National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Forcepoint Next Generation Firewall (NGFW)

Report Number: CCEVS-VR-10995-2019
Dated: 10/28/2019
Version: 0.2

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

David Challener
Meredith Hennan
Jay Turner
Kenneth Stutterheim

Common Criteria Testing Laboratory

Cody Cummins
Katie Sykes
Gossamer Security Solutions, Inc.
Catonsville, 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 Next Generation Firewall (NGFW) solution provided by Forcepoint. 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 Catonsville, MD, United States of America, and was completed in October 2019. 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 Stateful Traffic Filter Firewalls, Version 2.0 + Errata 20180314, 14-March-2018.

The Target of Evaluation (TOE) is the Forcepoint Next Generation Firewall (NGFW) 6.5.

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 6.5 (FWcPP20E) Security Target, version 1.5, 10/07/2019 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 **Protection Profile**	Forcepoint Next Generation Firewall (NGFW) 6.5 (Specific models identified in Section 8) collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0 + Errata 20180314, 14-March-2018
ST	Forcepoint NGFW 6.5 (FWcPP20E) Security Target, version 1.5, 10/07/2019
Evaluation Technical Report	Evaluation Technical Report for Forcepoint Next Generation Firewall (NGFW) 6.5, version 0.2, 10/08/2019
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
Developer	Forcepoint
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Catonsville, MD
CCEVS Validators	David Challener, Jay Turner, Meredith Hennan, Kenneth Stutterheim

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. The Forcepoint Next Generation Firewall (NGFW) system is composed of two physical appliances: the NGFW Engine and the Security Management Center (SMC) Appliance. The NGFW Engine controls connectivity and information flow between internal and external connected networks. The SMC Appliance provides administrative functionality supporting the configuration and operation of NGFW Engines. 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.

3.1 TOE Evaluated Configuration

The evaluated configuration consists of the following series and models

Forcepoint NGFW Security Management Center (SMC) Appliance running software version 6.5.7:

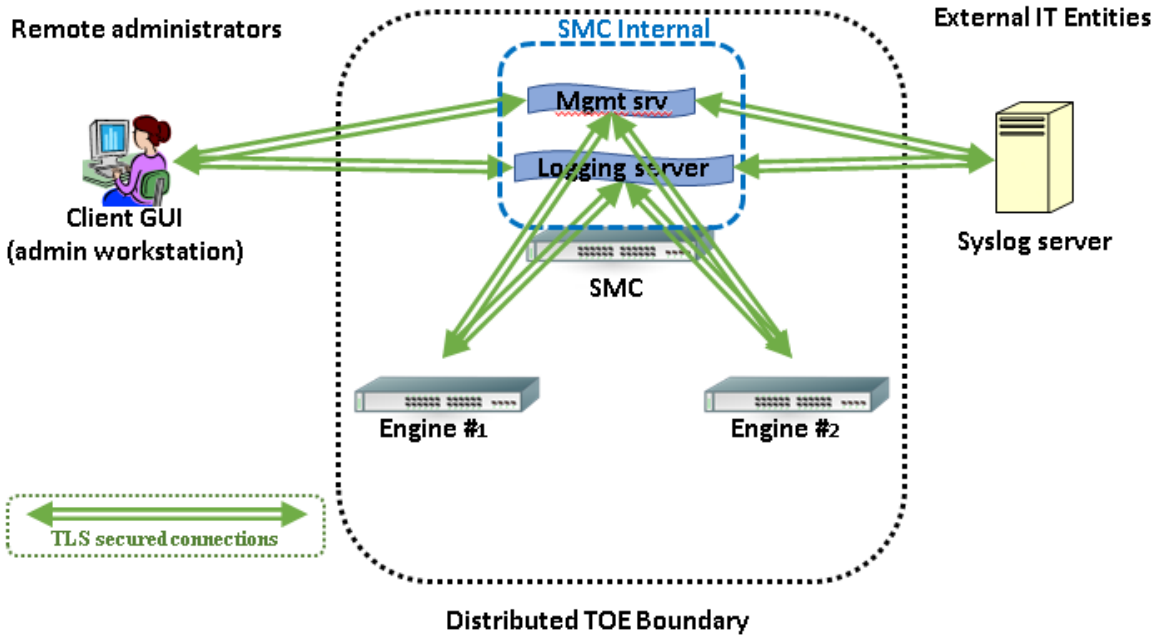
- Appliance SMC 1000 G2

Forcepoint NGFW Engine running software version 6.5.4 and including the following models:

