National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Forcepoint NGFW 6.10

Report Number: CCEVS-VR-11234-2021
Dated: December 16, 2021
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
Ted Farnsworth
Lisa Mitchell
Linda Morrision
Randy Heimann
The MITRE Corporation

Common Criteria Testing Laboratory

Cody Cummins
Katie Sykes
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary 1
2 Identification 1
3 Architectural Information 3
3.1 TOE Evaluated Platforms 3
3.2 TOE Architecture 3
3.3 Physical Boundaries 6
4 Security Policy 7
4.1 Security audit 7
4.2 Communication 8
4.3 Cryptographic support 8
4.4 User data protection 8
4.5 Firewall 8
4.6 Identification and authentication 8
4.7 Security management 9
4.8 Protection of the TSF 9
4.9 TOE access 9
4.10 Trusted path/channels 9
5 Assumptions & Clarification of Scope 9
6 Documentation 10
7 IT Product Testing 11
7.1 Developer Testing 11
7.2 Evaluation Team Independent Testing 11
8 Evaluated Configuration 11
9 Results of the Evaluation 11
9.1 Evaluation of the Security Target (ASE) 12
9.2 Evaluation of the Development (ADV) 12
9.3 Evaluation of the Guidance Documents (AGD) 12
9.4 Evaluation of the Life Cycle Support Activities (ALC) 12
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) 13
9.6 Vulnerability Assessment Activity (VAN) 13
9.7 Summary of Evaluation Results 14
10 Validator Comments/Recommendations 14
11 Annexes 14
12 Security Target 14
13 Glossary 14
14 Bibliography 15

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Forcepoint NGFW 6.10 solution provided by Forcepoint, LLC. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation 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 December 2021. 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 collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 (with the PP-Module for Stateful Traffic Filter Firewalls, version v1.4 + Errata 20200625, 25 June 2020.

The Target of Evaluation (TOE) is the Forcepoint NGFW 6.10.

The Target of Evaluation (TOE) identified in this Validation Report 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). This Validation Report 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 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 evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Forcepoint NGFW 6.10 Security Target, version 1.0, November 23, 2021 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, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common

Evaluation Methodology (CEM) 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 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 Validated Products 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 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 NGFW 6.10 (Specific models identified in Section 8)
Protection Profile	collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 (NDcPP22e) with the PP-Module for Stateful Traffic Filter Firewalls, version v1.4 + Errata 20200625, 25 June 2020 (STFFW14e)
ST	Forcepoint NGFW 6.10 Security Target, version 1.0, November 23, 2021
Evaluation Technical Report	Evaluation Technical Report for Forcepoint NGFW 6.10, version 1.1, December 16, 2021
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 extended
Sponsor	Forcepoint, LLC
Developer	Forcepoint, LLC
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	The MITRE Corporation Bedford, MA and McLean, VA

3 Architectural Information

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

The Forcepoint Next Generation Firewall is a stateful packet filtering firewall. Being a stateful packet filtering firewall, the NGFW filters network traffic optimized through the use of stateful packet inspection. The NGFW is intended to be used as a network perimeter security gateway that provides a controlled connection. The NGFW is centrally managed and generates audit records for security critical events.

The Forcepoint Next Generation Firewall (NGFW) system is composed of the NGFW Engine (a physical or virtual appliance) and the Virtual Security Management Center (SMC). The NGFW 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 NGFW Engines. Throughout the remainder of this document, references to the NGFW Engine are meant to reference the TOE's firewall engine, while references to the NGFW are meant to refer to the TOE as a whole.

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

The NGFW 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 NGFW Engine may be used in combination to provide a company with an overall network topology.

The NGFW Engine contains a hardened Linux operating system (with a 4.19 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 NGFW Engine, the SMC contains a hardened Linux-based operating system (which uses a 4.18 kernel) to support the management capabilities and allow for the operation and configuration of firewall engines.

