National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Trellix Intrusion Prevention System Sensor and Manager Appliances version 11.1

Report Number: **CCEVS-VR-VID11417-2024**

Dated: **May 20, 2024**

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

Randy Heimann

Lisa Mitchell

Linda Morrison

Clare Parran

Lori Sarem

Chris Thorpe

Common Criteria Testing Laboratory

Yogesh Pawar

Pratheek Menon

Sagar Pujari

George Kumi

Intertek Acumen Security

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 Trellix Intrusion Prevention System Sensor and Manager Appliances Series version 11.1 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 2024. 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 (NDcPP + IPS MOD) PP-Configuration for Network Device and Intrusion Prevention Systems (IPS), Version 1.0, 18 May 2021.

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory (CCTL) 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 Protection Profile. 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 evaluation technical report 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 evaluation technical report 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 Common Evaluation Methodology (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 information technology 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 TOE: the fully qualified identifier of the product as evaluated.
- The 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	Trellix Intrusion Prevention System Sensor and Manager Appliances version 11.1
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E), PP-Module for Intrusion Protection Systems (IPS), Version 1.0 (MOD_IPS_V1.0) (NDcPP + IPS MOD)
Security Target	Trellix Intrusion Prevention System Sensor and Manager Appliances version 11.1 Security Target v1.9
Evaluation Technical Report	Evaluation Technical Report for Trellix Intrusion Prevention System Sensor and Manager Appliances version 11.1
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Trellix (Musarubra US LLC)
Developer	Trellix (Musarubra US LLC)
Common Criteria Testing Lab (CCTL)	Intertek Acumen Security 2400 Research Blvd, Suite 395 Rockville, MD 20850, USA
CCEVS Validators	Randy Heimann, Lisa Mitchell, Linda Morrison, Clare Parran, Lori Sarem, Chris Thorpe

Table 1: Evaluation Identifiers

3 Security Problem Definition

3.1 Assumptions

The assumptions included in **Error! Reference source not found.**4 are drawn directly from [NDcPP] and [MOD_IPS].

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).

ID	Assumption
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. (The paragraph that follows is for x509v3 cert-based authentication. If not relevant, remove) 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.
A.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

ID	Assumption
A.CONNECTIONS/IPS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

Table 2: Assumptions

3.2 Threats

The threats included in The assumptions included in Error! Reference source not found.4 are drawn directly from [NDcPP] and [MOD_IPS].3 are drawn directly from the [NDcPP] and [MOD_IPS].

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

ID	Threat
	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

ID	Threat
	traffic and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.NETWORK_DISCLOSURE/IPS	Sensitive information on a protected network might be disclosed resulting from ingress-or egress-based actions.
T.NETWORK_ACCESS/IPS	Unauthorized access may be achieved to services on a protected network from outside that network, or alternately services outside a protected network from inside the protected network. If malicious external devices are able to communicate with devices on the protected network via a backdoor then those devices may be susceptible to the unauthorized disclosure of information.
T.NETWORK_MISUSE/IPS	Access to services made available by a protected network might be used counter to Operational Environment policies. Devices located outside the protected network may attempt to conduct inappropriate activities while communicating with allowed public services. E.g. manipulation of resident tools, SQL injection, phishing, forced resets, malicious zip files, disguised executables, privilege escalation tools, and botnets.
T.NETWORK_DOS/IPS	Attacks against services inside a protected network, or indirectly by virtue of access to malicious agents from within a protected network, might lead to denial of services otherwise available within a protected network. Resource exhaustion may occur in the event of co-ordinate service request flooding from a small number of sources.

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 (NDcPP + IPS MOD) PP-Configuration for Network Device and Intrusion Prevention Systems (IPS), Version 1.0.
- 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 PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

4 Architectural Information

The TOE is comprised of the Trellix Intrusion Prevention System (IPS) software running on one Trellix Intrusion Prevention System Manager Appliance and one or more Trellix Intrusion Prevention System Sensor (Sensor).

