National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Forcepoint Network Security Platform 7.3

Report Number: CCEVS-VR-VID11677-2026
Dated: September 2, 2026
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

Jenn Dotson
Sheldon Durrant
Randy Heimann
Lisa Mitchell
Jaemond Reyes
Lori Sarem

The MITRE Corporation

Common Criteria Testing Laboratory

Brandan deGuzman
Julia Miller

Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of Forcepoint Network Security Platform 7.3 solution provided by Forcepoint LLC. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in September 2026. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the:

- *PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways*, Version 2.0, 25 April 2024 consisting of the following components:
    - Base-PP: *Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 (NDcPP30e)
    - PP-Module: *PP-Module for Stateful Traffic Filter Firewalls*, Version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e)
    - PP-Module: *PP-Module for VPN Gateways*, Version 1.3, 16 August 2023 (VPNGW13)

The TOE is the Forcepoint Network Security Platform 7.3. The TOE identified in this VR has been evaluated at a NIAP approved 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). 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 (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, 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.

The technical information included in this report was obtained from the *Forcepoint Network Security Platform 7.3 Security Target*, version 0.7, September 1, 2026 and analysis performed by the Validation team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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 Validated Products 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 to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Forcepoint Network Security Platform 7.3
Protection Profile	*PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways*, Version 2.0, 25 April 2024 consisting of the following components: • Base-PP: *Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 (NDcPP30e) • PP-Module: *PP-Module for Stateful Traffic Filter Firewalls*, Version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e) • PP-Module: *PP-Module for VPN Gateways*, Version 1.3, 16 August 2023 (VPNGW13)
ST	*Forcepoint Network Security Platform 7.3 Security Target*, version 0.7, September 1, 2026
Evaluation Technical Report	*Evaluation Technical Report for Forcepoint Network Security Platform 7.3*, version 0.3, September 1, 2026
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Forcepoint LLC
Developer	Forcepoint LLC

Item	Identifier
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Jenn Dotson, Sheldon Durrant, Randy Heimann, Lisa Mitchell, Jaemond Reyes, Lori Sarem

3 Architectural Information

Note: The following architectural description is based on the description presented in the ST.

The Forcepoint Network Security Platform (FNSP) is a stateful packet filtering firewall and VPN gateway. Being a stateful packet filtering firewall, the FNSP filters network traffic optimized through the use of stateful packet inspection. Being a VPN gateway, the FNSP provides IPsec VPN functionality to secure network data exchanged with peer gateways and VPN clients. The FNSP is intended to be used as a network perimeter security gateway that provides a controlled connection. The FNSP is centrally managed and generates audit records for security critical events.

3.1 TOE Description

The FNSP is a stateful packet filtering firewall and VPN gateway. The FNSP system is composed of the Security Engine (a physical or virtual appliance) and the Virtual Security Management Center (SMC). The Security Engine controls connectivity and information flow between internal and external connected networks. The Virtual SMC Appliance provides administrative functionality supporting the configuration and operation of Security Engines. Throughout the remainder of this document, references to the Security Engine are meant to reference the TOE's firewall engine, while references to the FNSP are meant to refer to the TOE as a whole.

The Security Engine controls connectivity and information flow between internal and external connected networks. The Security Engine also provides a means to keep the internal host's IP-address private from external users. The Security Engine is intended to be used as a network perimeter security gateway that provides a controlled connection.

The Security Engine provides VPN gateway capabilities, allowing the Engine to use IKE/IPsec to protect traffic exchanged with remote peer gateways (for a site-to-site VPN configuration) and with VPN clients.

The FNSP is assumed to be installed and operated within a physically protected environment, administered by trusted and trained administrators over a trusted and separate management network. Multiple installations of the Security Engine may be used in combination to provide a company with an overall network topology.

The Security Engine contains a hardened Linux operating system (with a 6.6 kernel) executing on a single or multi-processor Forcepoint hardware platform.

The Virtual SMC Appliance (or SMC) contains the Management Server and Log Server. Like the Security Engine, the SMC contains a hardened Linux-based operating system (which uses a 5.14 kernel) to support the management capabilities and allow for the operation and configuration of firewall engines.

3.2 TOE Evaluated Platforms

Details regarding the evaluated configuration is provided in Section 8 below.

3.3 TOE Architecture

The FNSP system is a distributed TOE[1] consisting of the SMC Appliance and one or more Security Engines under the control of the SMC. These Security Engines provide firewall functionality, VPN gateway functionality, and communicate securely with the SMC using its embedded cryptographic library for all cryptographic functionality. The Virtual SMC Appliance provides Management Server, Log Server functionality, and securely managed Engines. As the SMC utilizes both Java and C, the SMC relies upon both Java and native cryptographic libraries for cryptographic functionality. In the evaluated configuration, the Virtual SMC Appliance communicates with Security Engines through a TLS-protected trusted channel.

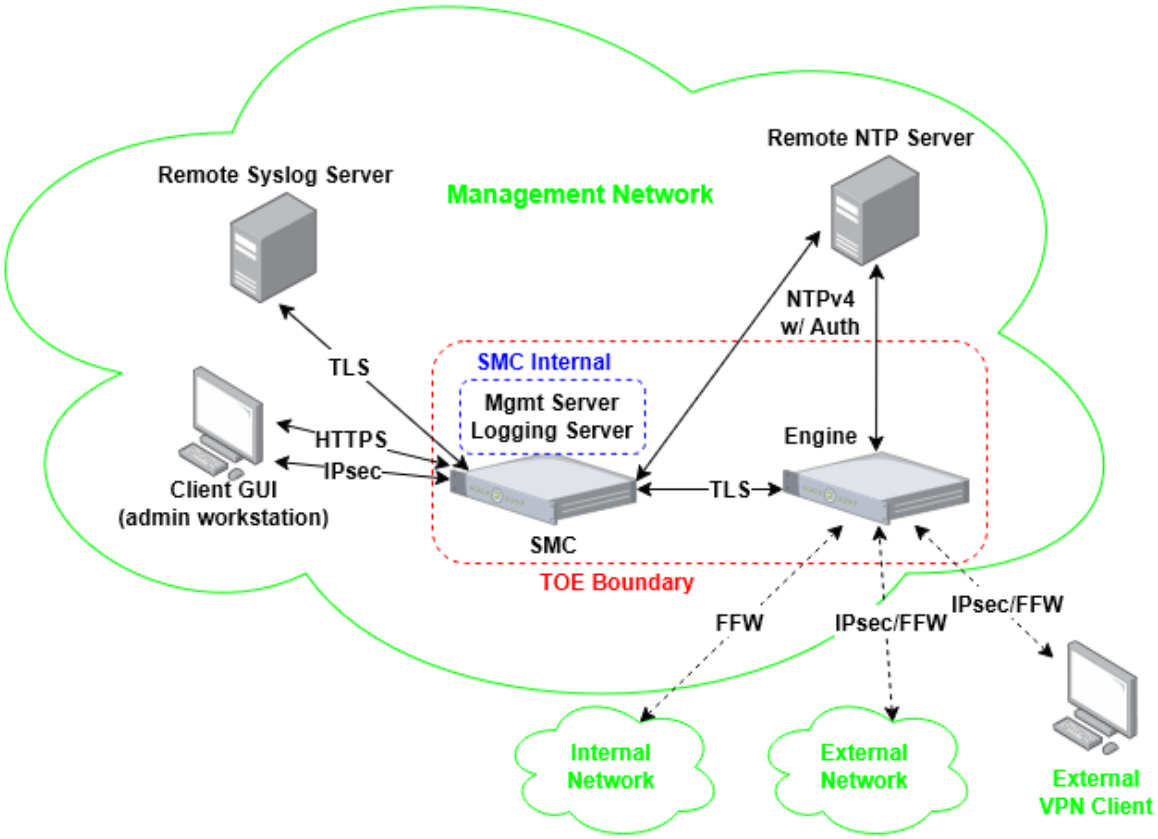

Figure 1 TOE Components, Communication Paths and IT Environment.

