LEARNING MADE EASY

Cato Networks Special Edition

Secure Access Service Edge (SASE)

for dummies®
A Wiley Brand

Converged SD-WAN and network security

Support all edges: physical, mobile, cloud

Cloud-native and global architecture

Brought to you by

CATO NETWORKS

Lawrence C. Miller
Eyal Webber-Zvik

About Cato Networks

Cato is the world's first SASE platform, converging SD-WAN and network security into a global, cloud-native service. Cato optimizes and secures application access for all users and locations. Using Cato, customers easily migrate from MPLS to SD-WAN, optimize connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud datacenters and mobile users into the network with a zero-trust architecture. With Cato, the network and your business are ready for whatever's next.

https://www.catonetworks.com

Secure Access Service Edge (SASE)

Cato Networks Special Edition

by Lawrence C. Miller and Eyal Webber-Zvik

for dummies®
A Wiley Brand

Secure Access Service Edge (SASE) For Dummies®, Cato Networks Special Edition

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

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

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

ISBN 978-1-119-72154-3 (pbk); ISBN 978-1-119-72155-0 (ebk)

Manufactured in the United States of America and Great Britain

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. For details on how to create a custom *For Dummies* book for your business or organization, contact info@dummies.biz or visit www.wiley.com/go/custompub. For details on licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

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

Project Editor: Martin V. Minner

Executive Editor: Steve Hayes

Editorial Manager: Rev Mengle

Business Development Representative: Molly Daugherty

Production Editor: Umar Saleem

Table of Contents

Introduction

Secure Access Service Edge (SASE) is a new enterprise infrastructure technology category introduced by Gartner in 2019. SASE converges the functions of networking and network security point solutions into a unified, global, cloud-native service. It is an architectural transformation of enterprise networking and security that enables IT to provide a holistic, agile, and adaptable service to the digital business. What makes SASE unique is its transformational impact across multiple IT domains.

Solving emerging business challenges with point solutions leads to technical silos that are complex and costly to own and manage. Complexity slows down IT and its response to these business needs. SASE changes this paradigm through a new networking and security platform that is identity-driven, cloud-native, globally distributed, and securely connects all edges to the wide-area network: datacenters, offices, cloud resources, mobile and remote users, and Internet of Things (IoT) devices.

With SASE, enterprises can reduce the time to develop new products, deliver them to the market, and respond to changes in business conditions or the competitive landscape.

About This Book

Secure Access Service Edge For Dummies, Cato Networks Special Edition, consists of five chapters that explore:

- Modern business trends and challenges and what it takes to become a digital business today (Chapter 1)
- Bringing networking and security together in a SASE solution (Chapter 2)
- The core capabilities of SASE (Chapter 3)
- Real-world industry use cases for SASE (Chapter 4)
- Key evaluation criteria to consider when selecting a SASE vendor (Chapter 5)

Each chapter is written to stand on its own, so if you see a topic that piques your interest, feel free to jump ahead to that chapter. You can read this book in any order that suits you (though I don't recommend upside down or backward).

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but I assume a few things nonetheless.

Mainly, I assume that you know a few things about cloud, networking, and security. Perhaps you're an IT, network, or security architect, or a CIO, CISO, or IT director. As such, this book is written primarily for technical readers who are evaluating solutions to address modern networking and security challenges in their enterprise networks.

If any of these assumptions describe you, then this is the book for you. If none of these assumptions describe you, keep reading anyway! It's a great book and you'll learn quite a bit about modern enterprise networking and security.

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:

REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays.

TECHNICAL STUFF

If you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon and is the stuff nerds are made of.

TIP

Tips are appreciated, never expected — and I sure hope you'll appreciate these useful nuggets of information.

IN THIS CHAPTER

- Understanding key technology trends and business drivers
- Looking at the evolution of networking and security architectures
- Recognizing modern network and security challenges
- Identifying the needs of the digital business

Chapter 1 Modern Business Trends and Challenges

In this chapter, you explore modern business and technology trends, how networking and security architectures have evolved, the limitations of these architectures in today's digital business world, and what it takes to become a digital business today.

Looking at What Drives Businesses Today

Several important trends over the past decade have reshaped enterprise networking and security requirements. This section explores several of these trends.

Digital transformation

Businesses everywhere are undertaking digital transformation initiatives to revolutionize the way they do business and reinvent their industries. Technology innovations have enabled many core business processes to be automated and optimized, enabling greater efficiency, quality, and overall productivity.

Cloud and mobility

Cloud and mobile computing are two of the most important trends of the past decade. The rapid growth of software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) public cloud offerings has enabled businesses to rapidly scale their operations to support growth and demand, leverage agility and flexibility in service offerings to accelerate time-to-market, and reduce capital expenditures (CapEx) by taking advantage of consumption-based, pay-as-you-go pricing.

Likewise, the proliferation of mobile devices and high-performance cellular networks, including 4G Long-Term Evolution (LTE) and 5G, enables individuals to work from practically anywhere on ever more powerful mobile devices.

Globalization

Globalization has been a business trend for many decades, but the Internet has accelerated this trend, enabling businesses of practically any size to compete in the global economy. But although the Internet has been a globalization enabler, it exposes new challenges and risks, due to the lack of secure, reliable, high-speed Internet connectivity in many regions of the world where businesses are seeking growth and expansion.

Globalization also enables organizations to diversify their workforce, selecting the best talent from practically anywhere in the world. Cloud and mobile computing have contributed to this opportunity by increasingly enabling employees to work from anywhere. The COVID-19 global pandemic has driven many organizations to rethink their policies regarding work-from-home, as they recognize not only the health and safety aspects of these arrangements, but also the productivity benefits. The next challenge for these organizations will be to ensure reliable and predictable secure network connectivity and data protection for their employees, regardless of where they work and the devices they use.

Risk and compliance

Businesses today face greater risk, not only because of increasingly sophisticated threats and large-scale attacks, but also due to an increasingly complex regulatory landscape. In addition to security requirements such as the U.S. Sarbanes-Oxley (SOX) Act, U.S. Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry (PCI) Data Security Standards (DSS), organizations in every industry must now also comply with stringent privacy regulations such as the European Union General Data Protection Regulation (GDPR), Australian Privacy Principles (APP), and California Consumer Privacy Act (CCPA).

Tracing the Evolution of Network and Security Architectures

When organizations began connecting their local area networks (LANs) across multiple locations in the 1980s, they used dedicated point-to-point (P2P) leased lines, then Frame Relay, to build their wide-area networks (WANs).

In the 2000s, multiprotocol label switching (MPLS) connections enabled carriers to replace Frame Relay, providing an IP-based solution to converge voice, video, and data on the same network. MPLS provides dependable network connections backed by service-level agreements (SLAs), but it is expensive and can take months to plan and provision.

In 2013, software-defined wide-area networks (SD-WAN) emerged as a viable and cost-effective alternative to MPLS — making it the logical next evolution in WAN architecture. By abstracting the network layer and routing traffic based upon centrally defined and managed policies, SD-WAN optimizes the routing and prioritization of application traffic.

At the same time, security teams have had to adapt to increasingly diverse and sophisticated threats and attack prevention. Initially, network firewalls were deployed at the perimeter between the “trusted” corporate network and the “untrusted” Internet. Organizations traditionally maintained the entire security stack in their headquarters or data center and backhauled all branch network traffic through this central location. Alternatively, they might deploy a partial security stack with reduced functionality in their branch locations to offload some of the network congestion. However, both options required a compromise between security and performance and neither option was optimal for serving the needs of the organization and its branch locations.

As applications increasingly started sharing the same ports and protocols — often to promote ease of installation and use by effectively circumventing traditional network firewalls — the need for application-aware next-generation firewalls emerged. Internet and SaaS traffic from branch locations also increased, as well as the scale and sophistication of cyberattacks and attack vectors. This situation led to more siloed point security solutions — such as secure web gateways (SWGs), intrusion detection systems and intrusion prevention systems (IPS), anti-malware, and others — being deployed in branch locations where specialized security and technical skills were generally not available.

REMEMBER

This evolution of network and security architectures has created new challenges for businesses that have embraced digital transformation, cloud, and mobile computing trends while struggling to compete in a global market and address greater risk and compliance requirements.

Understanding Current Network and Security Limitations

Networking and security teams have traditionally addressed emerging business needs with point solutions. For example, adding SD-WAN appliances to offload capacity-constrained and expensive MPLS connections to Internet links, or adding firewalls in branch offices to secure direct Internet access. 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, in a cost-effective way, to all business resources globally. This is an architectural challenge, not a functional problem, that requires the elimination of IT silos, as well as the use of point solution "band-aids" to address new business requirements.

Specific challenges and limitations associated with current network and security architectures include:

- **Location- and perimeter-based designs:** Network architectures have traditionally been designed with logical (IP-based) topologies overlaying a physical network, datacenter, servers, and applications. Similarly, security appliances, such as firewalls, are commonly deployed at the network perimeter between the "trusted" corporate network and the "untrusted" Internet. However, these location- and perimeter-based designs do not adapt easily to the dynamic nature of cloud computing and virtual resources. Applications and their associated microservices move dynamically across virtual machines and containers and between public and private clouds. The concept of perimeter-based security is still relevant, but with network traffic now flowing to multiple datacenters, public clouds (including SaaS, PaaS, and IaaS environments), and the Internet, there are now multiple perimeters that are more difficult to protect than a single perimeter.

- **Complexity in multiple network and security point solutions maintained by limited staff and requiring highly specialized skills:** Network and security engineers are highly skilled (and expensive) resources — and there is a growing worldwide shortage of qualified individuals to fill available positions in the workforce. Complexity in network designs and lack of interoperability between multiple disparate networking point products and technologies — such as SD-WAN, MPLS, private backbones, WAN optimizers, and VPNs — as well as siloed security technologies — such as next-generation firewalls, secure web gateways (SWGs), web application firewalls (WAFs), intrusion prevention systems (IPSs), software-defined perimeters (SDPs), cloud access security brokers (CASBs), content filtering, security information and event management (SIEM), and more — makes it still more challenging for network and security staff to learn different systems and technologies, and creates greater risk of outages and security vulnerabilities due to misconfiguration and improper or sub-optimal operation and troubleshooting.
- **Legacy technologies don’t adapt to modern needs:** Inefficient workarounds — such as backhauling branch office Internet and cloud traffic across MPLS connections and “tromboning” (that is, looping back) network traffic to force it through a perimeter firewall or other security device — create complexity and latency in network and security architectures.

Becoming a Digital Business

The digital business is all about speed: faster product development, faster time to market, and faster responsiveness to changing market conditions. Technology enables business agility.

Automation, agility, elasticity, and flexibility are key traits of the modern IT infrastructure, which is increasingly delivered in the cloud.

But unlike cloud computing, networking and security are painfully incompatible with the cloud-centric and mobile-first business of today. The network is rigid and static. Security is heavily fragmented across multiple domains of physical locations, cloud resources, and mobile users. Together, networking and security are slowing down the business as silos erected decades ago are stretched and patched to accommodate emerging business requirements.

Many telcos now offer to take care of all the complexity in networking and security for enterprise IT teams with a managed services "bundle." However, these services are built around their MPLS services and delivered in much the same manner as other telco services — which aren't known for their speed, agility, and customer experience. Being a digital business means being a cloud-first, fast, and agile business — which is incompatible with legacy telco carrier WAN architectures and network services. Legacy MPLS networks no longer work for the digital business because:

- MPLS is expensive, rigid, and not built for cloud access
- Direct and secure Internet access is needed everywhere while MPLS networks centralize Internet access and backhauls traffic to centralized Internet access points
- MPLS is limited to physical locations, making cloud and mobile resources second-class citizens
- MPLS networks require separate appliances and solutions, complicating network management and life cycle maintenance

Legacy telco carriers are the wrong partners for digital businesses because they are expensive, bureaucratic (it can take months to deploy new sites), slow (they rely on ticket-based service requests), and they provide limited customer visibility and control.

TIP

IT architecture must evolve beyond silos and point solutions to support the digital business today and in the future. This is the main driver for the Secure Access Service Edge (SASE).

IN THIS CHAPTER

- » Learning what SASE is — and isn't
- » Recognizing the benefits of cloud-native networking and security

Chapter 2
The Emergence of Convergence: SASE

In this chapter, you discover how SASE brings core networking and security capabilities together in a complete solution, and the benefits of leveraging a cloud-native networking and security architecture.

Defining SASE — Not New, Just Better Together

To address the needs of the digital business and secure the new enterprise multi-perimeter (discussed in Chapter 1), Gartner has defined a new architecture: Secure Access Service Edge (SASE). SASE converges the functions of network and security point solutions into a unified, global cloud service.

SASE architecture is built for full visibility to all traffic from all edges — physical, cloud, and mobile — including traffic between the edges (WAN), and from the edges to the Internet. SASE applies a rich set of security and networking engines on traffic, enabling full inspection for threat prevention and access control.

The key components of a SASE architecture (see Figure 2-1) include:

- **SASE cloud:** A globally distributed cloud service that delivers the networking and security capabilities to all edges. The SASE cloud operates as a single entity and its internal structure is transparent to the end-users.
- **SASE points of presence (PoPs):** A specific instance within the SASE cloud that hosts the resources needed to deliver the SASE capabilities including servers, network connectivity, and software. SASE PoPs are symmetrical, interchangeable, multi-tenant, and mostly stateless. They are built to serve any enterprise edge connected through them as an integral part of that particular enterprise network.
- **SASE edge:** Designed to connect a specific edge to the SASE cloud. SASE clients include SD-WAN appliances for branches, IPSec-enabled firewalls and routers, and device agents for Windows, Mac, iOS, Android, and Linux.
- **SASE management:** Configure all policies and view network and security analytics and real-time status, in an intuitive, single-pane-of-glass, cloud-based management console.

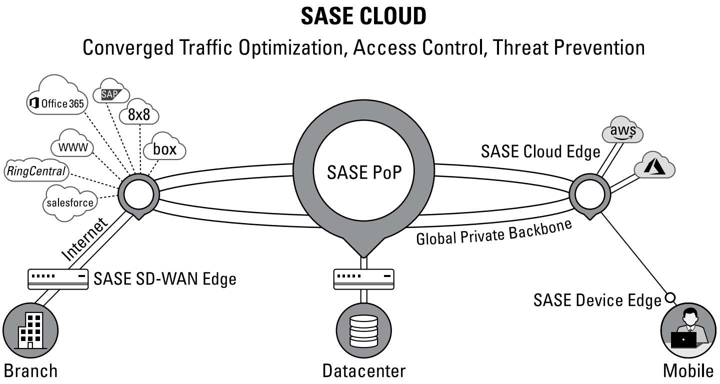


FIGURE 2-1: SASE extends networking and security to all edges including physical locations, clouds, users, and edge computing.

REMEMBER

SASE is a new category of cloud-native networking and security solutions, but the technologies and services delivered in a SASE solution are themselves not necessarily new — they are just converged into a unified, cloud-native solution.

SASE details an architectural transformation of enterprise networking and security that will enable IT to provide a holistic, agile, and adaptable service to the digital business. The individual technologies and services that comprise a SASE solution broadly consist of network-as-a-service and security-as-a-service offerings including:

- **Network as a service**
  - SD-WAN
  - WAN optimization
  - Bandwidth aggregation
  - Global private backbone
- **Security as a service**
  - Firewall as a service (FWaaS)
  - Secure web gateway (SWG)
  - Next-generation antimalware (NGAM)
  - Intrusion prevention system (IPS)
  - Cloud access security broker (CASB)
  - Software-defined perimeter (SDP), also referred to as Zero Trust network access (ZTNA)

TIP

Read Chapter 4 to learn about SASE network-as-a-service and security-as-a-service offerings.

SASE has four main characteristics. It is:

- **Identity-driven:** Unlike many networking and security point solutions that rely on IP addresses to identify a resource, SASE determines the true identity of every enterprise resource, whether it is a person, an application, a service, or a device. Identity, as part of a broad and dynamic context awareness, drives the risk and network service profile of every flow and the resulting combination of authentication methods, threat inspection, and data access authorization. Identity is integral through the access life cycle of a resource, from ensuring quality of service (QoS) to applying risk-driven security controls and more.
- **Cloud-native:** SASE is a cloud-native solution delivered in an "as-a-service" consumption model. A cloud-native

architecture leverages key cloud capabilities including multitenancy, scalability, velocity, efficiency, and ubiquity.

- **All edges:** SASE seamlessly supports all enterprise edges with full networking and security capabilities everywhere. By adopting a cloud-first approach to networking and security, SASE decouples many common capabilities, such as network optimization and threat prevention, from physical edge locations and places them in the cloud.
- **Globally distributed:** SASE is implemented as a globally distributed cloud platform. The SASE cloud design guarantees that wherever your resources are located, the full range of networking and security capabilities will be available to support them. SASE providers must strategically deploy global PoPs to deliver high-performance, low-latency service to enterprise edges including business locations, cloud applications, and mobile users.

TIP

Building a global cloud platform requires SASE providers to rapidly deploy PoPs into cloud and physical datacenters, ensure high capacity and redundant connectivity to support both WAN and cloud access, and apply end-to-end network optimization and security across all edges.

SASE: "NOT NEW" DOESN'T MEAN JUST MAKING WHAT'S OLD NEW AGAIN

The marketing campaigns among competing networking and security vendors — SASE "wannabes" — has already begun. Gartner warns that some traditional vendors will try to deliver a SASE-like solution based on wrapping their existing products in a SASE package. Such attempts will create a risk to service quality and delivery because these technologies were not designed for cloud-native delivery. In a nutshell, look carefully at the underlying SASE architecture to determine the fit with the expected outcomes. Here are a few examples to look out for.

Telco bundles are the exact opposite of SASE.

For more than a decade, telcos have offered to take away the complexity of managing your network and security stack with a bundle of point solutions they procure, install, and manage. Complexity didn't go away, and your spending increased to pay for both the products and the people to manage them. Also, you were dependent on the telco to do everything for you, often slowing the IT organization to a crawl.

This is the exact opposite of SASE: legacy appliances and fragmented management with limited or no visibility. SASE is built with the scalability, self-service, and agility of the cloud. Your telco isn't.

Virtual machines in the cloud are still a stack of appliances.

Instantiating virtual machines in an infrastructure-as-a-service (IaaS) environment like Amazon Web Services (AWS), Microsoft Azure, and the like is great, but not for SASE. Although it moves on-premises appliances to the cloud, they are still disparate point solutions that lack the cloud-native integration, single-pass processing, global reach, and elasticity of a SASE. And, depending on the vendor mix, you would still need to use multiple management consoles.

Service chaining sounds close, but not really.

Facing the reality of a multi-vendor environment, service chaining is a technique to link together multiple point solutions such as SD-WAN, secure web gateways (SWGs), firewalls, WAN optimizers, and more. Regardless of the use of multiple physical appliances or universal customer premises equipment (uCPEs), which host multiple virtual machines, those are still separate solutions that must be sized, scaled, and managed separately. Ultimately, SASE offers convergence as a key defining attribute. Service chaining isn't convergence but rather loosely coupled linking of point solutions.

The incomplete SASE: Cloud and WAN edge vendors must plug big holes in their offerings.

Security-as-a-service vendors have been working to deliver multiple security capabilities via their cloud services including secure web gateways (SWGs) and cloud access security brokers (CASBs). Those vendors still lack the key SASE elements of controlling network flows and natively supporting the WAN edge. Without a natively integrated and mature technology to reliably and securely connect all edges (offices, cloud datacenters, users, and devices) to the SASE Cloud, SWGs and CASBs remain a silo that needs integration with other products. Similarly, edge appliance vendors now face the task of building the breadth of SASE Cloud capabilities as globally distributed, cloud-native services.

Introducing Cloud-Native Networking and Security

The SASE architecture is made up of two core components:

- The **SASE Cloud** acts as an aggregator of networking and security capabilities.
- **SASE edge connectors** drive traffic from physical, cloud, and devices edges for SASE Cloud processing.

SASE uses a single-pass processing engine to efficiently apply network traffic optimization and security inspection with rich context for all traffic. Contrast the SASE model with stacking point products where each product analyzes traffic for a specific requirement, adds overhead for actions like decryption, and lacks the context generated in other network and security point products.

Selected SASE capabilities include:

- **Reliable connectivity:** All edges connect to the nearest SASE PoP, employ standard SD-WAN features, and have access to the SASE's global private backbone to provide global connectivity with guaranteed performance and availability.
- **Authentication:** Upon connection of an edge, dynamic risk assessment drives authentication based on the edge type and the configured policy.
- **Access control:** Access to key applications and service is controlled by application- and user-aware next-generation firewall policies. In addition, a Zero Trust network access (ZTNA) model ensures remote users can only access authorized applications rather than providing unrestricted access to entire networks.
- **Application performance optimization:** Application identification assigns priority to the traffic to optimize latency and loss-sensitive applications like voice over IP (VoIP) and virtual desktop infrastructure (VDI) over other traffic such as file transfers and general Internet browsing.

- **Decryption:** To enable advanced threat prevention, encrypted traffic is decrypted once to allow multiple engines, such as intrusion prevention and antimalware inspection, to process the traffic.
- **Threat prevention:** Multiple security engines parse the traffic to detect risky access and activity. These include secure web gateways (SWGs) that look for malicious web sites, anti-malware to prevent download and distribution of malicious files, intrusion prevention systems (IPS) to stop inbound and outbound anomalous connections that are indicative of malicious activity, and more.
- **Data loss prevention:** A cloud access security broker (CASB) provides full visibility into cloud application usage and the ability to control access and enforce granular enterprise policies. Data loss prevention rules provide additional tools to help detect sensitive data in the network flows and stop it from leaving the network.

The SASE architecture is designed to rapidly extend the "single pass traffic processing engine" to seamlessly and centrally add new capabilities.

TIP

SASE is a holistic platform that connects all edges to one logical network and inherently delivers the security capabilities they need. This lowers the cost, complexity, and risks of supporting the digital business in a dynamic environment. Key benefits of SASE include:

- **Enabling business agility:** Supported by the SASE architecture, IT can deliver optimized networking and robust security to all locations, applications, and users, regardless of where they are located. Provisioning of new resources and capabilities is fast and simple. Just deploy the right edge client and plug it into the SASE platform — pre-configured corporate policies drive the network and security experience.
- **Providing end-to-end visibility and control:** IT teams can leverage the convergence of network and security to manage all features and policies in a single interface, using a common terminology, and gain deep visibility into network and security events across all edges. Cross-team collaboration improves the overall service delivery to the business that often involves a combination of availability, performance, and security requirements.

- **Increasing operational efficiency:** With SASE, IT teams are relieved of the grunt work required to maintain on-premises network and security infrastructure including managing physical topology, redundancy, scaling, sizing, and upgrades. IT can focus on delivering better service and strategic value to the business, dedicating scarce resources and skills on business-specific problems rather than day-to-day firefighting and maintenance.
- **Reducing management complexity and total cost of ownership (TCO):** Simplifying the network and security stack by consolidating multiple point products in a single solution enables both vendors and customers to reduce the overall costs of acquiring, operating, and maintaining networking and security infrastructure.

IN THIS CHAPTER

- » Consuming network services using a cloud consumption model
- » Enabling advanced security capabilities as a service

Chapter 3 Understanding SASE Capabilities

In this chapter, you explore the networking and security capabilities of SASE, delivered as a cloud-based service to enterprises across all edges.

Network as a Service

Network as a service enables global connectivity for enterprises across all edges, including on-premises datacenters, cloud datacenters, headquarters and branch locations, public cloud services, the Internet, the Internet of Things (IoT), remote sites (including work-from-home), and mobile users.

Edge SD-WAN

Software-defined wide-area network (SD-WAN) is designed to address the changing requirements of enterprise networks driven by the growth of cloud and the Internet. SD-WAN is a more flexible solution than multiprotocol label switching (MPLS) for supporting a distributed workforce, and it is more reliable and scalable than virtual private network (VPN) based wide-area networks (WANs).

SD-WAN is implemented in SASE solutions as a means to securely and reliably connect a branch or a datacenter to the SASE cloud. Each edge appliance is connected over a set of network services (typically multiple Internet circuits, and sometimes MPLS). It continuously monitors the current availability and performance of each of these services. Traffic reaching a SASE point of presence (PoP) is classified based upon application and prioritized using a set of centrally managed policies before being sent to its destination.

SD-WAN makes it possible to replace regional MPLS, which is expensive and time-consuming to connect to new edge locations. It also allows security functionality to be distributed to all edges, eliminating the need to backhaul traffic through the enterprise datacenter for scanning before forwarding it to cloud services, a common but inefficient practice that increases latency and degrades performance.

Key edge SD-WAN capabilities include:

- **Link aggregation:** SD-WAN improves capacity and resiliency by balancing traffic across multiple links. Multiple link aggregation scenarios for MPLS and Internet circuits such as fiber, broadband cable, digital subscriber line (xDSL), and 4G Long-Term Ethernet or 5G are supported.
- **Dynamic path selection:** Applications deliver the optimum user experience with dynamic path selection and policy-based routing. SD-WAN monitors link quality metrics (including jitter, latency, and packet loss) and dynamically selects the optimum link based on preconfigured network rules. Applications can also be pinned to specific transports, such as restricting business-critical applications to a high-quality symmetric fiber link and other applications to a lower quality asymmetric link.
- **Bandwidth management and quality of service (QoS):** SD-WAN aligns network usage with business intent through bandwidth management (QoS) rules. The rules assure that more critical applications always receive the necessary upstream and downstream capacity, serving other applications on a best-effort basis. Rules contain priority, class of service, and capacity limits, if relevant. Administrators can modify or create rules, network-wide or per site.

- **Packet loss mitigation:** The effects of packet loss in the last mile are dramatically reduced by detecting lost packets nearly instantly in the nearby PoP rather than at the remote destination. Applications that are more sensitive to packet loss — such as voice, video, and remote desktop protocol (RDP) — can be set with packet duplication to assure 100 percent packet delivery. For other applications, when excessive packet loss is detected, SD-WAN automatically detects the change and switches traffic to an alternate link connecting the site and intelligently resumes use of primary links to avoid link flapping.
- **Border gateway protocol (BGP) integration:** When organizations consider WAN transformation, they often must face the challenge of integrating SD-WAN with their existing routing infrastructure. Without BGP routing protocol integration, companies end up having to manually configure multiple static paths to connect their routed and SD-WAN infrastructure.

Global private backbone

Enterprises have long struggled with finding reliable and affordable global connectivity. Global MPLS connections come at a high cost for limited bandwidth, if they're available at all. The Internet, already unpredictable, is only made worse by the latency of long-distance global connections.

A SASE provider provides customers with global connectivity by leveraging a worldwide network of PoPs interconnected across multiple tier-1 backbone carriers and backed by service-level agreements (SLAs) that guarantee network performance including availability, latency, packet loss, and jitter. The SASE provider monitors real-time performance of carrier networks and leverages quality-aware routing algorithms to automatically select the optimum path in real time — even if that path is indirect, via other PoPS — across the backbone.

A SASE platform has a multitenant WAN backbone built from globally dispersed PoPs that are fully meshed, creating a private and optimized global overlay. Edge resources — including physical locations, cloud datacenters, and remote users — establish secure tunnels to the nearest PoPs using IPsec or Datagram Transport Layer Security (DTLS). Cloud applications are accessed by routing traffic to the closest PoP as measured by latency and loss.

Secure and optimized cloud access

Connecting to the cloud can be complicated. It's not just a matter of connecting the cloud to your WAN. Backhauling Internet and cloud traffic from your remote branch locations to a central, secure Internet access point (for example, your datacenter) adds too much latency to cloud-bound traffic. It also consumes significant capacity, becoming quite expensive when the WAN is built on costly MPLS connections.

Instead, many organizations provide their offices and mobile users with direct Internet access. An Internet connection provides basic connectivity, but no performance, security, or reliability guarantees. Using the Internet requires organizations to think through several issues, including:

- Predictable application delivery when latency and packet loss will likely fluctuate across the Internet.
- Securing access to cloud datacenters requires different tools than those used for securing and managing access to physical datacenters.
- Enabling multiple locations and mobile users to efficiently access multiple clouds or multiple networks within one cloud.
- How security and networking affect cloud agility, scalability, and costs.

Site-to-site VPNs provide secure access but do nothing for performance and reliability. Premium cloud connectivity solutions, such as Amazon Web Services (AWS) DirectConnect and Microsoft Azure ExpressRoute, address performance and reliability issues, but are very expensive and not available in all areas, or for all edges.

A SASE cloud provider addresses cloud connectivity issues by integrating its core network with major cloud providers, such as AWS, Microsoft Azure, and Google Cloud Platform, making cloud connectivity available to all edges with the required reliability, performance, and security.

Cloud application traffic, such as Office 365, unified communications as a Service (UCaaS), and cloud enterprise resource planning

(ERP), is optimally routed over the SASE's global private backbone with end-to-end acceleration from the edge to the cloud application's datacenter.

Zero Trust Network Access (ZTNA)

Software-defined perimeter (SDP), also known as Zero Trust Network Access (ZTNA), is a new approach for securing remote access to business applications both on-premises and in the cloud. SDP is an integral part of Gartner's SASE framework.

Enterprises have long relied on VPNs to connect mobile or remote users to applications and other network resources. But traditional VPNs are poorly suited for the shift to the cloud and to the increase in work-from-home users. VPNs rely on appliances, such as firewalls or VPN concentrators, forcing remote users' traffic to specific physical locations. This architecture adds latency and creates capacity constraints. Once connected through a VPN, users are trusted with access to all resources on the network, increasing the risk of malware propagation and data breach on the enterprise network. And, to reach the VPN gateways, users must rely on the unreliable and unpredictable Internet connectivity. Overall, legacy VPN architectures expose the enterprise to attacks and adversely affect the user experience, especially when accessing cloud applications (see Figure 3-1).

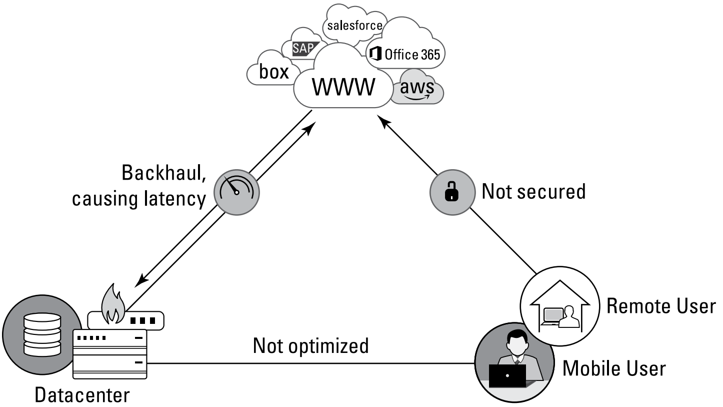


FIGURE 3-1: Remote and mobile access to on-premises and cloud applications is challenging with legacy VPN appliance-based architectures.

The SASE's cloud network is a full replacement for traditional VPN solutions. By running a mobile client or clientless browser access, the mobile device finds and connects to the nearest SASE PoP.

The user authenticates using single sign-on and multi-factor authentication. Once connected to the PoP, the user is part of the virtual enterprise WAN and can access specifically authorized applications.

With its global, SLA-backed backbone, the SASE's cloud network connects remote users to both physical and cloud datacenter resources anywhere in the world without the erratic performance and reliability of the Internet middle mile. Remote and mobile users are treated as first-class network citizens on the SASE platform, benefitting from all the network optimization and advanced security capabilities commonly limited to office users.

REMEMBER

Cloud-native SDP delivers secure remote access as an integral part of a company's global network and security infrastructure. A global, cloud-scale platform supports any number of remote users within their geographical regions. Performance improves with end-to-end optimized access to any application using a global private backbone. Risk is minimized before and after users access the network through strong authentication and continuous traffic inspection for threat prevention. Cloud-native SDP makes mobile access easy to deploy, easy to use, and easy to secure.

Security as a Service

Security as a service enables organizations of all sizes to apply enterprise-grade protection everywhere. Datacenters, branches, mobile users, and cloud resources can be protected under a unified policy with the same set of defenses. As a cloud service, SASE seamlessly optimizes and adapts security controls for emerging threats. Traditional tasks associated with point security solutions such as capacity planning, sizing, upgrades, and patches are eliminated for the customer.

Key security services to look for in a SASE solution include:

- Firewall as a service (FWaaS)
- Secure web gateway (SWG)

- Next-generation antimalware (NGAM)
- Intrusion prevention system (IPS) as a service
- Managed threat detection and response (MDR)

Firewall as a Service (FWaaS)

Firewall as a service (FWaaS) is a new and revolutionary way of delivering firewall and other network security capabilities as a cloud service. Enterprises typically deploy next-generation firewalls as physical or virtual appliances, either on-premises or in the cloud. Although form factors and deployment locations vary, the enterprise still needs to support the full appliance life cycle:

- Distributed locations need dedicated appliances that need to be sized and upgraded to accommodate business growth.
- Appliance software must be regularly patched and periodically upgraded.
- Policy management must be done on a per-appliance, per-location basis.

FWaaS doesn't merely hide physical firewall appliances behind "cloud duct tape." Instead, FWaaS truly eliminates the appliance form factor, making network security functions — such as web content filtering, intrusion prevention, anti-malware/next-generation anti-malware, security analytics, and managed threat detection and response (MDR) — available everywhere.

REMEMBER

With FWaaS, the entire organization is essentially connected to a single, logical global firewall with a unified application-and user-aware security policy.

Secure web gateway (SWG)

A secure web gateway (SWG) allows organizations to control access to resources on the Internet based on categories that are continuously maintained by the SWG vendor. For example, content such as pornography, drugs, violence, and sites carrying Internet-borne threats like phishing and malware can be blocked with a single rule. Similarly, a single rule can be set to limit access to social networks, news, and media streaming to off-business hours.

REMEMBER

SASE converges the capabilities of a next-generation firewall (WAN and Internet traffic inspection) and the extended coverage for mobile users of SWGs. A converged approach eliminates the need to maintain policies across multiple point solutions and the appliance life cycle.

Next-generation antimalware (NGAM)

Next-generation antimalware (NGAM) capabilities in SASE include:

- **Deep packet inspection** of traffic payload for clear and encrypted traffic (if enabled). File objects are constructed from the traffic stream, inspected, and blocked, if appropriate.
- **True file type detection** identifies the file type traversing the network, regardless of its file extension or the content-type header. This capability is used to detect all potential high-risk file types and defeat evasion techniques that are used by attackers and misconfigured web applications.
- **Malware detection and prevention** employs multi-layered and tightly integrated anti-malware engines. A signature- and heuristics-based inspection engine scans files in transit to ensure effective protection against known malware. This anti-malware engine uses global threat intelligence databases to stay current with the latest threat information. Machine learning and artificial intelligence are used to identify and block unknown malware, such as zero-day threats and polymorphic variants of known threats.

IPS as a Service

Intrusion prevention systems (IPSs) inspect WAN and inbound and outbound network traffic, including Secure Sockets Layer (SSL) encrypted traffic, and can either generate security events (in detection mode) or block malicious traffic (in prevention mode).

In SASE, IPS is delivered as a service, requiring no action by the customer organization. The SASE provider updates, tunes, and maintains IPS signatures including custom-developed signatures (based on big data collection and analysis of the organization's traffic) and signatures originating from external security feeds.

IPS as a Service is comprised of several layers of protection including:

- Behavioral signatures look for deviations from normal or expected behavior of systems or users. Normal behavior is identified using big data analytics and deep traffic visibility across networks.
- Reputation feeds leverage both in-house and external intelligence feeds to detect and prevent inbound or outbound communication with compromised or malicious resources.
- Protocol validation is used to validate packet conformance to the protocol, thereby reducing the attack surface from exploits using anomalous traffic.
- Known vulnerabilities published in common vulnerabilities and exposures (CVE) lists, as well as new vulnerabilities, are rapidly incorporated into the IPS inspection engine.
- Malware communication including outbound command and control (C&C) traffic is blocked, based on reputation feeds and network behavioral analysis.
- Geolocation enforces customer-specific geo-protection policies, optionally stopping traffic based on the source and/or destination country.
- Network behavioral analysis detects and prevents inbound and outbound network scans, limiting attackers' ability to gather intelligence about targeted networks.

IMPROVING SECURITY POSTURE WITH MANAGED THREAT DETECTION AND RESPONSE

A managed threat detection and response (MDR) service enables enterprises to offload the resource-intensive and skill-dependent process of detecting compromised endpoints to the SASE provider's security operations center (SOC). A full service MDR is seamlessly applied to customer networks. The SOC automatically collects and analyzes network flows, verifies suspicious activity, and notifies customers of compromised endpoints.

IN THIS CHAPTER

- » **Ringing up savings with SASE**
- » **Getting a healthy dose of secure global connectivity**
- » **Calculating the benefits of SASE for digital transformation**
- » **Building a global high-performance network**

Chapter 4
Looking at SASE in Action

In this chapter, you explore several industry use cases for SASE and learn about real-world customer successes with Cato Cloud.

Retail

From big-box chains to specialty stores, the retail industry's business model is built on relatively low operating margins — which requires frugal management of retail networks connecting remote store locations to headquarters. Retailers rely upon their wide-area networks (WANs) to securely process transactions, manage inventory, report sales, and deliver superior omni-channel customer experiences.

Although multiprotocol label switching (MPLS) networks may be fairly common WAN architectures for larger big-box stores in standalone locations, they can be cost-prohibitive and difficult — if not impossible — to install in shopping mall, strip mall, and specialty store locations. For these retailers, as well as popup stores, such as kiosks or seasonal stores, MPLS is impractical. Even with MPLS networks, retailers find it necessary to install secondary direct Internet access (DIA) connections, such as broadband, to provide omni-channel experiences to their customers over guest Wi-Fi networks.

TIP

SASE provides a turnkey solution that can be quickly deployed and centrally managed to address retail industry challenges in their edge networks.

BRAKE MASTERS PUTS THE BRAKES ON OUTAGES ACROSS 71 SITES

Brake Masters is an auto repair chain in the western United States with 71 company-owned retail stores and 30 franchises. Before migrating to Cato, the company-owned stores, served by Brake Masters IT, had redundant firewall appliances connected by T1 lines and MPLS. All traffic was sent from the retail locations to a datacenter in Tucson, Arizona. The primary applications were point-of-sale (PoS) systems and retail customer Wi-Fi.

The challenge: Outages keep business in second gear

The MPLS was “just plain unreliable” and slow, says Steve Waibel, the director of IT for Brake Masters. “We faced weekly outages in one store or another,” he says.

The network was also unable to deliver a decent guest Wi-Fi experience. The free Wi-Fi from Brake Masters was often limited to just 500 Kbps, far too slow for YouTube or to do much more than basic Web browsing. “We got quite a few complaints about that,” Waibel says.

And MPLS proved to be a drag on Brake Masters’ schedule for opening new stores. When a new store was ready to open, they were often waiting on connectivity. “We had an ongoing issue with provisioning MPLS,” Waibel says.

Cato gets Brake Masters cruising

Waibel knew he needed to fix his network and began researching SD-WAN vendors. “All totaled, we probably evaluated 10 to 12 SD-WAN vendors,” he says. But alternative SD-WAN solutions proved to be too expensive and complicated, requiring Brake Masters to maintain firewall appliances at every location. They also relied on the public Internet, which Waibel thought would be too unreliable and unpredictable for Brake Masters.

With Cato, Waibel found a solution that met his needs. Waibel chose to deploy Cato across all 71 locations, configuring sites with a Cato Socket, Cato's SD-WAN device, and dual last-mile Internet connections, typically cable and fixed wireless.

Brake Masters deploys sites quickly and improves performance

Waibel says Cato meets all the needs for retail locations, including easy management, deployment, and getting notifications of potential network problems before they're a big deal. "All that makes it very easy to run your retail establishments," Waibel says.

More specifically, opening new stores with Cato has been much faster and easier than with MPLS. "We order lines, and they're always in well before the store is done," Waibel says.

With Cato, he also vastly improved his customer Wi-Fi experience. "Since we moved to Cato, our bandwidth increased by approximately 30 times the speed we had before," Waibel says. "Now, the customer's Wi-Fi experience is much better. We've stopped receiving complaints since deploying Cato," Waibel says.

The changes in the last mile infrastructure also meant better uptime. "None of our sites have lost complete connectivity since deploying Cato," he says. "Sure, there are disruptions in the last mile, but the Cato Socket just moves the traffic over the secondary connection. The users never know the difference," Waibel says.

The portal makes it easy to set up a new site, manage a site, and manage firewall rules. "The management portal is well designed. It's my favorite feature," he says. "All the information you need to manage the network is right there."

A case in point is his security infrastructure. Instead of deploying branch security appliances, Waibel relies on Cato security services — NGFW, anti-malware, and Cato IPS. He administers his security rules centrally in the Cato management portal, automatically applying them to the stores everywhere — all without deploying additional security appliances.

And when there are problems, Waibel has been able to resolve disruptions far faster with Cato. "We get a view of every single store, and we can tell if there's a problem at any store," Waibel says. "Every day, we know exactly what's going on, and we can address any issues that might be there."

Pharmaceuticals

Life sciences and pharmaceutical companies require robust, secure networks that increasingly rely on high-performance connections to the cloud for access to massive cloud data lakes and data warehouses.

Network failures and errors can cause batch processing problems that potentially result in millions of dollars in losses. At the same time, security is of paramount concern with the need to ensure data integrity, as well as confidentiality in intellectual property.

CENTRIENT PHARMACEUTICALS QUADRUPLES CAPACITY

Centrient Pharmaceuticals is a global pharmaceutical company and a leader in sustainable antibiotics, next-generation statins, and antifungals. As with many enterprises, the IT team at Centrient Pharmaceuticals grew tired of the limitations of MPLS. Performance across the company's 10-site, global network was for the most part "solid," says Matthieu Cijsouw, Global IT Manager at Centrient. But as the applications' capacity requirements grew, increasingly the MPLS service was becoming congested.

"Users noticed that MPLS was slow. It took a long time for them to open documents," he says.

The high cost of MPLS bandwidth made upgrading global bandwidth unrealistic. "MPLS was about 4x more than Cato for a quarter of the bandwidth," he says.

And bandwidth wasn't the only problem. Agility was also limiting Centrient. It typically took him three to four months to move a location, a bit faster in Europe. "One time, we needed to move a sales office, and the MPLS connection was simply not ready in time. It led to operational issues and difficult workarounds," he says. "Needless to say that was not appreciated by the business."

Centrient evaluates SD-WAN alternatives

As his MPLS contract came up for renewal, Cijsouw started looking into SD-WAN. A technology partner recommended a combination of

SD-WAN appliances, firewalls, and secure web gateways (SWG). But Cijsouw thought the solution would be too complex and was troubled by the dependence on the Internet middle-mile. "Internet performance from many regions, particularly China mainland, fluctuates significantly during the day," he says. "We wanted a middle-mile solution."

After meeting with the Cato team, he decided to run a proof of concept (PoC). "We did load balancing, failover tests, and load tests and Cato passed them all," he says.

During the next phase, he put a production load on Cato Cloud to see if there would be any hiccups. Not only were there no problems, but users noticed that applications were even more responsive, he says.

"We migrated to Cato in stages, gaining confidence along the way," he says. "Even with a full deployment, I can bring up a global, site-to-site VPN in two hours should something happen, but I don't see that as a concern. Not only does Cato Cloud perform well, but the support Cato offers is insanely great. I never experienced such a fast response."

Centrient switches from MPLS to Cato Cloud

In the end, he decided to move all MPLS locations to Cato Cloud. "It only took us about a month," Cijsouw says, "The actual cutover was done in 30 minutes."

Most locations had been equipped with 6 Mbps MPLS connections. He replaced those with two, and in some cases, three local Internet connections for an aggregate capacity of 20 Mbps per site, burstable to 40 Mbps. Datacenter capacity is even higher, up to 50 Mbps, burstable to 100 Mbps — enough for current usage.

With Cato Cloud, Centrient gained deep visibility into network performance.

The additional connections were dual-homed for maximum availability. To ensure complete redundancy in the physical layers (including wiring and ducting), Cijsouw followed best practices and connected sites to the Internet with separate technologies — typically fiber and radio connections.

Not only has he reduced his costs, but with more capacity, his applications continue to perform as well as, if not better than, with MPLS.

(continued)

(continued)

"The voice quality of Skype for Business over Cato Cloud has been the same as with MPLS but, of course, at a fraction of the cost," he says. "In fact, if we measure it, the packet loss and latency figures appear to be even better."

His connections into China also work equally or "even better" than with MPLS, he says.

And with Cato Cloud, he gained greater visibility into his network. The reporting is very "accessible" with detailed statistics of online usage, he says.

A more agile future With Cato Cloud

As Cijsouw looks ahead, Cato Cloud will afford him flexibility — and negotiating strength — in other areas of his network. His firewall appliances, for example, are coming up for renewal in a year. Besides providing site security, they also serve as his mobile access solution. With Cato Security Services and Cato's mobile client bundled with Cato Cloud, he could replace both and save on licensing and operational costs. "Today, we outsource firewall maintenance for about 25 percent of our networking budget," he says. "With Cato that wouldn't be necessary."

Overall, how would he summarize his Cato experience? "It's been really excellent," he says.

"Product delivery and support have all been there. With Cato Cloud, not only did I receive a more agile infrastructure, but I also received an agile partner who can keep up with my needs. We operate faster because of Cato."

Financial Services

The financial services industry has traditionally built out robust MPLS networks designed to support highly transactional traffic that requires accuracy, speed, and security. However, as many financial institutions have increasingly expanded their local presence and online offerings, extending MPLS to remote locations has become increasingly difficult. Financial institutions need to undergo digital transformation to stay in business, forcing them to reconsider their network and security architecture, like many businesses in other industries.

TIP

Financial services firms can leverage SASE to ensure robust networking and security capabilities at their edge locations, with centralized management to help maintain stringent security, privacy, and regulatory compliance standards and requirements.

STANDARD INSURANCE USES CATO FOR CLOUD MIGRATION

Standard Insurance, a nationwide provider of insurance and financial products is based in Makati, the Philippines, with 60 branches, 700-plus dealer/agent networks, and 1,500 associates nationwide. In 2016, the company initiated a multiyear digital transformation project. The company was shifting to online selling and needed to evolve its aging backend software infrastructure. The system served the entire process of the insurance business, from application and proposal to policy issuance, administration, and claims — in other words, the life cycle of the company. The new, custom-developed platform, though, still ran in the company datacenter. A system failure would represent an existential threat to the company; moving the insurance software from the on-premises datacenter to Amazon Web Services (AWS) became a priority.

Prior to Cato, Standard Insurance used local firewalls and low-bandwidth, telco-provided IP-VPN services to connect branches to the company headquarters. Insurance agents and employees connected to the Makati headquarters to access the company's insurance application via VPN. Those sites were secured by branch firewall appliances connected by telco-provided VPN services. But the lack of telco coverage meant that Alf Dela Cruz, First Vice President, Head of IT Infrastructure and Cybersecurity at Standard Insurance, and his team had to manage multiple provider relationships to deliver comprehensive branch connectivity. It was a headache.

Security was also a concern. The local firewall appliances needed to be upgraded, which was a constant expense, and they were insufficient to protect the organization. After two ransomware incidents, the CEO demanded a dramatically improved security posture.

The complexity of the firewall appliances also complicated site deployments. "With a hardware firewall, we had to copy information to every site and make sure it stayed updated, and whatever changes we made at the head office needed to filter out to every branch," says Dela Cruz.

(continued)

(continued)

Cato cuts security costs in half

"When we learned about the Cato solution, we liked the idea of simple and centralized management. We wouldn't have to worry about the time-consuming process of patch management of on-premises firewalls," says Dela Cruz.

Cato connects all enterprise resources — locations, cloud resources, and mobile users — to a common, optimized global backbone, which today is built from more than 42 points of presence (PoPs) across the globe. With all traffic on the Cato backbone, Cato applies a common security policy to protect all resources. Next-generation firewall (NGFW), secure web gateway (SWG), URL filtering, and malware prevention are all built into the Cato service. Cato MDR, a managed threat detection and response (MDR) service, offloads the resource-intensive and skill-dependent process of detecting compromised endpoints onto the Cato SOC.

Cato simplifies network and security infrastructure

Cato won the day with its AWS connectivity. Cato's points of presence (PoPs) are co-located in the same physical datacenters as the Internet exchange points (IXPs) of Amazon AWS, Microsoft Azure, and other cloud datacenter services, providing fast access to cloud resources across cloud providers and global regions. "Once we migrated our critical applications into the AWS cloud, we took Cato even more seriously because of their compatibility with the cloud network. This allows our branches to easily connect to the AWS cloud via the Cato network," says Dela Cruz.

Implementing Cato also allowed Standard Insurance to shorten deployment times. Dela Cruz and his team could eliminate all branch firewalls and Internet-based VPNs, and instead, send a Cato Socket, Cato's small SD-WAN device, to each branch for a non-technical person to simply plug in. Once the Socket connects to the Internet, the Cato network recognizes it, joining the Socket into the SD-WAN. The Socket inherits the global security policies Dela Cruz and his team have configured for the network. "We can set up a branch in minutes with Cato," says Dela Cruz.

Enforcing one set of security rules in the cloud for all users and resources makes security much easier to manage and update. Policies can also be customized to meet the needs of individual locations, users, and more from the Cato management console.

As for the users, Standard Insurance employees enjoy a better user experience. Previously, IP VPN bandwidth was limited to 1 Mbps. "With Cato we increased Internet bandwidth by 10x, significantly improving performance without increasing costs," says Dela Cruz.

Standard Insurance will continue with its broader transformation efforts. Standard Insurance is looking to roll out more mobile clients to bring more dealers and agents onto the network.

"We are recommending Cato to our business partners," says Dela Cruz. "We love that the solution is cloud-based, easy to manage, and less expensive than other options."

Manufacturing

Manufacturing firms must address unique networking and security challenges. IT system maintenance and administration is often secondary to operational technology requirements, and qualified IT networking and security staff are not typically available at remote sites, resulting in limited IT support.

TIP

SASE supports manufacturing and industrial enterprises with a fully converged networking and security service. SASE is easy to install and maintain and leverages any available direct Internet access (DIA) connection, such as broadband or Long-Term Ethernet (LTE) cellular to provide secure network connectivity from everywhere to headquarters, datacenters, the cloud, and the Internet.

SALCOMP REPLACES GLOBAL MPLS AND FIREWALLS

When you're a primary manufacturer to major mobile phone companies, uptime and security are critical. A small hiccup in your production line could be disastrous for your customers — and your business. All of which might sound like a good reason for sticking with expensive managed MPLS services, until you consider that you're also being evaluated on budget management.

(continued)

(continued)

Such was the challenge for Ville Sarja. The seasoned CIO was responsible for the aging IT architecture at Salcomp, a global manufacturer of adapters for electronic devices, originally part of Nokia and now a primary supplier to Samsung and other leading mobile phone companies. "The IT template hadn't changed in nearly 20 years since Nokia spun out Salcomp," says Sarja.

During those two decades, though, Salcomp's business had changed significantly. The headquarters and the datacenter were still in Finland, but most manufacturing occurred in Brazil and the Asia Pacific. Offices had given way to more mobile users, particularly in China. The cloud had become far more popular, something Sarja was looking to leverage, and video conferencing had become the norm.

MPLS: Not suited for the future

The company's global MPLS network, which connected manufacturing plants in China, India, and Brazil with the datacenter and headquarters in Finland, consumed a "significant portion" of Salcomp's IT budget, says Sarja.

Global MPLS bandwidth was limited, which would prove problematic as traffic requirements grew. To address the situation, Salcomp deployed WAN optimizers at each end of his MPLS connections, but the WAN optimizers were challenging to configure, he says.

And for all of its touted uptime and availability, MPLS's dirty secret remains the last-mile connectivity problems that arise on global connections. Unable to control last miles outside of their regional networks, MPLS providers must rely on local third-party partners — often with mixed results. For that reason, Salcomp equipped locations with backup connections — local Internet access and firewall clusters running antimalware and IPS.

The last straw was MPLS's rigidity around new site installation. Says Sarja "In terms of deploying new sites, which [is] something we're doing more [of] in the past year, MPLS takes up to six months to have a circuit in place," he says.

Performance testing shows Cato blows away MPLS

Sarja and his team decided to run a POC, testing Cato Cloud from Salcomp's Finland datacenter and locations across China, Taiwan, and

India. They deployed a Cato Socket at each location with policies in the local firewall steering the pertinent traffic to Cato.

What Sarja found impressed him. Data throughput on Sharepoint file transfer testing from Taiwan to Finland with Cato was 30 times better than MPLS with a WAN optimizer; file sharing improved by more than 40 times.

Within China, Sarja found downloading a 116 MB Excel file across the site's 20 Mbps connection to Cato Cloud on average took 83 seconds. Across MPLS? Download times were 20 times longer.

Latency also dropped by 13 percent when tested from China to Finland across Cato. And not only was performance as good as if not better than MPLS, but Cato deployment was much quicker. He could use any Internet line to connect locations to Cato Cloud, eliminating the six-month deployment times required for MPLS.

Salcomp replaces MPLS with Cato Cloud

Sarja decided to move forward with a phased migration of Salcomp's production line onto Cato. Initially, the team connected the datacenter in Helsinki to Cato. Afterward, they migrated the Indian and Brazilian locations. During the final phase, Sarja moved over the China locations of Shenzhen and Guigang, as well as the Taiwan location in Taipei.

Across all locations, he replaced the routers, firewall appliances, and WAN optimizers with redundant Cato Sockets configured in high-availability mode. "With just one architecture, not three, we can make changes in a few minutes that required weeks with our MPLS provider," he says. Without local firewalls, Sarja relied on Cato Security Services to protect against network-based threats. Testing done by a leading mobile phone manufacturer vetted Cato's security, allowing Sarja to extend an IPsec tunnel from his Cato network to the mobile phone provider's premises.

Salcomp IT: Ready for today and positioned for tomorrow

Overall, Sarja says he's received the best feedback any CIO could want from his users — nothing. "Users just aren't complaining any longer," he says. And that's a very good thing.

Chapter 5

Ten Things to Consider When Evaluating a SASE Vendor

This chapter presents ten important capabilities and features to look for in a SASE vendor for your organization.

Convergence

SASE brings together core networking and security functions in a unified cloud-native platform delivered "as a service." Convergence of networking and security technologies in a fully integrated solution that provides end-to-end visibility and control, rather than using siloed point networking and security products, is a key characteristic of SASE.

Core network as a service functions in SASE include: a global private backbone, an edge software-defined wide-area network (SD-WAN), cloud access, and a mobile virtual private network (VPN).

Core security as a service functions in SASE include: firewall as a service (FWaaS), a secure web gateway (SWG), next-generation anti-malware (NGAM), intrusion prevention system (IPS) as a service, and managed threat detection and response.

TIP

A truly converged SASE solution will not increase latency for processing because all engines work together in parallel. Without single-pass processing, each networking and security element must process individual packets one after the other — resulting in degradation of application performance and a poor customer experience.

Cloud Native

Virtualized networking and security appliances, such as routers and firewalls, simply move traditional on-premises equipment to the cloud. Virtualization is an important enabling capability in the cloud, but it is only one component. A truly cloud-native solution also enables dynamic self-service, rapid scalability and elasticity, and an "as a service" consumption-based model, among other capabilities.

To enable a unified platform that delivers full capability networking and security services to all edges, everywhere, a SASE solution must be built in the cloud, for the cloud.

TIP

Cato Networks developed the Cato Cloud from scratch as a cloud-native service. It uses a single pass engine to process all traffic from the packet up and provide optimization and security. Cato Cloud does not use purpose-built appliances or virtual machines and is therefore able to provide customers the scalability, self-service, and agility of cloud providers.

Global

To serve the networking and security needs of global enterprises in a global economy, a SASE provider needs to have a global footprint. Relying on the Internet for wide-area network (WAN) connectivity across certain regions around the world can result in unpredictable performance, poor reliability, and security and privacy issues.

When evaluating a SASE provider, look for a company that has numerous points-of-presence (PoPs) around the world, that are interconnected by tier-1 backbone carriers with robust service-level agreements (SLAs), and that offers a service to replace multiprotocol label switching (MPLS) on your WAN.

TIP

Cato Cloud spans more than 55 PoPs from which the full capabilities of the SASE service are delivered. All of Cato's PoPs are interconnected by multiple tier-1 backbone carriers, forming a global private backbone that optimizes WAN, cloud, and mobile traffic. The PoP software applies deep packet inspection to secure the traffic against multiple threats as it flows through the Cato Cloud.

All Edges

SASE uniquely supports all enterprise edges including: on-premises data centers; branch offices and remote locations; public cloud services such as software as a service (SaaS), unified communications as a service (UCaaS), platform as a service (PaaS), and infrastructure as a service (IaaS); network-connected devices like printers, kiosks, and Internet of Things (IoT) devices; and mobile and work-from-home (WFH) users.

In a SASE deployment, physical locations use SD-WAN devices and multiple Internet links to maximize throughput, enforce quality of service (QoS), and overcome link failure or degradation. Mobile workers use a VPN client or clientless web access for enterprise-grade protection and optimized access to datacenter and cloud applications. Cloud datacenters connect to the SASE cloud over multiple tunnels, with all traffic secured and optimized regardless of the source edge.

TECHNICAL STUFF

SASE includes a thin-edge component to connect different edges to the nearest available SASE PoP. The edges work in tandem with the SASE cloud to ensure continuous service. The SASE cloud is designed to deliver the same set of capabilities from every PoP, and without dependency on customer-specific components, simplifying the shift of traffic across the SASE cloud.

TIP

Physical locations, mobile users on any device, and cloud datacenters and applications, all use Cato edge solutions to plug into the Cato Cloud. Physical locations use an edge SD-WAN device (Cato Socket), a VPN client application or a web browser is offered for mobile devices, and IPsec tunnels connect cloud resources to the Cato Cloud. Regardless of edge, Cato's full set of networking and security capabilities is readily available from any Cato PoP.

Unified Management

SASE eliminates the need for multiple disparate point solutions by converging core networking and security capabilities in a single unified solution. These siloed point solutions each have their own operating systems, management interfaces, and command syntaxes, requiring expensive and scarce technical skills and staff that aren't typically available at branch locations and can provide only limited support to remote and mobile users.

The unified management console in SASE simplifies management of fully converged networking and security functions, thereby accelerating deployment, administration, and troubleshooting, while reducing security risks and outages due to misconfiguration and complexity.

REMEMBER

Cato provides a cloud-based, self-service management application to control the entire SASE service. It includes full network and security policy configuration, and detailed analytics on network traffic and security events. Self-service management is a unique advantage of Cato over legacy managed network services providers that require customers to submit tickets for any change to the network. If needed, Cato and its partners also offer managed service options. In all cases, Cato maintains the underlying SASE platform, so customers do not need to upgrade, patch, or otherwise maintain the Cato Cloud.

All Traffic

Your SASE vendor must support all types of enterprise network traffic, including WAN traffic between branch locations and on-premises datacenters, the Internet, and public/private clouds. Additionally, your SASE vendor should support all connection types including multiprotocol label switching (MPLS), fiber, broadband cable, digital subscriber line (xDSL), 4G Long-Term Evolution (LTE), and 5G cellular connections.

TIP

Cato integrates with major cloud providers, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform with secure IPSec tunnels. By using its global backbone to optimally route traffic from the edge to cloud providers, Cato eliminates the need for premium cloud connectivity solutions such as AWS DirectConnect and Microsoft Azure ExpressRoute. The Cato Socket can also route site-to-site traffic over MPLS and the Internet to address regional and application-specific requirements.

Deployment Flexibility

Whether you're undergoing a complete WAN transformation, planning a greenfield network design, or migrating (and adding) individual sites gradually, your SASE vendor should support a full range of deployment options with a zero-touch, turnkey solution that can be quickly and easily deployed by technical or non-technical staff at all your network locations.

TIP

The Cato Socket is a zero-touch, SD-WAN device that is easily and quickly deployed at customer sites. Customers can deploy Cato Sockets themselves or use Cato Networks or its partners for remote assistance or onsite support. After being connected in just minutes, a site is automatically configured with relevant networking QoS, security, and failover policies.

Resiliency

Enterprise networks typically rely on MPLS for business-critical connections between their headquarters, branch locations, and on-premises data centers. As the cloud becomes an increasingly important element of business strategies resilient connectivity to public cloud providers becomes more essential. Premium cloud VPN connectivity solutions such as AWS DirectConnect and Microsoft Azure ExpressRoute are available, but costly.

Your SASE vendor must provide resilient connectivity between all your datacenters, clouds, the Internet, locations, and users. Look for a SASE vendor with a global private backbone network, numerous PoPs in regions around the world, tier-1 carrier interconnects, and meaningful SLA guarantees to provide resilient connectivity for your enterprise needs.

TIP

The Cato Socket SD-WAN device connects a physical location to the nearest Cato PoP via one or more last mile connections. Customers can choose any mix of fiber, cable, xDSL, and 4G LTE/5G cellular connections. The Socket applies multiple traffic management capabilities such as active-active link aggregation, application- and user-aware QoS prioritization, dynamic path selection to work around link blackouts and brownouts, and packet duplication to overcome packet loss.

Elasticity and Scalability

Elasticity and scalability are key characteristics of the cloud. The cloud enables business agility by dynamically scaling cloud resources up and out based on demand using a consumption-based cost model. These characteristics are also important in a SASE solution.

Look for a SASE vendor that extends the cloud consumption model to its full suite of SASE networking and security services and provides elasticity and scalability to support your growth.

TIP

A truly elastic SASE vendor should offer equally available functionality across all SASE PoPs, seamless out-of-the-box high-availability functionality, and a proven record of continuous service growth.

Self-Healing

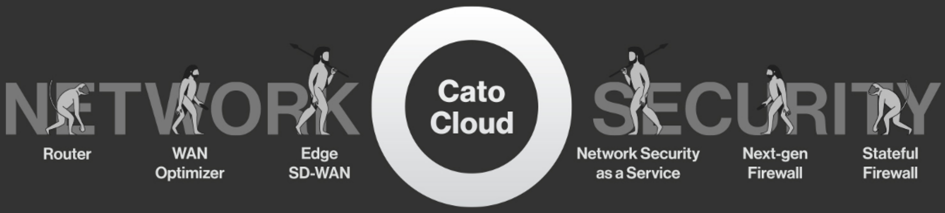
As with traditional network design, your SASE vendor must deliver a robust solution with no single points of failure and robust self-healing capabilities to automatically reroute network traffic in the event of a connectivity failure anywhere in the network — including the first, middle, and last mile.

TIP

The Cato Cloud backbone is continuously monitored and measured. Self-healing capabilities guarantee 99.999 percent service availability. Elastic, scale-up cloud software design principles assure seamless service infrastructure growth with minimal to no service downtime or disruptions.

CATO
NETWORKS

The World's First SASE Platform



Converged Capabilities

- Global Private Backbone
- Edge SD-WAN
- Security as a Service
- Cloud Integration and Acceleration
- Secure Remote Access (SDP/ZTNA)
- Unified Management

Key Use Cases

- Simple migration from MPLS to SD-WAN
- Optimized performance between global locations
- Direct, secure internet access everywhere
- Secure and optimize access to the cloud
- Cloud-scale remote access for everyone

CatoNetworks.com/SASE

Transform your business with a converged networking and security platform

Secure Access Service Edge (SASE) converges the functions of networking and network security point solutions into a unified, global, cloud-native service. With SASE, enterprises can reduce the time to develop new products, deliver them to the market, and respond to changes in business conditions or the competitive landscape. This book is your guide to addressing modern business needs with a comprehensive SASE solution.

Inside…

- Address the needs of digital business
- Learn what SASE is — and isn't
- Recognize the benefits of cloud-native networking and security
- Support all enterprise edges
- Achieve unified management
- Explore industry use cases

CATO NETWORKS

Lawrence C. Miller has worked in information technology for more than 25 years. He has written almost 200 For Dummies books. **Eyal Webber-Zvik** is Vice President, Product Marketing, at Cato Networks.

ISBN: 978-1-119-72154-3
Not For Resale

9 781119 721543

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT