Versa Secure Private Access

Introduction

Cloud has revolutionized the user experience for applications and data. Versa Networks has led the transformation by providing Software Defined Networking with SD-WAN and with SSE. Versa's Software Defined Solutions provide integrated Application, Network and User Intelligence in a single platform, with centralized management/monitoring, historical reporting, and automation at the WAN Edge, on private and public cloud instances

Today, enterprises are faced with the following reality:

- Digital Transformation has accelerated the migration of enterprise applications and work-loads 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 into a hy-brid workspace where employees are as likely to work from office as Work from Anywhere.

Challenge

Work From Anywhere (WFA) requires support for distributed users, distributed applications and multi-cloud for Enterprises. In this new era users and applications can be anywhere and everywhere, legacy Remote Access solutions that are appliance-based are challenging to scale, they do not meet latest Ze-ro Trust Network Access (ZTNA) security requirements and they do not offer the best application expe-rience.

In order to provide a secure, policy controlled and reliable application experience for employees Work-ing from Anywhere, there is a need to extend the principles of Software Defined Networking in this new class of solution to provide the right ZTNA solution that meets today's requirements. It is no longer sufficient to just provide VPN 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 Private Access: a software defined secure solution connecting your workers working from anywhere to your enterprise applications hosted in enterprise environment, private clouds or public clouds. Versa Secure Private Access (VSPA) protects both the applications and users using the latest Zero Trust Network Access framework.

Versa Secure Private Access (VSPA) is a cloud managed, cloud delivered, private access service effi-ciently connecting distributed users with distributed applications without compromising security or us-er experience. This ZTNA offering is based on the fundamental philosophy of verifying every network access request originated by the user. In the context of secure private access Versa's ZTNA scope trans-lates to:

- Enterprise grade authentication with Multi-Factor Authentication (MFA)
- End-point Information Profile and posture based policies
- User/user-group based policy control
- Network obfuscation and Enterprise topology hiding / obfuscation
- Application and Network Visibility
- Application Policy Control to restrict access of the applications
- Application traffic segmentation to separate traffic destined between different classes or apps or devices

The Versa Secure Private Access solution is a market leading Zero Trust Network Architecture (ZTNA) solution offered within Versa's Secure Access Service Edge (SASE) framework. VSPA integrates securi-ty, identity management, cloud delivered services and software defined networking and security 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

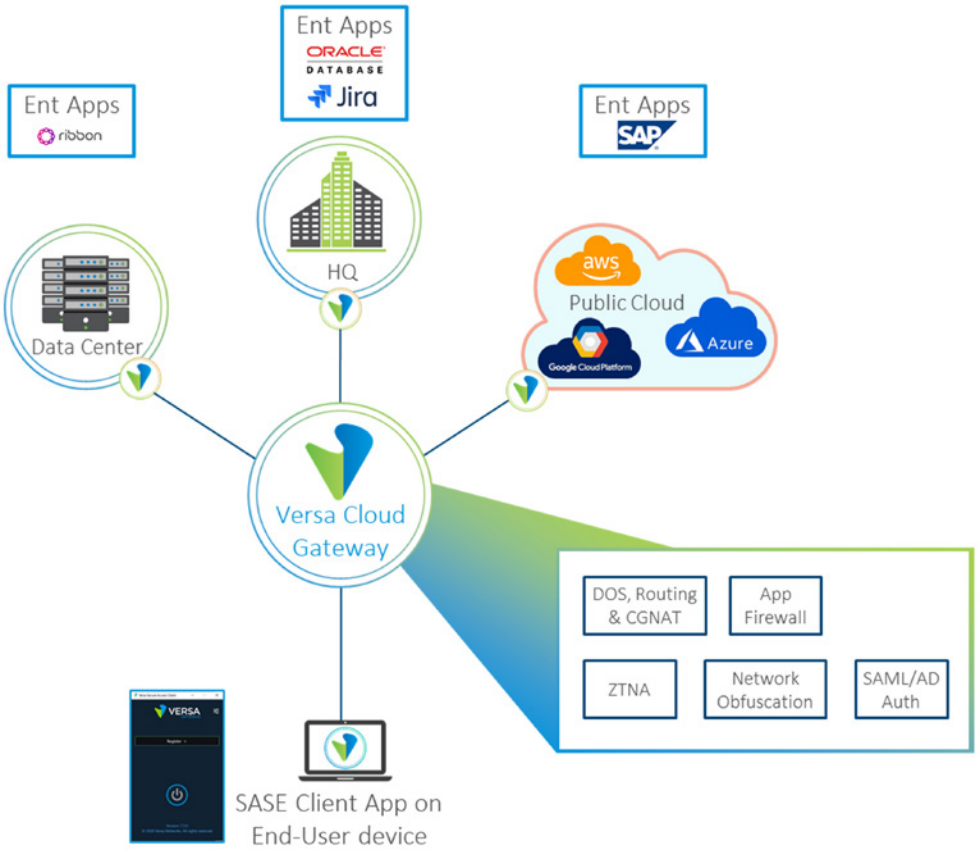
Service Components

VSPA is a globally distributed solution that connects distributed users to enterprise applications and re-sources. Enterprise applications and resources can be distributed across private cloud, enterprise data centers and public cloud instances. Versa Secure Private Access (VSPA) Solution consists of:

Versa Cloud Gateways (VCG), based on industry leading VOS™ platform. VCGs are globally distrib-uted, located close to users to provide distributed, low latency secure on-ramp solution for access to enterprise applications. VCGs authenticate users, authorize the application access and secure the en-terprise network from external threats. VCGs are built on VOS that integrates advanced routing, com-prehensive security, market leading SD-WAN along with secure private access. VCGs securely connect to and integrate with existing infrastructure in Enterprise network and datacenter.

Versa Client, a software agent/application that runs on client devices (i.e.,: Windows, MacOS com-puters, smart phones) providing a secure, encrypted SD-WAN like connection experience to client de-vices. Versa Client application uses secure and encrypted connection(s) from remote device to VCG(s). Upon authentication and access authorization through the VCG, users can now securely connect to en-terprise applications in public and private cloud

Versa SASE Portal, providing enterprise administrators ability to manage and monitor the SASE service in real-time and with historical reporting capabilities at network, application and user levels, also leveraging Versa's big-data based Analytics platform.



Key Service Capabilities

Secure Private Access

Versa Secure Private Access (VSPA) solution is a secure connectivity solution for remote users connect-ing to applications hosted by the enterprise. Versa Secure Private Access provides a Zero Trust connec-tivity to applications hosted in Enterprise Data Center, Private Cloud and/or Virtual Private Cloud in-stances of public cloud providers. Customers benefit from IPSec or SSL-VPN based secure connectivity for enterprise bound traffic from remote users towards the enterprise applications.

Policy Based Traffic Management

Versa Secure Private Access (VSPA) uses granular policy based application traffic management to con-trol and limit the application access and visibility capabilities. Users can be configured to use the Versa Client application 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 appli-cation is not accessible or not preferred. With support for multiple gateways*, customers can dedicate certain gateways for secure applications while allowing users to access generic applications from other gateways.

User Authentication and Authorization

Versa Secure Private Access (VSPA) leverages enterprise's preferred Identity Provider (or identity management solution) to authenticate and authorize the user. Versa Secure Private Access integrates with various types of authentication servers like Active Directory, SSO servers like OKTA and different authentication protocols like LDAP, RADIUS, and SAML. VSPA supports uses Enterprise Identity infor-mation to authorize users for application access policies.

Multi-Factor Authentication (MFA) using Email is supported by Versa Secure Private Access. Additional-ly, time-based One-Time Password (OTP) integration with Microsoft Authenticator, Google Authentica-tor and Duo is also available. VSPA is integrated with SSO Identity provider together with MFA as well.

End Point Information profile

Versa Secure Private Access detects and enforces policies based on the current profile and state of the end device. Versa Client constantly monitors security profile of the end user device including Operating System details, presence of certain key security applications like Anti-Virus, use of disk encryption, disk backup, last run time of these applications etc. Such collected information forms End-Point Information profile and VSPA enforces security policies based on the security posture assessed.

Application Firewall

Versa Secure Private Access enforces policies which authorize access to applications on a per applica-tion and user/user group basis. Enterprise 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.

