National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

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

Report Number: **CCEVS-VR-11253-2022**

Dated: **May 2nd, 2022**

Version: **1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell

Linda Morrison

Clare Parran

Ben Schmidt

The MITRE Corporation

Common Criteria Testing Laboratory

Acumen Security, LLC

Table of Contents

List of Tables

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 3 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Corelight Sensor AP 200, AP 1001, AP 3000 and AP 5000 Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in May 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP].

The Target of Evaluation (TOE) identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP]. This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Corelight Sensor AP 200, AP 1001, AP 3000 and AP 5000 BroLin v22.1
Protection Profile	Collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020 [NDcPP]
Security Target	Corelight Sensor AP 200, AP 1001, AP 3000 and AP 5000 BroLin v22.1 Security Target, Version 2.6, April 23, 2022
Evaluation Technical Report	Evaluation Technical Report for Corelight Sensor AP 200, AP 1001, AP 3000 & AP 5000, Version 0.6, April 23, 2022
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Corelight, Inc.
Developer	Corelight, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security 2400 Research Blvd Suite #395 Rockville, MD 20850
CCEVS Validators	Paul Bicknell, Linda Morrison, Clare Parran, Ben Schmidt

Table 1: Evaluation Identifiers

3 Assumptions, Threats & Clarification of Scope

3.1 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.

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). In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device 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

ID	Assumption
	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.
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.

Table 2: Assumptions

3.2 Threats

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

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

ID	Threat
	management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
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.

Table 3: Threats

3.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP]
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or

vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PP. Any additional security related functional capabilities included in the product were not covered by this evaluation.

4 Architectural Information

The TOE is the Corelight Sensor AP 200, AP 1001, AP 3000 and AP 5000 BroLin v22.1, a network device which is composed of hardware and software that offers a scalable solution to the end users.. The Sensor parses dozens of network protocols and generates rich, actionable data streams designed for security professionals.

5 Security Policy

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:

5.1.1 Security Audit

The TOE generates audit events for all start-up and shut-down functions, and all auditable events as specified in FAU_GEN.1.2 Table 13 of the ST. 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.

5.1.2 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.

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,

Cryptographic Method	Usage
	“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]].
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.

Cryptographic Method	Usage
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.
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 262000 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-

Cryptographic Method	Usage
	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 4: TOE Cryptography Implementation

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

Table 5: Cryptographic Algorithm Certificates

5.1.3 Identification and Authentication

The TOE provides authentication services for administrative users to connect to the TOEs 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 serial console. The SSHv2 interface supports authentication using SSH keys.

5.1.4 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

5.1.5 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.

5.1.6 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.

5.1.7 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.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Corelight Sensor AP 200, AP 1001, AP 3000 & AP 5000 Security Target, Version 2.6, April 23, 2022
- Corelight Sensor AP 200, AP 1001, AP 3000 & AP 5000 Common Criteria Guidance Document, Version 0.8, April 23, 2022.

Any additional customer documentation provided with the product, or available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated.

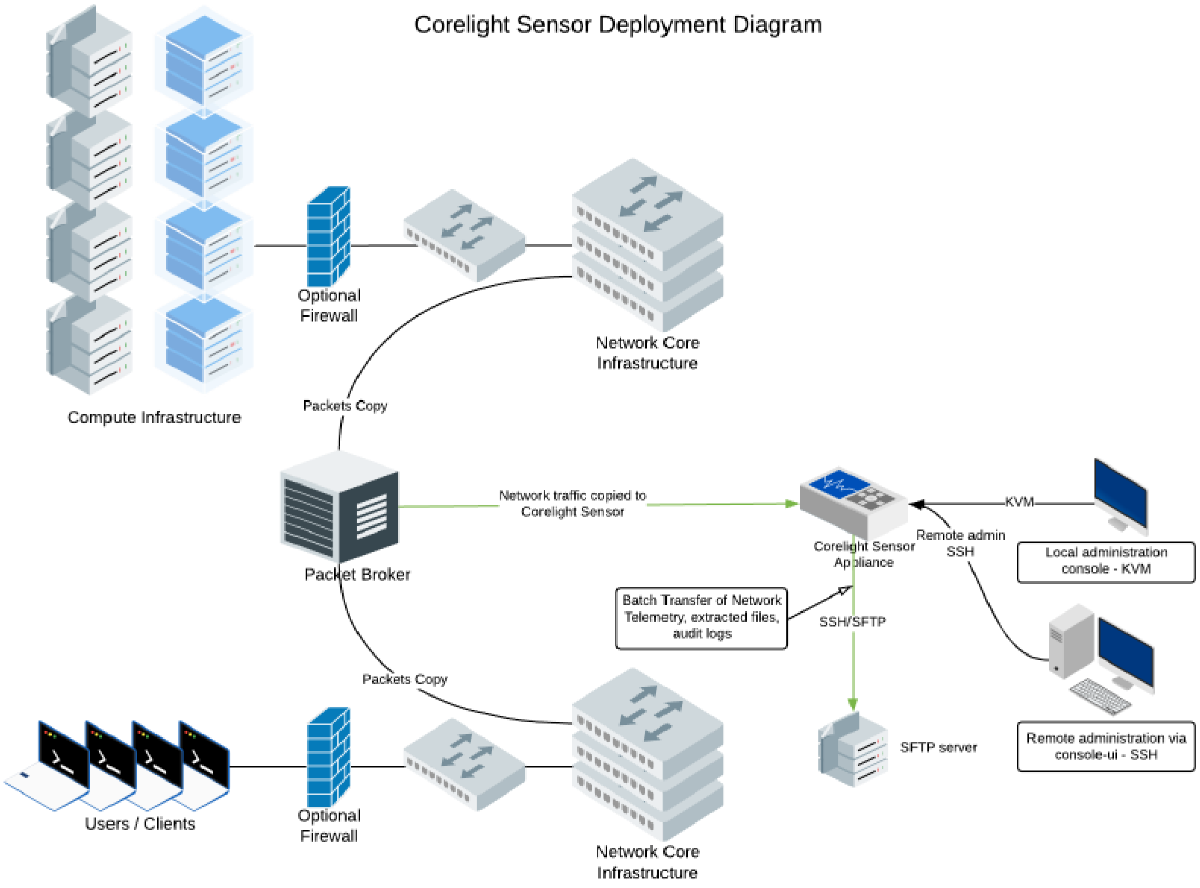
7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE in the evaluated configuration consists of the platform as stated in Section 1.3 of the Security Target. The TOE supports secure connectivity with another IT environment device as stated in Table 6.

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

Table 6: IT Components


Corelight Sensor Deployment Diagram
Compute Infrastructure
Optional Firewall
Network Core Infrastructure
Packets Copy
Packet Broker
Network traffic copied to Corelight Sensor
Corelight Sensor Appliance
KVM
Remote admin SSH
Local administration console - KVM
Batch Transfer of Network Telemetry, extracted files, audit logs
SSH/SFTP
SFTP server
Remote administration via console-ui - SSH
Packets Copy
Users / Clients
Optional Firewall
Network Core Infrastructure

7.2 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)

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Corelight Sensor AP 200, AP 1001, AP 3000 & AP 5000, which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP]. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and ETR. The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Corelight Sensor AP 200, AP 1001 & AP 3000 & AP 5000 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Corelight Sensor AP 200, AP 1001, AP 3000 & AP 5000 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP].

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the STs TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP] related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP] related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP] and recorded the results in a Test Report, summarized in the ETR and AAR.

The validator reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP], and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP], and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP], and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Corelight Sensor AP 200, AP 1001, AP 3000 & AP 5000 Common Criteria Guidance Document – v0.8, April 23, 2022,* document.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. All other functionality provided by the product needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable.

12 Security Target

Corelight Sensor AP 200, AP 1001, AP 3000 and AP 5000 BroLin v22.1 Security Target, Version 2.6 dated April 23, 2022.

13 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

Table 7: Acronyms

14 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

15 Bibliography

The Validation Team used the following documents to produce this VR:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Corelight Sensor AP 200, AP 1001, AP 3000 and AP 5000 BroLin v22.1 Security Target, Version 2.6, April 23, 2022.
6. Corelight Sensor AP 200, AP 1001, AP 3000 & AP 5000 Common Criteria Guidance Document, Version 0.8, April 23, 2022.
7. Assurance Activity Report for Corelight Sensor AP 200, AP 1001, AP 3000 and AP 5000 BroLin v22.1, Version 0.8, April 23, 2022.
8. Evaluation Technical Report for Corelight Sensor AP 200, AP 1001, AP 3000 & AP 5000, Version 0.6, April 23, 2022