VERSA NETWORKS

WHITE PAPER

Secure Internet Access

A Modern Approach to Protecting Web Traffic

Protecting the Modern Enterprise

‘Remote Access’ to an Enterprise initially only dealt with access to the Enterprise network. With the increasing frequency of malware infecting computers, the Enterprise concern turned to how to prevent malware infection and compromise of devices such as laptops and mobile phones which would eventually connect to the enterprise network remotely. Some enterprises mandated that corporate issued devices would need to constantly connect to the VPN to have either access to company resources or any connection to the external web. This was not an ideal solution to the problem in that it required the Enterprise to purchase and issue a computer to every remote worker, caused the bandwidth utilization at the VPN concentrator location to increase, and decreased the speed of internet connections causing issues with updates and downloads. To deal with these problems, Enterprises soon turned to a ‘Bring Your Own Device (BYOD)’ model or a VPN only for access to the internal corporate network. By not overloading the VPN connection, organizations helped reduce the Internet connection links load, provided control for important software updates, and, in the BYOD model: greatly reduced the infrastructure costs. However, this introduced a new issue – how to limit the exposure of the authorized computer from being compromised while it is NOT connected to the enterprise network. Enterprises realized that users accessing the Internet, either via a split-tunnel directly to the Internet or disconnecting from the corporate VPN, exposed the Enterprise network to potential threats and vulnerabilities.

Initially, Enterprises implemented Internet proxies that would sit between the authorized device and the Internet, and these proxies would then filter the Internet traffic and provide a level of malware protection. However, this model still had the issue of the increased Internet traffic at the proxy location. The increased load was due to the traffic coming to the Internet proxy, being forwarded out to the Internet destination (if authorized), being received from the Internet destination by the proxy, and then finally forwarded back to the authorized computer – all from the same connection. Thus, a single IP packet was counted twice on the link of the proxy. Also, proxies have resource limitations for the number of concurrent connections as well as number of simultaneous packets per second processed. In order to support all the traffic, organizations would need to deploy numerous proxies, both for redundancy and capacity. Lastly, the end user experience was also constrained as the Internet traffic was hair-pinned to an Enterprise location.

Coupled with the increasing need to protect intellectual property, private and sensitive data, or due to regulatory requirements, Enterprises also needed to make sure that information was not shared improperly. With these needs in mind, Enterprises started to seek out cloud delivered security services. Early implementations of the cloud delivered security services did not provide a secure method of private access, so a split tunnel model was deployed so Enterprise traffic was directed to the corporate VPN, and Internet traffic was then directed to the cloud security service. However, there are known vulnerabilities and exploits when utilizing some split-tunnel techniques. To protect against threats, Enterprises deployed the full tunnel models for both VPN and Internet access. While this did add extra protection, there was increased management costs to maintain both split tunnel and full tunnel models. Also, the end user experience was not optimal because if the user, who mainly uses Internet assets, needed to access a company asset, the end user needs to initiate the VPN, access the company asset, and then disconnect the VPN – causing more friction in their day-to-day functions.

Emergence of SASE

The emergence of Secure Access Service Edge (SASE) melded the broad spectrum of security services and Software Defined Wide Area Network (SD-WAN) together in a way that optimally provided Enterprises an architecture to protect users, devices, and applications anywhere in the world. Initially, the secure Internet access focused on the common use case of web access for the users, as most Internet assets are web based. The industry coined the term Secure Web Gateway (SWG) as the cloud delivered entity that authorized access and provided security functions such as firewall, encryption, URL filtering, and domain name filtering. The term SWG is still utilized today; even though, the traffic handled by the SWG is no longer only web traffic.

By coupling security services with SD-WAN, a SASE Solution provides not just the most secure connection between the user and the resource, but also the most optimal network path. SD-WAN allows for consideration of performance of the network and allows for assignment of policies per application. This allows for the best secure network performance per application.

With the migration to Secure Access Service Edge (SASE) models, the security providers, and the SD-WAN providers were able to pivot the solutions to include a Secure Internet Access solution to protect against Internet threats. However, there are many existing and legacy vendors that offer varying portfolio of products on what they define as 'Secure Internet Access' that are not consistent in features and capabilities. This variance in definition of 'Secure Internet Access' has led to much consumer confusion and market obscurity.

Three Models of Remote Access

Today, there are three models for employee remote access: (1) private-only access, (2) Internet-only access and (3) both private and Internet access.

1. Private-only access model represents a tight control by the Enterprise that wants all traffic to be directed only to the Enterprise. This may be due to regulatory requirements or a corporate need to provide all security via the enterprise network. Enterprises typically use this model when the majority of the assets an employee needs to access is contained within the Enterprise network.
2. Internet-only access model represents a scenario where the Enterprise assets are mainly cloud-based or most of the Enterprise applications are SaaS delivered. Thus, access to the private network either does not exist or is not needed. Example of this type of service might be a manufacturing plant where most work must be done on site and only supporting financial, human resources, or sales functions are cloud delivered. Alternatively, that Enterprise can be using a separate solution for VPN connectivity and if so, that will translate to a disconnected experience from the secure Internet access as the client will have to connect to the private network or resources or will have to connect to Internet in a mutually exclusive way. In this model, the user experience suffers.
3. The hybrid model of both private and Internet access is where the employee needs both Internet and private access at the same time. This model is the most common method of remote access and is utilized the most on the market. This integrated solution offers an ideal user experience because security policies and proxy functions will be consistent and used only once.

Most SASE providers offer solutions that incorporate all three remote access models. Best SASE practices also incorporate a single pane of glass for orchestration and management and a converged network delivery system.

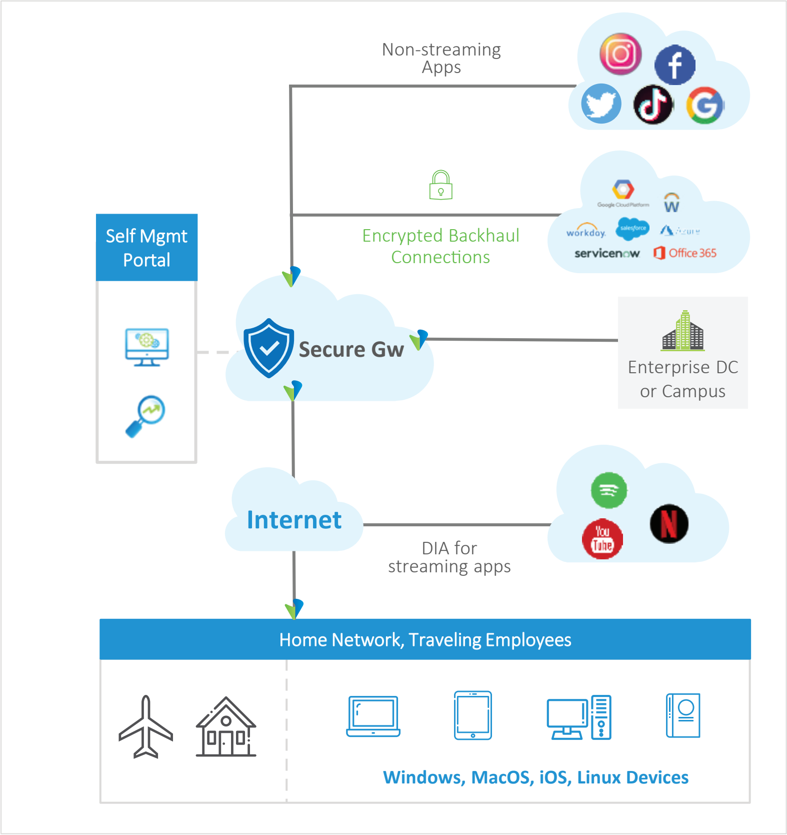
What is Secure Internet Access?

What is a Secure Internet Access? What are the components that make up Secure Internet Access and what are the benefits? Why is a native SASE vendor the best choice to deliver a strong and resilient Secure Internet Access solution?

Secure Internet Access typically includes integrated VPN solution to provide connectivity for remote users.

A typical VPN solution is composed of a VPN concentrator (appliance) installed on the Enterprise network (normally at a data center) and a VPN client installed on the device that the employee would utilize to create the secure connection to and from.

For a traditional VPN solution to provide the Internet Access, the Internet traffic is backhauled all the way to the enterprise location and then forwarded on to the Internet. This doubles the traffic on the VPN concentrator and also requires doubling the capacity of the Internet connection.



In a SASE model, Secure Internet Access has the same two components that the VPN service has. The VPN concentrator and the tunneled connection to the VPN concentrator. In this model, the Secure Gateway replaces the VPN Appliance. Unlike the VPN appliance that is installed within the Enterprise premises, the Secure Gateway is instantiated in the Cloud which allows for flexibility, scalability, and elasticity. A cloud instantiation provides multiple access points to single or multiple Secure Gateways allowing the solution to scale and provide connectivity for different availability zones or regions around the world.

Cloud-based Secure Gateway also provides many more security functions than the traditional VPN solution. An key functionality of a Cloud-based Secure Gateway is to limit the exposure of the authorized computer from being compromised while it is not connected to the Enterprise network. Clearly, accessing the Internet exposes the user's computer to many threats. Security services like a firewall, Data Loss Prevention, Malware protection, Cloud Access Security Broker, and many other functions need to be implemented to assure that the computer is not compromised while accessing the Internet. Such capabilities provide a comprehensive security to the clients and protect them from threats and vulnerabilities originated from the Internet.

Furthermore, the Secure Internet Access solution allows for two tunnel models when connecting to the Cloud-based Secure Gateway.

The first option is the use of a SASE Client. As seen below, a SASE Client that is installed on the employee device will connect to a Secure Gateway when accessing Internet resources. This connection provides an encapsulated and encrypted path to the SASE Service which provides numerous data privacy, security and performance benefits. This option is used typically when the user is connected from outside of the office.

The second option is to have an encapsulated and encrypted tunnel from either a router or firewall. This tunnel could be part of an SD-WAN solution or traditional routers or firewalls that exist in the Enterprise network. The encapsulated tunnel allows for inclusion of the Secure Internet Access solution to the Enterprise network based on standard IKEv2 based IPsec tunnels. Alternatively, SD-WAN would allow for a more granular control of the traffic across the encrypted tunneled connection as it deals with performance and application. The ability of the traditional tunneled connections to deal with application and performance or other granular aspects is generally lacking and basic traffic management capabilities of the router or firewall may be utilized in those gaps. Where there are multiple tunnel connections to the Secure Internet Access solution, the gateway would determine the best path for returning the traffic based upon the best performing tunneled connection, whether that is for all application flows or arbitraged for different application flows.

Stand-alone Secure Internet Access services would not have a connection back to the Enterprise network. A Hybrid model would include both the Internet access and the private access.

Since Secure Internet Access is part of a SASE Service, the SASE Service will provide security services at a Secure Gateway in which is part of the SASE Cloud. This set of security services may be extensive. Secure Internet Access solutions should offer the following security functions at minimum: a network firewall, an Identity and Access Management solution, a Cloud Access Security Broker, malware detection and response, a Data Loss Prevention (DLP) solution, an Intrusion Prevention System (IPS), and more. Each of these security services are necessary for assuring that the access is authorized and the data that is entering and leaving the Internet and cloud services are protected.

Versa Secure Web Gateway (SWG)

Versa Secure Web Gateway (SWG) is Versa Network's implementation of the Secure Internet Access. Versa Private Secure Access is an integral component of the Versa SASE Solution. Secure Internet Access can be purchased as Versa SASE Service (SASE-as-a-Service) or as a stand-alone Secure Internet access service (SWG-as-a-Service). Both options come with a SASE Client, Secure Gateways (as a Cloud Service), and an extensive suite of security services. However, the Versa SASE solution has more security services than the stand-alone SWG such as the ability to utilize SD-WAN for the network connectivity.

The Versa SASE Client has the ability to connect to multiple Secure Gateways from anywhere in the world. This approach provides resiliency because it does not have to re-establish a connection to the SASE service in the event of a network failure, allowing for optimal up-time. The Versa SASE Client can select the best Secure Gateway based upon performance metrics of the network connectivity to a given Secure Gateway and the performance of the Secure Gateway itself.

The Versa SASE Client is available on the following platforms:

- MacOS
- Windows10
- iPhone
- Android
- Linux

The SASE Client acts as the first point of policy enforcement. As an enforcement point, the client captures data regarding the connecting device and the user requesting access. Based upon appropriate corporate policy, the client will determine how the traffic gets steered to the SASE Service and which applications can be access directly from the Internet. The Versa SASE Client also has the ability to direct traffic based upon corporate policy through a secure, private connection.

Defining SWG Policies

Policies for the Secure Internet Access are broken into two parts:

1. the authentication and authorization of the user to use the SASE service; and
2. the authorization of the user to a perform an action through the service.

The SASE Client authenticates the user based upon multiple methods in alignment to the defined corporate policy. For example, this policy could require that the authentication be issued via SAML, LDAP, SSO and include a traditional login-password combination, multi-factor authentication, one-time password, or certificate authentication. Based on the policy, different authentication methods could also be triggered based on the contextual access of the user: geolocation, time, device health, and more. For example, an LDAP authentication is required when accessing from the employee's home, but additional multi-factor authentication is required for when the employee is traveling and accessing from new locations.

There are many offerings in the market that provide secure access to applications. Versa allows for organizations to:

- Apply policies to ensure that users who are authorized to access specific applications are only allowed to reach the intended application to protect against unauthorized access.
- Apply policies which hide the network topology of the applications from the users and vice versa to reduce the attack surface.

SASE Gateway provides secure access intelligently with a combination of Forward proxy, CGNAT, ALGs, and DNS proxy to ensure that the end user clients are not exposed to actual IP Address space where the applications are hosted. Thus, a malicious user who may have access to the device will not be able to perform reconnaissance on the internal network and are thwarted from performing further attacks. The Secure Internet Access solution works seamlessly with variety of other applications including FTP, Voice, and Video.

The SASE Client has the ability to enforce device compliance based upon many different factors like:

- Anti-Virus version
- Anti-Virus signature version

- Operating System type and version
- Operating System patch
- Corporate device or personal device
- Specific software installed on device
- Other parameters

By inspecting a multitude of risk factors on the device, organizations can establish an End Point Information Profile (EIP) when devices are connecting to the Enterprise network. Included in the EIP are additional checks such as a compliance check and reporting about the remote access attempt.

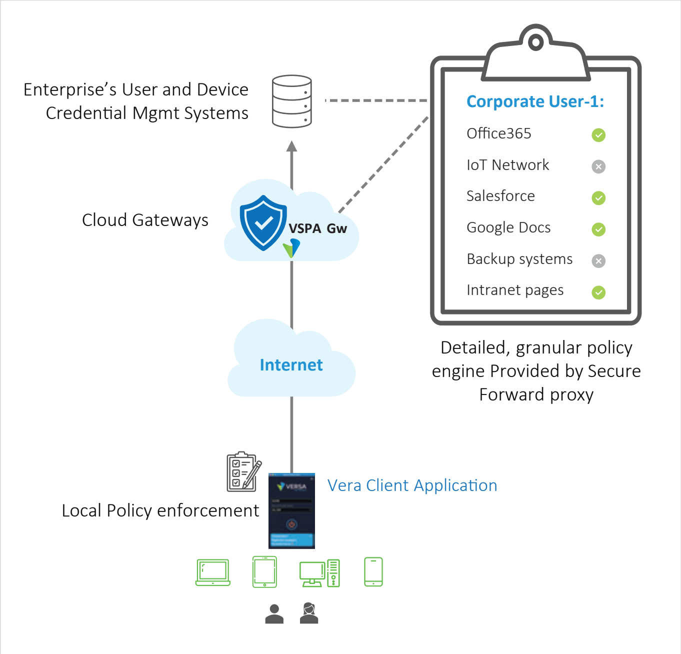
The EIP also provides the Enterprise with a method to deal with IoT devices. Typically, IoT devices do not allow for the implementation of a client. So, identification of the sanctioned IoT devices versus the rogue IoT devices is rather difficult. By using the EIP, the SWG solution can distinguish one IoT device from another and determine if it is authorized or not. Thus, organizations can apply the appropriate corporate policies depending on the level of risk.

Versa recommends looking for a solution that provides all this information visible through the big data-based analytics platform that is integrated in the SASE dashboard. This SASE dashboard will be extremely important for demonstrating corporate and regulatory compliance.

The Secure Internet Access solution must also authenticate a user when they are accessing via their compliant device and once authenticated, the corporate polices will determine if the user is allowed to perform the requested actions. Corporate policies can be applied at the application level to give a wide granularity of control such as requiring session authentication or restricting access within an application. In addition, corporate policies can be further narrowed to include a specific user and a specific application flow with a specific set of contextual parameters such as not allowing a remote user to access sensitive HR files within an application. The set of contextual parameters might include the EIP parameters, and the corporate policies would determine which security functions would be applied to the application flows.

This granular set of policies could be used to forward streaming applications directly to the Internet while other Internet traffic would be directed to the SWG solution. Another example would be that specific user (such as the CEO) is permitted to access a particular highly confidential file only from a specific device with a specific EIP.

For Bring Your Own Device (BYOD) scenarios, connections to the Versa SASE Service can be made without the installation of a Versa SASE Client. The Full-Forward IP proxy would provide a captive portal for these devices to register, get authorization, and then get access granted. Where a Versa SASE Client is not utilized to the secure connection, the secure connection can only send the traffic to the SASE Secure Gateway and at that point the SASE Service would be the enforcement point to implement the corporate security policies.



Leveraging Cloud Gateways

The Versa Secure Gateways can be implemented in numerous Cloud provider environments such as AWS, Equinix, Microsoft Azure and on hosting provider environments. Cloud Gateways allow for greater flexibility because multiple SASE services can be offered. Having a global, dispersed network of Points of Presence (PoPs) provide greater flexibility and fault tolerance. In addition, having more PoPs provides better customer performance because the connection can be determined by the best performance path through a Secure Gateway to leverage all of the SASE Services.

Since the Versa SASE solution utilizes a Full-Forward Proxy, the Enterprise cloud networks are obscured from the public and does not expose the actual IP addresses of the Enterprise cloud resources.

The Versa SASE solution allows the Enterprise to establish multiple Cloud providers or SaaS network connections either over a public Internet or via a private network access method, such as a SCI (AWS) or Express Track (Azure).

In addition, Versa SASE has the ability to connect to an Enterprise's private virtual cloud instances. By using Versa SASE Secure Gateways in Cloud instances, the Versa SASE Service can utilize SD-WAN capabilities within the Versa SASE Gateways to route the appropriate applications to the target Cloud instances based upon network performance and the performance of the application Cloud instances.

Versa Security Services

Versa has numerous security services that can be utilized to protect traffic and assure that the Enterprise is protected against breaches and threats. For example, any information that is crossing the Enterprise network should be analyzed for malicious content and any data that is leaving the Enterprise network needs to be cross referenced against the Data Loss Prevention policies and ensure that no intellectual property is being lost. In addition, devices accessing the Enterprise network need to meet the minimum corporate software compliance check and that all sensitive information has been secured.

In a Secure Internet Access solution, the corporate policies dictate which security services are applied to which users, application flows, devices, or connections. This can be a broad definition that applies to all user or all applications, or it can be a very granular policy that applies to a single user, single application, on a single device with a specific set of circumstances.

Versa offers the following security services:

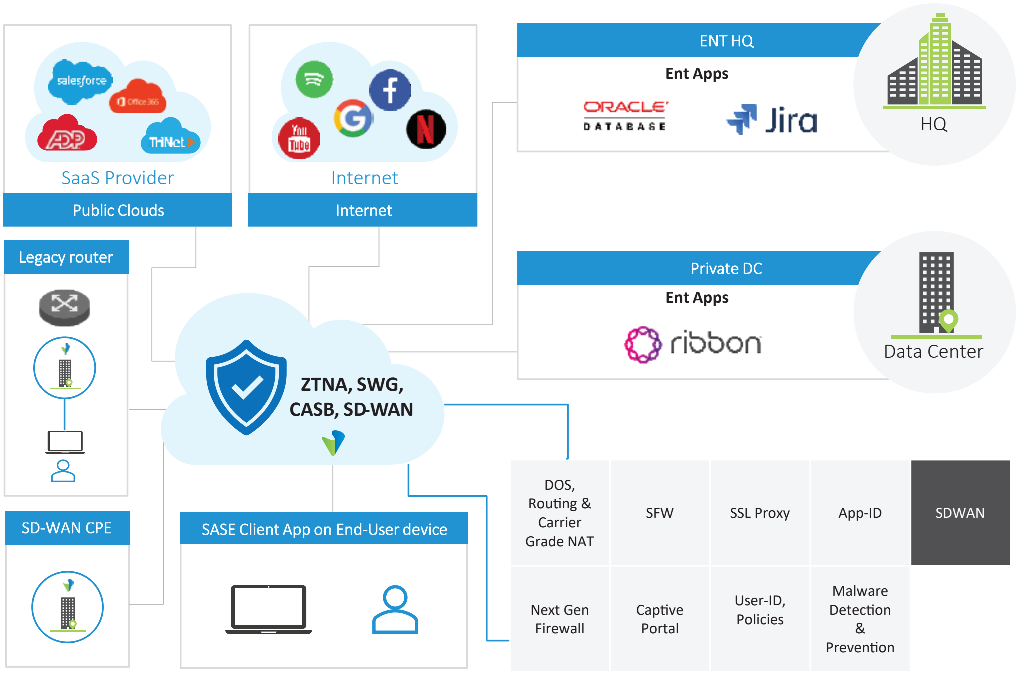
- Next Generation Firewall
- Application Aware Access Control
- Identity and Access Management
  - SSO
  - SAML
  - Active Directory
  - Multi-Factor Authentication
- Endpoint Security Compliance

    - Operating System Version
    - Anti-Virus Version
    - SASE Client Level
    - Firmware Level
    - Patch Level
- Cloud Access Security Broker
- Malware Detection and Response
- Data Loss Prevention
- Intrusion Detection and Prevention System (IPS/IDS)
- Secure DNS Proxy
- Domain Name Filtering
- URL Filtering
- Full-Forward IP Proxy
- Captive Portal

Specifically, Enterprises should consider SWG offerings that include multiple methods for URL classification, URL risk and reputation, and capabilities for managing traffic to those destinations. Versa SWG contains all these aspects and enables the Enterprise to craft granular policies that look at a variety of risk factors.

Given that 80 percent or more of Internet traffic is HTTP or HTTPS based, SWG offerings must have a full forward proxy. Versa SWG has a full forward proxy as well as an SSL-TLS proxy to help with the isolation of the HTTPS traffic. The SSL-TLS Proxy allows the SWG to apply security functions to the encrypted HTTP traffic and prevents encrypted connections from introducing malware or other malicious content to the Enterprise network. The full forward proxy handles the remaining internet traffic and provides the capability to inspect non-HTTP encrypted traffic.

Versa SWG and Versa SASE Services offer multiple methods to consume the security services listed above. Both Versa SWG and Versa SASE provides for multiple tiered levels of security to meet any business need.

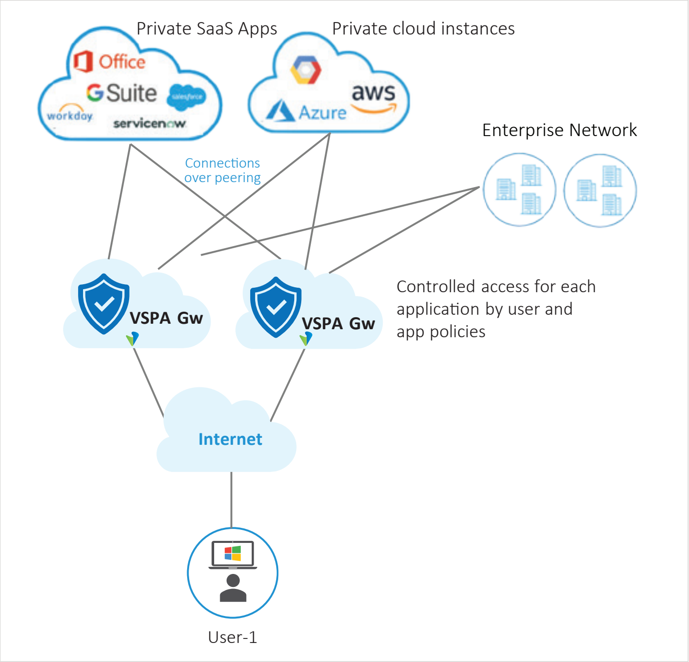


DOS, Routing & Carrier Grade NAT	SFW	SSL Proxy	App-ID	SDWAN
Next Gen Firewall	Captive Portal	User-ID, Policies	Malware Detection & Prevention	

The Enterprise Advantage with Versa SASE

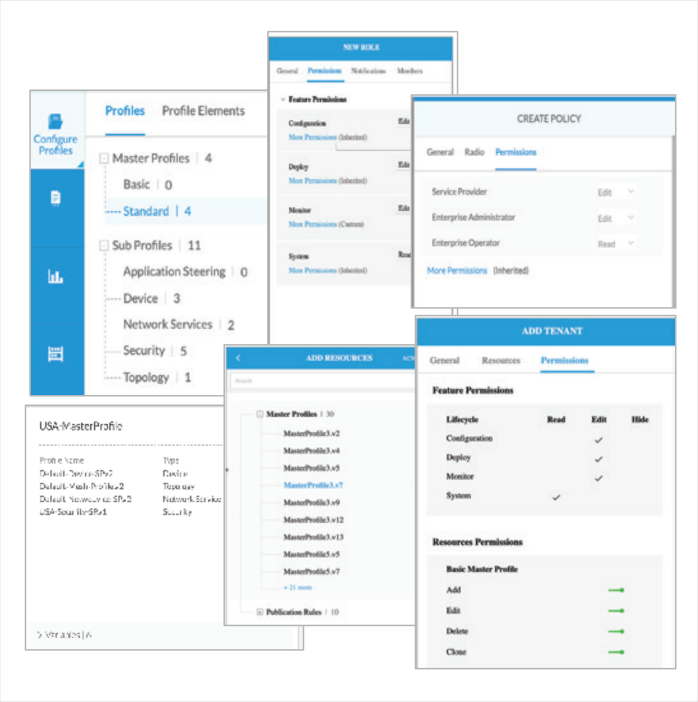
Utilizing Versa SASE provides benefits to the Enterprise customer in five different ways:

1. Since all the security services are being provided by the Versa SASE Service, application performance is improved by utilizing a single-pass architecture where networking and security services are being performed in one transaction without chaining together appliances, connections, or other services. The single-pass architecture allows for the IP packet to be inspected once and then security enforcement is performed on the IP packet concurrently. In a traditional architecture, many third-party security services would not receive the benefit of a single-pass architecture because the data packet would need to be analyzed in multiple products and services and every time would require rescanning the IP packet, thus causing delay and jitter.
2. The Versa SASE Service provides the ability to scale the security services to meet IP traffic flow demands. Based upon performance metrics, multiple security services can be instantiated at once. Also, different security services can be applied to the Enterprise traffic based upon specific enterprise policies such as the ability to use the Endpoint Security Compliance to either force compliance or add security services to devices that are not compliant. For example, Malware Detection and Response might be



added to an application flow for a given user where the user's device does not have the latest revision of Anti-Virus software.

3. By utilizing Versa SASE, Versa Secure Gateways, and Versa SASE Client, the Enterprise gets the best application flow performance as these components will use the industry's leading SD-WAN to determine the most optimal path. In this flow, the path to the application is optimized all while ensuring that all security checks are being enforced as dictated by the Enterprise policy.
4. Versa SASE allows for the security and network policies to be instantiated in a single orchestrator in a single pane of glass. In a central management, there is no need to configure multiple platforms. Through an easy-to-use configuration portal, Versa SASE allows for easy administration and management of security and network policies that are being enforced to all access points within the network.



5. Versa SASE allows for a common telemetry plane that has centralized analytics that visualizes all the pertinent information regarding the SASE Clients, Secure Gateways, security services, and SD-WAN. Analytics is critical to providing a seamless and complete view of the Enterprise traffic both from a forwarding and security perspective. In addition, the Versa Analytics platform has the ability to integrate with any existing and current Network Management systems.

Versa Networks realizes that any network transformation requires Enterprises to have the ability to protect the network investment that have already been made. Therefore, the Versa SASE Service does not mandate that all the security services or devices be exclusively from Versa, and the SASE platform integrates seamlessly with many leading vendors.

However, leveraging a single-pass architecture with Versa SASE delivers all the benefits of a "As-A-Service" model where you get optimal networking and security with low latency and costs. To meet the demands of a post-pandemic workforce that demands a new approach to the legacy VPN model, Versa Secure Web Gateway is the best solution for delivering Secure Internet Access from anywhere in the world all while protecting users, data, devices, and applications.

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