DATA SHEET

Versa Secure SD-LAN

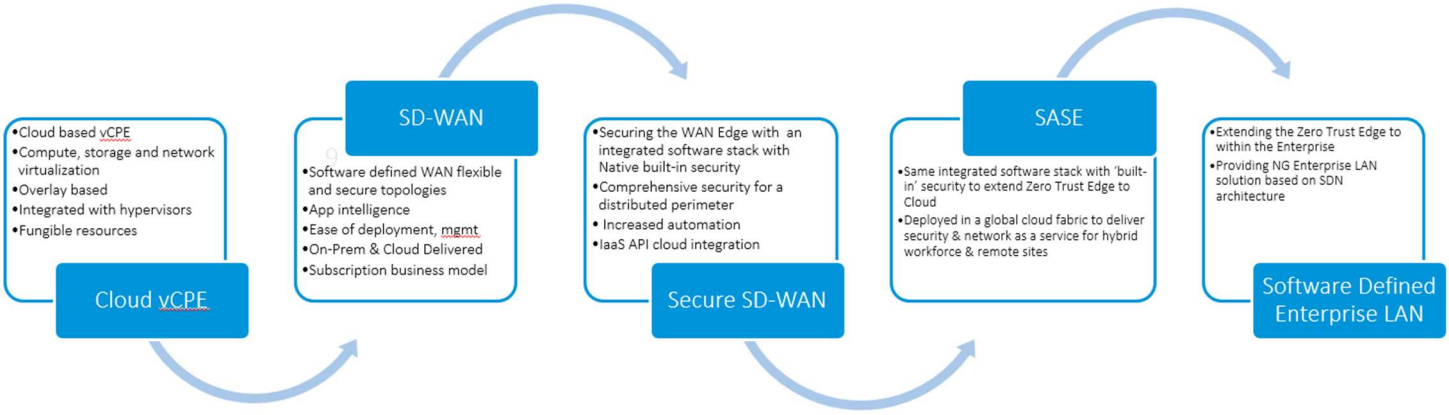
Combining switching, routing, security and network services to improve agility and reduce costs. With user, device, and application visibility and inline security policy enforcement, SD-LAN sets the foundation for Versa's Zero Trust Everywhere.

Background

Ethernet switches and WLAN APs are the main networking elements that provide wired and wireless connectivity within Enterprise LAN networks.

Enterprise networks have been deploying Ethernet switches for over 25 years. While fast adoption of new Ethernet interfaces with ever-increasing speeds and higher forwarding performances were happening, Ethernet switch-based Enterprise LAN solutions have been using a slower evolutionary approach to introduce new paradigms. One can say that today's Enterprise Ethernet LAN solutions have not evolved or transformed too far away solutions say from 10 or 15 years ago.

In contrast, other parts of the network have gone through major transformations using software defined approaches. Software Defined Networking transformations started first in Data Centers, moved to WAN with SD-WAN and moved to cloud with SASE or SSE. Each of these deployment areas highly benefited from this transformation. The remaining area that has not gone through transformation is Enterprise LAN networks.



Software defined transformations have had profound effects on sections of networks that they touched to. At the high level, Software Defined Networking provides:

- Users with security and connectivity, anytime, anywhere
- Decoupled hardware from software providing software-controlled network and security function placement flexibility and consumption
- Centralized management and control that administers connectivity and security functions across the network
- Streamlined IT management tasks
- And most importantly, enables Digital Transformation which is transformative with seamless application and user experience

Transformative effects and advantages of Software Defined Networking are such that parts of networks that have gone through that never want to come back to legacy ways of doing things.

The Need

We observe today that many of today's Enterprise LAN Switching solutions do not possess software defined characteristics. Solutions are still very much tied to specific hardware appliances, or vendor / platform specific proprietary solutions. Enterprises are looking for ways to separate themselves from such proprietary solutions and they are looking forward to using open, multi-vendor standard based solutions to achieve the best features, pricing and investment protection.

Today's Ethernet switch solutions are silo'ed and they operate in ways that are isolated from applications, security needs and user experience. This is due to the hardware centric approach and the narrow scope that is defined for these switches. Enterprise network operators are looking for Enterprise LAN solutions offering higher intelligence, especially on LAN edge, to be able to deploy much needed security perimeter, policy-based admission and administration of users, devices and apps starting from the edge of the LAN. Making these decisions on the edge of the LAN is very important as it becomes much harder to do later on within the Enterprise network and potential exposure to threats and vulnerabilities can be controlled and eliminated on the edge of the LAN.

Furthermore, in post pandemic era, Enterprises are now expecting cutting edge solutions such as Zero Trust Network Access (ZTNA) to be delivered on-premises within Enterprise LAN together with natively integrated effective security which essentially defines the next generation software defined perimeter solutions.

In addition, Enterprises want to implement highly granular network segmentation decisions based on device type (ie: IoT Devices), application class, security posture of network attached client device, users and more to separate traffic of each of these sub-classes to secure network infrastructure and network attached devices.

IoT/OT/BYOD devices, whether sanctioned or unsanctioned, are integral parts of Enterprise LAN networks. Customers are looking for integrated device fingerprinting solutions to identify and manage all network attached devices by type, posture, and assessed risk.

Enterprise administrators want to define policies once for user, app, device, security posture and see them follow the users.

Legacy solutions are unable to address these needs. All of these indicate the need for new class Ethernet switching solutions. One that is based on Software Defined architectures and approaches.

Introducing Versa Secure Software Defined LAN (SD-LAN)

Versa Networks introduces comprehensive and modern Secure Software Defined LAN solution. Versa Secure SD-LAN is built from ground up as a true SDN solution adhering to all of defining SDN characteristics.

Versa Secure SD-LAN solution is based on intelligent network edges while each edge node connects (preferably) with overlays to each other forming a software defined fabric on the LAN. Use of layer-3 transport based overlays simplifies LAN network design, deployment and operations tasks while keeping middle of LAN very simple with edges running all the intelligence. Keeping transport / middle of LAN simple and tasked with layer-3 forwarding at the underlay also eliminates traditional shortcomings coming from layer-2 underlays, giving the operator complete topological freedom, opportunity to use multiple active forwarding paths without using or relying on xSTP and fast convergence options. Now with this approach, Enterprises will be leveraging their investment fully across LAN switches and interfaces.

Versa Secure SD-LAN solution is built using the same Versa SDN building blocks in software. The very same VOS that is used on WAN edge for SD-WAN with integrated Security and on Versa Cloud Gateways for delivering cutting edge SASE functions is now enhanced further with version 22.1.1 to support top of the line merchant campus switching ASICs. Use of top-of-the-line campus and Enterprise class ASICs based Ethernet switches provides our customers with market leading switching capabilities in hardware. With the support of leading Ethernet switch ASIC based platforms, Versa Secure SD-LAN solution provides rich feature-set and line rate forwarding on Enterprise class Ethernet switches.

VOS running on Ethernet switches natively programs switching ASIC using its SDKs with L2, L3 (IPv4, IPv6, unicast, multicast)

forwarding, ACLs, QoS, shaping, various tagging, tunneling and micro-segmentation, flow offload functions. Furthermore, VOS running on the embedded compute subsystem of the same Ethernet switch continues to provide comprehensive L4-7 functions natively within the Ethernet switch. Such L4-7 functions include application intelligence, policy-based forwarding, comprehensive security and ZTNA functions. Versa Secure SD-LAN switches are designed in such a way that they facilitate seamless traffic exchange between switching ASICS and x86 compute to run line rate forwarding and stateful functions of sorts to offer the best of both worlds to our customers. The combination forms a highly transformative, industry first solution that sets the backbone of Versa Secure SD-LAN solution that covers connectivity, segmentation, and built-in comprehensive L4-7 Security for Enterprise LAN networks, all delivered from the same platform.

In addition to VOS, other elements that are used to deploy and manage other Versa solutions, namely Director, Controller, Analytics and Concerto are used on Versa Secure SD-LAN too. Such commonality of building blocks helps our customers deploy Versa Secure SD-WAN, Versa SSE and now Versa Secure SD-LAN together with consistent network function descriptions and forwarding implementation across layers of Enterprise devices. With these, now Versa Secure Software Defined Branch and Campus solution is formed.

Versa's Approach to Building Open Standards Based Secure SD-LAN

Versa uses proven industry standards-based technologies and building blocks to build its SDN solutions. Versa Secure SD-LAN follows the same principles. Versa Secure SD-LAN is built based on IETF and IEEE, industry-standard protocols and encapsulations to make use of proven, open technologies and to offer standards-based software defined solution to Enterprises.

Versa Secure SD-LAN leverages the same MP-BGP-based Control Plane that Versa currently uses today for its Secure SD-WAN and SASE Fabric solution. Versa's MP-BGP based control plane is used to distribute LAN reachability information and to establish standards-based LAN overlays with rich topology and connectivity options across the LAN. Versa's MP-BGP based control plane is now expanded to carry VXLAN label information between centralized controllers and distributed VOS instances running natively within Ethernet switches establish overlays between LAN endpoints and to exchange reachability information in a fully multi-tenant and multi-segmented way.

Use of MP-BGP based EVPN based VXLAN on the LAN provides technical advantages such as multiple active paths of forwarding for L2 and L3 flows, support for split LAG across Ethernet switches, minimized L2 BUM forwarding, proxy ARP, anycast gateway and others without any compromise in functionality and without any need for proprietary solutions of sorts.

This SDN technology was originally developed for SDN based Data Centers, which got expanded and baked over time. Today it is running the most critical Data Center networks. Use of such proven, multivendor, open protocols and technologies at the heart of Versa Secure SD-LAN solution also ensures successful interoperation with other vendors providing an open solution to our customers.

Versa Secure SD-LAN Architecture

Versa has been offering SDN solutions across WAN, and cloud fabrics with comprehensive security built in. The same SDN principles are now being applied to LAN environments with Versa Secure SD-LAN.

Versa Secure SD-LAN solution consists of distributed VOS instances running natively on platforms. Each VOS node is an independent L2, L3, L4-7 node which makes its own forwarding decisions using the configuration, policies, and network reachability information it has been provided. Each and every network element acts as a switch/router as well as a mini firewall. The distributed nature of Versa Secure SD-LAN solution to scale to very large networks.

While Data Plane is distributed, Management and Control Planes (Control Plane based on MP BGP Router Reflector design as articulated above) are centralized to provide centralized control and visibility from a single pane of glass. Centralized controllers facilitate the exchange of reachability information and set up network overlay paths while they can also influence forwarding decisions to achieve desired outcomes for our customers. Centralized Management Plane provided by Versa Director and Versa

Concerto administer ZTP, auto-provisioning of all VOS based devices (including SD-WAN, SD-LAN, cloud gateways and more) while providing true single pane of glass to manage the entire lifecycle of the whole network from a single place. Versa Director and Versa Concerto provide capabilities to manage configurations of entire network including topology definitions, policy definitions, L2-L3 and L4-L7 functions.

With this open, highly scalable and resilient SDN approach to Enterprise LAN, Versa aims to maximize uptime, eliminate single points of failure, eliminate proprietary solutions of sorts, eliminate operational complexities, eliminate the latencies, reduce the number of network elements by consolidation, reduce the capex and opex cost and to transform Enterprise LAN networks using Software Defined approach maximize benefits to our customers.

Ease of Brownfield Deployment

Versa Secure SD-LAN solution runs intelligence on the edges of the LAN, while keeping the middle, transport layer simple. That allows customers to start deploying Versa Secure SD-LAN from edge Ethernet switches while retaining their investment on aggregation or core Ethernet switches.

Versa Secure SD-LAN solution, being based on standards-based technologies allows our customers to form a multi-vendor solution that consists of Versa switches and other 3rd party products. Legacy Enterprise LAN networks can participate in Versa Secure SD-LAN using standard legacy encapsulations and protocols that are still supported by VOS. Brownfield parts of the network running such legacy network designs can be connected to Versa Secure SD-LAN using industry standard VXLAN on/off ramp capabilities. See below rich feature-set sections for more information.

Furthermore, the distributed nature of Versa Secure SD-LAN solution allows gradual insertion and deployment of Versa Secure SD-LAN switches.

Rich set of Switching and Routing Features

Versa Networks comes with heritage of carrier class routing and networking. Versa's rich set of Layer-2 and Layer-3 features include:

- Comprehensive Layer-2 features: Including Bridge-domains, virtual switches for multi-tenancy, xSTP, VLANs, VLAN manipulations, VLAN access/trunk mode, LLDP, IRB for integrated routing and bridging
- Comprehensive Layer-3 features: DHCP client/server/relay, VRFs, Static NAT, carrier class routing protocols: OSPFv2/3, RIP-v2, BGP/MP-BGP, IGMP v2/v3, PIM SM/SSM, Auto/Boot-strap RP, BFD, IPv6 extensions of routing protocols
- Rich set of platform features: LAG, rich set of QoS features (priority queuing, WRR, WRED and more), Shapers, Policers, ACLs, ZTP options, auto-provisioning, VRRP, Flow mirroring, Flow reporting, uCPE to host 3rd party VMs,
- Overlay based connectivity options: VXLAN, GRE, MP-BGP EVPN, MP-BGP L3VPN, IKEv2 IPSEC
- Network Access Control (NAC) capabilities: 802.1X single/multiple supplicants, RADIUS back-end, Certificate based and MAC bypass list-based authentication
- Microsegmentation: Line rate microsegmentation based on device posture, user, group and device fingerprints.

Such a rich set of L2, L3, platform level capabilities have been developed to meet a variety of the needs of our customers and to fulfill their deployment, interop requirements. Now these features and capabilities are available on Versa Secure SD-LAN platforms to use.

Natively Built-in Security, User and Application Intelligence

Versa Secure SD-LAN Ethernet switches run VOS natively with its comprehensive security stack. Versa's security stack for use by our customers can be summarized as follows:

- Stateful Firewall, CGNAT with ALS support, DOS Protection
- DNS Proxy, DNS Feeds and Filtering
- Application, User, Device policy-based traffic control

- IoT Security
- And Unified Threat Management capabilities

Versa chose to provide such comprehensive L4-7 security functions natively within Versa Secure SD-LAN platforms to address these needs:

- Provide natively built-in comprehensive network-based security functions on the edges of the network to offer a true secure perimeter for Enterprise LAN. This eliminates the need for Enterprise LAN operators from steering the traffic to dedicated, standalone firewall appliances with error-prone configuration-based approaches.
- Distributed smart SDN edges running L4-7 capabilities natively provided to achieve scalable, resilient, comprehensive security functions across the network eliminating the need for centralized dedicated security appliances that also becomes choke points and single points of failure.
- Security cannot be an afterthought or disconnected from the rest of the network. Versa is a firm believer of security being an integral part of edge solutions, whether it is SD-WAN Edge, cloud edge, SSE, or now SD-LAN edge.
- Policy consistency and portability for users and devices, which is a key tenet of SDN solutions. Now with security being an integral part of SD-LAN, security policies can follow the user or device, decoupled from legacy and static firewall appliances.
- And to address identification and protection needs for detecting and preventing malware and ransomware that is built to move laterally within the LAN

User Authentication, Authorization and Policy Control

Versa Secure SD-LAN integrates with a preferred Identity Provider or identity management solution to authenticate and to authorize a user. Versa Secure SD-LAN integrates with various types of authentication servers like Active Directory, SSO servers like OKTA and different authentication protocols like LDAP, RADIUS, and SAML. Versa Secure SD-LAN 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 Secure SD-LAN is integrated with SSO Identity provider together with MFA as well.

Single Policy Language and Single Policy Engine for the Whole Network

Versa's single, unified policy language is used also on Versa Secure SD-LAN solution. Security, routing, ZTNA, user or device, and/or application policies can be defined once and can then be applied across each and every layer of devices whether these devices are located on LAN edge, WAN or edge or on the cloud. Use of Versa's proven unified policy language and policy functions for Secure SD-LAN provides another major benefit and consistency to Enterprises.

A client entering to Enterprise's LAN which uses Versa Secure SD-LAN solution say from the LAN side will be admitted to the network using user, device, security, posture, or other combination of policies and based on associated connectivity and security privileges. Under the administration of these policies, the client device/user can communicate to the allowed destinations on LAN or on WAN while its traffic is isolated from layers of transport devices using tunnel overlays. If the same device moves to another part of the network, policies will follow the device, applying consistent solutions irrespective of the location where the user and device connect from.

ZTNA on-premises

Versa's market leading ZTNA on-premises capabilities provide secure connectivity and nextgen software defined solution for local users and devices connecting to LAN networks. For more details on Versa's ZT-Prem and ZT Everywhere Access (ZTEA), please refer to respective product information and datasheet.

Versa's on-premises ZTNA functions are delivered inline to provide comprehensive detection, identification, classification and control capabilities for client-based and clientless devices. Versa provides different on-premises deployment options for ZT-Prem. 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. 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 SD-LAN edge switches will allow Enterprise operators to implement L2-3 as well as L4-7 based control for user and device traffic with dynamic micro-segmentation implemented 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 drop, forward, log, or 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.

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 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.

Big-Data based Analytics and Predictive Analysis

Integrated with Versa Secure SD-LAN is Versa's cloud delivered AI/ML driven Analytics, Observability and Prediction Engine.

The Conversational Language Assistant enables context sensitive, intent based, troubleshooting interface usable by administrator not well-versed with Versa technology. The solution auto-corrects the responses and provides a automated workflow based troubleshooting experience.

AI/ML driven Big Data Analytics provides the near real-time visibility and historical reporting of the entire network. The Analytics system consumes telemetry data from the network and provides insights into the user, application and network performance and errors. The Observability platform provides actionable insight into the errors. Alarm correlation allows the NOC team to focus on resolving fundamental problems in the network and avoids distractions.

AI/ML driven prediction engine provides advanced insights into events and alarms before they occur allowing administrators precious time to prevent or minimize the impact of the occurrence. This includes ability to predict device performance issues, bandwidth and utilization of individual ports or appliances, application and user performance impacts.

AI driven Secure SD-LAN allows for a automated operation, workflow driven troubleshooting and insights to minimize the mean time to resolution (MTTR).

Genuine Multi-Tenancy

As with the rest of Versa solutions, Versa Secure SD-LAN supports genuine multi-tenancy across all layers of the solution, at the Data Plane, Management Plane, Control Plane and Analytics.

Versa's carrier class multi-tenancy allows multiple tenants to share common infrastructure while each tenant can operate independent of each other including separate L2-L3, L4-7 functions, topologies, users and RBAC definitions. Each device that is running VOS natively can be configured to support multiple tenants, providing unmatched M&A consolidation, shared LAN workspace infrastructure deployment, separated critical network infrastructure for compliance and/or business continuity and criticality purposes.

Versa's multi-tenant Secure SD-LAN setup is managed by parent tenant which is able to see and manage all tenants, while each sub-tenant will be able to see and manage only their resources. All of the multi-tenancy capabilities available in Secure SD-WAN, SSE solutions are available on Versa SD-LAN solution. For more information on Versa's market leading multi-tenancy capabilities please visit Versa's website or speak to your Versa representative.

Rich Platform Options

Versa Secure SD-LAN comes with hardware options to satisfy the diverse needs of our customers. Versa SD-LAN solution expands from WAN Edge to LAN Edge to provide a complete SDN based solution within the Enterprise LAN.

VOS runs natively on Cloud Services Gateway (CSG) appliances for WAN Edge purposes and on Cloud Services Switches (CSX family of products) for LAN switching purposes. CSX platforms are based on leading campus merchant silicon with x86 processors that run VOS natively. These two complexes are connected with specialized data paths to allow seamless exchange of network traffic between the two complexes associated key reference information to provide feature-rich line rate forwarding and comprehensive stateful L4-7 services. These building blocks set the foundation of Versa Secure SD-LAN in hardware.

CSX switches are ideal for Enterprises, covering a variety of deployment scenarios. CSX platforms as well as select CSG platforms are built on best-in-class campus switching silicon with leading characteristics in design, capacity, power consumption and functionality.

Here is a summary of Versa Secure SD-LAN platforms that Versa Secure SD-LAN is starting with:

CSG3000 Series: Consolidated WAN edge and Enterprise class switching platform that provides feature rich, high performance L2-L3, L4-7 capabilities thanks to combination of VOS and leading Enterprise class switching ASIC. CSG3000 comes in two flavors; CSG3300 and CSG3500 to offer different price and performance points for WAN Edge purposes while campus class switching complex between the two models is the same. CSG3000 provides collapsed LAN Edge, switch in-a-box and high-speed interfaces to act as aggregation point for edge/access switches.

CSX4000 Series: Enterprise class fixed edge switching platforms built with 48 port RJ45 PoE++ ports, and 10G/25G/100G uplink ports to provide non-oversubscribed, line campus class switching capabilities coupled together with VOS running natively inside. CSX4000 comes in several flavors to address 1GE, multi-rate GE access/edge port deployment needs of our customers.

CSX8000 Series: Enterprise class fixed aggregation and core switched starting from 48 ports of SFP+ with 100GE ports, and extending to 32 ports of 100GE port flavors, all running at wire rate. Based on the same campus class leading silicon family's higher spec ASICs, CSX8000 products provide line rate throughput up to 3.2 Tbps. Coupled together with VOS running natively on these platforms, CSX8000 provides options to address higher grade Ethernet switch needs of Versa Secure SD-LAN solution.

Versa Secure SD-LAN Licensing Overview

The Versa Secure SD-LAN is a subscription-based product offering. Versa Secure SD-LAN is licensed on a per platform basis. Versa Secure SD-LAN license comes in 3 tiers. Content of each tier can be summarized as follows:

- Essential: Carrier Class Routing, Switching, 3rd party VM based application hosting, ZTP, SD-LAN based Overlay Connectivity, 802.1X based Access Control
- Professional: Essential scope, plus User & Group Traffic Management, App-ID, App PBF, DNS Proxy & Security, Device Fingerprinting, Stateful Firewall, IP Reputation Feeds & Filtering, Web Security, URL Feeds & Security
- Elite: Professional tier's scope, plus UTM capabilities such as AV/Malware protection, IPS, File Filtering, SSL-TLS Proxy

Pre-requisite for ZT-Prem is Versa Secure SD-LAN Professional or Elite tiers. More details on each tier can be seen here and for a complete list of features supported at each tier please contact your Versa sales rep.

Features	Essential	Pro	Elite
Comprehensive Layer-2 features Including Bridge-domains, virtual switches for multi-tenancy, xSTP, VLANs, VLAN manipulations, VLAN access/trunk mode, LLDP, IRB for integrated routing and bridging	✓	✓	✓
Comprehensive Layer-3 features DHCP client/server/relay, VRFs, Static NAT, carrier class routing protocols: OSPFv2/3, RIP-v2, BGP/MP-BGP, IGMP v2/v3, PIM SM/SSM, Auto/Boot-strap RP, BFD, IPv6 extensions of routing protocols	✓	✓	✓
Rich set of platform features LAG, rich set of QoS features (priority queuing, WRR, WRED and more), Shapers, Policers, ACLs, ZTP options, auto-provisioning, VRRP, Flow mirroring, Flow reporting, uCPE to host 3rd party VMs	✓	✓	✓
Overlay based connectivity VXLAN, GRE, MP-BGP EVPN, MP-BGP L3VPN, IKEv2 IPSEC	✓	✓	✓
Network Access Control (NAC) 802.1X single/multiple supplicants, RADIUS back-end, Certificate based and MAC bypass list-based authentication	✓	✓	✓
User Authentication with Enterprise authentication server support Integration with LDAP/Active Directory, SAML based SSO, MFA support with Microsoft Authenticator, Google Authenticator, Duo, Captive Portal based		✓	✓
Stateful Firewall, CGNAT with ALS support, DOS Protection Providing L3-L4 security, stateful address translation with ALG support		✓	✓
DNS Proxy, DNS Feeds and Filtering		✓	✓
Device Fingerprinting Device Identification and Fingerprinting of rich set of devices, including IoT/OT/BYOD, Device Type Policies, device classifications, risk assessment		✓	✓
URL and IP Feeds, Classification, Filtering URL, and IP Feeds, Classification and Filtering to protect devices on LAN from talking to untrusted or suspicious destinations on the Internet		✓	✓
Application Identification Ability to identify market leading number of applications and map to different application classes to manage traffic of each application class		✓	✓
Application, User, Device policy-based traffic control Using rich set of policies provided by VOS's natively built-in VPEF function		✓	✓
IoT Security Recognition of IoT protocols and applications, filtering		✓	✓
Application Identification, Application Policy, Network and User visibility Big-data based detailed visibility and analysis capabilities		✓	✓
Micro-segmentation With tagging options including VLAN, VXLAN, SGT and more. Hardware acceleration included		✓	✓
Unified Threat Management NG-IPS, Antivirus, Malware Protection, File Filtering within the context of lateral movement protection, detection and prevention of spread of malware/ransomware within LAN			✓
SSL-TLS Proxy Including TLS 1.0/1.1/1.2/1.3 support to break and inspect TLS encrypted sessions that may be needed for encrypted application analysis, UTM functions on encrypted flows within the context of lateral movement detection and prevention			✓

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