Versa Secure Access

Introduction

Secure SD-WAN (Software Defined WAN) has revolutionized the user experience for Multi-Cloud/SaaS applications. Versa Networks has led this transformation by integrating in Application/ Network/ User Intelligence into a single platform, with centralized management/monitoring, historical reporting, and automation to the WAN Edge.

Today, enterprises 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.
- Users are connecting from everywhere. COVID-19 has changed the workplace to a new normal where employees Work from Anywhere, and the employee's home is the new office.

Challenge

Work from Anywhere culture implies distributed users and multi-cloud enterprises have distributed applications. Public Cloud infrastructure come with a big advantage: global availability of elastic compute and storage resources that can scale up/ down immediately. In this new era where users and applications can be anywhere and everywhere, traditional Remote Access solutions that are appliance-based are challenging to scale and do not offer the best application experience.

In order to extend a secure and reliable application experience for employees working from home or anywhere, there is a need to extend the principles of SDWAN induced user experience acceleration to users who are accessing the network remotely. It is no longer sufficient to just provide connectivity for remote users. Enterprises need a solution which extends their security perimeter all the way to the user and provides enhanced user experience, visibility into the application performance and usage.

Presenting Versa Secure Access: a secure solution connecting your workers working from anywhere to your enterprise applications hosted in enterprise environments, private clouds, or public clouds. The Versa Secure Private Access protects both the applications and users using a Zero Trust Network Access (ZTNA) framework.

Versa Secure Access is a cloud-managed, cloud-delivered private access service efficiently connecting distributed users with distributed applications without compromising on security or user experience. This is a ZTNA offering based on the fundamental philosophy of verifying every network access by a user. In the context of secure access, the ZTNA requirements translate to:

- Application Segmentation to restrict access of the applications
- Enterprise grade authentication with Multi-Factor Authentication (MFA)
- Per user/user-group based application control
- Network obfuscation and topology hiding
- Application and Network Visibility

The Versa Secure Access solution is a Zero Trust Network Architecture (ZTNA) built on the Secure Access Service Edge (SASE) framework: Integrating the Security, Identity management cloud and SD-WAN into a simple, hassle-free service that:

- Extends perimeter protection to the end-user device

- Delivers an always-on application experience
- Is highly scalable and extensible to allow users to work from anywhere

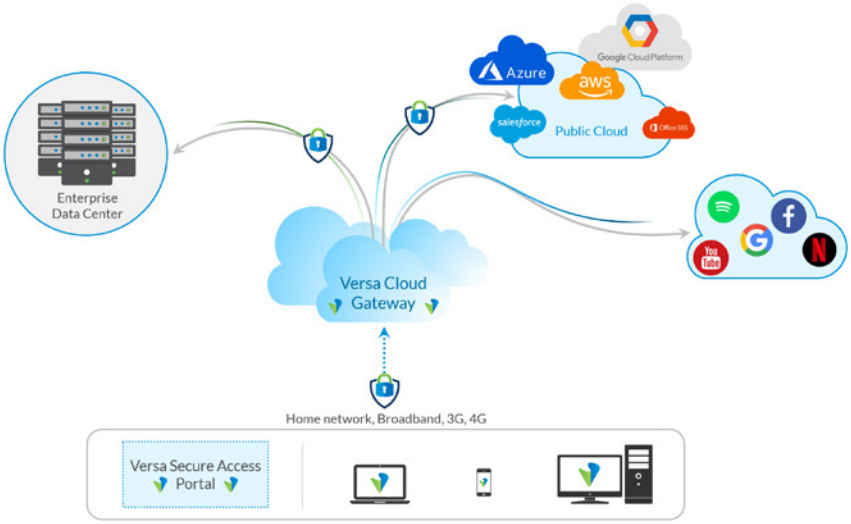
Service Components

Versa Secure Access is a distributed solution to connect distributed users to enterprise applications. The applications can be distributed across private cloud, enterprise data centers and public cloud. The Secure Access Solution consists of:

Versa Cloud Gateways are based on industry leading VOS™ platform. They are globally distributed to provide distributed secure on-ramps for access to enterprise applications. Gateways authenticate users, authorize the application access and secure the enterprise network from external threats. Versa Cloud Gateways are built on VOS that integrates advanced routing, comprehensive security, market leading SD-WAN along with secure access. The Versa Cloud Gateways securely connect to and integrate with existing infrastructure in Enterprise network and datacenter.

Versa Secure Access Client is software agent/application that runs on and extends SD-WAN to client devices (ie: Windows, MacOS computers, smart phones[1]). Versa Secure Access Client creates a secure and encrypted connection from remote device to the Versa Cloud Gateway. Upon authentication and access authorization through the Versa Cloud Gateway, users with VSAC can securely connect to enterprise applications in public and private cloud

Versa Secure Access Portal provides enterprise administrators the ability to monitor the service and provides real-time and historical reporting at a network, application, and user level leveraging Versa's big database Analytics platform.



Key Service Capabilities

Micro-segmentation

Versa Secure Access uses micro-segmentation to control and limit the application visibility to authorized users. Users can be configured to use the Versa Secure Access Client to connect to different gateways for different applications. Application and Gateway combination is dynamically configured to give best application experience and provides an additional level of security is provided by preventing the user from the accessing gateways from which the application is not accessible or not preferred. With support for multiple gateways*, customers can dedicate certain gateways for secure applications while allows users to access generic applications from other gateways.

User Authentication and Authorization

Versa Secure Access leverages the enterprise's preferred Identity Provider to authenticate and authorize the user. Versa Secure Access integrates with various types of authentication servers like Active Direc-tory, SSO servers like OKTA and different authentication protocols like LDAP, and SAML[2]. The Enterprise Identity is used to authorize the users for application access policies.

[1] Will be released with 6.4 version of the client
[2] Available with upgrade to 20.4 release of VOS
* Roadmap

Multi-Factor Authentication (MFA) using SMS and Email is supported by Versa Secure Access. Additionally, Time-based OTP integration with Microsoft Authenticator, Google Authenticator and Duo is available. VSA is integrated with SSO Identity provider MFA as well.

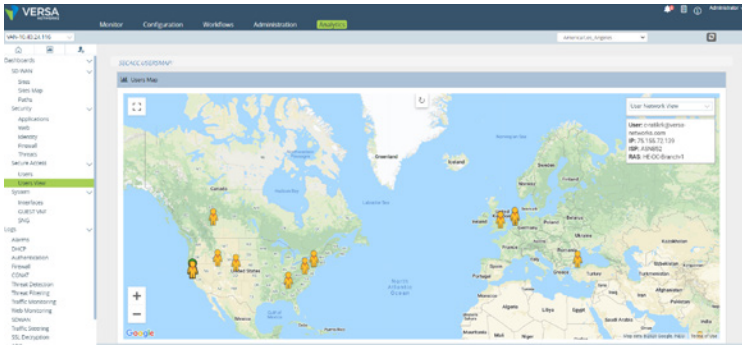
Application Firewall

Versa Secure Access enforces policies which authorizes access to application on a per user/user group basis. The applications can be defined using FQDN/Host name, wild cards, IP address subnet and ports or combination of these. The policies are based on the username/group information received during the authentication from enterprise identity servers.

Network Obfuscation

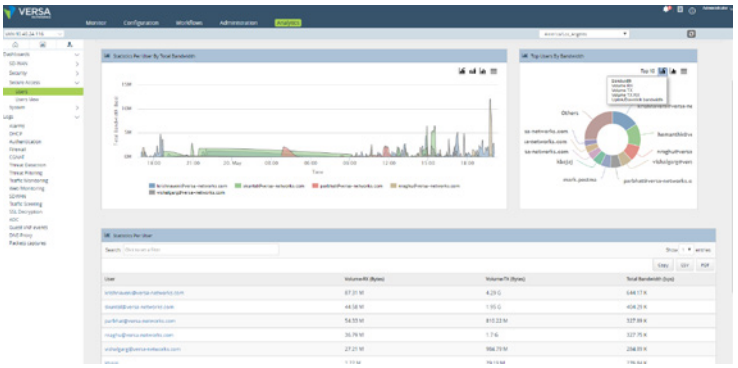
Network obfuscation is a security technique to hide internal network topology from remote users. Topology hiding protects the applications from multiple attack vectors like lateral movement, port-scanning, etc.

Versa Cloud Gateway obfuscates the application server IP address from the user and user IP address from the application server. This provides the highest level of protection from malicious actors in the internet.



Application and User visibility

Application, User and Network visibility is necessary to efficiently operate the network and to secure it from external threats. Versa secure access builds on top of big data based Versa Analytics platform to provide the network administrators with real time view as well as historical reporting of Users, Application and Network.



Assured Application Experience

Versa's market leading Secure SD-WAN functionality ensures the application experience for the users, no matter where they are connecting from. Versa secure access applies various techniques like SLA monitoring, Traffic engineering, Forward Error Correction* that have been extensively deployed in con-necting branches now to this software-based service

- Intelligent Gateway Selection ensures that the SASE client connects to the gateway which provides the best user experience. The SASE client choose the best gateway based on various parameters like server load, cloud gateway proximity, and network performance towards the gatway.
- Hot Stand-by feature ensures that the SASE client is simultaneously connected to multiple gateways. The SASE client monitors the performance towards individual gateways. Flows are routed towards alternate gateways instantaneously upon detection of degraded performance towards the primary cloud gateway.
- Traffic Steering is supported based on Application, FQDN, and/or Routes. The traffic steering policy determines breakout of traffic, selection of gateway and whether encryption is needed for traffic tunneled towards the gateway.
- VSA service also supports creation of encrypted and unencrypted tunnels towards the Cloud Gateways. The unencrypted tunnels provide better latency characteristics for real-time traffic which might support appplication-level encryption of the traffic.

Versa Secure Access supports geo-location, user and application policy to ensure clients connect to the closest gateway based on current user location. Versa Secure Access Client can connect to a multiple gateways* based on which application is being accessed. Versa Secure Access Client makes the routing decision to the best available gateway based on real time network information.

* Roadmap

Cloud hosted applications are accessed directly from the Versa Cloud Gateways. As the applications avoid hair pinning to enterprise DC only to break out into the cloud again, the application experience is improved. The resources required at the data center are also reduced.

Customers can also extend the connectivity to the Public cloud workloads and select SaaS applications over a private link.

Service Tiers

The Versa Secure Access subscription is available in two tiers:

Features	Essentials Standard	Professional Standard
SASE Client for Windows 10, MAC OS SASE client provides secure connectivity from end-user device to Versa cloud gateways.	✓	✓
Intelligent Gateway Selection The SASE Client automatically chooses the nearest and healthiest gateway based on proximity to the gateways, Load (CPU, Memory etc	✓	✓
Authentication with Enterprise authentication server Integration with LDAP/Active Directory, SAML based SSO, MFA support with Microsoft Authenticator, Google Authenticator, Duo	✓	✓
S2S tunnels to Enterprise DC	✓	✓
Perfect Forward Secrecy and Top of the Line Enterprise Class Encryption	✓	✓
Network Obfuscation Network topology hiding	✓	✓
Built in Security (SFW, DOS Protection)	✓	✓
Application, Network and User visibility	✓	✓
ISP and Connection Performance Visibility Provide network performance analytics (including ISP, Region etc	✓	✓
Service Reliance (Cold Standby)	✓	✓
App Whitelisted per User (10 Applications) Upto 10 Applications can be controlled per tenant	✓	✓
App Whitelisting for unlimited apps		✓
Redundant Gateway on Hot Stand-by		✓
Encrypted and Unencrypted tunnels to Gateway		✓
App based Traffic Steering		✓
Active-Active connections to multiple gateway		✓
Streaming to 3rd party analytics server		✓

Private Gateways

For customers who expect enhanced privacy, Versa Secure Access offers cloud hosted private cloud gateways. While ensuring the benefits of a cloud service, the private gateway provides unprecedented privacy to the customer by the means of dedicated gateway instances. In addition to the features supported by Professional Standard tier, the Professional Private tier includes:

- Direct Public Peering with SaaS applications (up to 2 SaaS Applications among selected apps)
- Direct Private Peering to Multi-Cloud (up to 2 VPCs in the same region)
- Dedicated gateways with redundancy

VERSA NETWORKS

Versa Networks, Inc, 6001 America Center Dr, 4th floor, Suite 400, San Jose, CA 95002 | Tel: +1 408.385.7660 | Email: info@versa-networks.com | www.versa-networks.com