Versa SD-WAN – Simple, Secure and Reliable Branch to Multi-Cloud Connectivity

Multi-cloud connectivity moves the Internet perimeter from a centralized and secure HQ location, to a distributed model, where every branch location receives direct and optimized cloud access with security. The combination of SD-WAN and multi-layered security is required to make this work.

Just as the cloud is more than the hosting and storage of apps over the Internet, SD-WAN is more than network circuit aggregation and dynamic path selection. Enterprises need more than WAN reliability, agility and simplicity. The rapid rise of cloud and SD-WAN has ushered in an era where on-demand services are accessed, and operational simplicity is table stakes. When branch and corporate offices connect to multiple clouds, IT needs cloud-intelligent, dynamic multi-path connectivity and robust security. These required services need a broad range of networking and security functions that include routing, SD-WAN, carrier-grade NAT, DOS, IP address management, stateful firewall, NGFW, IPS, IDS, antivirus, and malware - all within a single platform that is simple to deploy and easy to operate.

Integrating these necessary functions into a single software platform greatly reduces complexity, while providing advanced visibility that can be programmed with automated and contextual policies. The key to enabling a smooth multi-cloud migration path is a versatile and multi-service cloud-native platform.

The traditional hub and spoke connectivity model that connects branch users through private VPNs to a data center, or corporate HQ firewall, no longer works in today's multi-cloud environments. Enterprises are rapidly moving to direct and secure, Internet and cloud connectivity, for their branch locations. SD-WAN enables each branch location to take advantage of diverse connectivity, while IT enables corporate and Internet traffic simultaneously – on the same circuits. This outcome is accomplished by creating a split tunnel, where some traffic goes to the corporate office over the VPN, through a direct branch-to-branch secure overlay; while other traffic goes directly to the Internet or cloud.

Even with a cloud security solution, the branch perimeter still requires on-premises security to control and segment traffic, along with protecting ingress attacks. For example, a bank may want to segment retail and ATM traffic from investment services for compliance reasons, or a company may choose to segment guest WI-FI traffic based on security policies. Some organizations may inspect outbound HTTP traffic through a cloud-security service, but deploy on-premises security to protect inbound non-HTTP traffic. The critical component in each scenario is to simply and cost-effectively, have security embedded into the SD-WAN across the entire enterprise edge.

The WAN Shouldn't be a Roadblock for Accessing Multiple Clouds

Enterprises with traditional network architectures struggle with costly and insufficient bandwidth utilization. Security fears have caused them to inefficiently backhaul Internet-based cloud traffic through their corporate data centers. Traditional WAN architectures weren't built to support cloud apps. These networks were designed for fixed site-to-site VPN connections, where applications reside within the corporate data center. Traditional networks compensate for this difference, by making cloud applications trombone across the WAN estate with unnecessary hops, using up valuable bandwidth, and increasing packet loss and latency.

Versa seamlessly extends branch office connectivity, securely and intelligently, to private clouds, and public clouds, like AWS and Azure, and SaaS services, like Salesforce, Office 365, RingCentral and others. Beyond standard multi-path connectivity, Versa SLA monitoring and SD-WAN policy management are available for multi-cloud and SaaS workloads. This enables enterprises to easily apply contextualized user experience criteria, to dynamically steer traffic across paths. This contextualized experience ensures the user will receive the highest possible performance and reliability for all enterprise applications and workloads.

Versa's multi-tenant architecture allows any managed service provider (MSP) to deliver value-added, productized, experience-driven multi-cloud services. A single instance of VOS supports multi-cloud connectivity for multiple end-customers, while maintaining complete routing and management separation between them.

Multi-cloud is Driving the Digital Business Transformation

The enterprise imperative to achieve digital business transformation is propelling the migration to multi-cloud/SaaS and hybrid WAN architectures. SD-WAN is an enabler and accelerator for this transformation, because of several market transitions:

- **Integrated Security** symbiotic with virtual networking services is a must for all enterprises. While security is already on the minds of all enterprises, the cost and complexity of siloed approaches will not meet business needs going forward. Additionally, enforcement of the General Data Protection Regulation (GDPR) in the EU is going to ripple to other parts of the world. Protecting against data breaches, makes a multi-layer and full security implementation in the fabric of the network a requirement.
- **Consumerization of IT** in enterprise networking and the WAN Edge. Over the next 24 months, we anticipate the need for a radically simpler user and administrator experience. We expect enterprises will want the same simplicity of setup/configure/manage/operate that Amazon Alexa or Google Home provides to consumers today.
- **Micro-Segmentation** is required across the entire network because of the need to reduce risk zones from external threats and internal threats, which stems from the demand to consolidate disparate environments into a single network architecture. A platform must meet the needs of different lines of business across the same infrastructure, while providing isolated management and control.

Some SD-WANs Are Built for Multi-cloud, While Others Are Not

The high costs and long deployments of traditional networks are causing enterprises to refocus their WANs to include a mix of circuits, from MPLS, DIA and broadband Internet, to wireless and satellite, all seamlessly aggregated and optimized by the SD-WAN.

Most SD-WAN solutions address the costs and rigidity associated with traditional WAN architectures. However, some SD-WANs are built to support multi-clouds, while others are best-suited for aggregating multiple circuits and executing last-mile performance optimizations.

The key differentiation is how seamlessly the SD-WAN directly connects users and IoT devices to cloud services, and how business policies are defined and performed using proactive traffic steering based on application types and where they reside. This approach will inherently optimize network reliability and performance, and ensure security for every application, for any cloud and SaaS service.

Versa Operating System (VOS™), when deployed by Managed Service Providers (MSPs), enables a versatile and flexible platform to create OTT cloud-managed services. Versa Director provides the contextual visibility of users, devices, locations, circuits and applications, across branches and cloud environments. It also manages the templates used for automating Zero Touch provisioning of sites – whether on-premises, or in the cloud.

Versa Multi-Cloud Capabilities

- **Direct Cloud Access (DCA)** optimizations for popular and well-known cloud sites
- **Intelligent and dynamic** optimized multi-path traffic steering for cloud applications between local-access and hub-sites in cloud-exchanges
- **Multiprotocol BGP** advertisements of application performance metrics by Versa SD-WAN endpoints in cloud exchanges
- **Versa Director** directly instantiates Versa SD-WAN instances in private clouds hosted by Openstack and VMWare, and public clouds such as AWS, Microsoft Azure, Google Cloud and many others.

Security

Security is a big concern when mission-critical applications travel over Internet circuits. Those evaluating SD-WAN solutions need to diligently assess, via a third-party benchmark such as NSS Labs, what kind of integrated security, if any, was originally designed, tested and deployed natively within the core SD-WAN solution.

For direct cloud access from the branch, enterprises need an integrated and layered security approach. The Versa SD-WAN includes an integrated set of security services to address these requirements.

Versa Secure SD-WAN, certified by NSS and ICSA Labs, is the only cloud-native software platform that integrates next-generation firewall (NGFW) and unified threat management (UTM) services covering end-to-end software-based security functions in a single and unified software platform. This includes malware protection, lateral movement detection, URL and content filtering, IPS and anti-virus, secure web gateway (SWG), DDoS and dynamic VPN/next-generation VPN.

Many enterprises require micro-segmentation for security and compliance and risk management. Versa provides micro-segmentation through native hierarchical multi-tenancy across data plane, control plane, management and analytics. This allows enterprises to micro-segment their WAN and branch to meet compliance and other operational requirements. They can deliver application and cloud intelligent traffic engineering and SLAs to meet the varying needs of multiple lines of business and departments. Versa offers a high degree of flexibility, using service-chaining to forward specific traffic flows, like WAN optimization and security to meet compliance, and security and performance requirements when using third-party virtual or physical services.

