National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Versa Networks Versa Secure SD-WAN
Versa Operating System (VOS) 22.1 running on Versa CSG1500, CSG2500, CSG3500, CSG5000, Dell PowerEdge R7515, and Dell VEP4600, Versa Director 22.1 and Versa Analytics 22.1

Report Number:	**CCEVS-VR-VID11431-2024**
Dated:	**April 10, 2024**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers
Meredith Martinez
Elizabeth Scruggs
The Aerospace Corporation

Common Criteria Testing Laboratory

John Messiha
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary ... 1
2 Identification ... 2
3 Architectural Information ... 3
3.1 TOE Description ... 3
3.2 TOE Evaluated Platforms ... 3
3.3 TOE Architecture ... 4
3.4 Physical Boundaries ... 5
4 Security Policy ... 5
4.1 Security audit ... 6
4.2 Communications ... 6
4.3 Cryptographic support ... 6
4.4 User data protection ... 6
4.5 Firewall ... 6
4.6 Identification and authentication ... 7
4.7 Security management ... 7
4.8 Packet filtering ... 7
4.9 Protection of the TSF ... 7
4.10 TOE access ... 8
4.11 Trusted path/channels ... 8
4.12 Intrusion Prevention ... 8
5 Assumptions & Clarification of Scope ... 8
6 Excluded Functionality ... 9
7 Documentation ... 10
8 IT Product Testing ... 10
8.1 Developer Testing ... 10
8.2 Evaluation Team Independent Testing ... 10
9 Evaluated Configuration ... 11
10 Results of the Evaluation ... 12
10.1 Evaluation of the Security Target (ASE) ... 12
10.2 Evaluation of the Development (ADV) ... 13
10.3 Evaluation of the Guidance Documents (AGD) ... 13
10.4 Evaluation of the Life Cycle Support Activities (ALC) ... 13
10.5 Evaluation of the Test Documentation and the Test Activity (ATE) ... 14
10.6 Vulnerability Assessment Activity (VAN) ... 14
10.7 Summary of Evaluation Results ... 15
11 Validator Comments/Recommendations ... 15
12 Annexes ... 15
13 Security Target ... 15
14 Glossary ... 15
15 Bibliography ... 16

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Versa Networks Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on Versa CSG1500, CSG2500, CSG3500, CSG5000, Dell PowerEdge R7515, and Dell VEP4600, Versa Director 22.1 and Versa Analytics 22.1 solution provided by Versa Networks, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in April 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the PP-Configuration for Network Devices, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways, Version 1.2, 18 August 2023 (CFG_NDcPP-IPS-FW-VPNGW_v1.2) which includes the Base PP: collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e) with the PP-Module for Intrusion Prevention Systems (IPS), 1.0, 11 May 2021 (IPS10), the PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e), and the PP-Module for VPN Gateways, Version 1.3, 25 August 2023 (VPNGW13).

The Target of Evaluation (TOE) is the Versa Networks Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on Versa CSG1500, CSG2500, CSG3500, CSG5000, Dell PowerEdge R7515, and Dell VEP4600, Versa Director 22.1 and Versa Analytics 22.1.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory’s findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Versa Networks Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on CSG1500, CSG2500, CSG3500, CSG5000, Dell PowerEdge R7515, and Dell VEP4600, Versa Director 22.1, and Versa Analytics 22.1 Security Target, Version 1.9, March 28, 2024 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product’s evaluation. Upon successful completion of the evaluation, the product is added to NIAP’s Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Versa Networks Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on Versa CSG1500, CSG2500, CSG3500, CSG5000, Dell PowerEdge R7515, and Dell VEP4600, Versa Director 22.1 and Versa Analytics 22.1 (Specific models identified in Section 9)
Protection Profile	PP-Configuration for Network Devices, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways, Version 1.2, 18 August 2023 (CFG_NDcPP-IPS-FW-VPNGW_v1.2) which includes the Base PP: collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e) with the PP-Module for Intrusion Prevention Systems (IPS), 1.0, 11 May 2021 (IPS10), the PP-Module for Stateful Traffic Filter Firewalls,

Item	Identifier
	Version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e), and the PP-Module for VPN Gateways, Version 1.3, 25 August 2023 (VPNGW13)
ST	Versa Networks Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on CSG1500, CSG2500, CSG3500, CSG5000, Dell PowerEdge R7515, and Dell VEP4600, Versa Director 22.1, and Versa Analytics 22.1 Security Target, Version 1.9, March 28, 2024
Evaluation Technical Report	Evaluation Technical Report for Versa Networks Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on Versa CSG1500, CSG2500, CSG3500, CSG5000, Dell PowerEdge R7515, and Dell VEP4600, Versa Director 22.1 and Versa Analytics 22.1 , Version 0.2, March 28, 2024
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Versa Networks, Inc.
Developer	Versa Networks, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Jerome Myers, Meredith Martinez, Elizabeth Scruggs – The Aerospace Corporation

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The TOE is comprised of hardware and software and is defined as a distributed TOE comprising management, or “headend” components (Versa Director, Analytics, and VOS device configured an SD-WAN controller) and one or many VOS devices operating as data plane or “Branch” devices. The TOE is a network device with stateful firewall, IDS/IPS, and VPN gateway capabilities.

3.1 TOE Description

The TOE is a multitenant software platform that delivers software-defined Layer 3 to Layer 7 services with full programmability and automation. The TOE software platform addresses SD-WAN, SD-Security, and SD-Branch use cases for the WAN edge, delivering multiple functions in a single, unified software platform.

3.2 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 9 below.

3.3 TOE Architecture

The solution consists of the following components:

- Versa Operating System^{TM} (VOS^{TM}) device—A VOS device is the multiservice networking and security software platform that provides routing, advanced SD-WAN, and SD-Security in a single software package. A VOS device is deployed in the branch, hub, cloud, and data center.
- Versa Director—Versa Director is a centralized provisioning and management application that allows you to configure, deploy, manage, and orchestrate all your Versa VOS software instances. Versa Director integrates with third-party operations and business systems and with cloud management systems by using open and widely available protocols and API formats.
- Versa Analytics—Versa Analytics is a near real-time analytics engine that provides historical insights into contextual policy-to-event correlation and visibility based on application, user, device, and location.

VOS devices, Versa Director, and Versa Analytics can be deployed on Versa appliances—Cloud Services Gateways[1] (CSGs)—and on Versa-certified x86 third-party white box appliances; in private clouds on hypervisors (KVM and ESXi), and in public clouds (AWS, Azure, Google Cloud Platform[2]).

VOS software consists of a multitenant, single software stack that natively runs multiple services, such as routing, security, and other network-based functions. These services can be combined into logical service node groups (SNGs), which can be chained together to deliver multiple services in a single path. The same software provides the data and control plane functionality (SD-WAN Controller).

You configure and manage VOS instances through the Versa provisioning and management platform, Versa Director. VOS devices also generate a variety of audit logs and exports them to Versa Analytics.

VOS devices provide fully integrated Layer 4 through Layer 7 functions in platform-based software packages, including OVA, QCOW2, and ISO. VOS devices can be configured to be a data plane element (SD-Router; SD-WAN; or Secure SD-WAN at a branch, hub, or gateway) or a control plane element (SD-WAN Controller). VOS software provides a comprehensive set of built-in services for SD-WAN, basic networking and routing, security (IPS, Stateful Firewall, NGFW), and VPNs.

Versa Director is a provisioning and management platform that performs the following functions:

- Centralized single-pane-of-glass configuration, management, and monitoring of the controllers, branch sites, and hub sites
- Lifecycle management of Versa VOS instances

[1] «Cloud» is a marketing term only. The NIAP evaluation includes on-premise installations only.
[2] Deployment in cloud environments is not evaluated.

- System-level high availability (HA) deployed as an active-standby pair for redundancy
- Staging server during the bootstrapping process
- Virtual network function manager (VNFM)
- Zero-touch provisioning (ZTP) of VOS devices at branch and hub sites

Versa Analytics is an analytics platform that is purpose-built for VOS devices and managed services. Versa Analytics provides visibility into VOS devices. You can use the analyzed data to perform baselining, correlation, and prediction about the VOS devices. Versa Analytics provides real-time and historical data, and you can create reports about usage patterns, trends, security events, and alerts. Versa Director also provides role-based access to Versa Analytics.

Branch Versa VOS instances continually provide to Versa Analytics status and quantitative information about their links, network paths, and services. Additionally, every service running on a VOS instance, such as NGFW and URL filtering, generates flow-level and aggregate log messages that are sent to Versa Analytics. Using this information, Versa Analytics performs a number of functions, including networkwide analysis and optimization, troubleshooting, trending, capacity planning, dynamic application-based traffic steering, and security forensics. Versa Analytics passes the results of its analyses to Versa Director.

3.4 Physical Boundaries

On headend components (Director, Analytics, SD-WAN Controller), the boundary surrounds the entire VM image but excludes the hypervisor and underlying hardware. The VOS Branch device encompasses the VOS system image and the underlying hardware when deployed as bare metal, and only the VM image, excluding the hypervisor and hardware, when deployed as virtual.

4 Security Policy

This section summarizes the security functionality of the TOE:

1. Security audit
2. Communications
3. Cryptographic support
4. User data protection
5. Firewall
6. Identification and authentication
7. Security management
8. Packet filtering
9. Protection of the TSF
10. TOE access
11. Trusted path/channels
12. Intrusion Prevention

4.1 Security audit

The TOE provides extensive auditing capabilities by generating an audit record for each auditable event, thus generating a comprehensive set audit logs that identify specific TOE operations including audit records for security relevant events.

The TOE can audit events related to identification and authentication, administrative actions, and activities related to security functionality enforcement.

For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event.

Audit logs are buffered locally on each component and then forwarded to Analytics for storage and analysis. Logs are also sent to an external syslog server over a protected IPsec channel.

4.2 Communications

The TOE is a distributed TOE which uses IPsec for securing all internal communications. The TOE does not use a registration channel and satisfies all requirements of FTP_ITC.1 for internal trusted channels. Administrators must manually enable each component before joining the distributed TOE.

4.3 Cryptographic support

The TOE provides cryptography in support of secure connections, using IPsec for data plane encryption and IPsec, TLS, SSH, and HTTPS for control plane encryption.

The TOE provides key generation, key destruction and cryptographic operation functions supported by NIST approved cryptographic algorithms validated under the CAVP.

4.4 User data protection

The TOE ensures residual information is not leaked into subsequent packets by freeing the contents of packet buffers prior to de-allocation.

4.5 Firewall

The TOE implements a stateful firewall with support for rules covering IPv4, IPv6, TCP, UDP, and ICMP with optional logging on match, in addition to a baseline of default processing rules which ensure that the firewall properly rejects malformed packets or other anomalies.

The TOE also supports processing of dynamic protocols where control and data are processed on separate ports.

4.6 Identification and authentication

All TOE administrative users must be identified and authenticated. Administration may either be performed locally using the local console CLI or remotely using the web-based GUI or SSH CLI.

The TOE provides two pre-configured administrative accounts. The TOE requires that users associated with these accounts be identified and authenticated before permitted access to the TOE and TOE security functions. Users may authenticate using local password authentication. The TOE ensures that a minimum password length is supported in addition to the construction of complex user passwords. Failed authentication attempts will be tracked and eventually cause the administrator to be locked out until another administrator manually unlocks the account or after a defined time period elapses.

Pre-shared keys are supported for IPsec connections which may be generated externally or composed from a password.

X.509 certificates are used in support of IPsec connections (during IKE negotiations).

4.7 Security management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either via a local console connection, or through a secure SSH or HTTPS session.

The TOE provides the ability to manage all TOE administrators, all identification and authentication, all audit functionality of the TOE, all TOE cryptographic functionality, firewall, IDS/IPS, and VPN gateway functions.

TOE administrators of different roles have different privileges, and the TOE supports pre-defined administrator roles. By default, the system supports the following administrator roles, which cannot be deleted or edited: Admin and Operator, (non-admin users will not have access to the TOE). Admin has super-user privileges and can perform all operations on the TOE. Operator can perform operations like monitor, check-status, and review configuration.

4.8 Packet filtering

The TOE supports a packet filtering policy as described in Firewall above.

4.9 Protection of the TSF

The TOE internally maintains the date and time. This date and time are used as the timestamp that is applied to audit records generated by the TOE. Administrators can synchronize the system time with the NTP server time via NTP protocol.

Additionally, the TOE performs testing of all TSF binaries, cryptographic algorithms, and entropy sources to ensure correct operation. The TOE will shutdown its interfaces in the event of a self-test failure to prevent insecure operation.

The TOE will accept software upgrades that have been digitally signed or have been manually verified by the administrator using a hash prior to installation.

The TOE protects the storage of private keys, passwords and other sensitive data by restricting file permissions and does not provide any interface which allows exposure of sensitive plaintext data.

4.10 TOE access

When an administrative session is initially established, the TOE displays an administrator configurable warning banner. This is used to provide any information deemed necessary by the administrator.

After a configurable period of inactivity, local and remote administrative sessions will be terminated, requiring administrators to re-authenticate. Administrators may also manually terminate their own sessions.

The VPN gateway will provide dynamically assigned IP addresses to endpoints, and terminate inactive VPN sessions after inactivity. Connections may be restricted based on security posture, location, and time of day.

4.11 Trusted path/channels

The TOE supports establishing trusted paths between itself and remote administrators using SSH for CLI access and HTTPS for GUI access. The TOE supports use of IPsec and HTTPS/TLS for control plane connections, and IPsec for data plane connections (including distributed TOE channels between VOS Branches and the Versa Headend). The TOE supports IPsec to encrypt connections with external NTP servers and syslog servers.

4.12 Intrusion Prevention

The TOE supports both in-line and promiscuous inspection modes using both anomaly and signature-based detection along with IP filtering based on blacklists.

5 Assumptions & Clarification of Scope

Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e)

- PP-Module for Intrusion Prevention Systems (IPS), 1.0, 11 May 2021 (IPS10)
- PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e)
- PP-Module for VPN Gateways, Version 1.3, 25 August 2023 (VPNGW13)

That information has not been reproduced here and the NDcPP22e/IPS10/STFFW14e/ VPNGW13 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e/IPS10/STFFW14e/VPNGW13 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

Clarification of scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the collaborative Protection Profile for Network Devices and the Intrusion Prevention, Firewalls, and VPN Gateways Modules and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Network Devices, Firewall, IDS/IPS, VPN Gateway models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP22e/IPS10/STFFW14e/VPNGW13 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation, including the functionality listed in Section 6.

6 Excluded Functionality

The following features and functionality are excluded from this evaluation:

- Deployment in a cloud environment

- SSL/TLS Inspection
- Anti-virus
- Service Chaining
- Full Multi-Tenancy
- Context-Aware Policy
- External authentication using LDAP, RADIUS, TACACS+, or SAML
- High availability
- Wireless networking interfaces (WLAN, 3G, 4G, LTE, 5G)

7 Documentation

The following documents were available with the TOE for evaluation:

- Configure for NIAP Common Criteria, Version 1.0, March 29, 2024

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report for Versa Networks Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on Versa CSG1500, CSG2500, CSG3500, CSG5000, Dell PowerEdge R7515, and Dell VEP4600, Versa Director 22.1 and Versa Analytics 22.1, Version 0.2, March 28, 2024 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

8.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP22e/IPS10/STFFW14e/VPNGW13 including the tests associated with optional requirements. The AAR, in section 3.4.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

9 Evaluated Configuration

The evaluation configuration consists of the following components:

- Versa Operating System^{TM} (VOS^{TM}) device—A VOS device is the multiservice networking and security software platform that provides routing, advanced SD-WAN, and SD-Security in a single software package. A VOS device is deployed in the branch, hub, cloud, and data center.
- Versa Director—Versa Director is a centralized provisioning and management application that allows you to configure, deploy, manage, and orchestrate all your Versa VOS software instances. Versa Director integrates with third-party operations and business systems and with cloud management systems by using open and widely available protocols and API formats.
- Versa Analytics—Versa Analytics is a near real-time analytics engine that provides historical insights into contextual policy-to-event correlation and visibility based on application, user, device, and location.

TOE Model	Specifications
CSG1500	**CPU:** Intel Xeon D2177NT **Memory:** 64GB **Disk:** 16GB + 256GB SSD **Management port:** 1-Gigabit Ethernet **Data ports:** 6x SFP+ 10GE, 10x RJ-45 1GE **Console port:** RJ-45 serial
CSG2500	**CPU:** Intel Xeon Gold 6252N **Memory:** 96GB **Disk:** 1TB SSD **Management port:** 2x 1-Gigabit Ethernet **Data ports:** 8x SFP+ 10GE, 8x RJ-45 1GE **Console port:** RJ-45 serial
CSG3500	**CPU:** Intel Xeon D2177NT **Memory:** 32GB **Disk:** 16GB + 256GB SSD **Management port:** 1-Gigabit Ethernet **Data ports:** 2x SFP+ 10GE, 4x SFP+ 25G, 16x RJ-45 2.5G, 8x RJ-45 10G, 10GE, 2x QSFP28 100GE, 2x RJ-45 10GE **Console port:** RJ-45 serial

TOE Model	Specifications
CSG5000	**CPU:** AMD EPYC 7713P **Memory:** 256GB **Disk:** 1TB SSD **Management port:** 2x 1-Gigabit Ethernet **Data ports:** 16x SFP+ 10GE, 4x QSFP 100GE **Console port:** RJ-45 serial
Dell PowerEdge R7515	**CPU:** AMD EPYC 7773X **Memory:** 256GB **Disk:** 1TB SSD **Management port:** 2x 1-Gigabit Ethernet **Data ports:** 4x SFP+ 10GE, 4x QSFP 100GE **Console port:** RJ-45 serial
Dell VEP4600	**CPU:** Intel Xeon-D 2187NT **Memory:** 64GB **Disk:** 960GB SSD **Management port:** 2x 1-Gigabit Ethernet **Data ports:** 6x SFP+ 10GE, 4x 1GE **Console port:** RJ-45 serial

10 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on Versa CSG1500, CSG2500, CSG3500, CSG5000, Dell PowerEdge R7515, and Dell VEP4600, Versa Director 22.1 and Versa Analytics 22.1 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/IPS10/STFFW14e/VPNGW13.

10.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Versa Networks Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on Versa CSG1500, CSG2500, CSG3500, CSG5000, Dell PowerEdge R7515, and Dell VEP4600, Versa Director 22.1 and Versa

Analytics 22.1 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the NDcPP22e/IPS10/STFFW14e/VPNGW13 related to the examination of the information contained in the TSS.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDcPP22e/IPS10/STFFW14e/VPNGW13 and recorded the results in a Test Report, summarized in the AAR.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

On 3/28/24, The evaluator searched the following public vulnerability databases:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search)
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/)
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities)
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories)
- Exploit / Vulnerability Search Engine (http://www.exploitsearch.net)
- SecurITeam Exploit Search (http://www.securiteam.com)
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search)
- Offensive Security Exploit Database (https://www.exploit-db.com/)

with the following search terms: “Versa”, “Versa Networks”, “Versa Director 22.1”, “Versa Operating System 22.1”, “VOS 22.1”, “Versa SD-WAN Controller 22.1”, “Versa SD-WAN Branch 22.1”, “Versa Analytics 22.1”, “Versa CSG”, “Ubuntu 18.0.4.6 LTS”, “Bouncy Castle FIPS Java API 1.0.2.3”, “Bouncy Castle 1.0.2.3”, “Rambus Quicksec 6.1”, “Quicksec 6.1”, “OpenSSL 1.1.1-1ubuntu2.1~18.04.23”, “OpenSSL 1.1.1-1ubuntu2.1”, “OpenSSH 8.4p1-2”, “Linux kernel 5.4.0”, “Linux kernel 4.15.0-1117-fips”, “Linux kernel 4.15.0”, “Tomcat 9.0.82”, “rsyslog 8.32.0-1ubuntu4.2”, “rsyslog 8.32.0”, “ntp 1:4.2.8p10+dfsg-5ubuntu7.3+esm1”, “ntp 1:4.2.8p10”, “Intel Xeon”, “Intel Xeon CPU E5-2683 v4”, “Intel Xeon D-2187NT”, “Intel Xeon Gold 6252N”, “AMD EPYC 7713P”, “AMD EPYC”, “VMware ESXi 7.0U2”, “ESXi 7.0U2”, “Dell VEP 4600”, “Dell Poweredge R7515”, “MetaSwitch”, “Intel DPDK 16.04TCPTCP”.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

11 Validator Comments/Recommendations

All validator comments are addressed in other sections of this validation report.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Versa Networks Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on CSG1500, CSG2500, CSG3500, CSG5000, Dell PowerEdge R7515, and Dell VEP4600, Versa Director 22.1, and Versa Analytics 22.1 Security Target, Version 1.9, March 28, 2024.*

14 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.

- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

15 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e).

[5] PP-Module for Intrusion Prevention Systems (IPS), 1.0, 11 May 2021 (IPS10).

[6] PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e).

[7] PP-Module for VPN Gateways, Version 1.3, 25 August 2023 (VPNGW13).

[8] Versa Networks Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on CSG1500, CSG2500, CSG3500, CSG5000, Dell PowerEdge R7515, and Dell VEP4600, Versa Director 22.1, and Versa Analytics 22.1 Security Target, Version 1.9, March 28, 2024 (ST).

[9] Assurance Activity Report for Versa Networks Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on Versa CSG1500, CSG2500, CSG3500, CSG5000, Dell PowerEdge R7515, and Dell VEP4600, Versa Director 22.1 and Versa Analytics 22.1, Version 0.2, March 28, 2024 (AAR).

[10] Detailed Test Report for Versa Networks Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on Versa CSG1500, CSG2500, CSG3500, CSG5000, Dell PowerEdge R7515, and Dell VEP4600, Versa Director 22.1 and Versa Analytics 22.1, Version 0.2, March 28, 2024 (DTR).

[11] Evaluation Technical Report for Versa Networks Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on Versa CSG1500, CSG2500, CSG3500, CSG5000, Dell PowerEdge R7515, and Dell VEP4600, Versa Director 22.1 and Versa Analytics 22.1, Version 0.2, March 28, 2024 (ETR).