U.S. General Services Administration
Federal Acquisition Service (FAS)
Information Technology Category (ITC)
Enterprise Technology Solutions (ETS)
Technical Account Management Division (TAM)
Solutions Development (SD)

Secure Access Service Edge (SASE)

VERSION 1

AS OF JULY 2024

SASE Table of Contents

Secure Access Service Edge (SASE) Introduction

This technology book aims to provide an overview of Secure Access Service Edge (SASE) for United States (US) federal agencies. It contains a range of documents, including an executive summary, a white paper, use cases, and information on obtaining SASE products and services through GSA acquisition vehicles.

From its humble beginnings of moving secure access to an organization's cloud-based resources closer to the employees using those resources - and Gartner's coining of the SASE acronym in 2019 - to today's multipurpose driver in the cloud-based cybersecurity and other services spaces, SASE has undergone tremendous changes. Those changes continue to evolve and expand to the present day. GSA is providing to US government agencies the following as a general resource guide of SASE's place in IT Modernization efforts, along with GSA's recommendations for deploying SASE and how to purchase SASE from GSA's "Best in Class" (BIC) Indefinite Delivery Indefinite Quantity (IDIQ) Enterprise Infrastructure Solutions (EIS) contract and other contract vehicles.

1. EXECUTIVE SUMMARY

The Secure Access Service Edge (SASE) concept is the latest in enhanced security strategies and advanced toolsets that protect all users, devices, data, infrastructure, networks, and assets, no matter who is accessing them. SASE combines network and security measures into a single cloud-based service, improving accessibility, security, and controls. The growth in digital transformation makes SASE a key component in how agencies will manage and operate their networks in the future.

SASE is a Gartner framework consisting of key technologies; these include Firewall as a Service (FWAAS), Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Software Defined Wide Area Networks (SD-WAN), otherwise known as virtual network overlay services. Driving the adoption of a SASE platform is the migration to the cloud, or As-a-Service, and the growth of the remote workforce. These trends drive changes in agency security strategies and the methods used to protect the operating environments. In short, a SASE approach to network security acknowledges the need for the agency network operating environment to grow from a network perimeter security strategy to a strategy that focuses on policy enforcement points everywhere approach.

Because SASE incorporates network and security components, agencies must consider their existence in the current network environment, security postures, and agency-specific objectives for cloud-based services. While each agency is unique, there are common considerations to factor into decision-making:

1. **Single or Multiple Vendor Approach:** A single vendor reduces complexity and allows seamless handoff between the cloud and on-premise devices. A multiple-vendor approach provides broader access to providers with specialized skills and experience with individual component areas.
2. **Adaptive SASE Solutions:** These provide flexibility to meet an agency's unique needs.
3. **User Access Controls:** An agency should utilize a ZTNA solution and implement an agency-wide policy to authenticate users anywhere, provide access to specific applications, and allow for the appropriate monitoring, prevention, and countermeasures.
4. **Integrated Security Policy Enforcement:** The agency applies this approach within its SASE solution, and it is a factor in the broader network and security architecture.
5. **Evolving Threat Intelligence:** Integrated modern SASE security tools designed to keep up with the evolving threat landscape. These tools include manual controls, scripts, and limited threat intelligence tools using Artificial Intelligence (AI) driven Threat Intelligence.

6. **Use Case Considerations:** A SASE solution should meet specific agency requirements for cloud-based management, network agility, secure internet access, secure Software as a Service (SaaS), and flexible onboarding.

Developing detailed requirements is critical to determining which SASE solution is right for all levels of an agency's enterprise environment. Comprehensive stakeholder engagement is essential to ensure consideration and documentation of factors across the enterprise when designing and implementing a SASE solution. Selecting the right solution can be overwhelming, especially when considering whether to integrate existing components or, as more fully explained below, migrate to a single SASE provider solution, a multiple provider SASE solution, or even a hybrid SASE provider solution. Developing detailed requirements is the key.

2. SASE STRENGTHS, WEAKNESSES, OPPORTUNITIES, AND THREATS (SWOT) ANALYSIS

The Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis is a technique in strategic planning to help identify and focus on strengths, weaknesses, opportunities, and threats for an initiative or project. The following SASE strengths, weaknesses, opportunities, and threats are below:

TABLE 1 - SWOT ANALYSIS

Strengths	Weaknesses	Opportunities	Threats
Network & security cloud-based integration	Integrating legacy with cloud-based platforms	Collaboration of network and security teams	Skills management
Network performance & optimization	Fragmented and confusing ecosystem	Improved user experiences	Non-redundant, malfunctioning system failures
Enhance security capabilities	Performance of network security protocols & fragments in cloud environments	Zero Trust Architecture	Provider technical issues impact to enterprise
Increased agility	Complex procurement	Enhanced security visibility & controls	Lack of agency control in the cloud environment

STRENGTHS

The SASE platform components offer an integrated approach to network management and security for a cohesive networking environment that supports the growing migration to cloud services. Because of the way the SASE components work together, SASE allows agencies the flexibility to scale operations up or down as needed. Network performance improves by allowing access to cloud solutions without the need to pass through an agency data center while maintaining security at the edge of any device, regardless of the location. The increase in visibility and "real-time" control available to agencies offers the ability to optimize traffic using SASE tools' enhanced capabilities.