- Desktop models: 330, 335
- 1U models: 1101, 1105, 2101, 2105,
- 2U models: 3301, 3305
- 4U model: 6205
- Virtual model: ESXi 6.5 on Dell PowerEdge R440

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 Forcepoint NGFW Engine FIPS Object Module 2.0.14 library to provide all cryptographic functionality. The SMC Appliance provides Management Server, Log Server functionality, and securely manage Engines. As the SMC utilizes both Java and C, the SMC relies upon both SMC FIPS Java API 1.0.2 with a Java runtime environment and SMC FIPS Object Module 2.0.13 for cryptographic functionality. In the evaluated configuration, the 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 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.
- **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 SMC Appliance provides the majority of the administrative capabilities in the NGFW system through the SMC Client GUI. The 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 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 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 mainly through the Client GUI, a Java program provided by Forcepoint. The administrator may download the GUI from the SMC Appliance using the Java Web Start or alternatively install it from a Forcepoint provided installation package. 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 SMC Appliance involving the Management Server and Log Server are performed using the SMC FIPS Java API 1.0.2 (library). This provider provides the encryption, decryption, signing and hashing functions necessary to support the SMC Appliance use of the trusted channel mechanism and the trusted path mechanism. The SMC Appliance also uses the OpenSSL library to perform signature verification supporting the TOE trusted update mechanism.

The NGFW Engine utilizes its Forcepoint NGFW Engine FIPS Object Module 2.0.14 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 two or more physical components: one or more NGFW Engine appliances and the SMC Appliance. Each of these appliances have physical 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 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 (6.5) installed on a PC (admin workstation) in the environment, where the PC is expected to have a network pathway to the 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 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 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. The SMC Appliance then configures the NGFW Engine's time to be in synch with itself. The NGFW Engine synchronizes only with the SMC.

The NGFW Engine utilizes its Forcepoint NGFW Engine FIPS Object Module 2.0.14 to verify trusted engine software updates. The SMC Appliance uses its SMC FIPS Java API 1.0.2 Library to provide TLS (which protects the trusted channel mechanism and the trusted path mechanism) and uses its SMC FIPS Object Module 2.0.13 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	40G Fiber	Network I/O slots	Max FW throughput
330	Desktop Atom C3338	8	8	0	0	0	4 Gbps
335	Desktop Atom C3558	8	8 to 16	0	0	2	7 Gbps
1101	1U Pentium D1508	8x GE RJ45, 2x 10Gbps SFP+	8 to 16	2 to 6	0	1	50 Gbps
1105	1U Xeon D-1518	8x GE RJ45, 2x 10Gbps SFP+	8 to 16	2 to 6	0	1	60 Gbps
2101	1U Xeon D-1548	12x GE RJ45, 2x 10Gbps SFP+	12 to 28	2 to 10	0 to 4	2	60 Gbps
2105	1U Xeon D-1567	12x GE RJ45, 2x 10Gbps SFP+	12 to 28	2 to 10	0 to 4	2	80 Gbps

3301	2U Xeon E5-2618L v3	2x GE RJ45	2 to 34	0 to 16	0 to 8	4	80 Gbps
3305	2U Xeon E5-2680 v3	2x GE RJ45, 1x 40Gbps QSFP+	2 to 34	0 to 16	1 to 9	4	160 Gbps
6205	4U Xeon E5-2680 v4	2x GE RJ45	2 to 66	0 to 32	1 to 17	8	240 Gbps
ESXi 6.5	Xeon Silver 4112 on Dell PowerEdge R440	3x GE RJ45	N/A	N/A	N/A	N/A	N/A

The SMC model is as follows:

- SMC 1000 G2 with the Intel Xeon® Silver 4112 2.6GHz, 8.25M cache processor

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Communication
3. Cryptographic support
4. Firewall
5. Identification and authentication
6. Security management
7. Protection of the TSF
8. TOE access
9. 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.

