aws marketplace

SECURITY WHITEPAPER

Secure Access Service Edge: A Three-Part Guide to Assess, Implement, and Optimize

Part 1

By SANS Institute Senior Instructor
Dave Shackleford

In collaboration with:

SANS

Introduction

This whitepaper is the first installment in the *Secure Access Service Edge: A Three-Part Guide to Assess, Implement, and Optimize* series written by SANS Institute senior instructor Dave Shackleford. The series is designed to help you determine if Secure Access Service Edge (SASE) is right for your organization.

In this whitepaper, Shackleford examines important considerations and best practices for SASE. You'll discover how to design your security architecture, how to determine organizational readiness, and key technologies and capabilities to look for when comparing SASE solutions.

The featured solutions for this use case can be found in AWS Marketplace:

netskope

CATO NETWORKS

paloalto NETWORKS

FORTINET

VERSA NETWORKS

Browse AWS Marketplace to discover these and other products that enhance your overall cloud security posture.

Learn more by visiting AWS Marketplace →

SANS | Research Program

White Paper

Secure Access Service Edge: Does It Make Sense?

Written by **Dave Shackleford**

August 2024

aws marketplace

Introduction

Over the past several years, many organizations have begun transitioning to cloud-based security services, particularly brokering services and controls that can provide web content filtering, malware detection and prevention, core network access controls, identity and access management solutions, and even browser emulation for end users. As organizations look to embrace more secure cloud-native and cloud-compatible connectivity and detection/response capabilities, it may make sense to review existing perimeter security technologies and consider a shift to a new combined option known as secure access service edge (SASE), which brings these capabilities and more together under a single provider.

The Challenge Today

As organizations shift into more platform as a service (PaaS) and infrastructure as a service (IaaS) workloads and services, many aspects of IT operations, architecture, and security are changing significantly. This shift is leading to the development of hybrid-cloud networks, requiring network engineering and security architecture teams to look at new controls and methods for developing and implementing network security practices in their environments.

As cloud services mature, however, there are more capable network security controls, platforms, and services that teams can employ to build and maintain robust network security architectures for a layered defense. Leading cloud service providers now offer highly capable cloud-native security controls, and third-party solution providers have adapted most network security platforms and services to cloud environments. Enterprises now have even more options for building secure network designs for hybrid and public cloud deployments.

In a modern hybrid-cloud model with routing and connectivity between data centers, branch offices, and cloud providers, most organizations are employing a layered defense model that includes cloud-native network access controls within the cloud service environments. This includes network traffic capture and security monitoring capabilities, and third-party platforms and services that can help to augment and centralize network security functions. Although there is no single network security architecture that works for all organizations, there are more options than ever for implementing a mature network security stack for cloud operations.

For a hybrid-cloud network that interconnects through a brokering solution, there are some architectural themes organizations should prioritize:

- **Build in security at every layer.** For a hybrid SASE-based cloud, numerous layers of network defenses should be in place. For internal infrastructure, traditional network controls like firewalls, intrusion prevention, and load balancing should be in place, and cloud environments should also be constructed with a layered defense strategy. However, given that the cloud is entirely software-based, some new and varied layers and controls may make sense as either augmentation or replacement strategies compared to on-premises controls (for example, the use of security group access controls that are assigned to workloads).
- **Design for resiliency.** Cloud operations tend to move at a fast pace, and more changes tend to occur in cloud environments than in many on-premises networks. Software-based infrastructure allows for more immediate feedback loops when unplanned or undesirable changes or conditions are detected, and automated recovery options for network access, traffic controls, and more can be implemented immediately.
- **Design for elasticity.** In the cloud, scaling operations for workloads will affect network capacity and operations, and any controls implemented (particularly those that process or control traffic flow) will need to scale automatically as well.
- **Centralize operations where possible.** For many network and cloud engineering teams, it's easy to encounter operational capacity challenges as the hybrid network expands and grows. Be sure to prioritize centralized platforms and tools that can be used across both on-premises and cloud environments where possible (for example, leading firewall platforms that can be implemented in all types of data centers).

A cloud provider should usually have some key technologies in place. For each layer of network security, it's critical to realize that many things will change when moving to the cloud, and these should factor into decisions regarding SASE providers and services offered. Some major considerations include the following:

- **Not all vendor products are adapted for your cloud provider.** Although many of the major providers have adapted their products into virtual machine formats or brokering models that may be available in the cloud, not all have.
- **Not all features and capabilities may be present in third-party solutions.** Even if a product or service is available in a cloud format, it may offer different features or capabilities than organizations are accustomed to. Additionally, some platforms may not offer deep integration with cloud provider APIs, limiting scalability and automation functionality.

- **Performance is defined by software attributes, not hardware.** Many network security platforms rely on specialized chips and hardware, which you won't have in cloud environments. You'll need to provide the appropriate amount of software/virtualized resources, and enterprise network and security teams should plan costs accordingly.
- **Some types of monitoring will likely need to employ cloud-native services.** For example, east–west traffic control and monitoring will be best accomplished with native services like virtual private cloud (VPC) flow logs and VPC traffic mirroring. All enterprise network security strategies will naturally leverage some types of cloud-native controls. These represent new skills to learn, syntax to master, and configuration options to implement and maintain over time.

