VERSA OPERATING SYSTEM (VOS) 21.2.3 WITH OS SPACK 20230511 RUNNING ON VERSA CLOUD SERVICES GATEWAYS SECURITY TARGET

VERSION 1.8
AUGUST 11, 2023

Versa Networks – www.versa-networks.com
2550 Great America Way Suite 350, Santa Clara, CA 95054

TABLE OF CONTENTS

List of Figures

List of Tables

Document Control Information

Version	Date	Summary of Changes
1.0	2020-06-26	First version of the Security Target
1.1	2022-11-01	Added CSG TOE environment models
1.2	2023-01-05	Addressed lab comments
1.3	2023-01-20	Addressed lab observations
1.4	2023-03-27	Addressed lab observations
1.5	2023-05-22	Updated OS SPack
1.6	2023-06-14	Updated environment details
1.7	2023-06-26	Minor editorial changes
1.8	2023-08-11	Responses to OCSI comments

ABBREVIATIONS

Abbreviation	Description
AAA	Authentication Authorization Accounting
AES	Advanced Encryption Standard
API	Application Programming Interface
BFD	Bidirectional Forwarding Detection
BGP	Boarder Gateway Protocol
CBC	Block Cipher Mode
CC	Common Criteria for Information Technology Security Evaluation
CGNAT	Carrier-Grade NAT
CLI	Command Line Interface
COTS	Commodity Off-The-Shelf
CPE	Customer Premises Equipment
CSG	Cloud Services Group
EAL	Evaluation Assurance Level
FIPS PUB	Federal Information Processing Standards Publications
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
HTTPS	Hyper-Text Transport Protocol Secure
IKE	Internet Key Exchange
IDP	Intrusion Detection and Prevention
IDS	Intrusion Detection System
IPFIX	IP Flow Information Flow
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
KDF	Key Derivation Function
KVM	Kernel-based Virtual Machine
LDAP	Lightweight Directory Access Protocol
LTE	Long-Term Evolution
MP-BGP	Multiprotocol BGP
MPLS	Multi-Protocol Label Switching
NAT	Network Address Translation
NETCONF	The Network Configuration Protocol
NFV	Network Function Virtualization
NFVI	NFV Infrastructure
NGFW	Next Generation Firewall
NID	Network Interface Device
NIST SP	National Institute of Standards and Technology Special Publications
NTP	Network Time Protocol
OS	Operating System
PKI	Public Key Infrastructure
POP	Post Office Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RSA	Rivest-Shamir-Adleman
SA	Security Association
SAR	Security Assurance Requirements
SAML	Security Assertion Markup Language
SD-WAN	Software Defined WAN
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMS	Short Message Service
SNMP	Simple Network Management Protocol

Abbreviation	Description
SSH	Secure Shell
SSL	Secure Socket Layer
SW	Software
Syslog	System Logging Protocol
TACACS	Terminal Access Controller Access Control System
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Universal Serial Bus
UTC	Coordinated Universal Time
UTM	Unified Threat Management
VM	Virtual Machine
VMM	VM Monitor
VNF	Virtualized Network Function
VPN	Virtual Private Network
WAN	Wide Area network

DEFINITIONS

Definition	Description
Hyper-V	Microsoft Hyper-V (formerly known as Windows Server Virtualization) is a native hypervisor, which can create VMs on x86-64 systems running Windows. A server computer running Hyper-V can be configured to expose individual VMs to or more networks.
Hypervisor	Hypervisor (or VMM monitor) is a piece of computer software, firmware or hardware that creates and runs VMs.
KVM	Open source virtualization technology built into Linux. KVM can turn Linux into a hypervisor that allows a host machine to run multiple, isolated virtual environments called guests or VMs.
MPLS	Routing technique in telecommunications networks that directs data from one node to the next based on short path labels rather than long network addresses, thus avoiding complex lookups in a routing table and speeding traffic flows.
SSL/TLS	Protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet.
TSF	Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.
Ubuntu	Open source SW OS that runs from the desktop, to the cloud, to all Internet connected things.
VMware ESXi	Enterprise-class, type-2 hypervisor developed by VMware for deploying and serving virtual components. As a type-1 hypervisor, ESXi is not a software application that is installed on an OS; instead, it includes and integrates vital OS components, such as kernel.

NOTATIONS AND FORMATTING

The notations and formatting used in this ST are consistent with version 3.1 Revision 5 of the Common Criteria (CC).

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Deleted words are denoted by ~~strike-through text~~.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized* text in square brackets, [*Selection value*].

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value with bold face in square brackets, [**Assignment_value**].

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).

Assets: Assets to be protected by the TOE are given names beginning with "AS." – e.g. AS.CLASSIFIED_INFO.

Assumptions: TOE security environment assumptions are given names beginning with "A."- e.g., A.Security_Procedures.

Threats: Threats to the TOE are given names beginning with "T." – e.g., T.Filter_Fails.

Policies: TOE security environment policies are given names beginning with "P."—e.g., P.Information_AC.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE.", respectively, - e.g., O.Filter-msg and OE.Clearance.

1. Security Target Introduction

1.1. ST and TOE References

The following table identifies the Security Target (ST).

Item	Identification
ST Title	Versa Operating System (VOS) 21.2.3 with OS Spack 20230511 running on Versa Cloud Services Gateways Security Target
ST Version	1.8
ST Date	August 11, 2023
ST Author	Versa Networks

Table 1: ST references

The following table identifies the Target of Evaluation (TOE).

Item	Identification
TOE Name	Versa Operating System (VOS) 21.2.3 with OS SPack 20230511
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
TOE Version	VOS 21.2.3 with OS SPack 20230511
TOE Build Identifier	101702-dbe5d34

Table 2: TOE references

The following table identifies common references for the ST and the TOE.

Item	Identification
CC Version	3.1 Revision 5
Assurance level	EAL4+ augmented with ALC_FLR.1
Protection Profile	None

Table 3: ST and TOE references

1.2. TOE Introduction

SD-WAN is a software-defined approach that significantly can improve the deployment and operation of managed network services compared to traditionally Branch or WAN architectures, (i.e. Branch offices that connect to the rest of the business through an MPLS circuit or VPN). Applying a SD-WAN solution involves software based network and security technologies running on COTS hardware and white-box appliances.

SD-WAN are centrally managed and policy orchestrated, and zero-touch provisioned, , addressing operational challenges related to traditionally Branch or WAN architectures.

Applying SD-WAN to enterprise WANs and managed WAN services results in the ability to "software-define" the WAN, not just in form-factor, but also in deployment & provisioning, initial configuration, ongoing management & operations. Software-defined WAN de-couples' software from proprietary hardware, enabling the use of network and security functions in software running on commodity x86 servers and white box appliances. It also de-couples the underlying WAN transport, enabling the use of any WAN circuit type including MPLS, leased line, broadband Internet, and wireless 4G & LTE connections.

1.3. TOE Overview

Versa VOS is a multi-service, multi-tenant software platform built from ground up on cloud principles to deliver scale, segmentation, programmability, and automation. It provides both networking and security functions in a single software stack along with service chaining capabilities.

As part of its SD-WAN framework, Versa Networks uses the following TOE components:

- Branches, a CSG appliance or a bare-metal appliance running Versa VOS software on a white-labeled x86 network platform or an NID with an integrated x86 platform. (The Versa VOS can be configured as an SD-WAN Gateway to provide the capability to selectively route certain traffic between non-SD-WAN and SD-WAN networks).
- Regional SD-WAN Controller (Versa Staging/SD-WAN Controller), either distributed or centralized, which consist of Versa VOS with SD-WAN Controller functionality. (A SD-WAN Controller is deployed in the VOS "headend" which will also contain the Operational Environment components Versa Director and Versa Analytics).

The Versa VOS software is used to enable white-label x86 CPEs into SD-WAN-enabled CPE devices at remote Branches. Note that the same VOS software is used for handling the SD-WAN Controller function.

The following figure shows a logical view of the placement of the SD-WAN components, including the call flows for the TOE components. (A high-level view of call flows for Operational Environment components are indicated). The blue boxes represent TOE environment components while green boxes represent the TOE instances. Blue arrows represent logical interconnections between the TOE and external entities. Note: the VOS Branches also interface with Director and Analytics with REST API, IPFIX and NETCONF protocols however these are protected within an encrypted IPsec channel and routed through the SD-WAN Controller.

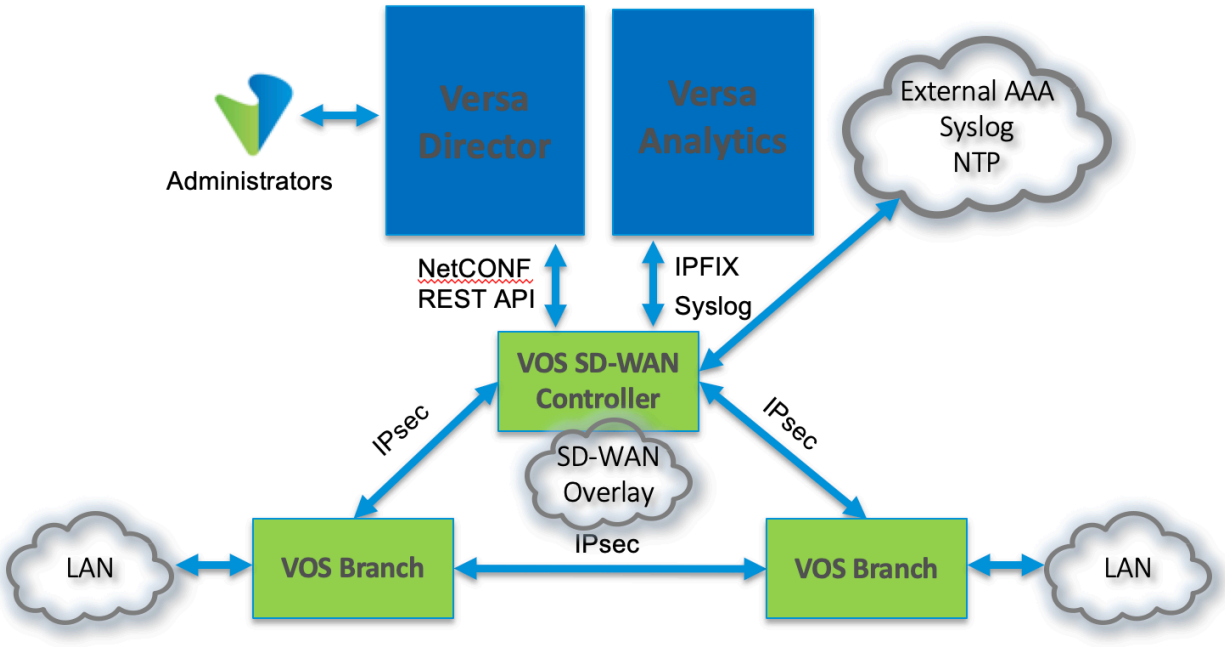

Figure 1: Versa SD-WAN solution

The Versa SD-WAN Controller performs the following tasks:

- The SD-WAN Controller authenticates the Branch Versa VOS devices using Pre-Shared Keys or PKI certificates as part of the IKE exchange.
- The secure channel established using IKE provides transport between Branch VOS devices and all Versa nodes (SD-WAN Controller, and the Operational Environment components Versa Director/Analytics). The Versa SD-WAN Controller serves as an attachment point for management purposes and for control plane information distribution using MP-BGP.
- The SD-WAN Controller uses an advanced, multi-instance MP-BGP route reflector to provide route and security association (SA) information to the Branch VOS nodes in the network group on a per-tenant (per-VPN) basis. Each Branch node advertises an inbound SA in addition to overlay route information.
- The SD-WAN Controller distributes IPSec private keys to Branch VOS nodes, to allow all VOS Branches to authenticate to each other. The IPSec key is negotiated between each pair of Branch VOS devices using Diffie-Hellman algorithm. Each pair of Branch VOS devices will arrive at a unique encryption key, by using the Diffie-Hellman algorithm.

Versa SD-WAN Controller plays a key role in the solution, providing a control plane entry point for Branch deployments. Control overlay tunnels from CPEs to Controllers carry MP-BGP (encapsulated with IPsec), which form the control plane of the Versa SD-WAN solution. Control plane failures between CPEs and Controllers are detected using by the IKE keep alive mechanism, the MP-BGP hold timer, and BFD. MP-BGP and IPSec IKE for the SD-WAN control plane run only between SD-WAN Controllers and CPEs in a hub-and-spoke topology, which allows the solution to scale to many thousands of CPEs.

If a complete loss of communication occurs between CPEs or gateways and their SD-WAN Controllers, either IKE dead-peer detection or BGP and BFD keep alive mechanism detects the loss of the SD-WAN solution control plane and forces the CPE-related forwarding plane to go down. When a BGP peer is detected as down, the associated routes are withdrawn from the

routing and forwarding tables, and the CPEs and gateways tear down the relevant overlay forwarding (data) tunnels.

The Versa VOS TOE boundary is presented in the figure below. 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.

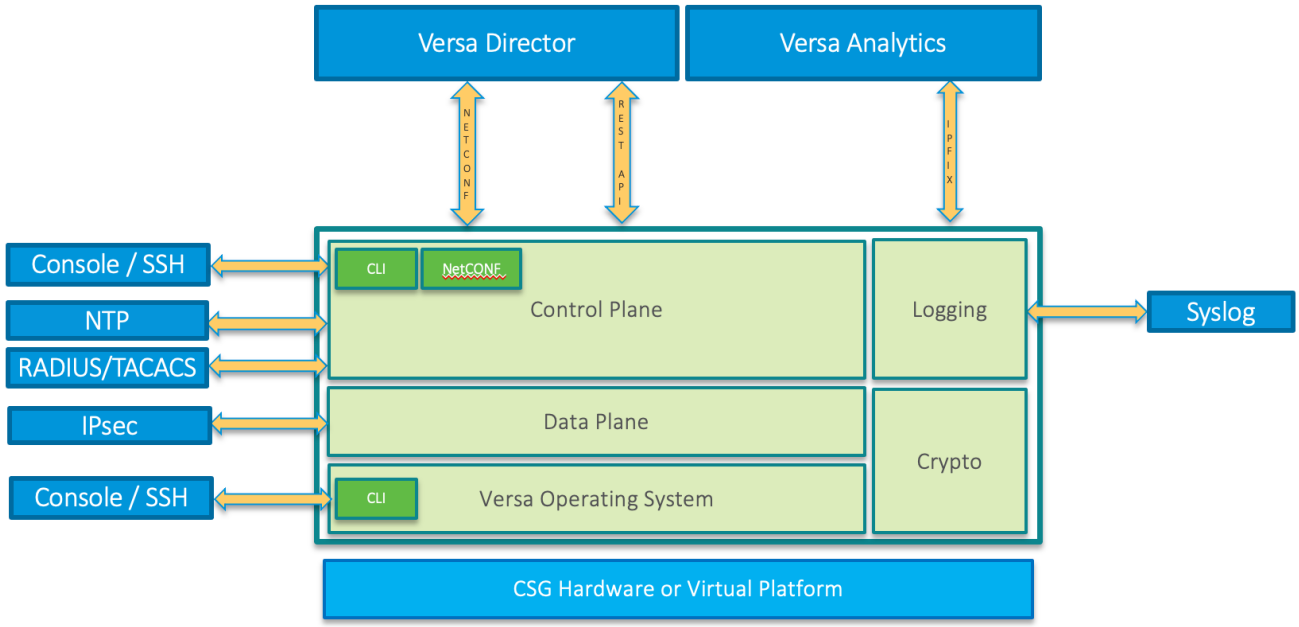

Figure 2: Versa VOS TOE Boundary

.

Versa VOS WAN edge software allows customers to implement a broad spectrum of software-defined solutions from SD-Routing, SD-Security, and Secure SD-WAN. Regardless of where VOS is deployed (on-premises or in the cloud), all network and security capabilities are provisioned and managed centrally through the complex of Director, Analytics and Controller (DAC). (The Operational Environment component Versa Director provides a single pane-of-glass management platform that can be used to provision, configure, manage, monitor, and operate the various Versa VOS appliances, regardless of their deployed location).

1.3.1. DEPLOYMENT OPTIONS

Versa VOS has multiple deployment options, including bare metal white box or CSG appliances, virtual machines (VMware ESXi, KVM) and Public Cloud. Customers can select the best infrastructure for their SD-WAN deployment at both the data center/PoP and Branch offices without being constrained by SD-WAN vendor proprietary hardware options.

The SD-WAN Controller can be deployed either as bare metal or as a hypervisor-based VM.

The evaluated configuration of the TOE consists of deployment directly on bare metal CSG appliances and virtual machines (VMware ESXi, KVM) only.

1.3.2. REQUIRED NON-TOE COMPONENTS

For Branches, the TOE consists of VOS software that executes either on:

- A hypervisor-based VM or
- a white box or a Versa CSG appliance as listed in Table 2

For SD-WAN Controllers, the TOE consists of software that executes either on:

- a hypervisor-based VM or
- a white box or a Versa CSG appliance as listed in Table 2

System requirements:

- Hypervisor supported in the evaluated configuration:
  - 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 white box or CSG appliances 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

External RADIUS/TACACS+ servers may be used for remote authentication which are secured via IPsec. The TOE may also be synchronized with an external NTP server which is also secured via IPsec.

1.4. TOE Description

The TOE boundary includes the VOS 21.2.3 software only deployed as SD-WAN Controller and Branch. A minimum of one SD-WAN Controller is required for SD-WAN. Multiple Controllers can be deployed in an SD-WAN to provide high availability. Because a Versa VOS device is multitenant, a software instance can serve as an SD-WAN Controller for up to 256 tenants.

The TOE environment comprises of the following:

- Versa CSG models and KVM virtual appliance as listed in Table 2 for Branch appliances.
- ESXi 7.0 and above or KVM for Controller virtual appliances.

The TOE software comprises of the following:

- Versa VOS 21.2.3 “wsm” image (for installation on CSG7xx, CSG3xx, and CSG1300)
- Versa VOS 21.2.3 “non-wsm” image (for installation on CSG1500 and higher including virtual deployment)

The TOE is delivered pre-installed on the underlying CSG hardware platform (shipped via normal couriers) or as a single binary image delivered electronically. Customers with an active service agreement and login credentials download the TOE images from https://download.versa-networks.com.

1.4.1. Physical scope

The physical boundary of the TOE is the software executing on any of the required non-TOE component platforms.

The following documents are included with the TOE:

- Versa Operating System (VOS) 21.2.3 with OS Spack 20230511 running on Versa Cloud Services Gateways Common Criteria Guidance Document, v1.7

1.4.2. Logical scope

The Versa VOS TOE is comprised of several security features:

1. Security Audit
2. Cryptographic Support

3. Identification and Authentication
4. Security Management
5. Protection of the TOE Security Functionality (TSF)
6. TOE Access
7. Trusted Path/Channels

Each of the security features identified consists of several security functionalities, as identified below.

1.4.2.1. 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, 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.

1.4.2.2. 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 supported by algorithms.

1.4.2.3. 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 via CLI-based provisioning scripts.

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 either local password authentication, or by an IPsec protected AAA server.

1.4.2.4. 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 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.

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.

1.4.2.5. 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.

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 configure the current system time manually or synchronize the system time with the NTP server time via NTP protocol. Additionally, the TOE performs testing by means of DNS Query, Ping and Traceroute to verify correct operation of the TOE.

The TOE allows authorized administrators to query the currently running TOE version and install updates which are digitally signed.

1.4.2.6. 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.

1.4.2.7. 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. The TOE supports IPsec to encrypt connections with remote authentication servers (RADIUS, TACACS+) and NTP servers.

1.4.3. TOE EVALUATED CONFIGURATION

The TOE is evaluated using the following configuration settings:

- 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.
- Remote logging is optional.
- Other than SD-WAN and IPsec protection features, data plane security features such as NGFW, IDP, Anti-virus, etc. are optional and not evaluated.
- 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.
- 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.

2. CONFORMANCE CLAIMS

This TOE and ST are conformant with the following specifications.

Item	Identification
Part 2 of the ISO/IEC 15408 international standard	Common Criteria security functional components, April 2017, Version 3.1, Revision 5, extended
Part 3 of the ISO/IEC 15408 international standard	Common Criteria security assurance components, April 2017, Version 3.1, Revision 5, conformant
Extended SFRs	FPT_TUD_EXT.1.
Protection Profiles	None
Packages	EAL4+ augmented with ALC_FLR.1

Table 4: Conformance Claims

3. Security Problem Definition

This chapter identifies the following:

- IT related threats to the organization countered by the TOE.
- Organizational security policies for the TOE as appropriate.
- Significant assumptions about the TOE's operational environment.

3.1. Threats

Potential assets are:

- Data, which is sensitive or security functional data, moved between TOE components and between TOE components and the operational environment of Versa Director and Versa Analytics;
- Keys, which are cryptographic keys contained in the TOE, for encryption of data in flight.

Potential threat agents are:

- Attackers, which are unauthorized persons or external IT entities not authorized to use the TOE itself;
- Administrator of the TOE.

The threat agent Attacker is assumed to have access to all publicly available information about the TOE and potential methods of attacking the TOE, and a level of resources consistent with an Enhanced-basic attack potential. It is expected that the Versa units will be protected to the extent necessary to ensure that they remain connected to the networks they protect.

The following table lists the threats addressed by the TOE and the TOE Environment.

Threat	Threat Description
T.ADMINACCESS	Personnel authorized for the TOE may not be able to view or manage security and configuration settings required for the TOE's intended function, rendering the TOE inoperable or resulting in ineffective security mechanisms.
T.ADMINERROR	The TOE may be incorrectly configured that may result in the ineffective security mechanisms, increasing risk of data breach or exploit. During operation, the administrator may unintentionally configure the TOE incorrectly, making the TOE inoperable or resulting in ineffective security mechanisms.
T.ADMINEXPLOIT	An attacker or unauthorized user may gain access to an administrator account, implying risk of data exploiting. Hacking methods can be used to exploit missing, weak, or incorrectly implemented access control in the TOE.
T.CRYPTCOMP	An attacker may compromise cryptographic keys and the data protected by the cryptographic mechanisms, implying risk of keys exploiting. The attacker may cause that keys associated with the cryptographic functionality are to be inappropriately accessed (viewed/modified/deleted), thus compromising the cryptographic mechanisms protected by those mechanisms.

Threat	Threat Description
T.HACKACCESS	An attacker may get undetected system access to the TOE due to missing, weak and/or incorrectly implemented access control, causing potential violations of integrity, confidentiality or availability, implying risk of data exploiting. The attacker may use hacking methods to exploit missing, weak, or incorrectly implemented access control in the TOE.
T.MALFUNCTION	The TOE may malfunction that may compromise information and data processing, implying risk of data and keys exploiting. The attacker may get unauthorized access to TOE resources. The TOE may malfunction that may compromise roles and permissions, implying risk of data and keys exploiting. An administrator may gain unauthorized roles and permissions in TOE.
T.WANCOMP	An attacker may gain unauthorized access to data, by observing the network traffic exchanged between instances of the TOE via the WAN, implying risk of data exploiting.
T.UNAUTHUPDATE	An attacker may attempt to perform an update of the product which compromise the security features of the TOE. Poorly chosen update protocols, signature generation and verification algorithms, and parameters allow an attacker to install software and/or firmware that bypasses the intended security features and provides an unauthorized access to data.

Table 5: Security Threats

3.2. Organizational Security Policies (OSP)

The following table lists the Organizational Security Policies imposed by an organization to address its security needs.

Organizational security Policies	Description
P.ACCOUNTABILITY	The authorized administrators of the TOE shall be held accountable for their actions.
P.ADMINACCESS	An authorized administrator must manage the TOE securely.
P.DETECT	To trace all security-related responsibilities, security-related events shall be documented, maintained, and analyzed, and such records can be checked.

Table 6: Organizational Security Policies

3.3. Assumptions

The specific conditions listed in the following table are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Assumptions	Description
A.NETWORK	There will be a network that supports communication between instances of the TOE and between the TOE and IT systems used to manage the TOE. This network functions properly.
A.NOGENPURP	There are no general-purpose computing capabilities (e.g., compilers or applications) available on the TOE, other than those services necessary for the operation, administration, and support of the TOE.
A.PHYSICAL	The TOE shall presumably be located in physically secure environment that can be accessed only by the authorized administrators.
A.TRUSTADMIN	The administrators of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines.

Table 7: TOE Environment Assumptions

4. Security Objectives

This chapter defines the security objectives for the TOE and its supporting environment. The security objectives are intended to counter identified threats, comply with defined organizational security policies, and address applicable assumptions.

4.1. TOE Security Objectives

This section defines the security objectives that are to be addressed by the TOE.

Security Objectives	Description
O.ACCESS	The TOE must allow only authorized administrators to access only appropriate TOE functions and data.
O.AUDIT	The TOE shall record, and export security-related events associated with administrators to enable tracing of responsibilities for security-related.
O.BANNER	The TOE will present configured banner text to administrators prior to administrator's attempting to login to the TOE.
O.CRYPTO	The TOE must protect the confidentiality and integrity of data passed between itself and authorized administrators, and between Versa Controllers and Versa Branches.
O.IDAUTH	The TOE must be able to identify and authenticate authorized administrators prior to allowing access to TOE security management functions.
O.MANAGE	The TOE must include a set of functions that allow effective management of its functions and data. The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE and provide protections for logged-in administrators.
O.PROTECT	The TOE must protect itself and its resources from unauthorized modifications and access to its functions and data.
O.TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.
O.TIME	The TOE shall provide reliable time stamps and the capability for the administrator to set the time-source used for these time stamps, in that the administrator can configure the TOE to synchronize its clocks with NTP servers.
O.VERUPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.

Table 8: Security Objectives for the TOE

4.2. Operational Environment Security Objectives

This section defines the security objectives that are to be addressed by the operational environment of the TOE.

Security Objectives	Description
OE.NETWORK	The administrator will install and configure a network that supports communication between instances of the TOE and between the TOE and IT systems used to manage the TOE. The administrator will ensure that this network functions properly.
OE.NOGENPURP	There are no general-purpose computing capabilities (e.g., compilers or applications) available on the TOE, other than those services necessary for the operation, administration, and support of the TOE.
OE.PHYSICAL	Those responsible for the TOE must ensure that the hardware on which the TOE and OS are installed, is protected from any physical attack.
OE.TRUSTADMIN	The administrator of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines.
OE.WANCOMM	The Operational Environment will provide any required protection from disclosure and/or modification for traffic traversing the WAN.

Table 9: Security Objectives for the Operational Environment

4.3. Security Objectives Rationale

The following tracing shows which security objectives address which threats, policies (OSPs) and assumptions.

	Threats							Policies			Assumptions				
	T.ADMINACCESS	T.ADMINERROR	T.ADMINEXPLOIT	T.CRYPTOCOMPR	T.HACKACCESS	T.MALFUNCTION	T.WANCOMP	T.UNAUTHUPDATE	P.ACCOUNTABILITY	P.ADMINACCESS	P.DETECT	A.NETWORK	A.NOGENPURP	A.PHYSICAL	A.TRUSTADMIN
TOE Security Objectives															
O.ACCESS	X		X		X					X					
O.AUDIT					X	X			X		X				
O.BANNER									X	X					X
O.CRYPTO					X	X									
O.IDAUTH			X		X				X						
O.MANAGE	X				X					X					
O.PROTECT				X	X	X									
O.TEST						X									
O.TIME									X		X				
O.VERUPDATES								X							
Operational Environment Security Objectives															
OE.NETWORK												X			
OE.NOGENPURP													X		
OE.PHYSICAL														X	
OE.TRUSTADMIN		X	X		X				X	X					X
OE.WANCOMM							X								

Table 10: Mapping of Objectives to Threats, Policies and Assumptions

The following table is a set of justifications that shows that all threats, policies (OSPs), and assumptions are effectively addressed by the security objectives.

Threat/Policy/Assumption	Security Objective Rationale
T.ADMINACCESS	*The TOE administrator may not be able to access TOE configuration functions.* O.ACCESS and O.MANAGE provide authorized administrators the capability to view and manage configuration settings.
T.ADMINERROR	*The TOE may be incorrectly configured that may result in the TOE's acquisition of ineffective security mechanisms.* OE.TRUSTADMIN ensures that the administrators are non-hostile and are trained to appropriately manage and administer the TOE.
T.ADMINEXPLOIT	*A person/company may gain access to an administrator account.* O.ACCESS restricts access to administrative functions to the authorized administrators. O.IDAUTH includes mechanisms to authenticate TOE administrators and place controls on administrator sessions. OE.TRUSTADMIN ensures that the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner.
T.CRYPTCOMP	*An attacker may compromise cryptographic keys and the data protected by the cryptographic mechanisms.* O.PROTECT ensures that the TOE will have adequate protection from external sources and that all TOE Security Policy functions are invoked.
T.HACKACCESS	*A person/company gets undetected system access to the TOE due to missing, weak and/or incorrectly implemented access control, causing potential violations of integrity, confidentiality, or availability.* O.ACCESS and O.IDAUTH provide the means to identify and authenticate the TOE administrators. The correct identity of the administrator is the basis for any decision of the TOE about an attempt of an administrator to access data. O.AUDIT provides the TOE the capability to detect and create records of security-relevant events associated with administrators and users. O.CRYPTO ensures the confidentiality and integrity of data passed between the TOE and the authorized administrator for management purposes, and between the TOE and remote servers. O.MANAGE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc. to the authorized administrators. These objectives ensure that no other administrator can modify the information flow policy to bypass the intended TOE security policy.

	O.PROTECT ensures that the TOE will have adequate protection from external sources and that all TOE Security Policy functions are invoked. OE.TRUSTADMIN ensures that the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner.
T.MALFUNCTION	*The TOE may malfunction which may compromise information and data processing. The TOE may malfunction which may compromise roles and permissions.* O.AUDIT provides the TOE the capability to detect and create records of security-relevant events associated with administrators and users. O.CRYPTO requires the TOE to implement cryptographic services to provide confidentiality protection of data in rest and flight. O.PROTECT ensures that the TOE will have adequate protection from external sources and that all TOE Security Policy functions are invoked. O.TEST ensures that failure of mechanisms do not lead to a compromise in the TSF.
T.WANCOMP	*A user may gain unauthorized access to data.* OE.WANCOMM protects information traversing the WAN from disclosure and/or modification if such protection is required.
T.UNAUTHUPDATE	*An attacker attempts to supply an update to the product that may compromise the security features of the TOE, implying risk of data exploiting.* O.VERUPDATES ensures that the administrator has not installed a malicious update, thinking that it was legitimate.
P.ACCOUNTABILITY	*The authorized administrators of the TOE shall be held accountable for their actions.* O.AUDIT ensures that the administrator's user-identifier is recorded when any security relevant change is made to the TOE (e.g. modifying TSF data, login sessions). O.BANNER ensures that Administrator knows which system do they log in and be aware of security. O.IDAUTH requires the TOE to identify and authenticate administrators prior to allowing any TOE access on behalf of those administrators. O.TIME ensures that audit logs have correct timestamps. OE.TRUSTADMIN ensures that the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner.
P.ADMINACCESS	*An authorized administrator must manage the TOE securely.* O.ACCESS and O.MANAGE provide authorized administrators the capability to view and manage configuration settings.

	O.BANNER ensures that Administrator knows which system do they log in and be aware of security. OE.TRUSTADMIN ensures that the administrators are non-hostile and are trained to appropriately manage and administer the TOE.
P.DETECT	*To trace all security-related responsibilities, security-related events shall be documented, maintained, and analyzed, and such records can be checked.* O.AUDIT ensures the collection of data on security relevant events. O.TIME ensures that the audit functionality can include reliable timestamps.
A.NETWORK	*There will be a network that supports communication between instances of the TOE and between the TOE and IT systems used to manage the TOE. This network functions properly.* OE.NETWORK restates it as an objective for the administrator to satisfy.
A.NOGENPURP	*There are no general-purpose computing capabilities (e.g., compilers or applications) available on the TOE, other than those services necessary for the operation, administration, and support of the TOE.* OE.NOGENPURP ensures that there are no general- purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) on the TOE.
A.PHYSICAL	*The TOE shall presumably be located in physically secure environment that can be accessed only by the authorized administrators.* OE.PHYSICAL ensures that the environment provides physical security, commensurate with the value of the TOE and the data it contains.
A.TRUSTADMIN	*The administrators of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines.* O.BANNER ensures that Administrator knows which system do they log in and be aware of security. OE.TRUSTADMIN ensures that the administrators of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines.

Table 11: Rationale between Objectives and SPDs

5. Extended Components Definition

If applicable, this chapter defines security components for the TOE not already defined in CC part 2 or CC part 3. The following extended component has been included in this Security Target because the Common Criteria components were found to be insufficient as stated.

5.1. Extended Components

Extended Component	Rationale
FPT_TUD_EXT.1	FPT_TUD_EXT.1 is modelled loosely on the component FPT_TST.1: TSF Testing. FPT_TUD_EXT.1 defines a new family, Trusted Update, and component which is needed to specify requirements for trusted updates to the TOE.

Table 12: Rationale for Extended Component

5.1.1. FPT_TUD_EXT.1 Trusted Update

Family Behavior: The family defines the requirements for securely updating the TOE by authorized administrators and verifying the integrity of the update package binary.

Component Leveling:
FPT_TUD_EXT: Trusted Update

Only one component, FPT_TUD_EXT.1 is included in this family.

FPT_TUD_EXT.1 Trusted Update provides the ability for authorized administrators to install updates to the TOE and verify the installed version along with verifying the integrity of the update image using a cryptographic mechanism defined in FCS_COP.1.

Management: FPT_TUD_EXT.1

The following actions could be considered for the management functions in FMT:

1. Installing updates to the TOE

Audit: FPT_TUD_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

1. Initation of update

Hierarchical to: No other components.
Dependencies: FCS_COP.1 Cryptographic operation

FPT_TUD_EXT.1.1 The TSF shall provide security administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide security administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a [*assignment: cryptographic mechanism for verifying updates*] prior to installing those updates.

6. Security Requirements

6.1. Security Functional Requirements (SFRs)

Functional Class	Functional Component	
FAU: Security audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
FCS: Cryptographic support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
FIA: Identification and authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of Identification
	FIA_USB.1	User-subject binding
FMT: Security management	FMT_MOF.1	Management of Security Functions Behaviour
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
FPT: Protection of the TSF	FPT_STM.1	Reliable time stamps
	FPT_TUD_EXT.1	Extended: Trusted Update
	FPT_TST.1	TSF testing
FTA: TOE access	FTA_SSL.3	TSF-initiated termination
	FTA_TAB.1	Default TOE access banners
FTP: Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

Table 13: Security Functional Requirements

6.1.1. SECURITY AUDIT (FAU)

6.1.1.1. FAU_GEN.1 AUDIT DATA GENERATION

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [*not specified*] level of audit; and
c) [**Auditable events listed in the following table**].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Time/date, Type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**additional information listed in the following table**].

SFR	Auditable Event	Additional Audit Record Contents
FAU_GEN.1	The TOE has been started	(Event Log) restart
FIA_UAU.1	All use of the authentication mechanism	Claimed identity of the administrator using the authentication mechanism
FIA_UAU.5	Decision of the authentication mechanism	Claimed identity of the administrator attempting to authenticate
FIA_UID.1	All use of the identification mechanism	Claimed identity of the administrator using the identification mechanism
FMT_MOF.1	All modifications in the behavior of the functions in the TSF	The identity of the administrator performing the function
FMT_MTD.1	All managing of TSF data	The identity of the administrator performing the function
FMT_SMF.1	Use of management functions	The identity of the administrator performing the function
FPT_STM.1	Changes to the time	None
FPT_TUD_EXT.1	Initiation of update	None
FTA_SSL.3	Automatic logout due to inactivity timer	None
FTP_ITC.1	Failure of the trusted channel functions	Identification of the initiator and target of failed trusted channels establishment attempt
FTP_TRP.1	Failure of the trusted path functions	Identification of the claimed administrator identity

Table 14: Auditable Events

6.1.1.2. FAU_GEN.2 USER IDENTITY ASSOCIATION

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3. FAU_SAR.1 AUDIT REVIEW

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [**administrators with the Admin and Operator roles**] with the capability to read [**all audit information**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.4. FAU_STG.1 PROTECTED AUDIT TRAIL STORAGE

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [*prevent*] unauthorised modifications to the stored audit records in the audit trail.

6.1.2. CRYPTOGRAPHIC SUPPORT (FCS)

6.1.2.1. FCS_CKM.1 CRYPTOGRAPHIC KEY GENERATION

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA, ECDSA**] and specified cryptographic key sizes [**2048 (bits), 4096 (bits), P-224, P-256, P-384, P-521**] that meet the following: [**FIPS PUB 186-4**].

6.1.2.2. FCS_CKM.4 CRYPTOGRAPHIC KEY DESTRUCTION

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zeroization of keys provided by VOS**] that meets the following: [**FIPS PUB 140-2**].

6.1.2.3. FCS_COP.1 CRYPTOGRAPHIC OPERATION

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [**the cryptographic operations specified in the following table**] in accordance with a specified cryptographic algorithm [**the cryptographic algorithms specified in the following table**] and cryptographic key sizes [**cryptographic key sizes specified in the following table**] that meet the following: [**standards listed in the following table**].

Operation	Algorithm	Key Size or Digest Length (bits)	Standard
Digital Signature	RSA, ECDSA	2048, 4096 P-224, P-256, P-384, P-521	FIPS PUB 186-4
Encryption/ Decryption	AES (modes: CBC, CTR, GCM)	128,192,256	FIPS PUB 197
Hashing	SHA	160, 256, 384, 512	FIPS PUB 180-4
HMAC	HMAC-SHA-1	160	FIPS PUB 198-1
	HMAC-SHA-256	256	FIPS PUB 198-1
	HMAC-SHA-384	384	FIPS PUB 198-1
	HMAC-SHA-512	512	FIPS PUB 198-1
Key Exchange	EC Diffie-Hellman	P-256, P-384, P-512	NIST SP 800-56A
TLS Session Keys Derivation	TLS KDF	SHA-256, SHA-384, SHA-512	NIST SP 800-135
SSH Session Key Derivation	SSH KDF	128, 192, 256	NIST SP 800-135
IKE Session Key Derivation	IKE KDF	128, 256	NIST SP 800-135

Table 15: Cryptographic Operations

6.1.3. IDENTIFICATION AND AUTHENTICATION (FIA)

6.1.3.1. FIA_ATD.1 USER ATTRIBUTE DEFINITION

Dependences: None.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**username, password, and role (Admin/Operator)**].

6.1.3.2. FIA_UAU.1 TIMING OF AUTHENTICATION

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [**viewing the login banner on**] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.3. FIA_UAU.5 MULTIPLE AUTHENTICATION MECHANISMS

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [**local password-based mechanism, RADIUS, TACACS+]** to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**following rules:**

- **administrators authenticate to interfaces (console and management port) using a locally held username and password;**
- **administrators authenticate to interfaces using a remote authentication server;**

- **administrators interacting with the Versa Director GUI are implicitly authenticated to the TOE by the cryptographically secured management/control plane interfaces (e.g. via NETCONF or REST API)**

6.1.3.4. FIA_UAU.7 Protected authentication feedback

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [**obscured feedback**] to the user while the authentication is in progress.

6.1.3.5. FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [**viewing the login banner on**] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.6. FIA_USB.1 User-subject binding

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**username**].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**the username is associated with an administrative session when I&A is successful**].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**the username does not change during a session**].

6.1.4. Security management (FMT)

6.1.4.1. FMT_MOF.1 Management of Security Functions Behaviour

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behaviour of, disable, enable, modify the behaviour of*] the functions [**specified in the following table**] to [**administrators with the roles specified in the following table**].

Function	Admin role	Operator role	Organization User
User login for individual administrator accounts	disable, enable	none	none
Remote event logging	determine the behaviour of, disable, enable,	none	none

Function	Admin role	Operator role	Organization User
	modify the behaviour of		

Table 16: Function behaviour for administrator roles

6.1.4.2. FMT_MTD.1 Management of TSF data

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [***manage***] the [**TSF data**] to [**the Admin and Organization User roles**].

6.1.4.3. FMT_SMF.1 Specification of Management Functions

Dependencies: None.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [**defined in the following table**].

Function	Admin role	Operator role	Organization User
Configure (including saving configuration)	X		X
Configure administrator	X		
Restore factory default	X		
Delete configuration file	X		
Roll back configuration	X		
Reboot	X	X	
View configuration information	X	X	X
View log information	X	X	X
Modify current admin password	X		
Modify own admin password	X	X	X
Ping/Traceroute	X	X	X
Install updates to the TOE	X		

Table 17: Function permissions for administrator roles

6.1.4.4. FMT_SMR.1 Security roles

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [**Admin,Operator, and Organization User**].

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

6.1.5. Protection of the TSF (FPT)

6.1.5.1. FPT_STM.1 Reliable time stamps

Dependencies: None.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.1.5.2. FPT_TUD_EXT.1 TRUSTED UPDATE

Dependencies: FCS_COP.1 Cryptographic operation

FPT_TUD_EXT.1.1 The TSF shall provide security administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide security administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a [**digital signature mechanism**] prior to installing those updates.

6.1.5.3. FPT_TST.1 TSF TESTING

Dependencies: None.

FPT_TST.1.1 The TSF shall run a suite of self-tests [*during initial start-up, periodically during normal operation, at the request of an authorised user*] to demonstrate the correct operation of [*the TSF*].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [***VOS daemons and cryptographic libraries***].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of [***VOS daemons and cryptographic libraries***].

6.1.6. TOE ACCESS (FTA)

6.1.6.1. FTA_SSL.3 TSF-INITIATED TERMINATION

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [**configured interval of user inactivity (default 5 minutes)**].

6.1.6.2. FTA_TAB.1 DEFAULT TOE ACCESS BANNERS

Dependencies: No dependencies.

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

6.1.7. TRUSTED PATH/CHANNELS (FTP)

6.1.7.1. FTP_ITC.1 INTER-TSF TRUSTED CHANNEL

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [*the TSF, another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**connections with remote: Versa Director, Versa Analytics, RADIUS/TACACS+, and NTP**].

6.1.7.2. FTP_TRP.1 Trusted path

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [*remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [*modification, disclosure*].

FTP_TRP.1.2 The TSF shall permit [*remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [**local and remote administration**].

6.2. Security Requirements Rationale

6.2.1. Relation between SFRs and security objectives

The following tracing shows which SFRs address which security objectives for the TOE.

Objectives / Requirements	O.ACCESS	O.AUDIT	O.BANNER	O.CRYPTO	O.IDAUTH	O.MANAGE	O.PROTECT	O.TEST	O.TIME	O.VERUPDATES
FAU_GEN.1		X								
FAU_GEN.2		X								
FAU_SAR.1	X	X				X				
FAU_STG.1							X			
FCS_CKM.1				X						
FCS_CKM.4				X						
FCS_COP.1				X						X
FIA_ATD.1					X					
FIA_UAU.1	X				X					
FIA_UAU.5					X					
FIA_UAU.7					X					
FIA_UID.1	X				X					
FIA_USB.1					X					
FMT_MOF.1	X					X	X			
FMT_MTD.1						X				
FMT_SMF.1						X	X			
FMT_SMR.1					X		X			
FPT_STM.1		X							X	
FPT_TUD_EXT.1										X
FPT_TST.1								X		
FTA_SSL.3						X				
FTA_TAB.1			X							
FTP_ITC.1				X						
FTP_TRP.1				X						

Table 18: Tracing of functional requirements to Objectives

The following set of justifications shows that all security objectives for the TOE are effectively addressed by the SFRs.

Security Objectives	Security Functional Requirement Rationale
O.ACCESS	*The TOE must allow only authorized administrators to access only appropriate TOE functions and data.* FAU_SAR.1 ensures that only authorized administrators can access and read audit records. FIA_UID.1 and FIA_UAU.1 ensure that administrators are identified and authenticated prior to being allowed access to TOE security management functionality. FMT_MOF.1 ensures that only authorized administrators have access to security management functions.
O.AUDIT	*The TOE shall record, and export security-related events associated with administrators to enable tracing of responsibilities for security-related.* FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that the administrator can audit any security relevant event that takes place in the TOE. FAU_GEN.2 ensures that the audit records associate an administrator identity with the auditable event. In the case of authorized administrators, the association is accomplished with the username. In all other cases, the association is based on the source identifier, which is presumed to be the correct identity, but cannot be confirmed since these subjects are not authenticated. FAU_SAR.1 provides the means to read the audit information. FPT_STM.1 supports the audit functionality by ensuring that the TOE can obtain a time stamp for use in recording audit events.
O.BANNER	*The TOE will present configured banner text to administrators prior to administrator's attempting to login to the TOE.* FTA_TAB.1 requires the TOE to display the login banners to administrators before the administrators log in.
O.CRYPTO	*The TOE must protect the confidentiality and integrity of data passed between itself and authorized administrators, and between Versa Controllers and Versa Branches.* FCS_CKM.1 ensures that the TOE can generate cryptographic keys. FCS_CKM.4 provides the functionality for ensuring that keys and key material is zeroized. FCS_COP.1 requires that for each cryptographic operation an approved algorithm is used, and if compliant that the algorithm meets the standard. FTP_ITC.1 specifies the use of that cryptography between the TOE and the remote servers. FTP_TRP.1 specifies the use of that cryptography between the TOE and the remote administrator.

O.IDAUTH	*The TOE must be able to identify and authenticate authorized administrators prior to allowing access to TOE security management functions.* FIA_ATD.1 ensures that the data required to identify and authenticate administrators is maintained by the TOE. FIA_UID.1 and FIA_UAU.1 ensure that administrators are identified and authenticated prior to being granted access to TOE security management functionality. FIA_UAU.5 defines the available authentication mechanisms in the TOE and specifies the rules that describe how the authentication mechanisms provide authentication and when each is to be used. FIA_UAU.7 ensures obscured password feedback when the administrator is logging in, thus serving to protect that data. FIA_USB.1 requires the TOE to bind the username to each management session upon successful I&A. FMT_SMR.1 supports the objective by providing roles which are used to provide administrators access to TOE security functionality.
O.MANAGE	*The TOE must include a set of functions that allow effective management of its functions and data. The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE and provide protections for logged-in administrators.* FAU_SAR.1 provides authorized administrators with the ability to read audit logs. FMT_MOF.1 provides functionality to manage the behaviour of the functions/features of the TOE restricted to authorized administrators and identifies the role required for specific actions. FMT_MTD.1 requires that the ability to manipulate TOE content is restricted to authorized administrators and identifies the role required for specific actions. FMT_SMF.1 provides the management functions supporting the specific security management claims and limiting access to that functionality to authorized administrators. FTA_SSL.3 requires the TOE to automatically terminate TOE sessions after a configured amount of inactivity. This protects against unauthorized access if users forget to terminate a session.
O.PROTECT	*The TOE must protect itself and its resources from unauthorized modifications and access to its functions and data.* FAU_STG.1 requires the TOE to prevent unauthorized modification or deletion of the audit records. FMT_MOF.1, FMT_SMF.1 and FMT_SMR.1 ensure that access to TOE security functions is limited to authorized administrators.
O.TEST	*The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.* FPT_TST.1 performs self-test to ensure the TOE is operating correctly and all functions are available and enforced.

O.TIME	*The TOE shall provide reliable time stamps and the capability for the administrator to set the time-source used for these time stamps, in that the administrator can configure the TOE to synchronize its clocks with NTP servers.* FPT_STM.1 requires that the TOE be able to provide reliable time stamps for its own use. Time stamps include date and time and are reliable in that they are always available to the TOE.
O.VERUPDATES	*The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.* FPT_TUD_EXT.1 and FCS_COP.1 ensure the update was downloaded via secure communications, is from a trusted source, and the update can be verified by cryptographic mechanisms prior to installation.

Table 19: Rationale between Objectives and SFRs

6.3. SFR Dependencies

The table below shows the dependencies of the security functional requirement of the TOE and gives a rationale for each of them if they are included or not.

SFR	Dependency	Dependency Rationale
FAU_GEN.1	FPT_STM.1	Included
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Included
FAU_SAR.1	FAU_GEN.1	Included
FAU_STG.1	FAU_GEN.1	Included
FCS_CKM.1	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	Included
FCS_CKM.4	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	Included
FCS_COP.1	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Included
FIA_ATD.1	None	
FIA_UAU.1	FIA_UID.1	Included
FIA_UAU.5	None	
FIA_UAU.7	FIA_UAU.1	Included
FIA_UID.1	None	
FIA_USB.1	FIA_ATD.1	Included
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Included
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Included
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	Included
FPT_STM.1	None	
FPT_TUD_EXT.1	FCS_COP.1	Included
FPT_TST.1	None	
FTA_SSL.3	None	
FTA_TAB.1	None	

SFR	Dependency	Dependency Rationale
FTP_ITC.1	None	
FTP_TRP.1	None	

Table 20: SFR's dependencies and rationale

6.4. SECURITY ASSURANCE REQUIREMENTS (SARS)

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 4+ level of assurance, as defined in the CC Part 3.

The assurance components are summarized in the table below.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.1 Basic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

Table 21: Assurance requirements

The SARs were chosen according to the EAL4 baseline augmented with ALC_FLR.1 for demonstration of flaw remediation.

7. TOE Summary Specification

7.1. TOE Security Functional Requirement Measures

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE, in the following table.

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Satisfied</th></tr>
<tr><td>FAU_GEN.1</td><td>Audit messages are generated for actions performed by users of the TOE. The VOS Branch devices and the SD-WAN Controllers generates alarms for critical event logs, and audit logs for any administrative operations performed on the TOE. The VOS and Controller devices send their logs to an Analytics node (in the Operational Environment), which displays the data graphically.

Versa VOS is operations-ready and supports standard protocols and log formats, including Syslog and IPFIX, making it compatible with existing network management, monitoring, and reporting systems.

When a Versa VOS Branch restarts, both alarms and logs are sent to the Versa Analytics (Operational Environment). Based on this information, the TOE sends to the Operational Environment a history of Versa VOS Branch availability over time.

The following states the log types of TOE:
<table><tr><th>Log Type</th><th>Description</th></tr><tr><td>Logon/Logoff events</td><td>Login/Logoff events are stored in Linux syslog. They can be configured to be exported to external syslog server as well.</td></tr><tr><td>Config/Management operations</td><td>Logs are stored in system audit logs, and Versa audit logs. They can be configured to be exported to external syslog server as well.</td></tr><tr><td>Traffic Logs</td><td>Forwarded to Analytics</td></tr></table></td></tr>
<tr><td>FAU_GEN.2</td><td>The TOE ensures each action performed by the administrator at the CLI or via external Director GUI is logged with the administrator’s identity and as a result events are traceable to a specific user.</td></tr>
<tr><td>FAU_SAR.1</td><td>The authorized administrators can read the audit records from the CLI.

Log messages can be sent to the file destinations by default. Log messages are logged to the following files on TOE:
• /var/log/syslog
• /var/log/fail2ban.log
• /var/log/account/pacct
• /var/log/audit/audit.log
• /var/log/versa/confd/audit.log
• /var/log/versa/confd/netconf.log
• /var/log/versa/confd/localhost:8443.access
• /var/log/versa/ipsec.log

Additionally, the TOE can be configured to forward logs to remote syslog server.</td></tr>
</table>

TOE SFRs	How the SFR is Satisfied
FAU_STG.1	Audit logs are protected with filesystem permissions where only the administrators with the "sudo" privilege or daemon service accounts have write access to the log file directories. The TOE does not provide any mechanism for administrators to modify audit information, but audit log files are deleted automatically according to configured parameters. Audit log settings are configured to automatically archive and rotate log files, based on size limit. Audit log files can also be manually deleted at the command of administrators with sudo privileges. While sudo privilege may provide the ability to modify log files, the administrators with this privilege are trusted not to do so.
FCS_CKM.1	In support of secure cryptographic protocols, the TOE supports the key generation scheme of RSA and ECDSA as specified in FIPS PUB 186-4. The TOE provides Key Generation capabilities in support of IPsec, SSH, and TLS: • Using 2048-bits and 4096-bits RSA, described in FIPS PUB 186-4. • Using P-224, P-256, P-384, and P-521 ECDSA, described in FIPS PUB 186-4.
FCS_CKM.4	The TOE meets all requirements specified in FIPS 140-2 for destruction of keys. All cryptographic keys within the TOE are able to be destroyed securely, rendering them completely inaccessible to an adversary. The TOE supports an erase command which deletes the encrypted VOS configuration database storing the user generated keys. The database encryption key is automatically generated during onboarding and may be installed on a protected location on disk, or a TPM (if present). The database encryption key may be destroyed by using the factory reset command. VOS also provides low-level tools allowing the key file contents to be overwritten with zeroes or random patterns prior to deletion.

TOE SFRs	How the SFR is Satisfied
FCS_COP.1	The TOE provides Digital Signature capabilities in support of IPsec, TLS, and SSH: • Using 2048 and 4096bits RSA, described in FIPS PUB 186-4. • Using P-224, P-256, P-384, and P-521 ECDSA, described in FIPS PUB 186-4. The TOE provides Encryption and Decryption capabilities in support of IPsec, TLS, and SSH: • Using 128, 192, and 256 bits AES, described in FIPS PUB 197. The TOE provides Hashing capabilities in support of IPSec, TLS, and SSH: • Using 160, 256, 384, and 512 bits SHA, described in FIPS PUB 180-4. The TOE provides HMAC capabilities in support of IPsec, TLS, and SSH: • Using 160, 256, 384, and 512 bits HMAC-SHA, described in FIPS PUB 198-1. The TOE provides Key Exchange capabilities in support of IPsec, SSH, and TLS: • Using P-256, P-384, and P-521 EC Diffie-Hellmann. The TOE provides TLS Session Keys Derivation capabilities: • Using 256, 384, and 512 bits TLS KDF, described in NIST SP 800-135. The TOE provides SSH Session Key Derivation capabilities: • Using 128, 192, and 256 bits SSH KDF, described in NIST SP 800-135. The TOE provides IKE Session Key Derivation capabilities: • Using 128 and 256 bits IKE KDF, described in NIST SP 800-135.
FIA_ATD.1	The TOE can identify administrators by a unique ID and enforces their authentication before granting them access to any TSF management interfaces using a password. The TOE associates one of the following roles to each user: Admin, Operator, and Organization User. The TOE also associates the following login methods to each user: • Admin: VOS CLI or system shell • Operator: VOS CLI • Organization User: VOS CLI

TOE SFRs	How the SFR is Satisfied
FIA_UAU.1 FIA_UID.1	The TOE requires each administrator to be successfully identified and authenticated before access is granted to any management functions except viewing the login banner. Administrative access to the TOE is facilitated through the TOE's CLI (console or and management port), and through the external Versa Director via NETCONF and REST API. The NETCONF protocol is used for publishing configuration changes to VOS, while the REST API is used for read-only monitoring (e.g., GET methods). The TOE mediates all administrative actions through local or remote management interfaces. Once a potential administrative user attempts to access an administrative interface either locally or remotely, the TOE prompts the user for a username and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access can be provided to the administrative functionality of the TOE until an administrator is successfully identified and authenticated. The TOE interacts with peer VOS branches which authenticate to each other and to the VOS controller using IKE pre-shared keys or PKI certificates during IPsec tunnel establishment. Additionally, all interactions with the Versa Director (config updates, etc.) are authenticated using RSA public keypairs exchanged during the TOE installation process. The Director authenticates NETCONF using SSH public key authentication using the admin account, and REST API using the restuser built-in account.
FIA_UAU.5	The TOE is configured for several types of login access: • By using SSH to the Management Port (port 22); • NETCONF supported by SSH (port 2022); • REST API over HTTPS • Console Login, by connecting to the Console Port on the appliance or using Hypervisor Console view. The TOE may be configured for remote authentication by using AAA servers (RADIUS or TACACS+), which can be used for CLI login. AAA login may be used to authenticate administrators via username and password.
FIA_UAU.7	When an administrator enters their password at the local Console or at the SSH Login using command line, the password is not echoed back. The TOE displays only '*' characters so that the administrator password is obscured. For remote session authentication, the TOE does not echo any characters as they are entered by the administrator. If the administrator is using an SSH client to connect to the TOE directly, some SSH clients do not echo back dots, while other SSH clients do echo back dots so that the administrator password is obscured.

TOE SFRs	How the SFR is Satisfied
FIA_USB.1	Upon successful I&A, attributes are bound to the session for the duration of the session. Only administrators with Operator or Organization user role logging into the TOE system, will be dropped into Versa CLI by default. The Versa CLI is configured by administrators with Admin role, with the restricted commands that are allowed/disallowed for the administrators with Operator and Organization user role. Based on the role, the access control to management functions is enforced for the duration of the session that the user is logged in.
FMT_MOF.1	The privileges for management of security functions for each role are clearly defined and enforced by the TOE. All administrative accounts are assigned one role, and every role must at least possess the "read-only" privilege, so all accounts are able to read the audit logs and view-only status information. Abilities to disable, enable, determine, and modify configuration settings is determined by the roles (and the privileges therein) assigned to each account. These privileges apply only to the administrator accounts with Admin role, whereas accounts with Operator or Organization user role have none of these privileges.
FMT_MTD.1	The TOE provides the ability for authorized administrators, with Admin role, to access TOE data, such as audit data, configuration data, security attributes, routing tables, and session thresholds. TOE automatically determine the role of the administrator when the administrator logs in, granting access to the Admin role to manage the TSF data with full administrative access to the CLI. Organization users can manipulate data only for specific functions depending on the access attributes associated with their account.
FMT_SMF.1	The TOE is configured restrict the ability to perform privileged managing functions to authorized administrators with Admin role. Privileged managing functions are where the commands are available to configure TOE data (including saving configuration), configure administrator, restore factory default, delete configuration file, roll back configuration, and modify current admin password. The TOE is configured to restrict the ability to perform non-privileged managing functions to authorized administrators with roles Admin and Operator. Non-privileged managing functions are where the commands are available to perform a reboot, view configuration information, view log information, modify own admin password, and perform ping and traceroute tests.

TOE SFRs	How the SFR is Satisfied
FMT_SMR.1	When the administrator logs in, the TOE automatically determines the role of the administrator. When the administrator is created, the administrator will be mapped to one of the roles, Admin, Operator, or Organization user. The Admin role is recognized by: • the 'admin' or 'versa' system users, when local authentication is used, • the 'aaaadmin' user when AAA (TACACS+/RADIUS) authentication is used • Newly created local accounts with Admin role The Operator role is recognized by: • Newly created local accounts with Operator role, • the 'aaauser' user when AAA (TACACS+/RADIUS) authentication is used. The Organization User role may access the VOS CLI only and may view or edit configuration specific to their RBAC privilege. By default, the admin role has privilege to all VOS CLI, system shell, and REST API commands. Operators are granted read-only access to configuration data and may only run a limited subset of job operations on the VOS CLI. Organization users may perform functions associated with the RBAC privilege assigned and may only access the VOS CLI.
FPT_STM.1	The TOE is configured to provide a source of date and time information used in audit event timestamps. The default time zone of the TOE components is UTC. The TOE can optionally be set to receive clock updates from an NTP server. This date and time are used as the timestamp that is applied to TOE generated audit.
FPT_TUD_EXT.1	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.

TOE SFRs	How the SFR is Satisfied
FPT_TST.1	The TOE run a suite of self-tests during initial start-up, periodically, and at the request of the administrator during normal operation to verify its correct operation. Power-on self-tests are automatically invoked by start-up scripts. Periodic self- tests are run automatically by the daemons/commands (during key generation functions), as applicable. The following binaries are critical to the TSF and are verified during POST using RSA 2048 SHA-256 signatures against an image verification public key preinstalled on the TOE: • *Versa-dnsd* • *Versa-ntpd* • *Versa-vsmd* • *Versa-vmod* • *Versa-dhcpd* • *Versa-certd* • *Versa-rtd* • *Versa-l2cd* • *Libcrypto.so.1.1* • *Libssl.so.1.1.* • *Libfipstest.so* For the VOS Cryptographic Subsystem, the following test validation routines are performed: • AES Known-Answer Test • RSA Known-Answer Test • SHA Known-Answer Test • HMAC Known-Answer Test • DRBG Known-Answer Test • ECDH Known-Answer Test • ECDSA Pairwise Consistency Test • SSH KDF Known-Answer Test • IKE KDF Known-Answer Test • TLS KDF Known-Answer Test The following conditional tests are performed during key generation operations: • Conditional Test for RSA Key Generation • Conditional Test for ECDSA Key Generation • Conditional Test for ECC DH Public/Private Key Validation • DRBG Health Test • Conditional Test for DRBG • Entropy Test
FTA_SSL.3	An administrator can configure maximum inactivity times for both local and remote user sessions. When a session is inactive (i.e., no session input) for a configured period (default 5 minutes), the TOE will terminate the session, requiring the administrator to log in again to establish a new session when needed.
FTA_TAB.1	The TOE has the functionality to present warning information to an administrator when attempting to login to the CLI. There is no limit to the number of characters that can be entered in the login banner file.

FTP_ITC.1
FTP_TRP.1

During startup of the Branch appliance, an IPSec tunnel is established with the SD-WAN Controller. All communication between Versa VOS (Branch appliance) and the Versa Director/Analytics (Operational Environment) is sent via the IPSec tunnel.

The TOE supports establishing trusted paths between VOS Branch and Controller, using the protocols/formats described in the table below.

Source	Destination	Protocol / Format
Branch	Controller	IPSec.
Branch	Controller	BGP Routing information of current Branch within IPSec.
Controller	Branch	BGP Routing information of other Branches within IPSec.
Branch	Controller	Security Association Information of current Branch within IPSec.
Controller	Branch	Security Association information of other Branches within IPSec.

The TOE supports establishing trusted paths between VOS Branch and Director/Analytics, using the protocols/formats described in the table below.

Source	Destination	Protocol / Format
Branch / Controller	Analytics	IPFIX logs within IPSec.
Director	Branch	Configuration information in NETCONF format within SSH session within IPSec.
Director	Branch	Rest API calls using HTTPS session within IPSec.

The TOE supports establishing trusted paths between Controller and Director/Analytics, using the protocols/formats described in the table below.

Source	Destination	Protocol / Format
Director	Controller	Configuration information in NETCONF format within SSH session using Management Interface of Controller (to configure the Controller itself)
Director	Controller	Rest API calls using HTTPS session using Management Interface of Controller (to monitor the Controller itself)
Director	Controller	Configuration information in NETCONF format within SSH session using Control Interface of Controller which is routed over IPSec to Branch (to configure the Branch)
Director	Controller	Rest API calls using HTTPS session using Control Interface of Controller which is routed over IPSec to Branch (to monitor the Branch)
Controller	Analytics	IPFIX Logs during the operation of Controllers from Control Interface of Controller to Analytics
Controller	Analytics	IPFIX Logs from Branch Appliances (received via IPSec) routed using

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Satisfied</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td></td><td>Control Interface of Controller to Analytics</td></tr>
</table>
The TOE supports establishing trusted paths between itself and external AAA systems, using the protocols/formats described in the table below.
<table>
<tr><td>Source</td><td>Destination</td><td>Protocol / Format</td></tr>
<tr><td>Controller</td><td>RADIUS</td><td>RADIUS secured with IPsec or on protected private network</td></tr>
<tr><td>Controller</td><td>TACACS+</td><td>TACACS+ secured with IPsec or on protected private network</td></tr>
</table>
The NTP Server from both the Controller and Branch instances are protected with an authentication key and may also be protected via the same IPSec mechanism protecting other data plane traffic.
</td></tr>
</table>

Table 22: Implementation of SFRs