the same Zero Trust Engine. Vendor consolidation SASE results in fewer systems to monitor and maintain, as well as improved network designs, which reduces operating expenses. And by leveraging artificial intelligence (AI)–driven operations and automating much of the detection and response activity, you reduce the number of support tickets and significantly decrease mean time to resolving issues.

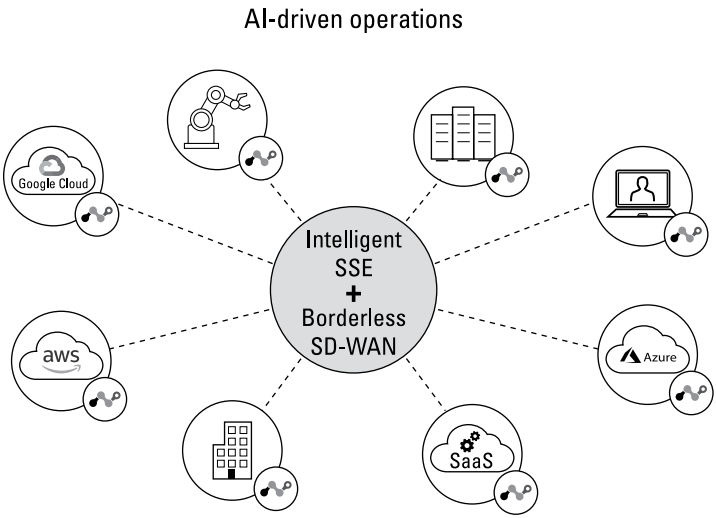

FIGURE 5-4: SASE consolidates multiple vendors, results in fewer systems to monitor, simplifies network designs, and realizes cost-efficiency advantages.

IN THIS CHAPTER

- Empowering your business with diverse network architectures
- Using a solution built for the cloud
- Securing and optimizing connectivity
- Exploring intelligent network access and advanced routing
- Finding out about comprehensive hybrid network security
- Delivering a first-class application experience anywhere
- Gaining greater context awareness
- Harnessing the power of artificial intelligence (AI)–driven operations
- Implementing a wireless-first strategy
- Achieving flexibility and efficiency with container orchestration

Chapter 6
Top Ten Capabilities Needed for Enterprise Adoption of Borderless SD-WAN

If you've made it this far, you're probably seriously considering adopting Netskope Borderless SD-WAN — either now or in the near future. And you're also likely wondering — given all the ways we've shown that Borderless SD-WAN surpasses traditional

software-defined wide-area network (SD-WAN) — what the differentiated capabilities are that you should look for in a Borderless SD-WAN solution to ensure it's right for your business.

In Chapter 5, we show how a single-vendor secure access service edge (SASE) solution simplifies the journey and delivers secure, reliable, optimized connectivity for every site, cloud, remote user, or internet of things (IoT) device. This allows everyone in a company to enjoy the benefits of a truly converged SASE platform that simplifies operations, applies uniform security, preserves network performance, and ensures SASE success.

Those who adopt Netskope's single-vendor SASE solution can help simplify their architecture with the Power of One (see Chapter 4) — namely, one platform, one lightweight software, and one policy to control all networking and security. To help summarize the benefits of Borderless SD-WAN, we present ten capabilities that can help jump-start an organization's journey toward Borderless SD-WAN adoption.


TIP

In case you're someone who reads books out of order (it's tempting to know the ending right away, isn't it?) and this is the first chapter you're reading, keep in mind that these capabilities provide the right framework to implement the Borderless SD-WAN solutions that are highlighted throughout the book. These are the *top* ten capabilities, but not the *only* capabilities; the list of what Borderless SD-WAN can do is far longer and highly adaptable to the needs of individual businesses. Use this list as context for the larger decisions you have to make when adopting a solution.

Empower Your Business with SASE Convergence

There's no wrong way to construct your Borderless SD-WAN and security architecture. What matters is that it fits the needs of your individual business — helping you to deliver the desired technical and business goals your organization is trying to achieve. By adopting a unified approach through Borderless SD-WAN and Netskope Intelligent Security Service Edge (SSE), organizations can eliminate the need for multiple point products and achieve operational efficiency. This convergence of connectivity and

security addresses various use cases, including multi-cloud environments, branches of any size, remote users, and IoT. Through a single lightweight software solution, Borderless SD-WAN seamlessly integrates with Netskope Intelligent SSE, resulting in a highly secure, optimized, and high-performing network for every remote user, device, site, and cloud. This integrated approach simplifies management and reduces complexity, allowing organizations to streamline their operations effectively.

Gain the Full Power of the Cloud with a Cloud-First Solution

To effectively implement high-performance SASE services, it's crucial to adopt a cloud-first approach for both SD-WAN and SSE services. This ensures flexibility and scalability.

Borderless SD-WAN with cloud-hosted management simplifies operations through centralized control and enables the rapid connectivity of users, devices, sites, and cloud resources, often within minutes. With comprehensive visibility and AI/machine learning (ML) insights across the network (see Chapter 4), issues can be quickly identified, reducing support tickets and minimizing the time to resolve problems. This ultimately helps maintain productivity for customers.

Borderless SD-WAN also employs a distinct separation of the data plane and control plane, allowing for scalability and resilience. The control plane, which can interoperate with routing protocols like Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF), is delivered as Software-as-a-Service (SaaS), eliminating the complexities associated with do-it-yourself (DIY) on-premises controller installations, thus simplifying management and reducing complexity. We discuss this further in Chapter 3.

By establishing a secure overlay that is agnostic to carriers and transports, Borderless SD-WAN creates a context-aware fabric connecting remote users, IoT devices, branch/data center sites, and multi-cloud environments. Additionally, Borderless SD-WAN and SSE services are hosted on Netskope NewEdge with geographically distributed points of presence (PoPs). This close proximity to

users and applications results in secure and optimized on-ramps to public and private clouds, including optimizations for demanding applications such as Zoom and Microsoft 365.

Cloud On-Ramp: Secure and Optimized Connectivity for Any-to-Any

Borderless SD-WAN ensures complete visibility and an optimized on-ramp for any user or site, enabling seamless connectivity to various cloud, SaaS, and private applications.

Through highly distributed cloud hubs within Netskope NewEdge, Borderless SD-WAN extends an organization's SD-WAN fabric from on-premises locations (such as branch offices, regional sites, campuses, data centers, remote locations, and mobile offices) and brings it as close as possible to SaaS and cloud services to optimize performance.

For instance, whether a user is accessing Zoom from a remote location with an endpoint SD-WAN or from a corporate branch using Netskope SASE gateway, the traffic will be optimized to ensure a high-quality user experience. Similarly, Borderless SD-WAN in NewEdge provides a highly optimized, low-latency middle-mile service that connects geographically dispersed branches to applications located in headquarters situated on different continents.

The tight integration of Borderless SD-WAN with SSE — as part of a complete SASE framework — ensures comprehensive protection against cyber threats, mitigating the risk of business interruptions.

In addition to providing SD-WAN capabilities for branches and remote users, Borderless SD-WAN can also connect enterprise resources scattered across multiple cloud environments, including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), into a unified network fabric. Leveraging advanced routing and native integration within cloud providers, Borderless SD-WAN seamlessly establishes connections between different regions within these cloud platforms. Moreover, it enables effortless integration with Netskope Intelligent SSE for cloud workloads through a single click.

Intelligent Network Access and Advanced Routing

Flexibility should be a key consideration for companies when selecting a product. Netskope Borderless SD-WAN offers a high level of flexibility by seamlessly integrating with Netskope Intelligent SSE through one-click intelligent access. This integration enables the seamless integration of Borderless SD-WAN with various security services such as secure web gateway (SWG), cloud access security broker (CASB), Zero Trust Network Access (ZTNA), data loss prevention (DLP), SaaS security posture management (SSPM), cloud security posture management (CSPM), Firewall-as-a-Service (FWaaS), and more, providing comprehensive protection against cyberattacks.

The security integration is available both at the branch level, through the SASE gateway, and at any remote location through a lightweight unified SASE client software running on users' laptops and for multi-cloud environments. This ensures that consistent and robust security measures are in place regardless of the location or device being used. Borderless SD-WAN's support for advanced routing protocols like OSPF and BGP also allows for smooth integration with existing enterprise infrastructure. Additionally, both control plane/data plane separation and cloud-scale key distribution ensures simplicity and scalability of the control plane, which can be efficiently delivered from the cloud.

Comprehensive Hybrid Network Security

Here's the deal: Adopting SD-WAN without built-in security can lead to a whole lot of complexity. Companies end up juggling two separate solutions, which can be a logistical nightmare. Not only does this create headaches in terms of management, but it can also compromise the effectiveness of both the security and SD-WAN components.

But fear not! Borderless SD-WAN takes a hybrid network security approach to security by integrating security on-premises and in the cloud. It has essential security services like next-generation firewall (NGFW) and an intrusion prevention system/intrusion detection

system (IPS/IDS) directly within its SASE gateway. This means that your east–west traffic gets protection right where it needs it.

But that's not all! Borderless SD-WAN goes above and beyond by providing comprehensive 360-degree protection through advanced security services delivered from the cloud. Think next-generation SWG (NG-SWG), CASB, ZTNA, SSPM, CSPM, FWaaS, and more. It's like having a security fortress surrounding your network, defending it from all angles.

Deliver a First-Class Application Experience Anywhere to Any Application

Companies should always prioritize delivering a consistent, reliable, and high-performance application experience to their users. This is precisely why adopting Borderless SD-WAN becomes crucial. It allows companies to rethink their networking, security, and optimization strategies to achieve this goal.

Borderless SD-WAN brings a range of capabilities such as dynamic path selection, sub-second failover, granular context-aware adaptive quality of experience (QoE), link remediation, and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) optimization. These functions work together to ensure optimal performance and user experience. It's important for companies not to compromise on these capabilities. By embracing Borderless SD-WAN, companies can transform their approach to networking and optimize it for delivering an exceptional application experience.

Context Awareness of User Identity, Device, and Application Risks for Better Controls

Borderless SD-WAN is designed to be context aware, providing real-time validation of user identity, device information, and application risks. This context awareness enables the

establishment of a true Zero Trust framework within the network. Borderless SD-WAN further stands out because of its ability to simplify the configuration of quality of service (QoS) policies. Traditional SD-WAN solutions would detect only a few thousand applications, and information technology (IT) administrators would need to individually configure QoS policies for those applications, which can be a time-consuming task.

The Netskope Zero Trust Engine can today detect more than 60,000 applications, assigning a Cloud Confidence Index (CCI) rating to each (see Chapter 2). This CCI rating serves as an enterprise-readiness score, indicating how well suited an application is for enterprise use. With Borderless SD-WAN, Netskope leverages these CCI ratings to provide intelligent QoS defaults right out of the box. This means that the network operations team no longer needs to manually configure QoS policies for each application, saving valuable time and effort.

Netskope's context-aware capabilities go beyond just user and application identification. They extend to automatically detecting all IoT devices, whether they're managed or unmanaged, which means Netskope can identify and manage the risks associated with compromised IoT devices. With this level of context-awareness, Netskope can effectively micro-segment the network based on AI/ML, isolating and controlling the access and behavior of IoT devices. This helps mitigate the potential impact of a compromised device, reducing the risk of unauthorized access or data breaches.

Simplified, Automated, AI-Driven Operations

Picture this: The Borderless SD-WAN solution is your trusty sidekick, always there to lend a helping hand. It's like having a personal assistant that takes care of all the nitty-gritty tasks, so you can focus on what really matters. By automating processes and leveraging AI-driven operations, this solution brings a whole new level of simplicity to your management tasks. Whether it's onboarding customers, setting up SASE gateways, managing endpoint SD-WAN, or dealing with multi-cloud environments, you can do it all easily from a centralized management platform.

But that's not all. The power of ML comes into play, making this Borderless SD-WAN solution truly extraordinary. It learns from your network, analyzes traffic flows, and understands your policies, which means it can proactively identify and address issues before they even become problems. It's like having a team of experts working around the clock to keep everything running smoothly.

Oh, and did we mention the time-saving benefits? With autonomous monitoring, anomalies are detected in a flash, and you can predict potential service provider service-level agreement (SLA) violations before they happen. You can resolve issues faster, minimizing downtime, and get back to business in no time.

Support for a Wireless-First Strategy

A comprehensive Borderless SD-WAN solution has your back when it comes to connectivity, offering a transport-independent design that adapts to your needs. It provides the flexibility to add 4G/5G connectivity options, ensuring reliable and effortless connectivity from anywhere. One of the great things about this solution is its ability to optimize cellular signal strength. So, even if you find yourself in a remote field office or setting up a temporary workspace without wired broadband access, you can still count on a solid and reliable connection. It's perfect for situations where a wired broadband connection may not be available, ideal, or even possible.

What's more, this Borderless SD-WAN solution is designed with global carrier interoperability in mind. It plays well with different carriers around the world, allowing you to choose the one that suits your needs or works best in your location. Whether you're dealing with micro branches, midsize offices, or large corporate environments, this solution has the flexibility and scalability to support your connectivity requirements.