The Security Engines are responsible for performing all firewall packet handling, analysis and filtering that is provided by the FNSP system, VPN gateway functionality (IKE/IPsec), as well as securely transmitting audit logs to the SMC's Log server.

The Management Server portion of the Virtual SMC Appliance provides most of the administrative capabilities in the FNSP system through a Management Client GUI interface. The Virtual SMC Appliance provides a very limited console interface that allows administrators to verify and update the virtual SMC's software, to manually set the time, and configure the console timeout.

[1] The TOE is a distributed TOE consistent with Use Case 3 as defined in the NDcPP30e.

The Security Engines do not have local administrative interfaces and can only be configured through the Virtual SMC Appliance. The Management Server is responsible for securely transferring the administrator defined configuration to Security Engines as the administrator makes configuration changes (these configuration changes are known as a 'security policy').

The Log Server in the Virtual SMC Appliance is responsible for securely collecting audit events from the Security Engine components of the TOE and securely re-transmitting the audit data to an external syslog server. The Management Server component directly transmits its audit data to an external syslog server.

The administrator interfaces with the TOE through a Management Client GUI (either the Forcepoint standalone Java Client installed from a Forcepoint provided installation package, through an HTTPS/TLS HTML5 web browser application, or either of those two methods but tunneled through IPsec). The Client GUI (along with the administrator's workstation on which the Client GUI runs), is part of the TOE's Operational Environment, and the Client GUI interacts with the Management Server which performs all identification, authentication, and permission enforcement. The Client GUI can also interact with the Log Server, allowing the administrator to query the Security Engine audit records that the Log Server has aggregated.

The following communication pathways are represented in Figure 1 TOE Components, Communication Paths and IT Environment.

- **Management Server to Log Server communications** use the internal loopback interface within the Virtual SMC Appliance. These communications involve the configuration of the Log Server by the Management Server.
- **Management and Log Server to External Syslog Server communications** use TLS to protect the audit data transmitted from the Management and Log Server to the external syslog server.
- **Management Server to External NTP Server communications** use SHA1 as the message digest algorithms for authentication with an NTP time source.
- **Security Engine to External NTP server communications** use SHA1 as the message digest algorithms for authentication with an NTP time source. Time on the Security Engine is updated by the SMC Management Server, or alternatively from an administrator configured NTP server.
- **Security Engine to Log Server communications** use the TLS-based trusted channel to protect the audit data transmitted from the Security Engine to the Log Server.
- **Security Engine to/from Management Server communications** use the TLS-based trusted channel to protect the configuration information exchanged between the Management Server and the Security Engine. Either party in this communication pathway can initiate communications. Typically, the Management Server initiates configuration changes by sending updated security policies to the Security Engine. However, the Security Engine also polls for configuration changes on a regular basis.

- **Client GUI to Management and Log Server communications** uses HTTP/TLS or IPsec[2] to protect the communication over which remote administration actions occur.
- The **Security Engines** control connectivity and information flow between **internal and external connected networks** that they are protecting.
- The **Security Engines** encrypt information flow between the Engine and remote VPN peers (gateways and clients) with IKEv2/IPsec.

The cryptographic operations occurring as part of the communication on the Virtual SMC Appliance involving the Management Server and Log Server are performed using the FNSP SMC FIPS Java API 2.0.1 (library). This provider provides the encryption, decryption, signing and hashing functions necessary to support the Virtual SMC Appliance use of the trusted channel mechanism and the trusted path mechanism. The Virtual SMC Appliance also uses the **Error! Reference source not found.** to perform signature verification supporting the TOE trusted update mechanism. The Virtual SMC Appliance's NTP daemon uses cryptography from the FNSP SMC FIPS Cryptographic Module for NTP 3.101.

The Security Engine utilizes its FNSP Security Engine FIPS Library 3.1.2 (based upon OpenSSL 3.1.2 FIPS) to provide the encryption, decryption, signing and hashing functions necessary to support the Security Engine's trusted update mechanism and its TLS, ITT secure channel. The Security Engine also uses its FNSP Security Engine FIPS Cryptographic Module 2.0 (based upon SafeZone FIPS Cryptographic Module 2.0) for IKE and uses its FNSP Engine Cryptographic Kernel Module 3.0 for IPsec.

3.4 Physical Boundaries

The TOE is composed of one or more Security Engine (physical or virtual) appliances and the Virtual SMC Appliance. Each of these has network connections to its environment, both to allow TLS protected management communications between the SMC and its Engines, and network connections allowing the Security Engines to monitor and filter network traffic. The Virtual SMC Appliance provides all management functionality, while the Security Engines provide all firewall packet filtering.

The TOE is accessed and managed from the Forcepoint SMC Client which can be used in a web browser or installed on a PC (admin workstation) in the environment, where the PC is expected to have a network path to the Virtual SMC Appliance.

The TOE can be configured to forward its audit records to an external syslog server in the environment. All audit records, sent to the external syslog server, are sent from the Virtual SMC Appliance. The Security Engine does not send audit data directly to an external syslog server. Instead, a Security Engine passes all its audit data to the Log Server on the Virtual SMC Appliance, which can (if configured) forward the data to the external syslog server.

The TOE's engines support IKE/IPsec connections with other engines as well as with external gateways. An administrator can manually set the TOE's internal clock through the SMC console or via synchronization with an external NTP server. The Virtual SMC Appliance then configures

[2] Note: IPsec protection of Client GUI traffic requires a VPN client on the admin workstation and configuration of a Security Engine to terminate the tunnel

the Security Engine's time to be in sync with itself. The Security Engine synchronizes with the SMC but can alternatively be configured separately to receive time from an NTP server directly.

The Security Engine utilizes its FNSP Security Engine FIPS Library 3.1.2 (based upon OpenSSL 3.1.2 FIPS) to verify trusted engine software updates and uses its FNSP Security Engine Cryptographic Kernel Module 3.0 to support IPsec connections. The Virtual SMC Appliance uses its FNSP SMC FIPS Java API 2.0.1 to provide TLS (which protects the trusted channel mechanism and the trusted path mechanism) and uses its FNSP SMC FIPS Library 3.0.7 (based on Oracle Linux 9 OpenSSL FIPS Provider 3.0.7-b27cdeb3ba51be46) to verify SMC updates.

4 Security Policy

This section summarizes the security functionality of the TOE:

1. Security audit
2. Communication
3. Cryptographic support
4. User data protection
5. Firewall
6. Identification and authentication
7. Security management
8. Packet filtering
9. Protection of the TSF
10. TOE access
11. Trusted path/channels

4.1 Security audit

The TOE generates audit events for numerous activities including policy enforcement, system management and authentication. A syslog server in the environment is relied on to store audit records generated by the TOE. The TOE generates a complete audit record including the IP address of the TOE, the event details, and the time the event occurred. The time stamp is provided by the TOE's Linux-based operating system in conjunction with the appliance hardware. When the syslog server writes the audit record to the audit trail, it applies its own time stamp, placing the entire TOE-generated syslog protocol message MSG contents into an encapsulating syslog record.

4.2 Communication

The TOE is a distributed solution consisting of the SMC and Security Engines. The SMC can manage one or more Security Engines. The TOE uses a registration process to join Engines to an SMC.

