# Versa Secure Access Fabric

## Introduction

SASE (Secure Access Service Edge) has transformed traditional WAN, Internet, and cloud user experience for large-scale enterprises and small-to-medium size businesses alike. Versa Networks has led this transformation by providing integrated SD-WAN, security, routing features in a single platform, with centralized management and monitoring, analytics and reporting, and 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 on the cloud or on both locations, all while being consumed as a service
- Users are connecting from everywhere. COVID-19 has changed the workplace dynamics to a new normal where employees can work from anywhere.
- High-performing and omni-present cloud connectivity have gained importance as applications move to the cloud for flexibility and scalability

Two trends transforming the enterprise environment is Cloud and Work from anywhere.

The momentum towards cloud is clear for past few years. Enterprises Applications are moving away from Data Center centric architecture to a Cloud oriented architecture. Enterprises find it convenient and cost effective to subscribe to a 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 "Virtual Private Cloud". In either of the 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 hybrid work style is adopted in which some days employees are working from home and on rest of the days they are working in the office. Enterprise IT Administrator now has limited control over the cloud-based application and 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 2 major challenges:

- The threat landscape expands 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 so effective. A new user experience paradigm is necessary to ensure applications experience and assured user productivity while apps and data may be residing on clouds.

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

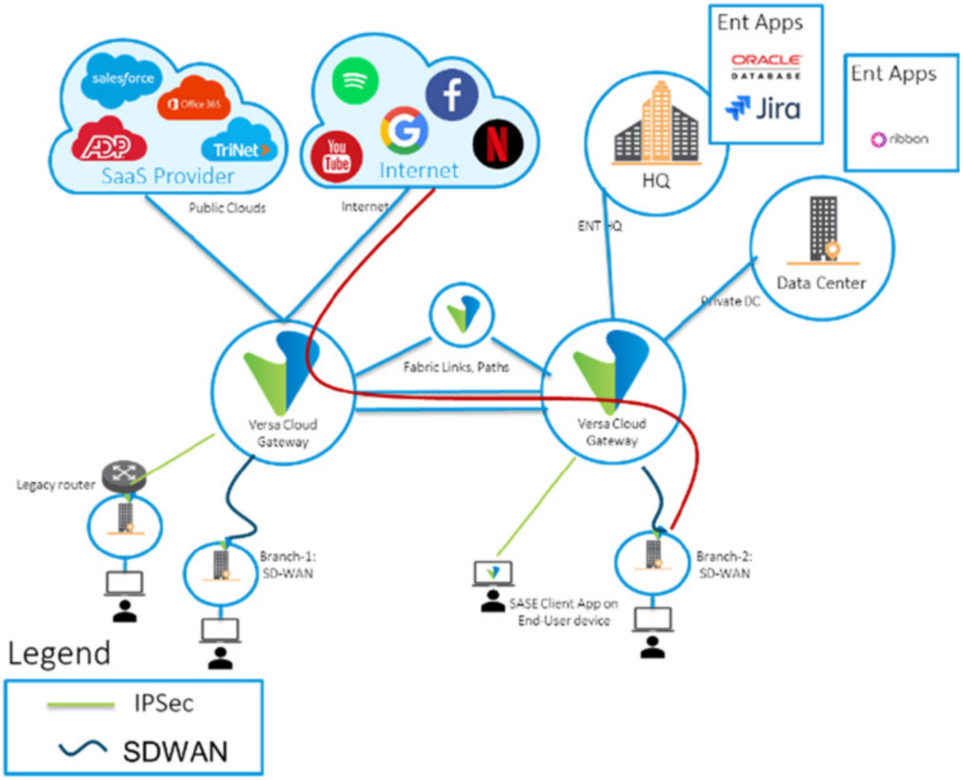
An assured, commonly used way to solve the need for assured user experience is to use MPLS links. MPLS links provide WAN connectivity with strict SLAs using MPLS VPNs. For that reason, MPLS VPN based architecture has been an essential part of enterprise WAN deployments for over two decades. As the cloud 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 these Enterprise who use MPLS services.

As enterprise architectures have moved towards cloud centric applications, Enterprises deploy a security solution in order to secure the branches. A more recent trend is to additionally leverage Network as a Service (NaaS) offered by Cloud Service Providers and/or backbone providers. NaaS provides Enterprises with a SLA backed backbone for better user experience and reliable application access. Especially when Enterprises deploys 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 NaaS solution to offer a Secure Network as a Service (SNaaS) solution to our customers. The combination delivers many interesting advantages to our customers that what meets the eye in 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 works as a seamlessly unified solution.

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 management allows define-once-policy i.e., an integrated policy for Security and QoS handling. Furthermore, NaaS part of the solution extends all the way to Versa Secure SD-WAN appliances on the branch effectively extending NaaS solution all the way to the WAN Edge of the customer.

## Versa Secure Access Fabric (VSAF)



VSAF is a user experience focused security and networking solution, combining best of both worlds. Versa SASE solution consists of:

Versa Cloud Gateways (VCG) are Points of Presence based on 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 Client is the software agent/application that runs on client device extending SD-WAN style connection capabilities all the way to end users. Versa Client creates a secure and encrypted connection from user devices to the Versa Cloud Gateways. Upon authentication and access authorization through the Versa Cloud Gateway, users with 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 Versa Cloud Gateways. VSF creates multi-tenant SD-WAN overlays between VCGs, forming an Application SLA-aware network for transporting customer's private and Internet bound traffic.

Versa SASE Portal provides enterprise administrators 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, user levels. Versa SASE Portal provides single mane of management for Security as well as Versa Secure Fabric (VSF).

## VSAF Building Blocks

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

Versa Secure Private Access (VSPA) to provide Zero Trust access to enterprise hosted private applications for remote users. 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, DLP. For more information, please refer to Versa Secure Private Access datasheet.

Versa Secure Internet Access (VSIA) secures users and devices from Internet-based threats. VSIA solution protects users accessing SaaS and Internet applications from remote and/or branch locations. VSIA solution provides security and access control based on user, user-group, device posture, geo-location, and other parameters. VSIA solution protects against Internet threats like virus, malwares, ransomwares via IPS, AV, URL filtering, Advanced Threat Protection (Sandboxing) and other built-in security capabilities. Cloud Access Security Broker, and Network based Data Loss Prevention prevent data exfiltration attempts and protect data stored in SaaS application as well as internet applications. For more information, please refer to Versa Secure Internet Access datasheet.

Versa SD-WAN on Versa Cloud Gateway Access, providing SD-WAN based connectivity and access to Versa Cloud Gateways fpr best user experience and SLA based connectivity. User traffic accessing VSPA and/or 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 SDWAN ensures enhanced application experience and also provides advanced application acceleration techniques such as Forward Error Correction, Packet Cloning, TCP-Optimization and more.

And Versa SASE Fabric (VSF) inter-connecting Versa Cloud Gateways to provide SLA and application performance aware connectivity solution to our customers. VSF is powered by Versa SDWAN to form a SDWAN overlay between the cloud gateways. VSF ensures that the application traffic takes the best available path which meets the application SLA requirements by using its built-in advanced Traffic Engineering capabilities. When connecting Versa WAN edge devices at enterprise locations, VSF forms an end-to-end QoS aware network to connect remote users as well as branch users/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, VSF provides 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 distribution of performance measure for end to end SLA computation between the cloud gateway
- Passive performance of SaaS application access
- Active performance measure of SaaS applications
- Real time distribution of performance measure to Versa SDWAN enabled branch devices
- Application Acceleration for application traffic

The core of Versa Secure Fabric consists of multi-tenanted Versa Cloud Gateways deployed globally. Versa Cloud Gateways are connected via private networks 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 Versa SASE Fabric that interconnects them.

VCGs communicate with each other via VSF which is a set of multi-tenanted SD-WAN overlays. Versa SD-WAN overlay implements a CFM Y1731 protocol between the cloud gateways to measure the network performance in real time. Even small change in the network performance is identified and reported. Additionally, every edge node measures performance towards the SaaS applications. All of such network and application performance information that is collected on real-time basis is used to make dynamic traffic steering decisions to provide 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 path.

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 is a efficiently distributes the performance of each every hop to every edge node allowing the edge node to calculate the end-to-end performance towards intended application. Thus, ensuring 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 VSAF offering, in a typical enterprise network, there are 4 general use cases which require security and efficient connectivity:

I. Remote users accessing SaaS applications: In this use case, the user connects over the Internet to a cloud hosted SaaS application. The application experience can be challenging for remote users who travel geographically distances to reach the serving SaaS application.

   The intelligent gateway selection ensures that the Versa Client connects to the closest high-performance gateway. Versa Cloud Gateway uses the intelligence received from SD-WAN TELS to identify the best path from the Versa Cloud Gateway towards the SaaS application. Versa uses both active and passive performance measurement tools to evaluate the performance of SaaS application via individual gateways. The application traffic traverses the chosen path ensuring assure user experience. The path performance is evaluated frequently. If the path performance degrades, the application flow may be rerouted.

II. Remote user accessing private application: In this use 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 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/DC.

   The application traffic traverses the chosen path ensuring assured user experience. The path performance is evaluated frequently. If the path performance degrades, the application flow may be rerouted.

III. User/Device behind branch accessing SaaS application: In this use case, 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 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 use case, 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 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.

## Service Tiers

| VSAF (all features are provided inline and through a single-pass architecture of VOS) | Essential | Professional | Elite |
|---|---|---|---|
| SLA Aware Versa SASE Fabric | ✓ | ✓ | ✓ |
| End to End SLA based SD-WAN between Cloud gateways powered by SD-WAN Traffic Engineering | ✓ | ✓ | ✓ |
| End to End SLA based SD-WAN between Branch to Branch via Cloud Gateways powered by SD-WAN Traffic Engineering | ✓ | ✓ | ✓ |
| Application Acceleration for traffic (TCP-Optimization, Forward Error Correction) | ✓ | ✓ | ✓ |
| Versa Secure Internet Access Essential Features:<br>• Connection from Enterprise sites via SDWAN Overlay, IPSec, GRE based tunnels<br>• Versa client application-based end-user device connectivity<br>• User and Device Authentication, Endpoint Posture based policies<br>• URL Filtering, IP Filtering, DNS Filtering<br>Refer VSIA Essential features in VSIA datasheet. | ✓ | ✓ | ✓ |
| Versa Secure Private Access Essential Features:<br>• User/User-group based application control and visibility<br>• Network Obfuscation<br>• Support for up to 10 Private applications<br>Refer VSPA Essential features in VSIA datasheet. |  | ✓ | ✓ |
| Versa Secure Private Access Professional Features:<br>• Support for unlimited Private applications<br>Refer VSPA Professional features in VSIA datasheet. |  | ✓ | ✓ |
| Versa Secure Internet Access Elite Features:<br>• API based Cloud Access Security Broker<br>• Data Loss Prevention<br>• Advanced Threat Prevention<br>• XOT security<br>Refer VSIA Elite features in VSIA datasheet. |  | Optional | ✓ |

For more details please refer to Feature Matrix of Versa Secure Access Fabric offering.