Full Support of Edge Compute

Borderless SD-WAN is all about being flexible and efficient. That's why container orchestration is a game changer. It lets you easily manage and deploy new services at the gateway without the hassle of maintaining a bunch of servers at every branch. Imagine having a digital experience management container on your SASE gateway — real-time monitoring of user experiences becomes a breeze! It can also let you dig into IoT data like a pro. It supports multi-cloud environments like AWS IoT Greengrass and Azure IoT Hub, so you can discover and analyze all that juicy IoT goodness right at the edge. Talk about being on the cutting edge!

Figure 6-1 shows the ten capabilities covered in this chapter.

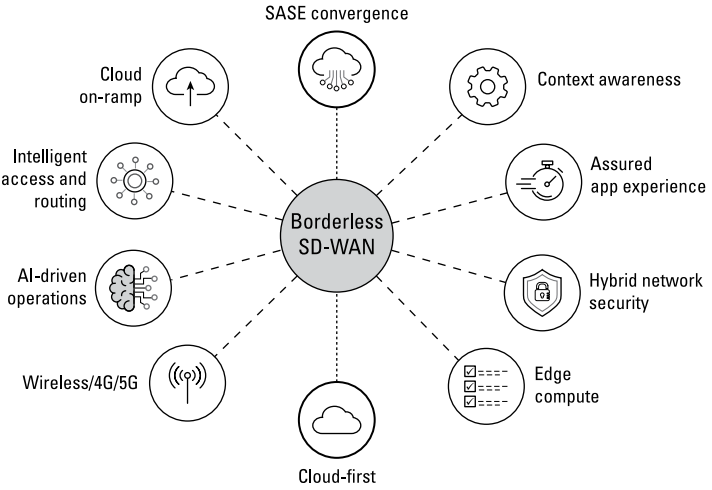

FIGURE 6-1: Ten capabilities that can help jump-start an organization's journey toward borderless SD-WAN adoption.

Ready for Anything

Netskope, a global SASE leader, helps organizations integrate networking and security seamlessly, leverage AIOps, apply zero trust principles and AI/ML innovations to secure data with high performance connectivity and comprehensive threat protection. Fast and easy to use, the Netskope platform provides optimized access and real-time security for people, devices, and data anywhere they go. Netskope helps customers reduce risk, accelerate performance, and get unrivaled visibility into any cloud, web, and private application activity. Thousands of customers trust Netskope and its powerful NewEdge network to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements. To learn how Netskope helps customers be ready for anything on their SASE journey, **visit netskope.com**.

netskope

Meet the demands of the borderless enterprise with Borderless SD-WAN

The enterprise's networking perimeter has expanded with the growth of micro branches, multi-cloud, remote work, telehealth, mobile fleet, and the internet of things (IoT). Today, users, devices, sites, and clouds are dispersed yet connected in numerous ways. Enter Borderless SD-WAN with new capabilities that offer secure, reliable, and fast connectivity — built on Zero Trust principles — scalable, AI-driven operations; assured application experience and security for 60,000+ apps; expanded support for 4G/5G wireless; and more.

Inside...

- Achieve fast and reliable connectivity
- Integrate networking and security seamlessly and accelerate SASE
- Find six solutions and ten capabilities for borderless enterprise
- Reduce IT costs and manage budgets
- Simplify architectures and run efficient operations

Netskope leaders **Parag Thakore** and **Muhammad Abid** are acknowledged experts with multiple patents in cloud computing, cybersecurity, and networking. Drawing from decades of experience across global organizations like Cisco, VeloCloud/VMWare, Infiot, Fortinet and T-systems, they've been pivotal in redefining Enterprise WAN and driving adoption of SD-WAN and SASE.

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

ISBN: 978-1-394-19893-1
Not For Resale

for dummies®
A Wiley Brand

Modern SD-WAN for SASE

for dummies®
A Wiley Brand

Modern SD-WAN for SASE

Netskope Special Edition

by Muhammad Abid and Parag Thakore

for dummies®
A Wiley Brand

Modern SD-WAN for SASE For Dummies®, Netskope Special Edition

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

ISBN 978-1-394-19893-1 (pbk); ISBN 978-1-394-19894-8 (ebk)

Publisher's Acknowledgments

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

Editor: Elizabeth Kuball
Acquisitions Editor: Traci Martin
Editorial Manager: Rev Mengle
Client Account Manager: Jeremith Coward
Production Editor: Saikarthick Kumarasamy
Special Help: Nicole Sholly

WILEY END USER LICENSE AGREEMENT

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