VERSA NETWORKS

SD-WAN and Secure Service Edge for DoD and Ultra-Secure Deployments

Abstract

This white paper describes how the Versa SD-WAN, ZTNA, and SASE solutions are very well suited for satellite, maritime, and federal networks that operate in adverse and DDIL (Denied, Disrupted, Intermittent, and Limited) conditions and which often leverage NSA's High Assurance Internet Protocol Encryption (HAIPE) or Commercial Solutions for Classified (CSfC)-based architectures.

Introduction

Versa Networks is a market leader in SD-WAN, SD-Security, and SASE technology, with over 120 service provider partners worldwide. In the United States (US), Versa's largest partners include Verizon, Lumen, and Comcast. Versa has the largest number of Global SD-WAN deployments. Versa solution is responsible for the networking and security of many global mission-critical networks in the financial, banking, energy, satellite, maritime, retail, health care, and other verticals where the best user-to-application performance in the face of all types of failures and security are the primary focus.

Gartner has recognized Versa in the upper right of the SD-WAN Magic Quadrant (MQ). **The Gartner MQ report included two subcategories where Versa placed #1**; those are:

1. Critical Capabilities
2. Large Complex Global Networks. Gartner has also produced a report on companies with the most SASE capabilities. Versa placed at the top of the Gartner SASE capabilities report delivering 13 out of 15 technologies identified by Gartner.

NSS Labs has tested Versa SD-WAN, NGFW (Next Generation Firewall), and NGIPS (Next Generation Intrusion Prevention System. Product efficacy with stopping attacks was very high, while the cost of Mbps secured was the lowest amongst OEMs.

Versa has married its native SD-WAN, SD-Security, and Multi-Cloud features to deliver a cohesive and comprehensive SASE and Multi-Cloud solution.

Some of the main differentiators between Versa and other solutions are:

- Integration of SD-WAN, SD-Security, and Multi-Cloud into a single platform.
- Single pane of management for SD-WAN, SD-Security, and Multi-Cloud.
- Unified policy management - One software stack (VOS) for on-premises, SASE cloud, and the edge.
- Multi-defense system-based threat protection and near real-time remediation.
- Zero Trust Network Access based on User, Group, Device Posture, Application, Content, Geo-Location, Entity Confidence Score, Security Tag associated with the source, and many more factors.
- Support for Secure Private Access, Secure Web Gateway (SWG), Cloud Access Security Broker services, Data Loss Prevention (DLP), Remote Browser Isolation (RBI), User Entity Behaviour Analytics, Security based on AI/ML, Dynamic Analysis of Malware using Sandboxing, and Next-Generation Unified Threat Management.
- VANI (AIOps) for Anomaly Detection, Traffic Prediction, Event Correlation, and Chatbot (Verbo).
- Optimal traffic steering and SaaS acceleration using Versa Traffic Engineered (TELS: Traffic Engineering Link State) SASE backbone.
- Dynamic Tenant & Virtual Gateway instantiation – elastic auto-scaling and network intelligence to meet real-time capacity demands.
- SD-WAN Lite for SASE Clients and Third-Party Routers
- Single Pass architecture - unparalleled performance at scale.

- Hierarchical Multi-tenancy & granular Role Based Access Control (RBAC).
- Versatile Service Chaining of Virtual Network Functions (VNFs) and Physical Network Functions (PNFs).
- Support for big data analytics.
- Integration with multiple security intelligence sources, including Cyber Situational Awareness (SA) tools for expedient global dissemination and real-time enforcement.

Figure 2 shows a periodic chart of the routing, SD-WAN, and secure services edge features that Versa supports. Using these capabilities, Versa enables its customers to do the following:

a. Deploy a secure traffic-engineered global SD-WAN and SASE network that can provide the best application experience for users and IoT devices, irrespective of their and applications' locations. This is shown in **Figure 1**.
b. Zero Trust Network Access based on User, Group, Device Posture, Application, Content, Geo-Location, Entity Confidence Score, Security Tag associated with the source, any layer3 to layer7 fields of the packet, and time of the day.
c. Multi-defense system-based threat protection and near real-time remediation.

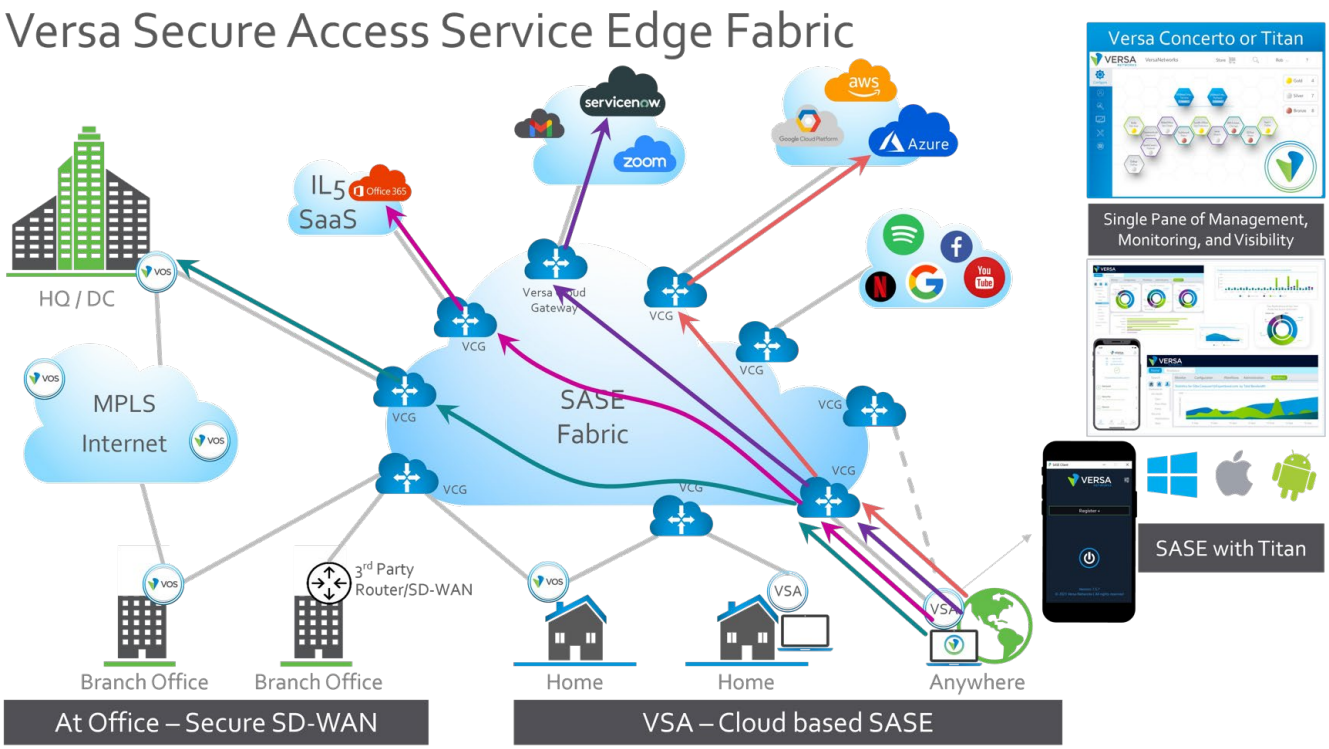

Figure 1

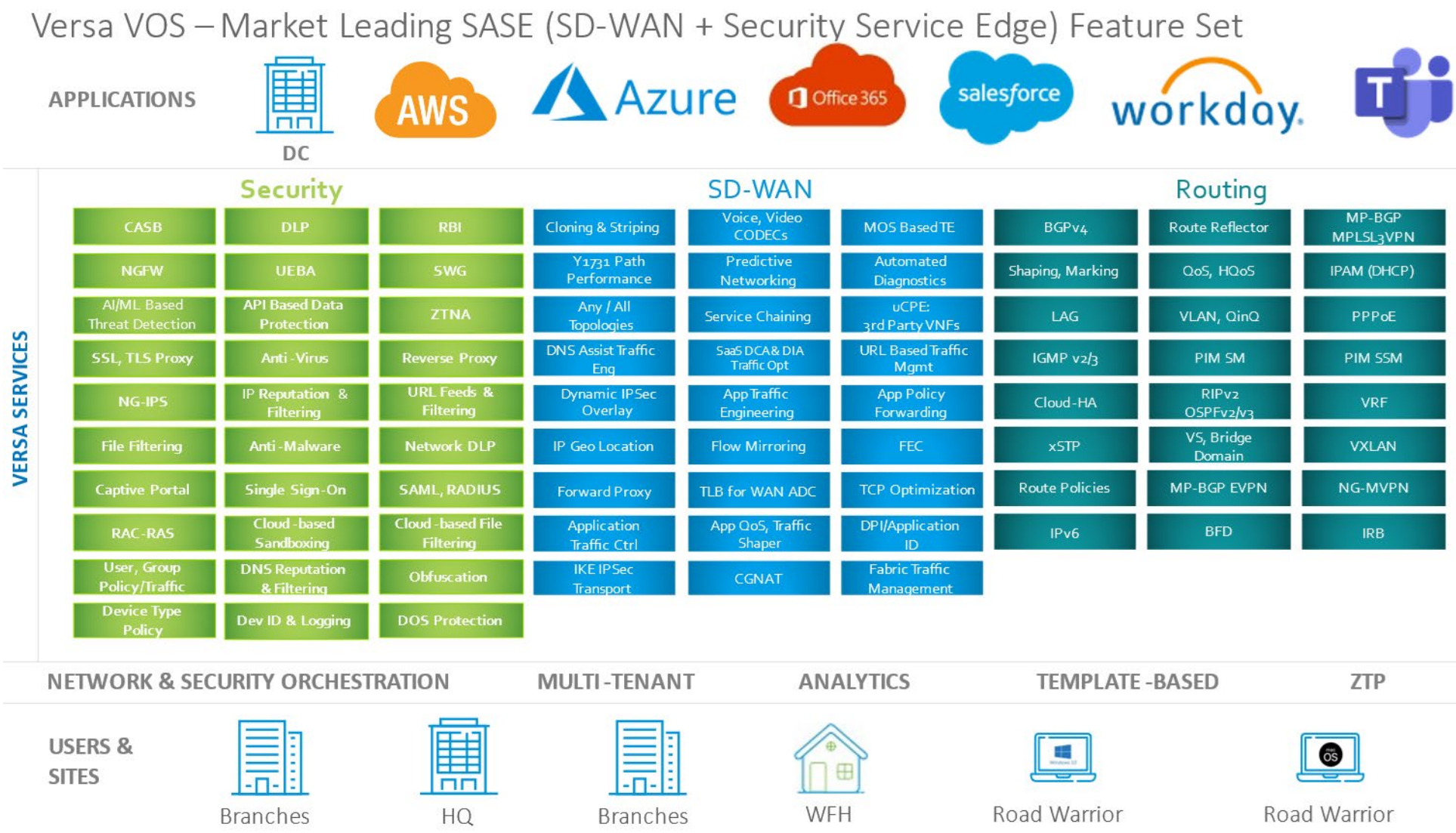

Figure 2

Features, Use, and Differentiators

Built Using IETF Standards-Based Protocols: Based on **BGP/MPLS VPN and Ethernet VPN, with the use of a Private SAFI** (Sub Address Family Identifier) to carry SD-WAN- related information such as

- Key management
- Access circuit state and status
- NAT-related information
- Information about SLA to critical applications

Key management and certificate management

- True emulation of IKE without using IKE.
- A branch's secret is never sent on the wire and can be rotated as often as every four minutes.
- A unique shared secret is algorithmically derived between every pair of branches.
- Advanced certificate management capabilities.
- Support for OCSP, CMPv2, SCEP, and ACME
- Support for external key management using **Key Management Interoperability Protocol (KMIP)** for deployments requiring keys generated by the tenant/customer.

Ability to be deployed in DDIL (Denied, Disrupted, Intermittent, and Limited) environments

- **Three VM images** - The minimum set of images to operate completely disconnected is three. All updates of security images are supported in a completely disconnected environment.
- **License centrally managed** by Versa Director. Versa Director is one of the three images where the license is loaded and does not require reaching back to or through the internet.
- **Versa Analytics** is one of the images. It provides operators with full visibility of security, connectivity, and performance.
- **Single Pane of Management** as well as Centralized Provisioning, Management, Monitoring, Visibility, and Big Data Analytics for all SASE services (SD-WAN, SSE) and multi-cloud
- **Most widely deployed SD-WAN solution** by Satellite-Based Service Providers, Shipping, and Maritime. Support for up to 14 underlay transport domains per node. It can simultaneously accommodate multiple underlays such as SATCOM (LEO, MEO, GEO), Private MPLS, LTE/5G, terrestrial fiber, broadband, and others.

Versatile Traffic steering, Traffic Conditioning, and Advanced TCP Optimization

- **Traffic steering based** on any layer3-layer7 fields of the packet**,** Layer7 application, URL category, user, group, device posture, Entity Confidence Score, Geo-Location, Security Tag associated with the source, time of the day, and other factors.
  - **Tunnel-less** on a per-flow basis. Versa can support Tunnel-less SD-WAN where and when required. Please refer to the section "**Versa's Tunnel-Less SD-WAN Solution**."
  - **Encryption** can be enabled or disabled on a per-flow basis.
  - Versa solution is very well suited and provides the best application experience for satellite, maritime, and federal networks that leverage NSA High Assurance Internet Protocol Encryption (**HAIPE**) or Commercial Solutions for Classified (**CSfC**)-based architectures that might experience **DDIL** and adverse conditions. Please refer to the section "**Versa SD-WAN for Classified Solution.**"

- **Traffic steering is based on the visibility of end-to-end dynamic path characteristics** such as packet loss, latency, and jitter. This feature provides more accurate and resilient end-to-end application SLAs. All other vendors select the best path based on SLA to the immediate next hop. Only Versa can steer traffic based on end-to-end path metrics.
- **Traffic conditioning using FEC, replication, and other measures**, which are all automatically triggered when SLA degrades and stopped when the SLA improves. These capabilities are available for all traffic types rather simply for voice and video.
- **Support advanced TCP optimization and congestion control algorithms** like BBR, Hybla, SACK, Recent Acknowledgement.

Comprehensive QoS Capabilities: Versa solution supports very comprehensive QoS (Layer3-QoS-Policy, AppQoS Policy, Policer, Marking, HQoS with 4K shapers and 64,000 queues) and SD-WAN traffic steering capabilities. Based on the layer3-layer7 fields within the received traffic, including application, URL category, and device posture, a forwarding class (FC) and packet-loss priority (PLP) is associated with a traffic flow. The FC and PLP prioritize and schedule the traffic within a VOS platform. Additionally, rewrites of inner and outer headers and egress-shaping are done based on the FC and PLP. Hence, mission traffic is prioritized over less-critical traffic within a Versa appliance as well as on transmission.

Very well suited for brownfield network deployments.