4.4 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.

4.5 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.

4.6 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). Administrators can also access the TOE via a local console which provides limited functionality.

4.7 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. The TOE also utilizes a dedicated, local network for communications between the TOE's components.

4.8 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.

4.9 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 TLS while registering new Engines with the SMC and once registered, the Engine and SMC use mutually-authenticated TLS 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 Stateful Traffic Filter Firewalls, Version 2.0 + Errata 20180314, 14-March-2018

That information has not been reproduced here and the FWcPP20E should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the FWcPP20E 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.

Clarification of scope
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 Protection Profile 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.

- 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 FWcPP20E 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 NGFW Common Criteria Evaluated Configuration Guide 6.5.4, Rev D
- Forcepoint NGFW 6.5 (FWcPP20E) Security Target

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 Assurance Activity Report (FWcPP20E) for Forcepoint NGFW 6.5, Version 0.2, 10/08/2019 (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 a Common Criteria Certification document and ran the tests specified in the FWcPP20E including the tests associated with optional requirements.

8 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 Next Generation Firewall (NGFW) TOE to be Part 2 extended, and to meet the SARs contained in the FWcPP20E.

8.1 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 Next Generation Firewall (NGFW) 6.5 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators 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.

8.2 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 FWcPP20E related to the examination of the information contained in the TSS.

The validators 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.

8.3 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 validators 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.

8.4 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 validators 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.

8.5 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 FWcPP20E and recorded the results in a Test Report, summarized in the AAR.

The validators 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.

8.6 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 and fuzz testing. Neither the public search for vulnerabilities nor the fuzz testing uncovered any residual vulnerability.

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 Engin (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 10/07/2019 with the following search terms: "TCP", "router", "switch", “UDP”, “IPv4”, “IPv6”, "TLS", "ICMP", "firewall", “Forcepoint”, "OpenSSL", “NGFW”, and “Bouncy Castle”.

The validators 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.

8.7 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.

9 Validator Comments/Recommendations

The virtualized product version was tested on a Dell PowerEdge R440 running ESXi 6.5. Any other combination of hardware and virtual platform was not tested and therefore there is no assurance that any other platform will perform as required by the protection profiles.

The SMC is intended to be managed on an IPv4 network per the Forcepoint Next Generation Firewall Installation Guide.

Although the product supports network time protocol (NTP), NTP is not to be used in the Common Criteria evaluated configuration.

Cryptographic modules other than OpenSSL FIPS Object Module SE #2398 version 2.0.13, Bouncy Castle FIPS Java API #3514 version 1.0.2 JCA/JCE provider, Forcepoint NGFW Cryptographic Library #2319, and OpenSSL FIPS Object Module SE #2398 version 2.0.14, have not been evaluated nor tested during this Common Criteria evaluation.

10 Annexes

Not applicable

11 Security Target

The Security Target is identified as: *Forcepoint NGFW 6.5 (FWcPP20E) Security Target, Version 1.5, 10/07/2019.*

12 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.

13 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 Stateful Traffic Filter Firewalls, Version 2.0 + Errata 20180314, 14-March-2018.

[5] Forcepoint NGFW 6.5 (FWcPP20E) Security Target, Version 1.5, 10/07/2019 (ST).

[6] Assurance Activity Report (FWcPP20E) for Forcepoint NGFW 6.5, Version 0.2, 10/08/2019 (AAR).

[7] Detailed Test Report (FWcPP20E) for Forcepoint NGFW 6.5, Version 1.0, 10/07/2019 (DTR).

[8] Evaluation Technical Report for Forcepoint Next Generation Firewall (NGFW), Version 0.2, 10/08/2019 (ETR)