SD-WAN

VERSA NETWORKS SD-WAN

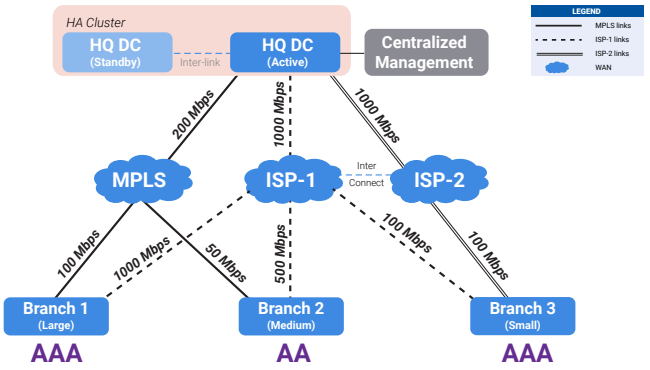
Q4 2020 OVERALL RATING AAA

Overview

Versa Networks offers a flexible, quick, and robust Zero-Touch Provisioning across the use cases we tested. Deployment was easy, and the product included comprehensive documentation. The centralized management covered all common use-cases.

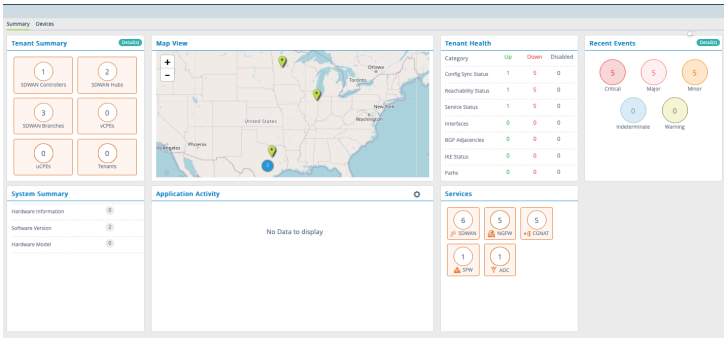
For the two use cases with voice and video (Branches 1 and 2), the quality of experience for voice was excellent (4.41 out of 4.41), and video was extremely good. For video, Branch 1 achieved 4.34 MOS and Branch 2 got 4.27 out of a total of 4.53, respectively.

The Rated (VPN) Throughput was excellent for Branch 1 and Branch 3. For Branch 2 performance was very good.



Summary of Results

MANAGEMENT AA



The centralized management system (CMS) covers all common SD-WAN and Secure SD-WAN use cases. Nevertheless, comprehensive search search and navigation would improve the user experience.

Versa offers options to deploy on-premises, on-cloud dedicated, and on a shared cloud. The management system is accessed through a web browser, and all browsers are supported.

The CMS supports role-based access control (RBAC) as well as comprehensive third-party authentication. It was straightforward to define and save multiple policies, and the CMS offered a wide range of polices, from general system configurations, application-based policies (for security and SD-WAN), and network traffic polices that can be defined to domains, users, specific devices, and IP ranges, etc. Inheritance (nested rules) is fully supported.

Logging is robust, and the use of standardized logging and reporting formats facilitated fast and accurate consumption of data. The system provides built-in reports as well as the ability to generate custom reports for outputs in a range of standard formats.

Quality of Experience	Branch 1	Branch 2	Branch 3
AAA	AAA	AAA	AAA

Versa performed excellent overall for the quality of experience. Voice MOS was excellent; video MOS was extremely good, with only minor degradation observed in a few tests; HTTP Connect times excellent; FTP latency excellent; Emails sent per second excellent. We saw very few spikes in latency during our testing.

Zero-Touch Provisioning	Branch 1	Branch 2	Branch 3
AAA	AAA	AAA	AAA

Versa offered flexible, quick, and robust Zero-Touch Provisioning when tested. The time to create a new configuration was very fast; cloning even faster. Versa also was verified to have persistence of data and AES-256 encryption over VPN tunnels.

WAN Performance	Branch 1	Branch 2	Branch 3
AAA	AAA	A	AAA

The Rated (VPN) Throughput was excellent for Branch 1, with 944 Mbps out of 1,000 Mbps, and for Branch 3, with 200 Mbps out of 200 Mbps. For branch 2, performance was very good with 417 Mbps out of 550 Mbps. When it came to maximum capacity, raw packet processing performance (UDP Throughput), HTTP capacity, and single application flows, Branch 1 and 3 performed as expected. For Branch 2, however, the performance was overall a little lower.

Security Effectiveness	Branch 1	Branch 2	Branch 3
A	A	A	A

Security Effectiveness was very good; Versa blocked 413 out of 481 evasions, 2,162 out of 2,246 exploits, and passed all the stability and reliability tests.

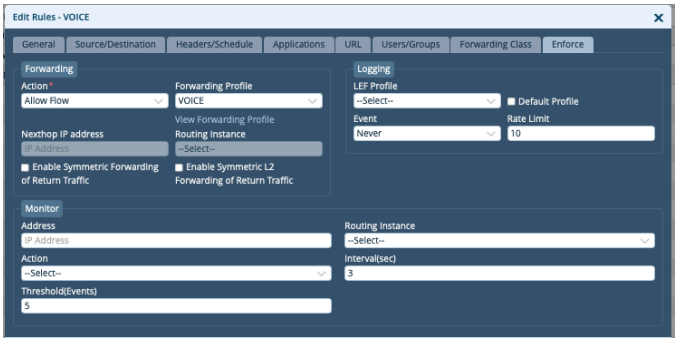
Management & Reporting Capabilities

Authentication

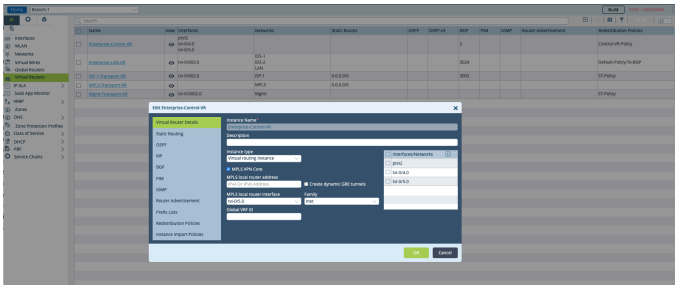
The management console supports four role-based access control (RBAC) methods for the following users: Dashboard Operator, Operator, Security Admin, Super Admin. Additionally, custom roles can be created. The system supports third-party authentication through Active Directory, RADIUS, TACACS+, KERBEROS, and LDAP.

Policy

The management system supports creating and saving multiple policies. Administrators then create multiple groups and apply policies, which are easily configured from the GUI. Once policies have been defined, they can be associated domains, specific sensors, group of sensors, all sensors, individual ports, port groups, etc. Policy diffs are supported natively in the system.



Inheritance (nested rules) is fully supported, including creation of groups and sub-groups, such that sub-groups can inherit certain aspects of configuration and policy definition from parent groups. Policy versioning and rollback are also available.

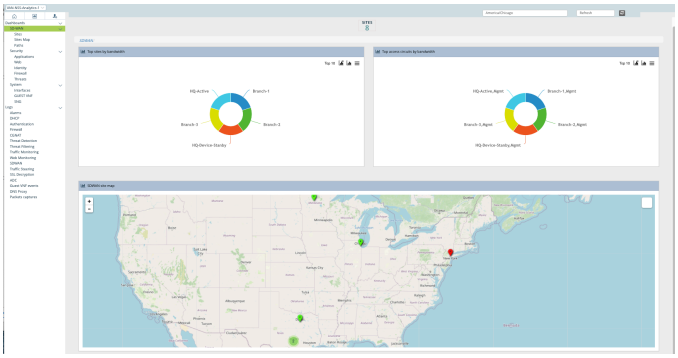


To prevent tampering, the policy and all messages between devices and centralized management carry an integrity check mechanism.

Logging

Logging is very robust and includes everything from policy changed, policy deployed, unsuccessful logins, hardware failure, and malicious traffic, etc. Log file maintenance is included, such as archiving, rotation of log files, restoring from archive, and reporting from archive. Furthermore, Versa offers an extensive integration with third parties for log handling. Logs can be forwarded to any third party in syslog and IPFIX format, but Versa also natively supports Splunk, Q1 Labs, ArcSight, RSA/EMC/, Symantec, LogLogic, and NetIQ.

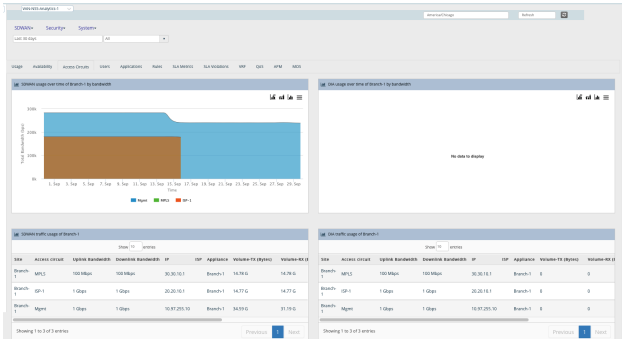
Alert Handling



All alerts are delivered to and handled by a single management console. Alerts can be viewed by selecting a device and viewing alerts specific to that device. The administrator views alerts through various dashboards, which are largely predefined by the system. Administrators are able to group alerts or filter for similar alerts. It is also possible to search for an alert.

Reporting

The system provides summary reporting on all alerts in a single central management console. It provides built-in reports covering typical requirements, such as a list bandwidth used, users, top applications, and SLA violations, and it supports reporting format standards such as syslog, CEF, and IETF.



The system includes a report generator that provides the ability to construct complex data filters and summarize alerts on the specified criteria to customize a report. Reports are exportable as HTML, Excel, CSV, or PDF formats and can be generated on demand, scheduled for delivery, or saved for subsequent use.

Change Control

Change control, rollback, and revision history are available.

Three-Year Total Cost of Ownership

Expected Costs	HQ (Versa Secure Access 1800)	Branch 1 (Versa Secure Access 1800)	Branch 2 (Versa Secure Access 240	Branch 3 (Versa Secure Access 220)	Centralized Management	Total Cost (All Products)
Installation Hours	8	8	8	8	Cloud based	
Initial Purchase Price	$7,500	$7,500	$1,335	$675	Bundled in the unit price	$17,010
Annual Cost of Support/Maintenance	$1,696	$1,696	$984	$379	N/A	$4,755
Other Annual Cost (AV, IPS, Cloud, etc.)	$0	$0	$0	$0	N/A	$0
Three-Year Total Cost of Ownership	$12,588	$12,588	$4,287	$1,811	N/A	$31,274
Total Cost Year 1	$9,196	$9,196	$2,319	$1,054	N/A	$21,765
Total Cost Year 2	$1,696	$1,696	$984	$379	N/A	$4,755
Total Cost Year 3	$1,696	$1,696	$984	$379	N/A	$4,755

Figure 1 – Three-Year TCO for Secure SD-WAN

Expected Costs	HQ (Versa Secure Access 1800)	Branch 1 (Versa Secure Access 1800)	Branch 2 (Versa Secure Access 240)	Branch 3 (Versa Secure Access 220)	Centralized Management	Total Cost (All Products)
Installation Hours	8	8	8	8	Cloud based	
Initial Purchase Price	$7,500	$7,500	$1,335	$675	Bundled in the unit price	$17,010
Annual Cost of Support/Maintenance	$1,289	$1,289	$747	$286	N/A	$3,611
Other Annual Cost (AV, IPS, Cloud, etc.)	$0	$0	$0	$0	N/A	$0
Three-Year Total Cost of Ownership	$11,367	$11,367	$3,576	$1,532	N/A	$27,842
Total Cost Year 1	$8,789	$8,789	$2,082	$961	N/A	$20,621
Total Cost Year 2	$1,289	$1,289	$747	$286	N/A	$3,611
Total Cost Year 3	$1,289	$1,289	$747	$286	N/A	$3,611

Figure 2 – Three-Year TCO for SD-WAN

In deploying an SD-WAN for the first time, some tuning and configuration is needed. Our engineers have captured this time using either local device management or cloud deployment options. The table accurately reflects the amount of time that our engineers, with the help of Versa engineers, needed to install and configure the SD-WAN to the point where it operated successfully in the test harness, passed legitimate traffic, and blocked and detected prohibited or malicious traffic. This closely mimics a typical enterprise deployment scenario for the tested SD-WAN configuration.

Calculations are based on vendor-provided pricing information. Where possible, the 24/7 maintenance and support option with 24-hour replacement is utilized, because this is the option typically selected by enterprise customers. Prices are for SD-WAN management and maintenance only; costs for central management solutions (CMS) may be extra.

- **Year 1 Cost** is calculated by adding installation costs (US$75 per hour fully loaded labor x installation time) + purchase price + first-year maintenance/support fees.
- **Year 2 Cost** consists only of maintenance/support fees.
- **Year 3 Cost** consists only of maintenance/support fees.

Test Environment

We developed a multi-test environment that includes a redundant HA cluster at the HQ DC location and three disparate branches representing large, medium, and small enterprises. The WAN environment is provisioned similar to those typically encountered over WAN link states. For example, the site locations are considered to be at a distance of ~1000 miles from the Headquarters (HQ DC), e.g., Denver (Colorado, USA) is HQ DC; San Francisco (California, USA) is Branch 1; Chicago (Illinois, USA) is Branch 2; Galveston (Texas, USA) is Branch 3. The test harness baseline is recorded to ensure consistent behavior, the vendor solution is deployed, and each test case is measured against the baseline. Note that ISP links had a latency of 30 milliseconds to simulate real-world impairments. For more details, please see the SD-WAN Test Methodology.

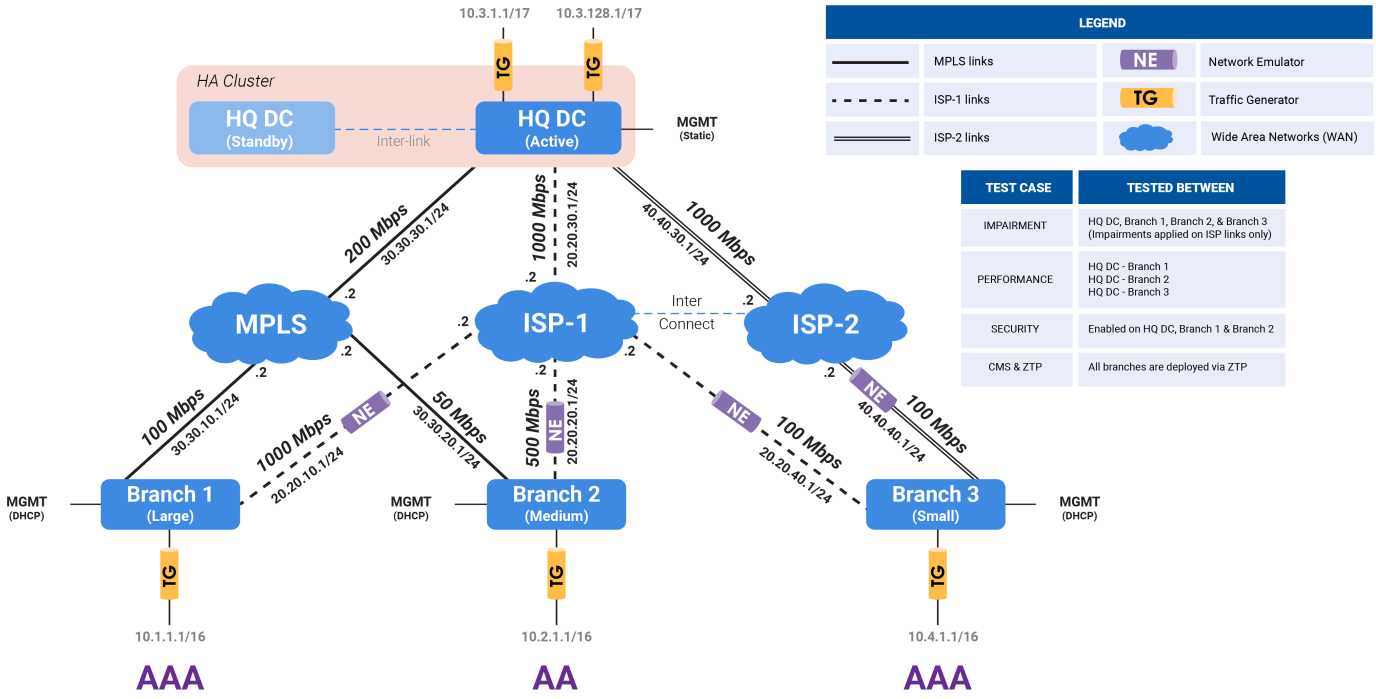


Figure 3 – Test Environment

Test Equipment

- TeraPackets (https://www.terapackets.com) - A special thank you for the tool and support.
- Ixia PerfectStorm One (IxLoad v9.0, Breaking Point v9.0)
- Network Emulator II (Network Emulator v3.2.0)
- Juniper EX-2000 (Switch and Routers)
- Packetator
- 64-bit Kali Linux 2018.4
- Microsoft Internet Explorer 11.0.9600.17843
- Mozilla Firefox 50.0.1
- 64-bit CentOS 6.5 with Bash 4.1.2(1), Apache 2.2.15, Postfix 2.6.6, Procmail 3.22
- 64-bit Ubuntu 18.04 LTS with Apache 2.4.29, Drupal 8.5.0, OpenSMTPD 6.6.1p1

Tested Products

- Versa Secure Access 1800 v.20.2.1 (GA) – HQ DC (2 devices)
- Versa Secure Access 1800 v.20.2.1 (GA) – Branch 1
- Versa Secure Access 240 v.20.2.1 (GA) – Branch 2
- Versa Secure Access 220 v.20.2.1 (GA) – Branch 3

Appendix

CyberRatings Classification Matrix	
RATING	DEFINITION
AAA	A product rated 'AAA' has the highest rating assigned by CyberRatings. The product's capacity to meet its commitments to consumers is extremely strong.
AA	A product rated 'AA' differs from the highest-rated products only to a small degree. The product's capacity to meet its commitments to consumers is very strong.
A	A product rated 'A' is somewhat less capable than higher-rated categories. However, the product's capacity to meet its commitments to consumers is still strong.
BBB	A product rated 'BBB' exhibits adequate stability and reliability. However, previously unseen events and use cases are more likely to negatively impact the product's capacity to meet its commitments to consumers.
	A product rated 'BB,' 'B,' 'CCC,' 'CC,' and 'C' is regarded as having significant risk characteristics. 'BB' indicates the least degree of risk and 'C' the highest. While such products will likely have some specialized capability and features, these may be outweighed by large uncertainties or major exposure to adverse conditions.
BB	A product rated 'BB' is more susceptible to failures than products that have received higher ratings. The product has the capacity to meet its commitments to consumers. However, it faces minor technical limitations that have a potential to be exposed to risks.
B	A product rated 'B' is more susceptible to failures than products rated 'BB'; however, it has the minimum capacity. Adverse conditions will likely expose the product's technical limitations that lead to an inability to meet its commitments to consumers.
CCC	A product rated 'CCC' is susceptible to failures and is dependent upon favorable conditions to perform expected functions. In the event of adverse conditions, the product is not likely to have the capacity to meet its commitments to consumers.
CC	A product rated 'CC' is highly susceptible to failures. The 'CC' rating is used when a failure has not yet occurred, but CyberRatings considers it a virtual certainty.
C	A product rated 'C' is highly susceptible to failures. The product is expected to fail under any abnormal operating conditions and does not offer a useful management systems and logging information compared with products that are rated higher.
D	A product rated 'D' is actively underperforming and failing and does not meet the use-case. The 'D' rating is used when the product is not operational without a major technical overhaul. Unless CyberRatings believes that such technical fixes will be made within a stated grace period (typically 30-90 calendar days), the 'D' rating also is an indicator that existing customers using the product have already experienced a failure and should take immediate action.

Authors

Ahmed Basheer, Thomas Skybakmoen, Vikram Phatak

Contact Information

CyberRatings.org
2303 Ranch Road 620 South
Suite 160, #501
Austin, TX 78734

info@cyberratings.org
www.cyberratings.org