Versa Secure Access Fabric

Secure Access Service Edge (SASE) has transformed the traditional WAN, internet, and cloud user experience for large-scale enterprises and small-to-medium size businesses alike. Versa has led this transformation by providing integrated SD-WAN, security, and routing features in a single platform, with centralized management and monitoring, analytics, and reporting, as well as automation on the WAN Edge.

Today, organizations are faced with the following reality:

- Digital transformation has accelerated the migration of enterprise applications and workloads from an enterprise datacenter to a variety of public clouds and/or SaaS services.
- Many networking functions, including security functions, running on-premises are now expected to run in the cloud or in both locations, all while being consumed as a service.
- Users are connecting from everywhere, both remotely and on-premises, and are frequently moving between the two in a hybrid workplace model.
- High-performing and omnipresent cloud connectivity has gained importance as applications move to the cloud for flexibility and scalability.

Two trends transforming the enterprise environment are cloud and work-from-anywhere.

The momentum towards cloud has been clear for the past few years. Enterprise applications are moving away from a data center-centric architecture to a cloud-based architecture. Enterprises find it convenient and cost-effective to subscribe to Software-as-a Service (SaaS) applications which are hosted in the cloud. In addition, many enterprises choose to leverage public cloud to host their own applications in a "Virtual Private Cloud." In either of these cases, the applications are hosted outside the perimeter of the enterprise, on clouds accessible over public internet.

A more recent trend is work-from-anywhere. Employees are much more likely to work remotely compared to the past. Even in the post-pandemic era, a hybrid work style has been adopted in which some days employees are working from home and the rest of the days they are working in the office. The enterprise IT administrator now has limited control over cloud-based applications and the data environment. Bring Your Own Device (BYOD) is another trend which further challenges the control enterprise administrators can exert over the employee, and how apps and data are being used. In short, business-critical enterprise applications are accessible over the Internet by employees situated outside the enterprise network perhaps via corporate devices or by personal devices.

This translates to two major challenges:

- The threat landscape has expanded dramatically. Perimeter-based security for users, applications, and data is not very effective any more as clouds are located outside of the enterprise perimeter. Hence a new security paradigm is necessary to protect the enterprise network and data.
- The application performance and user experience controls, which depend on the enterprise controlling the network and its assets on premises, are also not very effective. A new user experience paradigm is necessary to ensure applications experience and assure user productivity while apps and data may be residing on clouds.

Furthermore, contrary to popular perception, internet access is not homogeneous. The internet consists of peering arrangements between different service providers who would typically prefer the handover of IP packets to peering service providers as quickly as possible to keep their network costs to minimum. Hence a user's packet may hop from one provider network to another resulting in having no control or predictability, especially over long distances over Internet.

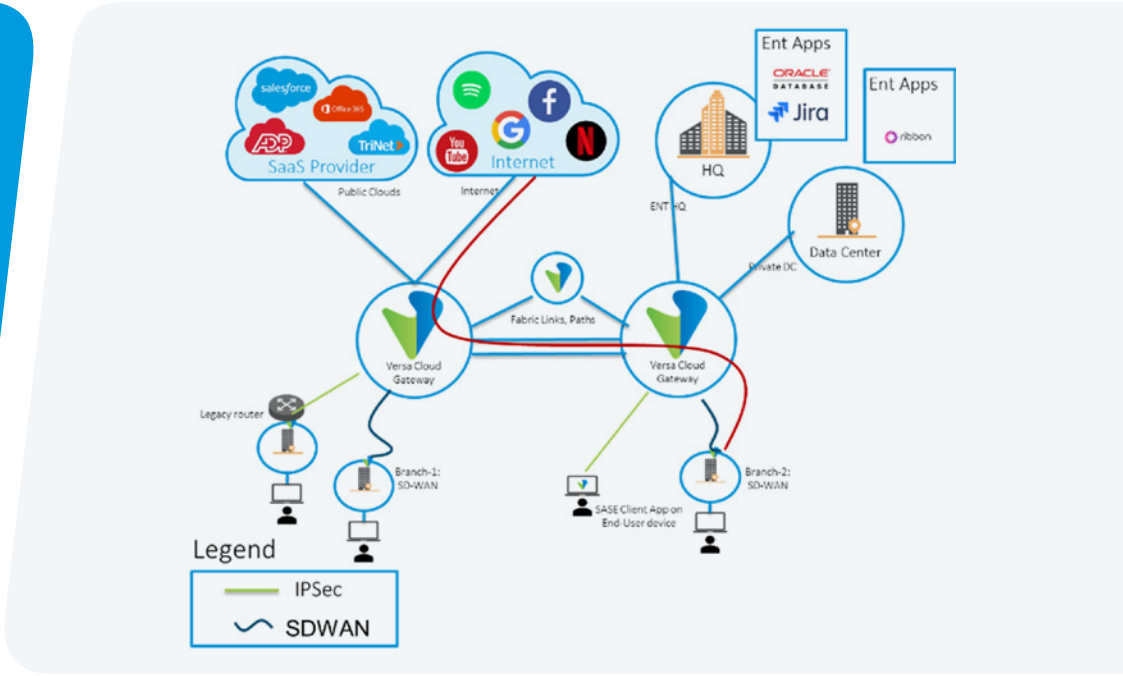
A common method to solve the need for an assured user experience is to use MPLS links. MPLS links provide WAN connectivity with strict SLAs using MPLS VPNs. For that reason, an MPLS VPN-based architecture has been an essential part of enterprise WAN deployments for over two decades. As cloud-based applications are accessible over the Internet access and no longer are limited to enterprise network. Therefore, typically a separate or bundled internet access solution would still be needed for enterprises that use MPLS services.

As enterprise architectures have moved towards cloud-centric applications, enterprises have deployed a security solution to secure the branches. A more recent trend is to additionally leverage Network-as-a-Service (NaaS) offered by Cloud Service Providers and backbone providers. NaaS provides enterprises with an SLA-backed backbone for a better user experience and reliable application access. Especially when enterprises deploy a cloud-based SSE service, there are many integration points between the NaaS provider and SSE provider which may not be optimal.

Versa Secure Access Fabric (VSAF) combines Versa's SSE offerings with a NaaS solution to offer a Secure Network-as-a-Service (SNaaS) solution to our customers. The combination delivers many interesting advantages to our customers than what meets the eye at first glance. Versa's globally distributed Points-of-Presence (PoPs) are set up to deliver SSE and NaaS services for our customers while security services and network connectivity work as a seamlessly unified solution.

A single-pass architecture of integrated SSE and NaaS reduces the processing latency experienced by user packets, as the packets do not need to be service-chained across different PoPs or virtual machines. Single-pane-of-glass management allows define-once policy i.e., an integrated policy for security and QoS handling. Furthermore, the NaaS part of the solution extends all the way to Versa Secure SD-WAN appliances on the branch, effectively extending the NaaS solution all the way to the WAN edge of the customer.

Versa Secure Access Fabric (VSAF) Building Blocks



VSAF is a user-experience-focused security and networking solution, combining the best of both worlds. Versa Unified SASE's operational components include:

Versa Cloud Gateways (VCG)

Are Points of Presence based on the industry leading VOSTM platform. VCGs are globally distributed to provide reliable and omni present secure on-ramps for access to enterprise applications. VCGs authenticate users, authorize application access, and secure enterprise networks from external threats. VCGs integrate advanced routing, comprehensive security, and market-leading SD-WAN, with secure access. VCGs securely connect to and integrate with Enterprise's existing network and datacenter infrastructure.

Versa SASE Client

Is the software agent that runs on a client device, extending SD-WAN style connection capabilities all the way to the end user. Versa SASE Client creates a secure and encrypted connection from user devices to the VCGs. Upon authentication and access authorization through the VCG, users with the Versa client can securely connect to enterprise applications that may be residing on public or private clouds.

Versa SASE Fabric

Forms the full mesh connectivity between VCGs. VSAF creates multi-tenant SD-WAN overlays between VCGs, forming an Application SLA aware network for transporting customers' private and Internet bound traffic.

Versa SASE Portal

Provides enterprise administrators with the ability to monitor and manage users and applications form a centralized console. Versa SASE Portal provides real-time and historical reporting at network, application, and user levels. Versa SASE Portal provides single-pane-of-glass management for security as well as VSAF.

VSAF Scope

Versa Secure Access Fabric (VSAF) is the name of the product offering which provides a combination of the following connectivity and security options:

Versa Secure Private Access (VSPA)

Provides Zero Trust access to enterprise-hosted private applications for remote users. The VSPA solution provides enterprise application access control based on user, user-group, device posture, geo-location, and other parameters. When combined with Versa Secure Internet Access (VSIA), the data can be protected using advanced security features like IPS, AV, and DLP. For more information, please refer to the VSPA Datasheet.

Versa Secure Internet Access (VSIA)

Secures users and devices from Internet-based threats. The VSIA solution protects users accessing SaaS and internet applications from remote and branch locations. VSIA provides security and access control based on user, user-group, device posture, geo-location, and other parameters, and protects against internet threats like virus, malware, ransomware via IPS, AV, URL filtering, Advanced Threat Protection (Sandboxing) and other built-in security capabilities. Cloud Access Security Broker (CASB) and network-based Data Loss Prevention (DLP) prevent data exfiltration attempts and protect data stored in SaaS applications as well as internet applications. For more information, please refer to the VSIA Datasheet.

Versa Secure SD-WAN on Versa Cloud Gateway Access

Provides SD-WAN-based connectivity and access to Versa Cloud Gateways fpr the best user experience and SLA-based connectivity. User traffic accessing VSPA and VSIA leverages Versa SD-WAN overlays on the access links between the enterprise edge (branch and remote user device) and Versa Cloud Gateways. Use of Versa's SD-WAN ensures an enhanced application experience and also provides advanced application acceleration techniques such as Forward Error Correction, Packet Cloning, TCP-Optimization and more.

Versa SASE Fabric

Interconnects Versa Cloud Gateways to provide SLA and application performance-aware connectivity solutions to our customers. VSAF uses the Versa Operating System's built-in SD-WAN capabilities to build an overlay fabric between the cloud gateways across the globe. Using this overlay fabric, VSAF ensures that the application traffic takes the best available path to meet application SLA requirements by using its built-in advanced traffic engineering capabilities. When connecting Versa WAN edge devices at enterprise locations, VSAF forms an end-to-end QoS-aware network to connect remote users as well as branch users and devices to SaaS and private applications.

Versa's cloud-managed, cloud-delivered Versa Secure Access Fabric (VSAF) solution helps secure enterprise sites, home offices, and traveling users accessing distributed applications without compromising security and user experience. In addition to securing the user and device traffic, VSAF provides an assured user experience using Versa's patented technology.

- SD-WAN powered middle-mile fabric to provide SLA aware network
- CFM Y.1731-based network performance management and fault detection
- Real-time end-to-end SLA computation between cloud destinations and users
- SaaS application access measurements using inline and active (synthetic) measurement methods
- Real-time distribution of performance data to Versa SD-WAN enabled branch devices
- Application acceleration for application traffic via TCP optimization and more

VSAF is built of multi-tenanted Versa Cloud Gateways deployed globally. Versa Cloud Gateways are connected via business class connections to provide a full mesh connectivity between the gateways and to offer business-class connection characteristics. When a customer subscribes to VSAF, the customer gets access to Versa Cloud Gateways and to the VSAF fabric that interconnects them.

VCGs connect each other via multi-tenanted SD-WAN overlays. A Versa SD-WAN overlay implements a CFM Y1731 protocol between the cloud gateways to measure the network performance in real time. Even small changes in the network performance are identified and reported. Additionally, every edge node measures performance towards the SaaS applications. All such network and application performance information that is collected on a real-time basis is used to make dynamic traffic steering decisions to provide an optimum user and application experience.

SaaS applications are complex implementations which vary from fully distributed to completely centralized architectures. Versa implements a variety of active and passive measurement techniques to measure performance of SaaS applications over various available paths.

SD-WAN Traffic Engineering Link State Protocol is implemented to distribute the performance (both network performance as well as SaaS application performance) to the edge nodes. SD-WAN TELS efficiently distributes the performance of each and every hop to every edge node, allowing the edge node to calculate the end-to-end performance towards the intended application. This ensures that the customer traffic always chooses the most appropriate path as defined by the policy.

Target Use Cases

While there may be many use cases addressed by the VSAF offering, in a typical enterprise network there are four general use cases which require security and efficient connectivity:

I. Remote users accessing SaaS applications: In this case, the user connects over the internet to a cloud-hosted SaaS application. The application experience can be challenging for remote users geographically distant from the SaaS application.

   The intelligent gateway selection ensures that the Versa SASE Client connects to the closest high-performance gateway. The Versa Cloud Gateway uses the intelligence received from SD-WAN TELS to identify the best path from the Versa Cloud Gateway to the SaaS application. The path performance is evaluated frequently, and if the path performance degrades, the application flow may be rerouted.

II. Remote user accessing private applications: In this case, the user connects over the internet to an enterprise-hosted private application. Typically, private applications are not distributed geographically. The user traffic, irrespective of where the user is located, may be served from a central location.

   The intelligent gateway selection ensures that the Versa SASE Client connects to the closest high-performance VCG. That VCG then uses the intelligence received from SD-WAN TELS to identify the best path towards the private application. If the application is hosted behind a Versa SD-WAN appliance, the SD-WAN TELS is extended to the branch or DC. The application traffic traverses the chosen path for an assured user experience. The path performance is evaluated frequently, and if the path performance degrades, the application flow may be rerouted.

III. User/Device behind branch accessing a SaaS application: In this case, the user or a device connects to the SaaS application over the internet link connected to the branch office. When the WAN edge device is a Versa Secure SD-WAN appliance, SD-WAN TELS is used to identify a dynamic path for the application flow based on the performance. The WAN Edge device chooses the next hop (Versa Cloud Gateway) which is more likely to provide better performance for the user.

IV. User/Device behind branch accessing SaaS application: In this case, the user or a device connects to the private application over the WAN link connected to the branch office. When the WAN edge device is a Versa Secure SD-WAN appliance, SD-WAN TELS is used to identify a dynamic path for the application flow based on the performance. The WAN Edge device chooses the next hop (Versa Cloud Gateway) that is more likely to provide better performance for the user.

Service Tiers

VSAF (all features are provided inline and through a single-pass architecture)	Essential	Professional	Elite
SLA-aware Versa SASE Fabric	✓	✓	✓
SD-WAN between cloud gateways powered by SD-WAN traffic engineering	✓	✓	✓
SD-WAN branch-to-branch via Cloud Gateways powered by SD-WAN traffic engineering	✓	✓	✓
Application acceleration for traffic (including TCP-optimization, Forward Error Correction)	✓	✓	✓
Versa Secure Internet Access Essential tier features, including: • Connection from enterprise sites via SD-WAN Overlay, IPSec, GRE-based tunnels • Versa endpoint client application-based end-user device connectivity • User and device authentication, endpoint posture-based policies • URL Feeds and Filtering, IP Feeds and Filtering, DNS Proxy *(for details, refer to the VSIA datasheet for VSIA Essential features)*	✓	✓	✓
Versa Secure Private Access Essential tier features, including • User/User-group based application control and visibility • Network obfuscation • Support for up to 10 private applications *(for details, refer to the VSPA datasheet for VSPA Essential features)*	✓	✓	✓
Versa Secure Internet Access Professional tier features, including: • UTM/UTP features including IPS, AV, malware protection, TLS Proxy • DNS Feeds and Filtering, DNS Security • File reputation and filtering • Inline CASB (Cloud Access Security Broker) • Shadow IT Discovery and Management • Clientless application access and protection *(for details, refer to VSIA datasheet for VSIA Professional features)*		✓	✓
Versa Secure Private Access Professional tier features: • Support for unlimited private applications • Clientless access to private resources using Terminal Server Agent (TSA), portal-based application access for HTTP(S) *(for details, refer to the VSPA datasheet for VSPA Professional features)*		✓	✓
Versa Secure Internet Access Elite tier features, including: • Inline DLP (Data Loss Prevention) • Endpoint DLP • Advanced Threat Prevention (ATP) Essentials scope • XOT security • API-DP Essential –,CASB for up to three IaaS or SaaS connectors • GenAI Firewall *(for details, refer to the VSIA datasheet for a list of VSIA Elite features)*		Optional	✓
Add-on options: • API-DP Professional scope • ATP Professional scope • RBI (Remote Browser Isolation)		Optional items	Optional items

(*) For more details please refer to the feature matrix of the Versa Secure Access Fabric offering.

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054
Tel: +1 408.385.7660 | Email: info@versa-networks.com | Website: www.versa-networks.com