A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3

Security Target

25-January-2023

Revision: 1.0 (NDcPPv2.2e ST)

TABLE OF CONTENTS

DISCLAIMER

1. SECURITY TARGET INTRODUCTION

This Security Target for A10 Networks ACOS 5.2.1-P3 on A10 Thunder series devices contains the following sections:

- Section 1: Security Target Introduction
- Section 2: CC Conformance Claims
- Section 3: Security Problem Definition
- Section 4: Security Objectives
- Section 5: Security Functional Requirements
- Section 6: Security Assurance Requirements
- Section 7: TOE Summary Specification

1.1 ST AND TOE REFERENCE

This section provides information needed to identify and control this ST and its TOE.

Name	**Description**
ST Title	A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3 - Security Target
ST Revision	1.0
Author	A10 Networks, Inc.
cPP/EP Conformance	[NDcPPv2.2e]
TOE Reference	A10 Networks Thunder Series Appliances
TOE Hardware Models	TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655
TOE Software Version	ACOS 5.2.1-P3
TOE OS Kernel Version	Linux 4.19 LTS
TOE Developer	A10 Networks, Inc.

1.2 TOE OVERVIEW

The Target of Evaluation (TOE) is A10 Networks, Inc. Thunder-series of network appliances executing A10's Advanced Core Operating System (ACOS) 5.2.1-P3, a network device as defined in NDcPPv2.2e. A10 Thunder-series appliances are devices to provide organizations with networking services and capabilities including:

- Application Delivery Control (ADC),
- Carrier-Grade Networking (CGN),
- Convergent Firewall (CFW), and
- SSL Insight (SSLi)

Thunder ADC features provide a performant solution that enables customer enterprise and web applications to be highly available, accelerated and secure.

Thunder CGN features provide a performant and transparent network address and protocol translation that allows service providers and enterprises to extend IPv4 network connectivity while simultaneously transitioning to IPv6 standards.

Thunder CFW incorporates multiple security functions for enterprise and service provider deployments, including scalable and performant firewall, IPsec VPN, secure web gateway, Carrier-Grade (CG) Networks Address Translation (NAT) with integrated DDoS protection and traffic steering.

Thunder SSLi is a comprehensive SSL/TLS decryption solution that enables security deployments to efficiently analyse all enterprise traffic, ensuring compliance and privacy, and increasing performance of the organization's security stack.

Thunder ACOS supports a 64-bit, multi-CPU architecture built from the ground up to provide ADC, CGN, CFW, and SSLi services with high performance, scalability and reliability.

The following Figure 1 depicts the TOE boundary. As shown, an A10 Thunder-series appliance is a single hardware device that has management ports and network (or data plane) ports.

The TOE interfaces with the following non-TOE systems in its operational environment.

- local and remote administrative interfaces,
- Syslog server interface for external audit log storage,
- Network Time Protocol (NTP) server interface for reliable time information in audit records, and
- File server interface for trusted updates and configuration backups

The TOE also interfaces with a Certification Authority (CA) for server certificates and certificate validation using Certificate Revocation Lists (CRLs) and the Online Certificate Status Protocol (OCSP).

The TOE was evaluated as a standalone network device only. ACOS ADC, CGN, CFW, and SSLi data plane functions, while included in the product, were not evaluated during the TOE's evaluation under the NDcPP.

Only the functionality described in Section 5 of this Security Target is considered to be within the logical boundary of the TOE.

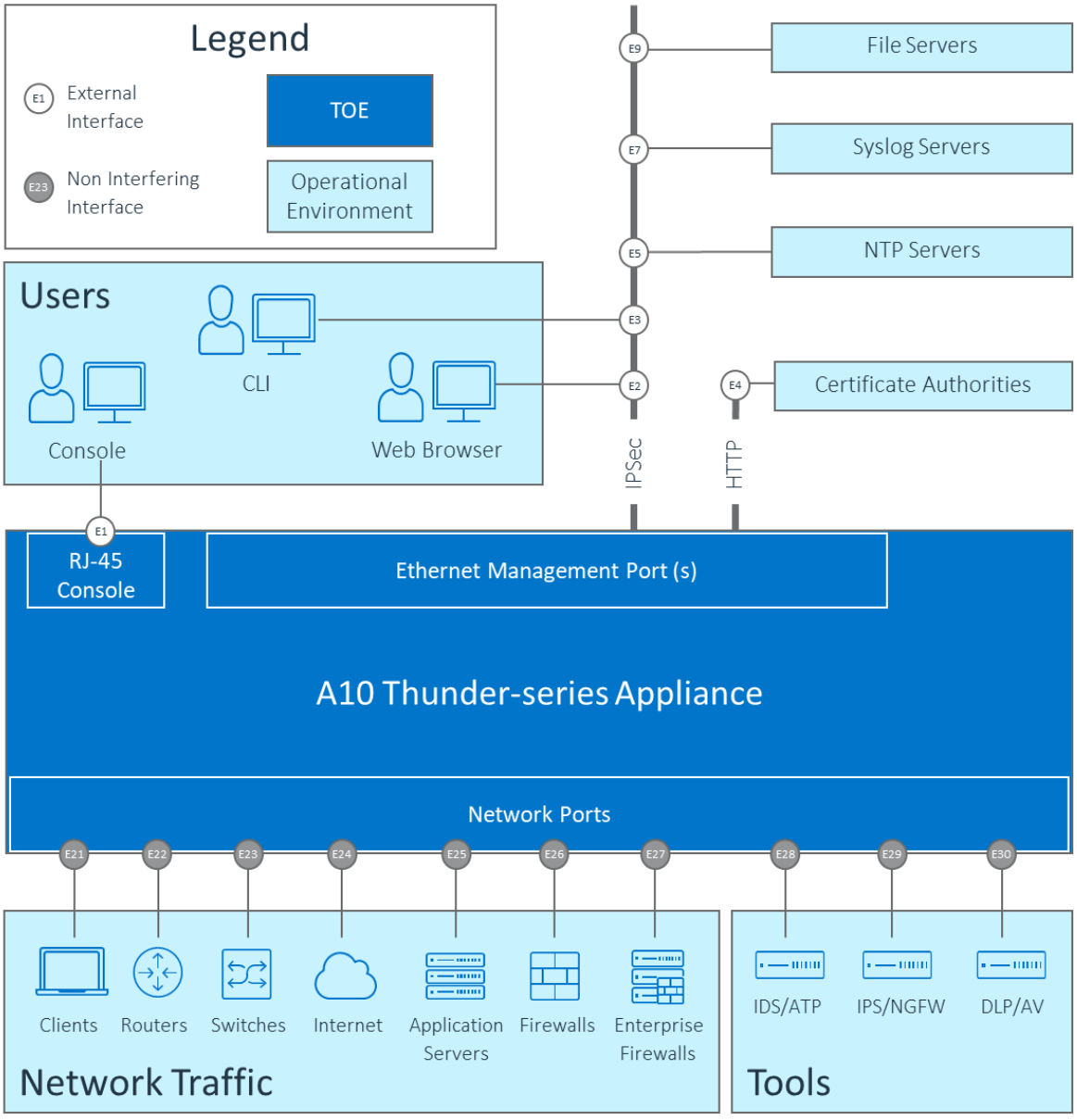

Figure 1: TOE Boundary for A10 Thunder-series Appliance

1.2.1 TOE Operational Environment

The TOE relies on a range of non-TOE devices for the operation of many of its features and capabilities when they are enabled. Though such devices may be necessary for the TOE's operation, they are not part of the TOE.

To the extent that TOE features and capabilities are enabled or supported by management operations on the TOE, the following additional non-TOE hardware (systems) and software elements can be necessary for the TOE's operation and are not part of the TOE. Communications with these elements will be as management plane trusted paths or trusted channels.

ELEMENT	DESCRIPTION
SYSLOG (audit log) Server	The TOE communicates with SYSLOG servers via IPsec for remote storage of audit and logging events reported by the TOE management and control planes.
NTP Servers	The TOE communicates with NTP servers via IPsec to synchronize date and time.
SSH Clients	The TOE can be managed via IPsec from terminal clients on remote administrator workstations accessing the management Command Line Interface (CLI) of the TOE.
Web GUI Browser Clients	The TOE can be managed via IPsec from web browsers on remote administrator workstations accessing the management web GUI of the TOE.
File Servers	The TOE communicates with file servers via IPsec to transfer files for purposes including: • configuration backup (restoration) from (to) the TOE • updates of the TOE • exporting and copying information from the TOE • importing information, including credentials and other data, to the TOE • loading management CLI and Web GUI credentials to the TOE
Distribution Points	The TOE communicates with CRL and OCSP distribution points via HTTP to confirming the validity and revocation status of certificates.

Table 2: Non-TOE Management Elements

1.2.2 TOE Documentation

The following constitute documentation of the TOE system and are downloadable from the A10 Networks support web site (https://support.a10networks.com). An A10 Networks support login ID and password is required to access online documentation.

- A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3 - Common Criteria Configuration Guide, 1.0, January 25,2023
- Thunder Series Installation Guide (for the given Thunder model)
- ACOS System and Network Configuration Documentation
    - ACOS 5.2.1-P3 System Configuration and Administration Guide **(SAG)**
- ACOS Admin and Application Access Security Documentation
    - ACOS 5.2.1-P3 Management Access and Security Guide **(MAS)**
    - ACOS 5.2.1-P3 IP Security Configuration Guide **(IPSEC)**
- ACOS Reference Documentation for User Interfaces Used to Configure the Device
    - ACOS 5.2.1-P3 Command Line Interface Reference **(CLI)**

1.3 TOE DESCRIPTION

The TOE is a standalone network device. The hardware and firmware components of the TOE are enclosed in a metal enclosure which is the physical boundary of the TOE.

The scope of each TOE appliance begins with a hardware appliance having physical connections to the deployed network environment. Within the appliance, ACOS is designed to control and enable access to the available functions (e.g., program execution, device access, facilitate device functions and capabilities). ACOS enforces applicable capability and security policies on network information flowing through the appliance.

By their nature TOE appliances are administratively closed systems, providing access only through ACOS defined interfaces (e.g. CLI and Web GUI) to administrators configured in ACOS for this purpose. TOE appliances do not expose OS Shell access to administrators.

At system start-up the system control is transferred from flash memory to dynamic memory under the control of ACOS using a built-in bootstrap. ACOS reads the configuration parameters from the configuration file in non-volatile memory and then initializes the necessary data structures in dynamic memory and begins operation.

During normal operation, IP packets are sent to the management IP address or through the appliance over one or more of its physical network interfaces. The appliance processes them according to the system's configuration and state information dynamically maintained by the appliance. This processing typically results in the data plane packets being forwarded out of the device over another interface. The TOE will process control and management plane packets destined for the TOE based on the requirements of the given protocol (e.g. IPSec, OSPF, etc).

1.3.1 TOE Models Evaluated

The following lists the TOE models in the evaluated configuration:

MODELS	DESCRIPTION
TH-4435	A10 Networks Thunder TH-4435 appliance
TH-5840-11	A10 Networks Thunder TH-5840-11 appliance
TH-7445	A10 Networks Thunder TH-7445 appliance
TH-7650-11	A10 Networks Thunder TH-7650-11 appliance
TH-7655	A10 Networks Thunder TH-7655 appliance

Table 1: Evaluated TOE Models

1.3.2 TOE Exclusions

The following are capabilities of the TOE but are not included in the evaluated configuration.

- **Insecure mode of operation** – the TOE provides an 'FIPS Mode' that enables the cryptographic self-tests and selected features. Operating the product outside of this mode of operation is not within the scope of the TSF.

- **Data plane features and capabilities** – The data plane of the TOE supports a vast majority of the distinguishing features and capabilities described in Section 1.2 above and is accordingly not within the scope of the TSF. To the extent that these features and capabilities involve configuration operations and exchanges on the management plane, these management-related communications are within the scope of the TSF.

- **Control plane features and capabilities** – To the extent that TOE features and capabilities are enabled and related control operations are to be performed, the following system functions and their related protocols may be necessary for the TOE's operation, though they are not within the scope of the TSF. Communications with these elements are beyond the scope of the NDcPP.

SYSTEM FUNCTION	PROTOCOLS
Management Control	DHCP, ICMP, IGMP, Traceroute
Routing Control	BGP, OSPF, RIP, ISIS, BDF
Link Layer Control	LACP, LLDP
A10 High Availability (HA) Control	A10 HA Protocols

Table 3: Non-TOE Control Elements (Protocols)

1.3.3 TOE Architecture

At the highest architectural level, the TOE consists of two (2) distinct planes, a management plane and a data plane. The management plane is responsible for summary control of the TOE device (startup, shutdown, etc), maintenance of the device configuration and stored information, and communications with external systems in the TOE's operational environment. The data plane processes traffic through the TOE.

The term ACOS (Advanced Core Operating System) is the name given to A10 distributed software installed and updated on the TOE. ACOS includes an underlying Linux-based operating system to support summary control and management services of the TOE.

ACOS management plane software and the Linux operating system operate on CPU cores separate from those used by the ACOS dataplane. Each plane operates with its own memory, along with memory shared to support cooperative access and processing needs within the system. The ACOS management plane employs the TOE's management port for communication with non-TOE elements in the TOE's operational environment. The TOE uses IPsec to protect communications with non-TOE systems in its operational environment, with cryptographic functionality provided by OpenSSL and the Linux Kernel Crytpo provider. Entropy and RNG needs of the ACOS management plane are supported by the Intel Secure Key capabilities of the underlying Intel Xeon processing devices.

The ACOS data plane software processes traffic through the TOE independent of the Linux OS/kernel using underlying A10 Flexible Traffic ASICs (FTAs), networking fabrics, and data plane processors included in the various TOE models. A10 Thunder models including those evaluated vary in terms of Xeon configuration (single vs dual), the underlying number of CPU cores supported, data plane port volumes/speeds, data plane FTAs, and data plane processors. Additional details for the various TOE models are included in the following subsection.

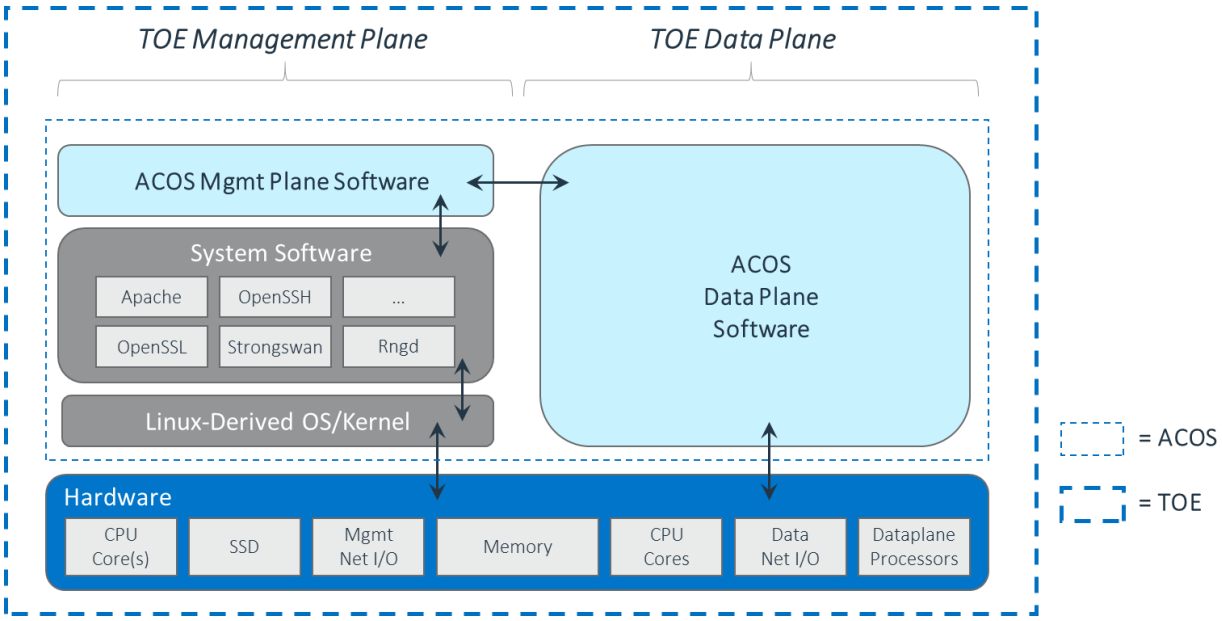

Figure 2: TOE Boundary for A10 Thunder-series Appliance

1.3.4 TOE Physical Boundary

The TOE is a hardware and software solution that is comprised of the security appliance models described above in Section 1.3 . The TOE guidance documentation that is considered to be part of the TOE can be found listed in the A10 Networks' Common Criteria Addendum document and is downloadable from the https://support.a10networks.com web site. An A10 Networks support login ID and password is required to access online documentation.

The network on which the TOE resides is considered part of the environment. The software is pre-installed and is comprised of only the software versions identified in Section 1.1. Software updates are downloadable from the A10 Networks web site. An A10 Networks support login ID and password is required to download software updates.

The model specific hardware and TOE configurations are shown in Table 4.

	TH-4435	TH-5840-11	TH-7445
1 GE Copper Ports	-	-	-
1 GE Fiber (SFP) Ports	-	-	-
1/10 GE Fiber (SFP+) Ports	16	48	48
25 GE Fibers (SFP28) Ports	-	-	-
40 GE Fiber (QSFP+)	-	-	-
100 GE Fiber	-	4 (QSFP28)	4 (QSFP28)
Management Ports	1 x Ethernet, 1 x RJ-45 Console, 1 x Lights Out Management		
Processor	Intel Xeon E5-2680v2 (10-cores) Ivy Bridge	Intel Xeon E5-2695v4 (18-cores) Broadwell	2x Intel E5-Xeon 2695v4 (36-cores) Broadwell
Memory	64 GB	64 GB/128 GB	128 GB
Storage	SSD	SSD	SSD
Hardware Acceleration	FTA-3, SPE	2 x FTA-4	3 x FTA-4, SPE
Data Plane Processor	Yes	Yes	Yes
Rack Units (mountable)	1 RU	1 RU	1 RU
Power Supply	Dual 1100W RPS,100 - 240 VAC, 50 – 60 Hz	Dual 1100W RPS,100 - 240 VAC, 50 – 60 Hz	Dual 1500W RPS,100 - 240 VAC, 50 – 60 Hz
Operating Temp	0° - 40° C	0° - 40° C	0° - 40° C

Table 4: TOE Appliances Models

	TH-7650-11	TH-7655
1 GE Copper Ports	-	-
1 GE Fiber (SFP) Ports	-	-
1/10 GE Fiber (SFP+) Ports	48	-
25 GE Fibers (SFP28) Ports	-	-
40 GE Fiber (QSFP+)	-	-
100 GE Fiber	4 (QSFP28)	16 (QSFP28)
Management Ports	1 x Ethernet, 1 x RJ-45 Console, 1 x Lights Out Management	
Processor	2x Intel Xeon Gold 6258R (56-cores)	2x Intel Xeon Gold 6258R (56-cores)
Microarchitecture	Cascade Lake	Cascade lake
Memory	256 GB	384 GB
Storage	SSD	SSD
Hardware Acceleration	2 x FTA-5	2 x FTA-5, SPE
Data Plane Processor	Yes	Yes
Rack Units (mountable)	1.5 RU	1.5 RU
Power Supply	Dual 1500W RPS,100 - 240 VAC, 50 – 60 Hz	Dual 1500W RPS,100 - 240 VAC, 50 – 60 Hz
Operating Temp	0° - 40° C	0° - 40° C

Table 4: TOE Appliances Models (cont)

1.3.5 TOE Logical Boundary

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Trusted Channel

1.3.5.1 Security Audit

Audit records are generated for various types of management activities and events. These records include the date and time stamp of the event, the event type, and the subject identity. The TOE can be configured to transmit audit data to a remote SYSLOG Servers using IPsec.

When SYSLOG Servers are unavailable, audit data is stored locally to ensure availability of the data. Local audit records provide administrators with a circular audit trail of configurable storage capacity. Locally stored audit logs can be backed up over an encrypted channel to an external file store.

1.3.5.2 Cryptographic Support

The TOE provides cryptographic support for services, based on OpenSSL and the Linux Kernel Crytpo provider, as described in Table 5. CAVP validation details for this support is provided in Table 6.

CRYPTOGRAPHIC METHOD	USE WITHIN THE TOE
Internet Key Exchange	Used to establish initial IPsec session.
ECDSA Signature Services	Used in IPsec session establishment
RSA Signature Services	Used in IPsec session establishment Used in secure software update
SP 800-90 DRBG	Used in IPsec session establishment.
SHS	Used in HMAC and digital signatures
HMAC	Used to provide IPsec traffic integrity verification
AES	Used to encrypt IPsec traffic
Diffie Hellman	Used in IPsec session establishment.

Table 5: TOE Cryptographic Services

ALGORITHM	CAVP CERT #	STANDARD	OPERATION	SFR
RSA	C1198, C1940 A1305	FIPS 186-4	Key Generation Signature Generation/ Verification	FCS_CKM.1 FCS_COP.1/SigGen
ECDSA	C1198, C1940	FIPS 186-4	Key Generation Signature Generation/ Verification	FCS_CKM.1 FCS_COP.1/SigGen
SP 800-90 DRBG	C1198, C1940	SP 800-90A	Random Bit Generation	FCS_RBG_EXT.1
SHS	C1198, C1940 A1181	ISO/IEC 10118-3:2004	Hashing	FCS_COP.1/Hash
HMAC-SHS	C1198, C1940 A1181	ISO/IEC 9797-2:2011	Keyed-Hashing	FCS_COP.1/KeyedHash
AES	C1198, C1940, A1181	AES specified in ISO 18033-3 CBC specified in ISO 10116 GCM specified in ISO 19772 CTR specified in ISO 10116	Encryption/ Decryption	FCS_COP.1/DataEncryption

Table 6: CAVP Certificates

1.3.5.3 Identification and Authentication

The TOE verifies the identity of users connecting to the TOE. All users must be identified and authenticated before being allowed to perform actions on the TOE. This is true of users accessing the TOE via the local console, or protected paths using the remote CLI or web GUI. Users authenticate to the TOE using username/password defined locally in the TOE.

The TOE provides a configurable number of maximum consecutive authentication failures that are permitted by a user. Once this number has been met, the account is locked for a configurable time interval or until manually unlocked by the Security Administrator of the TOE via the local console.

The Security Administrator can define passwords maintained by the TOE with lengths between 8 and 63 characters. Passwords that are maintained by the TOE can be composed of upper case, lower case, numbers and special characters. Password information is never revealed during the authentication process, including during login failures.

Before a user authenticates to the device, a configurable warning banner is displayed.

The TOE does not support remote communications with trusted systems in its operational environment outside the protection of IPsec. When establishing IPsec associations, the TOE verifies the identity of the IPsec peer device with either X.509 certificate validation or pre-shared keys, as configured. In addition to verifying the validity of certificates and verifying that the certificate chain ends in a trusted Certificate Authority (CA), the TOE can check their revocation status using CRL distribution points or OCSP responders via HTTP.

The TOE establishes secure channels with remote devices (VPN peers) to support communications with trusted peers. The secure channel is established only after each device authenticates the other. Device-level authentication is performed via IKE/IPsec mutual authentication. The TOE supports use of IKEv2 pre-shared keys for authentication of IPsec tunnels. The IKE phase authentication for the IPsec communication channel between the TOE and remote management servers is considered part of the Identification and Authentication security functionality of the TOE. The TOE also supports use of X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec connections.

1.3.5.4 Security Management

The TOE verifies the identity of administrators (users) connecting to the TOE. All administrators must be identified and authenticated before any action can be performed on the TOE. Administrators can access the TOE through the local console, through the remote CLI via SSH over IPsec, or through the web GUI via HTTPS over IPsec. The TOE will terminate all such sessions after a configurable period of inactivity.

Administrators authenticate to the TOE using a username and password as credentials when accessing the TOE by its local console, remote CLI, or web GUI. The TOE supports an internal database for local authentication. Before an administrator authenticates to the device, a customizable warning banner is configured to be displayed.

Passwords can consist of upper-case letters, lower-case letters, numbers, and special characters. Password information is never revealed during the authentication process, including during login failures. Excessive login failures can be configured to lockout the administrator username for a configurable duration or until manually unlocked by the device root administrator via the local console of the TOE.

The TSF determines the validity of the certificates by confirming the validity of the certificate chain and verifying that the certificate chain ends in a trusted Certificate Authority (CA). The TSF connects with a CRL distribution points or configured OCSP servers over HTTP to confirm certificate validity and detect certificate revocations.

1.3.5.5 Protection of the TSF

The TOE implements several features to protect itself to ensure the reliability and integrity of its security features. It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. Passwords within the TOE are hashed using SHA-256. Key data is stored in plaintext on the hard drive but cannot be accessed by any administrator.

The TOE has an underlying hardware clock that is used for accurate timekeeping and reliable time information to support log event timing precision and synchronization with configured NTP servers. This local TOE time can be manually set by the administrator.

The TOE runs a suite of self-tests at power-on to ensure the integrity of the device and system. This testing includes performing self-tests on the CPU, RAM, disk, and other components to detect when it is failing; along with FIPS power-on self-tests for the system.

Digital signatures are used to verify all updates that are applied to the TOE to ensure that the updates do not introduce malicious or other unexpected changes in the TOE.

1.3.5.6 TOE Access

The TOE protects against interference and tampering by untrusted subjects through identification, authentication, and access controls to constrain the ability configure and manipulate the TOE to only authorized administrators. Furthermore, ACOS is a closed system is not a general-purpose operating system.

Access to ACOS memory space is restricted to only A10 ACOS functions.

1.3.5.7 Trusted Path/Trusted Channel

The TOE protects interactive communication paths with remote administrators using IPsec for CLI access and web GUI access over peer-to-peer IPsec sessions. CLI access from remote SSH-based administrators and web GUI access from browser-based (HTTPS) administrators is protected by IPsec.

The TOE connects with the following over peer-to-peer IPsec sessions:

- File Servers for SCP/SFTP file transfers to/from the TOE and updates of the TOE
- SYSLOG Servers for audit logging
- NTP Servers for network date and time synchronization

2. CC CONFORMANCE CLAIMS

2.1 CC CONFORMANCE

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 5, dated: April 2017.

This TOE is conformant to:

- CC Part 2: Security functional components, April 2017, Version 3.1, Revision 5, extended.
- CC Part 3: Security assurance components, April 2017, Version 3.1, Revision 5, conformant.

2.2 PP CONFORMANCE

This TOE is conformant to:

- Collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e, 23-March-2020.

2.3 TECHNICAL DECISIONS

The following is the list of NIAP Technical Decisions that are applicable to the ST/TOE and a summary of their impact.

TD #	TITLE	APPLIC.	EXCLUSION RATIONAL (IF APPLIC)
0670	NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	No	The TOE does not claim TLSC or DTLSC
0639	NIT Technical Decision for Clarification for NTP MAC Keys	No	The TOE uses IPsec to protect NTP traffic.
0638	NIT Technical Decision for Key Pair Generation for Authentication	No	The TOE is not a Distributed TOE.
0636	NIT Technical Decision for Clarification of Public Key User Authentication for SSH	No	The TOE does not claim SSHC
0635	NIT Technical Decision for TLS Server and Key Agreement Parameters	No	The TOE does not claim TLSS
0634	NIT Technical Decision for Clarification required for testing IPv6	No	The TOE does not claim TLSC or DTLSC
0633	NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	Yes	
0632	NIT Technical Decision for Consistency with Time Data for vNDs	No	The TOE is not a vND.
0631	NIT Technical Decision for Clarification of public key authentication for SSH Server	No	The TOE does not claim SSHS
0592	NIT Technical Decision for Local Storage of Audit Records	No	The TOE does not FAU_STG.1, FAU_STG_EXT.2/LocSpace, or FAU_STG_EXT.3/LocSpace.
0591	NIT Technical Decision for Virtual TOEs and hypervisors	No	The TOE is not virtual and does not include a hypervisor
0581	NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	No	The TOE does not claim elliptic curve-based key establishment.
0580	NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	Yes	
0572	NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	No	The TOE does not claim TLSC or DTLSC
0571	NiT Technical Decision for Guidance on how to handle FIA_AFL.1	No	TOE devices all distinguish physical consoles
0570	NiT Technical Decision for Clarification about FIA_AFL.1	Yes	
0569	NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	No	The TOE does not claim TLSS or DTLSS
0564	NiT Technical Decision for Vulnerability Analysis Search Criteria	Yes	
0563	NiT Technical Decision for Clarification of audit date information	Yes	
0556	NIT Technical Decision for RFC 5077 question	No	The TOE does not claim TLSS

0555	NIT Technical Decision for RFC Reference incorrect in TLSS Test	No	The TOE does not claim TLSS
0547	NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	Yes	
0546	NIT Technical Decision for DTLS - clarification of Application Note 63	No	The TOE does not claim DTLS
0538	NIT Technical Decision for Outdated link to allowed-with list	No	No packages claimed
0537	NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	No	The TOE does not claim DTLS
0536	NIT Technical Decision for Update Verification Inconsistency	Yes	
0528	NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	Yes	
0527	Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	Yes	

Table 7: Technical Decisions (TDs)

2.4 CONFORMANCE RATIONALE

This ST provides exact conformance to NDcPPv2.2e. The security problem definition, security objectives and security requirements in this Security Target are all taken from the Protection Profile performing only operations defined there.

The TOE models claimed are all networking devices and therefore the NDcPPv2.2e protection profile is applicable.

3. SECURITY PROBLEM DEFINITION

3.1 THREATS

The threats to the TOE and TOE Environment are described in the table below:

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 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.

THREAT	DESCRIPTION
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.
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.

3.2 ASSUMPTIONS

The assumptions made in identification of the threats and security requirements for the TOE are described in the table below:

ASSUMPTION	DESCRIPTION	OPERATIONAL ENVIRONMENT
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.	OE.PHYSICAL
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).	OE.NO_GENERAL_ PURPOSE
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).	OE.NO_THRU_ TRAFFIC_ PROTECTION

ASSUMPTION	DESCRIPTION	OPERATIONAL ENVIRONMENT
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 being 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).	OE.TRUSTED_ ADMIN
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.	OE.UPDATES
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.	OE.ADMIN_ CREDENTIALS_ SECURE
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.	OE.RESIDUAL_INFORMATION

3.3 ORGANIZATIONAL SECURITY POLICY

Organizational Security Policy imposed by an organization to address its security needs is described in the table below:

SECURITY POLICY	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.

4. SECURITY OBJECTIVES

4.1 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

Security objectives for the Operational Environment are described in the table below:

SECURITY OBJECTIVES FOR THE OE	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.
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 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.
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.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.

5. SECURITY FUNCTIONAL REQUIREMENTS

5.1 CONVENTIONS

The CC defines the following operations on the Security Functional Requirements: Assignment, Refinement, Selection, Assignment within Selection, and Iteration. The conventions used in descriptions of the SFRs are as follows:

- Assignment: indicated with *italicized* text;
- Refinement made by PP author: indicated with **bold text** and ~~strikethroughs~~, if necessary;
- Selection: indicated with underlined text;
- Assignment within a Selection: indicated with *italicized and underlined text*;
- Iteration: indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3) and/or by adding a string starting with "/".

Extended SFRs are identified by having a label 'EXT' at the end of the SFR name.

Where compliance to RFCs is referred to in SFRs, this is intended to be demonstrated by completing the corresponding evaluation activities in [SD] for the relevant SFR.

5.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

NOTE: Selection-Based Requirement identifiers are indicated in **BOLD Underline**.

FUNCTIONAL CLASS	COMPONENT	COMPONENT DEFINITION
FAU: Security audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_STG_EXT.1	Protected Audit Event Storage
FCS: Cryptographic support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Establishment (Refined)
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
	FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
	FCS_RBG_EXT.1	Random Bit Generation
	FCS_IPSEC_EXT.1	IPsec Protocol
	FCS_NTP_EXT.1	NTP Protocol
FIA: Identification and authentication	FIA_AFL.1	Authentication Failure Management (Refinement)
	FIA_PMG_EXT.1	Password Management
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.2	Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
	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(1)/ManualUpdate	Management of Security Functions behaviour
	FMT_MTD.1/CoreData	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
	FMT_MOF.1/Functions	Management of security functions behaviour
	FMT_MTD.1/CryptoKeys	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)

FUNCTIONAL CLASS	COMPONENT	COMPONENT DEFINITION
FPT: Protection of the TSF	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_TST_EXT.1	TSF Testing
	FPT_TUD_EXT.1	Trusted Update
	FPT_STM_EXT.1	Reliable Time Stamps
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_TRP.1/Admin	Trusted Path (Refinement)

Table 8: Security Functional Requirements for the TOE

5.2.1 Security Audit (FAU)

Note: as this TOE is not distributed, none of the security functional requirements relating to distributed TOEs are specified for this TOE.

5.2.1.1 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 shut-down 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).
- [no other actions];

d) Specifically defined auditable events listed in **Table 9**.

FAU_GEN.1.2 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, 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 **Table 9**.

REQUIREMENT	AUDITABLE EVENTS	ADDITIONAL AUDIT RECORD CONTENTS
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
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.

REQUIREMENT	AUDITABLE EVENTS	ADDITIONAL AUDIT RECORD CONTENTS
FCS_RBG_EXT.1	None.	None.
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 identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	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 (if "terminate the session" is selected)	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.
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.

REQUIREMENT	AUDITABLE EVENTS	ADDITIONAL AUDIT RECORD CONTENTS
FTP_TRP.1/Admin	Initiation of the trusted path.	None.
	Termination of the trusted path.	
	Failure of the trusted path functions.	
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure
FCS_NTP_EXT.1	Configuration of a new time server.	Identity if new/removed time server
	Removal of configured time server.	
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate.	Reason for failure
	Any addition, replacement or removal of trust anchors in the TOE's trust store.	Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.
FIA_X509_EXT.2	None	None
FIA_X509_EXT.3	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.
FMT_MOF.1/Functions	None	None.

Table 9: Security Functional Requirements and Auditable Events

5.2.1.2 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.

5.2.1.3 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 [

- TOE shall consist of a single standalone component that stores audit data locally].

FAU_STG_EXT.1.3 The TSF shall [*overwrite previous audit records according to the following rule: [**oldest audit records are overwritten**]*] when the local storage space for audit data is full.

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.1 Cryptographic Key Generation (Refinement)

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-bit 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] 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].].

5.2.2.2 FCS_CKM.2 Cryptographic Key Establishment (Refinement)

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

- 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 [groups listed in RFC 3526].].

5.2.2.3 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

- 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 [zeroes]];]

that meets the following: No Standard.

5.2.2.4 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] mode and cryptographic key sizes [128 bits, 192 bits, 256 bits] that meet the following: AES as specified in ISO 18033-3, [CBC as specified in ISO 10116, GCM as specified in ISO 19772].

5.2.2.5 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*],
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [*256 and 384 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]; ISO/IEC 14888-3, Section 6.4].

5.2.2.6 FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

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 message digest sizes [160, 256, 384, 512] bits that meet the following: ISO/IEC 10118-3:2004.

5.2.2.7 FCS_COP.1/KeyedHash Cryptographic Operation (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] 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".

5.2.2.8 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)].

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] 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.

5.2.2.9 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 (RFC 3602), AES-CBC-192 (RFC 3602), AES-CBC-256 (RFC 3602) , AES-GCM-128 (RFC 4106), AES-GCM-192 (RFC 4106), AES-GCM-256 (RFC 4106)] 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-192, AES-CBC-256 (specified in RFC 3602), AES-GCM-128, AES-GCM-192, 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 [*1 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 [*1 to 8*] 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 [224] 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 Group(s) [

- [14 (2048-bit MODP)] according to RFC 3526,

].

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 all IKE protocols perform peer authentication using [RSA, ECDSA] that use X.509v3 certificates that conform to RFC 4945 and [Pre-shared Keys].

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: [SAN: IP address, SAN: Fully Qualified Domain Name (FQDN)] and [Subject: IP address, Subject: Fully Qualified Domain Name (FQDN)].

5.2.2.10 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.

5.2.3 Identification and Authentication (FIA)

5.2.3.1 FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within [*1 to 10*] 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 remote session using any authentication method that involves a password until [*an unlocking of the associated offending administrative account*] is taken by an Administrator; prevent the offending Administrator from successfully establishing remote session using any authentication method that involves a password until an Administrator defined time period has elapsed].

5.2.3.2 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 [*63*] characters.

5.2.3.3 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.

5.2.3.4 FIA_UAU_EXT.2 Password-based Authentication Mechanism

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

5.2.3.5 FIA_UAU.7 Protected Authentication Feedback

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

5.2.3.6 FIA_X509_EXT.1 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, a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3, Certificate Revocation List (CRL) as specified in RFC 5759 Section 5].
- 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.

5.2.3.7 FIA_X509_EXT.2 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 [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 [accept the certificate].

5.2.3.8 FIA_X509_EXT.3 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 [device-specific information, 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.

5.2.4 Security Management (FMT)

5.2.4.1 FMT_MOF.1/ManualUpdate Management of security functions behaviour

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

5.2.4.2 FMT_MTD.1/CoreData Management of TSF Data

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

5.2.4.3 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] capability prior to installing those updates ;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- [
    - Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full) ;
    - Ability to manage the cryptographic keys;
    - Ability to configure the cryptographic functionality;
    - Ability to configure the lifetime for IPsec SAs;
    - Ability to re-enable an Administrator account;
    - Ability to set the time which is used for time-stamps;
    - Ability to configure NTP;
    - Ability to configure the reference identifier for the peer;
    - Ability to import X.509v3 certificates to the TOE's trust store;]

5.2.4.4 FMT_SMR.2 Restrictions on 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.

5.2.4.5 FMT_MOF.1/Functions Management of security functions behaviour

FMT_MOF.1.1/Functions The TSF shall restrict the ability to [modify the behaviour of] the functions [audit functionality when Local Audit Storage Space is full] to Security Administrators.

5.2.4.6 FMT_MTD.1/CryptoKeys Management of TSF data

FMT_MTD.1.1/CryptoKeys The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

5.2.5 Protection of the TSF (FPT)

5.2.5.1 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.

5.2.5.2 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.

5.2.5.3 FPT_TST_EXT.1 TSF Testing (Extended)

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [during initial start-up (on power on)] to demonstrate the correct operation of the TSF: [*firmware integrity test, algorithm known answer tests*].

5.2.5.4 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 [the most recently installed version of the TOE firmware/software;].

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] prior to installing those updates.

5.2.5.5 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 [allow the Security Administrator to set the time, synchronise time with an NTP server].

5.2.6 TOE Access (FTA)

5.2.6.1 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.

5.2.6.2 FTA_SSL.3 TSF-initiated Termination (Refinement)

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

5.2.6.3 FTA_SSL.4 User-initiated Termination (Refinement)

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

5.2.6.4 FTA_TAB.1 Default TOE Access Banners (Refinement)

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.

5.2.7 Trusted path/channels (FTP)

5.2.7.1 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, [[*File Server(s), NTP Server(s)*]] 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 [*communication with*:

- *SYSLOG server(s) for external audit logging*
- *File server(s) for file imports, trusted updates, and file exports*
- *NTP server(s) for date and time synchronization*].

5.2.7.2 FTP_TRP.1/Admin Trusted Path

FTP_TRP.1.1/Admin The TSF shall be capable of using [IPsec] 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. SECURITY ASSURANCE REQUIREMENTS

6.1 SAR REQUIREMENTS

The TOE assurance requirements for this ST are listed in the collaborative Protection Profile for Network Devices, v2.2e (NDcPPv2.2e) and correspond to the set of SARs listed in Common Criteria Version 3.1, Revision 5.

ASSURANCE CLASS	ASSURANCE COMPONENTS
Security Target (ASE)	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)
	Security objectives for the operational environment (ASE_OBJ.1)
	Stated security requirements (ASE_REQ.1)
	Security Problem Definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Basic functional specification (ADV_FSP.1)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life cycle support (ALC)	Labelling of the TOE (ALC_CMC.1)
	TOE CM coverage (ALC_CMS.1)
Tests (ATE)	Independent testing – conformance (ATE_IND.1)
Vulnerability assessment (AVA)	Vulnerability survey (AVA_VAN.1)

Table 10: Security Assurance Requirements

6.2 SAR RATIONALE

This ST contains the assurance requirements from the collaborative Protection Profile for Network Devices, v2.2e. Since the SARs were taken directly from the NDcPPv2.2e which is an approved PP, the SAR rationale is presumed to be satisfied.

7. TOE SUMMARY SPECIFICATION

7.1 TOE SECURITY FUNCTIONS SPECIFICATION

This section describes the security functions provided by the TOE to meet the security functional requirements specified for the TOE in section 5.2.

7.1.1 SF.Security_Audit

The product supports audit records (logs), related to TOE management, device, and network processing events. The types of events audited are described in Table 11. The TOE provides administrators the ability to view events based on the log level (ranges from 0 to 7), administrator name, administrator IP address, and date/time.

If the internal audit storage is exhausted then the oldest records are overwritten first and no alerts are generated. The TOE never outputs sensitive information such as passwords or keys to the log records.

Types of Events Audited:

EVENT TYPE	SUMMARY INFORMATION SPECIFIED IN THE LOG RECORD
Logins and logoffs, authentication	Administrator name, IP address, date/time, outcome
Local/Remote management opertions	Administrator name, IP address, L4 port, date/time,
Time and network processing	IP addresses, protocol, ports, date/time
System upgrade, restart	Administrator name, upgrade version, date/time
CPU usage	CPU performance information, date/time
Alarms	Alarm inforrmation (fan, power supply, etc), date/time

Table 11: Types of Events Audited

7.1.1.1 FAU_GEN.1 Audit data generation

The TOE generates audit records for events including:

- starting and stopping the audit function,
- administrator commands, and
- all other events identified in Section 5.2.1.1.

Audit records include the date/time, event source (CLI/GUI), responsible administrator (user), IP address of the administrator, and additional event-specific content indicated in Section 5.2.1.1. CLI management operations are distinguished between local console and remote management in logged records by the indicated IP address, with:

- Local Console Operations Loopback IP Address (e.g. 127.0.0.1)
- Remote Management Operations Peer IP Address and TCP Port (e.g. 10.65.25.166:53288)

The successful outcome of events is implicit, without the adjacent event records indicating failure.

Importing, deleting, and generating cryptographic keys is audited including corresponding key name identifiers to identify the keys involved for such operation.

7.1.1.2 FAU_GEN.2 User identity association

The TOE identifies or associates the administrator (user) for each event based on the administrator's username or network identity (IP address) that elicited the event.

7.1.1.3 FAU_ STG_EXT.1 Protected Audit Event Storage

Generated audit records are stored in two files on the local filesystem of the standalone TOE, one for ACOS audit category records and one for ACOS event category records. Each record file supports a circular logging store with the oldest records overwritten first when the logging store is full.

The audit category logging store is configurable from 1000 to 30,000 records with 20,000 records as a default. The event category record logging store is configurable from 10,000 to 50,000 records with 30,000 records as a default. Only authorized administrators can enable/disable logging to the logging stores, clear the content of the logging stores, or alter the sizes of the logging stores. All TOE administrators are permitted to view contents of the logging stores. No other methods are supported by the TOE to change the content of records in the TOE's local audit stores.

The TOE can be configured to simultaneously report audit records for both logging stores to external SYSLOG servers in real-time, protected through the use of IPsec. Only authorized administrators can add, delete, or modify SYSLOG configuration settings.

7.1.2 SF.Cryptographic_Support

The TOE includes FIPS-capable libraries to provide implementations of all required cryptographic algorithms and mechanisms. The TOE includes NIST validated cryptographic algorithms providing supporting cryptographic functions. The functions indicated in Table 6 have been certified in accordance with the identified standards.

The TOE supports local and remote administrator authentication using a password-based method. The TOE will close the underlying TCP connections for sessions that exceed the TOE configuration for inactivity and release all resources for their sessions.

The TOE supports keys and Critical Security Parameters (CSPs) listed in Table 12 with the indicated origin, storage and zeroization of keys as relevant to FCS_CKM.4 and FPT_SKP_EXT.1.

Non-volatile keys and CSPs are overwritten with zeros repeatedly until read-verification succeeds when a secure reset operation on the TOE is performed. A secure reset operation is performed when an authorized administrator issues a “security-reset” CLI command on the TOE console to wipe the TOE or issues a “no system fips” (“system fips”) command on the TOE console to disable (enable) FIPS mode on the TOE. The “security-reset” CLI command will zeroize this key and CSPs and render the TOE unusable, suitable for decommissioning or return to the factory. Changing the FIPS mode will zeroize keys and CSPs, followed by a reboot of the device.

Key and CSP destruction is immediate upon the indicated operation.

KEY	ORIGIN	ZEROIZED UPON	STORAGE	ZEROIZATION
IKE Private Host Key	TOE Generated	Command	SSD	Overwritten by zeros when secure reset operation is performed.
IKE Pre-shared Auth Key	Entered	Command	SSD	Overwritten by zeros when secure reset operation is performed.
Local Administrator Password	Entered	Command	SSD	Overwritten by zeros when secure reset operation is performed.
X.509 certificates	Imported	Command	SSD	Overwritten by zeros when secure reset operation is performed.
Diffie Hellman private key	TOE generated	Session close	RAM	Keys are overwritten with zeros.
Diffie Hellman public key	TOE generated	Session close	RAM	Keys are overwritten with zeros.
IKE Master Secret	TOE generated	Handshake done	RAM	Keys are overwritten with zeros.
IKE Session Key	TOE generated	Session close or re-key	RAM	Keys are overwritten with zeros.
ESP Session Key	TOE generated	Session close or re-key	RAM	Keys are overwritten with zeros.
IKE-DH Private Exponent	TOE generated	Session close or re-key	RAM	Keys are overwritten with zeros.

Table 12: Cryptographic Keys and CSPs

7.1.2.1 FCS_CKM.1 Cryptographic Key Generation (Refinement)

In support of secure cryptographic protocols, the TOE supports RSA key generation schemes to be used with IPsec, in accordance with PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3 using 2048 bit keys.

The TOE also supports Elliptic Curve key generation schemes using the P-256, P-384 curves to be used in IPsec certificates in accordance with FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4.

The TOE implements FFC schemes using Diffie-Hellman group 14 for IPsec. The TOE implementation of Diffie-Hellman group 14 (2048 MODP) meets RFC 3526, Section 3.

The TOE also key generation using RSA for 2048-bit keys and ECDSA with P-256/P-384 curves when creating keypairs as part of Certificate Signing Request (CSR) generation.

The relevant key generation algorithms are validated under CAVP certificates # C1198 and C1940.

7.1.2.2 FCS_CKM.2 Cryptographic Key Establishment (Refinement)

See discussion in Section 7.1.2.1 above.

7.1.2.3 FCS_CKM.4 Cryptographic Key Destruction

The TOE meets all requirements specified in the NDcPPv2.2e for destruction of keys and Critical Security Parameters (CSPs). All keys and CSPs within the TOE are securely destroyed as per the descriptions given for and included in Table 12 above.

7.1.2.4 FCS_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)

The TOE provides encryption and decryption capabilities using 128, 192, and 256 bit AES in both CBC and GCM modes. AES is implemented in the following protocols: IPsec.

These AES algorithm meet ISO/IEC 10118-3:2004 with AES-CBC meeting ISO 10116, and AES-GCM meeting ISO 19772. These algorithms are validated under CAVP certificates # C1198, C1940, and A1181.

7.1.2.5 FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

IPsec tunnels can be configured to use RSA key sizes 2048 bits (or greater) or ECDSA with key size 256 and 384 bits using NIST curve P256 and P384 certificate for IPsec authentication. For verification of trusted updates, digital signatures use an RSA key size of 2048 bits.

7.1.2.6 FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512 with message digest sizes of 160, 256, 384, and 512 bits respectively. The TSF uses hashing services the following functions:

- SHA-1, SHA-256, SHA-384, and SHA-512 for IPsec data integrity and authentication, and digital signatures.
    - Relevant algorithms include: HMAC, RSA, and ECDSA
    - Only SHA-2 is used for digital signature generation
- SHA-256 for trusted update
    - Relevant algorithms include: RSA
- SHA-256 for password hashing

The SHA algorithm meets ISO/IEC 10118-3:2004 and is validated under CAVP SHS certificates # C1198, C1940, and A1181.

In addition, the TOE use MD5 hashing services for firmware integrity checking at device boot-time.

7.1.2.7 FCS_COP.1/KeyedHash Cryptographic Operation (Hash Algorithm)

The TOE provides keyed-hashing message authentication services in IPsec using HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with key sizes and 160, 256, 384, and 512 bits and digest sizes of 160, 256, 384, and 512 bits as specified in FIPS PUB 198-1 and FIPS PUB 180-4.

The block size is 512 bits for HMAC-SHA-1 and HMAC-SHA-256 algorithms and 1024 bits for HMAC-SHA-384 and HMAC-SHA-512 algorithms. The algorithm meets ISO/IEC 9797-2:2011 Section 7 and is validated under CAVP HMAC certificates #C1198, C1940, and A1181.

7.1.2.8 FCS_RBG_EXT.1 Random Bit Generation

The TOE implements a NIST-approved deterministic random bit generator (DRBG). The DRBG used by the TOE is CTR_DRBG with derivation function (DF) with AES. The TOE's DRBG implementation meets ISO/IEC 18031:2011 and is validated under CAVP certificates #C1198 and C1940.

The DRBG is seeded from the hardware entropy source (Intel RNG) of the underlying TOE CPU(s). Entropy from the noise source is extracted, conditioned and used to seed the DRBG with 256 bits of full entropy.

7.1.2.9 FCS_IPSEC_EXT.1 IPsec Protocol

The TOE supports IPsec tunnel-mode (conformant to RFCs 4301) for trusted channel communications with SCP/SFTP Servers (for file transfers to/from the TOE and updates of the TOE), NTP Servers (for network date and time synchronization) and SYSLOG Servers (for audit logging). Trusted path communications are also supported using IPsec tunnel-mode for remote administration of the TOE by CLI (SSH) management clients and Web/GUI (HTTPS) management browser clients.

The TOE supports for ESP protection with AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192 and AES-GCM-256 using HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512.

The TOE implements IKEv2 with:

- IKEv2 as defined in RFCs 5996 (including support for NAT traversal) and RFC 4868 for hash functions.

The TOE supports IKEv2 protection with AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, and AES-GCM-256.

The TOE supports configuration of IKE lifetimes as follows. The TOE will initiate SA renegotiation prior to expiration or consumption of these lifetimes.

- IKEv2 SA lifetime by length of time (300 seconds to 24-hours (86400 seconds))
- IKEv2 Child SA lifetimes of number of bytes (1 or unlimited MBytes)
- IKEv2 Child SA lifetimes length of time (300 seconds to 8-hours (28800 seconds)).

The TOE supports Diffie-Hellman Group 14 only.

The TOE uses AES-CTR DRBG to generate the secret value ‘x’ used in the IKEv2 Diffie-Hellman key exchange (“x” in g^x mod p). These exponents generated for DH Group 14 are 224-bits (28 bytes) long. Nonces generated using AES-CTR DRBG are 256-bits (32-bytes), which is more than 128-bits in size and half of the largest output size supported (SHA-512).

The TOE ensures that the strength of the symmetric algorithm negotiated to protect IKEv2 IKE SA connections is greater than or equal to the strength of the symmetric algorithm negotiated to protect the IKEv2 Child SA connections. During establishment of IKEv2 Child SA connection, the negotiated strength of IKEv2 IKE SA is compared against that configured in the TOE for IKEv2 Child SA connection. If the configured strength is greater than that negotiated strength, than the IPsec tunnel establishment is failed and a corresponding event is logged.

The TOE supports peer authentication with RSA and ECDSA for use with X.509v3 certificates (conformant to RFC 4945) or pre-shared keys for IPsec IKE. Pre-shared keys are manually entered as text-based strings when configuring IPsec tunnels via the CLI or Web/GUI administration interfaces with a length of 1 – 127 characters. Pre-shared keys entered are combinations of lower and upper-case characters, numeric digits, and supported special characters. For a given IPsec peer’s IKE configuration using a pre-shared key, the key must be the same on the configured IPsec peer as entered by the TOE administrator.

The TOE will attempt match an FQDN or IP Address value configured by an authorized administrator for the reference identifier of a given IPsec peer with values of the Subject or Subject Alternative Name (SAN, if present) fields in the peer’s certificate when establishing an IKE session with the peer. If neither of the fields match the configured reference identifier, the IPsec tunnel establishment is failed, and a corresponding event is logged.

The TOE’s IPsec Security Policy Database (SPD) is configured based upon the trusted paths and trusted channels protected using IPsec. IPsec SPD rules are configured using firewall-style Access Control Lists (ACLs) based IP addresses/ranges, L4 protocol, L4 port/selector, and precedence. When applied IPsec endpoints or endpoints via IPsec gateways/VPNs, ACL deny and permit rules effect SPD DROP and PROTECT actions for corresponding network traffic; respectively. Permit ACLs for other endpoints effect SPD BYPASS actions as they will allow network traffic to (from) the TOE unsecured by IPsec on the TOE.

TOE ACLs are processed with precedence of the order they are specified with by TOE administrators. A default discard rule must be defined by the TOE administrators to ensure that a packet not matching a prior ACL rule is discarded (dropped). TOE administrators are also responsible for ensuring that TOE ACLs do not overlap or conflict.

Incoming IPsec traffic received on the TOE management interface is decrypted and filtered through the configured ACLs with packets allowed for further processing by the TOE software elements. Outgoing traffic on the TOE management interface is first filtered through the configured ACLs for permitted matches with IPsec peers which are then allowed for IPsec processing or direct transmission. Such outgoing traffic then matched with an IPsec SA configured to support the destination and if matched will be processed and IPsec encrypted before being transmitted from the TOE.

7.1.2.10 FCS_NTP_EXT.1 NTP Protocol

The TOE supports NTP v4 (compliant with RFC 5905). The TOE can be configured for three (3) or more remote, NTP servers.

The TOE uses IPsec for trusted channels to communicate with these servers, thereby ensuring that the TOE is using an authentic time source and that integrity of time is maintained.

7.1.3 SF.Identification_Authentication

By default, the TOE is provisioned for a single administrator account named 'admin'. This permanent account, referred to as the root (master) administrator account, is privileged to use all management services of the TOE, without restriction.

The TOE authenticates administrators (users) against their username, password, and privilege level. The TOE supports two (2) fundamental privileges for administrators (users).

- read Allows the administrator to view and display TOE configuration elements.
- read+write Allows the administrator to create, modify, or delete TOE configuration elements; as well as to view and display them.

The TOE supports a password enforcement configuration where the minimum password length can be set by an administrator (user). The default minimum length is 8 and can be set as high as 63 characters. Passwords can be created by the root (master) administrator including lower-case, upper-case, numeric, and special characters.

The TOE can be configured to lockout remote administrators (users) after a number of successive, login failures (default is 5 failures) until manually unlocked by an authorized administrator or a configured period of time.

7.1.3.1 FIA_AFL.1 Authentication Failure Management

The TOE provides a counter that is incremented for consecutive failed remote authentication attempts via CLI or Web/GUI and will lock an administrator account when the failure counter threshold is reached. A valid login that occurs prior to the failure counter reaching its threshold will reset the counter to zero.

When this threshold is reached for a given administrator account, no authentication will be allowed for the account as the TOE's remote CLI and Web/GUI interfaces will refuse connections for the account from any endpoint in subsequent attempts. Once a connection is refused due to lockout for a given account, the administrator would have to re-login after the configurable lockout time period has elapsed or after a manual unlocking of the account is performed.

This lockout threshold of the TOE can be configured to any value from 1 - 10 failures. The lockout duration is a configurable number of minutes from 0 - 1440 minutes (24 hours), with a value of 0 to requiring manual unlocking by the root (master) administrator of the TOE via the local console.

Authentication failure counting is disabled for access attempts on to the local console of the TOE. Administrator accounts locked out due to remote login failures having exceeded the lockout threshold will still be able to login via the TOE console with valid credentials.

7.1.3.2 FIA_PMG_EXT.1 Password Management

Passwords maintained by the TOE can be composed using any combination of upper-case and lower-case letters, numbers, and special characters including the following. These password special characters are supported both for CLI and Web/GUI interfaces to successfully authenticate with the TOE.

- “ ”, “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(”, “)”, “ ”, “"”, “‘”, “+”, “,”, “-”, “.”, “/”, “:”, “;”, “<”, “=”, “>”, “?”, “[”, “\”, “]”, “ ”, “`”, “{”, “|”, “}”, “~”

The password policy is configurable by TOE administrators and supports the minimum password length of 8 characters and a maximum password length of 63 characters.

7.1.3.3 FIA_UIA_EXT.1 User Identification and Authentication

The TOE requires all administrators to be successfully identified and authenticated before any TSF-mediated actions are allowed to be performed, with the only exception being the display of a banner. A successful authentication is determined by a successful username and password combination accepted by the TOE. The configurable warning banner is displayed prior to the user being prompted to enter the username component of the credential when logging in to the TOE. Accordingly, the TOE does not allow a user to perform any other actions prior to authentication.

The administrator logs into the TOE through either the local TOE console using the CLI or remotely through IPsec using the CLI via SSH or the Web/GUI via HTTPS over IPsec

7.1.3.4 FIA_UAU_EXT.2 Password-based Authentication Mechanism

The TOE uses a local password-based authentication mechanism to login authorized administrative users locally via the TOE console.

7.1.3.5 FIA_UAU.7 Protected Authentication Feedback

The TOE does not echo passwords as they are entered; rather no characters are echoed during input on to the CLI at both the local console and for remote SSH sessions to the TOE via IPsec. ‘*’ characters are echoed when entering password to the Web/GUI. Accordingly, no observer can read the password off the screen of a terminal session to the local console of the TOE.

7.1.3.6 FIA_X509_EXT.1, 2, 3 X.509 Certificate Validation, Authentication, Requests

The TOE can use X.509 certificates for IPsec session authentications. The TOE can be configured with the certificates and their corresponding private keys by authorized administrators creating CSRs on the TOE, exporting the CSRs for certificate authority (CA) signing, and subsequently importing the CA-signed certificates to the TOE.

Authorized administrator can also import intermediate and root-CA certificates for the TOE to present in IPsec session establishments. Intermediate and root-CA (trust anchor) certificates can also be imported to the TOE to support IPsec peer authentications where the IPsec peers do not present these certificates. During IPsec session establishment the TOE will evaluate presented certificates first and when not presented will then evaluate locally available certificates corresponding to the IPsec peer’s certificate chain.

The TOE will validate presented or locally available certificates during IPsec session establishment. This validation includes checking to ensure that the basicConstraints extension and CA flag are set to TRUE for all CA certificates Revocation status is checked during IPsec session establishment for all certificates in the peer’s certificate chain (path) per OCSP or CRL servers indicated in the certificates. If the indicated OCSP server or CRL distribution point are unavailable to determine revocation status, the TOE will assume, by default, the certificate is not revoked. Invalid or revoked certificates detected will cause the IPsec session to fail to establish and with corresponding errors logged accordingly.

The TOE similarly validates certificates when imported to the TOE, albeit without revocation status checks. Certificates that fail this validation will not be included in the TOE's certificate store for use by IPsec and will be left inert until deleted by an authorized administrator.

When generating Certificate Signing Requests (CSRs), an authorized administrator can select the size of the key as 2048 bits for RSA and 256 or 384 bits for ECDSA. In addition to adding the public key to the certificate details, the administrator can provide information for the Common Name, Organization, Organizational Unit, and Country . The administrator can also provide the following additional TOE specific information:

- Locality
- State/Province
- E-Mail Address

When generating CSRs on the TOE, the Organization Unit (OU) information items is prompted with the name "Division".

7.1.4 SF.Security_Management

The TOE implements an internal access control mechanism that bases decisions about the use of functions and access to TOE data on privilege levels assigned for administrators (users). In this manner, the TOE ensures that only authorized administrators can access audit and configuration data, access policy and controls (ACLs), authentication, access banner, login failure lockout, and cryptographic settings of the TOE.

Once authenticated, authorized administrators (users) have access to the following security functions consistent with their assigned privileges:

- 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] capability prior to installing those updates
- Ability to configure the authentication failure parameters for FIA_AFL.1
- Ability to configure audit behaviour
- Ability to manage the cryptographic keys
- Ability to configure the cryptographic functionality
- Ability to configure the lifetime for IPsec SAs
- Ability to re-enable an Administrator account
- Ability to set the time which is used for time-stamps
- Ability to configure NTP
- Ability to configure the reference identifier for the peer
- Ability to import X.509v3 certificates to the TOE's trust store

7.1.4.1 FMT_MOF.1/ManualUpdate Management of security functions behaviour

Only authorized administrators (users) can update the TOE.

7.1.4.2 FMT_MTD.1/CoreData Management of TSF Data

Security management of the TOE is restricted to authorized administrators (users). The TOE does not support non-administrative users. All users of the TOE are considered administrative users. The only function of the TOE prior to a successful authentication (username and password combination) is the display of a previously configured banner. Administrative functions of the TOE are available only after successful authentication (login).

As described in 7.1.3. SF.Identification_Authentication above, only read+write privileged administrators can create, modify, or delete TOE configuration elements. This includes the generating and exporting of X.509 Certificate Signing Requests (CSRs) as well as importing and deleting of X.509 certificates. The TOE implementation does not support modifying (changing) X.509 certificates extant on the TOE.

7.1.4.3 FMT_SMF.1 Specification of Management Functions

Administrators can log into the TOE through either the local TOE console using the CLI or remotely through IPsec using the CLI via SSH or the Web/GUI via HTTPS.

The ability to perform security management functions on the TOE is restricted to authorized administrators as indicated above. All security management functions are available both locally and remotely to authorized, authenticated administrators.

7.1.4.4 FMT_SMR.2 Restrictions on security roles

The TOE provides administrative access to perform security management functions via

- local, serial console CLI
- remote, CLI
- remote , Web/GUI

The TOE maintains administrative user roles. Authorized administrators authenticated by TOE with the “read+write” privilege can perform security management functions not otherwise restricted to the root (master) administrator. Administrators with “read-only” privilege may view security management configuration settings and information, however they cannot create, import, add, or otherwise modify configuration settings.

7.1.4.5 FMT_MOF.1/Functions Management of security functions behaviour

The TOE restricts the ability to alter the configuration for external audit servers (e.g. add, delete, enable, disable, or modify). This ability, using the `acos-events` CLI command, is restricted to authorized administrators of the TOE.

7.1.4.6 FMT_MTD.1/CryptoKeys Management of TSF data

The TOE restricts the ability to manage IPSec private keys to authorized administrators of the TOE. This includes configuring IPsec pre-shared keys and generating/deleting IPsec RSA and ECDSA public and private keys using applicable configuration CLI commands or Web/GUI operations.

7.1.5 SF.TSF_Protection

The TOE is designed specifically to not provide access to locally stored passwords and cryptographic keys. Dynamically generated cryptographic keys, such as for IPsec sessions, are stored in RAM only. All cryptographic keys and password information that are non-volatilely stored are not accessible to administrators and no capabilities are provided to access the cryptographic keys or password information.

The TOE is a networking appliance that includes a hardware-based real-time clock. The TOE's embedded OS manages the clock and exposes administrator clock-related functions within the TOE device. The TOE also implements the inactivity timeout elements for terminating both local console and remote sessions to the TOE via IPsec.

The TOE includes a number of built in diagnostic tests that are run during start-up to determine whether the TOE is operating properly. The TOE will reboot when an error in self-testing of device memory, storage, or attached devices is encountered.

The TOE performs cryptographic algorithm known answer tests and firmware integrity tests when booting. Upon failure of its integrity or cryptographic self-tests, the TOE is put into FIPS failure mode. In this mode, the TOE will operate with nominal management services available from the TOE console only. Remote management to the TOE (trusted paths), connections to external servers (trusted channels), and TOE data-plane services will also not be available or operational..

The TOE supports loading a new software image manually by authorized administrators using CLI commands or the Web/GUI. Prior to actually installing an image the TOE verifies the integrity of the image and the image's RSA digital signature using the A10 Network's public key. An unverified image cannot be installed. The TOE comes preinstalled with the A10 Network's public key.

7.1.5.1 FPT_SKP_EXT.1 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)

The TOE is designed specifically to prevent access to locally-stored cryptographically protected administrative passwords or any keys stored in the TOE. The TOE does not implement any functions that will disclose to any administrator a stored cryptographic key or password. By its nature the TOE is an administratively closed systems, providing access only through defined interfaces (e.g. CLI, Web/GUI) to administrators configured to permit management access to the TOE. The TOE does not expose OS Shell access to administrators. See Table 12 for more information about keys stored on the TOE.

The TOE protects user administrative passwords by saving a SHA-256 hash of the password.

7.1.5.2 FPT_APW_EXT.1 Protection of Administrator Passwords

See TOE summary specifications for FPT_SKP_EXT.1 above.

7.1.5.3 FPT_TST_EXT.1 TSF Testing (Extended)

The TOE includes a suite of self-tests that execute at power-on or a reboot of the TOE to ensure the proper functioning of the TOE. These tests ensure that the integrity of the TOE firmware is maintained and verify cryptographic algorithms on the underlying processor match known, expected results. If any of the tests fail, the TOE will enter a limited operations mode until an Administrator intervenes. In this mode, the TOE will provide a nominal level of services sufficient to support local console CLI management access only for assessment and remediation of the failure.

Algorithm tests and firmware integrity tests include:

- AES Known Answer Test using GCM and ECB modes (encrypt/decrypt)
- SHS Known Answer Test as a part of the HMAC KAT. Also SHA-1 and SHA-256 are tested separately.
- HMAC Known Answer Test using SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 to also cover SHA POST
- SP800-90A DRBG Known Answer Test for CTR_DRBG: AES
- RSA Known Answer Test using 2048 bit key, SHA-256

- ECDSA Pairwise Consistency Test (sign/verify) using P-224, K-233 and SHA-512
- Firmware Integrity Test using MD5 hash of the firmware image

The firmware integrity test is sufficient to ensure that the TOE has not been corrupted and the algorithm tests are sufficient to ensure that the cryptographic functions are operating properly.

7.1.5.4 FPT_TUD_EXT.1 Trusted Update

The TOE provides functions to query the version of firmware on the TOE and to upgrade the firmware embedded in the TOE device. When installing updated firmware, RSA digital signatures and image integrity checks are used to validate the update and ensure it is an update intended and originated by A10 Networks.

The TOE firmware version can be queried by a 'show version' CLI command or by viewing the TOE's device information page in the Web/GUI. Firmware updates that succeed become active upon a reboot of the TOE device.

TOE update images are available from the A10 Networks support web site (https://support.a10networks.com). An A10 Networks support login ID and password is required to download these images. To perform an update an administrator will download a TOE update image to a local, trusted file server accessible to the TOE via IPsec. The administrator will then attempt to manually update using the 'upgrade' CLI command or equivalent Web/GUI operation.

This command (operation) will prompt the TOE to download the update image to the TOE device. The TOE will then verify the image integrity and RSA digital signature of the upgrade image before installation. If the image integrity and signature verifications succeed, the TOE will proceed with installation of the firmware update. Otherwise, the TOE will cease the update operation after deleting the temporary image and logging the trusted update failure.

7.1.5.5 FPT_STM_EXT.1 Reliable Time Stamps

The TOE provides a source of date and time information used in audit event timestamps. The clock function is reliant on the system clock provided by the underlying hardware. The TOE can optionally be set to receive clock updates from one or more NTP servers to synchronize the TOE with the network date and time.

This date and time of the TOE is used for timestamps applied in TOE generated audit records and is also used to track inactivity of administrative sessions, track administrator account lockout times, and support cryptographic operations based on time/date.

The TOE allows authorized administrators to set the date and time manually and/or configure NTP time sources for the TOE.

7.1.6 SF.TOE_Access

The TOE supports administrative access to the TOE CLI using the TOE local console and remotly using SSHv2 via IPsec. Administrative access is also supported to the TOE Web/GUI using HTTPS via IPsec from remote browser clients.

Authorized TOE administrators can configure banners that will be displayed when the TOE CLI is accessed via the local console or remotely using SSHv2 via IPsec or when the TOE Web/GUI is accessed using a web browser via IPsec. These banners will be displayed before identifying user credentials (username and password) are entered.

Authorized TOE administrators can configure a session inactivity timeout value for up to 60 minutes. This timeout will affect management sessions to the TOE CLI on the local console or remotely using SSHv2 via IPsec. A separate web service session timout value can be similarly configured to control session timeouts for access to the TOE's web GUI connections to the TOE's.

Such sessions that have no activity (commands or operations issued by the remote entity) for configured timeout durations will be terminated by the TOE. Administrators will need to login again after any session is terminated by the TOE due to inactivity timeouts. Administrators will also need to login again after they voluntary terminate their sessions. Administrators can logout of local or remote sessions at any time.

7.1.6.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

The TOE terminates sessions to the local console that have been inactive for an administrator-configured period of time. Administrators can use the 'terminal idle-timeout' CLI command or equivalent Web/GUI operation to configure the inactivity period after which a session to the local console will be terminated by the TOE. The inactivity period is a configurable number of minutes from 1 - 60 minutes (1 hour).

7.1.6.2 FTA_SSL.3 TSF-initiated Termination (Refinement)

The TOE terminates remote, administrative sessions that have been inactive for an administrator-configured period of time. The same 'terminal idle-timeout' CLI command or equivalent Web/GUI operation configures the inactivity period after which an inactive remote session to the TOE CLI using SSHv2 via IPsec will be terminated by the TOE. The inactivity period is a configurable number of minutes from 1 - 60 minutes (1 hour).

Administrators can use the 'web-service gui-timeout-policy idle' CLI command or equivalent Web/GUI operation to configure the inactivity period after which an inactive remote Web/GUI session using HTTPS via IPsec will be terminated. The inactivity period is a configurable number of minutes from 1 - 60 minutes (1 hour).

7.1.6.3 FTA_SSL.4 User-initiated Termination (Refinement)

The TOE allows interactive sessions to exit (logout) gracefully by command (operation). Administrative sessions to the TOE CLI using the local console or remotely accessing the CLI with SSHv2 via IPsec can terminate their sessions using the 'exit' CLI command.

Administrative sessions to the TOE Web/GUI via IPsec can terminate their sessions using the provided 'logout' option in the user control menu at the top right corner of the browser window.

7.1.6.4 FTA_TAB.1 Default TOE Access Banners (Refinement)

The TOE can be configured for advisory and consent banners displayed to interactive administrators accessing the TOE such that administrators may terminate these session before performing any function or operation on the TOE.

For local and remote CLI sessions to the TOE, a banner to be displayed before entering login credentials (username and password) can be configured using the 'banner login' CLI configuration command or equivalent Web/GUI operation. This banner is displayed before prompting for input credentials by the administrator.

For remote Web/GUI sessions to the TOE, a banner to be displayed before entering login credentials (username and password) can be configured on the 'System -> Settings -> Web' Web/GUI page. This banner is displayed in a pop-up window that must be accepted by clicking an "OK" button before the TOE's standard login page is displayed prompting inputs for username and password.

7.1.7 SF.Trusted_Path/Channels

The TOE supports interactive, trusted paths from remote administrators using SSHv2 over IPsec for CLI access and HTTPS over IPsec for Web/GUI access.

The TOE supports trusted channels protected by IPsec, including the following:

- File Servers for SCP/SFTP-based file transfers to/from the TOE and updates of the TOE
- SYSLOG Servers for audit logging
- NTP Servers for network date and time synchronization

In the evaluated configuration IPsec must be configured on the TOE for IPsec enabled endpoints (administrative clients and available servers) and or IPsec gateways providing connectivity to these clients and servers. If IPsec sessions are not instantiated or cannot be negotiated (instantiated), connections between these entities and the TOE will fail to establish. Established connections with these entities will be dropped if their underlying IPSec session(s) are terminated.

7.1.7.1 FTP_ITC.1 Inter-TSF trusted channel

The TOE must be configured for IPsec tunnel(s) to support the trusted channel communications with the entities listed above secured by and tunneled within IPsec sessions established using X.509 certificates or pre-shared keys. Trusted channels initiated by the TOE are to:

- SYSLOG Servers
- File Servers
- NTP Servers

7.1.7.2 FTP_TRP.1/Admin Trusted Path

The TOE supports IPsec to ensure secured communications with by remote administrators. Such remote sessions are protected from disclosure or modifications of exchanged data in the performance of administration actions and require administrator authentication before performing any functions on the TOE.

Administrative clients use the TOE CLI with SSHv2 tunneled over IPsec or the Web/GUI with HTTPS tunneled over IPsec.

8. ACRONYMS

ACRONYM/ABBREVIATION	MEANING
ACL	Access Control List
ACOS	Advanced Core Operating System
ADC	Application Delivery Controller
AES	Advanced Encryption Standard
AH	Authentication Header
ATP	Advanced Threat Protection
AV	Anti-Virus
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Common Criteria
CFW	Convergent Firewall
CGN	Carrier-Grade NAT
CLI	Command-line interface
CMVP	Cryptographic Module Validation Program
CRL	Certificate Revocation List
CSP	Critical Security Parameter
CSR	Certificate Signing Requests
DDoS	Distributed Denial of Service
DH	Diffie-Hellman
DLP	Data Loss Prevention
DNS	Domain Name System
ECDSA	Elliptic Curve Digital Signature Algorithm
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
GUI	Graphical User Interface
HMAC	Keyed-Hash Message Authentication Code
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDS	Intrustion Detection System
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
IPS	Intrusion Protection System

ACRONYM/ABBREVIATION	MEANING
IT	Information Technology
NAT	Network Address Translation
NDcPP	Network Device collaborative Protection Profile
NGFW	Next Generation Firewall
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
OCSP	Online Certificate Status Protocol
PP	Protection Profile
PKI	Public Key Infrastructure
PRF	Pseudo Random Function
PSK	Pre-Shared Key
PUBS	Publications
QSFP	Quad (4-channel) Small Form-factor Pluggable
QSFP28	Quad (4-channel) Small Form-factor Pluggable 28 GB data
RADIUS	Remote Authentication Dial-In User Service
RBG	Random Bit Generator
RSA	Rivest Shamir Adleman Algorithm
SA	Security Associations (IPSec)
SCP	Secure Copy Protocol
SD	Supporting Document
SECP	Standards for Efficient Cryptography Parameter
SF	Security Function
SFP	Security Function Policy
SFP	Small Form-factor Pluggable
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SSD	Solid State Disk
SSH	Secure Shell
SSLi	SSL Intercept
ST	Security Target
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification

ACRONYM/ABBREVIATION	MEANING
VPN	Virtual Private Network

9. REFERENCES

IDENTIFIER	REFERENCE
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, version 3.1, Revision 5
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated April 2017, version 3.1, Revision 5
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, April 2017, version 3.1, Revision 5
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, April 2017, version 3.1, Revision 5
[NDcPPv2.2e]	collaborative Protection Profile for Network Devices, Version 2.2e, 23-March-2020
[800-38A]	NIST Special Publication 800-38A Recommendation for Block 2001 Edition Recommendation for Block Cipher Modes of Operation Methods and Techniques, December 2001
[800-56A Rev 3]	NIST Special Publication 800-56A, Revision 3, April 18, 2018 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)
[FIPS 140-2]	FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules, May 25, 2001
[FIPS PUB 186-4]	FIPS PUB 186-4 Federal Information Processing Standards Publication Digital Signature Standard (DSS), July 2013
[FIPS PUB 198-1]	Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC), July 2008
[800-90Arev1]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Revision 1, June 2015
[FIPS PUB 180-4]	FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS), August 2015

REVISION HISTORY

REVISION	DATE	AUTHOR	DESCRIPTION
1.0	January 25, 2023	A10 Cert Team	Initial publication.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) enables service providers, cloud providers and enterprises to ensure their 5G networks and multi-cloud applications are secure. With advanced analytics, machine learning and intelligent automation, business-critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers in 117 countries worldwide.

For more information, visit: a10networks.com and @a10Networks.

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact