Versa Secure SD-WAN for Satellite Connectivity

Get the most out of your data transport mix

Secure SD-WAN has emerged as a critical architecture that enables organizations to make the most out of their satellite connectivity, whether it's the only data transport option or part of a mix of options. Versa Secure SD-WAN provides the networking agility and security necessary to intelligently optimize general corporate or IoT data traffic over satellite networks for use cases in defense, maritime, oil & gas, aviation, and many other vertical industries.

Benefits of the Versa SD-WAN solution that enable customers to optimize, secure, and increase the resilience of their satellite network communications include:

- **Advanced traffic engineering** to perform intelligent link bonding across multiple transport systems
- **The matching of applications in real time** to the path that best meets the needs of the specific application
- **An improved user experience** through advanced networking functions like TCP optimization and hierarchical class of service, despite any issues of high latency, packet loss and congestion
- **The ability to reduce network sprawl**, consolidate services, and minimize hardware, space and power requirements through an integrated security stack, the flexibility of running security functions in Versa's cloud gateways, and the option of deploying uCPE that integrates LTE and WiFi modems and the VNFs of other vendor
- **"Zero touch" provisioning capabilities** that enable customers to easily deploy network endpoints even in the most remote locations, and
- **Optional implementation of the full Versa SASE solution,** combining Versa's secure SD-WAN service with full SSE network security, including integrated Next-Generation Firewall, Secure Web Gateway, CASB, and Zero-Trust Network Access capabilities.

Optimizing the satellite connection with Versa

Traffic engineering

The advanced application-based traffic steering engine in Versa can be used to bond several different satellite paths together and either load balance or prioritize applications for different paths, including over multi-orbit networks. Versa considers the configured bandwidth for WAN interfaces and then load balances sessions effectively even when the links have differing bandwidths. Policies can be created where latency-tolerant traffic types, such as bulk updates, are sent to a GEO link to free up bandwidth on the lower latency links for the more latency-sensitive traffic such as Zoom calls or Teams traffic.

The traffic steering policies also enable very flexible WAN redundancy scenarios. Satellite backup policies can be set up for terrestrial traffic to switch to satellite in the case of fiber cuts or similar outages. The built-in monitoring feature can consider the health of the link so that if a weather event is causing "rain fade" on a MEO or LEO link, the traffic can switch over to the GEO link at a certain packet loss threshold. Similar policies can be used to automatically switch over paths in mobile deployments when latency or packet loss increases if a device moves from one coverage area to another.

Alternatively, policies can also be implemented to load balance across paths, even applying weighted algorithms to optimize the available bandwidth in every link. The traffic engineering policies make decisions on a per-session basis, which makes for a consistent, no-fuss user experience.

Versa can also implement traffic remediation techniques to overcome degraded links when there is no other transport available. VOS supports packet replication techniques that enable it to send copies of the same packet over different transport to ensure that it arrives to its destination one way or the other.

Furthermore, Versa integrates Forward Error Correction (FEC) into its network stack. FEC sends a hash packet for every set number of packets. This extra piece of information allows the system to recover any lost packet in transit. Since both these features add overhead, the system provides flexibility so that they can be turned on only under certain degraded link conditions.

Application monitoring

SaaS application monitoring can be provisioned to find the best gateway to use to reach cloud-based applications. By using SaaS monitoring, the system can measure the latency and loss of a particular link using active or passive mechanisms. Active mechanisms include generating test probes, such as sample HTTP connections, DNS probes, or even ICMP messages. The system can also gather information passively by measuring the retransmissions and RTT of TCP connections and deriving packet loss and latency measurements from them.

Tunneling overhead reduction

Overhead can be an issue with satellite networks. Legacy SD-WAN solutions usually require building and maintaining IPsec tunnels to form a secure overlay to manage and protect communications. Lightweight tunneling protocols reduce the overhead added for SD-WAN networks. Versa's tunnel-less SD-WAN solution identifies the mutable and immutable parameters of the packet headers and replaces the immutable parameters with a session identifier. That way it can reduce much of the overhead created by a tunnel and save valuable throughput on a satellite link. Furthermore, this allows us to achieve a higher MTU inside the SD-WAN overlay.

TCP optimization

Network latency and packet loss throttle TCP connections because they affect the way TCP negotiates connection windows. The Versa Secure SD-WAN includes a TCP optimization engine that helps reduce the effects of network impairments over application. First, the user can implement an intelligent TCP proxy that splits connections in situations where the user can improve the connection behavior. Furthermore, one can configure several available congestion avoidance protocols and buffer tuning settings. This enables the administrator to couple the Client and Server TCP buffers taking into consideration the latency and other network considerations. Finally, Versa implements different congestion avoidance protocols. The user can select the protocol that better suits its application and network conditions. The user can even configure protocols that are not available for the host operation systems.

TCP optimization is managed by traffic policies, so it can be applied only to specific types of traffic, and certain applications can get preferential treatment. Similar to the FEC feature, this feature can also be configured to only take effect under specific network latency conditions. Versa supports advanced TCP optimization features and congestion control algorithms like BBR, Hybla, SACK, and Recent Acknowledgement.

Hierarchical QoS

The Versa solution can optimize expensive satellite bandwidth even for a single path connection with application-aware QoS policies. In one example, a cruise ship operator had limited bandwidth and was getting many complaints about the performance of internet services from their passengers. Reviewing the data provided by Versa Analytics showed that passenger traffic included a lot of automatic traffic such as iCloud, Google Cloud, and software updates that was competing with the passenger's interactive traffic. Once policies were put into place to lower the priority of these apps, the number of passenger complaints dropped to a fraction of what they were.

Versa offers traffic shaping at the physical interface, logical interface, and forwarding-class level. With the adaptive-shaping feature, a spoke can signal its configured receive rate to remote hub devices to reduce the strain on the underlay network. Remote devices are told to shape traffic to the advertised rate and apply shaping so that the quality-of-service policy can be preserved and prevent traffic from using underlay resources, only to be dropped at a congested satellite modem.

DNS proxy

Versa Secure SD-WAN software has integrated a DNS proxy that enables network administrators to intercept DNS requests and provide them with special treatment. It can redirect the DNS request to the most optimal server, and even match based on the request conditions and steer it accordingly. Furthermore, it can reduce the latency for DNS lookups by caching results after the first lookup.

Advanced security

Versa provides integrated next- generation firewall (NGFW), secure remote access, and unified threat management (UTM) services that protect applications and user activity across the network. This allows the power and space footprint to be reduced compared to using separate network and security devices and allows simpler logistics for a total network solution.

Versa hardware can be added into a greenfield package to bundle SD-WAN and security functions as a single device. The functionality can be also added to replace existing security devices in brownfield SD-WAN implementation.

As part of the SASE framework, Versa offers its advanced security services both on-premises and in the Versa cloud. Versa has a global network of POPs where it has the ability of not only offering UTMaaS, but also some other advanced security services like DLP, CASB, and SWG.

When combined with the SaaS Monitor, the system can automatically determine which is the gateway that provides the best performance for critical applications. Also, the administrator can decide whether to run these services on-premises or in the cloud. Running services in the cloud allows users to deploy thinner branches. Satellite customers often have power and space limitations. So, they can choose to deploy a light hardware option on-premises and run their advanced security features in the Versa cloud.

Deployment options and assistance

Versa has a wide range of options adaptable to each customer's requirements for deploying its SD-WAN, including white-boxes, hypervisors, cloud environments, or Versa-branded boxes. Several models have LTE modems or Wi-Fi access points built directly into them to reduce the hardware footprint, and also support uCPE capabilities to integrate VNFs of other vendors. Reducing the number of appliances obviously helps organizations reduce their OPEX and CAPEX.

Configuration for these devices is highly templatized to keep network configurations consistent. The most common configuration tasks use Versa Workflows to create the initial templates. Optionally, Versa Titan™ and Concerto™ make managing device configurations even more streamlined.

Several provisioning options allow for sending new equipment to locations with minimal support from field engineers. For devices with internet connectivity, global Zero Touch Provisioning (ZTP) allows a factory-fresh device to securely reach out for its configuration automatically, without any input from an on-site technician. For deployments without internet connectivity, a technician can paste a URL via the LAN port to trigger the device provisioning. Device provisioning can also be triggered via a simple script. In all cases, the initial configuration is stored in Versa Director, waiting for a device to download it via one of the provisioning options. There is never any pasting of large quantities of configuration data over a slow console port!

Versa's systems engineering team has experience sizing, designing, and deploying our solutions in diverse satellite network environments, from airplanes to ocean-going vessels to oil rigs, and in various remote locations. We offer several levels of managed services to help ramp up a new Versa SASE network, and professional services to help design and plan network enhancements with new SASE features.

For more information on Versa Networks, please visit https://versa-networks.com, contact us at https://versa-networks/contact or follow Versa Networks on Twitter @versanetworks.

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