Corelight Sensor AP 200, AP 1001, AP 3000 and AP 5000 BroLin v22.1 Security Target

Document Version: 2.6
Date: April 23, 2022

intertek acumen security

2400 Research Blvd
Suite 395
Rockville, MD 20850

Revision History

Version	Date	Changes
0.1	11/01/2019	Initial version.
0.2	11/14/2019	Updated Sections 3 and 4.
0.3	1/14/2020	Updating SFRs.
0.4	1/15/2020	Updating SFRs.
0.5	1/30/2020	Updating SFRs.
0.6	2/6/2020	Added TOE deployment diagram and updated SFRs.
0.7	2/18/2020	Updated TDs.
0.8	4/7/2020	Updates based on testing.
0.9	6/11/2020	Removed Claims for TLS, X509 and AFL.
1.0	6/17/2020	Updated SFRs.
1.1	7/10/2020	Addressed Customer comments.
1.2	7/14/2020	Updated TDs.
1.3	8/19/2020	Updated ST to NDcPPv2.2e.
1.4	9/2/2020	Internal review of ST.
1.5	4/06/2021	Added AP5000 platform and updated 1.6.2 Cryptographic Support.
1.6	4/28/2021	Addressing QA comments and finalization for check in submission.
1.7	5/5/2021	Minor updates based on vendor feedback.
1.8	5/25/2021	Added newly released TDs.
1.9	6/1/2021	Updated SFRs.
2.0	7/15/2021	Updating SFRs and TSS.
2.1	8/31/2021	Updated CAVPs.
2.2	11/11/2021	Added AP3000 with newer processor.
2.3	12/03/2021	Updated to address ECR comments
2.4	02/23/2022	Updated to address QA comments.
2.5	4/1/2022	Updated based on ECR comments
2.6	4/23/2022	Updated based on ECR comments

Contents

1. Introduction

The Security Target (ST) serves as the basis for the Common Criteria (CC) evaluation and identifies the Target of Evaluation (TOE), the scope of the evaluation, and the assumptions made throughout. This document will also describe the intended operational environment of the TOE, and the functional and assurance requirements that the TOE meets.

1.1. Security Target and TOE Reference

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

Table 1 – TOE/ST Identification

Category	Identifier
ST Title	Corelight Sensor AP 200, AP 1001, AP 3000 and AP 5000 BroLin v22.1 Security Target
ST Version	2.6
ST Date	April 23, 2022
ST Author	Acumen Security, LLC.
TOE Identifier	Corelight Sensor AP 200, AP 1001, AP 3000 and AP 5000 BroLin v22.1
TOE Version	BroLin v22.1
TOE Developer	Corelight Inc.
Key Words	Network Device, Corelight Inc.

1.2. TOE Overview

Simple to deploy and integrate with existing analysis tools, the Corelight Sensor Appliances transform high-volume network traffic into high-fidelity data for incident response, intrusion detection, forensics and more. The Sensor parses dozens of network protocols and generates rich, actionable data streams designed for security professionals. The TOE includes the hardware models as defined in Table 2 in Section 1.3.

1.2.1. TOE Product Type

The Corelight Sensor AP 200, AP 1001, AP 3000 and AP 5000 BroLin v22.1 (hereafter referred to as the TOE) is a network device which is composed of hardware and software that offers a scalable solution to the end users. It satisfies all the criteria to meet the collaborative Protection Profile for Network Devices, Version 2.2e. [NDcPP v2.2e].

1.3. TOE Description

The TOE is a network device which is composed of hardware and software that offers a scalable solution to the end users. It satisfies all the criterion to meet the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e]. The TOE operating system is BroLin v22.1. The TOE boundary is the hardware appliance, which is comprised of hardware and software components.

The TOE is comprised of the following models as indicated:

Figure 1 – AP 5000

Figure 2 – AP 3000

Figure 3 – AP 1001

Figure 4 – AP 200

Table 2 – Corelight Sensor AP 200, AP 1001, AP 3000 & AP 5000

Specifications	AP 200	AP 1001	AP 3000(1)	AP 3000(2)	AP 5000
Processors	Intel Xeon Silver 4110 (Skylake)	Intel Xeon Silver 4116 (Skylake)	Intel Xeon Gold 6238 (Cascade Lake)	Intel Xeon Gold 6152 (Skylake)	AMD EPYC 7742 (Zen 2)
Size and Weight	1U half-depth rackmount (19 x 14.5 x 1.75 inches), 17 lbs.	1U rackmount (19 x 25.6 x 1.75 inches), 40 lbs	1U rackmount (19 x 25.6 x 1.75 inches), 34 lbs.	1U rackmount (19 x 25.6 x 1.75 inches), 34 lbs.	1U rackmount (19 x 27 x 1.7 inches) 48 lbs.
Monitoring Interface	Four 1G SFP interfaces in a powerful, specialized NIC. Support for copper and optical modules at 100M & 1G	Four 1G/10G SFP/SFP+ interfaces in a powerful, specialized NIC. Support for copper and optical modules at 1G and 10G	Four 1G/10G SFP/SFP+ interfaces OR two 10G QSF28 OR two 40G QSFP28 OR eight 10G QSFP28 interfaces in a powerful, specialized NIC. Support for copper and optical modules at 1G and 10G or 40G	Four 1G/10G SFP/SFP+ interfaces OR two 10G QSF28 OR two 40G QSFP28 OR eight 10G QSFP28 interfaces in a powerful, specialized NIC. Support for copper and optical modules at 1G and 10G or 40G	Two QSFP28 bays, capable of supporting eight 10G OR two 40G 8 OR two 100G interfaces in a powerful, specialized NIC
Management Interface	One 10/100/1000 copper ethernet port	One 10/100/1000 copper ethernet port and up to 2 10G ethernet ports	One 10/100/1000 copper ethernet port and up to 2 10G ethernet ports	One 10/100/1000 copper ethernet port and up to 2 10G ethernet ports	One 10/100/1000 copper ethernet port and up to 4 10G ethernet ports
Power	120/240 VAC 50/60 Hz single PSUs. Approximately 83W usage when idle and	120/240 VAC 50/60 Hz redundant dual PSUs. 700W at 110V or 750W at 220V. Approximate	120/240 VAC 50/60 Hz redundant dual PSUs. Approximately 161W usage when idle and 445W usage at load	120/240 VAC 50/60 Hz redundant dual PSUs. Approximately 161W usage when idle and 445W usage at load	120/240 VAC 50/60 Hz redundant dual PSUs. Approximately 443W usage when idle and 852W usage at load

Specifications	AP 200	AP 1001	AP 3000(1)	AP 3000(2)	AP 5000
	141W usage at load	ly 180W usage when idle and 290W usage at load			

1.4. TOE Evaluated Configuration

The TOE in the evaluated configuration consists of the platform as stated in Section 1.3. The TOE supports secure connectivity with another IT environment device as stated in Table 3:

Table 3 – IT Components

Component	Required	Usage
Audit server (via SFTP server)	Yes	The TOE exports audit events to an external SFTP server via SSH v2 protocol.
Management workstation with SSH client	Yes	This includes any IT Environment Management workstation with an SSH client

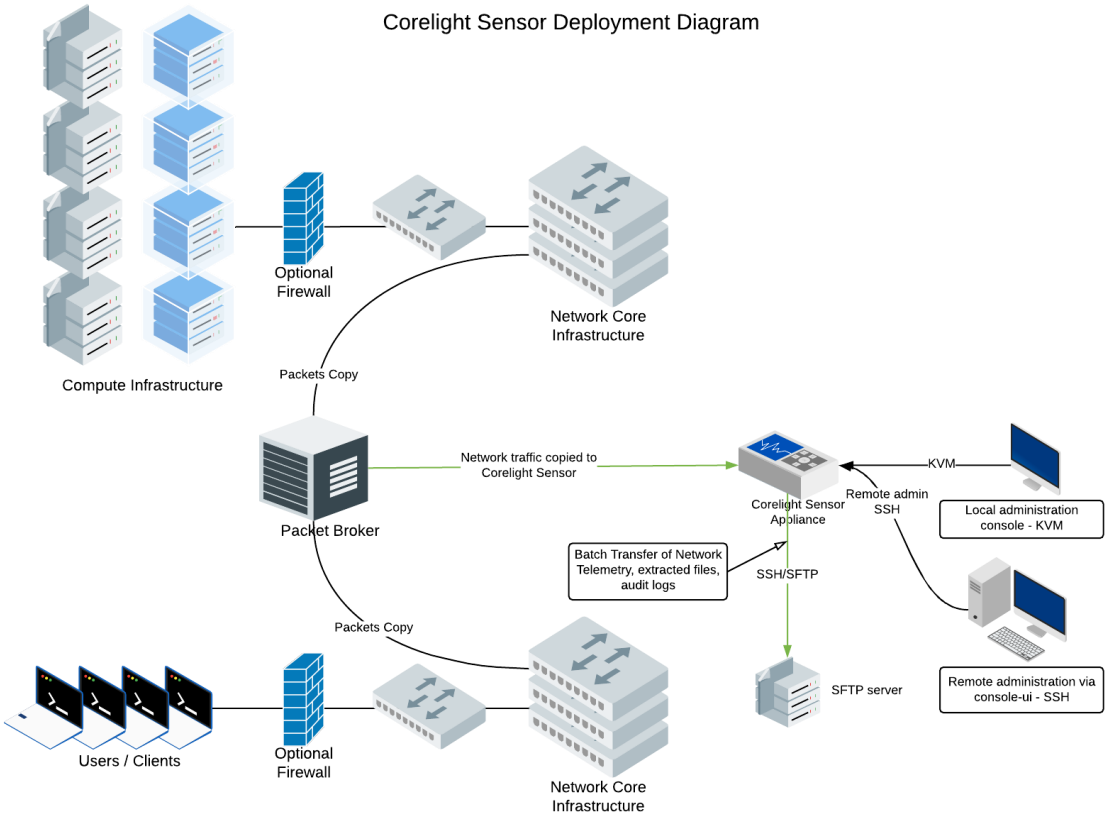

Figure 5 – Corelight Sensor Deployment Diagram

1.5. Physical Scope of the TOE

The TOE boundary is the hardware appliance which consists of hardware and software components. It is deployed in an environment which contains the various IT components as depicted in Figure 5. The TOE guidance documentation can be found on the Corelight website: https://www.corelight.com. An account is required to access the guidance documents and any software updates.

The TOE is shipped with the software pre-installed on it. Software updates are available for download from Corelight.

1.6. Logical Scope of the TOE

The TOE implements the following security functional requirements:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management

- Protection of the TSF
- TOE Access
- Trusted Path/Channels

Each of these security functionalities are listed in more detail below.

1.6.1. Security Audit

The TOE generates audit events for all start-up and shut-down functions, and all auditable events as specified in Table 13. Audit events are also generated for management actions specified in FAU_GEN.1. The TOE can store audit events locally and export them to an external audit server (via SFTP server using SSH v2). Each audit record contains the date and time of event, type of event, subject identity, and the relevant data of the event.

1.6.2. Cryptographic Support

The TOE provides cryptographic support for the services described in Table 4. The related CAVP validation details are provided in Table 5. The operating system is BroLin v22.1 which is based upon Linux Kernel version 4.19.143. The TOE leverages the Corelight Cryptographic Module for its cryptographic functionality.

Table 4 – TOE Cryptography Implementation

Cryptographic Method	Usage
FCS_CKM.1 Cryptographic Key Generation	• Cryptographic key generation conforming to FIPS PUB 186-4 Digital Signature Standard (DSS), Appendix B.3. • RSA Key sizes supported are 2048 and 3072 bits. • Cryptographic key generation conforming to FIPS PUB 186-4 Digital Signature Standard (DSS)", Appendix B.4. • Elliptic NIST curves supported are: P-256, P-384 and P-521. • 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.
FCS_CKM.2 Cryptographic Key Establishment	• RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1". • Elliptical curve-based establishment conforming to NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography". • FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [groups listed in RFC 3526].

Cryptographic Method	Usage
FCS_CKM.4 Cryptographic Key Destruction	• Refer to Table 17 for Key Zeroization details.
FCS_COP.1/DataEncryption	• AES encryption and decryption conforming to CBC as specified in ISO 10116, CTR as specified in ISO 10116 and GCM as specified in ISO 19772. • AES key size supported are 128 and 256 bits. • AES modes supported are CBC, CTR and GCM.
FCS_COP.1/SigGen	• RSA digital signature algorithm conforming to 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. • RSA key sizes supported are: 2048 and 3072 bits. • Elliptical curve digital signature algorithm conforming to FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST curves” ISO/IEC 14888-3, Section 6.4. • Elliptical curve key size supported is 256 bits. • Elliptic NIST curves supported are: P-256, P-384 and P-521.
FCS_COP.1/Hash	• Cryptographic hashing services conforming to ISO/IEC 10118-3:2004. • Hashing algorithms supported are: SHA-1, SHA-256, SHA-384 and SHA-512. • Message digest sizes supported are: 160, 256, 384 and 512 bits.
FCS_COP.1/KeyedHash	• Keyed-hash message authentication conforming to ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”. • Keyed hash algorithms supported are: HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512. • Key sizes supported are: 160, 256, 384 and 512 bits. • Message digest sizes supported are: 160, 256, 384 and 512 bits.
FCS_DRBG_EXT.1 Random Bit Generation	• Random number generation conforming to ISO/IEC 18031:2011. • The TOE leverages CTR_DRBG(AES) • CTR_DRBG seeded with a minimum of 256 bits of entropy.

Cryptographic Method	Usage
FCS_SSHC_EXT.1 SSH Client Protocol	• The TOE supports SSH v2 protocol compliant to the following RFCs: 4251, 4252, 4253, 4254, 4344, 5656, 6668, 8308 Section 3.1,and 8332. • SSH public-key authentication uses rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 and ecdsa-sha2-nistp521. • SSH transport uses the following encryption algorithms: aes128-cbc, aes256-cbc, aes128-ctr, and aes256-ctr. • Packets greater than 262144 bytes in an SSH transport connection are dropped. • SSH transport uses the following data integrity MAC algorithms: hmac-sha1, hmac-sha2-256, and hmac-sha2-512 • Key exchange algorithms supported are: diffie-hellman-group14-sha1 and ecdh-sha2-nistp256. • The TOE ensures that within SSH connections the same session keys are used for a threshold of no longer than one hour and no more than one gigabyte of transmitted data. • The TOE shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key as described in RFC 4251 Section 4.1.
FCS_SSHS_EXT.1 SSH Server Protocol	• The TOE supports SSH v2 protocol compliant to the following RFCs: 4251, 4252, 4253, 4254, 4344, 5656, 6668, 8308 Section 3.1, and 8332. • SSH public-key authentication supports the following: ssh-rsa, rsa-sha2-256, rsa-sha2-512 and ecdsa-sha2-nistp256. • SSH transport uses the following encryption algorithms: aes128-ctr, and aes256-ctr. • Packets greater than 262144 bytes in an SSH transport connection are dropped. • SSH transport uses the following data integrity MAC algorithms: hmac-sha1, hmac-sha2-256, and hmac-sha2-512 • Key exchange algorithms supported are: diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521. • The TOE ensures that within SSH connections the same session keys are used for a threshold of no longer than one hour and no more than one gigabyte of transmitted data.

Table 5 – Cryptographic Algorithm Certificates

Cryptographic Algorithms	CAVPs
AES	A1870
RSA	A1870, A1872
ECDSA	A1870
ECDSA KAS	A1871
HMAC	A1870
SHS	A1870
DRBG	A1870

1.6.3. Identification and Authentication

The TOE provides authentication services for administrative users to connect to the TOE's secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE supports password-based authentication and public key-based authentication. Password-based authentication can be performed on the local console. The SSHv2 interface supports authentication using SSH keys.

1.6.4. Security Management

The TOE supports local and remote management of its security functions including:

- Local console CLI administration
- Remote CLI administration via SSHv2
- Password configurations and authentication failure handling
- Users – Security Administrator (Admin)
- Configurable banners to be displayed at login
- Timeouts to terminate administrative sessions after a set period of inactivity
- Protection of secret keys and passwords

1.6.5. TOE Access

Prior to establishing an administration session with the TOE, a banner is displayed to the user. The banner messaging is customizable. The TOE will terminate an interactive session after 60 minutes of session inactivity. A user can terminate their local CLI session and remote CLI session by entering exit at the prompt.

1.6.6. Protection of the TSF

The TOE protects all passwords, pre-shared keys, symmetric keys and private keys from unauthorized disclosure. Passwords are stored on the file system in encrypted format. Passwords are stored as SHA-512 salted hash value as per standard Linux approach. The TOE executes self-tests during initial start-up to ensure correct operation and enforcement of its security functions. An administrator can install software updates to the TOE. The TOE internally maintains the date and time.

1.6.7. Trusted Path/Channels

The TOE supports SSH v2 for secure communication to the following IT entities: Audit server (via) SFTP server. The TOE supports SSH v2 (remote CLI) for secure remote administration.

1.7. Excluded Functionality

The following interfaces are not included as part of the evaluated configuration:

- NTP server (optional)
- telnet is disabled
- Local Web UI (HTTP and HTTPS is disabled)

1.8. TOE Documentation

The following documents are essential to understanding and controlling the TOE in the evaluated configuration:

Table 6 – TOE Documentation

Documentation	Version
Corelight Sensor AP 200, AP 1001, AP 3000 and AP 5000 BroLin v22.1 Security Target	2.6
Corelight Common Criteria Guidance document	0.8

1.9. Other References

In additional to TOE documentation, the following reference may also be valuable when understanding and controlling the TOE:

- collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e]

2. 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:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017: Part 2 extended
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017: Part 3 conformant

2.2. Protection Profile Conformance

This TOE is conformant to:

- collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e]

2.3. Conformance Rationale

This Security Target provides exact conformance to Version 2.2e of the Collaborative Protection Profile for Network Devices. The security problem definition, security objectives and security requirements in this ST are all taken from the Protection Profile performing only operations defined there.

2.4. NIAP Technical Decisions

All NIAP TDs issued to date and applicable to NDcPP v2.2e have been considered. Table 7 identifies all applicable TDs.

Table 7 – NIAP Technical Decisions

NIAP Technical Decision (TDs) for NDcPP v2.2e		
Technical Decision	**Applicable**	**Exclusion Rationale (if applicable)**
TD0592 – NIT Technical Decision for Local Storage of Audit Records	Yes	
TD0591 – NIT Technical Decision for Virtual TOEs and hypervisors	No	TOE is not virtual.
TD0581 – NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	Yes	
TD0580 – NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	Yes	
TD0572 – NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	No	TLS functionality is not claimed.

NIAP Technical Decision (TDs) for NDcPP v2.2e		
Technical Decision	**Applicable**	**Exclusion Rationale (if applicable)**
TD0571 – NiT Technical Decision for Guidance on how to handle FIA_AFL.1	Yes	
TD0570 – NiT Technical Decision for Clarification about FIA_AFL.1	Yes	
TD0569 – NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	No	DTLS functionality is not claimed.
TD0564 – NiT Technical Decision for Vulnerability Analysis Search Criteria	Yes	
TD0563 – NiT Technical Decision for Clarification of audit date information	Yes	
TD0556 – NIT Technical Decision for RFC 5077 question	No	TLS functionality is not claimed.
TD0555 – NIT Technical Decision for RFC Reference incorrect in TLSS Test	No	TLS functionality is not claimed.
TD0547 – NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	Yes	
TD0546 – NIT Technical Decision for DTLS - clarification of Application Note 63	No	DTLS functionality is not claimed.
TD0538 - NIT Technical Decision for Outdated link to allowed-with list	Yes	
TD0537 - NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	No	TLS functionality is not claimed.
TD0536 - NIT Technical Decision for Update Verification Inconsistency	Yes	
TD0528 - NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	No	NTP functionality is not claimed.
TD0527 - Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	No	X509 functionality is not claimed.

3. Security Problem Definition

The security problem definition has been taken from [NDcPP v2.2e] and is reproduced here for the convenience of the reader.

3.1. Threats

The threats for the Network Device are grouped according to functional areas of the device in the sections below:

Table 8 – Threats

ID	Threat
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.

ID	Threat
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

This section describes the assumptions made in identification of the threats and security requirements for network devices. The network device is not expected to provide assurance in any of these areas, and as a result, requirements are not included to mitigate the threats associated.

Table 9 – Assumptions

ID	Assumption
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
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.

ID	Assumption
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.

3.3. Organizational Security Policy

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. For the purposes of this cPP a single policy is described in the section below:

Table 10 – Organizational Security Policy

Documentation	Version
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

The security objectives have been taken from [NDcPP v2.2e] and are reproduced here for the convenience of the reader.

4.1. Security Objectives for the Operational Environment

The following subsections describe objectives for the Operational Environment:

Table 11 – Security Objectives for the Operational Environment

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

5. Security Requirements

This section identifies the Security Functional Requirements for the TOE and/or Platform. The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, dated: April 2017 and all international interpretations.

5.1. Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized* text;
- Refinement made by PP author: Indicated with **bold** text. All bold text from the PP was retained;
- 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).
- Where operations were completed in the PP itself, the formatting used in the PP has been retained.

Explicitly stated SFRs are identified by having a label 'EXT 'after the requirement name for TOE SFRs. Formatting conventions outside of operations matches the formatting specified within the PP.

5.2. TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear below in Table 12 are described in more detail in the following subsections:

Table 12 – TOE Security Functional Requirements

Requirement	Description
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_STG_EXT.1	Protected Audit Event Storage
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.2	Cryptographic Key Establishment
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)

Requirement	Description
FCS_RBG_EXT.1	Random Bit Generation
FCS_SSHC_EXT.1	SSH Client Protocol
FCS_SSHS_EXT.1	SSH Server Protocol
FIA_AFL.1	Authentication Failure Management
FIA_PMG_EXT.1	Password Management
FIA_UIA_EXT.1	User Identification and Authentication
FIA_UAU_EXT.2	Password-based Authentication Mechanism
FIA_UAU.7	Protected Authentication Feedback
FMT_MOF.1/ManualUpdate	Trusted Update - 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
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)
FPT_APW_EXT.1	Protection of Administrator Passwords
FPT_TST_EXT.1	TSF Testing (Extended)
FPT_TUD_EXT.1	Trusted Update
FPT_STM_EXT.1	Reliable Time Stamps
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 Banner
FTP_ITC.1	Inter-TSF Trusted Channel (Refinement)
FTP_TRP.1/Admin	Trusted Path (Refinement)

5.2.1. Class: Security Audit (FAU)

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).*
   - *[[Starting and stopping services]*
   - *no other actions];*
d) *Specifically defined auditable events listed in Table 13.*

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 13.*

Table 13 – Auditable Events

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.

Requirement	Auditable Events	Additional Audit Record Contents
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_RBG_EXT.1	None.	None.
FCS_SSHC_EXT.1	Failure to establish an SSH session	Reason for failure
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure
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.MOF.1/Services	None	None
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents
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.
FTP_TRP.1/Admin	• Initiation of the trusted path. • Termination of the trusted path. • Failure of the trusted path functions.	None.

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 [

- *The 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 events being replaced with new ones]*] when the local storage space for audit data is full.

5.2.2. Class: 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, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;*
- *FFC Schemes using 'safe-prime 'groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526].*

] ~~and specified cryptographic key sizes [assignment: *cryptographic key sizes]* that meet the following: [assignment: *list of standards].*~~

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: [

- *RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1",*
- *Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";*
- *FFC Schemes using "safe-prime" groups that meet the following: "NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [groups listed in RFC 3526].*

] ~~that meets the following: [assignment: *list of standards*].~~

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-pass] overwrite consisting of [zeroes, a new value of the key];*

]

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, CTR, GCM] mode* and cryptographic key sizes *[128 bits, 256 bits]* that meet the following: *AES as specified in ISO 18033-3, [CBC as specified in ISO 10116, CTR 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, 3072],*
- *Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256 bits]*

]

that meet the following*:* [

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

].

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 cryptographic key sizes [*assignment: cryptographic key sizes*]~~ 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 (Keyed Hash Algorithm)

FCS_COP.1.1/KeyedHash
The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [*HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512*] and cryptographic key sizes [*160, 256, 384,512 (in bits) used in HMAC*] **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 *[[2] software-based noise source]* with a minimum of [*256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

5.2.2.9. FCS_SSHC_EXT.1 SSH Client Protocol

FCS_SSHC_EXT.1.1
The TSF shall implement the SSH protocol in accordance with: RFCs *4251, 4252, 4253, 4254,* [*4344, 5656, 6668, 8268, 8308 Section 3.1, 8332*].

FCS_SSHC_EXT.1.2
The TSF shall ensure that the SSH protocol implementation supports the following user authentication methods as described in RFC 4252: public key-based, [*no other method*].

FCS_SSHC_EXT.1.3
The TSF shall ensure that, as described in RFC 4253, packets greater than [*262000*] bytes in an SSH transport connection are dropped.

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

FCS_SSHC_EXT.1.5
The TSF shall ensure that the SSH public-key based authentication implementation uses [*rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521*] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHC_EXT.1.6
The TSF shall ensure that the SSH transport implementation uses *[hmac-sha1, hmac-sha2-256, hmac-sha2-512]* as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHC_EXT.1.7
The TSF shall ensure that *[diffie-hellman-group14-sha1, ecdh-sha2-nistp256]* and *[no other methods]* are the only allowed key exchange methods used for the SSH protocol.

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

FCS_SSHC_EXT.1.9
The TSF shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key and [*no other methods*] as described in RFC 4251 section 4.1.

5.2.2.10. FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1
The TSF shall implement the SSH protocol in accordance with: RFCs 4251, 4252, 4253, 4254, [*4344, 5656, 6668, 8268, 8308 Section 3.1, 8332*].

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

FCS_SSHS_EXT.1.3
The TSF shall ensure that, as described in RFC 4253, packets greater than [*262000*] bytes in an SSH transport connection are dropped.

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

FCS_SSHS_EXT.1.5
The TSF shall ensure that the SSH public-key based authentication implementation uses [*ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256*] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6
The TSF shall ensure that the SSH transport implementation uses *[hmac-sha1, hmac-sha2-256, hmac-sha2-512]* as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7
The TSF shall ensure that *[ecdh-sha2-nistp256]* and *[diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, ecdh-sha2-nistp384, ecdh-sha2-nistp521*] are the only allowed key exchange methods used for the SSH protocol.

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

5.2.3. Class: Identification and Authentication (FIA)

5.2.3.1. Authentication Failure Management

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within *[3-15]* unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [*prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until 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 [*64*] 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.**

5.2.4. Class: Security Management (FMT)

5.2.4.1. FMT_MOF.1/ManualUpdate Management of Security Functions Behavior

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

5.2.4.2. FMT_MOF.1/Services Management of Security Functions Behavior

FMT_MOF.1.1/Services

The TSF shall restrict the ability to start and stop the services to Security Administrators.

5.2.4.3. FMT_MTD.1/CoreData Management of TSF Data

FMT_MTD.1/CoreData
The TSF shall restrict the ability to manage the *TSF data* to *Security Administrators*.

5.2.4.4. FMT_MTD.1/CryptoKeys Management of Cryptographic Keys

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

5.2.4.5. 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 start and stop services;*
  - *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 configure the cryptographic functionality;*
  - *Ability to configure thresholds for SSH rekeying;*
  - *Ability to re-enable an Administrator account;*
  - *Ability to set the time which is used for time-stamps;*
  - *Ability to manage the cryptographic keys;*
  - *No other capabilities*].

5.2.4.6. FMT_SMF.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.

5.2.5. Class: 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_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*].

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 [*no other TOE firmware/software version*].

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

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

5.2.5.5. FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1.1
The TSF shall run a suite of the following self-tests [*during initial start-up (on power on), at the request of the authorized user, at the conditions [by performing a system or card level restart command]]* to demonstrate the correct operation of the TSF:
[

- *SHA KAT Known Answer Test*
- *AES KAT Known Answer Test*
- *HMAC SHA KAT Known Answer Test*
- *DRBG KAT Known Answer Test*
- *ECDH KAT Known Answer Test*
- *GCM KAT Known Answer Test*

].

5.2.6. Class: 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

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. Class: Trusted Path/Channels (FTP)

5.2.7.1. FTP_ITC.1 Inter-TSF trusted channel (Refinement)

FTP_ITC.1.1
The TSF shall **be capable of using [*SSH*] to** provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [*[SFTP server]*]** 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 [*audit server (SFTP server)*

].

5.2.7.2. FTP_TRP.1/Admin Trusted Path (Refinement)

FTP_TRP.1.1/Admin
The TSF shall **be capable of using [*SSH*] 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*.

5.3. TOE SFR Dependencies Rationale for SFRs

The Collaborative Protection Profile for Network Devices contains all the requirements claimed in this ST. As such, the dependencies are not applicable since the PP has been approved.

5.4. Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the Collaborative Protection Profile for Network Devices which are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in the table below:

Table 14 – Security Assurance Requirements

Assurance Class	Assurance Components	Component Description
Security Target (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE summary specification
Development (ADV)	ADV_FSP.1	Basic functionality specification
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative Procedures
Life Cycle Support (ALC)	ALC_CMC.1	Labelling of the TOE

Assurance Class	Assurance Components	Component Description
	ALC_CMS.1	TOE CM coverage
Tests (ATE)	ATE_IND.1	Independent testing – conformance
Vulnerability Assessment (AVA)	AVA_VAN.1	Vulnerability survey

5.5. Rationale for Security Assurance Requirements

The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.

5.6. Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by Corelight to satisfy the assurance requirements. The table below lists the details:

Table 15 – TOE Security Assurance Measures

SAR Component	How the SAR will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.

SAR Component	How the SAR will be met
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope of error.
ALC_CMS.1	
ATE_IND.1	Corelight Inc. will provide the TOE for testing.
AVA_VAN.1	Corelight Inc. will provide the TOE for testing.

6. TOE Summary Specifications

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

Table 16 – TOE Summary Specification SFR Description

Requirement	TSS Description
FAU_GEN.1	The TOE generates a comprehensive set of audit logs that identify specific TOE operations whenever an auditable event occurs. Auditable events are specified in Table 13. Each audit record contains the date and time of event, type of event, subject identity, and the outcome (success or failure) of the event. All configuration changes are recorded with subject identity as the user request is made through the command line interface (CLI) with either local or remote connection. Administrative tasks of generating, deleting cryptographic keys contain the necessary audit information as mandated by FAU_GEN.1.1.
FAU_GEN.2	For audit events that result from actions of identified users, the TOE can associate each auditable event with the identity of the user that caused the event.
FAU_STG_EXT.1	The TOE can be configured to export audit events securely to an audit server using SSH v2 protocol. The audit server in this case is the SFTP server. The TOE is a standalone TOE that stores audit data locally. The TOE stores up to 100,000 audit records locally. When the local data is full, the oldest audit events are overwritten to allow new audit events to be created. The TOE is designed to store 100K records in the database. API queries however are limited to 7 days. Security Administrators can access the audit events and can clear the audit events. This way, audit events are protected against unauthorized access. The TOE transmits audit data to an external audit server periodically in batches. The audit log data is transferred in response to the expiration of a timer (3600 seconds). If there is an SSH connection failure, the TOE will continue to store local audit events on the TOE and will transmit any locally stored contents when connectivity to the audit server is restored.
FCS_CKM.1	The TOE supports RSA key sizes of 2048 bits and 3072 bits, for key generation conforming to Cryptographic key generation conforming to FIPS PUB 186-4 Digital Signature Standard (DSS), Appendix B.3. The RSA keys are used in support of digital signature for SSH communications. The TOE supports Elliptical NIST curve sizes of P-256, P-384 and P-521 conforming to Cryptographic key generation conforming to FIPS PUB 186-4 Digital Signature Standard (DSS)", Appendix B.4. The Elliptic keys are used in support of ECDH key exchange. The TOE supports 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. The TOE supports DHG14 key generation in support of DH key exchanges as part of SSH. Please refer to Table 5 Cryptographic Algorithm Certificates for NIST CAVPs for RSA and ECDSA.

<table>
<tr><th>Requirement</th><th>TSS Description</th></tr>
<tr><td>FCS_CKM.2</td><td>
The TOE supports Cryptographic Key Establishment using the following schemes:

RSA key based establishment conforming to RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. The TOE implements RSA key establishment scheme with key sizes of 2048 and 3072 bits.
Elliptical curve-based establishment conforming to NIST Special Publication 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.
FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and groups listed in RFC 3526.

RSA and ECC schemes are used in support of SSH communications and FFC based key exchange based on NIST SP 800-56Ar3/Diffie-Hellman Group 14 (RFC3526).
The TOE acts as both a sender and receiver for RSA based key establishment scheme and Elliptic curve-based key establishment scheme.
<table>
<tr><th>Scheme</th><th>SFR</th><th>Service</th></tr>
<tr><td>RSA
ECC</td><td>FCS_SSHC_EXT.1/
FCS_SSHS_EXT.1</td><td>Administration
Audit Server</td></tr>
<tr><td>FFC/DH14</td><td>FCS_SSHS_EXT.1</td><td>Audit Server
Administration</td></tr>
</table>
Please refer to Table 5 Cryptographic Algorithm Certificates for NIST CAVPs for RSA and ECDSA.
</td></tr>
<tr><td>FCS_CKM.4</td><td>The TOE satisfies all requirements as specified in FCS_CKM.4 of NDcPPv2.2e for destruction of keys and CSPs. Please refer to Table 17 Zeroization Table.</td></tr>
<tr><td>FCS_COP.1/DataEncryption</td><td>
The TOE supports AES encryption and decryption conforming to CBC as specified in ISO 10116, CTR as specified in ISO 10116 and GCM as specified in ISO 19772.
The AES key size supported are 128 bits and 256 bits and the AES modes supported are: CBC, CTR and GCM.
Please refer to Table 5 Cryptographic Algorithm Certificates for NIST CAVPs for AES.
</td></tr>
</table>

<table>
<tr><th>Requirement</th><th>TSS Description</th></tr>
<tr><td>FCS_COP.1/SigGen</td><td>The TOE provides Cryptographic signature generation and verification in accordance with the following cryptographic algorithms:
RSA digital signature conforming to 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.
The RSA key sizes supported are: 2048 and 3072 bits.
The TOE uses Elliptical curve digital signature algorithm conforming to FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST curves” [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4
The Elliptical curve key size supported is 256 bits.
Please refer to Table 5 Cryptographic Algorithm Certificates for NIST CAVPs for RSA and ECDSA.</td></tr>
<tr><td>FCS_COP.1/Hash</td><td>The TOE supports Cryptographic hashing services conforming to ISO/IEC 10118-3:2004. The hashing algorithms are used in SSH connections for secure communications.
The following hashing algorithms are supported: SHA-1, SHA-256, SHA-384 and SHA-512.
The message digest sizes supported are: 160, 256, 384 and 512 bits.
Please refer to Table 5 Cryptographic Algorithm Certificates for NIST CAVPs SHS.</td></tr>
<tr><td>FCS_COP.1/KeyedHash</td><td>The TOE supports Keyed-hash message authentication conforming to ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”. HMAC algorithms is used in support of SSH sessions.
<table>
<tr><th>HMAC Algorithms</th><th>Hash Functions</th><th>Block Size</th><th>Key lengths</th><th>MAC lengths</th></tr>
<tr><td>HMAC-SHA-1</td><td>SHA-1</td><td>160 bits</td><td>160 bits</td><td>160 bits</td></tr>
<tr><td>HMAC-SHA-256</td><td>SHA-256</td><td>512 bits</td><td>256 bits</td><td>256 bits</td></tr>
<tr><td>HMAC-SHA-384</td><td>SHA-384</td><td>1024 bits</td><td>384 bits</td><td>384 bits</td></tr>
<tr><td>HMAC-SHA-512</td><td>SHA-512</td><td>1024 bits</td><td>512 bits</td><td>512 bits</td></tr>
</table>
Please refer to Table 5 Cryptographic Algorithm Certificates for NIST CAVPs for HMAC.</td></tr>
<tr><td>FCS_RBG_EXT.1</td><td>The TOE uses CTR_DRBG conforming to ISO/IEC 18031:2011.
The CTR_DRBG is seeded by an entropy source that accumulates entropy from 2 software-based noise sources with a minimum of 256 bits of entropy. The min entropy claims that there is about 7 bits of entropy per every 8 bits.
Please refer to Table 5 Cryptographic Algorithm Certificates for NIST CAVPs for DRBG.</td></tr>
</table>

Requirement	TSS Description
FCS_SSHC_EXT.1.1	The TOE implements SSH protocol that complies with RFC(s) 4251, 4252, 4253, 4254, 4344, 5656, 6668, 8308 Section 3.1, and 8332.
FCS_SSHC_EXT.1.2	The TOE supports public key authentication. The following public key algorithms are supported: rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 and ecdsa-sha2-nistp521. This list conforms to FCS_SSHC_EXT.1.5.
FCS_SSHC_EXT.1.3	The TOE accepts packet size up to 262000 bytes and meets the requirements of RFC 4253.
FCS_SSHC_EXT.1.4	The TOE supports the following encryption algorithms: aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr for SSH transport. There are no optional characteristics specified for FCS_SSHC_EXT.1.4. This list is identical to those claimed for FCS_SSHC_EXT.1.4.
FCS_SSHC_EXT.1.5	The following are the public key algorithms supported: rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 and ecdsa-sha2-nistp521. There are no optional characteristics specified for FCS_SSHC_EXT.1.5. This list is identical to those claimed for FCS_SSHC_EXT.1.5.
FCS_SSHC_EXT.1.6	The TOE supports the following data integrity MAC algorithms: hmac-sha1, hmac-sha2-256, and hmac-sha2-512. This list corresponds to the list in FCS_SSHC_EXT.1.6.
FCS_SSHC_EXT.1.7	The TOE supports the following key exchange algorithms: diffie-hellman-group14-sha1 and ecdh-sha2-nistp256. This list corresponds to the list in FCS_SSHC_EXT.1.7.
FCS_SSHC_EXT.1.8	The TOE is capable of rekeying. The TOE verifies the following thresholds: • No longer than one hour • No more than one gigabyte of transmitted data The TOE continuously checks both conditions. When either of the conditions are met, the TOE will initiate a rekey.
FCS_SSHS_EXT.1.1	The TOE implements SSH protocol that complies with RFC(s) 4251, 4252, 4253, 4254, 4344, 5656, 6668, 8308 Section 3.1, and 8332.
FCS_SSHS_EXT.1.2	The TOE supports public key authentication and password-based authentication. The following public key algorithms: ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256. This list conforms to FCS_SSHS_EXT.1.5.
FCS_SSHS_EXT.1.3	The TOE accepts packet size up to 262000 bytes and meets the requirements of RFC 4253.
FCS_SSHS_EXT.1.4	The TOE supports the following encryption algorithms: aes128-ctr, aes256-ctr for SSH transport. There are no optional characteristics specified for FCS_SSHS_EXT.1.4. This list is identical to those claimed for FCS_SSHS_EXT.1.4.

Requirement	TSS Description
FCS_SSHS_EXT.1.5	The following are the public key algorithms supported: ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256. There are no optional characteristics specified for FCS_SSHS_EXT.1.5. This list is identical to those claimed for FCS_SSHS_EXT.1.5. The TOE verifies that the SSH client's presented public key matches one that is stored within the SSH server's authorized_keys file.
FCS_SSHS_EXT.1.6	The TOE supports the following data integrity MAC algorithms: hmac-sha1, hmac-sha2-256, and hmac-sha2-512. This list corresponds to the list in FCS_SSHS_EXT.1.6.
FCS_SSHS_EXT.1.7	The TOE supports the following key exchange algorithms: diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521. This list corresponds to the list in FCS_SSHS_EXT.1.7.
FCS_SSHS_EXT.1.8	The TOE is capable of rekeying. The TOE verifies the following thresholds: • No longer than one hour • No more than one gigabyte of transmitted data The TOE continuously checks both conditions. When either of the conditions are met, the TOE will initiate a rekey.
FIA_AFL.1	The TOE allows the administrator to configure the number of successive failed authentication attempts. When a user fails to authenticate a number of times equal to the configured limit, the TOE locks the claimed user identity until the configured time is reached. Administrators can configure unsuccessful authentication attempts range between 3 – 15 within 60 minutes. When the account is locked, the TOE does not permit any further actions until the account is accessible. The authentication failures cannot lead to a situation where no administrator access is available since the local CLI would not be subject to lockout.
FIA_PMG_EXT.1	The TOE provides the following password management capabilities for administrator passwords: • Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")" ," ~ "," ", """. • Minimum password lengths shall be configurable to 8 characters to maximum of 64 characters. The default minimum password length is 8 characters.

Requirement	TSS Description
FIA_UIA_EXT.1	The TOE does not permit any actions prior to Administrators logging into the TOE. They can view the banner at the login prompt. Administrative access to the TOE is facilitated through one of several interfaces: • Connecting to the console port by plugging a keyboard and monitor directly into the ports on the back of the TOE • Remotely connecting to each appliance via SSHv2 For local administration, the TOE prompts the user for a username and password. When the user provides the correct username and password, this is compared to the known user database and if they match then the user is granted access. Otherwise, the user will not be granted access to the TOE. The TOE does not provide a reason for failure in the cases of a login failure. For remote administration, the TOE supports RSA public key authentication. If the user uses public key-based authentication and it is successful, then the user is granted access to the TOE. If the user enters invalid user credentials, they will not be granted access and will be presented the login page.
FIA_UAU_EXT.2	The TOE provides a local password-based authentication mechanism to perform local administration user authentication.
FIA_UAU.7	Password are obscured to the users. For all authentication at the local CLI the TOE displays only "*" characters when the administrative password is entered.
FMT_MOF.1(1)/ManualUpdate	Only Security Administrators can perform manual software updates.
FMT_MOF.1/Services	Only Security Administrators have the ability to configure audit behavior.
FMT_MTD.1/CoreData	The TOE implements Role Based Access Control (RBAC). Administrative users are required to login before being provided with access to any administrative functions. The TOE restricts the ability to manage the TOE to Security Administrators, otherwise referred to as the Administrator role. The TOE maintains the following roles: Administrator, Network, and Monitor. Security functions and data are restricted to the Administrator role.
FMT_MTD.1/CrytpoKeys	Only Security Administrators can manage the cryptographic keys.

Requirement	TSS Description
FMT_SMF.1	The TOE provides all the capabilities necessary to securely manage the TOE. The administrative user can connect to the TOE using the CLI to perform the below functions via SSHv2, or at the local console. Refer to the Guidance documentation for configuration syntax, commands, and information related to each of these functions. The Security Administrator (admin) has the following 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 start and stop services; • 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 configure the cryptographic functionality; • Ability to configure thresholds for SSH rekeying; • Ability to re-enable an Administrator account; • Ability to set the time which is used for time-stamps; • Ability to manage the cryptographic keys;
FMT_SMR.2	The TOE maintains the following user role: Security Administrator (Admin).The Security Administrator can manage the TOE both locally and remotely.
FPT_SKP_EXT.1	The TOE stores all pre-shared keys, symmetric keys and private keys in a secure storage and is not accessible through an interface to administrators. Refer to Section 7 Cryptographic Key Destruction, Table 17 Zeroization Table for all detail on key storage.
FPT_APW_EXT.1	All passwords are stored in a secure directory that is not readily accessible to administrators through any interface. The passwords are stored as SHA-512 salted hash.

Requirement	TSS Description
FPT_TST_EXT.1	All crypto algorithms used by the management interface must go through power up self-tests (KAT) before they can be used to provide service. The TOE executes the following power-on self-tests: • SHA KAT Known Answer Test - The SHA algorithm is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating properly. • AES KAT Known Answer Test - The AES encryption and AES decryption algorithms are tested using test vectors. The results are compared against pre-computed results to ensure the algorithms are operating properly. • HMAC SHA KAT Known Answer Test - The HMAC algorithm is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating properly. • DRBG KAT Known Answer Test - The DRBG is seeded with a pre-determined entropy and the DRBG output is compared with output values expected for the pre-determined seed. • ECDH KAT Known Answer Test - The ECDSA Signature is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating properly. • GCM KAT Known Answer Test - The GCM algorithm is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating properly. When device detects a failure during one or more of the self-tests, it raises an alarm. The administrator can attempt to reboot the TOE to clear the error. If rebooting the device does not resolve the issue, then the administrator should contact their next level of support or their Corelight support group for further assistance. All power up self-tests execution is logged for both successful and unsuccessful completion. The Software Integrity Test is run automatically on start-up, and whenever the system images are loaded. These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected.
FPT_TUD_EXT.1	Security Administrators can query the current version of the TOE and they are able to perform manual software updates. The currently active version of the TOE can be queried by issuing the “corelight-client information get” command. When software updates are available, they can obtain, verify the integrity and install the updates. The software images are digitally signed using RSA digital signature mechanism. The TOE will use a public key in order to verify the digital signature, upon successful verification the image will be loaded onto the TOE. If the images cannot be verified, the image will not be loaded onto the TOE.

Requirement	TSS Description
FPT_STM.1	The TOE provides reliable time stamps. The clock function is reliant on the system clock provided by the underlying hardware. The following security functions make use of the time: • Audit events • Session inactivity
FTA_SSL_EXT.1	The TOE will terminate the local administrative session after a Security Administrator defined period of inactivity. The inactivity time-out can be configured by the following commands: corelight-client configuration update --security.auto_logout.enable=True corelight-client configuration update --security.auto_logout.timeout=<idle-minutes>
FTA_SSL.3	A Security Administrator can configure maximum inactivity times for administrative sessions through the TOE local CLI and remote SSH interfaces. The default inactivity time period is 60 minutes for both the CLI and SSH interfaces. The configuration of inactivity period is applied on a per interface basis. A configured inactivity period will be applied to both local and remote sessions in the same manner. When the interface has been idle for more than the configured period, the session will be terminated and will require authentication to establish a new session.
FTA_SSL.4	The Security Administrator can terminate their local CLI and remote SSH sessions by typing “exit” or “exit diag” at the prompt. To terminate local or remote session from the textual user interface, select from two options in the left-hand navigation with the arrow keys, and hit the Return/Enter key: - **Save and exit** - **Exit without saving**
FTA_TAB.1	Security Administrators can create a customized login banner that will be displayed at the following interfaces: • Local CLI • Remote CLI via SSH v2 This banner will be displayed prior to allowing Security Administrator access through those interfaces. The banner will be same for local CLI and SSH remote methods of access, and can be configured during initial configuration.
FTP_ITC.1	The TOE supports secure communication to the following IT entities: Audit server (via SFTP server). The TOE protects communications between the TOE and SFTP server using SSH v2 protocol. The TOE acts as a client. This provides a secure channel to transmit the audit events. The protocols listed are consistent with those included in the requirements in the ST.
FTP_TRP.1	The TOE supports SSH v2.0 for secure remote administration of the TOE. SSH v2.0 session is encrypted using AES encryption to protect confidentiality and uses HMACs to protect

Requirement	TSS Description
	integrity of traffic. The protocols listed are consistent with those specified in the requirement.

7. Cryptographic Key Destruction

The table below describes the key zeroization provided by the TOE and as referenced in FCS_CKM.4.

Table 17 – Zeroization Table

Keys	Purpose	Storage Location	Method of Zeroization
Diffie-Hellman Shared Secret	Provide Perfect Forward secrecy	RAM	Overwritten with zeros.
Passwords	User authentication	Only salted hash is stored in file system.	Encrypted passwords exist locally in a startup configuration file and replaced when that file is edited and saved. The passwords are stored in the file in protected form only. The interface is under 'System > Access'.
Diffie Hellman private exponent	Diffie Hellman key generation	RAM	Overwritten with zeros.
SSH Private Key	SSH server	SSD/File system	Overwritten with zeros. Destroyed by issuing a factory reset under 'Maintain'.
AES Key	Encrypt/decrypt	Keys are not stored Held in the RAM buffer in plaintext.	The key is overwritten with a pseudo-random pattern upon termination of the session or reboot of the appliance.
SSH Session Key	SSH server	SSH Session Key is stored only in RAM.	Overwritten with zeros.
RNG Seed	Output from TRNG is used to seed the DRBG	RAM	Overwritten with zeros.

8. Terms and Definitions

Table 18 provides a list of acronyms and abbreviations that appear within this document:

Table 18 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CC	Common Criteria
NDcPP	Network Device Collaborative Protection Profile
PP	Protection Profile
RSA	Rivest, Shamir, & Adleman
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification