Agenzia per la Cybersicurezza Nazionale

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 12/23

(Certificate No.)

Prodotto: *(Product)* **Versa Operating System (VOS) 21.2.3 with OS SPACK 20230511 running on Versa Cloud Services Gateways**

Sviluppato da: *(Developed By)* **Versa Networks Inc.**

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL4+
(ALC_FLR.1)

p. il Direttore Generale
dell'ACN

Il Capo Servizio
Certificazione e Vigilanza
(Andrea Billet)

[ORIGINAL SIGNED]

Roma, 14 novembre 2023

Common Criteria

SOGIS IT SECURITY CERTIFIED

This page is left intentionally blank

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Versa Operating System (VOS) 21.2.3 with OS SPACK 20230511 running on Versa Cloud Services Gateways

Version 1.0

14 November 2023

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First draft issue	14/11/2023

2 Table of contents

3 Acronyms

3.1 National scheme

DPCM	Decreto del Presidente del Consiglio dei Ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Agreement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other acronyms

AAA	Autentication Authorization and Accounting
CLI	Command Line Interface
CSG	Cloud Secure Gateway

FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GUI	Graphic User Interface
HTTP	HyperText Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
IT	Information Technology
KVM	Kernel based Virtual Machine
MD	Message Digest
NIC	Network Interface Card
OS	Operating System
RAM	Read Only memory
SD-WAN	Software-Defined Wide Area Network
SSH	Secure Shell
SSL	Secure Socket Layer
VM	Virtual Machine
VOS	Versa Operating System

4 References

4.1 Normative references and national Scheme documents

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 agosto 2023

[SOGIS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3, January 2010

4.2 Technical documents

[CCECG] Versa Operating System (VOS) 21.2.3 with OS SPACK 20230511 running on Versa Cloud Service Gateways Common Criteria Guidance Document, version 1.7 August 16th 2023

[ETR] "Versa Operating System (VOS) 21.2.3 with OS SPACK 20230511 running on Versa Cloud Services Gateways "Evaluation Technical Report, Version 3, CCLab Software laboratory (Budapest Site), September 13th 2023

[ST] Versa Operating System (VOS) 21.2.3 with OS SPACK 20230511 running on Versa Cloud Services Gateways Security Target, Versa Networks, version 1.8, August 11th , 2023

5 Recognition of the certificate

5.1 European recognition of CC certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT -Products. A higher recognition level for evaluations beyond EAL4 is provided for IT -Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under SOGIS-MRA for all declared assurance components.

5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] was ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all declared assurance components.

6 Statement of Certification

The Target of Evaluation (TOE) is the product "Versa Operating System (VOS) 21.2.3 with OS SPACK 20230511 running on Versa Cloud Services Gateways", developed by Versa Networks Inc.

The TOE is a multi-service, multi-tenant software platform built from the ground up on cloud principles to deliver scale, segmentation, programmability, and automation. It provides networking, SD-WAN and a full suite of security functions in a single software stack along with service chaining capabilities.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body "Organismo di Certificazione della Sicurezza Informatica (OCSI)", established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC version 3.1 for the assurance components, according to the information provided in the Security Target [ST] and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product "Versa Operating System (VOS) 21.2.3 with OS SPACK 20230511 running on Versa Cloud Services Gateways (CSG)" to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should also review the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Versa Operating System (VOS) 21.2.3 with OS SPACK 20230511 running on Versa Cloud Services Gateways
Security Target	Versa Operating System (VOS) 21.2.3 with OS SPACK 20230511 running on Versa Cloud Services Gateways Security Target, Version 1.8, August 11th, 2023 [ST]
Evaluation Assurance Level	EAL4 augmented with ALC_FLR.1
Developer	Versa Networks, Inc.
Sponsor	Versa Networks, Inc.
LVS	CCLab Software Laboratory (Budapest site).
CC version	3.1 Rev. 5
PP conformance claim	No conformance claimed
Evaluation starting date	15 December 2022
Evaluation ending date	22 August 2023

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description, please refer to the Security Target [ST].

The TOE is Versa Operating System (VOS) 21.2.3 with OS SPACK 20230511 running on Versa Cloud Services Gateways, based on Ubuntu Linux 18.04, implemented in the following deployment options: Versa SD-WAN Branch and Controller. The evaluated configuration of the TOE consists of deployment directly on bare metal CSG appliances and Virtual Machines (VMware ESXi, KVM).

In addition to the evaluated platforms, the TOE is also supported on Private and Public Clouds (AWS, Azure, Google Cloud Platform), Versa SD-WAN white-box appliances, Versa SD-LAN Switches, Versa Access Points and SD-NIC.

TOE environment is identified in Table 1 below:

Item	Identification
TOE Environment hardware appliances for bare metal installation	Versa CSG5000 Versa CSG2500 Versa CSG1500 Versa CSG1300 Versa CSG770 Versa CSG750 Versa CSG365 Versa CSG355
TOE Environment for Controller virtual appliance	Ubuntu 18.04 with ESXi
TOE Environment for Branch virtual appliance	Ubuntu 18.04 with KVM

Table 1 - TOE Environment based on the different implementation of TOE [ST]

For a detailed description of the TOE, consult sections 1.3 and 1.4 of the Security Target [ST]. The most significant aspects are summarized below.

7.3.1 TOE architecture

Versa VOS is a multi-service, *multi-tenant* software platform. Versa VOS runs on Versa Cloud Services Gateways, Versa SD-WAN appliances, Versa validated SD-WAN white box appliances, Versa Controller, Virtual Machines running in Public and Private Clouds.

The TOE is the Versa Operating System based on Ubuntu Linux 18.04. It has its own CLI apart from the Linux shell. The TOE can be configured via the CLI interface or from Versa Director using the NETCONF protocol. The TOE can operate in one of two evaluated configurations, SD-WAN Controller or Branch. SD-WAN is a software-defined approach that significantly improves the deployment and operation of managed network services compared to traditional Branch or WAN architectures.

The TOE can be divided into the following subsystems:

- Control plane subsystem
- Logging subsystem
- Data plane subsystem
- Cryptographic subsystem

- OS Subsystem

The Versa VOS TOE boundary is presented in Figure 1. The TOE boundary is represented by the blue line encompassing the components identified with solid light-green boxes. Administrative interfaces for the TOE are identified with dark green boxes.

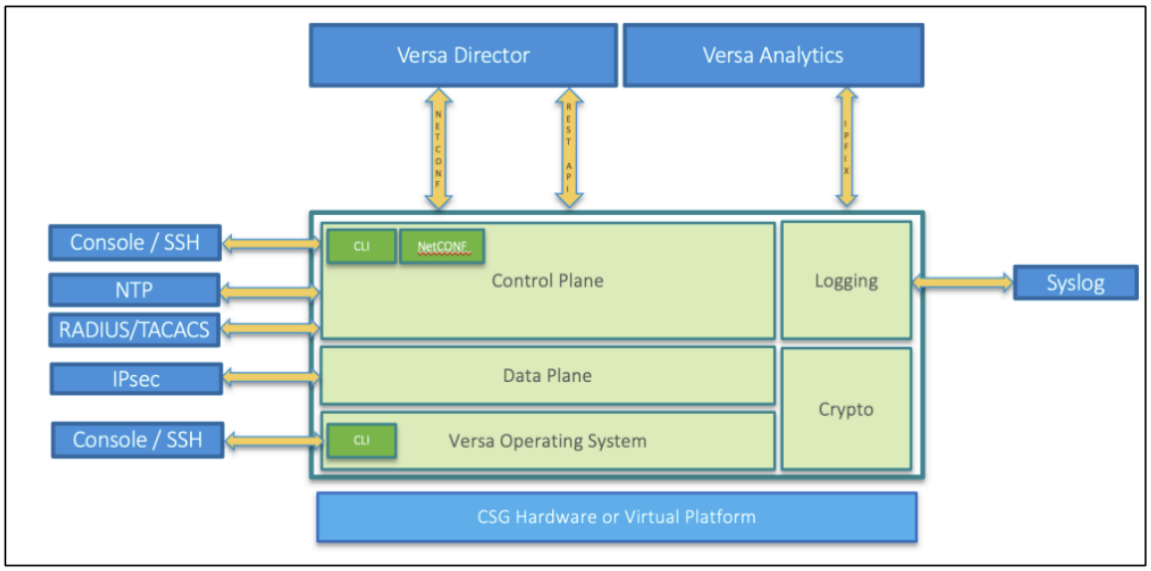

Figure 1 - Versa Subsystems and TOE boundary

The task of the Control Plane subsystem is monitoring and control. If there is any problem that the operator detects, operator or admin can intervene through this subsystem using the NETCONF protocol, via the Versa Director management system. The operator or admin may also access the device through the VOS CLI.

The Logging subsystem is responsible for creating and sending audit logs. The logs store the changes and make them traceable with timestamps and usernames. The manufacturer's own Versa Analytics or external syslog server can be used to store the logs. The logs can be divided into two main parts, data plane logs and system logs.

The Data Plane subsystem is responsible for the protection of network channels. The configuration of IPSEC is done by the Control Plane Subsystem.

The Cryptographic subsystem is responsible for encryption and secure remote access. OPENSSH can be used for secure remote login to the TOE. In addition, OPENSSL is responsible for generating PKI keys. The most important task of the subsystem is to establish IPSec for secure communication between two TOE components.

The TOE supports RADIUS and TACACS+ for remote external authentication. The TOE uses IPSec to protect the communication to external authentication servers. NTP is used to synchronize the TOE system clock for reliable audit record timestamps.

The TOE is based on Ubuntu Linux 18.04. The OS Subsystem comprises the Linux OS which is part of the TOE. The OS Subsystem implements filesystem and user/group/owner file/directory permissions, and *sudo* command for privileged operations from Administrator accounts, among others.

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in section 3 of the Security Target [ST].

For a detailed description of the TOE Security Functions, consult sections 1.4.2 and 7.1 of the Security Target [ST]. The most significant aspects are summarized in the following sections.

7.3.2.1 Security audit

The TOE provides 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, and administrative actions. The administrator may view the contents of the audit records, and 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.

7.3.2.2 Cryptographic Support

The TOE provides cryptography in support of connections, using IPSec for data planes, and IPSec, TLS/HTTPS, and SSH for control planes. The TOE provides key generation, key destruction and cryptographic operation functions.

7.3.2.3 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 SSH. Additionally, administration is typically performed via external Versa Director GUI via the HTTPS, IPsec, and SSH control plane interfaces. Initial provisioning is performed via staging Controller. Users may authenticate using either local password authentication, or by an IPsec protected AAA server.

7.3.2.4 Security Management

The TOE provides the ability to manage all TOE administrators, all identification and authentication, all audit functionality of the TOE, all TOE cryptographic functionality.

7.3.2.5 Protection of the TOE Security Functionality (TSF)

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to authorized administrators.

7.3.2.6 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, administrative sessions will be terminated, requiring administrators to re-authenticate.

7.3.2.7 Trusted path/Channels

The TOE supports establishing trusted paths between itself and remote administrators using SSH for CLI access. The TOE supports use of IPsec, SSH and HTTPS/TLS for control plane connections, and IPsec for data plane connections.

7.4 Documentation

The guidance documentation specified in "Annex A – Guidelines for the secure usage of the product" is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration, and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in section 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

All the SFRs have been selected or derived by extension from CC Part 2 [CC2].

The TOE has one extended component, namely: FPT_TUD_EXT.1 Trusted update. This SFR is a member of the Protection of the TSF (FPT) class and is implemented in the TOE the following way.

- The TOE components have specific versions that can be queried by an administrator. When updates are made available by Versa, an administrator can obtain and install those updates.
- Cryptographic checksums (i.e., digital signatures) are used to verify software update files (to ensure they have not been modified from the originals distributed by Versa) before they are used to update the applicable TOE components.

Please refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab Software Laboratory (Budapest site).

The evaluation was completed on August 22nd, 2023, with the issuance by LVS of the Evaluation Technical Report [ETR], which was approved by the Certification Body on September 12th, 2023. Subsequently, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in "Annex B – Evaluated configuration". Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; there is a probability though small that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to regularly check the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR] issued by the LVS CCLab Software Laboratory (Budapest site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "Versa Operating System (VOS) 21.2.3 with OS SPACK 20230511 running on Versa Cloud Services Gateways" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4 augmented with ALC_FLR.1, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in "Annex B – Evaluated configuration".

Table 2 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL4 augmented with ALC_FLR.1.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives for the operational environment	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Basic modular design	ADV_TDS.3	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass
Delivery procedures	ALC_DEL.1	Pass
Identification of security measures	ALC_DVS.1	Pass

Assurance classes and components		Verdict
Developer defined life-cycle mode	ALC_LDC.1	Pass
Well-defined development tools	ALC_TAT.1	Pass
Basic flaw remediation	*ALC_FLR.1*	*Pass*
Test	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - conformance	ATE_IND.1	Pass
Vulnerability assessment	**Class AVA**	Pass
Focused vulnerability analysis	AVA_VAN.3	Pass

Table 2 - Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in section 6 (Statement of Certification).

Potential customers of the product "Versa Operating System (VOS) 21.2.3 with OS SPACK 20230511 running on Versa Cloud Services Gateways" are suggested to properly understand the specific purpose of the certification by reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the "Security Objectives for the Operational Environment" specified in section 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Organizational Security Policies and Assumption described, respectively, in section 3.2 and 3.3 of the Security Target [ST] are complied.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, "Annex A – Guidelines for the secure usage of the product" includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([CCECG]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE delivery

TOE is delivered in hardware or via software.

Software releases are published to https://download.versa-networks.com from where customers can download and install the TOE.

Alongside the TOE, software releases will be published an MD5SUM file containing MD5 hashes corresponding to each of the software binary images. Customers may compare the hash of the downloaded file to the published hash values to ensure that the binary has not been modified in transit.

Releases are also password protected; the credentials are provided only to registered customers. The delivery of the software image is protected with an HTTPS session ensuring that the contents cannot be intercepted.

Versa also works with third party contract manufacturers for delivery of the software that is pre-installed on a CSG hardware appliance. The process for downloading and verifying the TOE during installation onto CSG hardware is similar to that which is described for general customers.

When a customer orders a CSG model it goes through sales and fulfilment and then an order is placed with the third-party contract manufacturer to build the appliance and load it with VOS. They will obtain the images the same way as described above for software download. They can also be verified using the published hash using procedure described in the guidance documentation [CCECG].

The manufacturer follows the Versa-defined build and verification procedure. They will load the ISO onto the device (during the install, there is a built-in checksum verification which will fail if the image is modified). After installation, they can run “Show system package info” to verify that the TOE was installed correctly. The customer can do the same. The command "show security osspack info" will return the currently installed OS SPACK.

Hardware is shipped to the customer using the agreed upon couriers directly from the contract manufacturer. The customers are provided with tracking information and a bill of materials describing the contents of the shipping container.

9.2 Identification of the TOE by the User

The TOE user can identify TOE components as described below:

- **Hardware**: The model name is marked on the front of the TOE hardware and the product number on the product label on the back.
- **Firmware**: The user can verify firmware version by checking the installed version as described in [CCECG].
- **Guidance documentation**: the version number is printed in the documents.

9.3 Installation, initialization, and secure usage of the TOE

TOE installation, configuration and operation should be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the Common Criteria Evaluated Configuration Guide [CCECG] contains detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure operation of the TOE in accordance with the security objectives specified in the Security Target [ST].

10 Annex B – Evaluated configuration

TOE is the Versa Operating System (VOS) 21.2.3 with OS SPACK 20230511.The evaluated configuration of the TOE consists of deployment directly on bare metal CSG appliances, Versa validated white-box appliances and virtual machines (VMware ESXi, KVM). Depending on the operation of the TOE, it can be divided into two parts.

The TOE is evaluated in the following configurations: SD-WAN Controller and Branch. Controller and Branch are almost identical to each other. Director will control the Branches through the Controller. The encrypted tunnel will be built between Branch and Controller.

Following settings have been applied for the evaluated configuration:

- Administrator credentials are authenticated by the TOE against a local database, and against an external database (like RADIUS, TACACS+).
- Log minimum severity level is set to debug.
- Logging severity level overrides are used (can be configured by Admin role).
- Local logging is always performed.
- Hardware acceleration features are disabled in the evaluated configuration.
- The TOE is certified to work in both FIPS and non-FIPS modes. All SFRs are enforced regardless of the operational mode.
- Other than SD-WAN and IPsec protection features, data plane security features such as NGFW, IDP, Anti-virus, etc. are **not evaluated.**
- Remote logging is optional.
- Versa Analytics and Versa Director are not part of the TOE boundary but are used to facilitate management of multiple distributed VOS devices. All management through these components is performed via SSH (NETCONF) and HTTPS (REST API) interfaces of the TOE which can be additionally encrypted with IPsec.

Preparative procedures are described in [CCECG].

10.1 TOE operational environment

The following required components are part of the Operational Environment (refer also to section 1.3.2 of the Security Target [ST]):

- A hypervisor-based VM
- A Versa validated SD-WAN white box or Versa CSG appliance

In case of bare-metal devices the hardware is determined by the device type and cannot be changed, the user has nothing to do with it.

For virtual platforms, the minimum requirements for running the VOS software are 4 cores, 8 GB of RAM, and 120 GB of hard disk drive; the evaluated hypervisors are as follows:

- VMware vSphere 7.0 and above (SD-WAN Controller)
- KVM on Ubuntu 18.04 (Branch)

For management of the Versa solution, the Versa Director and Versa Analytics are either deployed in a virtual or cloud environment or on a Versa validated SD-WAN white box or Versa CSG appliance and are used for the following functions:

- IPFIX and Syslog aggregation and analysis (Versa Analytics)

NETCONF and REST API for configuration and policy management/deployment and monitoring (Versa Director)

- HTTPS, SSH, and IPsec for protection of management and control planes

Administrator credentials are authenticated by the TOE against a local database, or against an external database (like RADIUS, TACACS+). The TOE may also be synchronized with an external NTP server which is also secured via IPsec.

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities.

11.1 Test configuration

Testing activities have been carried out from the LVS premises.

The Evaluators verified the configuration of the test environment, including the TOE, and found it to be consistent with the Common Criteria Evaluated Configuration Guide [CCECG] and the Security Target [ST].

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer used a testing approach that resulted in covering all the TSFIs with at least one test case. For each test case, the Developer's test documentation describes its purpose, the relevant TSFI(s) and SFR(s), test prerequisites, step-by-step test procedures, and expected test results.

11.2.2 Test coverage

The Evaluators have examined the test plan presented by the Developer and verified the complete coverage of the functional requirements (SFRs) and the TSFIs described in the functional specification.

11.2.3 Test results

The actual test results of all Developer's tests were consistent with the expected ones.

11.3 Functional and independent tests performed by the Evaluators

Before initiating the testing activity, the Evaluators verified that the TOE was configured correctly. They also verified that the test environment was properly set up.

Since TOE can be configured in FIPS mode and NON FIPS mode: both of those configurations have been tested by the evaluator.

All the actual test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked on the same TOE models already used for the functional test activities, verifying that the TOE and the test environment were properly configured.

The Evaluators could conclude that the TOE is resistant to an attack potential of Enhanced-Basic in its intended operating environment. No exploitable or residual vulnerabilities have been identified.