National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Forcepoint

10900-A Stonelake Blvd.

Austin, TX 78759, USA

Forcepoint NGFW 6.3.1

Report Number:	**CCEVS-VR-10854-2018**
Dated:	**March 12, 2018**
Version:	**1.0**

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

Patrick Mallett, PhD
Jerome Myers, PhD

Common Criteria Testing Laboratory

Tammy Compton
Raymond Smoley
Catherine 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 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 March 2018. 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 1.0, 27 February 2015 (FWcPP10).

The Target of Evaluation (TOE) is the Forcepoint NGFW 6.3.1.

The 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 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). 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 6.3.1 (FWcPP10) Security Target, version 1.0, March 5, 2018 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 6.3.1 (Specific models identified in Section 3.1)
Protection Profile	collaborative Protection Profile for Stateful Traffic Filter Firewalls, version 1.0, 27 February 2015 (FWcPP10)
ST	Forcepoint NGFW 6.3.1 Security Target, version 1.0, March 5, 2018
Evaluation Technical Report	Evaluation Technical Report for Forcepoint NGFW 6.3.1, version 0.2, March 5, 2018
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Forcepoint
Developer	Forcepoint
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Patrick Mallett, PhD Jerome Myers, PhD

3 Architectural Information

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

The Target of Evaluation (TOE) is the **Error! Reference source not found.** NGFW 6.3.1.

The Forcepoint NGFW 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.

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the following models:

- Forcepoint NGFW Security Management Center (SMC) Appliance running software version 6.3.1:

  Appliance

- Forcepoint NGFW Engine running software version 6.3.1 and including the following models:

  1U models:

  - 1101
  - 1105
  - 1402
  - 2101
  - 2105

  2U models:

  - 3301
  - 3305

  4U model:

  - 6205

3.2 TOE Architecture

The Forcepoint NGFW system is composed of two physical appliances: the NGFW Engine and the Security Management Center (SMC) Appliance. The NGFW Engine provides firewall functionality utilizing its Linux operating system and using its embedded **Error! Reference source not found.** library to provide all cryptographic functionality. The SMC Appliance provides Management Server and Log Server functionality. As the SMC utilizes both Java and C, the SMC relies upon both **Error! Reference source not found.** with a Java runtime environment and **Error! Reference source not found.** for cryptographic functionality. In the evaluated configuration, the SMC Appliance must be directly connected to the NGFW Engine through a dedicated, local network connection.

3.3 Physical Boundaries

The TOE is composed of two physical components: the NGFW Engine appliance and the SMC Appliance. Each of these appliances have physical network connections to its environment, one dedicated, local network connection to exclusively facilitate communication between the SMC and engine, as well as additional network connections that positions the NGFW Engine portion of the TOE to monitor and filter network traffic. The SMC Appliance provides all management functionality, while the NGFW Engine provides all firewall packet filtering.

The TOE is accessed and managed from the Forcepoint Security Management Center Client (6.3.1) installed on a PC 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.

The TOE can be configured to synchronize its internal clock using an NTP server in the operational environment. The SMC Appliance synchronizes with the external NTP server, then configures the NGFW Engine's time to be in synch with itself. The NGFW Engine does not synchronize directly with an external NTP server, but instead synchronizes only with the SMC.

The NGFW Engine utilizes its OpenSSL Library to verify trusted engine software updates. The SMC Appliance uses its **Error! Reference source not found.** Library to provide TLS (which protects the trusted channel mechanism and the trusted path mechanism) and uses its OpenSSL library to verify SMC updates.

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

Model	Form factor	Fixed ports	1G copper	10G Fiber	40G Fiber	Network I/O slots	Max FW throughput
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
1402	1U Xeon E5-1650 v2	4x GE RJ45	4 to 20	0 to 8	0 to 4	2	40 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

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. User data protection
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 Cryptographic support

Because the TOE consists of two components, each physical component of the TOE must be considered when discussing the TOE cryptographic support. Both components of the TOE utilize cryptography to verify trusted updates, and the SMC uses cryptography to support its use of the TLS protocol to protect network communication.

4.3 User data protection

The TOE ensures that residual information is protected from potential reuse in accessible objects such as network packets.

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.

5 Assumptions

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

- collaborative Protection Profile for Stateful Traffic Filter Firewalls, version 1.0, 27 February 2015 (FWcPP10)

That information has not been reproduced here and the FWcPP10 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 FWcPP10 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.

6 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 Stateful Traffic Filter Firewalls collaborative Protection Profile 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 FWcPP10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7 Documentation

The following documents were available with the TOE for evaluation:

- Forcepoint NGFW Common Criteria Evaluated Configuration Guide, Version 6.3.1 Rev E,

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Detailed Test Report (FWcPP10) for Forcepoint NGFW 6.3.1, Version 0.2, March 2, 2018 (DTR).

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the FWcPP10 including the tests associated with optional requirements.

9 Evaluated Configuration

The evaluated configuration consists of the following series and models

- Forcepoint NGFW Security Management Center (SMC) Appliance running software version 6.3.1:

    Appliance

- Forcepoint NGFW Engine running software version 6.3.1 and including the following models:

    1U models:
    - 1101
    - 1105
    - 1402
    - 2101
    - 2105

    2U models:
    - 3301
    - 3305

    4U model:
    - 6205

10 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 4 and CEM version 3.1 rev 4. The evaluation determined the NGFW TOE to be Part 2 extended, and to meet the SARs contained in the FWcPP10.

10.1 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 6.3.1 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.

10.2 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 FWcPP10 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.

10.3 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.

10.4 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.

10.5 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 FWcPP10 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.

10.6 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.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: "Forcepoint", "Stonesoft", "NGFW", "Next Generation Firewall", "SMC", "Security Management Center", "Crypto-J", "Openssl", "dnsmasq", "openldap", "Bouncy Castle" “FIPS Object Module” and “FIPS Java API”.

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.

10.7 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.

11 Validator Comments/Recommendations

None.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: Forcepoint NGFW 6.3.1 (FWcPP10) Security Target, Version 1.0, March 5, 2018.

14 Glossary

The following definitions are used throughout this document:

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

15 **Bibliography**

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

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2102.

[4] collaborative Protection Profile for Stateful Traffic Filter Firewalls, version 1.0, 27 February 2015 (FWcPP10).

[5] Forcepoint NGFW 6.3.1 (FWcPP10) Security Target, Version 1.0, March 5, 2018 (ST).

[6] Assurance Activity Report (FWcPP10) for Forcepoint NGFW 6.3.1, Version 0.4, March 5, 2018 (AAR).

[7] Detailed Test Report (FWcPP10) for Forcepoint NGFW 6.3.1, Version 0.2, March 2, 2018 (DTR).

[8] Evaluation Technical Report for Forcepoint NGFW, Version 0.2, March 5, 2018 (ETR).