- Support all major layer2 and layer3 (IPv4 and IPv6) protocols.
- Support for IPv4, IPv6, and dual-stack for VRFs, as well as underlay transport.

Support for **complex topologies** such as Full Mesh, Hub and Spoke, Partial Mesh, Spoke-Hub-Hub-Spoke, Hub-Controllers, Controller behind the hub, and many more.

Very rich template infrastructure: Versa supports a very rich template infrastructure that supports a hierarchy of templates. Using this hierarchy of templates, global policies can be defined with specific policies having higher precedence. This makes the overall configuration management simple and efficient. A device group is a collection of devices with similar but not identical configurations. A device group is typically associated with a device template and a set of service templates of different types, such as security service template, application steering service template, QoS service template, General service template, and others. A device group can be associated with multiple security service templates which are applied in an operator-specified order. Additionally, there can be device-specific security service templates.

CGNAT for v4 and v6: NAPT-44, DNAT-44, Dynamic NAT-44, Basic-NAT-44, Twice Basic NAT-44, NPT66, NAT64, MAP-E

Multiple options for Zero Touch Provisioning.

Universal CPE to host multiple VNFs. Service Chaining hosted VNFs and external physical PNFs.

Versa's Tunnel-Less SD-WAN Solution

Versa also offers a Tunnel-Less SD-WAN solution, which makes the network more scalable, and bandwidth-efficient, eliminating fragmentation of packets and better security. Some of the use cases that drove this tunnel-less solution were satellite, maritime, and federal networks that leverage NSA High Assurance Internet Protocol Encryption (HAIPE) or Commercial Solutions for Classified (CSFC)-based architectures.

In the case of all Tunnel-less solutions, the inner packet is divided into mutable and immutable fields. **Figure 3** shows all the common fields of an IP header, TCP header, and UDP header. A subset of immutable fields within an IP header, TCP header, and UDP header, which are invariant for the duration of a 5-tuple flow are show in blue color. All solutions associate some form of a cookie, label, flow-id, or a (source-port, destination-port) pair with the immutable fields. This cookie/label/flow-id/port-pair is communicated with the entire payload packet from a sender SD-WAN CPE (SDWAN-CPE1) to a receiver SD-WAN CPE (SDWAN-CPE2) at least once. Once a remote SDWAN-CPE (e.g., SDWAN-CPE2) has learned the mapping of the sender (e.g., SDWAN-CPE1) and communicates it to the sender, the sender (SDWAN-CPE1) encodes its flow-id in the SDWAN-header and skips all immutable fields of the payload packet in the traffic that is sent from SDWAN-CPE1 to SDWAN-CPE2. Please note that within the Versa Tunnel-less solution, a sender SD-WAN CPE skips many other IP, TCP, and UDP fields of the payload packet when sending traffic to a peer SD-WAN CPE. These are not described in this document.

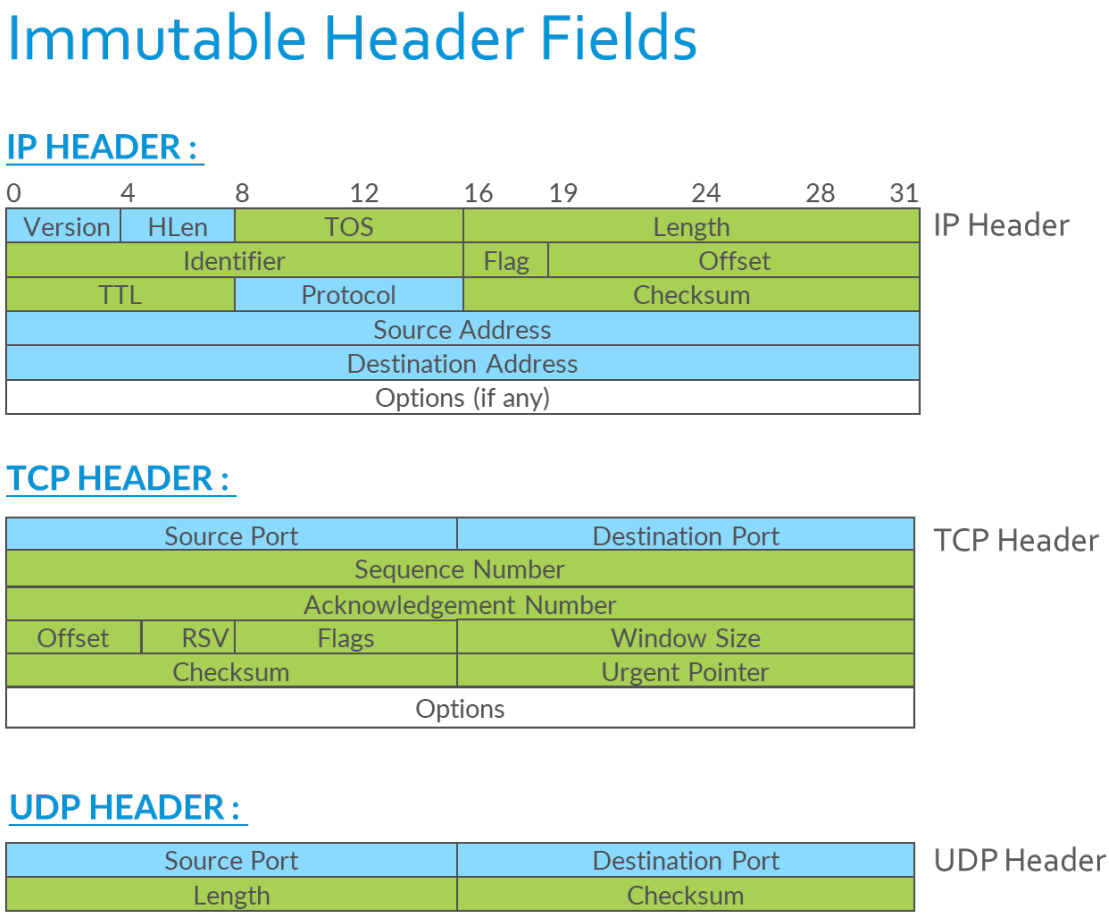

Figure 3

A detailed packet flow in the case of the Versa Tunnel-less solution is described in **Figure *4***, where Client5 (C5) is communicating with Server7 (S7) through SD-WAN CPE-1 and SD-WAN CPE-2.

1. Step-1 shows a packet from Client5 to Server7 with Payload1 from C5 to S7.
2. On receiving this packet for a new 5-tuple flow, SD-WAN CPE-1 validates his packet, creates a C5 to S7 session, chooses FlowId51 for this flow and runs all the rich Layer3-Layer7 services (ZTNA, SD-WAN, UTM, CASB, SWG, HQoS, etc.). Information relating to all services is sent to Versa Analytics.
3. Next, as shown in step-3, CPE1 encrypts the packet received from C5 to S7, encodes its local flow id (CPE1-To-CPE2 FlowId51) in the outer UDP-header, and sends the packet to SD-WAN CPE2 along the best underlay path for the application to which this packet belongs.
4. On receiving this packet from CPE-1 for a new 5-tuple flow, SD-WAN CPE-2 creates a session, saves the FlowId51 that it received from CPE1 which it would use in future packets, decrypts and validates the packet, allocates its own FlowId22 for this flow and runs all the rich Layer3-Layer7 services (ZTNA, SD-WAN, UTM, CASB, SWG, HQoS, etc.). Information relating to all services is sent to Versa Analytics. This is shown in step 4.
5. CPE2 forwards the decrypted packet from Client5 to Server7. This is shown in step 5.
6. Step 6 shows the response from Server7 to Client5 with Payload2.
7. On receiving this S7 to C5 packet, SD-WAN CPE-2 validates this packet, runs all the rich Layer3-Layer7 services (ZTNA, SD-WAN, UTM, CASB, SWG, HQoS, etc.), encrypts the packet received from S7 to C5, encodes its local flow id (CPE2-To-CPE1 FlowId22) in the outer UDP-header, and sends the packet to SD-WAN CPE1 along the best underlay path for the application to which this packet belongs. SD-WAN CPE2 also informs SD-WAN CPE1 that it has learned FlowId51 that CPE1 has allocated for this flow. This is shown in step 7.
8. In step 8, SD-WAN CPE1 updates the session state with the fact that CPE2 has learned about its FlowId51 and is ready to receive packets that are encoded with FlowId51.
9. After performing all the necessary services on the decrypted packet, CPE1 forwards the packet with Payload2 from Server7 to Client5. This is shown in step 9.
10. After receiving packet with Payload3 from Client5 to Servier7 (step 10), SD-WAN CPE1 validates and runs through all services. Next it creates a new payload which only has the mutable fields of Client5 to Server7 packet with Payload3. It encrypts this payload, encodes its local flow id (CPE1-To-CPE2 FlowId51) in the outer UDP-header, and sends the packet to SD-WAN CPE2 along the best underlay path for the application to which this packet belongs. SD-WAN CPE1 also informs SD-WAN CPE2 that it has learned FlowId22 that CPE2 has allocated for this flow. This is shown in step 11.
11. In step 12, SD-WAN CPE2 updates the session state with the fact that CPE1 has learned about its FlowId22 and is ready to receive packets that are encoded with FlowId22.
12. After performing all the necessary services on the decrypted packet, CPE2 forwards the packet with Payload3 from Client5 to Server7. This is shown in step 13.
13. After receiving packet with Payload4 from Server7 to Client5 (step 14), SD-WAN CPE2 validates and runs through all services. Next it creates a new payload which only has the mutable fields of Server7 to Client5 packet with Payload4. It encrypts this payload, encodes its local flow id (CPE2-To-CPE1 FlowId22) in the outer UDP-header, and sends the packet to SD-WAN CPE1 along the best underlay path for the application to which this packet belongs. This is shown in step 15.
14. After performing all the necessary services on the decrypted packet, CPE1 forwards the packet with Payload4 from Server7 to Client5. This is shown in step 16.

Packet Flow:

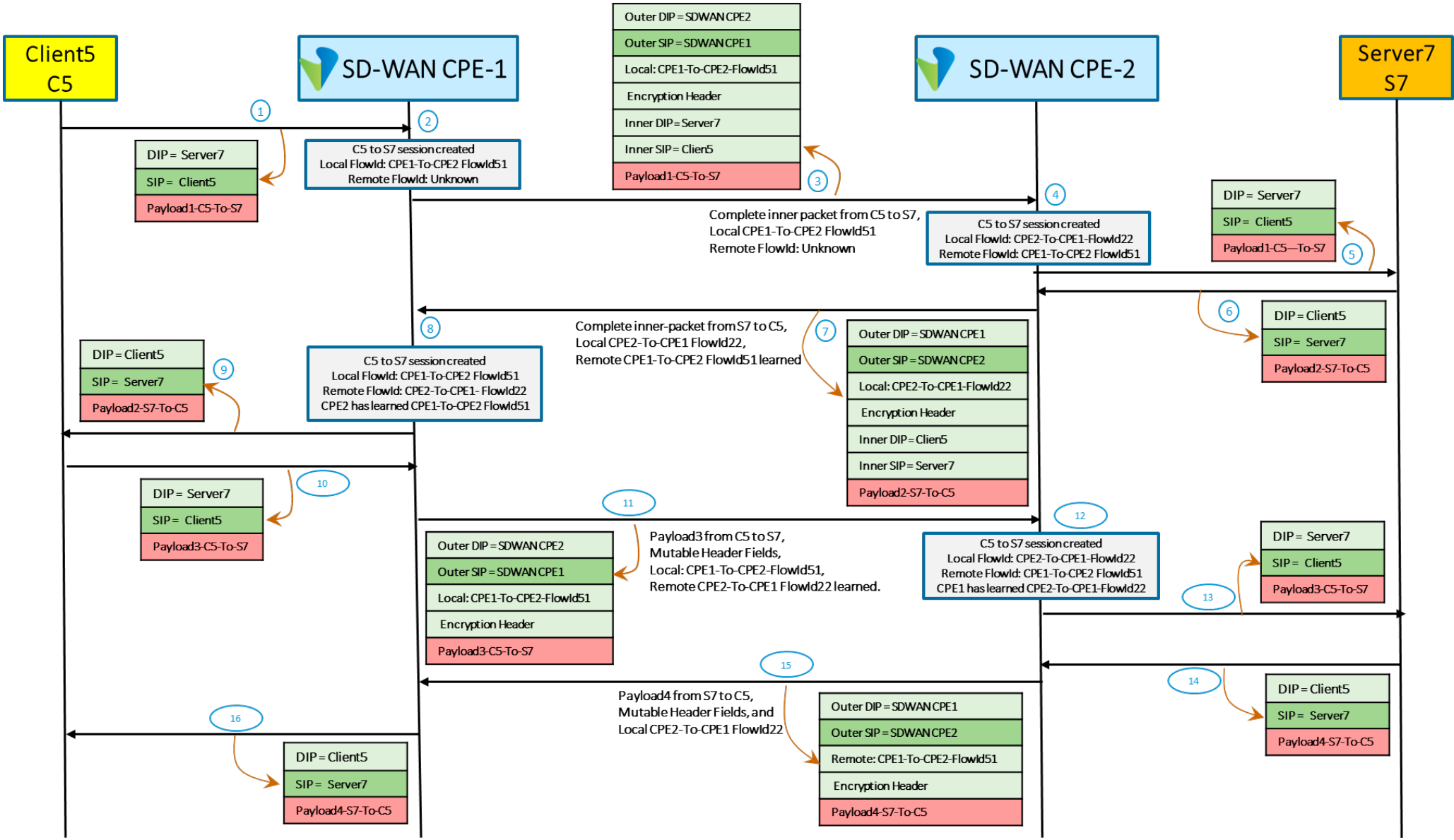

Figure 4

In Versa's tunnel-less solution, the first packet from an ingress SD-WAN node to a peer SD-WAN node and vice versa will have complete information, while all subsequent packets from either direction will only carry the metadata along with the payload, allowing us to accommodate larger payloads or conserve bandwidth usage based on our use case.
Compared to existing tunnel-less technologies on the market, Versa's innovative Tunnel-Less solution has significant advantages, some of which are listed below.

a. The Versa solution only needs to open only a single port, "4790" or “4500,” within the SD-WAN underlay as opposed to several ports that other technologies require.
b. The Versa Tunnel-less solution does not invalidate the sequence numbers of received packets, nor does it add any meta-data to TCP SYN packets, which might not be acceptable to firewalls and transit devices. As a result, unlike other solutions, TCP packets do not have to be transformed into UDP packets.
c. The Versa Orchestrator supports a very rich template infrastructure using which a group of devices can be configured centrally with similar configurations which need not be identical. As a result, information relating to tenants, services, and security policies does not have to be carried as part of any meta-data.
d. The Versa Tunnel-less solution is unaffected by the presence of NAT devices and firewalls in the underlay transport networks. The Versa solution does not require keep-alive packets for individual user sessions so that NAT sessions do not expire.
e. A Versa Branch (VOS) uses a variant of Connectivity Fault Management/Y.1731 (CFM: IEEE 802.1ag) to monitor all the possible paths to other branches with which it needs to communicate directly. A path is defined by the transport address on one branch to a transport address on another branch. VOS uses this variant of CFM to build a database of information about (Latency, Jitter, Packet Loss, and Roundtrip Delay) to other SD-WAN sites over various access circuits. This SLA measurement is done per (Transport-Classifier, Transport-Path), where Transport-Classifiers are DSCP and MPLS EXP. Since the SLA offered by an underlay transport path is mainly dependent on (Transport Classifier, Transport-Path), the Versa solution is much more scalable than doing end-to-end active SLA measurement for individual user sessions. Versa does support passive monitoring of individual sessions.
f. Versa encryption supports IETF-compliant replay protection, initialization vector, HMAC, and just about every cipher. The Versa SD-WAN CPEs do not require Time Based HMAC (which requires the SD-WAN CPEs to have accurately synchronized clocks) for detecting a replay of packets.
g. Tunnelling can be enabled or disabled on a per-flow basis between any two sites.
h. Encryption can be enabled or disabled on a per-flow basis.
i. The Versa solution supports very efficient switchover of underlay transport paths and changes to transport addresses of SD-WAN CPEs.
j. Versa solution is based on protocols and mechanisms which have powered mission-critical networks over many years. The Versa solution can adapt very well to any brownfield network and allows gradual migration to SD-WAN.
k. This Tunnel-Less SD-WAN solution works cohesively and in conjunction with Versa’s best and most comprehensive set of SD-WAN features, such as application steering based on Layer7 application, user, group, URL category, device posture, entity confidence score and other factors, versatile traffic conditioning capabilities using FEC, replication, and stripping, advanced TCP congestion control algorithms like BBR, Hybla, RACK, Tail-Loss Probes, and SACK, and SD-WAN Traffic Engineering Link State.

Inter-operability with other Tunnel-Less SD-WAN Solutions

SD-WAN creates a virtual private network that is transport-agnostic, application-aware, and supports centralized management and provisioning. It is essential that an SD-WAN solution can easily insert itself into a brownfield network and allow for gradual migration from the existing MPLS or DMVPN networks to the SD-WAN network.

As explained above, in the case of all Tunnel-less solutions, the inner packet is divided into mutable and immutable fields. All solutions associate some form of a cookie, label, flow-id, or a (source-port, destination-port) pair with the immutable fields. This cookie/label/flow-id/port-pair is communicated with the entire payload packet from a sender SD-WAN CPE (SDWAN-CPE1) to a receiver SD-WAN CPE (SDWAN-CPE2) at least once. Once a remote SDWAN-CPE (e.g., SDWAN-CPE2) has learned the mapping of the sender (e.g., SDWAN-CPE1) and communicates it to the sender, the sender (SDWAN-CPE1) encodes its flow-id in the SDWAN-header and skips all immutable fields of the payload packet in the traffic that is sent from SDWAN-CPE1 to SDWAN-CPE2.

Because of the different ways (flow-ids, combination of outer source-port and destination-port) that various vendors have chosen to encode the immutable data, they can only inter-operate at the boundaries (NNI: Network to Network Interface) of the different vendors' SDWAN networks. Some of the reasons this is indeed the case is because key management, encoding of packets, encryption/decryption, the control plane (propagation of routes), management plane (configuration and monitoring), and visibility plane (big data analytics) are very different for all the vendors.

Two vendors can inter-operate using IETF-based protocols like E-BGP, IKE-based IPsec, and TWAMP. Two vendors can also add the capability to decode and encode each other's data-plane formats.

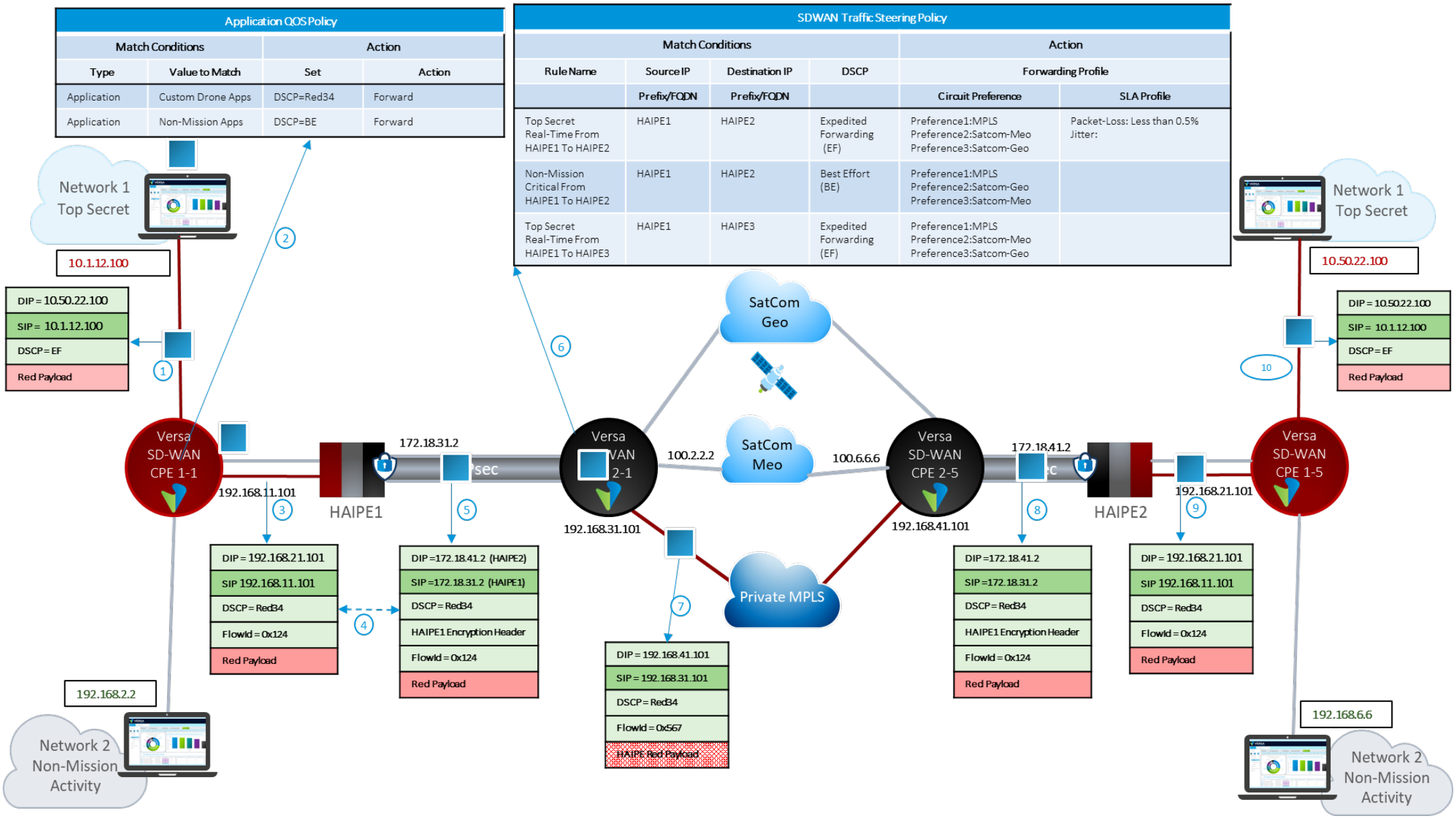

Figure 5

Versa SD-WAN for Classified Solution

Figure 5 describes how Versa solution provides its comprehensive SD-WAN and ZTNA capabilities in federal networks that leverage NSA High Assurance Internet Protocol Encryption (HAIPE) or Commercial Solutions for Classified (CSfC)-based architectures. Such deployments typically have multiple layers, where a black network consisting of several SATCOM, MPLS, Cellular (4G/5G), and other underlays provide transport to the red network.

1. CPE 2-1 and CPE 2-5 are Versa SD-WAN CPEs at the edges of the amorphous and ubiquitous black fabric. These CPEs provide comprehensive SD-WAN and SD-Security capabilities. In the example shown, the black fabric has three underlay networks – SatCom-Meo, SatCom-Geo, and Private MPLS.

2. CPE 1-1 and CPE 1-5 are Versa SD-WAN CPEs at the edges of red-site-1 and red-site-2. These SD-WAN CPEs also provide comprehensive SD-WAN and SD- Security capabilities. These CPEs could receive either top-secret data or non-mission critical data. Traffic exiting the red sites is typically encrypted by HAIPEs.
3. A laptop with address 10.1.12.100 at red-site-1 on the left of **Figure 5** would like to communicate top-secret mission-critical information to an endpoint with IP address 10.50.22.100, located at red-site-2, as shown by step-1 in the figure. Based on user configuration, SD-WAN CPE-1-1 would do the following on receiving this traffic.
    - **Classify** the packet based on application, URL category, user, group, device posture, entity confidence score, security group tag, and any layer 3-7 fields of the received packet (**classification information**).
    - The DiffServ code point of the packet egressing SD-WAN CPE-1-1 from its WAN interface (with IP address 192.168.11.101) would be determined either by a mapping table that uses the **classification information** or by copying the DSCP of the received packet or some combination of the two. Thus, mission-critical and non-mission-critical flows would be associated with appropriate DSCPs. This is shown by step 2.
    - Associate a flow-id with this flow.
    - Encrypt or not-encrypt this flow.
    - Next, the best underlay transport is chosen based on SD-WAN traffic steering policies, which take into consideration the application type and SLA offered by various underlay paths.
    - The packet then goes through "scheduling and shaping" and is forwarded to the next hop that belongs to the best underlay. This is shown by step 3 in the figure.

4. On receiving this traffic, HAIPE1 could choose to encrypt this traffic. HAIPE1 could be configured to copy the DSCP of the received packet to the outer header, which the HAIPE1 would add. This is shown in step 4. Then, as shown in step 5, HAIPE1 would encapsulate the packet with an outer header and forward the packet to CPE 2-1.

5. On receiving this packet, SD-WAN CPE 2-1 at the edge of the black network would do the following
    - Associate an appropriate flow-id

- As shown in step 6 of **Figure 5**, CPE 2-1 determines the appropriate underlay based on configured SD-WAN Traffic Steering Policy rules that would depend on the following.
  i. The Source-IP (IP address 172.16.1.1 of the source HAIPE), Destination-IP address (the IP address 172.16.5.5 of the destination HAIPE), and the DSCP of the received packet.
  ii. Configured preference for the various underlay networks for this class of the traffic
  iii. The real-time SLA observed on the various underlay networks (MPLS, Satcom-Meo, SatCom-Geo in this example).
- Does traffic conditioning using some combination of forward error correction and packet replication depending on the SLA offered by the underlay transports.
- Does packet stripping if required.
- Applies advanced congestion control algorithms like BBR and Hybla if any non- encrypted TCP traffic is received.
- The packet then goes through "scheduling and shaping" and is forwarded to the remote SD-WAN CPE 2-5 using the best underlay. This is shown by step 7 in the figure.

6. SD-WAN CPE 2-5 at the edge of the black network would do the following
   - Removes the SD-WAN header.
   - Restores the HAIPE1 to HAIPE2 packet.
   - Performs any necessary flow processing and remediation if FEC and packet replication were enabled.
   - Routes the traffic towards HAIPE2 as shown in step 8 of **Figure 5**.

7. HAIPE2 would decrypt the traffic and forward the traffic towards SD-WAN CPE 1-5 at the edge of the red- site-2, as shown in step 9.

8. SD-WAN CPE 1-5 at the edge of the red site-2 would do the following
   - Remove the SD-WAN header.
   - Restore the Endpoint-1 to Endpoint-2 packet
   - Perform any necessary flow processing and remediation if FEC and packet replication were enabled.
   - Route the traffic towards Endpoint-2 as shown in step-10 of **Figure 5**.

Non-mission critical packets, for example, from 192.168.2.2 at red-site-1 to 192.168.6.6 at red-site-2, are similarly steered appropriately based on the traffic steering and traffic conditioning configuration.

Versa Real Time Monitor and Versa Analytics

The Versa Real Time Monitor provides real-time information about all the networking, SD-WAN, and security services that are configured on each Versa appliance. It also provides information relating to the health (CPU, Memory, Bandwidth on each of the interfaces, Load) of the VOS instances.

Versa Analytics is a big data solution that analyses logs and events and provides powerful reports, analytics, and feedback to Versa Director. It integrates natively with third-party data reporting and SIEM products, such as HP ArcSight, Splunk, IBM QRadar, LogRhythm, and Elastic Search. VOS™s at branch sites continuously provide Versa Analytics monitoring information related to links, network paths, security events, services, applications, etc. Additionally, every service on the VOS™, such as the next-generation firewall, IDS/IPS, URL-filtering, CASB, SWG, DLP, RBI, UEBA, DNS Proxy, and other modules, generate flow-level and aggregate log messages that are consumed by the Versa Analytics platform. All this information can be leveraged for functions such as capacity planning and security forensics. **Figure 6**, **Figure 7** **Figure 8** , and **Figure 9** provide a few examples of information available using Versa Analytics.

Versa Analytics sends these logs to Versa UEBA over a KAFKA bus. Versa UEBA can track and flag anomalous events by all entities, such as users, laptops, phones, IoT devices, and more. If a user or an IoT device exhibits anomalous behavior, then its Entity Confidence Score (ECS) is degraded. This ECS is used in different types of policies, such as the Security Access Control Policy and Traffic Monitoring Policy. If the ECS of an entity degrades, then it is published to all subscribers (such as Versa Cloud gateways) using the Versa Message Service. The Versa Cloud Gateways can enforce real-time remediation when the ECS degrades.

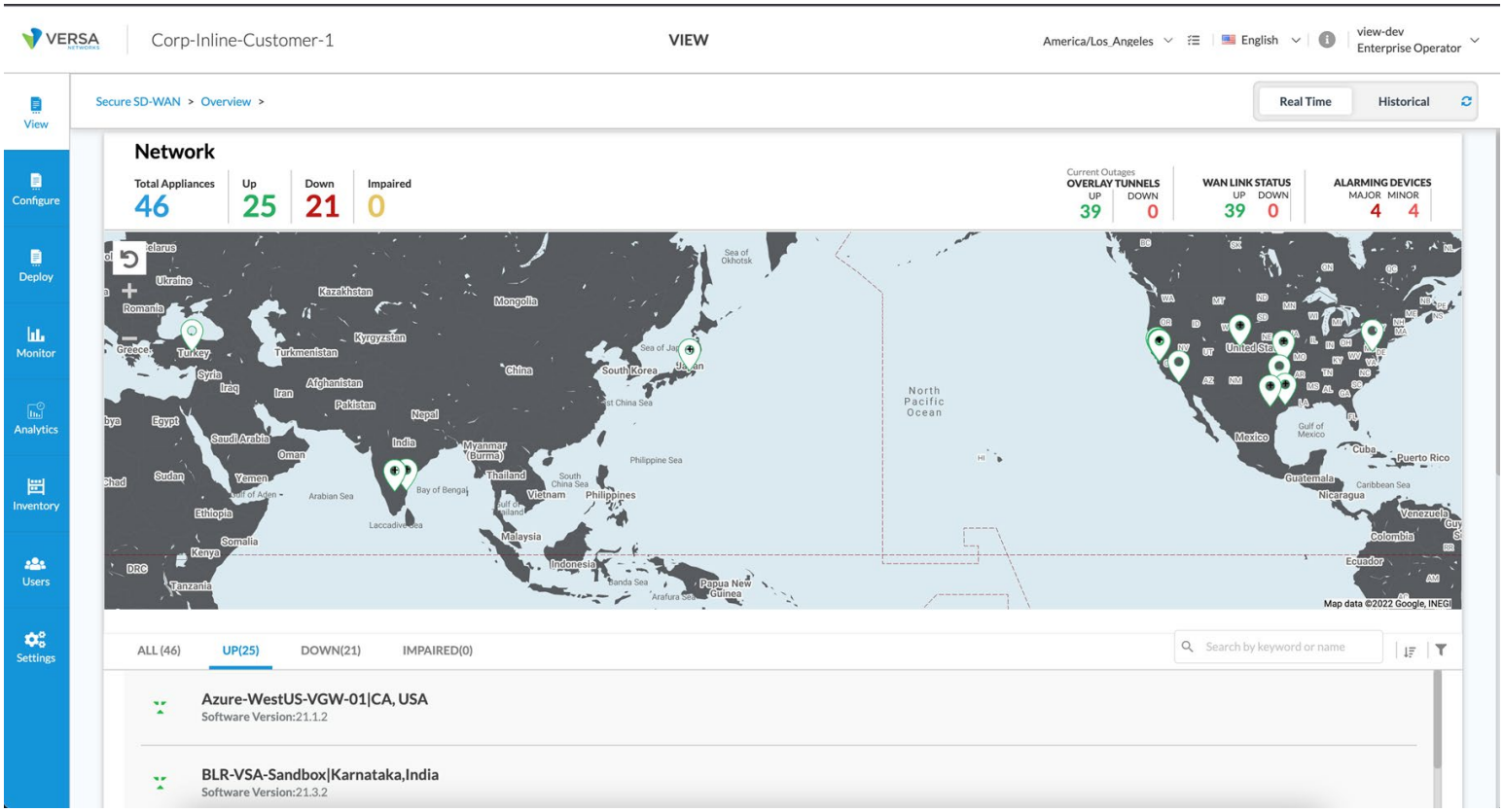

Figure 6

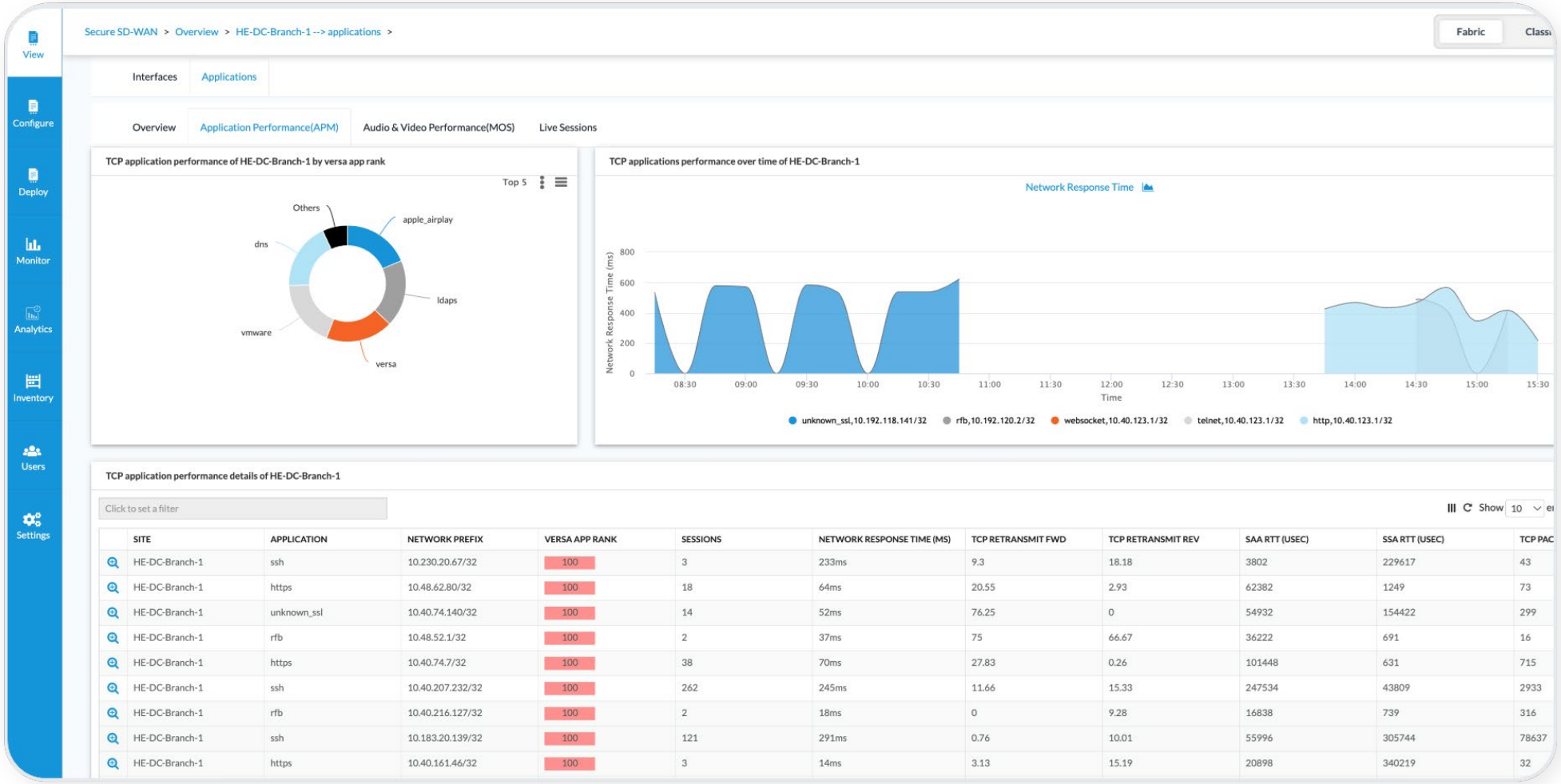

Figure 7

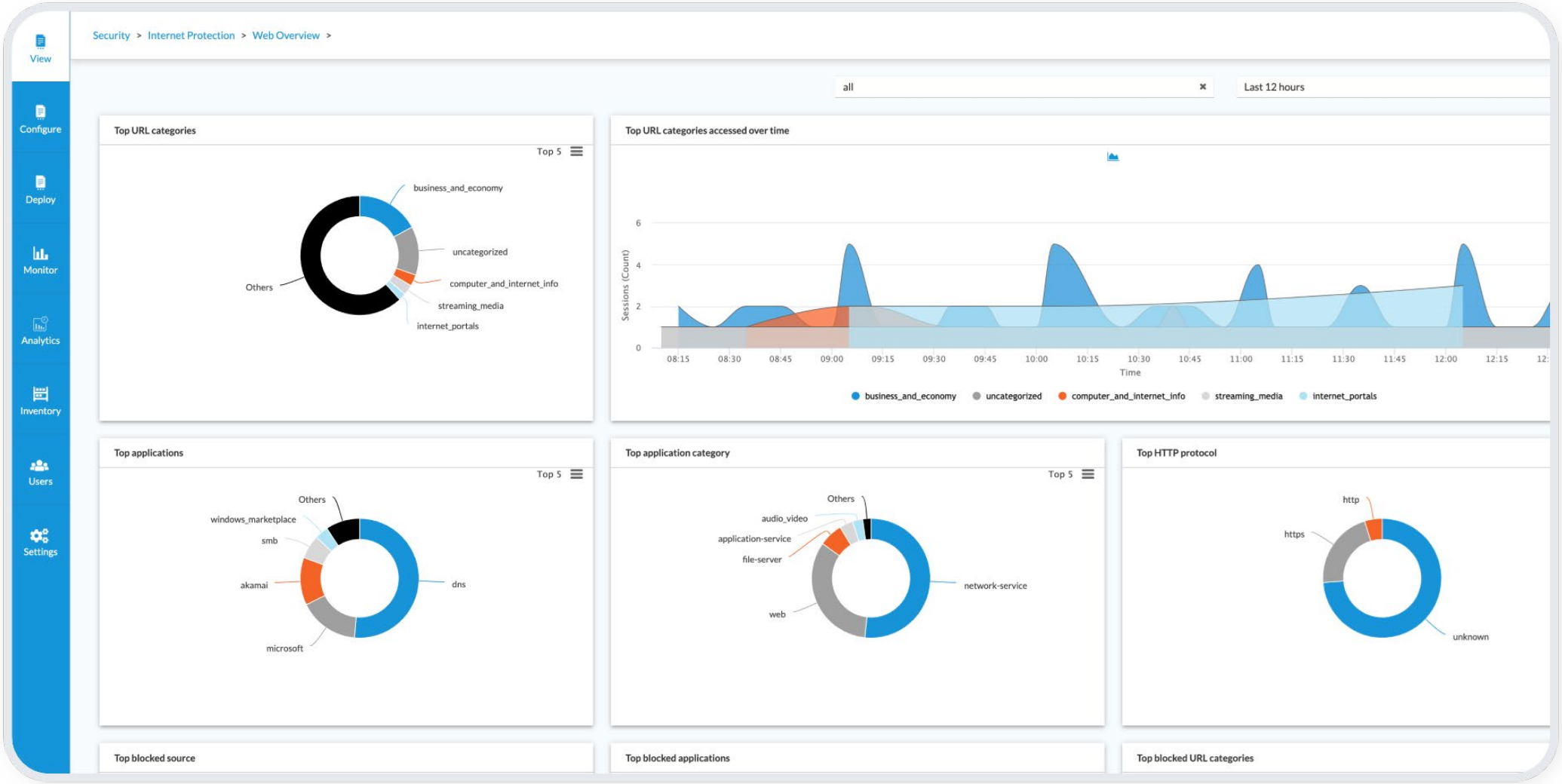

Figure 8

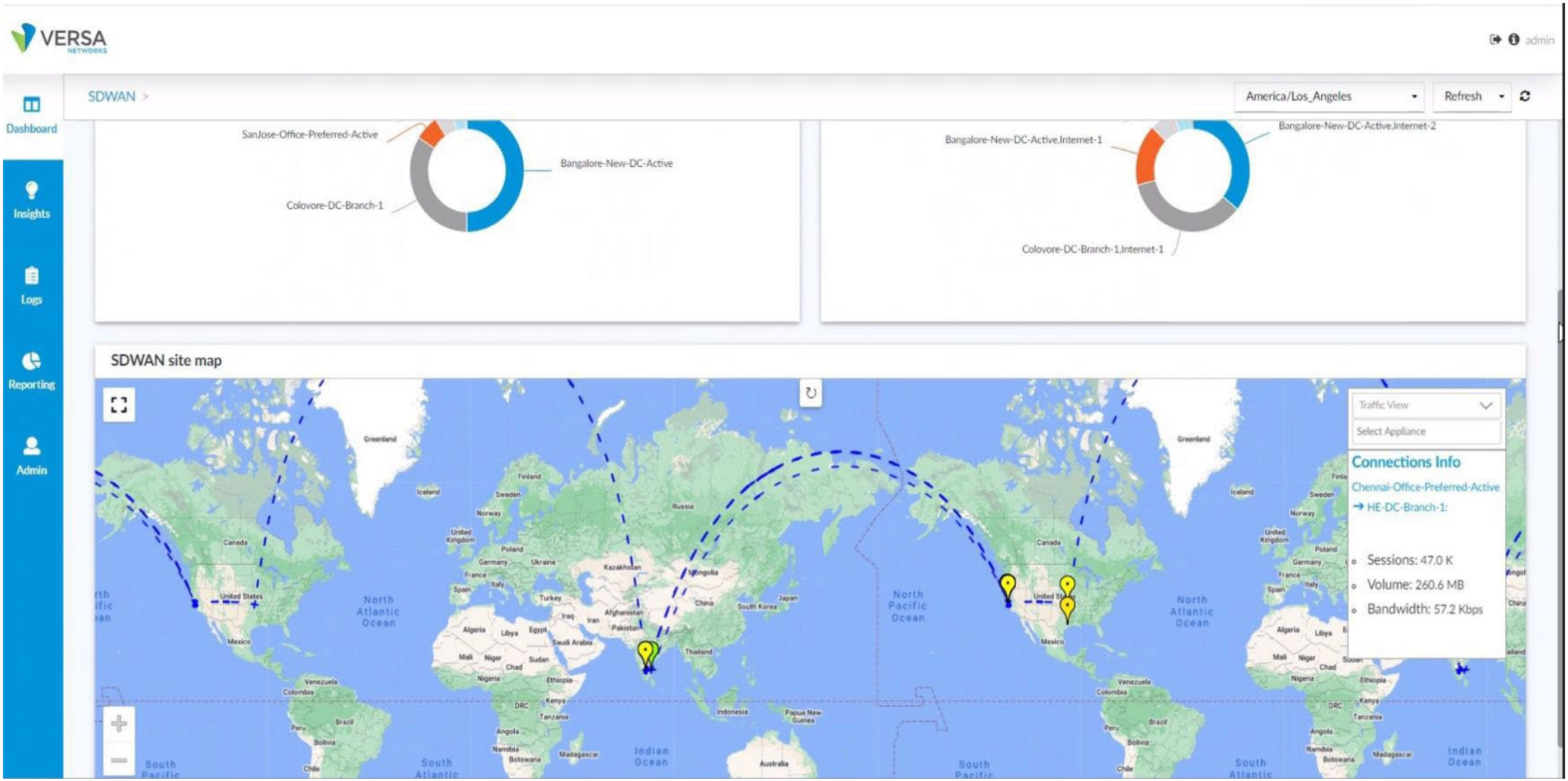

Figure 9

Summary

The Versa SD-WAN, ZTNA and Secure Services Edge solution provides a secure traffic-engineered global SD-WAN and SASE network that offers the best application experience for users and IoT devices, irrespective of their and applications' locations, including under DDIL and adverse conditions. The Versa solution is very well suited for satellite, maritime, and federal networks that leverage NSA High Assurance Internet Protocol Encryption (HAIPE) or Commercial Solutions for Classified (CSfC)-based architectures.

https://versa-networks.com
For more details call, email or visit us.
Our team is here to help.

VERSA NETWORKS

Versa Networks, Inc, 2550 Great America Way, 3rd floor, Suite 350, Santa Clara, CA 95054
+1 408.385.7660 | info@versa-networks.com | www.versa-networks.com