VERSA NETWORKS

VERSA SECURE SD-WAN
VERSA OPERATING SYSTEM (VOS) 22.1 RUNNING ON VERSA CSG1300, CSG1500, CSG2500, CSG3500, CSG5000, CSG5200, DELL POWEREDGE R7515, DELL POWEREDGE R7615, DELL POWEREDGE XR5610, DELL VEP1445, DELL VEP1485 AND DELL VEP4600, VERSA DIRECTOR 22.1 AND VERSA ANALYTICS 22.1

SECURITY TARGET

VERSION 2.0
JANUARY 23, 2025

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

LIST OF FIGURES

LIST OF TABLES

REVISION HISTORY

Version	Date	Summary of Changes
1.0	2022-12-02	First draft of the Security Target
1.1	2023-01-12	Addressed CCTL comments
1.2	2023-08-14	Adjusted SFR claims
1.3	2023-08-29	Updated for VPNGW v1.3
1.4	2023-09-11	Addressed CCTL comments
1.5	2023-10-19	NIAP check-in comments
1.6	2024-01-29	Addressed CCTL comments
1.7	2024-03-01	Addressed CCTL comments
1.8	2024-03-05	Addressed CCTL comments
1.9	2024-03-28	Addressed ECR comments
2.0	2025-01-23	Maintenance updates

ACRONYMS

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 Gateway
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

Abbreviation	Description
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
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 a shorthand phrase in parenthesis following the component identifier, (e.g. FMT_MTD.1/CryptoKeys).

Assumptions: TOE security environment assumptions are given names beginning with "A."

Threats: Threats to the TOE are given names beginning with "T."

Policies: TOE security environment policies are given names beginning with "P."

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE.", respectively.

All operations performed by the PP author are unmodified in this document and follow the same conventions as they appear in the source PP documents.

1. INTRODUCTION

1.1. ST AND TOE REFERENCES

The following table identifies the Security Target (ST).

Item	Identification
ST Title	Versa Networks Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on CSG1300, CSG1500, CSG2500, CSG3500, CSG5000, CSG5200, Dell PowerEdge R7515, Dell PowerEdge R7615, Dell PowerEdge XR5610, Dell VEP1445, Dell VEP1485, and Dell VEP4600 Versa Director 22.1, and Versa Analytics 22.1 Security Target
ST Version	2.0
ST Date	January 23, 2025
ST Author	Versa Networks, Inc.

Table 1: ST References

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

Item	Identification
TOE Identifier	Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on CSG1300, CSG1500, CSG2500, CSG3500, CSG5000, CSG5200, Dell PowerEdge R7515, Dell PowerEdge R7615, Dell PowerEdge XR5610, Dell VEP1445, Dell VEP1485, and Dell VEP4600 Versa Director 22.1, and Versa Analytics 22.1
TOE Platforms for VOS Branches	**Physical appliances:** Versa CSG1300 Versa CSG1500 Versa CSG2500 Versa CSG3500 Versa CSG5000 Versa CSG5200 Dell PowerEdge R7515 Dell PowerEdge R7615 Dell PowerEdge XR5610 Dell Virtual Edge Platform (VEP) 1445 Dell Virtual Edge Platform (VEP) 1485 Dell Virtual Edge Platform (VEP) 4600 **Virtual appliance:** Versa VOS VM on Ubuntu 18.04 with KVM
TOE Platforms for Versa Director, Versa Analytics and VOS SD-WAN Controller	**Virtual appliances:** Versa Director VM on ESXi 7.0 Versa Analytics VM on ESXi 7.0 Versa VOS SD-WAN Controller (VOS) VM on ESXi 7.0

Item	Identification
TOE Software Version	22.1

Table 2: TOE References

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

Item	Identification
CC Version	3.1 Revision 5
Protection Profile	CPP_ND_V2.2E
PP-Modules	MOD_VPNGW_V1.3, MOD_IPS_V1.0, MOD_CPP_FW_V1.4E
PP-Config	NDcPP-IPS-FW-VPNGW_V1.2

Table 3: CC and PP Conformance Claims

1.2. TOE Introduction

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

The solution consists of the following components:

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

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

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

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

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

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

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

- Centralized single-pane-of-glass configuration, management, and monitoring of the controllers, branch sites, and hub sites
- Lifecycle management of Versa VOS instances
- System-level high availability (HA) deployed as an active-standby pair for redundancy
- Staging server during the bootstrapping process
- Virtual network function manager (VNFM)
- Zero-touch provisioning (ZTP) of VOS devices at branch and hub sites

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

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

1.3. TOE Overview

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

The following figure shows a logical view of the placement of the Versa Secure SD-WAN distributed TOE components. TOE components are depicted with green boxes. Within the blue box is the TOE management component, comprising the VOS SD-WAN Controller, Director, and Analytics.

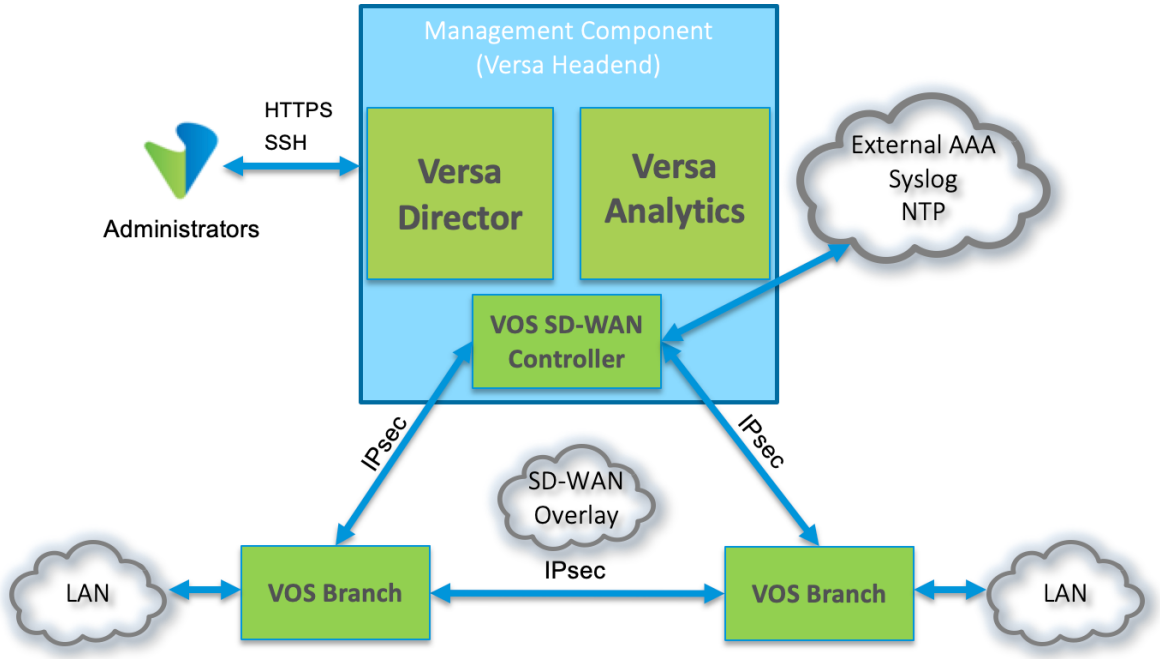

Figure 1: Versa solution

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

All Versa TOE components are built on a security-hardened Ubuntu 18.04 as the underlying OS.

1.3.1. TOE Deployment Use Cases

The TOE meets the following approved deployment use cases in the evaluated configuration:

- Both Virtual Network Device (vND) only and Physical Network Device (pND) as defined by CPP_ND_V2.2E. pND applies only to the Versa VOS Branch component when operating on the hardware identified in Table 2. All other components including the virtual VOS Branch follow the vND only use case.
- Distributed TOE (Distributed Network Devices plus Management Component required to fulfill cPP requirements) as defined by CPP_ND_V2.2E
    - The Versa Headend is the Management Component which is comprised of the Versa Director, Analytics and SD-WAN Controller services executing on a hypervisor and attached to an isolated internally protected communication link
- Remote Client Headend as defined by MOD_VPNGW_V1.2
- Stateful Traffic Filter Firewall as defined by MOD_CPP_FW_V1.4E
- Distributed System as defined by MOD_IPS_V1.0

1.3.2. Required non-TOE components

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

- a VM on a general-purpose x86 server running KVM on Ubuntu 18.04

For SD-WAN Controllers, Director and Analytics (Versa Headend):

- a VM on a general-purpose x86 server running ESXi 7.0

The following non-TOE systems must be deployed in the environment:

- Syslog server for audit forwarding for secured via IPsec
- NTP server for time synchronization for all TOE components secured via IPsec
- X.509 Public Key Infrastructure for certificate enrollment and revocation checking
- VPN client software (MacOS, Windows 11, Versa Secure Access client)
- Management workstation with native IPsec support for securing management traffic along with a standards-based web-browser and SSH client

1.4. PHYSICAL SCOPE

The solution is managed via a single instance of the Director, Analytics, and Controller, collectively comprising the Versa Headend.

One SD-WAN Controller is required per 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. In the evaluated configuration, a single SD-WAN Controller is utilized with three Branch devices.

1.4.1. TOE HARDWARE

The required TOE hardware for the Versa Headend (Director, Analytics, Controller) is a general-purpose x86 server capable of running ESXi 7.0 with a recommended 64GB or more of memory, a16-core CPU, and at least two 1-Gigabit Ethernet ports.

The TOE hardware for Versa Headend, VOS Branch physical and virtual network devices is comprised of the appliances as identified in Table 2: and described below.

The TOE appliances deliver carrier-grade reliability, high performance, and high compute capacity for enterprise-grade routing, SD-WAN, next-generation security, and uCPE scenarios. They are designed for deployment in large enterprise branches, campus sites, or data centers that require advanced secure SD-WAN along with comprehensive advanced application and cloud-intelligent SD-WAN services on premises.

The following figures depict the hardware appliances that are part of the physical ND TOE:

Figure 2: Dell Virtual Edge Platform (VEP) 1445 and VEP1485

Figure 3: Dell Virtual Edge Platform (VEP) 4600

Figure 4: Dell PowerEdge R7515

Figure 5: Dell PowerEdge XR5610

Figure 6: Dell PowerEdge R7615

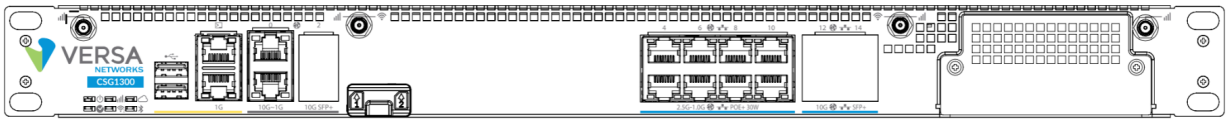

Figure 7: Versa CSG1300

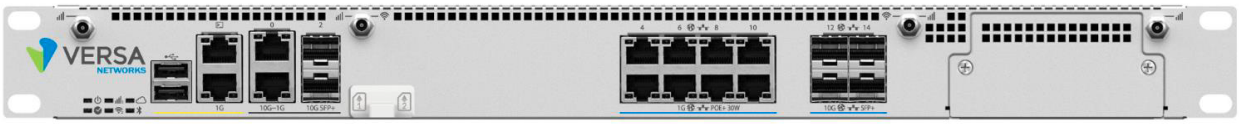

Figure 8: Versa CSG1500

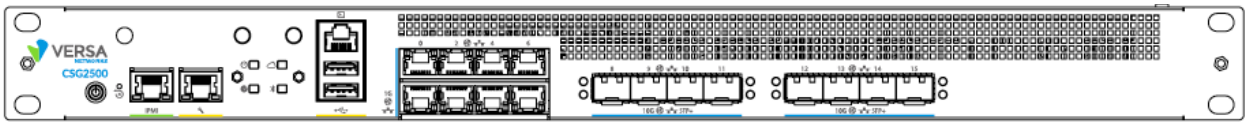

Figure 9: Versa CSG2500

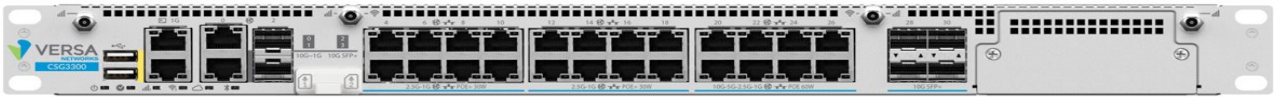

Figure 10: Versa CSG3500

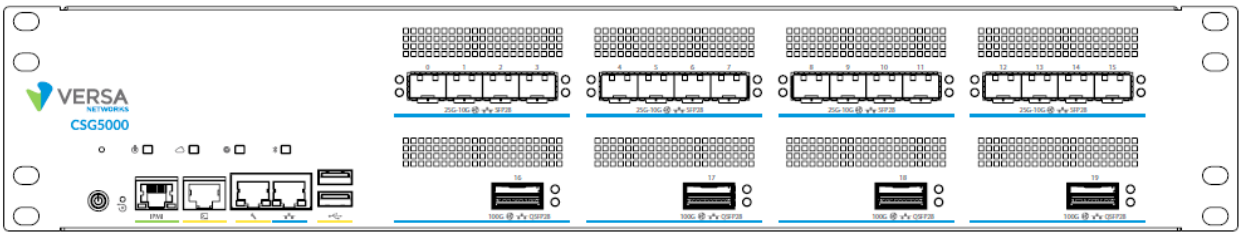

Figure 11: Versa CSG5000

Figure 12: Versa CSG5200

The CSG1000 series appliances come with at least one LAN and one WAN port, including Ethernet and non-Ethernet (ADSL2+/VDSL2 and T1/E1) interfaces and wireless (3G, 4G LTE, LTE Advanced, 5G, and WiFi access point) WAN and LAN access technologies. Non-Ethernet and Wireless interfaces are not included in the evaluation.

The CSG2500, CSG3500, CSG5000, CSG5200, Dell PowerEdge R7515, R7615, XR5610, VEP1445, VEP1485 and VEP4600 appliances come with at least one LAN and one WAN port, which may be 1-Gigabit Ethernet, SFP+ based 10-Gigabit Ethernet, QSFP28 based 100-Gigabit Ethernet, or SFP28 based 25-Gigabit Ethernet interfaces.

All appliances provide dedicated 1-Gigabit Management Ethernet ports and RJ-45 serial console ports. USB ports are utilized for manufacturing purposes only and are not functional during normal operation.

The below table provides detailed specifications for each TOE hardware model:

TOE Model	Specifications
CSG1300	**CPU**: Intel Atom C3958 **Disk**: 128GB SSD **Memory**: 32GB **Management port**: 1-Gigabit Ethernet **Data ports**: 2x 10GE RJ-45, 6x 10GE SFP+, 8x 1GE **Console port**: Rj-45 serial
CSG1500	**CPU:** Intel Xeon D2177NT **Memory:** 64GB **Disk:** 16GB + 256GB SSD **Management port:** 1-Gigabit Ethernet **Data ports:** 2x 10GE RJ-45, 6x 10GE SFP+, 8x 1GE Ethernet **Console port:** RJ-45 serial
CSG2500	**CPU:** Intel Xeon Gold 6252N **Memory:** 96GB **Disk:** 1TB SSD **Management port:** 2x 1-Gigabit Ethernet **Data ports:** 8x 10GE SFP+, 8x 1GE RJ-45 **Console port:** RJ-45 serial
CSG3500	**CPU:** Intel Xeon D2177NT **Memory:** 64GB **Disk:** 256GB SSD **Management port:** 1-Gigabit Ethernet **Data ports:** 2x 10GE SFP+, 4x 25/10GE SFP28, 16x 2.5GE RJ-45, 8x 10GE RJ-45, 2x 100GE QSFP28, 4x 25/10GE SFP28, 2x 10GE RJ-45 **Console port:** RJ-45 serial
CSG5000	**CPU:** AMD EPYC 7713P **Memory:** 256GB **Disk:** 1TB SSD **Management port:** 2x 1-Gigabit Ethernet **Data ports:** 16x 25/10GE SFP28, 4x 100GE QSFP28 **Console port:** RJ-45 serial
CSG5200	**CPU:** AMD EPYC 9654P **Memory:** 512GB **Disk:** 2TB SSD **Management port:** 2x 1-Gigabit Ethernet **Data ports:** 16x 10GE SFP28, 4x 100GE QSFP28 **Console port:** RJ-45 serial
CSG5250	**CPU:** AMD EPYC 9654P **Memory:** 512GB **Disk:** 2TB SSD **Management port:** 2x 1-Gigabit Ethernet **Data ports:** 8x 25/10GE SFP28, 6x 100GE QSFP128 **Console port:** RJ-45 serial

TOE Model	Specifications
Dell PowerEdge R7515-V2800	**CPU:** AMD EPYC 7713P **Memory:** 256GB **Disk:** 1TB SSD **Management port:** 1-Gigabit Ethernet **Data ports:** 8x 10GE SFP+, 4x 100GE QSFP **Console port:** RJ-45 serial
Dell PowerEdge R7615-V2900	**CPU:** AMD EPYC 9654P **Memory:** 512GB **Disk:** 1TB SSD **Management port:** 1-Gigabit Ethernet **Data ports:** 8x 10GE SFP+, 4x 100GE QSFP **Console port:** RJ-45 serial
Dell PowerEdge XR5610-V950	**CPU:** Intel Xeon Silver 4514Y **Memory:** 64GB **Disk**: 960GB SSD **Management port:** 1-Gigabit Ethernet **Data ports:** 8x 25/10GE SFP28, 4x 1GE RJ-45, 4x 10GE SFP (disabled) **Console port:** RJ-45 serial
Dell VEP1445-V220	**CPU:** Intel Atom C3758 **Disk:** 240GB SSD **Memory:** 16GB **Management port:** 1-Gigabit Ethernet **Data ports:** 2x 10GE SFP+, 5x 1GE RJ-45 **Console port:** microUSB
Dell VEP1485-V240	**CPU:** Intel Atom C3958 **Disk:** 240GB SSD **Memory:** 32GB **Management port:** 1-Gigabit Ethernet **Data ports:** 2x 10GE SFP+, 5x 1GE RJ-45 **Console port:** microUSB
Dell VEP4600-V900	**CPU:** Intel Xeon D 2187NT **Memory:** 64GB **Disk:** 960GB SSD **Management port:** 2x 1-Gigabit Ethernet **Data ports:** 6x SFP+ 10GE, 4x 1GE **Console port:** RJ-45 serial
Versa Headend (as evaluated)	**CPU:** Intel Xeon-D 1587 **OS:** ESXi 7.0 **Memory:** 64GB **Disk:** 1TB SSD **Management port:** 1-Gigabit Ethernet **Data ports:** 2x 1-Gigabit Ethernet **Console port:** RJ-45 serial
Versa VOS (virtual Branch)	**CPU:** Intel Xeon-D 1587 **OS:** Ubuntu 18.04 with KVM **Memory:** 64GB **Disk:** 1TB SSD **Management port:** 1-Gigabit Ethernet **Data ports:** 2x 1-Gigabit Ethernet **Console port:** RJ-45 serial

Table 4: TOE Hardware

1.4.2. TOE SOFTWARE

The TOE software comprises of the following:

- Versa Director, Analytics, and SD-WAN Controller virtual appliance version 22.1 hosted on ESXi 7.0
- Versa VOS Branch virtual appliance version 22.1 hosted on KVM Hypervisor on Ubuntu 18.04
- Versa VOS Branch version 22.1 image installed on bare metal TOE hardware appliances in Table 2:

The TOE is a distributed TOE with the boundary encompassing the bare metal appliances in Table 2: with the VOS software image described in the above list. For virtual appliances, the boundary encompasses only the virtual appliance software image and not the virtualization system or underlying hardware. The TOE software images include a hardened Ubuntu 18.04 as the underlying OS.

1.4.3. LOGICAL SCOPE

The Versa VOS TOE is comprised of several security features:

1. Security Audit
2. Communications
3. Cryptographic Support
4. User Data Protection
5. Firewall
6. Identification and Authentication
7. Security Management
8. Packet Filtering
9. Protection of the TOE Security Functionality (TSF)
10. TOE Access
11. Trusted Path/Channels
12. Intrusion Prevention

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

1.4.3.1. SECURITY AUDIT

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

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

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

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

1.4.3.2. COMMUNICATIONS

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

1.4.3.3. CRYPTOGRAPHIC SUPPORT

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

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

1.4.3.4. USER DATA PROTECTION

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

1.4.3.5. FIREWALL

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

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

1.4.3.6. IDENTIFICATION AND AUTHENTICATION

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

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

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

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

1.4.3.7. SECURITY MANAGEMENT

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

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

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

1.4.3.8. PACKET FILTERING

The TOE supports a packet filtering policy as described in 1.4.3.5 above.

1.4.3.9. PROTECTION OF THE TOE SECURITY FUNCTIONALITY (TSF)

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

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

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

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

1.4.3.10. TOE ACCESS

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

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

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

1.4.3.11. TRUSTED PATH/CHANNELS

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

1.4.3.12. INTRUSION PREVENTION

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

1.4.4. DOCUMENTATION

The TOE includes the following documentation:

- Versa Operating System (VOS), Versa Director and Versa Analytics Version 22.1 Common Criteria Hardening Guide

1.4.5. TOE EVALUATED CONFIGURATION

The TOE is evaluated using the following configuration settings:

- Administrator credentials are authenticated by the TOE against a local database.
- 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 in addition to remote logging to an external audit server.
- FIPS mode enabled

The following features are excluded from the evaluated configuration:

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

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, conformant
Part 3 of the ISO/IEC 15408 international standard	Common Criteria security assurance components, April 2017, Version 3.1, Revision 5, conformant
Protection Profiles	collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E)
PP-Modules	• PP-Module for Intrusion Protection Systems (IPS), Version 1.0 (MOD_IPS_V1.0) • PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625 (MOD_FW_1.4E) • PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3 (MOD_VPNGW_1.3
PP-Config	PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways v1.2

Table 5: Conformance Claims

2.1. TECHNICAL DECISIONS

The following NIAP Technical Decisions are applicable to the TOE:

NIAP Technical Decisions	Applicable (Y/N)
0813 – GCM Nonce Reuse Test for MOD_VPNGW • References: Section 2.1.1.1	No
0811 – Correction to Referenced SFR in FIA_PSK_EXT.3 Test • References: FIA_PSK_EXT.3, MOD_VPNGW_V1.3-SD	No
0800: Updated NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance • References: FCS_IPSEC_EXT.1.7, FCS_IPSEC_EXT.1.8, CPP_ND_V2.2-SD	Yes
0792 – NIT Technical Decision: FIA_PMG_EXT.1 - TSS EA not in line with SFR • References: FIA_PMG_EXT.1, CPP_ND_V2.2-SD	Yes
0790 – NIT Technical Decision: Clarification Required for Testing IPv6 • References: FCS_DTLSC_EXT.1.2, FCS_TLSC_EXT1.2, CPP_ND_V2.2-SD	No
0781 – Correction to FIA_PSK_EXT.3 EA for MOD_VPNGW_v1.3 • References: FIA_PSK_EXT.3	No
0738 – NIT Technical Decision for Link to Allowed-With List • References: Chapter 2	Yes
0722 – IPS_SBD_EXT.1.1 EA Correction • References: IPS_SBD_EXT.1.1	Yes
0670 – NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing • References: ND SD2.2, FCS_TLSC_EXT.2.1	No

0639 – NIT Technical Decision for Clarification for NTP MAC Keys • References: FCS_NTP_EXT.1.2, FAU_GEN.1, FCS_CKM.4, FPT_SKP_EXT.1	Yes
0638 – NIT Technical Decision for Key Pair Generation for Authentication • References: NDSDv2.2, FCS_CKM.1	Yes
0636 – NIT Technical Decision for Clarification of Public Key User Authentication for SSH • References: ND SD2.2, FCS_SSHC_EXT.1	No
0635 – NIT Technical Decision for TLS Server and Key Agreement Parameters • References: FCS_TLSS_EXT.1.3, NDSD v2.2	Yes
0632 – NIT Technical Decision for Consistency with Time Data for vNDs • References: ND SD2.2, FPT_STM_EXT.1.2	Yes
0631 – NIT Technical Decision for Clarification of public key authentication for SSH Server • References: ND SDv2.2, FCS_SSHS_EXT.1, FMT_SMF.1	Yes
0595 – Administrative corrections to IPS PP-Module • References: FAU_GEN.1.1/IPS, Table 4	Yes
0592 – NIT Technical Decision for Local Storage of Audit Records • References: FAU_STG	Yes
0591 – NIT Technical Decision for Virtual TOEs and hypervisors • References: A.LIMITED_FUNCTIONALITY, ACRONYMS	Yes
0581 – NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3 • References: FCS_CKM.2	Yes
0580 – NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e • References: FCS_CKM.1.1, FCS_CKM.2.1	Yes
0572 – NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers • References: FTP_ITC.1	Yes
0571 – NiT Technical Decision for Guidance on how to handle FIA_AFL.1 • References: FIA_UAU.1, FIA_PMG_EXT.1	Yes
0570 – NiT Technical Decision for Clarification about FIA_AFL.1 • References: FIA_AFL.1	Yes
0569 – NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7 • References: ND SD v2.2, FCS_DTLSS_EXT.1.7, FCS_TLSS_EXT.1.4	Yes
0564 – NiT Technical Decision for Vulnerability Analysis Search Criteria • References: NDSDv2.2, AVA_VAN.1	Yes
0563 – NiT Technical Decision for Clarification of audit date information • References: NDcPPv2.2e, FAU_GEN.1.2	Yes

0556 – NIT Technical Decision for RFC 5077 question • References: NDSDv2.2, FCS_TLSS_EXT.1.4, Test 3	Yes
0555 – NIT Technical Decision for RFC Reference incorrect in TLSS Test • References: NDSDv2.2, FCS_TLSS_EXT.1.4, Test 3	Yes
0551 – NIT Technical Decision for Incomplete Mappings of OEs in FW Module v1.4+Errata • References: Sections 5.3.2 and 5.3.4	Yes
0547 – NIT Technical Decision for Clarification on developer disclosure of AVA_VAN • References: ND SDv2.1, ND SDv2.2, AVA_VAN.1	Yes
0546 – NIT Technical Decision for DTLS - clarification of Application Note 63 • References: FCS_DTLSC_EXT.1.1	No
0545 – NIT Technical Decision for Conflicting FW rules cannot be configured (extension of RfI#201837) • References: FWMOD SD v1.3, FWMOD SD v1.4e, FFW_RUL_EXT.1.8	Yes
0537 – NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3 • References: FIA_X509_EXT.2.2	Yes
0536 – NIT Technical Decision for Update Verification Inconsistency • References: AGD_OPE.1, ND SDv2.1, ND SDv2.2	Yes
0528 – NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4 • References: FCS_NTP_EXT.1.4, ND SD v2.1, ND SD v2.2	Yes
0527 – Updates to Certificate Revocation Testing (FIA_X509_EXT.1) • References: FIA_X509_EXT.1/REV, FIA_X509_EXT.1/ITT	Yes

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

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

Threat	Threat Description
T.UNAUTHORIZED_ ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_ COMMUNICATION_ CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.WEAK_AUTHENTICATION_ ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.

Threat	Threat Description
T.SECURITY_ FUNCTIONALITY_ COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_ FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.DATA_INTEGRITY (VPNGW)	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to modify the data without authorization. If known malicious external devices are able to communicate with devices on the protected network or if devices on the protected network can communicate with those external devices then the data contained within the communications may be susceptible to a loss of integrity.
T.NETWORK_ACCESS (VPNGW + FW +IPS)	**VPNGW** Devices located outside the protected network may seek to exercise services located on the protected network that are intended to only be accessed from inside the protected network or only accessed by entities using an authenticated path into the protected network. Devices located outside the protected network may, likewise, offer services that are inappropriate for access from within the protected network. From an ingress perspective, VPN gateways can be configured so that only those network servers intended for external consumption by entities operating on a trusted network (e.g., machines operating on a network where the peer VPN gateways are supporting the connection) are accessible and only via the intended ports. This serves to mitigate the potential for network entities outside a protected network to access network servers or services intended only for consumption or access inside a protected network. From an egress perspective, VPN gateways can be configured so that only specific external services (e.g., based on destination port) can be accessed from within a protected network, or moreover are accessed via an encrypted channel. For example, access to external mail services can be blocked to enforce corporate policies against accessing uncontrolled email servers, or, that access to the mail server must be done over an encrypted link. **FW** With knowledge of the services that are exported by machines on a subnet, an attacker may attempt to exploit those services by mounting attacks against those services. **IPS** Unauthorized access may be achieved to services on a protected network from outside that network, or alternately services outside a protected network from inside the protected network. If malicious external devices are able to communicate with devices on the protected network via a backdoor then those devices may be susceptible to the unauthorized disclosure of information.
T.NETWORK_DISCLOSURE (VPNGW + FW + IPS)	**VPNGW**

Threat	Threat Description
	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If known malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices (e.g., as a result of a phishing episode or by inadvertent responses to email messages), then those internal devices may be susceptible to the unauthorized disclosure of information. From an infiltration perspective, VPN gateways serve not only to limit access to only specific destination network addresses and ports within a protected network, but whether network traffic will be encrypted or transmitted in plaintext. With these limits, general network port scanning can be prevented from reaching protected networks or machines, and access to information on a protected network can be limited to that obtainable from specifically configured ports on identified network nodes (e.g., web pages from a designated corporate web server). Additionally, access can be limited to only specific source addresses and ports so that specific networks or network nodes can be blocked from accessing a protected network thereby further limiting the potential disclosure of information. From an exfiltration perspective, VPN gateways serve to limit how network nodes operating on a protected network can connect to and communicate with other networks limiting how and where they can disseminate information. Specific external networks can be blocked altogether or egress could be limited to specific addresses or ports. Alternately, egress options available to network nodes on a protected network can be carefully managed in order to, for example, ensure that outgoing connections are encrypted to further mitigate inappropriate disclosure of data through packet sniffing. **FW** An attacker may attempt to "map" a subnet to determine the machines that reside on the network, and obtaining the IP addresses of machines, as well as the services (ports) those machines are offering. This information could be used to mount attacks to those machines via the services that are exported. **IPS** Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions.
T.NETWORK_MISUSE (VPNGW + FW + IPS)	**VPNGW** Devices located outside the protected network, while permitted to access particular public services offered inside the protected network, may attempt to conduct inappropriate activities while communicating with those allowed public services. Certain services offered from within a protected network may also represent a risk when accessed from outside the protected network. From an ingress perspective, it is generally assumed that entities operating on external networks are not bound by the use policies for a given protected network. Nonetheless, VPN gateways can log policy violations that might indicate violation of publicized usage statements for publicly available services. From an egress perspective, VPN gateways can be configured to help enforce and monitor protected network use policies. As explained in the other threats, a VPN gateway can serve to limit dissemination of data, access to external servers, and even disruption of services – all of these could be related to the use policies of a protected network and as such are subject in some regards to enforcement. Additionally, VPN gateways can be configured to log network usages that cross between protected and external networks and as a result can serve to identify potential usage policy violations.

Threat	Threat Description
	FW An attacker may attempt to use services that are exported by machines in a way that is unintended by a site's security policies. For example, an attacker might be able to use a service to "anonymize" the attacker's machine as they mount attacks against others. **IPS** Access to services made available by a protected network might be used counter to operational environment policies. Devices located outside the protected network may attempt to conduct inappropriate activities while communicating with allowed public services (e.g. manipulation of resident tools, SQL injection, phishing, forced resets, malicious zip files, disguised executables, privilege escalation tools, and botnets)
T.REPLAY_ATTACK (VPNGW)	If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a "replay" attack. This method of attack allows the individual to capture packets traversing throughout the network and send the packets at a later time, possibly unknown by the intended receiver. Traffic is subject to replay if it meets the following conditions: • Cleartext: an attacker with the ability to view unencrypted traffic can identify an appropriate segment of the communications to replay as well in order to cause the desired outcome • No integrity: alongside cleartext traffic, an attacker can make arbitrary modifications to captured traffic and replay it to cause the desired outcome if the recipient has no means to detect these
T.MALICIOUS_TRAFFIC (FW)	An attacker may attempt to send malformed packets to a machine in hopes of causing the network stack or services listening on UDP/TCP ports of the target machine to crash.
T.NETWORK_DOS (IPS)	Attacks against services inside a protected network, or indirectly by virtue of access to malicious agents from within a protected network, might lead to denial of services otherwise available within a protected network.

Table 6: 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.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.
P.ANALYZE (IPS)	Analytical processes and information to derive conclusions about potential intrusions must be applied to IPS data and appropriate response actions taken.

Table 7: 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.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). f a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.
A.NO_THRU_TRAFFIC_ PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

Assumptions	Description
A.ADMIN_CREDENTIALS_ SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.VS_TRUSTED_ ADMINISTRATOR (applies to vNDs only)	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
A.VS_REGULAR_UPDATES (applies to vNDs only)	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.VS_ISOLATION	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
A.VS_CORRECT_ CONFIGURATION	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.
A.CONNECTIONS (VPNGW + IPS)	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE's security policies will be enforced on all applicable network traffic flowing among the attached networks.

Table 8: 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.ADDRESS_FILTERING (VPNGW)	To address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services, and network-based reconnaissance, compliant TOE's will implement packet filtering capability. That capability will restrict the flow of network traffic between protected networks and other attached networks based on network addresses of the network nodes originating (source) or receiving (destination) applicable network traffic as well as on established connection information. Addressed by: FPF_RUL_EXT.1, FTA_VCM_EXT.1 (optional)
O.AUTHENTICATION (VPNGW)	To further address the issues associated with unauthorized disclosure of information, a compliant TOE's authentication ability (IPSec) will allow a VPN peer to establish VPN connectivity with another VPN peer and ensure that any such connection attempt is both authenticated and authorized. VPN endpoints authenticate each other to ensure they are communicating with an authorized external IT entity. Addressed by: FCS_IPSEC_EXT.1 (refined from Base-PP), FIA_X509_EXT.1/Rev (from Base-PP), FIA_X509_EXT.2 (refined from Base-PP), FIA_X509_EXT.3 (from Base-PP), FTP_ITC.1/VPN, FPF_MFA_EXT.1 (optional), FTA_SSL.3/VPN (optional), FTA_TSE.1 (optional), FCS_EAP_EXT.1 (selection-based), FIA_HOTP_EXT.1 (selection-based), FIA_PSK_EXT.1 (selection-based), FIA_PSK_EXT.2 (selection-based), FIA_PSK_EXT.3 (selection-based), FIA_PSK_EXT.4 (selection-based), FIA_PSK_EXT.5 (selection-based), FIA_TOTP_EXT.1 (selection-based)
O.CRYPTOGRAPHIC_ FUNCTIONS (VPNGW)	To address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption of services, and network-based reconnaissance, compliant TOE's will implement cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the TOE. Addressed by: FCS_COP.1/DataEncryption (refined from Base-PP), FCS_IPSEC_EXT.1 (refined from Base-PP), FCS_CKM.1/IKE, FCS_EAP_EXT.1 (selection-based), FIA_PSK_EXT.1 (selection-based), FIA_PSK_EXT.2 (selection-based).
O.FAIL_SECURE (VPNGW)	There may be instances where the TOE's hardware malfunctions or the integrity of the TOE's software is compromised, the latter being due to malicious or non-malicious intent. To address the concern of the TOE operating outside of its hardware or software specification, the TOE will shut down upon discovery of a problem reported via the self-test mechanism and provide signature-based validation of updates to the TSF. Addressed by: FPT_TST_EXT.1 (refined from Base-PP), FPT_TUD_EXT.1 (refined from Base-PP), FPT_FLS.1/SelfTest, FPT_TST_EXT.3

Security Objectives	Description
O.PORT_FILTERING (VPNGW)	To further address the issues associated with unauthorized disclosure of information, etc., a compliant TOE's port filtering capability will restrict the flow of network traffic between protected networks and other attached networks based on the originating (source) or receiving (destination) port (or service) identified in the network traffic as well as on established connection information. Addressed by: FPF_RUL_EXT.1
O.SYSTEM_MONITORING (VPNGW)	To address the issues of administrators being able to monitor the operations of the VPN gateway, it is necessary to provide a capability to monitor system activity. Compliant TOEs will implement the ability to log the flow of network traffic. Specifically, the TOE will provide the means for administrators to configure packet filtering rules to 'log' when network traffic is found to match the configured rule. As a result, matching a rule configured to 'log' will result in informative event logs whenever a match occurs. In addition, the establishment of security associations (SAs) is auditable, not only between peer VPN gateways, but also with certification authorities (CAs). Addressed by: FAU_GEN.1/VPN, FPF_RUL_EXT.1
O.TOE_ADMINISTRATION (VPNGW)	TOEs will provide the functions necessary for an administrator to configure the packet filtering rules, as well as the cryptographic aspects of the IPsec protocol that are enforced by the TOE. Addressed by: FMT_MTD.1/CryptoKeys (refined from Base-PP), FMT_SMF.1/VPN
O.RESIDUAL_ INFORMATION (FW)	The TOE shall implement measures to ensure that any previous information content of network packets sent through the TOE is made unavailable either upon deallocation of the memory area containing the network packet or upon allocation of a memory area for a newly arriving network packet or both. The requirements on making residual information of network packets unavailable are defined in FDP_RIP.2.The SFR completely covers the objective.
O.STATEFUL_ TRAFFIC_FILTERING (FW)	The TOE shall perform stateful traffic filtering on network packets that it processess. For this the TOE shall support the definition of stateful traffic filtering rules that allow to permit or drop network packets. The TOE shall support assignment of the stateful traffic filtering rules to each distinct network interface. The TOE shall support the processing of the applicable stateful traffic filtering rules in an administratively defined order. The TOE shall deny the flow of network packets if no matching stateful traffic filtering rule is identified. Depending on the implementation, the TOE might support the stateful traffic filtering of Dynamic Protocols (optional). The requirements on performing stateful traffic filtering on network packets, the support of the definition of stateful traffic filtering rules, the assignment of the stateful traffic filtering rules to each distinct network interface, the processing of the applicable stateful traffic filtering rules in an administratively defined order and on denying the flow of network packets if no matching stateful traffic filtering rule is identified are defined in FFW_RUL_EXT.1. The requirements on stateful traffic filtering of Dynamic Protocols are defined in FFW_RUL_EXT.2 (optional). The requirement on providing the ability to define firewall rules is defined in FMT_SMF.1/FFW.

Security Objectives	Description
O.IPS_ANALYZE (IPS)	Entities that reside on or communicate across monitored networks must have network activity effectively analyzed for potential violations of approved network usage. The TOE must be able to effectively analyze data collected from monitored networks to reduce the risk of unauthorized disclosure of information, inappropriate access to services, and misuse of network resources. Addressed by: IPS_ABD_EXT.1, IPS_IPB_EXT.1, IPS_NTA_EXT.1, IPS_SBD_EXT.1, FPT_FLS.1 (optional), IPS_SBD_EXT.2 (optional), FRU_RSA.1 (implementation-dependent)
O.IPS_REACT (IPS)	The TOE must be able to react in real-time as configured by the Security Administrator to terminate and block traffic flows that have been determined to violate administrator-defined IPS policies. Addressed by: IPS_ABD_EXT.1, IPS_SBD_EXT.1, FAU_ARP.1 (objective)
O.SYSTEM_MONITORING (IPS)	To be able to analyze and react to potential network policy violations, the IPS must be able to collect and store essential data elements of network traffic on monitored networks. Addressed by: FAU_GEN.1/IPS, FAU_STG.1/IPS (optional), FAU_STG.4 (optional), FAU_SAR.1 (objective), FAU_SAR.2 (objective), FAU_SAR.3 (objective)
O.TOE_ADMINISTRATION (IPS)	To address the threat of unauthorized administrator access that is defined in the Base-PP, conformant TOEs will provide the functions necessary for an administrator to configure the IPS capabilities of the TOE. Addressed by: FMT_SMF.1/IPS

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.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_ PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
OE.NO_THRU_TRAFFIC _PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.

Security Objectives	Description
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_ CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.COMPONENTS_ RUNNING	For distributed TOEs, the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.
OE.RESIDUAL_ INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.
OE.VM_ CONFIGURATION (applies to vNDs only)	For vNDs, the Security Administrator ensures that the VS and VMs are configured to • reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and • correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting). The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualisation features such as cloning, save/restore, suspend/resume, and live migration. If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.
OE.CONNECTIONS (VPNGW + IPS)	The TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

Table 9: Security Objectives for the Operational Environment

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 Extended Components Definition is defined in the PP and PP-Modules claimed by the TOE and is not reproduced here. No additional Extended Components are applicable beyond those prescribed by the PP and its PP-Modules.

6. Security Requirements

6.1. Security Functional Requirements (SFRs)

Functional Class	Functional Component	
FAU: Security Audit	FAU_GEN.1	Audit data generation
	FAU_GEN.1/IPS	Audit data generation (IPS)
	FAU_GEN.1/VPN	Audit data generation (VPN gateway)
	FAU_GEN_EXT.1	Security audit data generation for distributed TOEs
	FAU_GEN.2	User identity association
	FAU_STG.1	Protected audit trail storage
	FAU_STG_EXT.1	Protected audit event storage
	FAU_STG_EXT.4	Protected local audit event storage for distributed TOEs
	FAU_STG_EXT.5	Protected remote audit event storage for distributed TOEs
FCO: Communication	FCO_CPC_EXT.1	Component registration channel definition
FCS: Cryptographic support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.1/IKE	Cryptographic key generation (for IKE peer authentication)
	FCS_CKM.2	Cryptographic key establishment
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1/ DataEncryption	Cryptographic operation (AES data encryption and decryption)
	FCS_COP.1/Sig Gen	Cryptographic operation (Digital signature generation and verification)
	FCS_COP.1/Hash	Cryptographic operation (Hashing)
	FCS_COP.1/ KeyedHash	Cryptographic operation (Keyed-hash algorithm)
	FCS_IPSEC_EXT.1	IPsec protocol
	FCS_HTTPS_EXT.1	HTTPS protocol
	FCS_NTP_EXT.1	NTP protocol
	FCS_RBG_EXT.1	Random bit generation

Functional Class	Functional Component	
	FCS_SSHS_EXT.1	SSH server protocol
	FCS_TLSS_EXT.1	TLS server protocol with mutual authentication
FDP: User Data Protection	FDP_RIP.2	Full residual information protection
FFW: Firewall	FFW_RUL_EXT.1	Stateful traffic filter firewall
FIA: Identification and authentication	FIA_AFL.1	Authentication failure management
	FIA_PMG_EXT.1	Password management
	FIA_UIA_EXT.1	User identification and authentication
	FIA_UAU_EXT.2	Password-based authentication mechanism
	FIA_X509_EXT.1/ Rev	X.509 certificate validation
	FIA_X509_EXT.2	X.509 certificate authentication
	FIA_X509_EXT.3	X.509 certificate requests
FMT: Security management	FMT_MOF.1/ Functions	Management of security functions behavior
	FMT_MOF.1/ ManualUpdate	Management of security functions behavior
	FMT_MOF.1/ Services	Management of security functions behavior
	FMT_MTD.1/ CryptoKeys	Management of TSF data
	FMT_MTD.1/ CoreData	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMF.1/FFW	Specification of management functions
	FMT_SMF.1/IPS	Specification of management functions
	FMT_SMF.1/VPN	Specification of management functions
	FMT_SMR.2	Restrictions on security roles
FPF: Packet Filtering	FPF_RUL_EXT.1	Packet filtering rules
FPT: Protection of the TSF	FPT_APW_EXT.1	Protection of Administrator passwords
	FPT_FLS.1/ SelfTest	Failure with preservation of secure state (self-test failures)

Functional Class	Functional Component	
	FPT_SKP_EXT.1	Protection of TSF data (for reading of all pre-shared, symmetric and private keys)
	FPT_STM_EXT.1	Reliable time stamps
	FPT_TUD_EXT.1	Trusted update
	FPT_TST_EXT.1	TSF testing
	FPT_TST_EXT.3	Self-test with defined methods
FTA: TOE access	FTA_SSL_EXT.1	TSF-initiated session locking
	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
	FTA_TAB.1	Default TOE access banners
FTP: Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_ITC.1/VPN	Inter-TSF trusted channel (VPN communications)
	FTP_TRP.1	Trusted path
IPS: Intrusion Prevention	IPS_ABD_EXT.1	Anomaly-based IPS functionality
	IPS_IPB_EXT.1	IP blocking
	IPS_NTA_EXT.1	Network traffic analysis
	IPS_SBD_EXT.1	Signature-based IPS functionality

Table 10: Security Functional Requirements

6.1.1. SECURITY AUDIT (FAU)

6.1.1.1. FAU_GEN.1 AUDIT DATA GENERATION

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) *All administrative actions comprising:*

- *Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).*
- *Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*

- *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
- *Resetting passwords (name of related user account shall be logged).*
- ***[Starting and stopping of services.]***

d) Specifically defined auditable events in **the table in FAU_GEN.1.2**.

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 cPP/ST, *information specified in column three of* ***the table below***.

SFR	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_GEN_EXT.1	None.	None.
FAU_STG.1	None.	None.
FAU_STG_EXT.1	None.	None.
FAU_STG_EXT.4	None.	None.
FAU_STG_EXT.5	None.	None.
FCO_CPC_EXT.1	• Enabling communications between a pair of components. • Disabling communications between a pair of components.	Identities of the endpoint pairs enabled or disabled.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/ DataEncryption	None.	None.
FCS_COP.1/ SigGen	None.	None.
FCS_COP.1/ Hash	None.	None.
FCS_COP.1/ KeyedHash	None.	None.

SFR	Auditable Events	Additional Audit Record Contents
FCS_HTTPS_EXT.1	Failure to establish a HTTPs session.	Reason for failure.
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.
FCS_NTP_EXT.1	• Configuration of a new time server. • Removal of configured time server.	Identity if new/removed time server.
FCS_RBG_EXT.1	None.	None.
FCS_SSHS_EXT.1	• Failure to establish an SSH session.	Reason for failure.
FCS_TLSS_EXT.1	• Failure to establish a TLS session	Reason for failure.
FDP_RIP.2	None.	None.
FFW_RUL_EXT.1	Application of rules configured with the 'log' operation.	• Source and destination addresses • Source and destination ports • Transport Layer Protocol • TOE Interface
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/ Rev	• Unsuccessful attempt to validate a certificate • Any addition, replacement or removal of trust anchors in the TOE's trust store	• Reason for failure of certificate validation • Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
FIA_X509_EXT.2	None.	None.

SFR	Auditable Events	Additional Audit Record Contents
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ Functions	None.	None.
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update.	None.
FMT_MOF.1/ Services	None.	None.
FMT_MTD.1/ CoreData	None.	None.
FMT_MTD.1/ CryptoKeys	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMF.1/FFW	All management activities of TSF data (including creation, modification and deletion of firewall rules).	None.
FMT_SMR.2	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update (success or failure)	None.
FPT_STM_EXT.1	Discontinuous changes to time – either Administrator actuated or changed via an automated process.	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.

SFR	Auditable Events	Additional Audit Record Contents
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	• Initiation of the trusted channel. • Termination of the trusted channel. • Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1	• Initiation of the trusted path. • Termination of the trusted path. • Failure of the trusted path functions.	None.

Table 11: Audit Events

6.1.1.2. FAU_GEN.1/IPS AUDIT DATA GENERATION (IPS)

FAU_GEN.1.1/IPS The TSF shall be able to generate an IPS audit record of the following IPS auditable events:

a) Start-up and shut-down of the **IPS** functions;
b) All **IPS** auditable events for the [not specified] level of audit; and
c) [*All dissimilar IPS events;*
d) *All dissimilar IPS reactions;*
e) *Totals of similar events occurring within a specified time period;*
f) *Totals of similar reactions occurring within a specified time period;*
g) *The events in **the table in FAU_GEN.1.2/IPS**.*
h) *[no other auditable events]*].

FAU_GEN.1.2/IPS The TSF shall record within each **IPS auditable event** record at least the following information:

a) *Date and time of the event, type of event **and/or reaction**, ~~subject identity, and the outcome (success or failure) of the event~~; and;*

b) *For each **IPS** audit**able** event type, based on the auditable event definitions of the functional components included in the PP~~/ST~~, [information specified in column three of **the table below**].*

SFR	Auditable Events	Additional Audit Record Contents
FMT_SMF.1/IPS	Modification of an IPS policy element.	Identifier or name of the modified IPS policy element (e.g. which signature, baseline, or known- good/known-bad list was modified).

SFR	Auditable Events	Additional Audit Record Contents
IPS_ABD_EXT.1	Inspected traffic matches an anomaly-based IPS policy.	• Source and destination IP addresses. • The content of the header fields that were determined to match the policy. • TOE interface that received the packet. • Aspect of the anomaly-based IPS policy rule that triggered the event (e.g. throughput, time of day, blocking notification to firewall).
IPS_IPB_EXT.1	Inspected traffic matches a list of known-good or known-bad addresses applied to an IPS policy.	• Source and destination IP addresses (and, if applicable, indication of whether the source and/or destination address matched the list. • TOE interface that received the packet. • Network-based action by the TOE (e.g. allowed, blocked, sent reset).
IPS_NTA_EXT.1	• Modification of which IPS policies are active on a TOE interface • Enabling/disabling a TOE interface with IPS policies applied. • Modification of which mode(s) is/are active on a TOE interface	• Identification of the TOE interface • The IPS policy and interface mode (if applicable)
IPS_SBD_EXT.1	Inspected traffic matches a signature-based IPS rule with logging enabled.	• Name or identifier of the matched signature. • Source and destination IP addresses. • The content of the header fields that were determined to match the signature. • TOE interface that received the packet. • Network-based action by the TOE (e.g. allowed, blocked, sent reset).

Table 12: IPS Events

6.1.1.3. FAU_GEN.1/VPN Audit Data Generation (VPN Gateway)

FAU_GEN.1.1/VPN 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) Indication that TSF self-test was completed

c) Failure of self-test

d) All auditable events for the [*not specified*] level of audit; and

e) [*auditable events defined in* ***the table below***].

SFR	Auditable Events	Additional Audit Record Contents
FAU_GEN.1/VPN	No events specified.	N/A
FCS_CKM.1/IKE	No events specified.	N/A
FMT_SMF.1/VPN	All administrative actions.	No additional information.

SFR	Auditable Events	Additional Audit Record Contents
FPF_RUL_EXT.1	Application of rules configured with the 'log' operation.	• Source and destination addresses • Source and destination ports • Transport layer protocols
FPT_FLS.1/SelfTest	No events specified.	N/A
FPT_TST_EXT.3	No events specified.	N/A
FTP_ITC.1/VPN	• Initiation of the trusted channel. • Termination of the trusted channel. • Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.

Table 13: Auditable Events for Mandatory, Optional, Selection-based and Implementation-dependent Requirements (VPN Gateway)

FAU_GEN.1.2/VPN The TSF shall record within each audit record at least the following information:

a) Date and time of the event, 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 defined in* ***the table in FAU_GEN.1.1/VPN*** *for each auditable event, where applicable*].

6.1.1.4. FAU_GEN.2 User identity association

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.

6.1.1.5. FAU_STG.1 Protected audit trail storage

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.

6.1.1.6. FAU_GEN_EXT.1 Security audit generation for distributed TOEs

FAU_GEN_EXT.1.1 The TSF shall be able to generate audit records for each TOE component. The audit records generated by the TSF of each TOE component shall include the subset of security relevant audit events which can occur on the TOE component.

6.1.1.7. FAU_STG_EXT.1 Protected audit event storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself. In addition [

- *The TOE shall be a distributed TOE that stores audit data on the following TOE components:* [***Analytics node, Director node, VOS appliances***],

- *The TOE shall be a distributed TOE with storage of audit data provided externally for the following TOE components: [**VOS appliances and Director node will forward generated audit data to Analytics node.**]*

FAU_STG_EXT.1.3 The TSF shall [***[perform log rotation and archival of locally stored audit data according to a defined schedule, and require authorized Security Administrators to delete archives through manual or automated methods]***] when the local storage space for audit data is full.

6.1.1.8. FAU_STG_EXT.4 Protected local audit event storage for distributed TOEs

FAU_STG_EXT.4.1 The TSF of each TOE component which stores security audit data locally shall perform the following actions when the local storage space for audit data is full: [

Component	Action
VOS SD-WAN Controller and Branch	***perform log rotation and archival of locally stored audit data according to a defined schedule, and require authorized Security Administrators to delete archives through manual or automated methods***
Versa Director	***perform log rotation and archival of locally stored audit data according to a defined schedule, and require authorized Security Administrators to delete archives through manual or automated methods***
Versa Analytics	***perform log rotation and archival of locally stored audit data according to a defined schedule, and require authorized Security Administrators to delete archives through manual or automated methods***

].

6.1.1.9. FAU_STG_EXT.5 Protected remote audit event storage for distributed TOEs

FAU_STG_EXT.5.1 Each TOE component which does not store security audit data locally shall be able to buffer security audit data locally until it has been transferred to another TOE component that stores or forwards it. All transfer of audit records between TOE components shall use a protected channel according to [*FTP_ITC.1*].

6.1.2. Communications (FCO)

6.1.2.1. FCO_CPC_EXT.1 Component registration channel definition

FCO_CPC_EXT.1.1 The TSF shall require a Security Administrator to enable communications between any pair of TOE components before such communication can take place.

FCO_CPC_EXT.1.2 The TSF shall implement a registration process in which components establish and use a communications channel that uses [*No channel*] for at least TSF data.

FCO_CPC_EXT.1.3 The TSF shall enable a Security Administrator to disable communications between any pair of TOE components.

6.1.3. CRYPTOGRAPHIC SUPPORT (FCS)

6.1.3.1. FCS_CKM.1 CRYPTOGRAPHIC KEY GENERATION

FCS_CKM.1.1 The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- *RSA schemes using cryptographic key sizes of 2048-bits and 3072-bits[3] or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;*
- *ECC schemes using 'NIST curves' [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;*
- *FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526].*

].

6.1.3.2. FCS_CKM.1/IKE CRYPTOGRAPHIC KEY GENERATION (FOR IKE PEER AUTHENTICATION)

FCS_CKM.1.1/IKE The TSF shall generate **asymmetric** cryptographic keys **used for IKE peer authentication** in accordance with a specified cryptographic key generation algorithm: **[**

- ***FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3 for RSA schemes,***
- ***FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4 for ECDSA schemes and implementing "NIST curves" P-384 and [P-256, P-521]***

] and [

- ***No other key generation algorithm]***

] *and specified cryptographic key sizes [equivalent to, or greater than, a Symmetric key strength of 112 bits].*

6.1.3.3. FCS_CKM.2 CRYPTOGRAPHIC KEY ESTABLISHMENT

FCS_CKM.2.1 The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method: [

- *Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";*
- *FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [and groups listed in RFC 3526].*

].

6.1.3.4. FCS_CKM.4 CRYPTOGRAPHIC KEY DESTRUCTION

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

[3] Applied CSfC selections for VPN Gateways.

- *For plaintext keys in volatile storage, the destruction shall be executed by a [single overwrite consisting of [zeroes]];*
- *For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [*
    - *logically addresses the storage location of the key and performs a [single] overwrite consisting of [a new value of the key];*
    - *instructs a part of the TSF to destroy the abstraction that represents the key]*

that meets the following: *No Standard.*

6.1.3.5. FCS_COP.1/DataEncryption Cryptographic operation (AES data encryption/decryption)

FCS_COP.1.1/DataEncryption The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in **[*CBC*, *GCM*] and [*CTR*]** mode and cryptographic key sizes **[*128 bits*, *256 bits*] and [*no other cryptographic key sizes*]** that meet the following: AES as specified in ISO 18033-3, **[*CBC as specified in ISO 10116*, *GCM as specified in ISO 19772*] and [*CTR as specified in ISO 10116s*]**.

6.1.3.6. FCS_COP.1/SigGen Cryptographic operation (Signature generation and verification)

FCS_COP.1.1/SigGen The TSF shall perform *cryptographic signature services (generation and verification)* in accordance with a specified cryptographic algorithm *[*

- *RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [**2048 bits or 3072 bits**[4]],*
- *Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [**256 bits, 384 bits or 521 bits**]]*

that meet the following: [

- *For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,*
- *For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4].*

6.1.3.7. FCS_COP.1/Hash Cryptographic operation (Hashing)

FCS_COP.1.1/Hash The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm *[SHA-1, SHA-256, SHA-384, SHA-512]* ~~*and cryptographic key sizes [assignment: cryptographic keyu sizes]*~~ and **message digest sizes [*160, 256, 384, 512] bits*** that meet the following: *ISO/IEC 10118-3:2004*.

6.1.3.8. FCS_COP.1/KeyedHash Cryptographic operation (Keyed hash algorithm)

FCS_COP.1.1/KeyedHash The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm *[HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512]*

[4] Applied CSfC selections for VPN Gateways.

and cryptographic key sizes [*160, 256, 384, 512 bits]* **and message digest sizes [*160, 256, 384, 512] bits*** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

6.1.3.9. FCS_HTTPS_EXT.1 HTTPS PROTOCOL

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS.

FCS_HTTPS_EXT.1.3 If a peer certificate is presented, the TSF shall [*not establish the connection*] if the peer certificate is deemed invalid.

6.1.3.10. FCS_IPSEC_EXT.1 IPSEC PROTOCOL

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched and discards it.

FCS_IPSEC_EXT.1.3 The TSF shall implement [*tunnel mode*].

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms **[*AES-CBC-128*, *AES-CBC-256 (specified in RFC 3602)*, *AES-GCM-256 (specified in RFC 4106)*] and [*no other algorithm*]** together with a Secure Hash Algorithm (SHA)-based HMAC [*HMAC-SHA-1*, *HMAC-SHA-256*, *HMAC-SHA-384*, *HMAC-SHA-512*].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [

- *IKEv2 as defined in RFC 5996 and [with mandatory support for NAT traversal as specified in RFC 5996, section 2.23)], and [RFC 4868 for hash functions]].*

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [*IKEv2*] protocol uses the cryptographic algorithms [*AES-CBC-128, AES-CBC-256 (specified in RFC 3602), AES-GCM-256 (specified in RFC 5282)*]

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [

- IKEv2 SA lifetimes can be configured by a Security Administrator based on
    - [*length of time, where the time values can be configured within [**2 minutes to 24**] hours*]

].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [

- IKEv2 Child SA lifetimes can be configured by a Security Administrator based on
    - [*number of bytes;*
    - *length of time, where the time values can be configured within [**2 minutes to 24**] hours*]

].

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [**256 bits for DH group 19, 384 bits for DH group 20**] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in [*IKEv2*] exchanges of length [

- *at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash*

].

FCS_IPSEC_EXT.1.11

The TSF shall ensure that IKE protocols implement DH Groups

- **19 (256-bit Random ECP), 20 (384-bit Random ECP) according to RFC 5114 and**
- [*[no other DH Groups] according to RFC 5114*].

FCS_IPSEC_EXT.1.12 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [*IKEv2 IKE_SA*] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [*IKEv2 CHILD_SA*] connection.

FCS_IPSEC_EXT.1.13 The TSF shall ensure that [*IKEv2*] protocols perform peer authentication using [*RSA, ECDSA*] that use X.509v3 certificates that conform to RFC 4945 and [*no other method*].

FCS_IPSEC_EXT.1.14 The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: **Distinguished Name (DN),** [*SAN: IP address, SAN: Fully Qualified Domain Name (FQDN), SAN: user FQDN*].

6.1.3.11. FCS_NTP_EXT.1 NTP PROTOCOL

FCS_NTP_EXT.1.1 The TSF shall use only the following NTP version(s) [*NTP v4 (RFC 5905)*].

FCS_NTP_EXT.1.2 The TSF shall update its system time using [*[IPsec] to provide trusted communication between itself and an NTP time source*].

FCS_NTP_EXT.1.3 The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

FCS_NTP_EXT.1.4 The TSF shall support configuration of at least three (3) NTP time sources in the Operational Environment.

6.1.3.12. FCS_RBG_EXT.1 RANDOM BIT GENERATION

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [*CTR_DRBG (AES-256), HMAC_DRBG (SHA-512)*[5]].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [*[1] platform-based noise source, [1] software-based noise source*] with a minimum of [*256 bits]* of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

[5] Applied CSfC selections for TLS Protected Server.

6.1.3.13. FCS_SSHS_EXT.1 SSH SERVER PROTOCOL

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol in accordance with: RFCs 4251, 4252, 4253, 4254, [*4344, 5656, 6668*].

FCS_SSHS_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following user authentication methods as described in RFC 4252: public key-based, [*password-based*].

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [**262131 bytes**] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [*aes128-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com*].

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [*ecdsa-sha2-nistp256, ecdsa-sha2-nistp384*] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [*hmac-sha2-256, hmac-sha2-512, implicit*] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 The TSF shall ensure that [*ecdh-sha2-nistp256*] and [*ecdh-sha2-nistp384*] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHS_EXT.1.8 The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

6.1.3.14. FCS_TLSS_EXT.1 TLS SERVER PROTOCOL WITHOUT MUTUAL AUTHENTICATION

FCS_TLSS_EXT.1.1 The TSF shall implement [*TLS 1.2 (RFC 5246*] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[

- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*

] and no other ciphersuites.

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [*TLS 1.1*].

FCS_TLSS_EXT.1.3 The TSF shall perform key establishment for TLS using [*Diffie-Hellman groups [ffdhe2048*], *ECDHE curves* [*secp256r1, secp384r1, secp521r1] and no other curves*]].

FCS_TLSS_EXT.1.4 The TSF shall support [*no session resumption or session tickets*].

6.1.4. User Data Protection (FDP)

6.1.4.1. FDP_RIP.2 Full residual information protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*allocation of the resource to*] all objects.

6.1.5. Firewall (FFW)

6.1.5.1. FFW_RUL_EXT.1 Stateful traffic filtering

FFW_RUL_EXT.1.1 The TSF shall perform stateful traffic filtering on network packets processed by the TOE.

FFW_RUL_EXT.1.2 The TSF shall allow the definition of stateful traffic filtering rules using the following network protocol fields:

- *ICMPv4*
  - *Type*
  - *Code*
- *ICMPv6*
  - *Type*
  - *Code*
- *IPv4*
  - *Source Address*
  - *Destination Address*
  - *Transport Layer Protocol*
- *IPv6*
  - *Source address*
  - *Destination Address*
  - *Transport Layer Protocol*
  - *[no other field]*
- *TCP*
  - *Source Port*
  - *Destination Port*
- *UDP*
  - *Source Port*
  - *Destination Port*

and distinct interface.

FFW_RUL_EXT.1.3 The TSF shall allow the following operations to be associated with stateful traffic filtering rules: permit or drop with the capability to log the operation.

FFW_RUL_EXT.1.4 The TSF shall allow the stateful traffic filtering rules to be assigned to each distinct network interface.

FFW_RUL_EXT.1.5 The TSF shall:

a) *accept a network packet without further processing of stateful traffic filtering rules if it matches an allowed established session for the following protocols: TCP, UDP, [no other protocols] based on the following network packet attributes:*

1. *TCP: source and destination addresses, source and destination ports, sequence number, Flags;*
2. *UDP: source and destination addresses, source and destination ports;*
3. *[no other protocols].*

b) *Remove existing traffic flows from the set of established traffic flows based on the following: [session inactivity timeout, completion of the expected information flow].*

FFW_RUL_EXT.1.6 The TSF shall enforce the following default stateful traffic filtering rules on all network traffic:

a) *The TSF shall drop and be capable of [counting] packets which are invalid fragments;*

b) *The TSF shall drop and be capable of [counting] fragmented packets which cannot be re-assembled completely;*

c) *The TSF shall drop and be capable of logging packets where the source address of the network packet is defined as being on a broadcast network;*

d) *The TSF shall drop and be capable of logging packets where the source address of the network packet is defined as being on a multicast network;*

e) *The TSF shall drop and be capable of logging network packets where the source address of the network packet is defined as being a loopback address;*

f) *The TSF shall drop and be capable of logging network packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0) or an address "reserved for future use" (i.e. 240.0.0.0/4) as specified in RFC 5735 for IPv4;*

g) *The TSF shall drop and be capable of logging network packets where the source or destination address of the network packet is defined as an "unspecified address" or an address "reserved for future definition and use" (i.e. unicast addresses not in this address range: 2000::/3) as specified in RFC 3513 for IPv6;*

h) *The TSF shall drop and be capable of logging network packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified; and*

i) *[no other rules].*

FFW_RUL_EXT.1.7 The TSF shall be capable of dropping and logging according to the following rules:

- *The TSF shall drop and be capable of logging network packets where the source address of the network packet is equal to the address of the network interface where the network packet was received;*
- *The TSF shall drop and be capable of logging network packets where the source or destination address of the network packet is a link-local address;*

c) *The TSF shall drop and be capable of logging network packets where the source address of the network packet does not belong to the networks associated with the network interface where the network packet was received.*

FFW_RUL_EXT.1.8 The TSF shall process the applicable stateful traffic filtering rules in an administratively defined order.

FFW_RUL_EXT.1.9 The TSF shall deny packet flow if a matching rule is not identified.

FFW_RUL_EXT.1.10 The TSF shall be capable of limiting an administratively defined number of *half-open TCP connections. In the event that the configured limit is reached, new connection attempts shall be dropped and the drop event shall be [counted, logged].*

6.1.6. IDENTIFICATION AND AUTHENTICATION (FIA)

6.1.6.1. FIA_AFL.1 AUTHENTICATION FAILURE MANAGEMENT

FIA_AFL1.1 The TSF shall detect when an Administrator configurable positive integer within [**1 to 18446744073709551615**] unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely using a password.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [*prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until [**manual unlock action**] is taken by an Administrator; prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until an Administrator defined time period has elapsed*].

6.1.6.2. FIA_PMG_EXT.1 PASSWORD MANAGEMENT

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [“”, “’”, **“+”**, ”,”, **“-“**, **“.”**, **“/”**, **“:”**, **“;”**, **“<”**, **“=”**, **“>”**, **“?”**, **“@”**, **“[“**, “\”, **“]”**, “_”, “`”, **“{“**, “|”, **“}”**, **“~”**]];

b) Minimum password length shall be configurable to between [8 and 25] characters.

6.1.6.3. FIA_UIA_EXT.1 USER IDENTIFICATION AND AUTHENTICATION

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [*no other actions*].

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

6.1.6.4. FIA_UAU_EXT.2 PASSWORD-BASED AUTHENTICATION MECHANISM

FIA_UAU_EXT.2.1 The TSF shall provide a local [*password-based, SSH public key-based*] authentication mechanism to perform local administrative user authentication

6.1.6.5. FIA_UAU.7 PROTECTED AUTHENTICATION FEEDBACK

FIA_UAU.7.1 The TSF shall provide only ***obscured feedback*** to the user while the authentication is in progress **at the local console**.

6.1.6.6. FIA_X509_EXT.1/REV X.509 CERTIFICATE VALIDATION

FIA_X509_EXT.1.1/Rev The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation **supporting a minimum path length of three certificates.**

- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [*the Online Certificate Status Protocol (OCSP) as specified in RFC 6960*]
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
  - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

FIA_X509_EXT.1.2/Rev The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

6.1.6.7. FIA_X509_EXT.2/REV X.509 CERTIFICATE AUTHENTICATION

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for **IPsec and [*HTTPS*, *TLS*]** and [*no additional uses*].

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [*not accept the certificate*].

6.1.6.8. FIA_X509_EXT.3/REV X.509 CERTIFICATE REQUESTS

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [*Common Name, Organization, Organizational Unit, Country*].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

6.1.7. SECURITY MANAGEMENT (FMT)

6.1.7.1. FMT_MOF.1/FUNCTIONS MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOR

FMT_MOF.1.1/Functions The TSF shall restrict the ability to [*determine the behaviour of, modify the behaviour of*] the functions [*transmission of audit data to an external IT entity*] to *Security Administrators*.

6.1.7.2. FMT_MOF.1/MANUALUPDATE MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOR

FMT_MOF.1.1/ManualUpdate The TSF shall restrict the ability to enable the functions *to perform manual updates to Security Administrators*.

6.1.7.3. FMT_MOF.1/SERVICES MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOR

FMT_MOF.1.1/Services The TSF shall restrict the ability to **start and stop** ~~the functions~~ **services** to *Security Administrators*.

6.1.7.4. FMT_MTD.1/CORE DATA MANAGEMENT OF TSF DATA

FMT_MTD.1.1/CoreData The TSF shall restrict the ability to manage the *TSF data to Security Administrators.*

6.1.7.5. FMT_MTD.1/CRYPTO KEYS MANAGEMENT OF TSF DATA

FMT_MTD.1.1/CryptoKeys The TSF shall restrict the ability to [[*manage*]] the [*cryptographic keys **and certificates used for VPN operation***] to [*Security Administrators*].

6.1.7.6. FMT_SMF.1 SPECIFICATION OF MANAGEMENT FUNCTIONS

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using [digital signature, hash comparison] capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
- [*Ability to start and stop services;*
- *Ability to modify the behaviour of the transmission of audit data to an external IT entity;*
- *Ability to manage the cryptographic keys;*
- *Ability to configure the cryptographic functionality;*
- *Ability to configure the lifetime for IPsec SAs;*
- *Ability to configure the interaction between TOE components;*
- *Ability to re-enable an Administrator account;*
- *Ability to configure NTP;*
- *Ability to configure the reference identifier for the peer;*
- *Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;*
- *Ability to import X.509v3 certificates to the TOE's trust store;*
- *Ability to manage the trusted public key database;*].

6.1.7.7. FMT_SMF.1/IPS SPECIFICATION OF MANAGEMENT FUNCTIONS

FMT_SMF.1.1/IPS The TSF shall be capable of performing the following management functions:

- [*Enable, disable signatures applied to sensor interfaces, and determine the behavior of IPS functionality*
- *Modify these parameters that define the network traffic to be collected and analyzed:*
  - *Source IP addresses (host address and network address)*
  - *Destination IP addresses (host address and network address)*

    - *Source port (TCP and UDP)*
    - *Destination port (TCP and UDP)*
    - *Protocol (IPv4 and IPv6)*
    - *ICMP type and code*
- *Update (import) signatures*
- *Create custom signatures*
- *Configure anomaly detection*
- *Enable and disable actions to be taken when signature or anomaly matches are detected*
- *Modify thresholds that trigger IPS reactions*
- *Modify the duration of traffic blocking actions*
- *Modify the known-good and known-bad lists (of IP addresses or address ranges)*
- *Configure the known-good and known-bad lists to override signature- based IPS policies*].

6.1.7.8. FMT_SMF.1/FFW Specification of Management Functions

FMT_SMF.1.1/FFW The TSF shall be capable of performing the following management functions:

- *Ability to configure firewall rules;*

6.1.7.9. FMT_SMF.1/VPN Specification of Management Functions

FMT_SMF.1.1/VPN The TSF shall be capable of performing the following management functions

- [*Definition of packet filtering rules*
- *Association of packet filtering rules to network interfaces*
- *Ordering of packet filtering rules by priority*
- [*No other capabilities]*].

6.1.7.10. FMT_SMR.1 Security roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security Administrator.*

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

FMT_SMR.2.3 The TSF shall ensure that the conditions

- *The Security Administrator role shall be able to administer the TOE locally;*
- *The Security Administrator role shall be able to administer the TOE remotely*

are satisfied.

6.1.8. Packet filtering (FPF)

6.1.8.1. FPF_RUL_EXT.1 Packet filtering rules

FPF_RUL_EXT.1.1 The TSF shall perform packet filtering on network packets processed by the TOE.

FPF_RUL_EXT.1.2 The TSF shall allow the definition of packet filtering rules using the following network protocols and protocol fields: [

- IPv4 (RFC 791)

    - source address
    - destination address
    - protocol
- IPv6 (RFC 8200)
    - source address
    - destination address
    - next header (protocol)
- TCP (RFC 793)
    - source port
    - destination port
- UDP (RFC 768)
    - source port
    - destination port

].

FPF_RUL_EXT.1.3 The TSF shall allow the following operations to be associated with packet filtering rules: permit and drop with the capability to log the operation.

FPF_RUL_EXT.1.4 The TSF shall allow the packet filtering rules to be assigned to each distinct network interface.

FPF_RUL_EXT.1.5 The TSF shall process the applicable packet filtering rules (as determined in accordance with FPF_RUL_EXT.1.4) in the following order: [*Administrator-defined*].

FPF_RUL_EXT.1.6 The TSF shall drop traffic if a matching rule is not identified.

6.1.9. PROTECTION OF THE TSF (FPT)

6.1.9.1. FPT_APW_EXT.1 PROTECTION OF ADMINISTRATOR PASSWORDS

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

6.1.9.2. FPT_FLS.1/SELFTEST FAILURE WITH PRESERVATION OF SECURE STATE (SELF-TEST FAILURES)

FPT_FLS.1.1/SelfTest The TSF shall **shut down** when the following types of failures occur: [*failure of the power-on self-tests, failure of integrity check of the TSF executable image, failure of noise source health tests*].

6.1.9.3. FPT_SKP_EXT.1 PROTECTION OF TSF DATA (FOR READING OF ALL PRE-SHARED, SYMMETRIC, AND PRIVATE KEYS)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

6.1.9.4. FPT_STM_EXT.1 RELIABLE TIME STAMPS

FPT_STM_EXT.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2 The TSF shall [*synchronise time with an NTP server*].

6.1.9.5. FPT_TST_EXT.1 TSF TESTING

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [*initial start-up (on power on), at the conditions [**during random number and key generation operations**]*] to demonstrate the correct operation of the TSF: **noise source health tests,** [**the tests defined in the following table**].

Self-Tests Implemented by the TSF	
Versa Director and Analytics	HMAC-SHA2-256 integrity test
	AES encrypt and decrypt known-answer-test
	SHA-1, SHA2-256, and SHA2-512 known-answer tests
	HMAC-SHA2-256 and HMAC-SHA2-512 known-answer tests
	ECDSA pairwise consistency test
	RSA signature generation and verification known-answer tests and pairwise consistency test
	ECDH computation known-answer test
	HASH_DRBG known-answer test
	CTR_DRBG known-answer test
	TLS KDF known-answer test
	SSH KDF known-answer test
	Continuous random number generator test
	Entropy Health Tests
VOS Controller and Branch	RSA 2048 integrity test
	AES encrypt and decrypt known-answer tests
	RSA signature generation and verification known-answer tests and pairwise consistency test
	SHA-1, SHA2-256, SHA2-384, and SHA2-512 known-answer tests

	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512 known-answer tests
	CTR_DRBG known-answer test
	ECDH computation known-answer test
	ECDSA pairwise consistency test
	TLS KDF known-answer test
	SSH KDF known-answer test
	IKEv2 KDF known-answer tests
	Continuous random number generator test
	Entropy Health Tests

Table 14: TSF Self-Tests

6.1.9.6. FPT_TST_EXT.3 SELF-TEST WITH DEFINED METHODS

FPT_TST_EXT.3.1 The TSF shall run a suite of the following self-tests [[when loaded for execution]] to demonstrate the correct operation of the TSF: [integrity verification of stored executable code].

FPT_TST_EXT.3.2 The TSF shall execute the self-testing through [a TSF-provided cryptographic service specified in FCS_COP.1/SigGen].

6.1.9.7. FPT_TUD_EXT.1 TRUSTED UPDATE

FPT_TUD_EXT.1.1 The TSF shall provide *Security Administrators* the ability to query the currently executing version of the TOE firmware/software and [*no other TOE firmware/software version*].

FPT_TUD_EXT.1.2 The TSF shall provide *Security Administrators* the ability to manually initiate updates to TOE firmware/software and [*no other update mechanism*].

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

6.1.10. TOE ACCESS (FTA)

6.1.10.1. FTA_SSL_EXT.1 TSF-INITIATED SESSION LOCKING

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [*terminate the session]* after a Security Administrator-specified time period of inactivity.

6.1.10.2. FTA_SSL.3 TSF-INITIATED TERMINATION

FTA_SSL.3.1 The TSF shall terminate a **remote** interactive session after a *Security Administrator-configurable time interval of session inactivity*.

6.1.10.3. FTA_SSL.4 USER-INITIATED TERMINATION

FTA_SSL.4.1 The TSF shall allow **Administrator**-initiated termination of the **Administrator's** own interactive session.

6.1.10.4. FTA_TAB.1 DEFAULT TOE ACCESS BANNERS

FTA_TAB.1.1 Before establishing an **administrative user** session the TSF shall display a **Security Administrator-specified** advisory **notice and consent** warning message regarding use of the TOE.

6.1.11. TRUSTED PATH/CHANNELS (FTP)

6.1.11.1. FTP_ITC.1 INTER-TSF TRUSTED CHANNEL

FTP_ITC.1.1 The TSF shall **be capable of using [*IPsec*]** to provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [*[NTP server, VPN endpoints]*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data.**

FTP_ITC.1.2 The TSF shall permit **the TSF or the authorized IT entities** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**IPsec tunnels, syslog forwarding, NTP synchronization**].

6.1.11.2. FTP_ITC.1/VPN INTER-TSF TRUSTED CHANNEL (VPN COMMUNICATIONS)

FTP_ITC.1.1/VPN The TSF shall **be capable of using IPsec to** provide a communication channel between itself and **authorized IT entities supporting VPN communications** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

FTP_ITC.1.2/VPN The TSF shall permit [*the authorized IT entities*] to initiate communication via the trusted channel.

FTP_ITC.1.3/VPN
The TSF shall initiate communication via the trusted channel for [*remote VPN gateways or peers*].

6.1.11.3. FTP_TRP.1/ADMIN TRUSTED PATH

FTP_TRP.1.1/Admin The TSF shall **be capable of using [*SSH, TLS, HTTPS*]** to provide a communication path between itself and **authorized remote Administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and provides detection of modification of the channel data.**

FTP_TRP.1.2/Admin The TSF shall permit remote **Administrators** to initiate communication via the trusted path.

FTP_TRP.1.3/Admin The TSF shall require the use of the trusted path for *initial Administrator authentication and all remote administration actions.*

6.1.12. INTRUSION PREVENTION (IPS)

6.1.12.1. IPS_ABD_EXT.1 ANOMALY-BASED IPS FUNCTIONALITY

IPS_ABD_EXT.1.1 The TSF shall support the definition of [*anomaly ('unexpected') traffic patterns] including the specification of [*

- *throughput ([**packets per second**]);*
- *time of day;*
- *frequency;*
- *thresholds;]*

and the following network protocol fields:

- [*all packet header and data elements defined in IPS_SBD_EXT.1*].

IPS_ABD_EXT.1.2 The TSF shall support the definition of anomaly activity through [*manual configuration by administrators*].

IPS_ABD_EXT.1.3 The TSF shall allow the following operations to be associated with anomaly-based IPS policies:

- In any mode, for any sensor interface: [
  - *allow the traffic flow*
  - *send a TCP reset to the source address of the offending traffic*
  - *send a TCP reset to the destination address of the offending traffic*
  - *send an ICMP [port] unreachable message*]
- In inline mode: [
  - *allow the traffic flow*
  - *block/drop the traffic flow*
  - *and [no other actions]*].

6.1.12.2. IPS_IPB_EXT.1 IP BLOCKING

IPS_IPB_EXT.1.1 The TSF shall support the configuration and implementation of known-good and known-bad lists of [*source, destination*] IP addresses and [*no additional address types*].

IPS_IPB_EXT.1.2 The TSF shall allow [*Security Administrators*] to configure the following IPS policy elements: [*known-good list rules, known-bad list rules, IP addreses, [no other IPS policy elements*].

6.1.12.3. IPS_NTA_EXT.1 NETWORK TRAFFIC ANALYSIS

IPS_NTA_EXT.1.1 The TSF shall perform analysis of IP-based network traffic forwarded to the TOE's sensor interfaces, and detect violations of administratively-defined IPS policies.

IPS_NTA_EXT.1.2 The TSF shall process (be capable of inspecting) the following network traffic protocols:

- [*Internet Protocol version 4 (IPv4), RFC 791*
- *Internet Protocol version 6 (IPv6), RFC 2460*
- *Internet control message protocol version 4 (ICMPv4), RFC 792*
- *Internet control message protocol version 6 (ICMPv6), RFC 2463*
- *Transmission Control Protocol (TCP), RFC 793*
- *User Data Protocol (UDP), RFC 768*].

IPS_NTA_EXT.1.2 The TSF shall allow the signatures to be assigned to sensor interfaces configured for promiscuous mode, and to interfaces configured for inline mode, and support designation of one or more interfaces as 'management' for communication between TOE and external entities without simultaneously being sensor interfaces.

- Promiscuous (listen-only) mode: [***Ethernet***];
- Inline (data pass-through) mode: [***Ethernet***];
- Management mode: [***Management Ethernet***];
- [*No other interface types*].

6.1.12.4. IPS_SBD_EXT.1 SIGNATURE-BASED IPS FUNCTIONALITY

IPS_SBD_EXT.1.1 The TSF shall support inspection of packet header contents and be able to inspect at least the following header fields: [

- *IPv4: version; header length; packet length; ID; IP flags; fragment offset; time to live (TTL); protocol; header checksum; source address; destination address; IP options; and [type of service (ToS)]*.
- *IPv6: version; payload length; next header; hop limit; source address; destination address; routing header; and [traffic class, flow label]*.
- *ICMP: type; code; header checksum; and [ID, sequence number, [**variable field based on type and code**]]*.
- *ICMPv6: type; code; and header checksum.*
- *TCP: source port; destination port; sequence number; acknowledgement number; offset; reserved; TCP flags; window; checksum; urgent pointer; and TCP options.*
- *UDP: source port; destination port; length; and UDP checksum*].

IPS_SBD_EXT.1.2 The TSF shall support inspection of packet payload data and be able to inspect at least the following data elements to perform string-based pattern- matching: [

- *ICMPv4 data: characters beyond the first 4 bytes of the ICMP header.*
- *ICMPv6 data: characters beyond the first 4 bytes of the ICMP header.*
- *TCP data (characters beyond the 20 byte TCP header), with support for detection of:*

  i. *FTP (file transfer) commands: help, noop, stat, syst, user, abort, acct, allo, appe, cdup, cwd, dele, list, mkd, mode, nlst, pass, pasv, port, pass, quit, rein, rest, retr, rmd, rnfr, rnto, site, smnt, stor, stou, stru, and type.*
  ii. *HTTP (web) commands and content: commands including GET and POST, and administrator- defined strings to match URLs/URIs, and web page content.*
  iii. *SMTP (email) states: start state, SMTP commands state, mail header state, mail body state, abort state.*
  iv. *[no other types of TCP payload inspection];*

- *UDP data: characters beyond the first 8 bytes of the UDP header;*
- [***no other types of packet payload inspection***]].

IPS_SBD_EXT.1.3 The TSF shall be able to detect the following header-based signatures (using fields identified in IPS_SBD_EXT.1.1) at IPS sensor interfaces: [

a) *IP Attacks*
   i. *IP Fragments Overlap (Teardrop attack, Bonk attack, or Boink attack)*
   ii. *IP source address equal to the IP destination (Land attack)*

b) *ICMP Attacks*
   i. *Fragmented ICMP Traffic (e.g. Nuke attack)*
   ii. *Large ICMP Traffic (Ping of Death attack)*

c) *TCP Attacks*
   i. *TCP NULL flags*
   ii. *TCP SYN+FIN flags*
   iii. *TCP FIN only flags*
   iv. *TCP SYN+RST flags*

d) *UDP Attacks*
   i. *UDP Bomb Attack*
   ii. *UDP Chargen DDoS Attack]*.

IPS_SBD_EXT.1.4 The TSF shall be able to detect all the following traffic-pattern detection signatures, and to have these signatures applied to IPS sensor interfaces: *[*

a) Flooding a host (DoS attack)
   i. ICMP flooding (Smurf attack, and ping flood)
   ii. TCP flooding (e.g. SYN flood)

b) Flooding a network (DoS attack)

c) Protocol and port scanning
   i. IP protocol scanning
   ii. TCP port scanning
   iii. UDP port scanning
   iv. ICMP scanning].

IPS_SBD_EXT.1.5 The TSF shall allow the following operations to be associated with signature- based IPS policies:

- *In any mode, for any sensor interface: [*
  - *allow the traffic flow;*
  - *send a TCP reset to the source address of the offending traffic;*
  - *send a TCP reset to the destination address of the offending traffic;*
  - *send an ICMP [port] unreachable message;]*
- *In inline mode:*
  - *block/drop the traffic flow;*
  - *and [allow the traffic flow with following exceptions: [**DoS attacks**]*].

IPS_SBD_EXT.1.6 The TSF shall support stream reassembly or equivalent to detect malicious payload even if it is split across multiple non-fragmented packets.

6.2. SECURITY ASSURANCE REQUIREMENTS (SARS)

The TOE assurance requirements for this ST consist of the SARs prescribed by the PP and its PP-Modules.

The assurance components are summarized in the table below.

Assurance Class	Assurance Components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labeling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Table 15: Assurance requirements

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 each component of the TOE, in the following sections.

7.1.1. Security audit generation (FAU_GEN.1, FAU_GEN.1/IPS, FAU_GEN.1/VPN, FAU_GEN.2, FPT_STM_EXT.1)

<table>
<tr><th>TOE SFRs</th><th>TOE Component</th><th>How the SFR is Satisfied</th></tr>
<tr><td>FAU_GEN.1

FAU_GEN.2

FAU_GEN.1/VPN

FAU_GEN_EXT.1</td><td>VOS

Director

Analytics</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 Director devices send their logs to an Analytics node.

The TSF supports standard protocols and log formats, including Syslog, IPFIX, SNMP and NETCONF, all of which are transported via IPsec tunnels.

The following states the log types of TOE and the component on which each is generated:
<table>
<tr><th>Log Type</th><th>Component</th><th>Description</th></tr>
<tr><td>Audit start/stop</td><td>VOS, Director, Analytics</td><td>Startup and shutdown of appliance and/or auditing function</td></tr>
<tr><td>Logon/Logoff events</td><td>Director</td><td>Success and failed administrator logins, lockout events, session timeouts, session terminations</td></tr>
<tr><td>Config/Management operations</td><td>Director</td><td>All management functions</td></tr>
<tr><td>NTP logs</td><td>VOS, Director, Analytics</td><td>Clock synchronization, server configuration</td></tr>
<tr><td>Firewall logs</td><td>VOS</td><td>Firewall logs, netflows, rule configuration</td></tr>
<tr><td>IDP logs</td><td>VOS</td><td>Threat logs, signature-based matches, anomaly-based matches, IP filter matches, rule configuration</td></tr>
<tr><td>IPsec VPN logs</td><td>VOS, Director, Analytics</td><td>IPSec session start/stop, failures</td></tr>
<tr><td>HTTPS logs</td><td>Director</td><td>HTTPS session start/stop, failures</td></tr>
<tr><td>SSH logs</td><td>Director</td><td>SSH session start/stop, failures</td></tr>
<tr><td>Device alarms</td><td>VOS</td><td>Critical device errors and alarms</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th>TOE Component</th><th>How the SFR is Satisfied</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Software upgrades</td><td>VOS, Director, Analytics</td><td>Initiation and result (success or failure)</td></tr>
<tr><td>Registration/ deregistration</td><td>VOS, Director</td><td>Adding or removing a branch site or TOE component</td></tr>
<tr><td>X.509 logs</td><td>VOS, Director, Analytics</td><td>Failure to validate, Import of CA trust anchor</td></tr>
<tr><td>Key generation</td><td>VOS, Director, Analytics</td><td>IPsec, SSH, and TLS key generation events. Key is identified by key name record or filename.</td></tr>
<tr><td>Self-tests</td><td>VOS, Director, Analytics</td><td>Self-test outcomes (success or failure)</td></tr>
</table>

The TOE ensures each action performed by the administrator at the CLI or via GUI is logged with the administrator's identity and as a result events are traceable to a specific user.
</td></tr>
<tr><td>FAU_GEN.1/IPS</td><td>VOS, Analytics</td><td>LEF profiles may be associated with IP-filtering profiles, NGFW access policies, DoS protection profiles, and vulnerability profiles, which ensure that the matching traffic is logged or counted. The following traffic types will result in a counter increment:
• IPv4 packets containing specific ID, FLAGS, FRAG, TTL, CHECKSUM, SRC, DST, or OPTIONS header field values.
• ICMP packets containing specific TYPE, CHECKSUM, or CODE header field values.
• TCP packets containing specific SPORT, RESERVED, FLAGS, or OPTIONS header field values.
• UDP packets containing specific SPORT header field values
• IPv6 packets containing specific PLEN header field value, or containing two routing headers
• ICMPv6 packets containing specific CODE or CHECKSUM header field values.
• ICMPv4 and ICMPv6 payloads containing a detection string.
• IPv4 packets with same SRC and DST IP
• TCP packets containing NULL flag
• TCP packets containing SYN + FIN flags
• TCP packets containing FIN + ONLY flags
• TCP packets containing SYN + RST flags
• ICMP or IPv4 packet containing IP Fragment Overlap
Thresholds may be configured on a vulnerability profile according to the following:</td></tr>
</table>

TOE SFRs	TOE Component	How the SFR is Satisfied
		• Track By—Select the threshold tracking based on either source address, destination address, or both source and destination addresses. • Interval—Enter an interval, in seconds. • Threshold—Enter the number of hits per interval based on the traffic direction. Signature based detection applies a set of pre-defined rules or custom rules. Rules are based on the snort rule format. Snort rules are divided into two logical sections, the rule header and the rule options. The rule header contains the rule's action, protocol, source and destination IP addresses and netmasks, and the source and destination ports information, and a series of customizable rule options which cover all the fields described in IPS_SBD_EXT.1.
FPT_STM_EXT.1	VOS Director Analytics	The TOE is configured to provide a source of date and time information used in audit event timestamps, certificate validity checking, time-based rekeying, session timeouts, user account lockout periods, time-of-day access, etc. The default time zone of the TOE components is UTC. The TOE must be set to receive clock updates from an NTP server which is secured via IPsec.

7.1.2. Security Audit Storage (FAU_STG.1, FAU_STG_EXT.1, FAU_STG_EXT.4, FAU_STG_EXT.5)

TOE SFRs	TOE Component	How the SFR is Satisfied
FAU_STG.1 FAU_STG_EXT.1 FAU_STG_EXT.4 FAU_STG_EXT.5	VOS Director Analytics	The TOE is a distributed TOE which stores local audit data on the following components: • VOS SD-WAN Controller and Branch devices (with the exception of traffic logs which are buffered in memory and forwarded in real-time to Analytics without being locally stored) • Versa Director • Versa Analytics The Versa Director, VOS SD-WAN Controller and Branch devices are configured to send log data to the Analytics node over an internal IPsec tunnel in real-time. The Analytics node performs data analysis and provides reports and data visualization on syslogs received from other TOE components and is configured to export all TOE logs to an external syslog receiver via IPsec in real time. The TSF restricts access to audit logs stored on each component to authorized Security Administrators. Audit log settings can be configured to automatically archive and rotate log files via cron job, based on size limit specified by *logrotate.d* parameters (defined by number of bytes). By default, log files are rotated daily, or when the log file reaches 50MB. A maximum of 7 log files are retained, with the oldest log file deleted as rollover occurs. Audit log files may also be deleted manually or automatically according to configured parameters. Audit log files can

TOE SFRs	TOE Component	How the SFR is Satisfied
		be deleted at the command of administrators with the Admin role, where administrators with super user privileges can manually delete the audit logs. Only authorized Security Administrators can read the audit records. Director logs all administrative operations such as create, modify, and delete in the *ProviderDataCenterSystemAdmin.log* file. User activities such as login, change password, etc. are stored in the *SystemUser.log* file. Tenant operations are stored in *Tenant-name.log*. For CLI operations, each action is recorded in *Shell.log*. For custom roles, actions performed by the role are recorded in *Role-name.log*. VOS 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* The Security Administrator enables the log export functionality (LEF) on the VOS device. VOS devices export log data in IPFIX and syslog formats. To export log data from VOS devices to an Analytics node, the Security Administrator configures a log export template, a collector, and a LEF profile, and then selects the LEF profile when configuring a feature or service. The logs for the feature or service are forwarded to the active collector named in the LEF profile. The LEF profile can be applied in one of the following ways: • Associate the LEF profile with a feature or service. • Associate the LEF profile with a traffic-monitoring policy rule. • Associate the LEF profile with the logging control configuration. • Assign a LEF profile to be the default. The method used depends on the type of logs being exported. Logs are generated in syslog format and include a label, called the syslog identifier, identifying the log type. Each feature or service has one or more associated syslog identifiers. For logs sent to Analytics clusters and Netflow collectors, LEF adds an IPFIX overhead. When a LEF profile is associated with a traffic-monitoring policy rule, the VOS device generates syslog messages for selected types of traffic monitoring flows. When a LEF is associated with the logging control configuration, the VOS device generates syslog messages globally for all traffic-monitoring flows. A LEF profile automatically sends logs of the following types to the active collector once they have been specified in the profile. The syslog identifier or identifiers corresponding to each log type are displayed in parentheses. • Alarm logs (alarmLog) • SD-WAN link and rule statistics monitoring (bwMonLog, infUtilLog) • System logs (systemLoadLog)

TOE SFRs	TOE Component	How the SFR is Satisfied
		• Firewall Logs (accessLog, sfwAccessLog, denyLog, monStatsLog) • Flow logs (flowIdLog, flowMonHttpLog, flowMonLog) • Packet Capture Logs (pcapLog) • DDoS Logging (dosThreatLog) • IP filtering logs (ipfLog) • IP guard logs (ipguardLog) • IDP logging (idpLog) • Malformed packet log (malformedPktLog) • Secure access logs (secAccGlobalStatsLog, secAccUserStatsLog) • Traffic detection function logs (tdfPeakBwLog, tdfTcpPerfLog, tdfUsageReport) • URL filtering logs (urlfLog) • Antivirus log (avLog) The Security Administrator must initially configure an Analytics node to collect logs. These nodes are called Analytics log collector nodes, and they collect log messages (simply called logs), which include alarms from all the VOS Branch and Controller devices in the network, in IPFIX format. Analytics log collector nodes run two programs, called the log collector exporter and the Versa Analytics driver, to accept and process the incoming logs. The log collector exporter program listens for incoming connections containing logs, called log export functionality (LEF) connections, and stores the logs on the Analytics node. The Analytics driver then processes these logs into the Analytics datastore. The System Administrator configures the log collector exporter stream incoming logs to an external third-party collector by configuring a remote collector. A remote collector streams the logs to one or more third-party collectors in syslog format via IPsec in realtime. An Analytics log collector node processes incoming logs in the following sequence: 1. The local collector on the Analytics log collector node receives logs sent from Versa Operating System™ (VOS™) devices. 2. The local collector stores the logs in clear text files in its log storage directory, with one subdirectory for each organization. Each organization subdirectory contains a further subdirectory named for the routing instance that forwarded the log, and the incoming logs are collected into log files in these subdirectories. 3. Any log files created in the routing instance subdirectories under /var/tmp/log are automatically processed into the cluster datastores by the Versa Analytics driver. 4. After processing the log files, the Versa Analytics driver moves the log file into a backup directory under the /var/tmp/log directory. 5. A cron job stored in /etc/cron.d/log-archive periodically archives all log files stored in the backup directories under

TOE SFRs	TOE Component	How the SFR is Satisfied
		/var/tmp/log. Also, any additional log archive cron jobs that you have configured archive logs stored in non-default log storage directories. The log archive cron jobs convert the clear text files in the log storage directories to compressed gzip format and move them to a log archive directory. The archiving time interval can be hourly, weekly, or daily. 6. Authorized Security Administrators may delete archived logs manually using a CLI command which can be scripted and periodically run or executed on a schedule with a cron job.

7.1.3. CRYPTOGRAPHIC SUPPORT – KEY MANAGEMENT (FCS_CKM.1, FCS_CKM.1/IKE, FCS_CKM.2, FCS_CKM.4, FCS_RBG_EXT.1, FMT_MTD.1/CRYPTOKEYS, FPT_SKP_EXT.1)

TOE SFRs	TOE Component	How the SFR is Satisfied
FCS_CKM.1 FCS_CKM.1/IKE FCS_CKM.2	VOS Director Analytics	The TSF provides the following key generation capabilities: • Using RSA 3072 bits or greater as described in FIPS PUB 186-4 B.3.3 • Using ECDSA P-256, P-384, or P-521 as described in FIPS PUB 186-4 B.4.1 and B.4.2 • Using FFC Schemes using "safe-prime" groups per NIST SP 800-56Arev3 (available for TLS v1.2 connections only). RSA and ECDSA keypairs are used in the following functions: • X.509 certificates used in TLS and IPsec (FCS_TLSS_EXT.1, FCS_TLSS_EXT.2, FCS_IPSEC_EXT.1) • Verification of TSF binary integrity (FPT_TUD_EXT.3) • SSH host key identification and public key authentication (FCS_SSHS_EXT.1) The TSF supports the ECDH key establishment with the ephemeralUnified scheme and P-256, P-384, P-521 curves in accordance with SP 800-56Arev3 for the following functions.: • Administrative sessions to the SSH CLi (FCS_SSHS_EXT.1) • Administrative sessions to the HTTPS web UI (FCS_HTTPS_EXT.1, FCS_TLSS_EXT.1) • IKE/IPsec sessions (FCS_IPSEC_EXT.1) The TSF supports DH key establishment using FFC Schemes using "safe-prime" groups for TLS only.
FCS_CKM.4	VOS Director Analytics	The TOE meets all requirements specified in FIPS 140-2 for destruction of keys. All the keys stored within the TOE can be zeroized.

TOE SFRs	TOE Component	How the SFR is Satisfied
		The list of all relevant keys (including the origin and storage of each), and all key destruction scenarios are described in section 7.3. No configurations or circumstances exist that do not conform to the key destruction requirement.
FCS_RBG_EXT.1	VOS Director Analytics	The TOE headend (Director/Analytics) uses a HMAC_DRBG and CTR_DRBG for generation of seed values for private/public keypairs. All entropy is seeded from Linux RNG from CPU jitter as the primary entropy source. Both DRBGs are seeded with an estimated 256 bits of entropy. VOS uses a CTR_DRBG with 256 bits of entropy seeded from RDRAND instruction in the compatible CPU.
FMT_MTD.1/CryptoKeys	VOS Director Analytics	The list of all relevant keys (including the generation and input operations by Administrators), are described in section 7.3.
FPT_SKP_EXT.1	VOS Director Analytics	The list of all relevant keys (including the origin and storage of each), are described in section 7.3. All keys are stored either in non-persistent RAM or persistent Flash. No interfaces exist which enable inspection of plaintext key components. All persistent keys are stored in the Linux filesystem and are restricted via adequate file permissions.

7.1.4. CRYPTOGRAPHIC SUPPORT – ALGORITHMS (FCS_COP.1/DATAENCRYPTION, FCS_COP.1/SIGGEN, FCS_COP.1/HASH, FCS_COP.1/KEYEDHASH)

TOE SFRs	TOE Component	How the SFR is Satisfied
FCS_COP.1/ DataEncryption	VOS Director Analytics	The TSF provides data encryption and decryption capabilities in support of IKE/IPsec, TLS, and SSH using 128 and 256 bits AES in CBC, CTR, and GCM modes as described in FIPS PUB 197 and NIST SP 800-38D.
FCS_COP.1/SigGen	VOS Director Analytics	The TSF provides digital signature capabilities: • Using RSA PKCS-PSS or PKCS#1 with 3072 bits or greater as described in FIPS PUB 186-4. • Using ECDSA with P-256, P-384, and P-521 as described in FIPS PUB 186-4. RSA and ECDSA signatures are used in the following functions: • X.509 certificates used in TLS and IPsec (FCS_TLSS_EXT.1, FCS_TLSS_EXT.2, FCS_IPSEC_EXT.1) • Verification of TSF binary integrity (FPT_TUD_EXT.3) SSH host key identification and public key authentication (FCS_SSHS_EXT.1)

TOE SFRs	TOE Component	How the SFR is Satisfied
FCS_COP.1/Hash	VOS Director Analytics	The TSF provides hashing capabilities in support of HMAC operations and digital signature functions: • Using SHA-1, SHA-256, SHA-384, and SHA-512 as described in FIPS PUB 180-4.
FCS_COP.1/KeyedHash	VOS Director Analytics	The TSF provides HMAC capabilities: • Using 160, 256, 384, and 512 bits HMAC-SHA, described in FIPS PUB 198-1. • HMAC-SHA-1 supports a key length of at least 160 bits with a MAC length of 160 and block size of 512 bits. • HMAC-SHA-256 supports a key length of at least 256 bits with a MAC length of 256 bits and a block size of 512 bits. • HMAC-SHA-384 supports a key length of at least 384 bits with a MAC length of 384 bits and a block size of 1024 bits. • HMAC-SHA-512 supports a key length of at least 512 bits with a MAC length of 512 bits and a block size of 1024 bits.

7.1.5. Cryptographic support – Protocols (FCS_HTTPS_EXT.1, FCS_IPSEC_EXT.1, FCS_NTP_EXT.1, FCS_TLSS_EXT.1, FCS_SSHS_EXT.1)

TOE SFRs	TOE Component	How the SFR is Satisfied
FCS_HTTPS_EXT.1 FCS_TLSS_EXT.1	Director	The TSF implements a HTTPS server in compliance with RFC 2818 and implements X.509 certificates for server self-identification. The TSF implements TLSv1.2 as a server without mutual authentication for securing management connections to the Director UI. TLS v1.1, 1.0, SSL 3.0, SSL 2.0, and any other unsupported TLS versions will be rejected. The TSF implements the following ciphersuites for each implementation of TLS in accordance with RFC 5289: • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 The TSF supports ECDH with secp256r1, secp384r1, and secp521r1 curves and ffdhe2048 and ffdhe3072 and ffdhe4096 groups for use in key establishment. The TSF does not support session resumption or session tickets.
FCS_IPSEC_EXT.1	VOS Director Analytics	The TSF supports the establishment of IPsec connections for the following: • Site-to-site VPN tunnels between Branch sites • External communications to syslog and NTP servers • End-user VPN client connections For site-to-site and internal/external connections, the TSF supports X.509 certificates for peer authentication. The TSF supports tunnel mode. IKEv2 is supported for Phase 1 negotiation.

TOE SFRs	TOE Component	How the SFR is Satisfied

		Each of the IPsec implementations within the TSF support the following encryption ciphers for IKEv2 SA and Child SAs. A configuration parser ensures that the strength of the IKEv2 SA cipher cannot be less than the IKEv2 Child SA cipher:
		• AES-CBC-128,
		• AES-CBC-256
		• AES-GCM-256
		The TSF supports the following data integrity algorithms for IKEv2 SA and Child SAs:
		• HMAC-SHA-1,
		• HMAC-SHA-256,
		• HMAC-SHA-384,
		• HMAC-SHA-512
		The TSF supports the following ECDH groups for key establishment. The "x" in g^x mod p is generated from the output of the DRBG and is twice the strength of the negotiated group (i.e., between 256 and 512 bits). Nonces are randomly generated according to the negotiated ECDH group and are at least 128 bits and at least half the size of the negotiated PRF. The negotiated ECDH group will be selected based on the strongest mutually accepted group configured on each IPsec endpoint:
		• 19 (256-bit Random ECP),
		• 20 (384-bit Random ECP),
		The TSF supports the following algorithms for X.509 peer certificate authentication:
		• RSA (2048 or 3072 bits),
		• ECDSA (256, 384, or 521 bits)
		The TSF supports IKEv2 with NAT Traversal.
		The TSF enforces the following lifetime values for IKEv2 SAs:
		• Between 2 minutes and 24 hours (configurable)
		The TSF enforces the following lifetime values for IKEv2 Child SAs:
		• Between 2 minutes and 24 hours (configurable),
		• Number of bytes (configurable)
		For IKE authentication using X.509 certificates, the peer identifier presented in the certificate is matched to the peer identifier configured in the IPsec VPN policy. The following are acceptable fields for use in certificate matching:
		• Distinguished Name
		• Subject Alternative Name
		  ○ IP address
		  ○ FQDN

TOE SFRs	TOE Component	How the SFR is Satisfied
		○ User FQDN (email address) The TSF supports the construction of a SPD consisting of BYPASS (e.g., no encryption), DISCARD (e.g., drop the packet), and PROTECT (e.g., encrypt the packet) rules through a combination of IPsec SAs, IP forwarding rulesets and traffic filters. The packet processing algorithm is described as follows: 1. A packet is received on an interface and is placed into an outbound queue for processing. 2. If the packet does not violate any inspection policies or default firewall rules, the packet is matched against a set of rules in a top-down order until a match is found. 3. If the packet matches a rule which is marked as drop, the packet will be immediately discarded. 4. If the packet matches a rule which is marked as permit, the packet will be forwarded and transmitted from the destination interface. If the packet is not flagged by the IPsec VPN policy, or is not part of an existing SA, the packet will flow in plaintext. 5. If the packet matches an IPsec VPN policy, the packet will be forwarded encrypted according to the SA, if the packet matches an existing SA. If the packet does not match an existing SA, a new one will be established and upon completion of the SA, the packet will be forwarded encrypted. 6. If the packet does not match any of the configured rules, it will be dropped by a default deny rule.
FCS_NTP_EXT.1	VOS Director Analytics	The TSF supports synchronization of its system clock with an external NTPv4 server. Authenticity and integrity of the time updates is protected using an IPsec tunnel.
FCS_SSHS_EXT.1	Director	The TSF supports SSHv2 for securing the management path to the Versa Director for CLI management operations. The TSF supports password-based authentication in addition to the following public key algorithms for SSH client authentication and for the SSH host key: • ecdsa-sha2-nistp256, • ecdsa-sha2-nistp384, The TSF accepts SSH clients presenting a public key found in the server's *authorized_keys* file. If no match is found, the server will revert to password-based authentication. The TSF supports the following encryption algorithms: • aes128-ctr • aes256-ctr • aes128-gcm@openssh.com • aes256-gcm@openssh.com

TOE SFRs	TOE Component	How the SFR is Satisfied
		The TSF supports the following message integrity algorithms: • hmac-sha2-256 • hmac-sha2-512 • implicit The TSF supports the following key exchange algorithms: • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 The TSF will reject large packets as defined by RFC 4253 if the payload size exceeds 262,131 bytes. The TSF will automatically trigger a rekey if either of the configured thresholds (one gigabyte and one hour) are reached.

7.1.6. CRYPTOGRAPHIC SUPPORT – SELF TESTS (FPT_TST_EXT.1, FPT_TST_EXT.3, FPT_FLS.1/SELFTEST)

TOE SFRs	TOE Component	How the SFR is Satisfied
FPT_TST_EXT.1 FPT_TST_EXT.3 FPT_FLS.1/SelfTest	VOS Director Analytics	The TSF runs a suite of self-tests during initial start-up and periodically during normal operation to verify its correct operation. The complete list of self-tests implemented by each TOE component are described in section 6.1.9.5. Power-on self-tests are automatically invoked by start-up scripts. Periodic self- tests are run automatically by the daemons/commands, 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* The following output to *versa-service.log* demonstrates a successful verification of the cryptographic self-tests: AES Selftest PASSED AES-CCM Encrypt selftest PASSED AES-CCM Decrypt selftest PASSED

TOE SFRs	TOE Component	How the SFR is Satisfied
		AES-GCM Encrypt Selftest PASSED AES-GCM Decrypt selftest PASSED AES-XTS-128 selftest PASSED AES-XTS-256 selftest PASSED AES-CMAC selftest PASSED HMAC SHA1 HMAC SHA224 HMAC SHA256 HMAC SHA384 HMAC SHA512 HMAC Self test PASSED Generated RSA Sign and Verified. RSA Selftest PASSED ECDH Self test Passed ECDSA selftest for Signature generation and Signature verification Passed 16 DRBG selftest PASSED KDF SSH selftest PASSED KDF TLS selftest PASSED SHA1 Self test PASSED The implementation of self-tests by the TSF provides coverage of each TSF-relevant cryptographic function employed by each TOE component and covers the integrity of binaries critical to the operation of the TSF, along with other critical functions such as entropy noise source health testing. Therefore, the tests are sufficient to demonstrate that the TSF is operating correctly. In the event of a failed self-test, the TSF will shut down its interfaces and prevent traffic from flowing through the TOE.

7.1.7. IDENTIFICATION AND AUTHENTICATION – PASSWORD AUTHENTICATION (FIA_AFL.1, FIA_UAU_EXT.1, FIA_UIA_EXT.1, FIA_PMG_EXT.1, FPT_APW_EXT.1)

TOE SFRs	TOE Component	How the SFR is Satisfied
FIA_AFL.1	Director	The Director enforces account lockouts for the GUI, console and SSH CLI after the configured number of unsuccessful authentication attempts has been reached. On each attempt, a counter is incremented until the value is reached, upon which the user account will be locked and will no longer be able to login until: • The administrator-configured unlock time period elapses • Another administrator manually unlocks the account The time-based unlock feature ensures that administrators will be automatically re-enabled, to prevent situations where all administrative accounts are permanently locked out. The local console is not subject to lockout.
FIA_PMG_EXT.1	Director	Administrative passwords may be composed of any combination of upper and lower case letters, numbers, and the following special characters: ! @ # $ % ^ & * ( ) " ' + , - . / : ; < = > ? @ [\ ] _ ` { | } ~ Minimum password length is configurable to between 8 and 25 characters.
FIA_UIA_EXT.1 FIA_UAU_EXT.1	Director	The TOE can identify administrators by a unique ID and enforces their authentication before granting them access to any TSF management interfaces. The TOE supports two levels of administrators, which are the roles Admin and Operator. 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 Director CLI (console or and management port via SSH), and through the Director GUI (management port via HTTPS/TLS). The TOE mediates all administrative actions through the CLI and GUI. 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 the administrative functionality of the TOE until an administrator is successfully identified and authenticated. Security Administrators are identified through their login session to the Director GUI and CLI. From this session, the administrator may access CLIs on each component from within existing authenticated IPsec tunnels between TOE components using usernames and passwords configured on each device. With the exception of the Director management interfaces, all TOE components will only be accessible via the Director through the IPsec channel. Local console interfaces

TOE SFRs	TOE Component	How the SFR is Satisfied
		may be enabled on Controller and Branch devices for emergency access situations.
FIA_UAU.7	Director	When an administrator is authenticating to Versa Director, dots will be echoed back on the Director GUI. However, when an administrator is logging in to the Director CLI using local console or SSH login, the password is not echoed back.
FPT_APW_EXT.1	Director	Operator passwords are stored as SHA-512 hashes. UIs involving password manipulation (e.g. change own password, user creation, set another user's password by Admin) are designed such that there is no display of the stored credential in plaintext. During entry, passwords are obfuscated in accordance with FIA_UAU.7.

7.1.8. IDENTIFICATION AND AUTHENTICATION – VPN (FIA_X509_EXT.1/REV, FIA_X509_EXT.2, FIA_X509_EXT.3)

TOE SFRs	TOE Component	How the SFR is Satisfied
FIA_X509_EXT.1/Rev FIA_X509_EXT.2	VOS Director Analytics	The TSF supports X.509 certificates for authentication of IPsec peers as well as identification of the Director GUI to browser clients. Both manual and automated certificate enrollment methods are supported. Certificates used in Director TLS server functions are stored separately in protected keystores used only by the web application server. The server configuration file specifies which certificate and trust anchor to use for server authentication. This certificate is installed during the initial configuration as specified in the administrative guidance. To configure a VOS device to use certificates for VPN authentication, a certificate server is configured via the Director that hosts the certificates. When the Branch or Controller device requires a certificate, it sends a certificate request to the server. The supported automated methods are: Certificate Management Protocol (CMP) and Simple Certificate Enrollment Protocol (SCEP). Within the IPSec VPN profile, the trust anchor and certificate must be specified in order to determine which certificate to use for connections. OCSP is the supported protocol for revocation status validation. The VOS device can also be configured to enforce signature validation of the OCSP responses and terminate the IPsec session if the OCSP responder is unreachable or the response is unknown. In order to enroll certificates, a proper CA certificate chain must first be installed both on Director and VOS. Validation checks occur on the following certificates and under the following conditions: • Importing CA certificates into the trust store

TOE SFRs	TOE Component	How the SFR is Satisfied
		○ BasicConstraints flag is present and set to TRUE ○ Intermediate CA certificates are properly chained • Importing end-entity certificates into the trust store ○ Valid CA chain is installed and terminated at the root CA ○ CA certificates contain BasicConstraints flag and is set to TRUE • During IPsec session establishment ○ Peer certificate signatures can be successfully verified up to the root of trust ○ Peer certificates are not expired ○ OCSP response indicates a non-revoked peer certificate and the OCSP responder certificate is valid and contains the OCSP signing extended key usage ○ Peer certificate chains containing EC certificates use named elliptic curves ○ Peer reference identifier matches the expected identifier
FIA_X509_EXT.3	VOS Director Analytics	Director nodes support X.509 certificates for securing the HTTPS web GUI, in the following formats: • PEM-encoded certificate—PEM encoding uses Base64-encoded ASCII files. It does not store the certification path or private key information. The Director node uses the versa_director_web_client.crt certificate based on PEM encoding. • DER-encoded certificate—DER encoding is the binary form of the certificate. This format supports encoding of private keys. The Director node uses the versa_director_web_client.cer certificate based on DER encoding. The Director node uses Java Keystore (JKS) as the keystore format. CSRs and private keys are generated using the Director and exported to TOE components over existing IPsec tunnels. CSRs support definition of Common Name, Organization, Organizational Unit, and Country.

7.1.9. SECURITY MANAGEMENT (FMT_MTD.1/COREDATA, FMT_MOF.1/FUNCTIONS, FMT_MOF.1/SERVICES, FMT_SMF.1, FMT_SMF.1/VPN, FMT_SMF.1/FFW, FMT_SMF.1/IPS, FMT_SMR.2)

TOE SFRs	TOE Component	How the SFR is Satisfied
FMT_MOF.1/Functions FMT_MOF.1/Services FMT_MTD.1/CoreData	Director	All security management functions are performed via the Director component through the GUI or CLI (either remotely or via local console). The TOE supports a Security Administrator role which is mapped to "Admin", as well as a lower-privilege "Operator" role. All administrative accounts are assigned to only one role. The TOE provides the ability for Security Administrators to access and modify TSF data, such as audit data, configuration data, certificates and private keys, security policies (IPS, firewall and VPN), and all other security configuration data. 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 accounts with Admin role, whereas accounts with Operator role do not have these privileges. The TOE restricts the ability to perform administrative functions such as starting and stopping services (IPsec tunnels, etc.) and configuration of the log export functions to the Security Administrator. The configuration of the IPsec tunnels for securing distributed TOE traffic is also restricted to Security Administrators. Management of the X.509 certificate trust store is restricted to Security Administrators. Refer to FIA_X509_EXT.1/Rev, FIA_X509_EXT.2, and FIA_X509_EXT.3 for additional information. No administrative functions are available prior to authentication as a Security Administrator or to any non-privileged user.
FMT_SMF.1 FMT_SMF.1/VPN FMT_SMF.1/IPS FMT_SMF.1/FFW	Director	All administrative actions defined in FMT_SMF.1, FMT_SMF.1/VPN, FMT_SMF.1/IPS, and FMT_SMF.1/FFW may be performed via the Director GUI. A subset of these functions are also available via the remote or local CLI. Refer to the *Versa Operating System (VOS), Versa Director and Versa Analytics Version 22.1 Common Criteria Hardening Guide* for a complete description of all security management functions available through each interface. 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 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	TOE Component	How the SFR is Satisfied
FMT_SMR.2	Director	When the administrator logs in (for both CLI and GUI), the TOE automatically determines the role of the administrator. When the administrator is created, the administrator will be mapped to a one of the roles, Admin or Operator. The Admin role is recognized by the 'admin' user, when local authentication is used. This is equivalent to the "Security Administrator" role. The Operator role is recognized by any user that belongs to 'versa' group, when local authentication is used.

7.1.10. TRUSTED UPDATE (FPT_TUD_EXT.1, FMT_MOF.1/MANUALUPDATE)

TOE SFRs	TOE Component	How the SFR is Satisfied
FMT_MOF.1/ ManualUpdate FPT_TUD_EXT.1	VOS Director Analytics	Each TOE component has a specific version that can be queried by an administrator. When updates are made available by Versa, an administrator can obtain and install those updates from downloads.versa.com. 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. Versa packages are signed with RSA-SHA256. At the package update or package installation time, the preinstalled RSA public key is used to do signature verification. If the signature is not matched, the package upgrade will fail. The Security Administrator may also verify the integrity of the installation images manually by calculating a hash of the image and comparing it against the SHA256 checksums published along with the update packages. The currently running TOE version may be queried by running the *show system package-info* command or by viewing the 'About Versa Director' page in the GUI. The Branch and Controller devices may be queried by clicking on the 'Appliances' view. Each TOE component may be upgraded manually using the Director CLI by the Security Administrator. Each TOE component is updated individually. When an update is executed, it is immediately activated following the successful completion of the manual upgrade process. The TOE does not have the capability to have multiple system images in active memory that can be activated/deactivated on the fly, thus the concept of delayed activation is not supported. The TOE however does allow for multiple system images to be stored on the internal disk, but they cannot be activated unless the administrator performs an upgrade or downgrade process. In other words, only the currently installed image can be used to boot the TOE, and only one image may be installed at a time. In order for the TOE to use an alternate image, the upgrade process must be used.

7.1.11. TOE ACCESS (FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4, FTA_TAB.1)

TOE SFRs	TOE Component	How the SFR is Satisfied
FTA_SSL_EXT.1 FTA_SSL.3 FTA_SSL.4	Director	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 of time, the TOE will terminate the session, requiring the administrator to log in again to establish a new session when needed. The default is set to 15 minutes. The CLI interface must be configured and can support values between 15 and 43200 seconds. Administrators may terminate their own session by selecting the 'Logout' operation from the GUI or by typing 'exit' or 'logout' at the CLI.
FTA_TAB.1	Director	The TOE has the functionality to present warning information to an administrator when attempting to login. There is no limit to the number of characters that can be entered in the login banner field through the GUI, but the banner is truncated to a 64K character limit for display. The administrator may manually edit the */opt/versa/etc/banner.net* file to present the login message to CLI users prior to authenticating.

7.1.12. TRUSTED PATH/CHANNEL COMMUNICATIONS (FCO_CPC_EXT.1, FTP_ITC.1, FTP_ITC.1/VPN, FTP_TRP.1/ADMIN)

TOE SFRs	TOE Component	How the SFR is Satisfied
FCO_CPC_EXT.1	VOS Director Analytics	VOS devices are added to the distributed TOE using Zero-Touch Provisioning. Two enablement methods are supported in the evaluated configuration: • URL-based ZTP—URL-based ZTP allows an onsite administrator to activate a VOS device. The administrator connects a laptop to the VOS device and clicks an email link to a staging Controller node, which completes the activation process. • From the CLI—A site administrator can connect to the CLI on a VOS device and run a staging script that activates the device. Both methods require a Security Administrator with direct control of the device and requires positive enablement on each component prior to joining the distributed TOE. No registration channel is used. Once activated, TOE components will communicate via the IPsec trusted channel defined in FPT_ITC.1. Without performing the enablement steps, the TOE components will not have the parameters necessary to establish a connection. Only Security Administrators may disable and remove TOE components via the Director.
FTP_ITC.1	VOS	During startup of the Branch appliance, an IPsec tunnel is established with the SD-WAN Controller. All communication between Versa VOS

<table>
<tr><th>TOE SFRs</th><th>TOE Component</th><th>How the SFR is Satisfied</th></tr>
<tr><td>FTP_ITC.1/VPN</td><td>Director
Analytics</td><td>(Branch appliance) and the Versa headend is sent via the IPsec tunnel.

The TOE supports establishing trusted channels between internal TOE components using the protocols described in the table below. All internal communications between the Versa headend and remote VOS Branch devices will be routed through this tunnel.
<table>
<tr><th>Source</th><th>Destination</th><th>Protocols / Data</th></tr>
<tr><td>VOS Branch</td><td>Headend - VOS Controller</td><td>IPsec /
Distributed TOE internal communications
Audit logs
TSF data</td></tr>
</table>
The TOE supports establishing trusted channels between TOE components and external entities:
<table>
<tr><th>Component</th><th>Destination</th><th>Protocol / Format</th></tr>
<tr><td>All</td><td>NTP server</td><td>Time synchronization via NTP within IPsec.</td></tr>
<tr><td>All</td><td>Syslog server</td><td>Syslog forwarding to an external receiver within IPsec.</td></tr>
<tr><td>VOS Branch</td><td>Peer VPN Gateway</td><td>Site-to-site IPsec tunnels</td></tr>
<tr><td>VOS Branch</td><td>VPN Client</td><td>IPsec VPN client connections.</td></tr>
</table>
All IPsec endpoints are authenticated using X.509 certificates.</td></tr>
<tr><td>FTP_TRP.1/Admin</td><td>Director</td><td>Remote administration of the TOE is performed via SSHv2 access to the Versa Director CLI and HTTPS/TLS access to the Director GUI.</td></tr>
</table>

7.1.13. STATEFUL TRAFFIC FILTERING (FPF_RUL_EXT.1, FFW_RUL_EXT.1, FDP_RIP.2)

TOE SFRs	TOE Component	How the SFR is Satisfied
FFW_RUL_EXT.1 FPF_RUL_EXT.1	VOS	During the VOS boot process, first the root partition and filesystem is located, checked and mounted. Next the init process is started, which runs the initialization scripts. These scripts involve different startup events that eventually bring the Versa networking services online. All packets are serviced by the kernel hooks. Every packet that enters the networking system (incoming or outgoing) will trigger these hooks as it progresses through the stack, allowing programs that register with these hooks to interact with the traffic at key points. The kernel modules associated with network processing register at these hooks in order to

TOE SFRs	TOE Component	How the SFR is Satisfied
		ensure that the traffic conforms to the conditions laid out by the firewall rules. If the Versa networking services have not been initialized successfully, or have failed to load, no packets will be permitted to flow through the TOE. The TSF also supports DoS protection to ensure that the traffic processed cannot exceed the capabilities of the networking stack, and will ensure that access policies are consistently enforced even during DoS attacks. VOS devices support routed, or Layer 3, interfaces. The interface associated with each physical network interface (PNIC) or virtual network interface (VNIC) is configured with an IP address. Based on the routing configuration, the traffic from the tenant is forwarded to the interfaces on the VOS device. The VOS device supports several routing instances or virtual routing functions (VRFs). Each VRF is associated with one or more interfaces on the VOS device, and the VOS device supports static routing, BGP, and OSPF. The traffic of a particular tenant enters a VOS device because the IP address of the routed interface is the next-hop address of the tenant traffic's final destination. Firewall policies can be applied on the traffic entering a VOS device, and the traffic is routed to the next hop (based on routing configuration) only if the security policy allows the traffic to be forwarded. A VOS firewall device can be installed as a bare metal or a virtual machine (VM). The security policies are applied to the traffic that enters the firewall through physical or virtual interfaces. The VOS firewall recognizes VLAN tags for incoming traffic and adds the appropriate VLAN tags to the outbound traffic. The following are typical scenarios for configuring traffic on a PNIC: • Non-VLAN Traffic—Traffic that is not tagged with VLAN and enters the firewall using PNIC is mapped to a single tenant. • VLAN Traffic—Traffic tagged with VLAN is mapped to one or more tenant. The VOS device creates a unique subinterface for each VLAN. Use one or more VLAN to configure the traffic identification for each tenant hosted on the VOS device. The following are typical scenarios for configuring traffic on a VNIC: • VLAN-mapped VNIC— If the VNIC is mapped by the hypervisor to a specific VLAN for the traffic that enters through the PNIC, then when the traffic enters the firewall through the VNIC, the VLAN is already stripped by the hypervisor. Therefore, all the traffic that enters through the VNIC is mapped to a single tenant. In this scenario, a single VNIC cannot support traffic from multiple tenants. • PNIC-mapped VNIC with non-VLAN traffic—When the hypervisor directly maps the VNIC to the PNIC without any VLAN stripping and if the traffic that enters the firewall through the VNIC is not VLAN tagged, all traffic that enters through the VNIC is mapped to a single tenant.

<table>
<tr><th>TOE SFRs</th><th>TOE Component</th><th>How the SFR is Satisfied</th></tr>
<tr><td></td><td></td><td>

PNIC-mapped VNIC with VLAN traffic—When the hypervisor directly maps the VNIC to the PNIC without any VLAN stripping and if the traffic that enters the firewall through the VNIC is VLAN tagged, traffic that belongs to different VLANs is mapped to one or more tenants.
You create a unique subinterface for each VLAN. You can configure the traffic identification using one or more VLANs for each tenant hosted on the VOS device.

The TSF supports a stateful packet filtering policy, and the following attributes are configurable within stateful traffic filtering rules for the associated protocols:
<table>
<tr><td>ICMPv4</td><td>Type</td></tr>
<tr><td></td><td>Code</td></tr>
<tr><td>ICMPv6</td><td>Type</td></tr>
<tr><td></td><td>Code</td></tr>
<tr><td>IPv4 (RFC 791)</td><td>Source address</td></tr>
<tr><td></td><td>Destination Address</td></tr>
<tr><td></td><td>Transport Layer Protocol</td></tr>
<tr><td>IPv6 (RFC 8200)</td><td>Source address</td></tr>
<tr><td></td><td>Destination Address</td></tr>
<tr><td></td><td>Transport Layer Protocol</td></tr>
<tr><td>TCP (RFC 793)</td><td>Source Port</td></tr>
<tr><td></td><td>Destination Port</td></tr>
<tr><td>UDP (RFC 768)</td><td>Source Port</td></tr>
<tr><td></td><td>Destination Port</td></tr>
</table>
Versa uses industry-standard network traffic generators to perform interoperability testing to ensure RFC compliance with the above standards.

All interfaces of the TOE are subject to processing rules which can be applied to each distinct network interface or sub-interface as described above.

The TSF is able to classify traffic according to stateful TCP and UDP sessions. To classify the traffic, stateful firewall verifies its destination port and then tracks the state of the traffic and monitors every interaction of each connection until it is closed. Stateful firewall grants or rejects access based not only on port and protocol but also on the packet history in the state table. When stateful firewall receives a packet, it checks the state table for an established connection or for a request for the incoming packet from an internal host. If nothing is found, the packet's access is subject to the access policy rule. Connections are removed after administrator-defined protocol timeout values and applied on the next received packet. If the session has been closed, the next received packet would be rejected.
</td></tr>
</table>

TOE SFRs	TOE Component	How the SFR is Satisfied
		For stateful firewall, Security Administrators configure a security access policy to classify traffic using a security access policy. A security access policy includes the stateful firewall rule that collates the defined objects and assigns an action to take based on the match conditions. Stateful firewall focuses on examining the information in Layer 2 (link layer), Layer 3 (network), and Layer 4 (transport) packets. For these packets, their Layer 3 and 4 information (IP address and TCP/UDP port number) is verified against the information stored in the state table to confirm that they are part of the current exchange. This method increases overall firewall performance because only the initiating packets must be unencapsulated for these layers and all layers up to the application layer (Layer 7). For more advanced inspection capabilities, stateful targets vital packets for Layer 7 (application) examination, such as the packet that initializes a connection. If the inspected packet matches an existing firewall rule that permits it, the packet is passed and an entry is added to the state table. From this point forward, because the packets in that communication session match an existing state table entry, they are allowed access without a call for further application layer inspection. Each security access policy consists of one or more rules. Each rule consists of match criteria and enforcement actions. You can use one or more of these traffic attributes to specify the match criteria: • IP headers • Domain names • Services, based on port and protocol • Source and destination geographic location • Source and destination IP addresses • Source and destination zones • Time-of-day scheduling For TCP, the TSF uses the following attributes to determine if packets are associated with an existing session: source and destination addresses, source and destination ports, sequence number, and individual flags. While UDP is a stateless protocol, the TSF uses the following attributes to determine if packets are associated with an existing session: source and destination addresses, source and destination ports. ICMP is also a stateless protocol however the TSF uses the following attributes to determine if packets are associated with an existing session: source and destination addresses, type, and code. A rule is triggered when all match criteria defined in the rule matches the payload. All rules in the security access policy are evaluated starting with the first rule in the policy. The first rule that matches is selected and the corresponding security actions are enforced. No other rules are evaluated once a match is found. It is recommended that in a security policy to configure more specific rules first and then configure generic rules, followed by a final deny-all

TOE SFRs	TOE Component	How the SFR is Satisfied

		rule. The TOE does not prevent administrators from applying conflicting rules.
		
		For a stateful firewall policy, administrators may configure the following enforcement actions:
		
		• Logging
		  o Start
		  o End
		  o Both
		  o Never
		• Action
		  o Allow—Allow sessions that match the configured rule to pass.
		  o Deny—Drop sessions that match the rule.
		  o Reject—Drop sessions that match the rule and sends a TCP reset (RST) or a UDP ICMP port unreachable message.
		
		The TSF may be configured to automatically drop the following packet types within an access policy (which in turn may associated with a LEF profile for logging):
		
		• All fragmented packets (counters)
		• Loose-source routing
		• Strict-source routing
		• Record route
		• Broadcast source
		• Multicast source
		• Loopback source address
		• Unspecified or reserved IP (RFC 5735, RFC 3513)
		• Packets where the source address is equal to the address of the network interface where the network packet was received
		• Packets where the source or destination address of the network packet is a link-local address
		• Packets where the source address does not belong to the networks associated with the network interface where the network packet was received – the access policy will determine which zones the rules are associated with and therefore the networks associated with each zone.
		
		The TSF implements TCP SYN flood protection under DoS Protection or Zone Protection profiles. DoS protection is applied where the TOE is deployed at the perimeter of a network on which services are accessed externally through the VOS, where Zone Protection is applicable to an entire zone. Thresholds may be set for the number of TCP packets per second across three levels:

TOE SFRs	TOE Component	How the SFR is Satisfied
		• Alarm rate – the rate at which a log will be generated • Action rate – The rate at which the TOE will drop packets. By default, the firewall uses SYN Cookies to track valid connections, but may be configured to randomly drop packets. • Maximum rate – The rate at which all packets would be dropped for a configurable duration. Stale connections (including half-open connections) will be removed after the defined protocol timeout value.
FDP_RIP.2	VOS	The TSF ensures that no data will be reused when processing network packets. When received on an interface, traffic is copied from the NIC into the userspace Versa services (bypassing Linux kernel) using mbufs. Each packet that is copied is associated with an mbuf. When the software is initialized, a pool of mbufs is instantiated and handed to the Versa applications for processing. The data plane management service will recycle mbufs for packets that enter and leave the device, in which case the mbuf is zeroized before being allocated for the next packet.

7.1.14. INTRUSION DETECTION AND PREVENTION (IPS_ABD_EXT.1, IPS_IPB_EXT.1, IPS_NTA_EXT.1, IPS_SBD_EXT.1)

TOE SFRs	TOE Component	How the SFR is Satisfied

IPS_IPB_EXT.1	VOS	IP address filters are based on the following IP address attributes:
		• IP reputation—Administrators can create IP-filtering profiles with the following predefined IP reputations:
		  ○ BotNets
		  ○ Denial of service
		  ○ Phishing
		  ○ Proxy
		  ○ Reputation
		  ○ Scanners
		  ○ Spam sources
		  ○ Web attacks
		  ○ Windows exploits
		• Geolocation—Versa Networks provides a list of predefined regions that you can use to create IP-filtering profiles based on geolocation.
		Administrators define IP-filtering profiles to filter traffic based on the IP address attributes. Each IP-filtering profile object can specify the following:
		• Allow lists for IP addresses
		• Deny lists for IP addresses
		• DNS reverse lookup configurations

TOE SFRs	TOE Component	How the SFR is Satisfied
		• Rules for geolocation-based actions • Rules for IP reputation–based actions Administrators can configure rules to match the IP address based on the following match criteria: • Destination IP address • Source IP address • Source and destination IP address • Source or destination IP address Administrators can enforce the following actions when a session's IP address matches the conditions in an IP-filtering profile: • Allow • Alert • Drop packet • Drop session • Reset
IPS_ABD_EXT.1 IPS_NTA_EXT.1 IPS_SBD_EXT.1	VOS	NGFW provides network protection beyond the protection based on ports, protocols, and IP addresses. In addition to traditional firewall capabilities, NGFW includes filtering functions such as intrusion prevention system (IPS). IP filtering and vulnerability policies are applied to NGFW security access policies. In the policy, administrators define the traffic to match based on various parameters, such as zones and applications, and configure the policy to enforce the action defined in vulnerability profile. It is recommended to use the predefined vulnerability profiles, however administrators may create custom vulnerability profiles. Then, the administrator must associate the vulnerability profiles with a next-generation firewall (NGFW) security profile (also called an access policy profile) in an NGFW policy. An NGFW security profile comprises an ordered set of one or more policy rules. Each policy rule comprises a set of match criteria and enforcement actions. As with firewall access policies, a rule is triggered when all match criteria defined in the rule matches the payload. All rules in the security access policy are evaluated starting with the first rule in the policy. The first rule that matches is selected and the corresponding security actions are enforced. No other rules are evaluated once a match is found. It is recommended that in a security policy to configure more specific rules first and then configure generic rules, followed by a final deny-all rule. The TOE does not prevent administrators from applying conflicting rules. Since IP filtering, vulnerability, and override settings may all be associated with an access rule, it is recommended to create the rules in the order in which the desired filtering needs to occur.

TOE SFRs	TOE Component	How the SFR is Satisfied
		The following protocols are supported for NGFW and IDP inspection policies: • IPv4 • IPv6 • ICMPv4 • ICMPv6 • TCP • UDP Versa uses industry-standard network traffic generators to perform interoperability testing to ensure compliance with the above protocols. Management Ethernet interfaces are logically separated from the Ethernet data ports and cannot be used as a sensor interface. The TSF supports both in-line and promiscuous modes on any available Ethernet data port. A minimum of two Ethernet data ports is required for in-line mode. Rules may be associated with distinct network interfaces, or groups of interfaces, referred to as zones. A zone profile defines flood protection, scan protection, and traffic anomaly protection information, and it is applied to all traffic flows that enter the zone through the interfaces associated with the zone. The zone protection profile can detect and prevent the following types of traffic from entering the networks in the zone: • Traffic floods of various protocols, such as TCP, UDP, and ICMP • Port scans, host sweeps, and other types of reconnaissance traffic • Malicious or spoofed packets Signature based detection applies a set of pre-defined rules or custom rules. Rules are based on the snort rule format. Snort rules are divided into two logical sections, the rule header and the rule options. The rule header contains the rule's action, protocol, source and destination IP addresses and netmasks, and the source and destination ports information, and a series of customizable rule options which cover all the fields described in IPS_SBD_EXT.1.5. Using the «content» keyword allows for a string in quotes to be used for detection. Contents match on bytes. There are 256 different values of a byte (0-255). You can match on all characters; from a to z, upper case and lower case, and special characters. Not all of the bytes are printable characters, and others have sig. For these bytes, heximal notations are used. The TSF also supports anomaly detection, which monitors a network for unusual events or trends. Vulnerability profiles may be configured to compare an observed event with the baseline of the normal

TOE SFRs	TOE Component	How the SFR is Satisfied
		traffic. Anomaly detection detects patterns that are normally not present in the traffic, so it is useful for detecting new attacks. The following actions may be configured in a vulnerability profile which are taken on matching anomaly rules: • Allow • Alert • Drop packet • Drop session • Reject • Reset client • Reset server Throughput rates are configured within a DoS protection profile. Time of day settings are configured via Schedule Objects which are applied to NGFW security policies. Frequency options are set under Thresholds within a vulnerability profile. Thresholds may be defined for each Security Scanner, or protocol parser. Within a zone protection profile, the following options may be selected in order to drop packets involved in attacks as defined in IPS_SBD_EXT.1. These include: • Fragmented IP packets • Spoofed IP packets • Fragmented ICMP packets • Large ICMP packets • Packets with improper TCP flags • Malformed UDP packets DoS Flood thresholds may be defined for ICMP, IP, TCP, and UDP. For TCP, packets may be randomly dropped or SYN cookies may be used to ensure that valid connections are not dropped during a SYN flood attack. SYN cookies are the default behavior.

7.2. NIST CAVP CERTIFICATES

The table below details the NIST CAVP certificates used to satisfy FCS_CKM.*, FCS_COP.1/*, and FCS_RBG_EXT.1 requirements.

Algorithm	Requirement (SFR)	Mode/Method	Capabilities	Operational Environment	CAVP Certificate
Versa Java Crypto Module					
AES	FCS_COP.1/ DataEncryption	FIPS PUB 197 CBC	• Direction: Decrypt, Encrypt • Key Length: 128, 256	OpenJDK 11 on Ubuntu 18.04 on ESXi 7.0 on Intel (R) Xeon (R) D-1587 with AES-NI	A5145
	FCS_COP.1/ DataEncryption	NIST SP 800-38D GCM	• Direction: Decrypt, Encrypt • IV Generation: External • Key Length: 128, 256 • Tag Length: 96, 128 • IV Length: 96 • Payload Length: 64, 128, 192 • AAD Length: 128, 256		
ECDSA	FCS_CKM.1 FCS_COP.1/ SigGen	FIPS PUB 186-4 KeyGen KeyVer SigGen SigVer	• Curve: P-256, P-384, P-521 • Secret Generation Mode: Extra Bits, Testing Candidates • Hash Algorithm: SHA-256, SHA2-384, SHA2-512		
DRBG	FCS_RBG_EXT.1	NIST SP 800-90A HMAC_DRBG	• Prediction Resistance: Yes • Supports Reseed • Mode: SHA2-512 • Entropy Input: 512 • Nonce: 512 • Personalization String Length: 512 • Additional Input: 512 • Returned Bits: 2048		
HMAC	FCS_COP.1/ KeyedHash	FIPS PUB 198-1 HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512	• MAC: 256, 384, 512 Increment 8 • Key Length: 8-2048 Increment 8		
KAS-ECC	FCS_CKM.2	SP 800-56Arev3	• Domain Parameter Generation Methods: P-256, P-384, P-521		

Algorithm	Requirement (SFR)	Mode/Method	Capabilities	Operational Environment	CAVP Certificate
			• Function: Key Pair Generation, Partial Validation • Scheme: ephemeralUnified: • KAS Role: Initiator, Responder • KDF Methods: oneStepKdf: • Auxiliary Function Methods: ○ SHA-256, SHA-384, SHA-512 • MAC Salting Methods: default, random • Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo • Fixed Info Encoding: Concatenation • Key Length: 256		

KAS-FFC-SSC	FCS_CKM.1, FCS_CKM.2	SP 800-56Arev3	• Domain Parameter Generation Methods: FC, MODP-2048, MODP-4096, MODP-8192
			• Scheme:
			  ○ dhEphem
			  ▪ KAS Role: initiator, responder		

RSA	FCS_CKM.1
	FCS_COP.1/ SigGen
		FIPS PUB 186-4
		KeyGen
		SigGen
		SigVer
			• Key Generation Mode: B.3.3
			  ○ Properties:
			  ▪ Modulo: 2048, 3072
			  ▪ Primality Tests: Table C.2
			• Public Exponent Mode: Random
			• Private Key Format: Chinese Remainder Theorem
			• Signature Type: PKCS 1.5, PKCSPSS
			• Properties:
			  ○ Modulo: 2048, 3072
			  ▪ Hash Algorithm: SHA2-256,		

Algorithm	Requirement (SFR)	Mode/Method	Capabilities	Operational Environment	CAVP Certificate
			SHA2-384, SHA2-512		
SHS	FCS_COP.1/ Hash	FIPS PUB 180-4 SHA-1 SHA2-256 SHA2-384 SHA2-512	• Message Length: 0-65536 Increment 8		
VOS TLS Cryptographic Module					
AES	FCS_COP.1/ DataEncryption	FIPS PUB 197 CBC, CTR	• Direction: Decrypt, Encrypt • Key Length: 128, 256	Ubuntu 18.04 on AMD EPYC 7713P with AES-NI Ubuntu 18.04 on ESXi 7.0 on Intel (R) Xeon (R) D-1587 with AES-NI (Versa Controller) Ubuntu 18.04 on ESXi 7.0 on Intel (R) Xeon (R) D-1587 with AES-NI (Versa Director)	A5144
	FCS_COP.1/ DataEncryption	GCM	• Direction: Decrypt, Encrypt • IV Generation: Internal • IV Generation Mode: 8.2.1 • Key Length: 128, 256 • Tag Length: 32, 64, 96, 104, 112, 120, 128 • IV Length: 96, 1024 • Payload Length: 504, 512, 1016, 1024 • AAD Length: 0, 504, 512, 1016, 1024		
ECDSA	FCS_CKM.1/ IKE FCS_COP.1/ SigGen	FIPS PUB 186-4 KeyGen KeyVer SigGen SigVer	• P-256, P-384, P-521 • Secret Generation Mode: Extra Bits, Testing Candidates • Curve: P-256, P-384, P-521 • Hash Algorithm: SHA2-256, SHA2-384, SHA2-512	Ubuntu 18.04 on Intel (R) Xeon (R) D-2187NT with AES-NI Ubuntu 18.04 on Intel (R) Xeon (R) Gold 6252N with AES-NI Ubuntu 18.04 on KVM on Ubuntu 18.04 on Intel (R) Xeon (R) D-1587 with AES-NI	
DRBG	FCS_RBG_EXT.1	SP 800-90A CTR_DRBG	• Mode: AES-256 • Derivation Function Enabled: Yes • Additional Input: 0-256 • Entropy Input: 256 • Nonce: 128 • Personalization String Length: 0-256 • Returned Bits: 128		
HMAC	FCS_COP.1/ KeyedHash	FIPS PUB 198-1 HMAC-SHA-1 HMAC-SHA2-256	• MAC: 160, 256, 384, 512 • Key Length: 8-524288 Increment 8		

Algorithm	Requirement (SFR)	Mode/Method	Capabilities	Operational Environment	CAVP Certificate
		HMAC-SHA2-384 HMAC-SHA2-512			

KAS-ECC	FCS_CKM.2	SP 800-56Arev3	• Domain Parameter Generation Methods: P-256, P-384
			• Scheme:
			  ○ ephemeralUnified:
			  ▪ KAS Role: initiator, responder		

RSA	FCS_CKM.1
	FCS_COP.1/ SigGen
		FIPS PUB 186-4
		KeyGen
		SigGen
		SigVer
			• Key Generation Mode: B.3.3
			  ○ Properties:
			  ▪ Modulo: 2048, 3072
			  ▪ Primality Tests: Table C.2
			• Public Exponent Mode: Random
			• Private Key Format: Standard
			• Signature Type: PKCS 1.5, PKCSPSS
			• Properties:
			  ○ Modulo: 2048, 3072
			  ▪ Hash Algorithm: SHA2-256, SHA2-384, SHA2-512		

SHS	FCS_COP.1/ Hash	FIPS 180-4 SHA-1 SHA2-256 SHA2-384 SHA2-512	• Message Length: 0-51200 Increment 8		
VOS IPsec Cryptographic Module					

Algorithm	Requirement (SFR)	Mode/Method	Capabilities	Operational Environment	CAVP Certificate
AES	FCS_COP.1/ Data Encryption	FIPS PUB 197 CBC, CTR	• Direction: Decrypt, Encrypt • Key Length: 128, 256	Ubuntu 18.04 on AMD EPYC 7713P with AES-NI Ubuntu 18.04 on ESXi 7.0 on Intel (R) Xeon (R) D-1587 with AES-NI Ubuntu 18.04 on Intel (R) Xeon (R) D-2187NT with AES-NI Ubuntu 18.04 on Intel (R) Xeon (R) Gold 6252N with AES-NI Ubuntu 18.04 on KVM on Ubuntu 18.04 on Intel (R) Xeon (R) D-1587 with AES-NI	A5147
	FCS_COP.1/ Data Encryption	GCM	• Direction: Decrypt, Encrypt • IV Generation: Internal • IV Generation Mode: 8.2.1 • Key Length: 128, 256 • Tag Length: 64, 96, 128 • IV Length: 96 • Payload Length: 504-896 Increment 8 • AAD Length: 256-1024 Increment 8		
ECDSA	FCS_COP.1/ SigGen	FIPS PUB 186-4 SigGen SigVer	• P-256, P-384, P-521 • Secret Generation Mode: Extra Bits, Testing Candidates • Curve: P-256, P-384, P-521 • Hash Algorithm: SHA2-256, SHA2-384, SHA2-512		
HMAC	FCS_COP.1/ KeyedHash	FIPS PUB 198-1 HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512	• MAC: 160, 256, 384, 512 • Key Length: 8-512000 Increment 8		
KAS-ECC-SSC	FCS_CKM.2	SP 800-56Arev3	• Domain Parameter Generation Methods: P-256, P-384 • Scheme: o ephemeralUnified:		

Algorithm	Requirement (SFR)	Mode/Method	Capabilities	Operational Environment	CAVP Certificate
			▪ KAS Role: initiator, responder		
RSA	FCS_COP.1/ SigGen	FIPS PUB 186-4 SigGen SigVer	• Key Generation Mode: B.3.3 o Properties: ▪ Modulo: 2048, 3072 ▪ Primality Tests: Table C.2 • Public Exponent Mode: Random • Private Key Format: Standard • Signature Type: PKCS 1.5 • Properties: o Modulo: 2048, 3072 ▪ Hash Algorithm: SHA2-256, SHA2-384, SHA2-512		
SHS	FCS_COP.1/ Hash	FIPS 180-4 SHA-1 SHA2-256 SHA2-384 SHA2-512	• Message Length: 0-51200 Increment 8		

7.3. CRITICAL SECURITY PARAMETERS

The table below identifies critical security parameters utilized by the TSF.

Key	Algorithm/ Type	Generation/Input	Storage	Zeroization
Versa Director				
SSH host keypair	ECDSA	Seed generated internally from DRBG. Private key generated from KeyGen function. Public key derived from private key.	Plaintext (Flash)	Linux *rm* command
SSH user public key	ECDSA	Entered by operator	Plaintext (flash)	Linux *rm* command
SSH ECDH public/private keypair	ECDH domain parameters	Generated according to SP 800-56Arev3	Plaintext (RAM)	Automatically overwritten with zeroes at the end of SSH session
SSH session encryption key	AES key used to protect SSH sessions.	Derived according to SP 800-135rev1.	Plaintext (RAM)	Automatically overwritten with zeroes at the end of TLS session
SSH session authentication key	HMAC key used to protect SSH sessions.	Derived according to SP 800-135rev1.	Plaintext (RAM)	Automatically overwritten with zeroes at the end of SSH session
TLS server public/private keypair	ECDSA, RSA	Seed generated internally from DRBG. Private key generated from KeyGen function. Public key derived from private key.	Plaintext (Flash)	Linux *rm* command
TLS ECDH public/private keypair	ECDH domain parameters	Generated according to SP 800-56Arev3	Plaintext (RAM)	Automatically overwritten with zeroes at the end of TLS session
TLS session encryption key	AES key used to protect TLS sessions.	Derived according to SP 800-135rev1.	Plaintext (RAM)	Automatically overwritten with zeroes at the end of TLS session
TLS session authentication key	HMAC key used to protect TLS sessions.	Derived according to SP 800-135rev1.	Plaintext (RAM)	Automatically overwritten with zeroes at the end of TLS session
TLS pre-master secret	Shared secret used to derive master keys	Generated according to SP 800-56Arev3	Plaintext (RAM)	Automatically overwritten with zeroes at the end of TLS session
TLS master secret	Used to derive session keys	Derived according to SP 800-135rev1	Plaintext (RAM)	Automatically overwritten with zeroes at the end of TLS session

Key	Algorithm/ Type	Generation/Input	Storage	Zeroization
Operator password	SHA-512 hash	Entered from operator during password change events	SHA-512 hash	Overwritten with new hash value
Versa VOS SD-WAN Controller				
IPsec public/private keypair	RSA, ECDSA	Seed generated internally from DRBG. Private key generated from KeyGen function. Public key derived from private key.	Plaintext (Flash)	*request system load-default* command
IPsec ECDH public/private keypair	ECDH domain parameters	Generated according to SP 800-56Arev3	Plaintext (RAM)	Automatically overwritten with zeroes at the end of IPsec session
IKE/IPsec session encryption key	AES key used to protect IKEv2 SA and Child SAs.	Derived according to SP 800-135rev1.	Plaintext (RAM)	Automatically overwritten with zeroes at the end of IPsec session
IKE/IPsec session authentication key	HMAC key used to protect IKEv2 SA and Child SAs.	Derived according to SP 800-135rev1.	Plaintext (RAM)	Automatically overwritten with zeroes at the end of IPsec session
Versa VOS Branch				
IPsec public/private keypair	RSA, ECDSA	Seed generated internally from DRBG. Private key generated from KeyGen function. Public key derived from private key.	Plaintext (Flash)	*request system load-default* command
IPsec ECDH public/private keypair	ECDH domain parameters	Generated according to SP 800-56Arev3	Plaintext (RAM)	Automatically overwritten with zeroes at the end of IPsec session
IKE/IPsec session encryption key	AES key used to protect IKEv2 SA and Child SAs.	Derived according to SP 800-135rev1.	Plaintext (RAM)	Automatically overwritten with zeroes at the end of IPsec session
IKE/IPsec session authentication key	HMAC key used to protect IKEv2 SA and Child SAs.	Derived according to SP 800-135rev1.	Plaintext (RAM)	Automatically overwritten with zeroes at the end of IPsec session

7.4. IPv4 AND IPv6 TRANSPORT LAYER PROTOCOLS

The below table identifies all IPv4 and IPv6 Transport Layer Protocols.

IPv4	
Transport Layer Protocol 1	Internet Control Message
Transport Layer Protocol 2	Internet Group Management
Transport Layer Protocol 3	Gateway to Gateway
Transport Layer Protocol 4	IP in IP (encapsulation)
Transport Layer Protocol 5	Stream
Transport Layer Protocol 6	Transmission Control
Transport Layer Protocol 7	UCL
Transport Layer Protocol 8	Exterior Gateway Protocol
Transport Layer Protocol 9	Any private interior gateway
Transport Layer Protocol 10	BBN RCC Monitoring
Transport Layer Protocol 11	Network Voice Protocol
Transport Layer Protocol 12	PUP
Transport Layer Protocol 13	ARGUS
Transport Layer Protocol 14	EMCON
Transport Layer Protocol 15	Cross Net Debugger
Transport Layer Protocol 16	Chaos
Transport Layer Protocol 17	User Datagram
Transport Layer Protocol 18	Multiplexing
Transport Layer Protocol 19	DCN Measurement Subsystems
Transport Layer Protocol 20	Host Monitoring
Transport Layer Protocol 21	Packet Radio Measurement
Transport Layer Protocol 22	XEROX NS IDP
Transport Layer Protocol 23	Trunk 1
Transport Layer Protocol 24	Trunk 2
Transport Layer Protocol 25	Leaf 1
Transport Layer Protocol 26	Leaf 2
Transport Layer Protocol 27	Reliable Data Protocol
Transport Layer Protocol 28	Internet Reliable Transaction
Transport Layer Protocol 29	ISO Transport Protocol Class 4
Transport Layer Protocol 30	Bulk Data Transfer Protocol
Transport Layer Protocol 31	MFE Network Services Protocol
Transport Layer Protocol 32	MERIT Internodal Protocol
Transport Layer Protocol 33	Sequential Exchange Protocol
Transport Layer Protocol 34	Third Party Connect Protocol
Transport Layer Protocol 35	Inter-domain Policy Routing Protocol
Transport Layer Protocol 36	XTP
Transport Layer Protocol 37	Datagram Delivery Protocol

Transport Layer Protocol 38	IDPR Control Message Transport Protocol
Transport Layer Protocol 39	TP++ Transport Protocol
Transport Layer Protocol 40	IL Transport Protocol
Transport Layer Protocol 41	Simple Internet Protocol
Transport Layer Protocol 42	Source Demand Routing Protocol
Transport Layer Protocol 43	SIP Source Route
Transport Layer Protocol 44	SIP Fragment
Transport Layer Protocol 45	Inter-domain Routing Protocol
Transport Layer Protocol 46	Reservation Protocol
Transport Layer Protocol 47	General Routing Encapsulation
Transport Layer Protocol 48	Mobile Host Routing Protocol
Transport Layer Protocol 49	BNA
Transport Layer Protocol 50	SIPP Encap Security Payload
Transport Layer Protocol 51	SIPP Authentication Header
Transport Layer Protocol 52	Integrated Net Layer Security TUBA
Transport Layer Protocol 53	IP with Encryption
Transport Layer Protocol 54	NBMA Next Hop Resolution Protocol
Transport Layer Protocol 61	Any host internal protocol
Transport Layer Protocol 62	CFTP
Transport Layer Protocol 63	Any local network
Transport Layer Protocol 64	SATNET and Backroom EXPAK
Transport Layer Protocol 65	Kryptolan
Transport Layer Protocol 66	MIT Remote Virtual Disk Protocol
Transport Layer Protocol 67	Internet Pluribus Packet Core
Transport Layer Protocol 68	Any distributed file system
Transport Layer Protocol 69	SATNET Monitoring
Transport Layer Protocol 70	VISA Protocol
Transport Layer Protocol 71	Internet Packet Core Utility
Transport Layer Protocol 72	Computer Protocol Network Executive
Transport Layer Protocol 73	Computer Protocol Heart Beat
Transport Layer Protocol 74	Wang Span Network
Transport Layer Protocol 75	Packet Video Protocol
Transport Layer Protocol 76	Backroom SATNET Monitoring
Transport Layer Protocol 77	SUN ND PROTOCOL Temporary
Transport Layer Protocol 78	WIDEBAND Monitoring
Transport Layer Protocol 79	WIDEBAND EXPAK
Transport Layer Protocol 80	ISO Internet Protocol
Transport Layer Protocol 81	VMTP
Transport Layer Protocol 82	SECURE VMTP
Transport Layer Protocol 83	VINES
Transport Layer Protocol 84	TTP

Transport Layer Protocol 85	NSFNET IGP
Transport Layer Protocol 86	Dissimilar Gateway Protocol
Transport Layer Protocol 87	TCF
Transport Layer Protocol 88	IGRP
Transport Layer Protocol 89	OSPFIGP
Transport Layer Protocol 90	Sprite RPC Protocol
Transport Layer Protocol 91	Locus Address Resolution Protocol
Transport Layer Protocol 92	Multicast Transport Protocol
Transport Layer Protocol 93	AX.25 Frames
Transport Layer Protocol 94	IP within IP Encapsulation Protocol
Transport Layer Protocol 95	Mobile Internetworking Control Protocol
Transport Layer Protocol 96	Semaphore Communications Security Protocol
Transport Layer Protocol 97	Ethernet within IP Encapsulation
Transport Layer Protocol 98	Encapsulation Header
Transport Layer Protocol 99	Any private encryption scheme
Transport Layer Protocol 100	GMTP
IPv6	
Transport Layer Protocol 1	Internet Control Message
Transport Layer Protocol 2	Internet Group Management
Transport Layer Protocol 3	Gateway to Gateway
Transport Layer Protocol 4	IPv4 encapsulation
Transport Layer Protocol 5	Stream
Transport Layer Protocol 6	Transmission Control
Transport Layer Protocol 7	CBT
Transport Layer Protocol 8	Exterior Gateway Protocol
Transport Layer Protocol 9	Any private interior gateway
Transport Layer Protocol 10	BBN RCC Monitoring
Transport Layer Protocol 11	Network Voice Protocol
Transport Layer Protocol 12	PUP
Transport Layer Protocol 13	ARGUS
Transport Layer Protocol 14	EMCON
Transport Layer Protocol 15	Cross Net Debugger
Transport Layer Protocol 16	Chaos
Transport Layer Protocol 17	User Datagram
Transport Layer Protocol 18	Multiplexing
Transport Layer Protocol 19	DCN Measurement Subsystems
Transport Layer Protocol 20	Host Monitoring
Transport Layer Protocol 21	Packet Radio Measurement
Transport Layer Protocol 22	XEROX NS IDP
Transport Layer Protocol 23	Trunk 1
Transport Layer Protocol 24	Trunk 2

Transport Layer Protocol 25	Leaf 1
Transport Layer Protocol 26	Leaf
Transport Layer Protocol 27	Reliable Data Protocol
Transport Layer Protocol 28	Internet Reliable Transaction
Transport Layer Protocol 29	Transport Protocol Class 4
Transport Layer Protocol 30	Bulk Data Transfer Protocol
Transport Layer Protocol 31	MFE Network Services Protocol
Transport Layer Protocol 32	MERIT Internodal Protocol
Transport Layer Protocol 33	Datagram Congestion Control Protocol
Transport Layer Protocol 34	Third Party Connect Protocol
Transport Layer Protocol 35	Inter-domain Policy Routing Protocol
Transport Layer Protocol 36	XTP
Transport Layer Protocol 37	Datagram Delivery Protocol
Transport Layer Protocol 38	IDPR Control Message Transport Protocol
Transport Layer Protocol 39	TP++ Transport Protocol
Transport Layer Protocol 40	IL Transport Protocol
Transport Layer Protocol 41	IPv6 encapsulation IPv6
Transport Layer Protocol 42	Source Demand Routing Protocol
Transport Layer Protocol 43	Intentionally blank
Transport Layer Protocol 44	Intentionally blank
Transport Layer Protocol 45	Inter-domain Routing Protocol
Transport Layer Protocol 46	Reservation Protocol
Transport Layer Protocol 47	General Routing Encapsulation
Transport Layer Protocol 48	Dynamic Source Routing Protocol
Transport Layer Protocol 49	BNA
Transport Layer Protocol 50	Intentionally Blank
Transport Layer Protocol 51	Intentionally Blank
Transport Layer Protocol 52	Integrated Net Layer Security
Transport Layer Protocol 53	IP with Encryption
Transport Layer Protocol 54	NBMA Address Resolution Protocol
Transport Layer Protocol 55	Mobility
Transport Layer Protocol 56	Transport Layer Security Protocol using Kryptonet key management
Transport Layer Protocol 57	SKIP
Transport Layer Protocol 58	ICMP for IPv6
Transport Layer Protocol 59	No Next Header for IPv6
Transport Layer Protocol 60	Intentionally Blank
Transport Layer Protocol 61	Any host internal protocol
Transport Layer Protocol 62	CFTP
Transport Layer Protocol 63	Any local network
Transport Layer Protocol 64	SATNET and Backroom EXPAK
Transport Layer Protocol 65	Kryptolan

Transport Layer Protocol 66	MIT Remote Virtual Disk Protocol
Transport Layer Protocol 67	Internet Pluribus Packet Core
Transport Layer Protocol 68	Any distributed file system
Transport Layer Protocol 69	SATNET Monitoring
Transport Layer Protocol 70	VISA Protocol
Transport Layer Protocol 71	Internet Packet Core Utility
Transport Layer Protocol 72	Computer Protocol Network Executive
Transport Layer Protocol 73	Computer Protocol Heart Beat
Transport Layer Protocol 74	Wang Span Network
Transport Layer Protocol 75	Packet Video Protocol
Transport Layer Protocol 76	Backroom SATNET Monitoring
Transport Layer Protocol 77	SUN ND PROTOCOL Temporary
Transport Layer Protocol 78	WIDEBAND Monitoring
Transport Layer Protocol 79	WIDEBAND EXPAK
Transport Layer Protocol 80	ISO Internet Protocol
Transport Layer Protocol 81	VMTP
Transport Layer Protocol 82	SECURE VMTP
Transport Layer Protocol 83	VINES
Transport Layer Protocol 84	TTP
Transport Layer Protocol 85	Internet Protocol Traffic Manager
Transport Layer Protocol 86	NSFNET IGP
Transport Layer Protocol 87	Dissimilar Gateway Protocol
Transport Layer Protocol 88	TCF
Transport Layer Protocol 89	EIGRP
Transport Layer Protocol 90	OSPFIGP
Transport Layer Protocol 91	Sprite RPC Protocol
Transport Layer Protocol 92	Locus Address Resolution Protocol
Transport Layer Protocol 93	Multicast Transport Protocol
Transport Layer Protocol 94	AX.25 Frames
Transport Layer Protocol 95	IP within IP Encapsulation Protocol
Transport Layer Protocol 96	Mobile Internetworking Control Pro.
Transport Layer Protocol 97	Semaphore Communications Sec. Pro.
Transport Layer Protocol 98	Ethernet within IP Encapsulation
Transport Layer Protocol 99	Encapsulation Header
Transport Layer Protocol 100	GMTP
Transport Layer Protocol 101	Ipsilon Flow Management Protocol
Transport Layer Protocol 102	PNNI over IP
Transport Layer Protocol 103	Protocol Independent Multicast
Transport Layer Protocol 104	ARIS
Transport Layer Protocol 105	SCPS Transport Layer Protocol
Transport Layer Protocol 106	QNX

Transport Layer Protocol 107	Active Networks
Transport Layer Protocol 108	Payload Compression Protocol
Transport Layer Protocol 109	Sitara Networks Protocol
Transport Layer Protocol 110	Compaq Peer Protocol
Transport Layer Protocol 111	IPX in IP
Transport Layer Protocol 112	Virtual Router Redundancy Protocol
Transport Layer Protocol 113	PGM Reliable Transport Protocol
Transport Layer Protocol 114	Any 0-hop protocol
Transport Layer Protocol 115	Layer Two Tunneling Protocol
Transport Layer Protocol 116	D-II Data Exchange (DDX)
Transport Layer Protocol 117	Interactive Agent Transfer Protocol
Transport Layer Protocol 118	Schedule Transfer Protocol
Transport Layer Protocol 119	SpectraLink Radio Protocol
Transport Layer Protocol 120	UTI
Transport Layer Protocol 121	Simple Message Protocol
Transport Layer Protocol 122	SM
Transport Layer Protocol 123	Performance Transparency Protocol
Transport Layer Protocol 124	ISIS over IPv4
Transport Layer Protocol 125	FIRE
Transport Layer Protocol 126	Combat Radio Transport Protocol
Transport Layer Protocol 127	Combat Radio User Datagram
Transport Layer Protocol 128	SSCOPMCE
Transport Layer Protocol 129	IPLT
Transport Layer Protocol 130	Secure Packet Shield
Transport Layer Protocol 131	Private IP Encapsulation within IP
Transport Layer Protocol 132	Stream Control Transmission Protocol
Transport Layer Protocol 133	Fibre Channel
Transport Layer Protocol 134	RSVP E2E IGNORE
Transport Layer Protocol 135	Mobility Header
Transport Layer Protocol 136	UDPLite
Transport Layer Protocol 137	MPLS in IP
Transport Layer Protocol 138	MANET Protocols
Transport Layer Protocol 139	Host Identity Protocol
Transport Layer Protocol 140	Shim6 Protocol
Transport Layer Protocol 141	Wrapped Encapsulating Security Payload
Transport Layer Protocol 142	Robust Header Compression