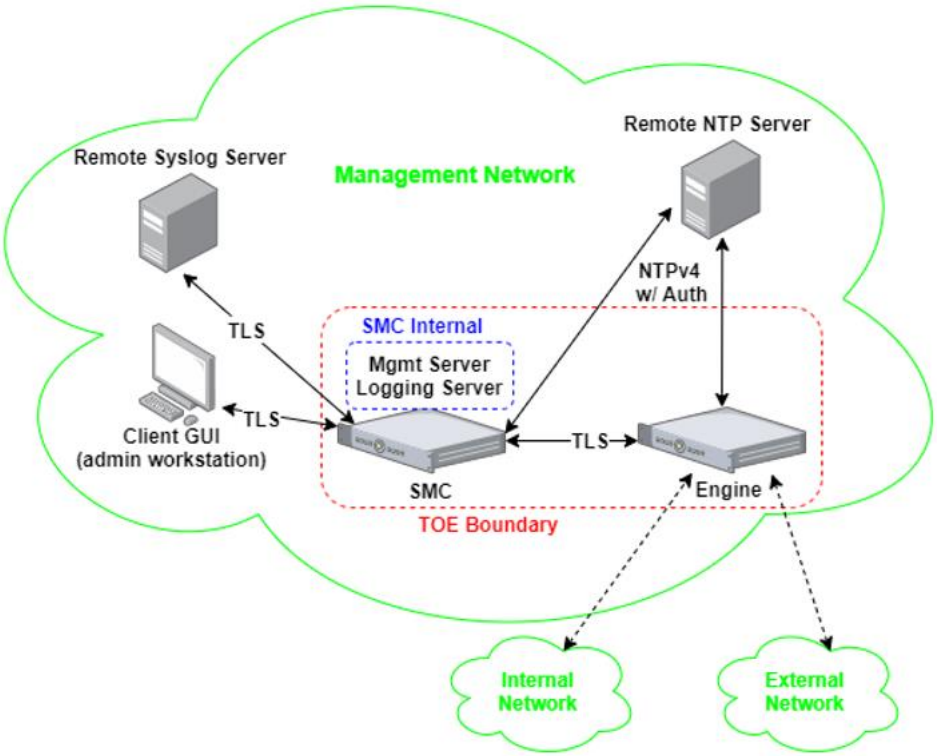
3.1 TOE Evaluated Platforms

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

3.2 TOE Architecture

The Forcepoint Next Generation Firewall (NGFW) system is a distributed TOE consisting of the Security Management Center (SMC) Appliance and one or more NGFW Engines under the control of the SMC. These NGFW Engines provide firewall 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 NGFW Engines through a TLS-protected trusted channel.



TOE Components, Communication Paths and IT Environment.

The following communication pathways are represented in the Figure above:

- **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.
- **NGFW Engine to External NTP server communications** use SHA1as the message digest algorithms for authentication with an NTP time source. Time on the NGFW Engine is updated by the SMC Management Server, or alternatively from an administrator configured NTP server.
- **NGFW Engine to Log Server communications** use the TLS-based trusted channel to protect the audit data transmitted from the NGFW Engine to the Log Server.

- **NGFW Engine to/from Management Server communications** use the TLS-based trusted channel to protect the configuration information exchanged between the Management Server and the NGFW Engine. Either party in this communication pathway can initiate the communications. Typically, the Management Server initiates configuration changes by sending updated security policies to the NGFW Engine. However, the NGFW Engine also polls for configuration changes on a regular basis.
- **Client GUI to Management and Log Server communications** uses TLS to protect the communication over which remote administration actions occur.
- The **NGFW Engines** control connectivity and information flow between **internal and external connected networks** that they are protecting.

The NGFW Engines (a.k.a., the Engines) are responsible for performing all firewall packet handling, analysis and filtering that is provided by the NGFW system as well as securely transmitting audit logs to the SMC's Log server.

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

The NGFW 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 NGFW 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 NGFW 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 or through an HTML5 web browser application). The Client GUI (along with the administrator's workstation on which the Client is installed), 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 NGFW Engine audit records that the Log Server has aggregated.

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 SMC FIPS Java API 1.0.2.1 (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 OpenSSL library to perform signature verification supporting the TOE trusted update mechanism. The Virtual SMC Appliance's NTP daemon uses cryptography from the SMC FIPS Crypto graphic Module for NTP 3.53.

The NGFW Engine utilizes its Forcepoint NGFW FIPS Library 1.1.1 to provide the encryption, decryption, signing and hashing functions necessary to support the NGFW Engine's trusted update mechanism and its TLS, ITT secure channel.

3.3 Physical Boundaries

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

The TOE is accessed and managed from the Forcepoint Security Management Center Client (6.10) installed on a PC (admin workstation) in the environment, where the PC is expected to have a network pathway 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 NGFW Engine does not send audit data directly to an external syslog server. Instead, a NGFW Engine passes all of its audit data to the Log Server on the Virtual SMC Appliance, which can (if configured) forward the data to the external syslog server.

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

The NGFW Engine utilizes its Forcepoint NGFW FIPS Library 1.1.1 based upon OpenSSL 1.1.1 (which utilizes the Forcepoint NGFW FIPS Cryptographic Module 1.2 to verify trusted engine software updates. The Virtual SMC Appliance uses its SMC FIPS Java API 1.0.2.1 to provide TLS (which protects the trusted channel mechanism and the trusted path mechanism) and uses its SMC FIPS Library 1.1.1 based on OpenSSL to verify SMC updates.

Each Engine model provides different performance as described in the table below.

Model	Form factor/CPU	Fixed ports	1G copper	10G Fiber	Network I/O slots
N120	Desktop Intel Atom C3338(Denverton)	8	8	0	0
N120W	Desktop Intel Atom C3338(Denverton)	8	8	0	0
N120WL	Desktop Intel Atom C3338(Denverton)	8	8	0	0
N60	Desktop Intel Atom C3338(Denverton)	4	4	0	0
2201	1U Intel Xeon D-2123IT (Skylake)	9x GE RJ45, 4x 10Gbps SFP+	9 to 17	4 to 12	1
2205	1U Intel Xeon D-2145NT (Skylake)	9x GE RJ45, 8x 10Gbps SFP+	9 to 17	8 to 16	1

2210	1U Intel Xeon D-2177NT (Skylake)	9x GE RJ45, 8x 10Gbps SFP+	9 to 16	8 to 16	1
3401	2U Intel Xeon Silver 4210 (Cascade Lake)	1x GE RJ45, 2x 10Gbps SFP+	1 to 65	2 to 66	8
3405	2U Intel Xeon Silver 4216 (Cascade Lake)	1x GE RJ45, 2x 10Gbps SFP+	1 to 65	2 to 66	8
3410	2U Intel Xeon Gold 6230N (Cascade Lake)	1x GE RJ45, 2x 10Gbps SFP+	1 to 65	2 to 66	8
ESXi 7.0	Intel Xeon Silver 4208 (Cascade Lake)	N/A	N/A	N/A	N/A

The SMC model is as follows:

- Virtual SMC Appliance on ESXi 7.0 on Dell PowerEdge R440 with Intel Xeon® Silver 4208 (Cascade Lake)

4 Security Policy

This section summaries 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. Protection of the TSF
9. TOE access
10. 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 Security Management Center and NGFW Engines. The Security Management Center can manage one or more NGFW 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 types of components (the SMC and its Engines) of the TOE utilize cryptography to verify trusted updates, for TLS protected management communications between the SMC and its Engines, and the SMC uses cryptography to support its use of the TLS protocol to protect network communications with external IT entities. Additionally, the TOE provides the ability to synchronize its time with a 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 NGFW 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, with the exception of reading the login banner, and performing firewall packet filtering operations. The TOE authenticates administrative users. In order for an administrative user to access the TOE, a user account including a user name 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 NGFW 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 Protection of the TSF

The TOE provides a variety of means of protecting itself. The TOE performs self-tests that cover the correct operation of the TOE. It provides functions necessary to securely update the TOE. It's 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.

