National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Fortinet FortiMail Appliances running Software version 6.0, Version 1.0

Report Number: CCEVS-VR-10899-2019

Dated: 1/17/2019

Version: 0.3

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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Meredith Hennan

Kenneth Stutterheim

The Aerospace Corporation

Common Criteria Testing Laboratory

Anthony Busciglio

Thibaut Marconnet

Danielle F Canoles

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Fortinet FortiMail Appliances 6.0 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in January 2019. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements defined in collaborative Protection Profile for Network Devices (NDcPP) + Errata 20180314 version 2.0e (NDcPPv2.0e).

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. 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 4), as interpreted by the Assurance Activities contained in the Supporting Document, Evaluation Activities for Network Device cPP, March 2018 Version 2.0+Errata20180314. 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 provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The 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(s) 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	Fortinet FortiMail Appliances running Software version 6.0
Protection Profile	collaborative Protection Profile for Network Devices (NDcPP) + Errata 20180314 version 2.0e (NDcPPv2.0e)
Security Target	Fortinet FortiMail Appliances Security Target, version 1.5, January 2019
Evaluation Technical Report	Fortinet FortiMail Appliances ETR
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Fortinet, Inc.
Developer	Fortinet, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security 2400 Research Blvd Suite 395 Rockville, MD 20850
CCEVS Validators	Meredith Hennan, Kenneth Stutterheim

3 Architectural Information

FortiMail appliances are specialized email security systems that provide multi-layered protection against blended threats comprised of spam, viruses, worms and spyware. FortiMail’s inbound filtering engine blocks spam and malware before it can clog networks and affect users. FortiMail’s dynamic and static user-blocking provides granular control over all email policies and users. Secure content delivery is enforced with FortiMail’s Identity-Based Encryption (IBE), S/MIME, or TLS email encryption options. FortiMail’s predefined or customized dictionaries prevent accidental and intentional loss of confidential data. These mail related features were not evaluated and no claims can be made or inferred regarding their effectiveness or correct operation.

Administration of the system may be performed locally through the Command Line Interface (CLI) using an administrator console or remotely via a network management station through the FortiMail Web-based manager (using HTTPS). The administrator accesses the CLI via terminal emulation software (e.g. Hyperterm) on a computer connected to the appliance via a serial cable. Access to the FortiMail administrative functions including the audit data is restricted to authenticated Administrators. Administrator authentication is performed by the appliance.

FortiMail supports two high availability modes. Config-only mode provides load balancing and allows up to 25 FortiMail units to share a common configuration but operate as separate FortiMail units. In Active-passive mode a second (passive) FortiMail unit can be configured as a failover device if the primary (active) FortiMail unit fails. All data from the active unit, except for the Bayesian database, is duplicated to the passive unit. Evaluation testing was conducted on a single Fortimail appliance (2000E) and the availability mode claims were not validated.

FortiMail supports three modes of operation: gateway mode, transparent mode and server mode. Gateway mode and transparent mode are within the scope of this evaluation. In all modes, the FortiMail system provides antivirus, antispam, content filtering, email routing and email archiving functionality with only minor changes to existing networks. Note however, that these features are not within the scope of this evaluation.

Fortinet Entropy Token (delivered as part of the TOE) is a USB-based cryptographic support processor that is an option for FortiMail and is required in the evaluated configuration. For this TOE, Fortinet Entropy Token is used as an entropy source only.

4 Security Policy

Protected Communications:

The TOE protects the integrity and confidentiality of communications as follows:

- TLS connectivity with the following entities:
    - Audit Server (with device level authentication)
    - Web Browser (on a management workstation)

Secure Administration:

The TOE enables secure local and remote management of its security functions, including:

- Local console CLI administration
- Remote GUI administration via HTTPS/TLS
- Administrator authentication using a local database or via X.509 certificates to the remote GUI
- Timed user lockout after multiple failed authentication attempts
- Password complexity enforcement
- Role Based Access Control - the TOE supports several types of administrative user roles. Collectively these sub-roles comprise the "Security Administrator"
- Configurable banners to be displayed at login
- Timeouts to terminate administrative sessions after a set period of inactivity
- Protection of secret keys and passwords

Trusted Update:

The TOE ensures the authenticity and integrity of software updates through digital signatures and requires administrative intervention prior to the software updates being installed.

Security Audit:

The TOE keeps local and remote audit records of security relevant events. The TOE internally maintains the date and time which can be set manually.

Self-Test:

The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions.

Cryptographic Operations:

The TOE provides cryptographic support for the services described in the table below. The Fortinet FortiMail appliance leverages the 'Fortinet FortiMail RNG Cryptographic Library Version 6.0' and 'Fortinet FortiMail RNG Cryptographic Library Version 6.0' for cryptography.

TOE Provided Cryptography	
Cryptographic Method	**Use within the TOE**
TLS Establishment	Used to establish initial TLS session.
RSA Signature Services	Used in TLS session establishment. Used in secure software update
SP 800-90 DRBG	Used in TLS session establishment.

TOE Provided Cryptography	
Cryptographic Method	**Use within the TOE**
SHS	Used in secure software update
HMAC-SHS	Used to provide TLS traffic integrity verification
AES (CBC)	Used to encrypt TLS traffic

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

A.PHYSICAL_PROTECTION
The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the [NDcPPv2.0e] will not include any requirements on physical tamper protection or other physical attack mitigations. The [NDcPPv2.0e] will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.

A.LIMITED_FUNCTIONALITY
The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general-purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

A.NO_THRU_TRAFFIC_PROTECTION
A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPPv2.0e. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).

A.TRUSTED_ADMINISTRATOR
The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

A.REGULAR_UPDATES
The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

A.ADMIN_CREDENTIALS_SECURE
The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.

A.COMPONENTS_RUNNING (applies to distributed TOEs only)
For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.

A.RESIDUAL_INFORMATION
The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

T.UNAUTHORIZED_ADMINISTRATOR_ACCESS
Threat agents may attempt to gain Administrator access to the network device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.

T.WEAK_CRYPTOGRAPHY
Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

T.UNTRUSTED_COMMUNICATION_CHANNELS
Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.

T.WEAK_AUTHENTICATION_ENDPOINTS
Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.

T.UPDATE_COMPROMISE
Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

T.UNDETECTED_ACTIVITY
Threat agents may attempt to access, change, and/or modify the security functionality of the network device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.

T.SECURITY_FUNCTIONALITY_COMPROMISE
Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.

T.PASSWORD_CRACKING
Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.

T.SECURITY_FUNCTIONALITY_FAILURE
An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

5.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the NDcPP.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PP. Any additional security related functional capabilities included in the product were not covered by this evaluation. Specifically, enabling and using NTP and SSH services is not permitted in the evaluated configuration.

6 Documentation

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

- Fortinet FortiMail Appliances Security Target, version 1.5, January 2019
- Fortinet Fortimail v6.0 CC Guidance Documentation, Version 1.2, January 2019

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 Fortinet Fortimail v6.0 CC Guidance Documentation, Version 1.2, January 2019.

Consumers are encouraged to download that guidance document from the NIAP website to ensure the device is configured as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE is comprised of three models of the Fortinet FortiMail Appliances as shown below.

	CPU	Storage	RAM
FML-2000E	Intel Xeon E5	2x 2TB HDD (max 8)	32GB
FML-3000E	Intel Xeon E5	2x 2TB HDD (max 12)	32GB
FML-3200E	Intel Xeon E5	2x 2TB HDD (max 12)	64GB

The TOE evaluated configuration consists of the appliances listed above. The TOE supports secure connectivity with several IT environment devices as shown below.

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with Web Browser	Yes	This includes any IT Environment Management workstation with a Web Browser installed that is used by the TOE administrator to support TOE administration through HTTPS protected channels. Any web browser that supports TLS 1.1 or greater may be used.
Audit Server	Yes	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE. The syslog server must support communications using TLS 1.1 or TLS 1.2.

The network on which the TOE resides is considered part of the environment. The software version 6.0 is pre-installed on the TOE hardware. In addition, software images are downloadable from the Fortinet website. A login ID and password is required to download a software image from that website.

7.2 Excluded Functionality

The following functionality was not evaluated as part of this NDcPPv2.0e Common Criteria evaluation,

- Antivirus
- Antispam
- Content Filtering
- Email Routing
- Email Archiving
- Mail Transfer Agent (MTA) Functionality
- SMTP/SMTPS Routing
- S/MIME/TLS email encryption
- Identity-Based Encryption (IBE)
- High Availability Modes

Additional features including SSH administration and NTP are not to be used in the evaluated configuration. Of the three modes of operation available, only gateway mode and transparent mode are within the scope of this evaluation.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Fortinet FortiMail Appliances 6.0, which is not publicly available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