4.3 Cryptographic support

Because the TOE consists of distributed components, each physical component of the TOE must be considered when discussing the TOE cryptographic support. Both components (the SMC and its Engines) of the TOE utilize cryptography to verify trusted updates and for TLS protected management communications between the SMC and its Engines. The Engine also uses cryptography for Engine support of IPsec connections. The SMC uses cryptography to support its use of the TLS protocol to protect administrative HTTPS connections and to protect network communications with external IT entities. Additionally, the TOE provides the ability to synchronize its time with an NTP server using NTPv4. The time data is protected by a SHA1 message digest.

4.4 User data protection

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. New packet data is used to overwrite any previous data in a buffer and any additional buffer space is padded with zeros before the packet is forwarded. Residual data is never transmitted from the TOE.

4.5 Firewall

The TOE provides an information flow control mechanism using a rule base that comprises a set of security policy rules, i.e., the firewall security policy. The Security Engine enforces the firewall security policy on all traffic that passes through the engine, via its internal or external network Ethernet interfaces.

4.6 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, except for reading the login banner, and performing firewall packet filtering operations. The TOE authenticates administrative users. For an administrative user to access the TOE, a user account including a username and password must be created for the user.

The TOE supports X509v3 certificate validation during negotiation of TLS protected syslog and for secure communications between distributed TOE components (SMC and Security Engine). Certificates are validated as part of the authentication process when they are presented to the TOE and when they are loaded into the TOE.

4.7 Security management

Security management commands are limited to authorized users (i.e., administrators) and available only after they have provided acceptable user identification and authentication data to the TOE. Administrators access the TOE remotely using a TLS protected communication channel between the Management Server and the Client GUI (which runs on a workstation in the IT environment or in a web browser). Administrators can also access the TOE via a local console which provides limited functionality.

4.8 Packet filtering

Please see Section 4.5 Firewall for a description of the TOE's packet filtering mechanism.

4.9 Protection of the TSF

The TOE provides a variety of means of protecting itself. The TOE protects communications between the SMC and Security Engines using TLS as a trusted channel. Mutual authentication using client-side x.509v3 certificates is supported by the TLS communication between the distributed TOE components. The TOE performs self-tests that cover the correct operation of the TOE. It provides functions necessary to securely update the TOE. Its Linux-based operating system utilizes a hardware clock to ensure reliable timestamps. It protects sensitive data such as

stored passwords and cryptographic keys so that they are not accessible through the TOE, even to a Security Administrator.

4.10 TOE access

The TOE can be configured to display a logon banner before a user session is established. The TOE also enforces inactivity timeouts for local and remote sessions.

For VPN, the TOE can terminate VPN client sessions that have been inactive for the administrator defined time interval. The TOE can deny VPN client sessions based upon location (as determined by IP address), time and day. The TOE can assign private IP addresses to VPN clients.

4.11 Trusted path/channels

The TOE protects interactive communication with administrators using HTTPS/TLS for Client GUI access, ensuring both integrity and disclosure protection. If the negotiation of an encrypted session fails, the attempted connection will not be established.

The TOE protects communication with network peers, such as an external syslog server, using TLS connections to prevent unintended disclosure or modification of logs. Mutual authentication using client-side x.509v3 certificates is supported by the SMC TLS client for syslog over TLS.

The TOE protects data traffic sent between Security Engines or to remote/external gateways using IPsec. The TOE can be configured to provide VPN Clients with access to the SMC's Management Server, allowing a remote administrator to securely access the SMC through a browser tunneled within IPsec.

The TOE protects communications between distributed components using a TLS-based trusted channel. The TOE uses a distinct TLS channel while registering new Engines with the SMC and once registered, the Engine and SMC communication is replaced with a different mutually authenticated TLS channel to protect management communications.

5 Assumptions & Clarification of Scope

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- *collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 (NDcPP30e)
- *PP-Module for Stateful Traffic Filter Firewalls*, Version 1.4 + Errata 20200625, 25 June 2020 (STFFE14e)
- *PP-Module for Virtual Private Network (VPN) Gateways*, Version 1.3, 16 August 2023 (VPNGW13)

That information has not been reproduced here and the NDcPP30e/STFFW14e/VPNGW13 should be consulted if there is interest in that material.

5.2 Clarification of scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP30e/STFFW14e/VPNGW13 as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. 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 assurance activities specified in the NDcPP30e/STFFW14e/VPNGW13 and performed by the Evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guides identified in Section 6, additional customer documentation for the specific Firewall, VPN Gateway models was not included in the scope of the evaluation and, therefore, should not be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP30e/STFFW14e/VPNGW13 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- *Forcepoint Network Security Platform 7.3.2 Common Criteria Evaluated Configuration Guide*, Revision A, 2 September 2026
- *Network Security Platform 7.3 Installation Guide*, Revision A, 11 June 2025
- *Network Security Platform 7.3.0 Product Guide*, Revision A, 10 June 2025

Any additional customer documentation provided with the product, or that is available online, was not included in the scope of the evaluation and, therefore, should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary *Detailed Test Report for Forcepoint Network Security Platform 7.3*, Version 0.3, September 1, 2026 (DTR), as summarized in the evaluation Assurance Activity Report for Forcepoint Network Security Platform 7.3, Version 0.3, September 1, 2026 (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The Evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP30e/STFFW14e/VPNGW13 including the tests associated with optional requirements. The AAR, in section 3.4.1, lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The TOE consists of the following Engine models:

Model	Form factor/CPU
120	Desktop Intel® Atom C3338R (Goldmont)
120W	Desktop Intel® Atom C3338R (Goldmont)
120WL	Desktop Intel® Atom C3338R (Goldmont)
120L	Desktop Intel® Atom C3338R (Goldmont)
125L	Desktop Intel® Atom C3338R (Goldmont)
60	Desktop Intel Atom C3338 (Goldmont)
60L	Desktop Intel® Atom C3338R (Goldmont)
61	Desktop Intel® N50 (Alder Lake)
352	Desktop Intel® Atom C5315 (Tremont)
355	Desktop Intel® Atom C5325 (Tremont)
1202	Desktop Intel® Atom P5322 (Tremont)
2201	1U Intel® Xeon D-2123IT (Skylake)
2205	1U Intel® Xeon D-2145NT (Skylake)
2210	1U Intel® Xeon D-2177NT (Skylake)
2305	1U Intel® Xeon D-2876NT (Ice Lake)
2310	1U Intel® Xeon D-2896NT (Ice Lake)
3401	2U Intel® Xeon Silver 4210 (Cascade Lake)
3405	2U Intel® Xeon Silver 4216 (Cascade Lake)
3505	2U Intel® Xeon Silver 4416+ (Sapphire Rapids)
3510	2U Intel® Xeon Gold 6428N (Sapphire Rapids)
ESXi 8.0	Intel® Xeon Silver 4208 (Cascade Lake)

The SMC model is the Virtual SMC Appliance on ESXi 8.0 on Dell PowerEdge R440 with Intel Xeon® Silver 4208 (Cascade Lake).

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 all 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 Forcepoint Network Security Platform 7.3 TOE to be Part 2 extended and to meet the SARs contained in the NDcPP30e/STFFW14e/VPNGW13.

9.1 Evaluation of the Security Target (ASE)

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 Forcepoint Network Security Platform 7.3 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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 the Development (ADV)

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 ST and Guidance documents. Additionally, the Evaluation team performed the assurance activities specified in the NDcPP30e/STFFW14e/VPNGW13 related to the examination of the information contained in the TSS.

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.

9.3 Evaluation of the Guidance Documents (AGD)

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. All the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

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.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

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 the Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the NDcPP30e/STFFW14e/VPNGW13 and recorded the results in a Test Report, summarized in the ETR and AAR.