Solution

SASE solutions should offer a range of capabilities and services that likely include:

- Secure Web Gateway (SWG) controls such as web content filtering and site reputation and threat intelligence
- Zero Trust Network Access (ZTNA) controls that can authenticate workloads and end-user systems, as well as provide behavioral analysis of access models and connectivity that can modify access controls dynamically based on specific scenarios and interaction
- Identity and access management (IAM) integration and role-based policies (which should include federation and SSO, as well as MFA support and more)
- Core network firewalling and access controls
- SaaS security controls similar to traditional cloud access security broker (CASB) solutions
- Software-defined wide area network (SD-WAN) connectivity options for interconnecting all locations, including cloud service environments, branch locations, traditional data centers, and end users

Organizations should perform an analysis of current technologies that comprise SASE—what do you have, and what do you need? It's very common for many enterprises to have a fairly disjointed vendor strategy that ends up being fragmented and difficult to manage, and can lead to increased costs. Security, network, and cloud engineering teams should evaluate marketplace offerings for SD-WAN, CASB, ZTNA, SWG, and more to determine whether a single option that is compatible with all use cases and business environments may make more sense.

SASE solutions should connect applications in different locations through a uniform "connectivity layer," so users can access all their applications, whether in the cloud or a data center. The connectivity layer should offer advanced application and user access control policies to provide access to the public cloud (PaaS and IaaS), SaaS apps, and data center applications. The brokering fabric delivers network protection controls in the "security service layer," including antimalware controls, intrusion prevention policies, and detection of exploits and malicious behaviors (similar to policies associated with leading next-generation firewall [NGFW] and network threat detection platforms traditionally used in on-premises data centers).

Conclusion

For any organization considering a move to SASE, consider how this type of solution will align with/contrast with/replace existing solutions and more legacy on-premises controls and services. Take the following into consideration:

- Are you already preparing to update and/or migrate existing controls and services in the most prevalent SASE capability categories?
- Are you considering SD-WAN as a replacement for more traditional WAN networking technologies like multiprotocol label switching (MPLS)?
- Are you seeking to unify security controls in a platform that can protect end users and branch locations from common online threats?
- Are the platforms compatible with existing cloud service environments, as well as identity and endpoint controls already in use?

Making the move to SASE is a major decision, and organizations should ensure the right mix of teams are aligned on how to best move forward.

Sponsor

SANS would like to thank this paper's sponsor:

aws marketplace

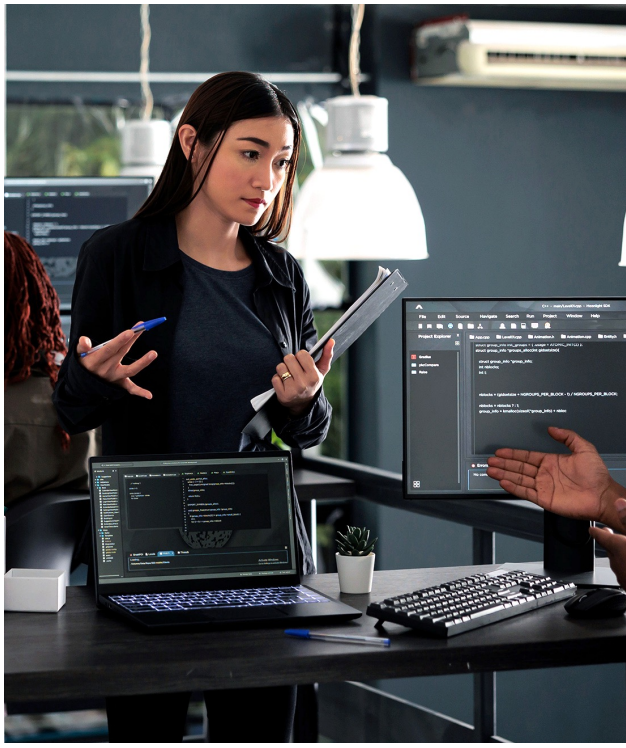
aws marketplace

Why use AWS Marketplace?

AWS Marketplace is a digital software catalog that makes it easy to find, try, buy, deploy, and manage software that runs on AWS. AWS Marketplace has a broad and deep selection of security solutions offered by hundreds of independent software vendors, spanning infrastructure security, logging and monitoring, identity and access control, data protection, and more.

Customers can launch pre-configured solutions in just a few clicks in both Amazon Machine Image (AMI) formats and SaaS subscriptions, with entitlement options such as hourly, monthly, annual, and multi-year contracts.

AWS Marketplace is supported by a global team of solutions architects, product specialists, and other experts to help IT teams connect with the tools and resources needed to streamline migration journeys to AWS.



How to get started with SASE solutions in AWS Marketplace

Download the rest of the series:

Secure Access Service Edge: *A Three-Part Guide to Assess, Implement, and Optimize*—Part 2

Download now →

Secure Access Service Edge: *A Three-Part Guide to Assess, Implement, and Optimize*—Part 3

Download now →

Discover solutions:

Find SASE security tools available to protect your AWS architecture

Visit AWS Marketplace →

Talk to an expert:

Speak to a solutions architect who can help solve your business challenges.

Get connected →

In collaboration with SANS