The Trellix Intrusion Prevention System (IPS) Sensor performs stateful inspection on a per-packet basis to discover and prevent intrusions, misuse, denial of service (DoS) attacks, and distributed denial of service (DDoS) attacks. Trellix Intrusion Prevention System (IPS) is available in multiple Sensor appliances providing different bandwidth and deployment strategies. These models are listed in Table 7.

Trellix IPS Manager (IPS Manager) is used to manage, push configuration data and policies to the Sensors. Communication between Manager and Sensors uses secure channels that protect the traffic from disclosure and modification. Authorized administrators may access the Manager via a GUI (over HTTPS) or a CLI (via SSH or a local connection). Sensors may be accessed via CLI (via SSH or a local connection) for initial setup. Once initial setup is complete, all management occurs via the Manager.

The Sensor's presence on the network is transparent. The Sensor is protected from the monitored networks as the system is configured to not accept any management requests or input from the monitored networks.

4.1 IPS Manager Architecture

The Manager Appliance is the management console of the Trellix Intrusion Prevention System (IPS). The Manager Appliance is a 1-U rack dense chassis with multi-core Intel XEON Series Processor. The Manager Appliance runs on a pre-installed, hardened MLOS operating system and comes pre-loaded with the IPS Manager software. Manager is used, to manage, push configuration data and policies to the Sensors.

4.2 Sensor Architecture

The primary function of the Sensor (also referred to as the Collector Component) is to analyze traffic on selected network segments and respond when an attack is detected. The Sensor examines the header and data portion of every network packet; scanning for patterns and behavior in the network traffic that indicates malicious activity.

The Sensor can operate in three modes:

Inline: The product is installed as an appliance within the network that applicable traffic must flow through.

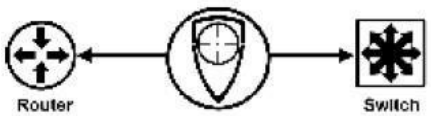

Figure 1: Sensor in "Inline" mode

Tap: The network traffic flows between the clients and servers, and the data is copied by the tap to the Sensor, which is essentially invisible to the other network entities. Note that the TOE cannot inject response packets back through an external tap, so Sensors offer response ports through which a response packet (such as a TCP reset) can be injected to close a malicious connection.

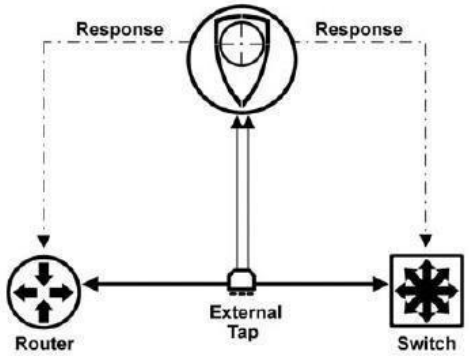

Figure 2: Sensor in "Tap" mode

Span: The traffic is spanned off either the server side or the client side of a router or switch, copying both the incoming and outgoing traffic from any one of the ports. This requires a special network device that has a span port capability. Note that SPAN mode is also a "sniffing" mode, which—unlike inline mode—does not enable the TOE to prevent attacks from reaching their targets. However, while the TOE can issue response packets via the Sensor's response ports, some switches allow response packets to be injected by an IPS back through the SPAN port.

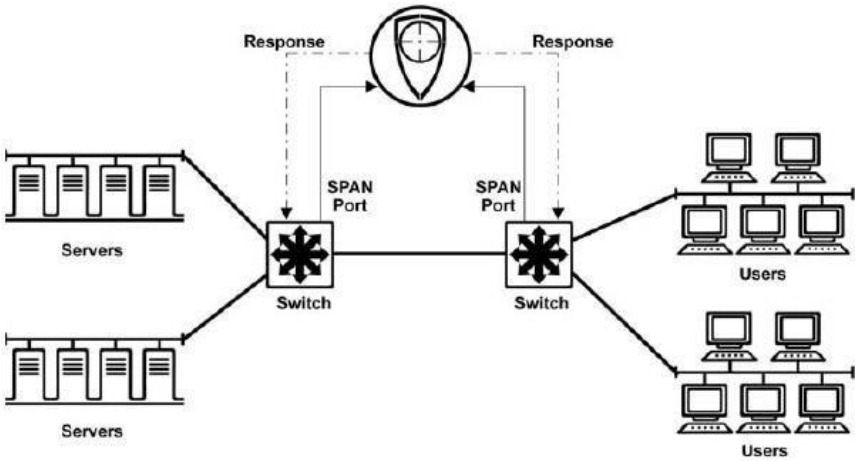

Figure 3: Sensor in "Span" mode

A single multi-port Sensor can monitor many network segments in any combination of operating modes: monitoring or deployment mode for the Sensor; SPAN mode, TAP mode,

or INLINE mode.

The IPS's Virtual IDS (VIDS) feature enables users to further segment a port on a Sensor into many "Virtual Sensors". A VIDS can be dedicated to a specific network port with monitoring rules appropriate for that segment. These rules may be different than the rules used to monitor other segments.

Alternately, if a monitored network segment includes the use of Virtual LANs (VLANs) or Classless Inter- Domain Routing (CIDR), one or more VIDS can be directed at monitoring them, with VIDS each configured with distinct monitoring rules. Note that VIDS are not particularly security relevant in and of themselves, but rather serve to organize and distinguish monitoring rules.

5 Security Policy

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices, hereafter referred to as NDcPP v2.2e or NDcPP.

5.1 Security Audit

The TOE generates audit records related to TOE operation and administration. These audit records are stored on the IPS Manager (and stored in a local database) and are also forwarded to an external audit server. The database stores 50,000 audit records. When the database reaches capacity, the oldest audit records are overwritten.

The Sensor generates audit records and forwards the audit records to the IPS Manager, the Sensor caches audit records in a local file. The audit file can be uploaded to Manager (or any other SCP server using the "auditlogupoload" CLI command). If the file reaches capacity, new events are dropped.

Only authenticated users can view audit records.

5.2 Communication

The TOE is a Distributed TOE. It is a combination of:

- One or more IPS Sensor appliances with their software [Sensor]
- One IPS Manager appliance with its software [Manager]

Each component is delivered with the TOE software installed. A security Administrator can enable or disable communications between any pair of TOE components. The communication between the TOE components is secured via TLS with Mutual Authentication as per the secure channel requirements in FPT_ITT.1.

5.3 Cryptographic Support

The TOE uses symmetric key cryptography to secure communication between the Sensors and the Manager for the following functionality:

- Exchange of configuration information (including IPS policies)
- Time/date synchronization from the Manager to Sensors
- Transfer of IPS data to the Manager
- Transfer of audit records to the Manager
- Distribution of TOE updates to Sensors

Connections between the Manager and Sensors are secured using TLS.
Connections between the Manager and the Audit Server (for audit record upload) are secured using TLS.
Connections between the Sensor and the SCP Server is secured using SSH.

Sessions between the Management Workstation and the TOE are secured using SSH or HTTPS. Administrators can connect to the Manager via HTTPS or SSH. Administrators can connect to the Sensor via SSH.

Local console connections between the Console Workstation and the TOE are physically secured.

For all cryptographic operations performed by the TOE, the cryptographic algorithms have been validated as identified in the table below.

The following table presents a listing of each IPS Manager algorithm certificates and the associated OE. [NSM-MAPL-NG (XEON SILVER 4210) and NSM-MAPL -NG (XEON SILVER 4114)]

Functions	Algorithms	Mode Supported	IPS CAVP Certs.	Name	OE
Data Encryption	AES-GCM	GCM (128, 256)	A4660	Network Security Manager Bouncy Castle	MLOS 3 on Intel Xeon Scalable Processors (Silver 4114, Skylake) MLOS 3 on Intel Xeon Scalable Processors (Silver 4210, Cascade Lake)
			A2624	Trellix OpenSSL FIPS Object Module	
Hash	SHS (Cryptographic hashing)	SHA-1, SHA-256, SHA-384, SHA-512	A4660	Network Security Manager Bouncy Castle	
			A2624	Trellix OpenSSL FIPS Object Module	
Random Number Generation	Counter DRBG	CTR_DRBG (AES-256)	A4660	Network Security Manager Bouncy Castle	
			A2624	Trellix OpenSSL FIPS Object Module	
Key Generation	RSA KeyGen (FIPS186-4)	Mode: n(2048), n = 2048 SHA(256)	A4660	Network Security Manager Bouncy Castle	
			A2624	Trellix OpenSSL FIPS Object Module	
	ECDSA KeyGen (FIPS186-4) ECDSA KeyVer (FIPS186-4)	P-256, P-384	A4660	Network Security Manager Bouncy Castle	
			A2624	Trellix OpenSSL FIPS Object Module	

Key Establishment	KAS ECC Sp800-56Ar3 (Key Pair Generation, Partial Validation)	P-256, P-384	A4660	Network Security Manager Bouncy Castle	
Digital Signature services	ECDSA SigGen (FIPS186-4) ECDSA SigVer (FIPS186-4)	P-256	A4660	Network Security Manager Bouncy Castle	
			A2624	Trellix OpenSSL FIPS Object Module	
	RSA SigGen (FIPS186-4) RSA SigVer (FIPS186-4)	Mode: n(2048), n = 2048 SHA(256)	A4660	Network Security Manager Bouncy Castle	
			A2624	Trellix OpenSSL FIPS Object Module	
Keyed Hash	HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	Mode: SHA-256, SHA-384, SHA-512	A4660	Network Security Manager Bouncy Castle	
			A2624	Trellix OpenSSL FIPS Object Module	

Table 4: CAVP Manager Certificate References

The following table presents a listing of each IPS Sensor algorithm certificates and the associated OEs. [NS9500, NS7600, NS7500, NS3600, NS3200]

Functions	Algorithms	Mode Supported	IPS CAVP Certs.	Name	OE
Data Encryption	AES-GCM	GCM (128, 256)	A3350	Trellix IPS Sensor Crypto Lib	Intel(R) Atom(R)C Series

Hash	SHS (Cryptographic hashing)	SHA-1, SHA-256, SHA-384, SHA-512	A3350	Trellix IPS Sensor Crypto Lib	(C2538, Rangeley) Intel(R) Xeon(R) (D-1734NT, Ice Lake) Intel(R) Xeon(R) Scalable Processors (GOLD 5218N, Cascade Lake) Intel(R) Xeon(R) Scalable Processors (GOLD 6230, Cascade Lake) Intel(R) Xeon(R) Silver (4416+, Sapphire Rapids)
		SHA-256, SHA-384	A3353	Trellix IPS Sensor XySSL Lib	
Random Number Generator	Counter DRBG	CTR_DRBG (AES-256)	A3350	Trellix IPS Sensor Crypto Lib	
Key Generation	RSA KeyGen (FIPS186-4)	Mode: n(2048), n = 2048 SHA(256)	A3350	Trellix IPS Sensor Crypto Lib	
	ECDSA KeyGen (FIPS186-4) ECDSA KeyVer (FIPS186-4)	P-256, P-384	A3350	Trellix IPS Sensor Crypto Lib	
Key Establishment	KAS ECC SSC Sp800-56Ar3 (Domain Parameter Generation)	P-256, P-384	A3350	Trellix IPS Sensor Crypto Lib	
Digital Signature services	ECDSA SigGen (FIPS186-4) ECDSA SigVer (FIPS186-4)	P-256	A3350	Trellix IPS Sensor Crypto Lib	
	RSA SigGen (FIPS186-4) RSA SigVer (FIPS186-4)	Mode: n(2048), n = 2048 SHA(256)	A3350	Trellix IPS Sensor Crypto Lib	

	RSA SigVer (FIPS186-4)		A3353	Trellix IPS Sensor XySSL Lib	
Keyed Hash	HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	Mode: SHA-256, SHA-384, SHA-512	A3350	Trellix IPS Sensor Crypto Lib	

Table 5: CAVP Sensor Certificate References

5.4 Identification and Authentication

Administrators connecting to the TOE are required to enter an IPS administrator username and password to authenticate the administrative connection prior to access being granted.

The Manager and Sensors authenticate to one another through a shared secret that is configured during the initial installation and setup process of the TOE. Although in the evaluated configuration, the Manager supports use of a default self-signed certificate for trust establishment with the sensor, such a channel is out of scope for this evaluation. The sensor-Manager channel must be established using CA-signed certificates.

5.5 Security Management

An administrative CLI can be accessed via the Console port or SSH connection, and an administrative GUI can be accessed via HTTPS. These interfaces are used for administration of the TOE, including audit log configuration, upgrade of firmware and signatures, administration of users, configuration of SSH and TLS connections.

Only administrators authenticated to the “Admin” role are considered to be authorized administrators.

5.6 Protection of the TSF

The presence of the Sensors' components on the network is transparent (other than network packets sent as reactions to be configured IPS conditions). The Sensors are protected from the monitored networks as the system is configured to not accept any management requests or input via the monitored interfaces.

The TOE users must authenticate to the TOE before any administrative operations can be performed on the system.

The TOE ensures consistent timestamps are used by synchronizing time information on the Sensors with the Manager, so that all parts of the IPS system share the same relative time information.

Synchronization occurs over a secure communications channel. Time on the Manager may be configured by an administrator.

The administrator can query the currently installed versions of software on the Sensor using the "show" command, which returns details about the software and hardware version. A trusted update of the TOE software can be performed from the Manager UI, which is then pushed out to the Sensors.

A suite of self-tests is performed by the TOE at power on, and conditional self-tests are performed continuously.

5.7 TOE Access

The TOE monitors local and remote administrative sessions for inactivity and terminates the session when a threshold time is reached. An advisory notice is displayed at the start of each session.

5.8 Trusted Path/Channels

The TSF provides the following trusted communication channels:

- TLS for an audit server
- TLS for communication between Manager and Sensors
- SSH for communication with an SCP Server for updates

The TOE implements TLS/HTTPS and SSH for protection of communications between itself and the administrators.

5.9 Intrusion Prevention

The IPS Sensors provides the following IPS-based Functionality:

- Anomaly-based traffic patterns definition, including the specification of frequency and specific network protocol fields
- IP blocking based on known-good and known-bad list of rules, IP addresses (source, destination), ACLs, and alert filters
- IP-based network traffic analysis
- Signature-based traffic analysis

6 Documentation

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

- Trellix Intrusion Prevention System Sensor and Manager Appliances version 11.1 Security Target v1.9 [ST]
- Trellix Intrusion Prevention System 11.1.x Installation Guide
- Trellix Intrusion Prevention System 11.1.x Product Guide
- Trellix Intrusion Prevention System Manager Appliance Product Guide
- Trellix Intrusion Prevention System NS-series Sensor Product Guide
- Trellix Intrusion Prevention System 11.1 (FIPS and CC Certification Guide)

7 TOE Evaluated Configuration

7.1 TOE Environment

The following environmental components are required to operate the TOE in the evaluated configuration:

Components	Description
Local Management Console	Any computer using terminal emulation software to access the console interface of CLI of the Manager or Sensor.
Remote Management Workstation	Any computer that provides a supported browser may be used to access the Manager via the GUI or using SSH client software to access the CLI.
External IT systems	IT systems exchanging network traffic generate the packets that are analyzed by the TOE.
Update Server	An SCP server used for updating the Sensor software securely over a remoteconnection.
Syslog Server	A syslog server that constantly receives audit logs from the Manager component over a secure TLSv1.2 channel.

Table 6: Required Environmental Components

This section provides an overview of the TOE architecture, including physical boundaries, security functions, and relevant TOE documentation and references.

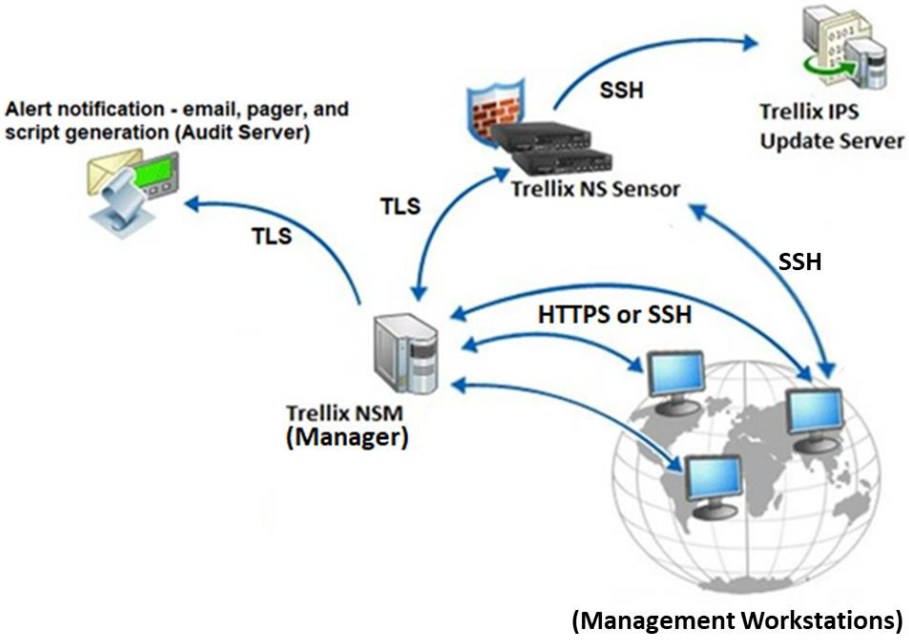

Figure 1– Representative TOE Deployment

7.2 Physical Boundaries:

The TOE is a software and hardware Distributed TOE. It is a combination of:

- One or more IPS Sensor appliances with their software [Sensor]
- One IPS Manager appliance with its software [Manager]

Each component is delivered with the TOE software installed. The following table lists all the instances of the Sensors that are included in the evaluation. All listed Sensor appliances offer the same security functionality but vary in the type and number of processors, amount of memory, and storage.

Model	CPUs	Memory (Size and Qty)	Storage	Micro-architecture
Trellix Intrusion Prevention System Sensor Appliances				
IPS-NS9500	2 x XEON GOLD 6230	12 x 16GB	2 x 240GB SSD	Cascade Lake
IPS-NS7600	1 x XEON SILVER 4416+	6 x 32GB	1 x 400GB SSD	Sapphire Rapids
IPS-NS7500	1 x XEON GOLD 5218N	6 x 16GB	1 x 240GB SSD	Cascade Lake
IPS-NS3600	1 x XEON D-1734NT	2 x 32GB	1 x 400GB SSD	Ice Lake
IPS-NS3200	1 x ATOM C2538	2 x 4GB	1 x 30GB SSD	Rangeley
Trellix Intrusion Prevention System Manager Appliance				
NSM-MAPL-NG	1 x XEON SILVER 4210	4 x 16GB	2 x 2TB HDD	Cascade Lake
NSM-MAPL -NG	1 x XEON SILVER 4114	4 x 16GB	2 x 2TB HDD	Skylake

Table 7: TOE Appliance Series and Models

In the evaluated configuration, the devices are placed in Network Device collaborative Protection Profile (NDcPP) mode by configuration according to the Administrative Guidance.

7.3 Excluded Functionality

The following product functionality is not included in the CC evaluation:

- IPS can be configured to maintain accurate time via NTP. NTP must be disabled in the evaluated configuration.
- The Manager can manage Sensors that are not FIPS compliant. All Sensors must be in FIPS mode in the evaluated configuration.
- The Manager can manage Sensors that are using self-signed X.509 certificates. In the evaluated configurations, all Sensors must use CA-signed certificates.
- IPS can be configured to authenticate users via an LDAP server (rather than relying solely on internal user accounts). This optional functionality was not evaluated.

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 Trellix Intrusion Prevention System Sensor and Manager Appliances, which is not publicly available. The Assurance Activities Report 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 (NDcPP + IPS MOD) PP-Configuration for Network Device and Intrusion Prevention Systems (IPS). The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

All testing was carried out at the Acumen Security offices located at 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from 27th May 2023 to 20th March 2024.

The TOE was in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. At the start of each day, the test bed was verified to ensure that it was not compromised. All evaluation documentation was always kept in a secure repository.

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 the 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 Trellix Intrusion Prevention System Sensor and Manager Appliances to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDcPP + IPS MOD.

9.1 Evaluation of Security Target

The Evaluation team applied to 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 Trellix Intrusion Prevention System Sensor and Manager Appliances 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 (NDcPP + IPS MOD) PP-Configuration for Network Device and Intrusion Prevention Systems (IPS).

The Validation team 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 Security Target's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the (NDcPP + IPS MOD) PP-Configuration for Network Device and Intrusion Prevention Systems (IPS) related to the examination of the information contained in the TOE Summary Specification.

The Validation team 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 (NDcPP + IPS MOD) PP-Configuration for Network Device and Intrusion Prevention Systems (IPS) related to the examination of the information contained in the operational guidance documents.

The Validation team 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 Validation team 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 (NDcPP + IPS MOD) PP-Configuration for Network Device and Intrusion Prevention Systems (IPS) and recorded the results in a Test Report, summarized in the ETR and Assurance Activities Report.

The Validattion team 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 (NDcPP + IPS MOD) PP-Configuration for Network Device and Intrusion Prevention Systems (IPS), 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 Validation team 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 (NDcPP + IPS MOD) PP-Configuration for Network Device and Intrusion Prevention Systems (IPS), 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 (NDcPP + IPS MOD) PP-Configuration for Network Device and Intrusion Prevention Systems (IPS), 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 following guides:

- Trellix Intrusion Prevention System 11.1.x Installation Guide
- Trellix Intrusion Prevention System 11.1.x Product Guide
- Trellix Intrusion Prevention System Manager Appliance Product Guide
- Trellix Intrusion Prevention System NS-series Sensor Product Guide
- Trellix Intrusion Prevention System 11.1 (FIPS and CC Certification Guide)

No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Section 7.3 of this document and section 1.5 of the ST defines product functionality not included in the scope of the evaluation. 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

Trellix Intrusion Prevention System Sensor and Manager Appliances version 11.1 Security Target v1.9

13 Glossary

The following definitions are used throughout this document:

Term	Definition
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.

Table 8: Glossary

14 Bibliography

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

- Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
- Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
- Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
- Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
- Trellix Intrusion Prevention System Sensor and Manager Appliances version 11.1 Security Target v1.9
- Trellix Intrusion Prevention System 11.1.x Installation Guide
- Trellix Intrusion Prevention System 11.1.x Product Guide
- Trellix Intrusion Prevention System Manager Appliance Product Guide
- Trellix Intrusion Prevention System NS-series Sensor Product Guide
- Trellix Intrusion Prevention System 11.1 (FIPS and CC Certification Guide)
- Evaluation Technical Report for Trellix Intrusion Prevention System Sensor and Manager Appliances version 11.1 v1.3
- Assurance Activity Report for Trellix Intrusion Prevention System Sensor and Manager Appliances version 11.1 v1.4