VMware SASE for Service Providers

The need for SASE

Interest in SASE is increasing. Enterprise organizations are transforming their businesses to be more agile to stay competitive in today's world. They are moving applications to the cloud, or using SaaS and allowing users to access these applications from the office, home, or away.

Enterprise IT must support this transformation by ensuring that users can have the same application experience regardless of whether users are inside or outside the office, while also ensuring security of their network, applications, and data. The need for this transformation is increasing with the large shift to remote work which will continue to grow.

To support the transformation, enterprise IT needs to implement operationally efficient solutions that provide workers in the branch, home, or away with secure, reliable, consistent access to applications and services—which can be located in the cloud, SaaS, or legacy data center—while also protecting against internal and external security threats. However, enterprise IT finds itself short on budget, personnel and skills as they are faced with having to deploy advanced security services.

This situation presents an opportunity for service providers to offer a SASE platform. However, a DIY model involves considerable effort. The answer is for service providers to partner with VMware and offer SASE services using VMware SASE™ for fast time to market, and then optionally consider an on-premises model.

The burden on IT

Current operational practices for many enterprises separate networking and security stacks, saddling both IT and end users with multiple pain points.

- User and device proliferation: The way people work has dramatically shifted. From traditionally being deskbound 9-to-5, employees today are increasingly out of the office and off corporate networks. They expect the digital business experience to offer a familiar, easy-to-use, mobile-like simplicity across all their platforms. Consumerization is forcing IT to support an end-user compute experience where users have the choice to bring their own devices and apps to work, with personal and work data co-existing in the same environment.
- Inefficient Cloud/SaaS access: Most enterprises run their applications across multiple public and private clouds. This puts an additional strain on operational resources, security, and quality of service. Cloud and SaaS applications require efficient, optimized access and infrastructure specifically architected to support them. A traditional hardware-heavy, transport-dependent network that relies on backhauling all cloud traffic through a single choke point in the data center cannot support the requirement for quick, efficient cloud access.

- **Poor application quality**: Corporate networks were engineered to provide reliable, optimal performance for mission-critical applications while supporting the day-to-day operations of the entire enterprise. This is true not just on the campus but also at branch sites and field offices. As workers move further from traditional corporate environments, enterprise IT must address the challenges posed by these home and remote locations. Employees must still be able to work efficiently when consuming bandwidth-intensive services, downloading image files, and collaborating with customers.
- **Compromised security**: Enterprise IT is already faced with the challenges of separate networking and security stacks for their own networks. This problem will be compounded by the growth of remote and home workers. Employees accessing corporate networks from their home machines or home networks heighten the risk of compromising the organization's security through data breaches and attacks. IT needs a way to secure the users' home networks and devices while managing the risk of what data leaves the enterprise network.
- **Operational complexity and expenses**: Traditional hub-and-spoke networks are not designed for cloud access. Environments built around legacy hardware-centric architectures cannot scale rapidly or cost-effectively. Ensuring future corporate productivity will require increasing the size of the network to provide reliable connectivity to home and remote workers. Separate stacks for the branch network, remote access, network security, and content security is not only operationally inefficient; it creates support complexity.

Security evolution

Enterprises have spent the last 30 years building networks and security for the data center. Now that applications are moving to the cloud, IT has to catch up. They are struggling to protect users from web threats, and they have to build that infrastructure quickly. Enterprise security strategy must evolve to treat the cloud as a central point of concern. An increasing volume of traffic will connect there rather than to legacy data centers while users will continue to demand responsive and resilient connectivity. The complexity of architectures needed to properly monitor, inspect, and secure this traffic will increase dramatically; corporate IT teams will be overburdened without a solution that unifies connectivity and security within a central management context.

The SASE model brings this picture together. Optimized cloud-native SD-WAN networking and cloud security, unified with intrinsic security, meets user demands for modern cloud-based services while ensuring the security of corporate data and systems.

SASE is the solution

The answer to providing security for application traffic going to the cloud is secure access service edge (SASE). It converges cloud networking and cloud security to deliver flexibility, agility, security, and scale for enterprises of all sizes. SASE presents enterprise IT with a significant set of capabilities and benefits. Its as-a-service model simplifies adoption and ongoing operation.

SASE applies necessary security services for SaaS and IaaS traffic. It is provided as a service in the cloud. Traffic comes to the SASE service directly over the Internet from the remote location. SASE avoids backhauling traffic to the data center and the need to build out security services in the data center. There are no CAPEX costs because it is offered as a service.

The SASE opportunity for service providers

SASE presents an opportunity for service providers to offer services that addresses network and security issues and improves network efficacy for their customers. With

SASE service providers will improve their competitive position, reduce customer churn, and increase loyalty.

Customers benefit from a SASE service through increased security, reliability, and WAN availability, which increases the ability to migrate applications to the cloud and to use SaaS applications with better security, reliability, and performance.

VMware SASE offers the service provider a complete solution that is tailored to their requirements. Choosing the VMware SASE solution as a service avoids the need to build out a solution, and time to market is almost immediate.

To get service providers up and running VMware has a program called **Ready, Set, Go** to assist with onboarding, and a partner marketing team that can put together programs to assist with customer acquisition.

VMware SASE

VMware SASE is based on the idea that the cloud is the network. It is architected to leverage the power of the cloud while minimizing complexity at the edge, offering an easy to consume one-stop-shop for security and network services. It delivers a unified edge and cloud service model with a single place to manage business policy, security rules, configuration, monitoring, operations, and troubleshooting. VMware SASE provides customers with the intrinsic security measures necessary to operate in the digital world effectively.

The VMware SASE architecture provides on-demand cloud services that are delivered with high performance and zero trust security—with lower costs—and close to users so that latency is reduced. VMware SASE delivers comprehensive capabilities that address networking and security needs for distributed enterprises. These services are configured to be content aware using policies based on user intentions and permissions. This makes VMware SASE the right solution for addressing networking and security needs for distributed enterprises.

Key features include:

- **A multi-tenant platform** that combines industry-leading VMware SD-WAN™, Zero Trust Network Access (ZTNA), secure web gateway (SWG), and firewall-as-a-service in a point of presence (PoP) for secure access to public and private cloud applications.
- **Advanced analytics and intelligence** on application performance, providing end-to-end visibility from the device to the PoP to the application.
- **A single interface** to manage business policies spanning multiple security and network services.
- **Open connectivity for third-party services** (e.g., security, analytics, mid-mile) in addition to integrated services that ensure efficient resource utilization.

VMware SASE is an extensible platform. You can choose the services to offer. Thin edge services can be delivered on the edge device. Thick cloud services can be delivered from the PoP. This platform provides for evolving networking and security at your own pace. Service providers can access the PoPs in an over-the-top (OTT) model, delivering hyperscale with global reach.

VMware SASE global PoPs

VMware SASE PoPs are a hyper-scale global network of multi-tenant cloud gateways and orchestrators. They have a global presence reaching 85% of the world's major metropolitan areas with a sub-10ms response. These SASE PoPs are placed at strategic cloud locations to establish direct peering connections with all major SaaS/IaaS providers, providing sub-5ms latency between the PoPs and cloud applications. This proximity translates to a fast onramp to cloud between user requests, packet steering, content inspection, and application access. With over 150 PoPs around the world, VMware has

the global presence to deliver new networking and security services as well as integrations with best-of-breed security partners.

VMware SD-WAN

SD-WAN is a key building block for SASE. It is responsible for providing reliable transport by controlling the connectivity, management, and services that connect its users and branch locations to cloud services. SD-WAN transforms connectivity, simplifying remote user and branch office networking while assuring optimal application performance and cost-effectiveness.

SD-WAN is delivered as a cloud service with a separate management plane, control plane, and data plane. This separation improves service network agility by moving the intelligence from the data plane into a programmable control plane. The management plane simplifies day-to-day operations and creates a flexible architecture that addresses the demands of modern SASE implementations.

VMware Orchestrator

The VMware SD-WAN Orchestrator is a unified cloud-hosted management platform that centralizes policy creation, distribution, automation and control. It simplifies day-0 to day-2 operations to alleviate installation, deployment, monitoring, and troubleshooting challenges through automation. The VMware Orchestrator provides a consolidated management view along with end-to-end network and application performance visibility. This orchestration layer is failsafe, highly resilient and simplifies end user deployments — meaning no IT administrator-dependent branch office installation is required.

VMware SD-WAN Edge

VMware SD-WAN Edges provide SD-WAN data plane functionality. They can be deployed anywhere, including branch offices and home offices. The Edge provides WAN connectivity and replaces the branch office router. SD-WAN Edges are also installed at data center sites and configured as hubs. An SD-WAN Edge can be deployed as physical hardware, a virtual appliance, or instantiated from a cloud provider marketplace.

VMware SD-WAN Gateway

The first VMware SASE PoP component provides the basic building block of SD-WAN services. VMware SD-WAN Gateways provide assured, reliable application delivery to mobile clients, branches, and campuses—even under unfavorable network conditions. Inside the SASE PoP, SD-WAN Gateways provide optimized cloud access directly to the doorstep of SaaS and IaaS offerings.

VMware SD-WAN Gateway and SD-WAN Edge services include application steering, Dynamic Multipath Optimization™ (DMPO), underlay visibility and reporting, on-demand mesh VPN, stateful firewall, and multi-cloud network orchestration. Branch sites equipped with a VMware SD-WAN Edge will extend an SD-WAN overlay connection to the VMware SD-WAN Gateway. The traffic originating in these branches will benefit from VMware's patented DMPO protocol.

The SD-WAN Gateway component of the SASE PoP is stateless, horizontally scalable, and multi-tenant. They are hosted by VMware and technology partners.

VMware SASE security services

VMware Secure Access

VMware Secure Access uses a software client to implement a Zero Trust Network Access (ZTNA) model that allows only trusted devices and users access to enterprise applications and resources. Individual users are mapped to application policies—both for on-premises and SaaS/IaaS applications—that apply regardless of where they are located. This reduces IT's policy management burden, helping to reduce operating costs.

ZTNA changes the game for secure remote connectivity. It implements a zero-trust model, where users have no visibility into corporate resources, much less access to them, without explicit permission. Users access each individual application, not the full enterprise network, via a secure, encrypted connection. The network automatically applies the right security (services), allowing only trusted devices (context) and users (identity) to access the application. The network does this for both on-premises and cloud-hosted applications.

ZTNA maps each user to the policy defined for that specific application, regardless of whether the user is inside or outside the office. This allows IT personnel to maintain a single set of policies per user, reducing operational complexity and costs. It also ensures a consistent application experience, no matter where users connect from (e.g., remote or branch) or where the application resides (e.g., branch, data center, cloud, or Internet).

VMware Cloud Web Security

VMware Cloud Web Security™ brings together best-of-breed security capabilities: SSL proxy, URL filtering, anti-malware, cloud access security broker (CASB), data loss prevention (DLP), remote browser isolation (RBI), and more. Incorporating these services into the VMware SASE PoP, Cloud Web Security provides secure, direct, and optimal access to SaaS and public Internet access.

When traffic arrives at a SASE PoP, the SD-WAN Gateway component redirects it to the applicable services. These services implement policies assigned by the SASE orchestration engine, a management component responsible for global organization and distribution of enterprise policy. A common security services traffic flow begins with SSL proxy services, then URL filtering, followed by anti-malware processing. Further granular inspection can be performed by doing cloud sandboxing. Other services may also be employed based on policy specifics, such as cloud firewall (FWaaS), if the traffic is ultimately destined for an on-premises data center.

The following sections explore the purposes and capabilities of individual Cloud Web Security services.

SSL proxy

SSL proxy sits between the client and server. A key function of the SSL proxy is to emulate server certificates. This allows a web browser to use a trusted certificate to validate the identity of the webserver. SSL encrypts data to ensure that communications are private and the content has not been tampered with.

The SSL proxy acts as a client for the server by determining the keys to encrypt and decrypt. It also acts as a server for the client by authenticating the original server certificate and issuing a new certificate along with a replacement key. The proxy encrypts and decrypts in each direction (i.e., client and server). Keys are different for both encryption and decryption. It hands off HTTPS traffic to the HTTP proxy for protocol optimization and other acceleration techniques.

In a VMware SASE Secure Web Gateway, traffic is decrypted by an SSL proxy, directed for inspection by enterprise security policies, then re-encrypted before leaving the SASE PoP.

URL filtering

The VMware SASE PoP cloud-delivered URL filtering service follows category-based classification. It supports wildcard-based URL permit and deny lists for HTTP and HTTPS traffic. Policy configuration and management are accomplished through the VMware Orchestrator. URL policies are part of the security rules distributed by the VMware Orchestrator.

While the most common reason for the restriction is user safety (e.g., malware propagation, phishing), businesses may choose to block content they find inappropriate

(e.g., violence, shopping, gambling) or that violates compliance regulations. They may also restrict sites that can impact overall network performance (e.g., bandwidth consumption from streaming media).

Anti-malware and anti-virus

Anti-malware solutions protect endpoints from threats such as malware, spyware, adware, and worms, securing corporate data from corruption or theft. Modern offerings often combine advanced malware protection capabilities and sandboxing technology. Cloud Web Security provides next-general anti-malware protection along with anti-virus, web isolation, and e-mail protection services. All these services are configurable directly from the VMware Orchestrator and delivered by VMware SASE PoP Cloud Web Security services.

Cloud sandboxing

Cloud sandboxing is used to protect against web-based threats caused by the downloading, installation, and execution of unknown software code, which could otherwise allow hackers to access personal data or get access into the enterprise network.

Cloud sandboxing protects users, networks, and data by detecting and quarantining threats before they can gain a foothold on or spread from an endpoint. A cloud sandbox provides a safe environment for opening suspicious files, running untrusted programs, or downloading URLs without affecting the devices they are on. Malware is prevented from ever reaching the endpoint, whether it has been properly detected or not. It can be used any time, for any situation, to safely examine a file or code that could be malicious before passing it on in full to the end user—all the while keeping it isolated from an endpoint and the enterprise network.

Sandboxing assesses a given file and categorizes content as safe or unsafe. If malware is detected, it blocks or drops the malicious file. If the file is safe, users will be allowed access.

Cloud access security broker

Cloud access security broker (CASB) functionality is used to protect end users when accessing sanctioned and unsanctioned applications. It provides real-time visibility and control for all incoming and outgoing traffic. Sanctioned applications reside in the public SaaS cloud (e.g., Office365, Salesforce), while un-sanctioned applications are on the public Internet (e.g., personal e-mail). The cloud-delivered CASB provides visibility and control into web traffic, policy compliance, threat protection, and data leak prevention. As part of VMware SASE PoP Cloud Web Security services, the CASB solution offers a fully functional API that controls the lateral movement of data within the SaaS environment. It operates according to defined enterprise security policies, enforcing malware prevention and encryption.

Data loss prevention

Data loss prevention (DLP) systems traditionally prevent sensitive corporate information from leaking out from the perimeter. As the nature of the enterprise perimeter has evolved, so too must the capabilities and coverage of DLP solutions; they must grow to address the demands of cloud services, web traffic, and highly mobile users.

Data loss prevention uses digital markers, file fingerprinting, document filtering, and pattern matching techniques to identify and block unauthorized communication of sensitive data (e.g., credit card information, Social Security numbers, personal health information) outside the network. DLP differs from other security inspections as it primarily focuses on internal network data rather than threats from outside enterprise networks.

Remote browser Isolation

Remote browser isolation (RBI) creates a lightweight sandbox environment for evaluation and viewing of content. Web browser sessions are isolated from the network and executed remotely in a cloud-based platform. Only safely rendered information is returned to the actual browser, providing a secure browsing experience to the end user. This technology can also enhance the overall user experience by abstracting performance from specific endpoint hardware, allowing a higher degree of security processing regardless of endpoint capabilities. RBI can be performed server-side, which eliminates the need for a user to install additional agents to receive advanced web protection.

VMware SASE cloud firewall

VMware's SASE PoP cloud firewall (FWaaS) component integrates next-generation firewall and advanced security functionalities such as intrusion protection service (IPS), advanced threat detection (ATD), anti-malware, and URL filtering. It is a core part of the SASE solution, providing complete security coverage at Layers 2 through 7. These capabilities help protect enterprise applications and data by offering visibility of and control over traffic moving between branches and private data centers. SASE PoP cloud firewall components protect traffic types of web/non-web/transport layer security (TLS) and clear traffic between enterprise branch sites, remote users, IaaS, and private data center applications.

VMware Edge Network Intelligence

VMware Edge Network Intelligence™ leverages multiple sources of data to provide a coherent and correlated set of actionable insights. It examines the network experience from the perspective of end-users and IoT devices, bringing together visibility and performance information about networks (e.g., LAN, SD-WAN, Wi-Fi), services (e.g., DHCP, DNS, RADIUS), and applications (e.g., Zoom, Microsoft 365, Workday).

VMware Edge Network Intelligence focuses on the enterprise edge with a vendor-agnostic approach to optimize end-user and device performance and security. VMware Edge Network Intelligence AIOps use cases span endpoint devices, LAN, Wi-Fi, IoT devices, WAN, application performance, SD-WAN, and VMware SASE components and environments..

VMware Edge Network Intelligence capabilities are deployed in multiple areas of a VMware SASE PoP environment. They are used to monitor the overall quality of the SASE service, tracking resource utilization and component degradation. Issues can be resolved proactively to avoid service disruption and maintain an optimal network state.

VMware Edge Network Intelligence also monitors application performance and user experience at the flow level. It tracks the latency between individual hops (e.g., user to SASE PoP) to understand when performance varies against the baseline. The system not only can report a problem but also pinpoint a component or link for corrective action. The VMware SASE solution brings security information into this environment to further expand visibility into potential root causes.

The VMware SASE difference

VMware SASE services are delivered through a network of 3000+ cloud gateways in hundreds of PoPs. This environment is supported globally by VMware and hundreds of service provider partners. Depending on business needs and preferences, it can be available as a managed service or a DIY offering. It is designed for easy adoption and consumption while taking advantage of the benefits of the cloud for global reach, rapid scalability, and minimized operational complexity. This global reach allows IT to address the needs of all employees regardless of their location while simplifying the deployment, management, and maintenance of the infrastructure.

The solution provides customers with the intrinsic security required for operation in the connected digital world.

Cloud first

VMware SASE is based on the idea that the Ccoud is the network. Through its global PoP network, it provides simplified, cost-effective connectivity to cloud- and SaaS-based applications while also ensuring end-to-end security with flexible deployment choices for work-at-home users. SASE leverages the power of cloud networking to support dynamic, flexible scaling. Organizations can start small, then grow their remote digital workforce through the unique architecture of cloud gateways and cloud-based management.

Intrinsic security

Through a cloud security model that encompasses user identity, device posture, and network location, VMware SASE unifies network and application security policies for branch and remote workers. The solution's comprehensive suite of security features includes contextual access, network security, application protection, and network separation—allowing it to align with and realize the latest concepts in zero trust.

Application quality assurance

With the VMware SASE platform, organizations can ensure the availability and performance of mission-critical applications, even with degraded network conditions or congestion. By combining application recognition, traffic prioritization, and shaping with the ability to measure network path performance, the solution steers traffic on a packet-by-packet basis to achieve the highest quality of experience for end users. The solution also employs artificial intelligence for comparative application performance benchmarking to identify sources of and solutions to network issues. The platform removes the requirement for VPN concentrators in the data center, eliminating a common bottleneck. This further reduces latency and improves network bandwidth utilization for users trying to reach cloud and SaaS destinations.

Operational simplicity and ROI

The VMware SASE platform provides operational simplicity and lowers operational expenses. It allows the enterprise to procure, manage, and troubleshoot SD-WAN, ZTNA, SWG, and firewall functionality from a single vendor, avoiding the inefficiencies inherent in patching together multiple disparate solutions.

Service providers can manage business policies spanning multiple security and network services through a single-pane-of-glass management portal.

The cloud-delivered network of VMware SASE PoPs spans the globe and is available as a service to minimize the internal operational burden.

VMware Edge Network Intelligence, a key analytics functionality of SD-WAN, constantly assesses the state of both LAN and WAN, producing actionable and insightful reports to aid troubleshooting and fault isolation.

VMware SASE ensures the availability, security, and performance of mission critical applications from the branch, home, or away and for users on company-owned or BYO devices.

A single integrated management platform simplifies operations and reduces support complexities by unifying networking and security, while a broad ecosystem and open architecture allows service providers to control their choice of SASE services.

Benefits for service providers

Services integration with API

The API enables service providers to connect SD-WAN to their backend systems for a better customer experience. They can automate installation and setup of SD-WAN components. Service providers can create, retrieve, update, delete users with all types of roles. APIs can be used securely in the network for authentication, identity management and more.

Simplified operations

The VMware SD-WAN Orchestrator is the central management platform for configuration and management of VMware SD-WAN. It provides a single point of management with features including multi-tenancy, and roles-based access.

Extensible Architecture

VMware SASE enables integration with a choice of services from VMware or from other vendors. It does not lock the service provider to a fixed set of services. Existing services can be migrated to the VMware platform and new services can be added as needed to meet customers' needs.

Choice of deployment

VMware SASE can be used in an over the top (OTT) model for fast time to market. There is also the option to deploy on-premises at service provider PoPs using the VMware deployment model.

Ready-Set-Go onboarding program

To get service providers up and running fast VMware provides a service called Ready-Set-Go that includes help with contracts, legal, marketing and deployment.

Conclusion

VMware SASE is available today for enterprises ready to transform their access infrastructure. Service providers can get to market fast by partnering with VMware and offering SASE services in an OTT model.

This SASE architecture brings together VMware SD-WAN, VMware Workspace ONE, Secure Access, and other components under a single management and orchestration framework. VMware's worldwide network of VMware SASE PoPs is the vehicle that delivers the solution.

VMware SASE simplifies application connectivity for any user—office, branch, home, mobile—on any device to any workload. It provides a common environment for end-to-end policy, ensuring both consistent security and optimized performance. Automation tools enable self-healing of ongoing network problems while data aggregation and event correlation streamline troubleshooting and root cause analysis. The centralized management model removes the need for highly skilled staff at branch sites and allows the enforcement of holistic business-centric policy across the network.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com