Versa Zero Trust On-Premises and Zero Trust Everywhere Access

A secure access solution is for on-site users connecting to private applications. It applies granular, Zero Trust access policies to users and devices based on identity, device posture, and application.

Background

Today, enterprises are faced with the following reality:

- Digital Transformation. The migration of enterprise applications and workloads from an enterprise datacenter to a variety of public clouds and/or SaaS services continues to accelerate.
- Hybrid Workforce. In post COVID-19 world, employers are adopting a hybrid workspace approach in which employees are working in the office on some days of the week and working from home on the rest of the week.

Cloud delivered Zero Trust Network Access (ZTNA) solutions, such as Versa Secure Private Access (VSPA), securely connect remote workers to enterprise applications hosted in enterprise environments, private clouds, or public clouds. VSPA protects both the applications and users using the latest Zero Trust Network Access framework and capabilities. VSPA is a cloud managed, cloud delivered, private access service efficiently connecting distributed users with distributed applications without compromising security and/or user experience. Please see here for more information on VSPA: https://versa- networks.com/documents/datasheets/versa-secure-private-access.pdf

Now with employees coming back to the offices and using a hybrid workstyle, Enterprises are demanding an equivalent, ZTNA solution that is delivered from the office itself.

Challenges faced by Enterprises Today

Today, Enterprises widely use Network Access Control (NAC) to administer access control to Enterprise's office or on-premises networks. NAC solutions typically rely on 802.1X to admit a user onto Enterprise LAN environment. 802.1X uses Enterprise certificate-based authentication to authenticate corporate compute devices onto the network. IoT, personal or unmanaged network devices typically do not accept or use Enterprise certificates. Hence such devices are either admitted onto the network using MAC-based authentication bypass lists or get admitted typically onto a default / common VLAN or guest VLAN or a Guest WiFi SSID. NAC solutions do not provide any further checks, controls or capabilities that extend beyond initial admission into the Enterprise LAN. NAC solutions do not provide visibility or control on network activities either.

Such NAC-based solutions can also be bypassed by techniques that include spoofed MAC addresses, and compromised credentials. The unauthorized user or devices are then given open network access to sensitive Enterprise resources. Also, NAC based solutions provide one time-based checks and once the user or device is admitted to the network, rarely any checks or re-authentications are implemented after.

Furthermore, even effectively working NAC-based access control is insufficient in today's ever sophisticated network. Identity based policy control, security posture assessment, detailed device identification / profiling and segmentation are required within Enterprise LAN environments to provide a secure and segmented approach to Enterprise LAN network and associated resources.

Ongoing security posture assessments and policy-based traffic control are a must. For instance, a perfectly legitimate user who may have disabled his corporate issued laptop's AV software, thinking that it may slow down his computer, poses a major risk to the Enterprise network. Malware or ransomware may be using his computer as an intermediate host to spread itself across network attached assets.

Software Defined Perimeter (SDP) solutions tried to tackle some of these changes - in many cases using the platform lens of the vendor that focused on disjointed parts of the problem that the specific platform could address rather than totality of needs.

Major parts of the solution were missed translating to vendors throwing more discrete or bolt-on products to address missing pieces. For instance, SDP solutions adopted by Ethernet switch vendors focused mostly on traditional NAC, and network-based security, posture assessment, policy-based traffic control or device identification and device-based traffic management and other aspects got left out. Vendors suggested standalone firewalls, separate policy servers, standalone policy enforcement appliances, bolt-on device fingerprinting solutions and others to try to address each point problem, one by one, without solving the problem in a cohesive way or in totality. This translated to a very complex, intrusive, and costly to deploy and operate set of solutions which were not consistent or effective, resulting poor adoption and unmet needs in the market.

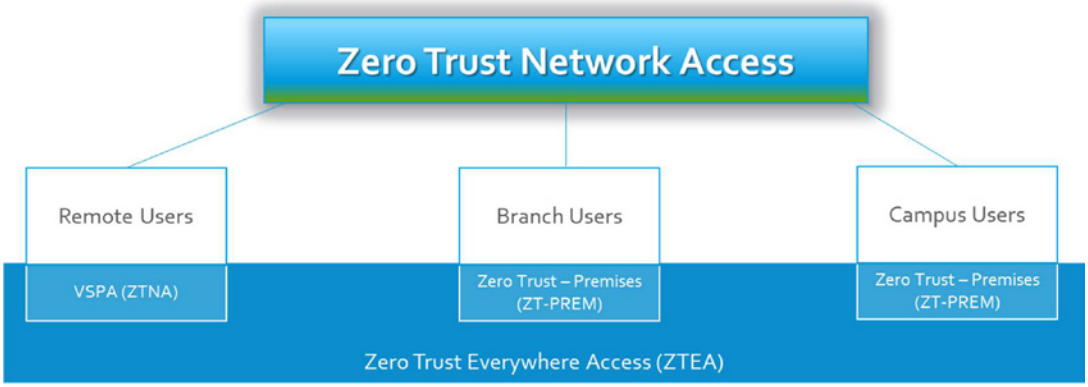
With the pandemic, awareness for the need of zero trust-based solutions heightened and Enterprise network operators started inquiring for such solutions from ZTNA vendors. Most ZTNA vendors offer primarily cloud delivered ZTNA solutions today.

However, cloud delivered ZTNA solutions do not address such needs of on-prem workforce. Cloud delivered ZTNA solutions require traffic to be processed by cloud-based gateways introducing unwanted latency, traffic u-turns, traffic steering complexity and unpractical expectations. It also doesn't offer any solutions for IoT, unmanaged or personal devices. Hence cloud-based ZTNA solutions do not have much to offer in the East-West direction of traffic within an Enterprise LAN deployment. On-premises based, modern ZTNA solutions are required to address all of these needs.

Introducing Versa ZTNA on-Prem and ZTNA Everywhere Access

Versa Zero Trust – Premises (ZT-Prem) is a secure access solution for branch and campus users connecting to applications and workloads hosted in the enterprise datacenters or private clouds. It applies granular, Zero Trust access policies to users and devices based on continuous assessment of identity, device posture, and application. The product is designed to be integrated into any campus or branch architecture as a standalone appliance.

Versa Networks offers a comprehensive ZTNA solution to be deployed on-premises with Versa ZTNA on-Prem and Versa ZTNA Everywhere Access product offerings.



Versa ZTNA On-Premises (Versa ZT-Prem) is based on the same principles of cloud-delivered ZTNA offering of Versa, namely Versa Secure Private Access (VSPA), adopted for the needs of ZTNA on-premises. Versa ZT-Prem is built on the fundamental philosophy of providing granular policy and security posture-controlled network access originated by network attached user or device. Versa ZT-Prem scope translates to:

- 802.1X based NAC to provide base level network access control
- Enterprise grade authentication with Multi-Factor Authentication (MFA), Active Directory integration
- End-point Information Profile (EIP) and security posture assessment
- Security Posture based access control, micro-segmentation and traffic management

- 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
- Device fingerprinting, classification, placement and access control including corporate sanctioned, unsanctioned, personal and IoT devices
- Extensive traffic segmentation options using VLAN, VXLAN, IPSec, SGT and other standards-based options
- Clientless and client app based ZTNA solution, provided fully inline

The Versa ZT-Prem solution is a market-leading Zero Trust Network Architecture (ZTNA) solution offered as part of the Versa Unified SASE platform. Versa ZT-Prem integrates security, user and device identity-based management and perimeter control into a simple, hassle-free service that:

- Provides modern, zero trust based Enterprise Perimeter Security
- Extends perimeter protection to the end-user device
- Allowing users, devices and resources on-premises to connect securely
- Delivers secure application experience
- Is highly scalable and extensible operating at high performance that Enterprise LAN solutions need

The Versa ZTNA Everywhere Access (aka ZTEA) combines Versa's market leading, cloud-delivered ZTNA solution, Versa Secure Private Access (VSPA) with on-premises delivered ZT-Prem, providing the best of both ZTNA solutions to Enterprise operators. Using ZTEA, Enterprise operators can leverage a consistent and comprehensive, market leading ZTNA solution for their remote as well as their on-premises users satisfying today's hybrid workstyle requirements. Furthermore, Versa ZTEA provides effective on-premises based ZTNA solution for IoT, unmanaged, and personal devices as well.

ZT-Prem Components

Versa ZT-Prem is an on-premises delivered ZTNA solution that provides modern zero-trust based network access control and effective secure software perimeter for Enterprise LAN. Versa ZT-Prem Solution consists of:

Versa Client

An optional software agent/application that runs on devices (e.g. Windows, MacOS computers, smart phones) providing a secure connection experience to Enterprise network or resources. Versa Client application uses secure and encrypted connection(s) from client device to Versa Cloud Gateways when a user is connecting from a remote location. The same Versa Client application intelligently discovers and connects to locally deployed Versa Policy Enforcement Point (VPEF) when the user comes to the office, eliminating the need to run separate app for client-based connection needs for on-prem ZTNA deployments. Upon authentication and access authorization through the Versa Policy Enforcement Function (VPEF) within VOS, users can now securely connect to enterprise applications and resources based on their security posture, user and device privileges, and under policy governance as defined by Enterprise admins.

VOS providing Versa Policy Enforcement Point (VPEF)

VPEF functions built-in within VOS need to be placed within branch or campus locations. VPEF should preferably be located as close as possible to network attached users or devices to provide distributed, low latency, secure ZTNA policy enforcement point(s). VPEF authenticates users, authorizes network access,

implements security posture assessment, associated policy enforcement functions while providing modern ZTNA based software defined security for enterprises. Versa's ZTNA on premises functions are developed to protect Enterprise networks

from threats that may be coming from within the LAN. VPEF function is built within VOS natively, seamlessly integrated with advanced routing, comprehensive security, market leading SD-LAN, SD-WAN capabilities. VPEFs also provide secure connection, policy-based segmentation and traffic management capabilities in ways that integrate seamlessly with existing infrastructure in Enterprise networks, thanks to Versa's comprehensive networking stack. VPEF function can be placed on any or all VOS instances on a customer's network. VPEFs located on-premises can be configured with the same, or different ZTNA policies, based on Enterprise's needs.

Versa SASE Portal

Provides enterprise administrators with the ability to manage and monitor the cloud-based, on-prem or both ZTNA deployments in real-time and with historical reporting capabilities at network, application and user levels, also leveraging Versa's big-data based Analytics platform. Unified SASE portal provides our customers easy to use single pane of glass to define, administer, and monitor ZTNA and security policies whether they run on the cloud or on premises.

Single, unified bigdata-based Analytics provides deep insights onto traffic, user activity, network access and security event details for on-prem or cloud-delivered ZTNA solutions.

Versa ZT-Prem solution can also be managed by on-prem deployable Versa Head-End cloud based Versa Hosted Head-End, Versa recommends cloud based Versa Hosted Head-End option to benefit from ease of deployment, to leverage the same head-end for Versa Zero Trust Everywhere Access purposes.

Versa ZT-Prem Deployment Options

ZTNA on-premises capabilities are provided by VOS instance(s) deployed on premises. Hence VOS presence on-premises is pre-requisite for ZT-Prem. Versa provides different on-premises VOS deployment options for our customers. Such deployment options include VOS running on Secure SD-LAN Ethernet switches, dedicated ZTNA appliances or Secure SD-WAN routers located on the WAN edge of the network. When deployed, Versa Client will intelligently discover such VOS instances running VPEF functions and will talk to closest one(s) to implement ZTNA on-premises functions. Such intelligent discovery and VPEF leverage provide unmatched deployment flexibility together with comprehensive coverage for Enterprise operators.

For clientless devices, such as IoT devices, personal devices and others, VOS needs to be placed inline within the traffic to identify, assess and to deliver appropriate ZTNA functions.

It is recommended to deploy and leverage Versa's on-premises ZTNA functions as close as possible to network attached devices and users, such as at the edge of LAN. Deployment of ZTNA functions in closest proximity to users and devices allows identification of devices, assessment of security posture, identification of apps and implementation of policy-based network control and security functions on the entry point to the network. For instance, deploying Versa ZT-Prem on Versa's edge Ethernet switches running VOS natively will allow Enterprise operators to implement L2-3 as well as L4-7 based control of user and device traffic policies along with dynamic micro-segmentation right on the Ethernet switch itself. If desired, traffic can be examined further by Versa's built-in L4-7 security functions and managed based on security, network access, application policies. Outcome of such access control and security check and policy implementation may be to drop, forward, log, or to place traffic into specific micro-segment of network, which then can be sent to its destination(s) preferably using SD-LAN overlays in independent ways from underlying network infrastructure. Such functions implemented inline closest to the user provides most comprehensive ZTNA coverage for Enterprise operators. For more information on Versa's Secure SD-LAN product offering, please refer to respective datasheet and materials.

In addition to LAN Edge deployment options, Versa ZT-Prem can also be deployed on existing Versa SD-WAN appliances or on dedicated appliances allocated for ZTNA purpose.

Versa ZT-Prem is an inline delivered functionality and the only requirement for ZT-Prem deployment is to get VOS deployed inline within paths of the traffic. Inline deployment requirement can be satisfied by using any of these deployment options outlined above. If the VOS instance(s) is deployed several hops away from network attached devices, by using rich networking features, traffic encapsulation options (ie: VXLAN overlays) and standards-based protocols, traffic can be steered to VOS instance(s) across the LAN to deliver ZTNA functions inline.

Zero Trust Everywhere Access (ZTEA) Components

Versa ZTEA is a bundle of Versa ZT-prem offering delivered on-premises and Versa Secure Private Access offering delivered from Versa Cloud Gateways (VCG). The combination offers our customers a consistent and comprehensive ZTNA solution whether working from home or in the office. Note that ZTEA is only managed by cloud-based Versa SASE Portal which is also referred as Versa Hosted Head-End.

Key Product Capabilities

ZTNA On-Premises

Versa ZT-Prem solution provides secure connectivity and software defined network access solution for local users and devices connecting to Enterprise LAN networks. Versa ZT-Prem provides Zero Trust based connectivity to Enterprise applications and resources.

Customers benefit from Versa's modern on-premises delivered ZTNA solution that comes integrated with client based and clientless options. Client based option provides detailed security posture assessment and policy based granular admission control, micro- segmentation and application of security functions based on the information obtained by the Versa Client app. Clientless option provides inline fingerprinting, NAC and traffic analysis functions to identify, categorize / classify devices, users and manage traffic for a broad set of devices.

Policy Based Traffic Management

Versa Policy Enforcement Function (VPEF) within VOS uses granular policy- based application traffic management to control and limit the application access and visibility capabilities. VOS provides a complete lifecycle approach to ZTNA starting with identification, assessment of security posture, which then gets followed up with policy-based access control, policy controlled micro-segmentation, security function implementation for traffic type, security posture level, etc and finally with monitoring functions. VPEF is the unified policy engine that provides all such policy functions. In the case of ZT-Prem, any VOS deployed on-premises can be the VPEF point, and the policy associated with the user or device will follow the client.

In the case of cloud delivered VSPA, VPEF function is fulfilled by each Versa Cloud Gateway that is just a cloud deployed instance of VOS. VSPA is available to our customers as a standalone solution or as part of Versa Zero Trust Everywhere Access (ZTEA) which bundles VSPA and ZT-Prem together.

User Authentication and Authorization

Versa ZT-Prem leverages a preferred Identity Provider or identity management solution to authenticate and authorize the user. Versa ZT-Prem integrates with various types of authentication servers like Active Directory, SSO servers like Okta and different authentication protocols like LDAP, RADIUS, and SAML. Versa ZT-Prem supports uses Enterprise Identity information to authorize users for application access policies.

Multi-Factor Authentication (MFA) using Email is supported by Versa ZT-Prem. Additionally, time-based One-Time Password (OTP) integration with Microsoft Authenticator, Google Authenticator and Duo options are also available. Versa ZT-Prem is integrated with SSO Identity provider together with MFA as well.

End Point Information profile

Versa ZT-Prem detects and enforces policies based on the current profile and state of the end device. Versa Client app constantly monitors the 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 Versa ZT-Prem enforces security policies based on the security posture assessed.

ZTNA for Clientless Devices

Versa ZT-Prem and ZTEA solutions provide ZTNA for clientless devices as well. Such devices include sanctioned or unsanctioned IoT devices, other network connected equipment, personal devices and more.

VOS comes with built-in capabilities to identify and fingerprint over 1 million types of devices. Once enabled, VOS will look at different attributes of traffic generated by devices while running inline. Such attributes will then be compared against different traffic fingerprinting and device identification information within the device database and devices can be identified accordingly. Once identified, devices will be mapped to different device types and risk profiles to make overall device management task easy for network operators. Device information details that are extracted from inline fingerprinting-based analysis can be as detailed as OS, patch level, depending on the device that is fingerprinted. Now armed with detailed information on a per device, and device classification by type and risk, Versa's rich set of security, network admission control, network placement and micro-segmentation decisions can be implemented on a per device level granularity. Even if traffic for multiple devices comes to VOS from a shared port, policies can be applied at a device level granularity to provide the right level of ZTNA capabilities.

Micro-Segmentation

Another cutting-edge feature of Versa ZT-Prem is its ability to micro-segment client device traffic based on device type, security posture, user, application and other variables. Versa's powerful policy engine allows our customers to define their own policy rules and map them to different micro segments to fine granular separation of traffic types from each other.

VOS supports different segmentation options such as VLAN, VXLANs and SGT tags to implement micro-segmentation. SGT tag based micro-segmentation is the preferred choice as it allows dynamic assignment of SGT tag values to subsets of traffic based on changing security posture of devices and users w/out changing assigned VLAN, VXLAN IDs or IP subnets. Devices that degrade in security posture over time (ie: AV engine gets disabled on a corporate laptop that runs Versa Client App) will automatically get mapped to restricted access class, identifiable with its SGT tag value, and if desired, network-based security functions such as NGFW and UTM can be applied to it. Once the security posture of the device recovers, then it can regain its access privileges dynamically.

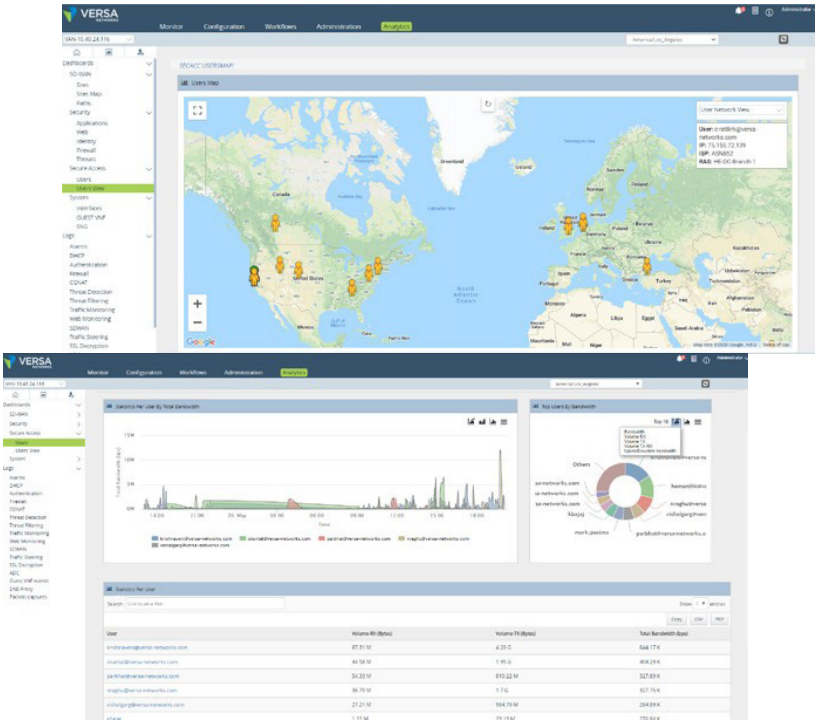
Propagation of SGT tags across Versa Secure SD-LAN and Versa Secure SD-WAN solutions allow consistent policy and traffic management decisions to be implemented across the network for the traffic class, providing a network level secure, and comprehensive ZTNA solution regardless of where traffic gets originated from and where it is destined to.

Application and User visibility

Application, User and Network visibility is necessary to efficiently operate the network and to secure it from external threats. Versa ZT-Prem and ZTEA 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 ZTEA offering inherited various capabilities like SLA monitoring, traffic engineering, and other application focused features that are carried over from Versa Secure SD-WAN learnings and experiences. Furthermore, ZT-Prem and ZTEA comes with key capabilities that translate to better application experience for our customers:



- Intelligent Gateway Selection ensures that the Versa client connects to the nearest and/or most suitable gateway within the campus and when working from home providing the best user experience. The Versa client chooses the best gateway based on various parameters.

- ZT-Prem and ZTEA services support use of encrypted and unencrypted tunnels towards the VOS instances running on-premises (in the case of VZ-Prem) and on the cloud (in the case of VCGs). It is not required to use encrypted tunnels while running ZT-Prem however it is highly recommended to use such encrypted tunnels when connecting over Internet to VCGs.

Licensing Overview

The Versa ZT Prem is a subscription product offering. Versa ZT-Prem is licensed on a per authorized user-basis. It is a network wide license which is not restricted to any given VOS instance, hence providing customer to use ZT-Prem license in a flexible way w/out worrying about per device or site level capacity restrictions. Versa ZT-Prem license is a single tier, making it very easy to purchase and deploy. Versa ZT-Prem features are summarized below:

Features	Scope
Versa Client for Windows 10, MAC OS, IOS, An-droid, Chromebook, Linux, Windows 8 and Win-dows 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 most suitable on-premises gateway based on a number of parameters	✓
Authentication with Enterprise authentication server Integration with LDAP/Active Directory, SAML based SSO, MFA support with Microsoft Authenticator, Google Authenticator, Duo	✓
Tunnel-based and tunnel-less deployment options Versa ZT-Prem support use of IPSEC tunnels to encrypt traffic over untrusted LAN environments (ie: multi-tenant or shared workspaces), as well as tunnelless modes. It is typical to deploy Versa ZT-Prem without any tunnels on Enterprise LAN	✓
Deployment Flexibility Versa ZT-Prem can be deployed on Versa Secure SD-LAN, Secure SD-WAN or on dedicated appliances within Enterprise LAN	✓
Integration with Brownfield Network Thanks to underlying VOS with very rich set of standard based routing protocols, encapsulations, ZT-prem delivering VOS instances can easily integrate with existing brownfield network to place VOS inline within the path of network traffic	✓
Network Obfuscation Network topology hiding using variety of techniques including micro-segmentation, policy-based traffic management capabilities	✓
Built in Security (SFW, DOS Protection) Versa ZT-Prem comes with comprehensive ZTNA scope. In addition, as it is built on top of underlying VOS platform license, it also leverages built-in security functions of the underlying VOS license.	✓
Application, Network and User visibility Big-data based detailed visibility and analysis capabilities thanks to Versa Analytics	✓
Application, User, Device traffic control Using rich set of policies provided by VOS's natively built-in VPEF function	✓
Security Posture Assessment Using Versa Client based End-Point Information Profile (EIP) and inline fingerprinting-based security posture assessment	✓
3rd Party EIP based Security Posture Assessment Integration with 3rd party client app based EIP and use of that information for Versa ZTNA purposes	✓
Micro-Segmentation Ability to dynamically divide network traffic to small segments and assign classes of traffic based on security posture, device and user types, privileges, application classes and more to minimize exposure and attack surface areas	✓

The Versa Zero Trust Everywhere Access (ZTEA) is a bundled offering that combines (cloud-delivered) VSPA at Professional tier with (on-premises delivered) ZT-Prem, allowing our customers to use ZTNA from anywhere, everywhere.

ZTEA is a subscription-based product offering licensed on a per authorized user-basis. It is a network wide license which is not restricted to any given VOS instance, providing customer flexibility to use ZTEA license in a flexible way. Versa ZTEA comes with built-in bundle price advantages, making it advantageous for our customers to enroll to this bundled offering. ZTEA subscription may require surcharges for international deployments as cloud-based delivery costs can vary by location. ZTEA uses the same surcharges as VSPA as ZTEA is built on top of it.

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