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, reliable, application experience for employees to the 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 cloud managed cloud delivered Zero Trust Network Architecture service to efficiently connect distributed users with distributed applications without compromising on security or user experience. Zero Trust Network Architecture (ZTNA) is based on the fundamental philosophy of trusting no one. In the context of secure access, the requirements translate to the following differentiated features of Versa Secure Access:

- **Application Segmentation** to restrict access of the applications
- **Enterprise grade authentication** with Multi-Factor Authentication (MFA)
- **Granular application control**
- **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

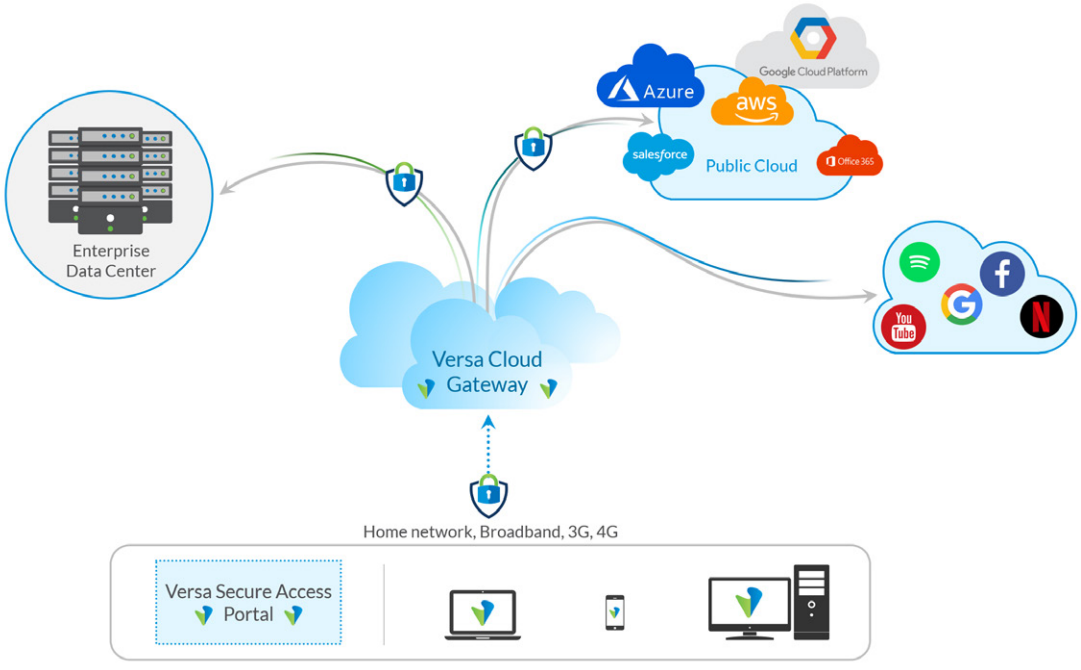
Service Components

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 VOSTM 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 cli-ent devices (ie: Windows, MacOS computers, smart phones[1]). Versa Secure Access Client creates a se-cure 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 is provides enterprise administrators ability to monitor and manage granular view of users and applications. Versa Secure Access Portal provides real-time and historical reporting at a network, application or user level.



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

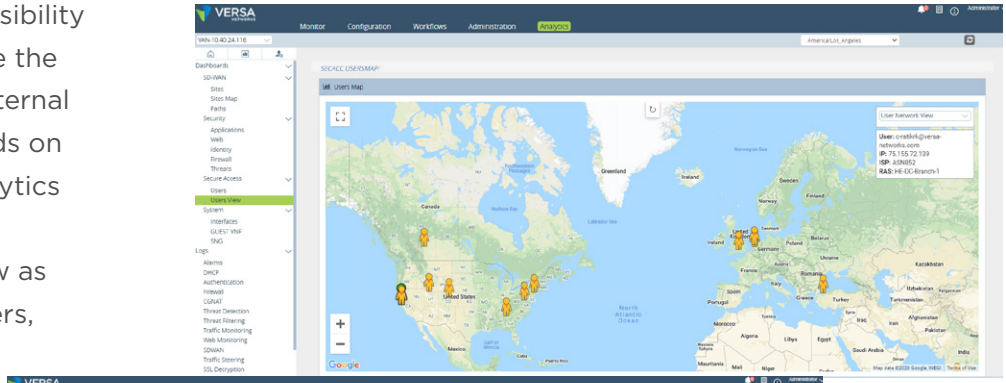
Versa Secure Access leverages the enterprise's preferred Identity Provider to authenticate and authorize the user. Versa Secure Access integrates with various types of authentication servers like RADIUS, Active Director, SSO servers like OKTA and different authentication protocols like EAP, LDAP, Kerberos,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

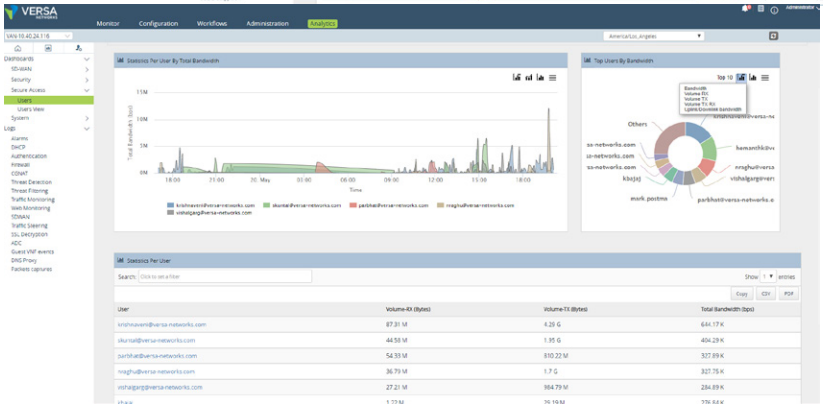
Application Firewall

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.

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[2], Traffic engineering[2], Forward Error Correction* that have been extensively deployed in connecting branches now to this software based service.

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.

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.

Private Gateways

For customers who expect enhanced privacy, Versa Secure Access also offers cloud hosted private gateways. While ensuring the benefits of a cloud service, the private gateways provide unprecedented privacy to the customer.

Service Tiers

The Versa Secure Access is offered in following flavors:

Features	Essentials	Essentials-Private	Professional	Professional - Private
VPN Client for Windows 10, MAC OS	✓	✓	✓	✓
Connections to multiple Cloud Gateways*	✓	✓	✓	✓
Authentication with Enterprise authentication server	✓	✓	✓	✓
S2S tunnels to Enterprise DC	✓	✓	✓	✓
Perfect Forward Secrecy and Top of the Line Enterprise Class Encryption	✓	✓	✓	✓
Built in Security (SFW, DOS Protection)	✓	✓	✓	✓
Application, Network and User visibility	✓	✓	✓	✓
Service Reliance (Overcoming Gateway failure)	✓	✓	✓	✓
App Whitelisted per User (5 Applications)	✓	✓	✓	✓
App Whitelisting for unlimited apps			✓	✓
Streaming to 3rd party analytics server			✓	✓
Direct Connectivity to SaaS apps[2]				2 Apps
Direct Connectivity to Multi-Cloud				2 VPC connections (Same region)
Dedicated back up Gateway within geo location				✓

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

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