The Validation 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 NDcPP30e/STFFW14e/VPNGW13, and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities.

The Evaluation team searched the following public vulnerability databases:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search)
- MITRE CVE Database, National Vulnerability Database, and CVE details (https://www.cve.org/, https://web.nvd.nist.gov/vuln/search, and https://www.cvedetails.com/vulnerability-search.php)
- Known Vulnerability Exploit Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/)
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities)
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories)
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search)
- Offensive Security Exploit Database (https://www.exploit-db.com/)

The Evaluation team performed the vulnerability searches with the following key words. The last search was performed on 8/17/2026:

• Forcepoint • Forcepoint Network Security Platform 7.3 • Forcepoint NSP • NSP • Security Management Center • Virtual SMC • SMC • Security Engine • SMC FIPS Java API 2.0.1 • SMC FIPS Cryptographic Module for NTP 3.101 • Forcepoint Network Security Platform FIPS Library 3.1.2 • OpenSSL 3.1.2 • SafeZone FIPS Cryptographic Module 2.0 • SMC FIPS Library 3.0.7 • Intel Atom C3338 • Intel Atom C3338R • Intel N50 • Intel Atom C5315 • Intel Atom C5325 • Intel Atom P5322 • Intel Xeon D-2123IT • Intel Xeon D-2145NT • Intel Xeon D-2177NT • Intel Xeon D-2876NT • Intel Xeon D-2896NT • Intel Xeon Silver 4208	• Intel Xeon Silver 4210 • Intel Xeon Silver 4216 • Intel Xeon Silver 4416+ • Intel Xeon Gold 6428N • 120 • 120W • 120WL • 120L • 125L • 60 • 60L • 61 • 352 • 355 • 1202 • 2201 • 2205 • 2210 • 2305 • 2310 • 3401 • 3405 • 3505 • 3510 • ESXi 8.0 • Linux kernel 5.14 • Linux kernel 6.6

The Evaluation team conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

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.

9.7 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 followed the procedures defined in the CEM, performed the Assurance Activities in the NDcPP30e/STFFW14e/VPNGW13 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 instructions in the Guidance documents defined in Section 6. No other versions of the TOE and software, either earlier or later, were evaluated.

The evaluated functionality is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionalities provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

Per NIAP/CCEVS Publication #6, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Forcepoint Network Security Platform 7.3 Security Target*, Version 0.7, September 1, 2026.

13 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.

14 Bibliography

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

[1] *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, April 2017.

[2] *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components*, Version 3.1, Revision 5, April 2017.

[3] *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components*, Version 3.1 Revision 5, April 2017.

[4] *collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 (NDcPP30e).

[5] *PP-Module for Stateful Traffic Filter Firewalls*, Version 1.4 + Errata 20200625, 25 June 2020 (STFFE14e).

[6] *PP-Module for Virtual Private Network (VPN) Gateways*, Version 1.3, 16 August 2023 (VPNGW13).

[7] *Forcepoint Network Security Platform 7.3 Security Target*, Version 0.7, September 1, 2026 (ST).

[8] *Forcepoint Network Security Platform 7.3.2 Common Criteria Evaluated Configuration Guide*, Revision A, September 2, 2026 (AGD).

[9] *Network Security Platform 7.3 Installation Guide*, Revision A, 11 June 2025 (AGD).

[10] *Network Security Platform 7.3.0 Product Guide*, Revision A, 10 June 2025 (AGD).

[11] *Assurance Activity Report for Forcepoint Network Security Platform 7.3*, Version 0.3, September 1, 2026 (AAR).

[12] *Detailed Test Report for Forcepoint Network Security Platform 7.3*, Version 0.3, September 1, 2026 (DTR).

[13] *Evaluation Technical Report for Forcepoint Network Security Platform 7.3*, Version 0.3, September 1, 2026 (ETR).