Multi-tenancy is embedded into the entire VOS – including Secure SD-WAN (on-premises or cloud), management and analytics. VOS enables service providers to utilize a single software image that provides a secure and scalable infrastructure for thousands of tenants. Versa enables multi-tenancy for virtual infrastructure that extends hierarchical control to MSP customers, while providing a secure and protected virtual SD-WAN overlay per tenant. This delivers scale, lowers cost, streamlines integration, and increases the total addressable market opportunity. With a single platform, an MSP can scale from small-branch to extra-large branch configurations, for both on-premises and clouds.

Versa supports service chaining of third-party security and WAN optimization VNF/PNFs, as well as cloud-based security services, like ZScaler and others. Additionally, VOS can be deployed as the uCPE platform, and natively host third-party virtual appliances.

In addition to seamless connectivity between on-premises and clouds, Versa is also differentiated by its embedded security. In a "cloud branch," or acting as a VPC/VNET gateway, we provide security for applications that are known within our robust detection library, or user-defined application signatures, for unique application and database workloads hosted in the cloud. Versa security provides AV, IPS, Anti-Malware, DLP and even lateral-movement detection within the cloud. This protects the cloud-perimeter – while preventing malicious events from impacting compute, storage and network resources in the cloud.

Versa's integrated approach and minimal virtual footprint reduces the cost of a comprehensive multi-cloud WAN and branch architecture, which enables simplified policies, fewer virtual resources, and lower cost. Other SD-WAN solutions have to either leverage "good-enough" native security, or add a separate virtual security solution into their overall policy management, traffic steering, cloud-footprint cost and bandwidth utilization.

Versa does not limit or reduce the capability of cloud-connected branches. Enterprises can take advantage of our advanced traffic steering policies, security policies and robust connectivity, which allows them to create enterprise-grade networking and security architectures within a single enterprise domain.

Application Intelligence

Seamless, secure connectivity to multiple cloud services is one of the more prominent benefits of a cloud-smart SD-WAN. Enterprises are deploying SD-WAN to enable secure, high-performing private and public cloud connectivity for branch offices, irrespective of the cloud platform, application and type of network transport.