WEAKNESSES

SASE weaknesses may present when integrating legacy systems with cloud-based solutions and security. If poorly coordinated, this integration can create a fragmented ecosystem and confuse teams. Moreover, teams must prevent disruptions in legacy network operations through cloud-based security integration. Security strategies must go beyond the network perimeter and factor security at the edge to accommodate remote and mobile users. SASE can create complexity when attempting to procure a complete solution that may or may not involve multiple vendors. The selection of a single provider ensures greater accountability for all components.

OPPORTUNITIES

SASE opportunities include a meeting of the minds between network and security teams to create a cohesive enterprise operation that complements both environments. Implementing SD-WAN with a Zero Trust Architecture (ZTA) approach enhances network management capabilities, applies changes faster, and ensures security regardless of where or how a user connects. Implementing a SASE platform approach expands user connectivity options and offers flexibility when accessing information systems.

THREATS

Threats for SASE include the limited knowledge of working in an integrated cloud environment and the failure to proactively plan for and provide training to network and security resources. A more significant concern is the vulnerability of a single point of failure (SPOF) of non-redundant or sole provider technical issues or malfunctions. If not effectively managed, this could cause an entire failure of the networking ecosystem. Lack of agency control in a SASE environment threatens agency-specific policy and protocol enforcement. Procurements should address this issue as a SASE solution requirement.

3. OVERVIEW OF SECURE ACCESS SERVICE EDGE (SASE)

SASE is an identity-driven service that enables agencies to authenticate users via robust digital identity capabilities. SASE incorporates distinct cloud security tools and components to proactively identify and remediate security threats. The core SASE components are essential to managing and protecting network traffic, users, applications, devices, and infrastructure.

FIGURE 1: NETWORK AND SECURITY SERVICES

SASE bundles various network and security services using the requestor's digital identity to determine access to the environment and information. SASE is a cloud security platform designed to meet the evolution of digital transformation, cloud services, and a remote or mobile workforce. The diagram below shows the integration of the network and security core components that make up a SASE solution:

1. **Firewall as a Service (FWaaS)** – An advanced Layer 7 next-generation firewall (NGFW) used to protect networks and cloud infrastructure. FWaaS capabilities secure WAN and LAN traffic using access controls, advanced threat protection, intrusion prevention systems (IPS), and DNS security.

2. **Secure Web Gateway (SWG)** – Defends against malicious web traffic and malware.
3. **Zero Trust Network Access (ZTNA)** – ZTNA protects remote users and agency data and enforces security policies dynamically through Policy Enforcement Point driven access.
4. **Cloud Access Security Broker (CASB)** – Protect cloud-based traffic flow with zero-trust access control and policy enforcement in the cloud environment.
5. **Software Defined Wide Area Networks (SD-WAN)** – SD-WAN offers a virtualized network architecture that sits above the physical connection and allows enterprises to leverage tools that help to connect users to applications securely.

Whether an agency utilizes a single-vendor approach or consolidates multiple vendor solutions to combine network and security services, the SASE approach uses the latest technologies to advance traditional network and security management tools and secure the evolving digital landscape. SASE is built on a framework, so the solution is a real-time snapshot unique to each agency.

4. EXECUTIVE BRIEFING

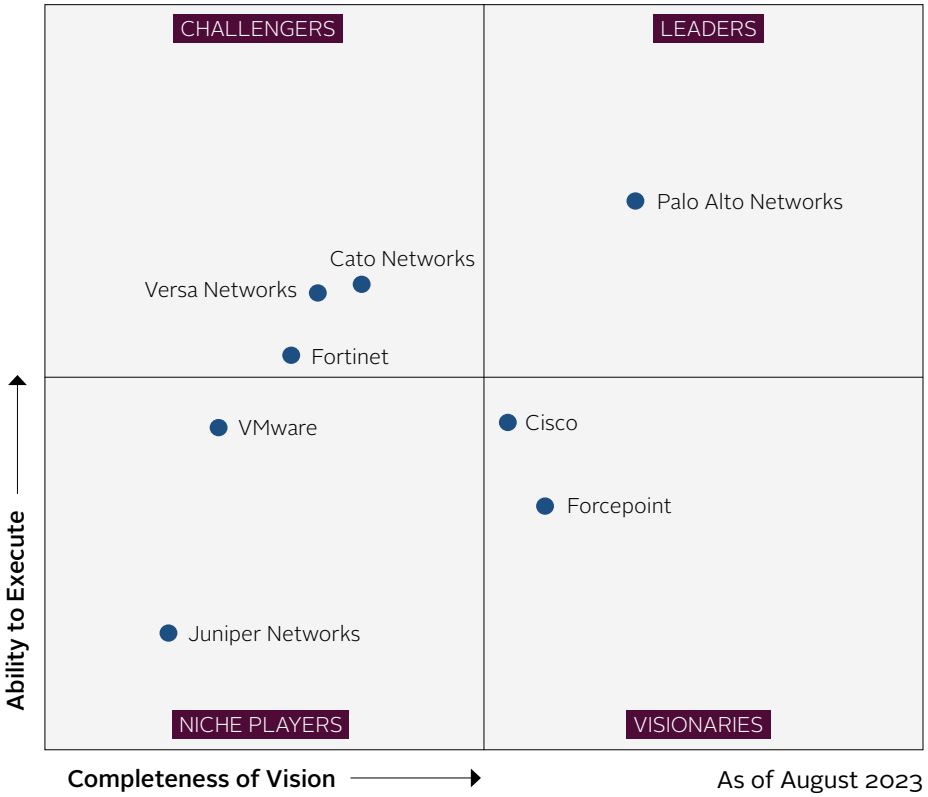
Agencies have an opportunity to optimize their operating environments with SASE. SASE allows agencies to release themselves from the limitations of service delivery dependency on legacy hardware-based networks and data center-driven architecture. These limitations are removed even with a network delivered set of cloud services. The workforce is now unrestricted within the network perimeter, and agencies are often migrating more services to the cloud. This unrestricted workforce and migration to cloud services allows for greater ease in administering updates, making changes, and timely availability of services to the end user. The remote and mobile workforce is driving a change that requires an innovative approach to security; SASE provides this by combining network and security tools in a cloud environment.

- SASE provides greater network visibility and controls while enhancing the overall user experience.
- Consolidation is a cost-effective strategy for SASE implementation. Engaging enterprise stakeholders (Leadership, policymakers, network, and security) is essential to success.

Gartner's 2021 Emerging Technologies and Trends Impact Radar: Security[1] shows SASE Mass high because SASE has a direct impact on the future of its five contributing market segments: SD-WAN, Firewall As-a-Service, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Zero Trust Network Access (ZTNA); predicting that they will largely go away, eventually engulfed by SASE (1 to 3 years). According to Gartner: "Security leaders need to employ a proactive or offensive cyber defense focus to protect against evolving attack methods because detection and response focused on security measures alone will not keep pace."

1 Emerging Technologies and Trends Impact Radar: Security, Gartner, October 12, 2021

FIGURE 2: MAGIC QUADRANT FOR SINGLE-VENDOR SASE



Gartner identifies industry leaders in their Magic Quadrant for Single Vendor SASE[2]. While vendors may offer a single-vendor solution, Gartner found that they often do not provide breadth and depth functionality with integration across all components, a single management plane, and a unified data model and data lake. SD-WAN providers have added a cloud-based security stack to their offerings. In contrast, Security Service Edge (SSE) providers have acquired SD-WAN to deliver single-vendor SASE. Gartner identifies three primary options for SASE adoption (single vendor, explicit pairing of two vendors (network/security), and a managed SASE; smaller enterprises prefer the single vendor approach. By 2025, Gartner estimates that 80% of enterprises will have adopted a strategy to unify web, cloud services, and private application access using a SASE/SSE architecture, up from 20% in 2021.

SASE has the following four defining traits[3]:

1. **Global SD-WAN service:** SASE uses an SD-WAN service with a private backbone, which avoids latency issues from the Internet and connects the individual points of presence (POPs) used for security and networking software.
2. **Distributed inspection and policy enforcement:** SASE services do not just connect devices; they protect them. Inline traffic encryption and decryption are a minimum requirement.
3. **Cloud architecture**: SASE services should use cloud resources and architectures with no specific hardware requirements but should not include service chaining. Software should be multi-tenant for cost-effectiveness and able to instantiate for rapid expansion.
4. **Identity-driven**: SASE services have access based on user identity markers, such as specific user devices and locations, instead of the site.

5. GSA IS HERE TO HELP

If you would like more information on the topics covered in this paper, please contact your designated GSA representative at https://gsa.gov/nspsupport or call 855-482-4348 to get in touch. GSA offers multiple products, services, and solutions to support your planning, implementation, and continued support of the components of your SASE.

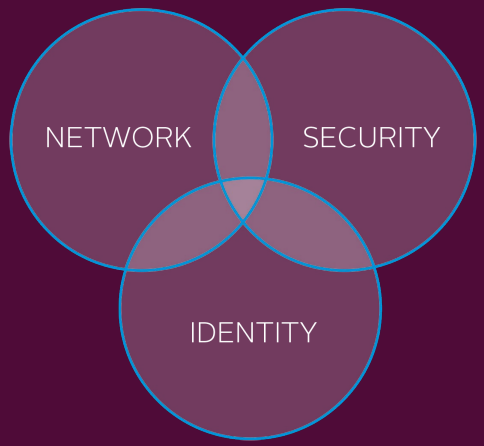
2 Gartner, Magic Quadrant for Single-vendor SASE, August 2023

3 SASE, TechTarget, Kina Yasar, Technical Writer, Amit Bareket, Perimeter 81,

Secure Access Service Edge (SASE) Slip Sheet

SASE HIGHLIGHTS

SASE is an identity-driven service that enables agencies to authenticate users via robust digital identity capabilities. SASE incorporates distinct cloud security tools and components to proactively identify and remediate security threats. The core SASE components are essential to managing and protecting network traffic, users, applications, devices, and infrastructure elements. The five core SASE components:



- **Firewall-as-a-Service (FWaaS)**: Secures WAN and LAN traffic.
- **Secure Web Gateway (SWG)**: Defends against malicious web traffic and malware.
- **Zero Trust Network Access (ZTNA)**: Protects remote users and enforces security policies dynamically.
- **Cloud Access Security Broker (CASB)**: Protect cloud-based data.
- **SD-WAN solutions**: Virtual Network Overlays.

BUSINESS VALUE

SASE is essential to secure the evolving digital landscape, migrate to cloud services, and accelerate remote and mobile work capabilities.

- Ensure Robust Network Performance, User Experience, and Security
- Maintain Higher Visibility and Control in the Cloud
- Protect Against Cloud-Enabled SaaS and Web Threats
- Prevent Data Exposure, Theft, and Insider Risk
- Achieving Cost Savings and Operational Efficiencies

FOR MORE INFORMATION: Contact your designated GSA representative at www.gsa.gov/nspsupport or call 855-482-4348.

CONTRIBUTORS: General Services Administration (GSA), JPI Solutions (JPI)

RECOMMENDATIONS

Infrastructure and operations leaders responsible for cloud and edge connectivity strategies should:

- Engage the security organization and establish a cross-functional SASE strategy team to speed the time to value and increase the chances of a successful implementation.
- Choose single-vendor SASE offerings that provide single-pass scanning, a single unified console, and a data lake covering all functions to improve user experience and staff efficacy.
- Evaluate a single-vendor SASE offering and two explicitly partnered vendors, and manage SASE offerings to provide the most flexibility in selection and timing.
- Have the SASE team rank RFI/RFP requirements based on what is mandatory versus preferred or optional to understand the trade-offs when using a single-vendor SASE offering; the offering may not be best of breed in all areas.
- Run a functional pilot with real-world users and locations before selecting a single-vendor SASE offering to ensure functionality and performance meet requirements.

HOW TO GET

GSA provides access to contract vehicles, such as Enterprise Infrastructure Solutions (EIS), with services available to customize a solution to fit your SASE needs:

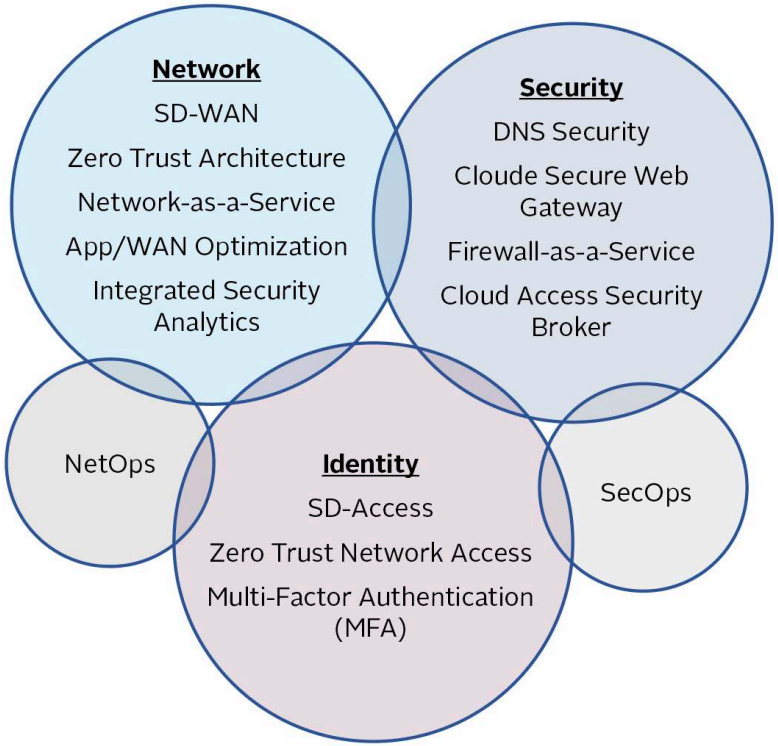
- **Managed Services:** Managed Network Service (MNS) and Managed Security Services (MSS)
- **As-a-Service cloud offerings:** Network as a Service (NaaS), Software as a Service (SaaS)
- **Ancillary Services:** Service Related Equipment (SRE), Service Related Labor (SRL)
- **Professional Services:** Program, project, and technical as needed

Secure Access Security Edge White Paper

INTRODUCTION

Secure Access Service Edge (SASE)[4] is a term coined by Gartner analysts Neil McDonald and Joe Skorupa in a July 2019 networking hype cycle and market trends report, as well as a Gartner report in August of the same year. The SASE framework leverages five core components: Firewall as a Service (FwaaS), Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), CASB, and Software Defined Wide Area Networks (SD-WAN), which are key to the adoption of innovative modernization of network and security operations. These integrated core components span across an agency's Information Technology (IT) network, security, and identity areas of operation.

FIGURE 1: COMPONENTS OF SASE



SASE incorporates distinct cloud security tools and components that offer extensive and robust functionalities, including:

- Managing network traffic, users, applications, devices, and infrastructure components;
- Enabling companies to authenticate users via robust digital identity capabilities, and
- Proactively identify and remediate security threats.

4 Wikipedia, December 2023

A subset of SASE is Gartner's Security Service Edge (SSE) Magic Quadrant, which addresses access to the web, cloud services, and private applications regardless of a user's location. SSE aims to provide a consolidated network security architecture in a single solution[5].

A Managed Threat Detection and Response (MDR) service is another component worthy of attention in this multi-layer defense environment. A growing workforce and explosion of IT and IoT endpoints rapidly expand an organization's attack surface[6]. MDR security platforms provide turnkey, remotely delivered, 24/7 security operations center (SOC) capabilities. They are usually cloud-managed, combining advanced analytics, threat intelligence, and human expertise to contain threats. Security and risk leaders should look for specific features and capabilities unique to an organization's security situation. The core capabilities of an MDR solution that make it essential to a SASE solution include:

- Enterprise-wide endpoint visibility
- Advanced threat detection
- Signal fidelity
- Incident Response capabilities
- Global threat visibility and threat intelligence

FEDERAL GUIDANCE AND EFFORTS SUPPORTING SASE

Executive Office of the President, Office of Management and Budget (OMB), released Memorandum M-22-09 on January 26, 2022, *Moving the US Government Toward Zero Trust Cybersecurity Principles*, setting forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal year (FY) 2024 to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns targeting Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government. The foundational tenet of the ZTA model is that no actor, system, network, or service operates outside or within the trusted security perimeter. This strategic approach significantly emphasizes stronger enterprise identity and access controls, including multi-factor authentication (MFA). SASE embraces these same principles.

The National Institute of Standards of Technology (NIST), SP 800-215, Guide to a Secure Enterprise Network Landscape, provides guidance on the new enterprise network landscape from a secure operations perspective. It specifically references the consideration of security feature enhancements to traditional network appliances in the form of point security solutions, network configurations for various security functions, security frameworks that integrate these individual network configurations, and the evolving wide area network (WAN) infrastructure to provide a comprehensive set of security services for the modern enterprise network landscape (e.g., SASE). Section 6: Secure Wide Area Network Infrastructure for Enterprise Network references SD-WAN, Cloud Access, and Integrated Security Services Architecture.

THE SASE LIFECYCLE PHASES

A. Emerging – SASE is becoming the go-to approach to Network and Security services in an increasingly mobile market that utilizes cloud-based services. The ability to process information from any location and device and rapidly share the information in real-time will further drive SASE. For example:

5 Check Point, SSE vs SWG,
6 Who are the Top 10 MDR Providers, Netify, Robert Sturt, January 21, 2022

i. Research and Development - Quantum SASE offers greater scalability and efficient delivery of internet security 2x faster than today's SASE solutions. Combined with full mesh Zero Trust Access and optimized SD-WAN performance, the prominent Quantum SASE value is its ease of use.

ii. Early Solutions—SASE has increased with the migrations to cloud services and remote working. Agencies are integrating SASE components paralleled with broader edge computing (SSE), SD-WAN, and the adoption of Zero-Trust technologies. The Cybersecurity and Infrastructure Security Agency (CISA) provides guidance on how organizations can utilize the Zero Trust Maturity Model 2.0 in designing and implementing a zero-trust architecture, which includes a focus on Policy Enforcement Points in the operational environment.

B. **Initial Adoption** – For years, agencies have modified how they do business and provide services to their end-users and partners. This modification has resulted in an approach that creates silos of functional network and security applications. This approach has worked to date, although it brings added costs, inefficient cyber protections, and latency in delivering services to end-users.

C. **Broad Acceptance** – The rise of cloud services and remote working has driven the need to evolve security approaches across the enterprise as adopted under Trusted Internet Connection (TIC) 3.0. For example, security at Policy Enforcement Points (PEPs) is a method to protect network environments, devices, data, and users regardless of the access point or method used.

D. **Decline** – The consolidation of Network and Security services will drive out separate service and support team silos and foster greater coordination and collaboration across operational areas.

E. **End of Sale** - Vendors no longer sell or install the service. For example, edge devices, line cards, and chassis will not have an end-of-life, but legacy hardware may sunset.

F. **End of Life** – SASE continues to evolve, and end-of-life will include early versions or solutions for SASE.

G. **Additional Application Paths** – Because SASE is the convergence of multiple components, each component will evolve. Upgrades to existing SASE components will require agencies to integrate and update specific elements of the SASE solution or redesign their existing SASE framework. The foregoing may drive agencies toward a single-vendor solution to minimize complexity.

NOTE: Zero Trust Network Access is a Zero Trust Architecture (ZTA) component for more information.

TECHNICAL SPECIFICATIONS

The SASE technical specifications are unique to each agency's enterprise architecture and integration of the five core SASE components:

1. **Zero Trust Network Access (ZTNA)** – Protects remote users and enforces security policies dynamically, utilizing an identity and access management process at network-segmented policy enforcement points where the device, endpoint, applications, and data security are applied.

2. **Cloud Access Security Broker (CASB)** – Protects cloud-based data using on-premises or cloud-hosted software or hardware between the cloud solution provider and the end user.

3. **SD-WAN solutions –** Provides centralized management and visibility using software-defined networking concepts to distribute network traffic across the network and connect branch offices and users to agency data centers or cloud-based and SaaS applications.

4. **Secure Web Gateway** (SWG) – Designed to implement and enforce an organization's web security policies and defend against malicious web traffic and malware. A SWG utilizes an on-premise or cloud-based service between the user and the Internet to inspect web requests and block malicious applications and websites, making them inaccessible.

5. **Firewall as a Service** (FWaaS) – Secures WAN and LAN traffic using a cloud-based service that provides hyperscale, next-generation firewall (NGFW) capabilities, including web filtering, advanced threat protection (ATP), intrusion prevention system (IPS), and Domain Name System Security (DNS)[7].

FIGURE 2: CORE SASE COMPONENTS

The SASE technical specifications directly relate to whether a single-vendor, multi-vendor, or hybrid approach best meets agency requirements. Technical specifications unify network and security operations by integrating components and streamlining operations. The SASE solution must create a streamlined and secure network architecture that spans from central headquarters to remote locations and mobile end users.

SASE allows consistent and ubiquitous delivery of security policies by applying a zero-trust policy for every connection between entities and the apps/services they are trying to access. Thus, organizations can easily meet industry compliance and organization defined security standards to meet their business needs. Below are some considerations for evaluating SASE Solutions.

- Ability to integrate within the existing ecosystem
- Built on a secure architecture that is flexible, scalable, and adaptable for maximum performance
- Cloud-based solution with multi-service and multi-tenant capabilities at scale
- Solution with centralized policy configuration and management with distributed security enforcement (e.g., PEPs)
- A robust intrusion detection/prevention security stack coupled with an advanced Firewall as a Service
- Combines SD-WAN, routing, and encryption with single operating system security capabilities
- Analytics that provide full visibility for every component of the SASE ecosystem
- SaaS delivered solutions that enable dynamic scalability to meet customer needs and deliver optimal performance
- Leverage Artificial Intelligence (AI)/Machine Learning (ML) to identify and utilize the security policy enforcement point closest to the user/device from which the requested application is accessed.
- The complexity of managing networking and security integration into a unified SASE architecture
- Cost and time-intensive process of replacing existing legacy systems with a SASE framework
- Accommodating growing network traffic and user demands by effectively scaling the SASE solution

7 What is FWaaS?, Fortinet,

RECOMMENDED ACTIONS FOR AGENCIES

Infrastructure and operations leaders responsible for cloud and edge connectivity strategies should:

- Engage the security organization and establish a cross-functional SASE strategy team to speed the time to value and increase the chances of a successful implementation.
- Choose single-vendor SASE offerings that provide single-pass scanning, a single unified console, and a data lake covering all functions to improve user experience and staff efficacy.
- Evaluate a single-vendor SASE offering and two explicitly partnered vendors, and manage SASE offerings to provide the most flexibility in selection and timing.
- Have the SASE team rank Request for Information (RFI)/Request for Proposal (RFP) requirements based on what is mandatory versus preferred or optional to understand the trade-offs when offering a single-vendor SASE; the offering is not best of breed in all areas.
- Run a functional pilot with real-world users and locations before selecting a single-vendor SASE offering to ensure functionality and performance meet requirements.

CONCLUSION

SASE will continue to play a key role in the evolution of IT and the modernization of enterprise networks. Moreover, SASE is a critical enabler of secure cloud-based solutions and innovation. Automation, consolidation, and migration of network and security solutions are key to keeping pace with the rapidly changing environment and growing end-user expectations. The challenge to agencies is determining the best deployment approach to meet their unique requirements.

SASE Use Cases

The challenge facing most agencies regarding SASE is deciding what approach works best in their environment[8]. While a multitude of strategies are available, consider these three approaches.

- Single-vendor Approach
- Multi-vendor Approach
- Hybrid Approach

FIGURE 1: SASE USE CASE APPROACHES – PROS AND CONS

Single Vendor SASE	
PROS	**CONS**
Simplicity & Ease of Management	Limited Choice & Flexibility
Best performance & optimization	Vendor Lock-in
Improved Supportability	Lacks Best-of Breed
Lower Total Cost of Ownership (TCO)	

Multi-Vendor SASE	
PROS	**CONS**
Best of Breed Options	More Complex
Greater Flexibility	Varying Levels of Interoperability
Better Reliability	Disjoined Administration
Workforce Adaptable	High Traffic Latency
	Higher Total Cost of Ownership (TCO)

Hybrid SASE	
PROS	**CONS**
Specialized Expertise	Separate Network & Security Teams
Increased Flexibility	Integrated Interoperability
Reliability	Increased Network Latency
Supports Hybrid Workforce	Degraded User Experience
	Higher Total Cost of Ownership (TCO)

A. SINGLE-VENDOR APPROACH

A Single-vendor approach and consolidation of SASE components offers a streamlined, cost-effective, and flexible approach with centralized controls for administration and policy enforcement on-premise and in the cloud.

8 Single-Vendor vs. Two-Vendor SASE: Which Is Right for Your Business?, Vmware, Shoaib Yusuf, March 28, 2023

BENEFITS OF A SINGLE-VENDOR APPROACH

- **Single Source of Truth**: A single-vendor solution is easier to achieve and allows teams to focus on problem-solving and achieving goals.
- **Better Data Correlation**: Provides a better understanding of data flowing across workspaces and how to deal with issues.
- **Expedited Root-Cause Analysis**: A comprehensive view allows for rapid root-cause analysis and issue resolution.
- **Easier Identification of Security Breaches**: Improved visibility increases an agency's ability to stay on top of breaches and anomalies, with an additional capability to predict potential breaches.
- **Minimize Downtime and Lost Revenue**: A streamlined source of information fosters better understanding and the ability to quickly identify and resolve issues, decreasing downtime and revenue loss.
- **Reduced CapEx and OpEx**: Fewer tools and licenses equal reduced cost resulting from a well-planned tool consolidation strategy.

CHALLENGES OF A SINGLE-VENDOR APPROACH

- **Single Point of Failure**: This approach completely relies on one vendor, leaving the agency vulnerable should the vendor system(s) fail.
- **Functional Weaknesses**: A single vendor may have gaps in functionality and limited flexibility to meet an agency's needs. These weaknesses are especially evident in an evolving digital landscape.
- **Vendor Lock-in**: Switching vendors can be difficult and costly once implemented with a single vendor.
- **Limited expertise**: Network and Security domains are quite different, which makes finding a single vendor with a prominent level of expertise in both exceedingly difficult. Vendors often excel in only one of the two areas and gravitate toward capabilities based on their specific, unique expertise.

A single-vendor approach is usually more suitable for smaller agencies that have minimal network and security silos and limited resources. The simplicity and lack of complexity also lead to easier deployment.

2. MULTI-VENDOR APPROACH

A Multi-vendor approach may best meet the needs of various organizations within an agency. This approach benefits a larger networking environment with greater information technology (IT) resources. A multi-vendor approach involves at least two vendors providing all the SASE functionality, often focusing on the Network and another on security.

BENEFITS OF A MULTI-VENDOR APPROACH

- **Specialized Expertise:** A multi-vendor approach allows the agency to select the best vendors in their area and focus more on that segment. This approach allows for greater potential to quickly adapt and integrate innovative solutions to meet evolving industry requirements.
- **Increased Flexibility:** Multiple vendors provide greater flexibility to meet specific agency needs and the ability to switch vendors if needed with minimal disruption to the other segment. A network solution is often easier to swap than a security solution.
- **Reliability:** Network and security maintenance, such as upgrades or configuration changes, performed independently without impacting departments

CHALLENGES OF A MULTI-VENDOR APPROACH

- **Separate network and security teams:** A Multi-vendor approach adds complexity and often requires added IT resources to manage and maintain the solution. The impact is a greater susceptibility to misconfigurations, implementation issues, and delayed deployment. It may also lead to challenges in isolating and identifying root causes, resolving problems, accessing logs, and sharing incident information.
- **Interoperability:** An agency may find it difficult to ensure that varying vendor approaches will result in interoperability between network and security solutions. This approach requires greater coordination in integrating, implementing, and maintaining the SASE environment.
- **Network Traffic Latency:** Traffic traversing multiple hops to process specific network or security processing of routing and security decisions can increase latency and bandwidth availability, ultimately impacting the user experience.
- **Total Cost of Ownership**: A multi-vendor approach often results in higher-cost solutions, fewer discount options, and greater administration costs.

Integrating network and security components is essential to ensure a sound operational mesh of functionality when working with multiple vendor solutions. A multi-vendor solution may also hinder digital transformation and adherence to security regulations and compliance across the enterprise.

C. HYBRID APPROACH

The Hybrid SASE approach allows for incremental implementation toward a full SASE environment. A Hybrid approach does not require agencies to transition all security assets to a cloud-based solution at one time and supports both hardware-based and cloud-based solutions. This approach best suits a hybrid work environment that factors integrated architectures with program-specific requirements into operations.

BENEFITS OF A HYBRID APPROACH

- **Centralized visibility and policy management:** Provides enterprise-wide security operations and policy enforcement during the transition to a full SASE deployment.
- **Hybrid Workforce:** Enables network and security operations to maintain a positive user experience and data protection unique to on-premise and remote workers.
- **Flexible Reliability:** It supports various approaches to accessing the Internet and cloud services, utilizing an integrated approach of SASE components.

CHALLENGES OF A HYBRID APPROACH

- **Tool Sprawl:** Often includes a maintained and managed patchwork of multi-vendor network and security solutions, resulting in integration challenges and complexity.
- **Performance:** Maintaining network performance while ensuring security visibility and protections often impacts the overall user experience.
- **Cost:** Often includes a maintained and managed patchwork of multi-vendor network and security solutions, resulting in integration challenges and complexity.

A Hybrid SASE approach relies on a solid foundation of zero-trust network architecture to maintain visibility and controls for data, threat, and risk management. Today's hybrid workforce warrants addressing access to the Internet and services beyond the traditional use of disparate network and security appliances, Virtual Private Network (VPN) and Multiple Protocol Layered Service (MPLS) split-tunneling, and a latency hindered user experience.

D. CONCLUSION

The agency's needs drive the approach to SASE, as do the size of the networking environment and budgetary constraints. Each approach brings benefits and challenges in deployment with varying degrees of complexity. While the single-vendor approach is less complex, it hinders the agency's access to best-of-breed providers by locking in one vendor. The multi-vendor approach allows an agency to access the best of breed. Still, it brings added complexity to deployment and management between the network and security teams. The Hybrid approach allows an agency to leverage existing on-premise resources, is the most complex of the three approaches, but offers incremental deployment of a SASE framework. A few looming considerations remain:

- Does it make sense to integrate existing components or migrate to a single SASE provider?
- How will enhanced capabilities, such as increased visibility and "real-time" controls, benefit the agency's ability to optimize the operating environment?
- What is the SASE cost-benefit and return on investment?

Regardless, Gartner predicted that by 2023, a 70% deployment rate of all enterprise workloads in cloud infrastructure and platform services. The agency's best approach will consider many factors determined through matrixed collaboration on requirements across network and security teams and key stakeholders.

GSA IS HERE TO HELP

If you would like more information on the topics covered in this paper, please contact your designated GSA representative at https://gsa.gov/nspsupport or call 855-482-4348 to get in touch. GSA offers multiple products, services, and solutions to support your planning, implementation, and continued support of the components of your SASE. Thank you for reading!

How to Get SASE

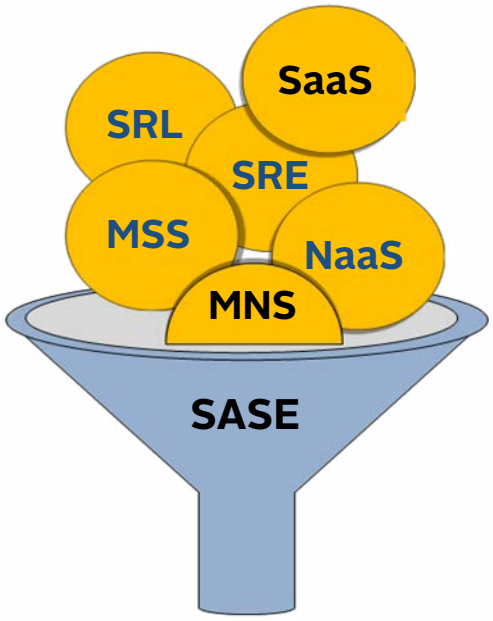
1. ORDERING GUIDANCE

Developing specific agency requirements for SASE is a critical first step. This step requires that an agency understand the current environment and its goals for the future environment. What does this mean?
Critical decisions regarding:

- Network Architecture – traditional/ZTNA
- Security Posture and Policy
- Consolidation of services
- On-premise, cloud-based, or a hybrid approach
- Single-vendor, multi-vendor, or hybrid solutions

Regardless of the approach, GSA has Best-in-class (BIC) contract vehicles, such as Enterprise Infrastructure Solutions (EIS), available to customize a solution to best fit your SASE needs:

FIGURE 1: SASE PRICING COMPONENTS



- Managed Network Service (MNS)
- Managed Security Services (MSS)
- As-a-Service cloud offerings: Network as a Service (NaaS), Software as a Service (SaaS)
- Service Related Equipment (SRE)
- Service Related Labor (SRL)
- Professional Services

These EIS services combine on an individual case basis (ICB) to customize the solution and integrate industry leaders in SASE using Task Order Unique CLINs (TUCs) that allow flexibility.

SASE Lessons Learned and Frequently Asked Questions (FAQ)

1. LESSONS LEARNED

- Engage all the right stakeholders: Leadership, Engineering, Network Operations, and Systems/Applications.
- Leverage the cloud-based security tools and apply consistent security policies.
- Include data loss prevention rules and consider Artificial Intelligence (AI) and Machine Learning (ML) technologies.
- Pre-test your SASE before full migration; include integrated solutions (e.g., SD-WAN).
- Begin by focusing on one thing, such as internet-bound access, and then move to other priorities.

2. FREQUENTLY ASKED QUESTIONS (FAQ)

What is SASE?

SASE is a cloud-native architecture that unifies SD-WAN with security functions like SWG, CASB, FWaaS, and ZTNA.

What are the architectural requirements of SASE?

SASE has four main characteristics: cloud-native, supports all edges, identity-driven, and globally distributed.

Can an agency deploy SASE without SD-WAN?

In simple terms, no; SASE relies on the SD-WAN network optimization and native cloud security features.

How is SASE different from CASB?

CASB is a Software as a Service (SaaS) application. SASE provides full network and security integration.

Are multi-factor authentication (MFA) and identity access management (IAM) a part of the SASE solution?

SASE combines components to include Zero Trust; MFA and IAM fall under this security area.

What should an agency consider before migrating to a SASE environment?

An agency should consider the following: its current cloud security capabilities, the type and volume of Internet and accounting for the cloud traffic, its inventory of security stack policies and consoles, and its enterprise goals and objectives.

3. ACRONYMS

Acronym	Description
AI	Artificial Intelligence
API	Application Programming Interface
BIC	Best In Class
CapEx	Capital Expense
CASB	Cloud Access Security Broker
CDN	Content Delivery Network
CISA	Cybersecurity and Infrastructure Security Agency
DNS	Domain Name System
EIS	Enterprise Infrastructure Solutions
FAQ	Frequently Asked Questions
FWAAS	Firewall as a Service
FY	Fiscal Year
GSA	General Services Administration
ICB	Individual Case Basis
IPS	Intrusion Prevention System
IT	Information Technology
LAN	Local Area Network
MFA	Multi-Factor Authentication
MDR	Managed Threat Detection and Response
ML	Machine Learning
MNS	Managed Network Service
MPLS	Multiple Protocol Layered Service
MSS	Managed Security Services
NaaS	Network as a Service
NGFW	Next-Generation Firewall
NIST	National Institute of Standards of Technology

Acronym	Description
OMB	Office of Management and Budget
OpEx	Operational Expense
PEP	Policy Enforcement Points
RBI	Remote Browser Isolation
RFI	Request for Information
RFP	Request for Proposal
SaaS	Software as a Service
SASE	Secure Access Service Edge
SD WAN	Software Defined Wide Area Networks
SOC	Security Operations Center
SPOF	Single Point of Failure
SRE	Service Related Equipment
SRL	Service Related Labor
SSE	Security Service Edge
SWG	Secure Web Gateway
SWOT	Strengths, Weaknesses, Opportunities, and Threats
TIC	Trusted Internet Connection
TCO	Total Cost of Ownership
TUC	Task Order Unique CLIN
VPN	Virtual Private Network
WAAPaaS	Web Application and API Protection as a Service
WAN	Wide Area Network
ZTA	Zero Trust Architecture
ZTNA	Zero Trust Network Access

Contributors

FIGURE 2 CONTRIBUTORS

Organization	Introduction	Slip Sheet	White Paper	Use Cases	How To Get	FAQ/Lessons Learned
General Services Administration (GSA)	X	X	X	X	X	X
JPI Solutions (JPI)	X	X	X	X	X	X