4.9 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.

4.10 Trusted path/channels

The TOE protects interactive communication with administrators using TLS for 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.

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

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

- collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 with the PP-Module for Stateful Traffic Filter Firewalls, version v1.4 + Errata 20200625, 25 June 2020

That information has not been reproduced here and the NDcPP22e/STFFW14e should be consulted if there is interest in that material.

Clarification of scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e/STFFW14e as described for this TOE in the Security Target. 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 collaborative Protection Profile for Network Devices with the PP-Module for Stateful Traffic Filter Firewalls 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 Guide, additional customer documentation for the specific Firewall models was not included in the scope of the evaluation and therefore should not to 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 NDcPP22e/STFFW14e 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 Next Generation Firewall 6.10 Common Criteria Evaluated Configuration Guide, Revision B

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 to 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 NGFW 6.10, Version 1.0, December 16, 2021 (DTR), as summarized in the evaluation Assurance Activity Report.

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 NDcPP22e/STFFW14e including the tests associated with optional requirements. Section 3.4.1 of the AAR lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The TOE is Forcepoint NGFW 6.10 which consists of:

- Forcepoint NGFW Security Management Center (SMC) Virtual Appliance running software version 6.10 on ESXi 7.0.

- Forcepoint NGFW Engine running software version 6.10 and includes the following models:

    - Desktop models: N120, N120W, N120WL, N60
    - 1U models: 2201, 2205, 2210
    - 2U models: 3401, 3405, 3410
    - Virtual model: ESXi 7.0

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 ETR. The reader of this document can assume that all assurance 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

NGFW 6.10 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/STFFW14e.

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 NGFW 6.10 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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 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 Security target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the NDcPP22e/STFFW14e related to the examination of the information contained in the TSS.

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.

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

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.

9.4 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 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 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 NDcPP22e/STFFW14e and recorded the results in a Test Report, summarized in the AAR.

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.

9.6 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 evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

1 The evaluation team performed a public search for vulnerabilities in order to ensure there are no publicly known and exploitable vulnerabilities in the TOE from the following sources:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search)
- 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)
- Exploit / Vulnerability Search Engine (http://www.exploitsearch.net)
- SecurITeam Exploit Search (http://www.securiteam.com)
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search)
- Offensive Security Exploit Database (https://www.exploit-db.com/)

The search was performed on 12/15/2021 with the following search terms: "Forcepoint", "SMC", "Openssl", "NGFW 6.10", "Bouncy Castle", "ESXi 7.0", "Intel Atom", "Intel Xeon D", "Intel Xeon Scalable", "SMC FIPS Java API", "SMC FIPS Cryptographic Module for NTP", "SMC FIPS Library", "Forcepoint NGFW FIPS Cryptographic Module", "TCP", "UDP", "IPv4", "IPv6", "TLS", "Firewall".

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.

9.7 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 testing 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, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The Validation team suggest that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the Security Target. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Forcepoint NGFW 6.10 Security Target, Version 1.0, November 23, 2021*.

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 2.2e, 23 March 2020 (NDcPP22e)

[5] PP-Module for Stateful Traffic Filter Firewalls, version v1.4 + Errata 20200625, 25 June 2020 (STFFW14e)

[6] Forcepoint NGFW 6.10 Security Target, Version 1.0, November 23, 2021 (ST).

[7] Assurance Activity Report for Forcepoint NGFW 6.10, Version 1.1, December 16, 2021 (AAR).

[8] Detailed Test Report for Forcepoint NGFW 6.10, Version 1.0, December 16, 2021 (DTR).

[9] Evaluation Technical Report for Forcepoint NGFW 6.10, Version 1.1, December 16, 2021 (ETR)