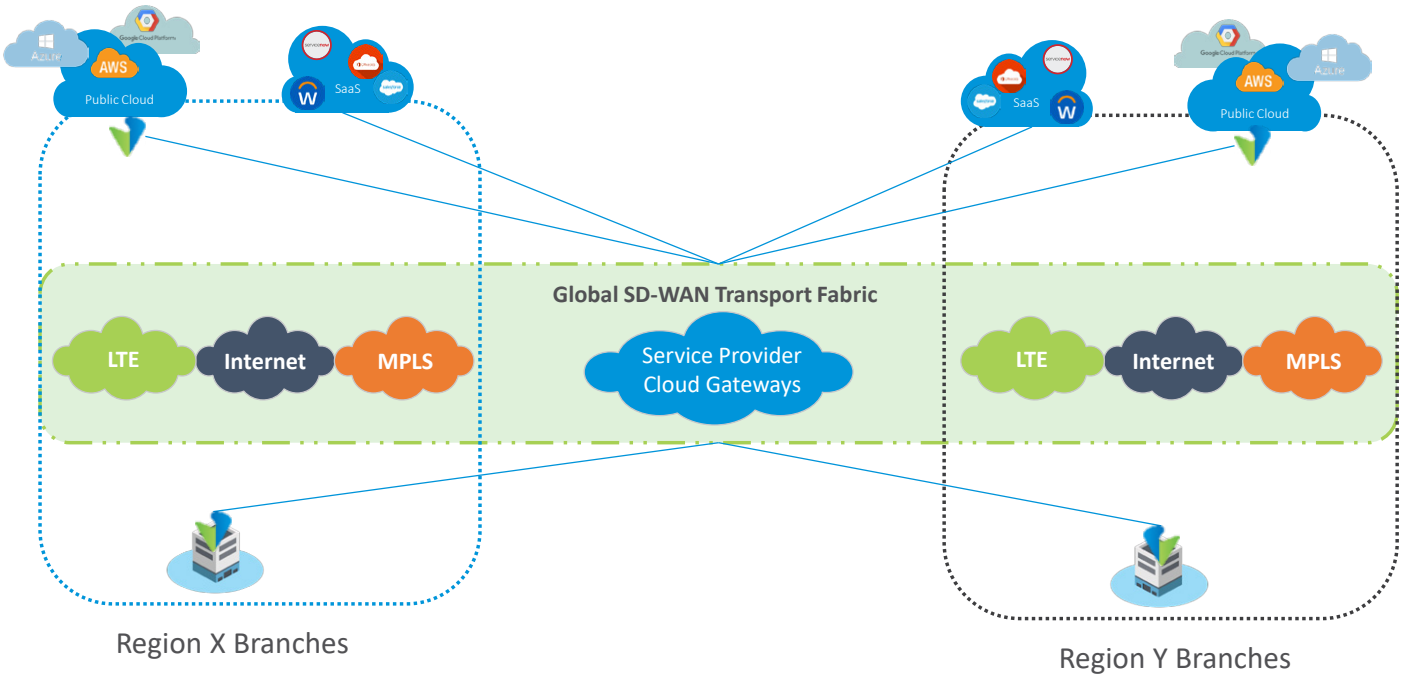
Versa supports path selection based on Versa Link Score (VLS). This is a composite score that takes into consideration TCP parameters, MOS-like scoring, round-trip-time, round-trip-delay, jitter, delay, loss and application performance metrics. Versa utilizes a MOS-like engine for all traffic flows across the SD-WAN. Using the "experience calculation" with active or passive monitoring, we can determine how the app is performing, combined with network monitoring. This allows us to deliver application intent/intelligent routing to multiple cloud/SaaS services that are mapped to the user-experience.

Simple, Secure and Reliable Branch to Multi-Cloud Connectivity

An ideal multi-cloud strategy will support diverse business needs and cloud diversity, with cloud-to-cloud inter-connectivity for workload migration, security, management, and monitoring.

With Versa, enterprises can now leverage the cost advantages, flexibility, scalability, and ease-of-access provided by commodity Internet links connecting to multiple clouds, without worrying about the security, performance and reliability of mission-critical data being compromised.

Optimized Multi-Cloud Connectivity



IaaS Market-Leader Integration

Microsoft Azure: Utilizing Versa Secure SD-WAN as on-premises branch solution, enables customers who have business applications (cloud workloads) in Microsoft Azure to gain optimized connectivity to them by providing cloud workloads close to the users. Additionally, it enables dynamic, secure branch-to-branch and branch-to-Azure secure connectivity with SD-WAN application-aware intelligent traffic steering across the Microsoft global backbone, which has more than 130 edge sites worldwide. Learn more here.

Amazon AWS: The Versa solution, available in the AWS Solution Space, is designed to allow for easier enterprise-branch WAN connectivity that extends to customers' cloud environments with all the advantages of Secure SD-WAN, including fully encrypted traffic through DCA (direct cloud access) and direct Internet conduits, and HA edge routing through

Versa leveraging Amazon Transit Virtual Private Clouds (VPCs). This next-generation branch-cloud network topology is based on an architecture scalable across thousands of applications and VPCs, as well as thousands of on-premises nodes that automatically spin up SD-WAN tunnels to customers' SD-WAN virtual appliances deployed in their Amazon VPCs. Learn more here.

Versa Networks

Gartner WAN Edge Infrastructure Magic Quadrant Visionary and NSS Recommended NGFW

Simple – Secure – Reliable

Transforming the WAN edge for Multi-Cloud

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