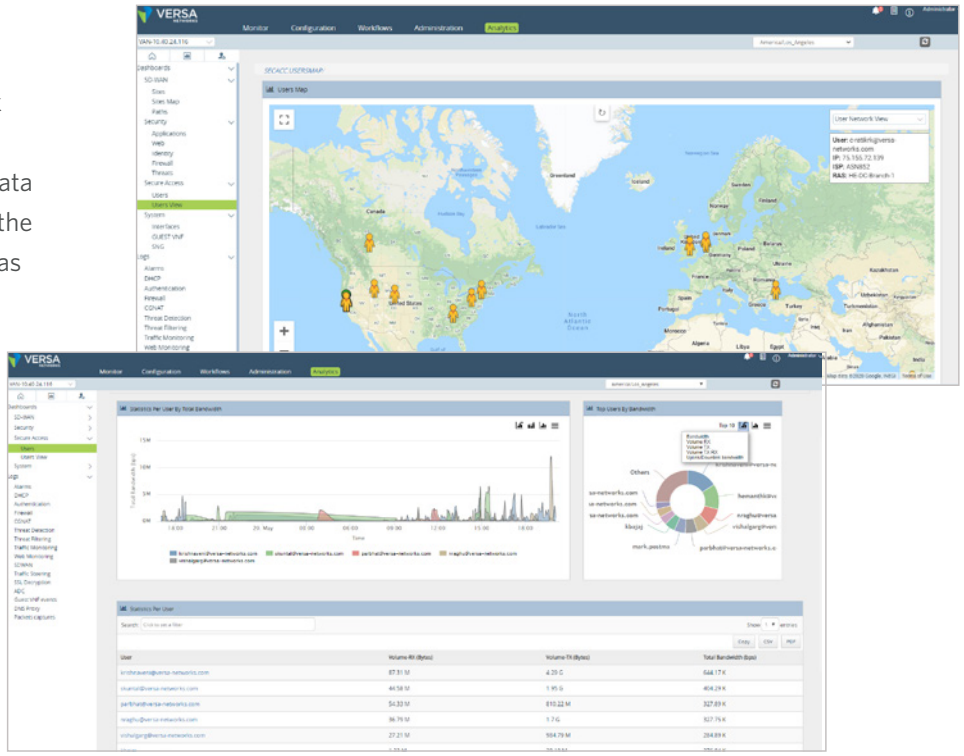
Network Obfuscation

Network Obfuscation is a security technique to hide internal network topology from remote users. Network obfuscation such as hiding Enterprise network topology details protects applications from multiple attack vectors like lateral movement, port scanning etc.

Versa Cloud Gateway running VSPA obfuscates Enterprise's application server IP addresses from the user and user IP addresses from the application servers. The user traffic is authorized and translated towards the application and vice versa using Versa's built-in secure proxy functions. This provides high-est level of protection from malicious actors and malware that may be running within Enterprise client devices w/out being detected by the Anti-Virus software of the client..

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 Private Access builds on top of big data based Versa Analytics plat-form 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 Private Access applies various techniques like SLA monitoring, Traffic engineering, that have been extensively deployed in connecting branches now to this software based service.

- Intelligent Gateway Selection ensures that the Versa client connects to the gateway which pro-vides the best user experience. The Versa client chooses the best gateway based on various pa-rameters like server load, cloud gateway proximity, network performance towards the gate-way.
- Hot Stand-by feature ensures that the Versa client is simultaneously connected to multiple gateways. The Versa 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.
- VSPA 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 application level encryption of the traffic.

Versa Secure Private Access supports geo-location, user and application policy to ensure clients con-nect to the closest gateway based on current user location. Versa Client can connect to a multiple gateways based on which application is being accessed. Versa 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.

Service Tiers

The Versa Secure Private Access subscription is available in two tiers

Features	Essentials	Professional
Versa Client for Windows 10, MAC OS, IOS, Android, Chromebook, Linux, Windows 8 and Windows 7 Versa client provides secure connectivity from end-user device to Versa cloud gateways.	✓	✓
Intelligent Gateway Selection The Versa 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	✓	✓
Geo-redundant Gateways for High Availability	✓	✓
App Whitelisting for unlimited apps		✓
Zero Trust Policies based on posture of the user device		✓
Encrypted and Unencrypted tunnels to Gateway		✓
App based Traffic Steering		✓
Streaming to 3rd party analytics server		✓

Versa also provides bundling options for Versa Secure Private Access with other Versa Cloud Hosted SASE Services. For details, please reach out to your Versa Account representative.

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