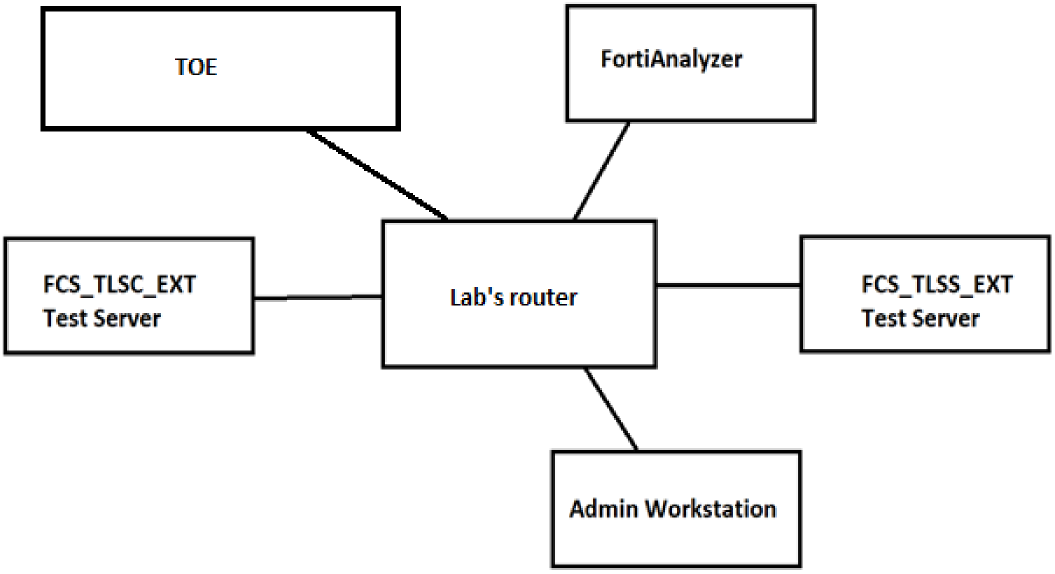
No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the Supporting Document, Evaluation Activities for Network Device cPP, March 2018 Version 2.0+Errata20180314. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

8.3 Test Configuration

Below is a visual representation of the components included in the test bed, the details of the configuration are in section 4.2



The TOE testing was conducted on the FML-2000E Fortimail Appliance in Gateway Mode. The FortiAnalyzer in the test configuration was used as the audit repository.

8.4 Testing Tools

The following test tools were used as part of testing:

- Wireshark 2.4.4
- Syslog, FortiAnalyzer, 6.0

- OpenSSL, 1.0.2
- Acumen-TLS, 1.0 (CCTL Proprietary)
- Acumen-TLSS, 1.0 (CCTL Proprietary)

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). Those results are summarized in the publicly available Assurance Activity Report (AAR) for this evaluation. The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Fortinet FortiMail Appliances 6.0 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

9.1 Evaluation of Security Target

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 Fortinet FortiMail Appliances 6.0 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the NDcPP.

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.

9.2 Evaluation of Development Documentation

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the NDcPPv2.0e related to the examination of the information contained in the TOE Summary Specification.

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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the NDcPP related to the examination of the information contained in the operational guidance documents.

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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 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.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDcPPv2.0e and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validators reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDcPP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The CCTL conducted an examination of publicly available information for vulnerabilities associated with the product on December 7, 2018 and again on January 17,2019 using the sources and search terms listed below:

- http://nvd.nist.gov/
- http://www.us-cert.gov
- http://www.securityfocus.com/

The evaluator performed the public domain vulnerability searches using the following key words:

- Fortinet, Inc.
- Fortinet FortiMail Appliances
- Fortinet FortiMail SSL Cryptographic Library Version 6.0
- FortiMail RNG Cryptographic Library Version 6.0
- FML-2000E
- FML-3000E
- FML-3200E
- Mail Server

- TCP

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 addressed the vulnerability analysis Assurance Activities in the NDcPPv2.0e, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the Supporting Document, Evaluation Activities for Network Device cPP, March 2018 Version 2.0+Errata20180314, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

Consumers are encouraged to understand the scope of the device functionality includes functions that were not tested as part of the evaluation. A list is included in section 7.2 above: Excluded Functionality.

Administrators should note that SSH and NTP are not approved for use in the evaluated configuration. As well, even though testing was conducted using a FortiAnalyzer as a syslog server, other syslog servers can be used as long as a trusted channel is established and maintained per the CC guidance.

11 Annexes

Not applicable.

12 Security Target

Fortinet FortiMail Appliances Security Target, version 1.5, January 2019

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 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 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. collaborative Protection Profile for Network Devices (NDcPP) + Errata 20180314 version 2.0e (NDcPPv2.0e)
6. Supporting Document, Evaluation Activities for Network Device cPP, March 2018, Version 2.0+Errata20180314 (SD)
7. Fortinet FortiMail v6.0 CC Guidance Documentation, Version 1.2, January 2019 (AGD)
8. Fortinet, Inc. Common Criteria Security Target, Version 1.5, January 2019. (ST)
9. Fortinet FortiMail Appliances v6.0 Evaluation Technical Report, Version 1.3, January 2019. (TOE-ETR) <Evaluation Sensitive>
10. Test Plan for Fortinet FortiMail Appliances, Version 1.2, January 2019. (DTR) <Evaluation Sensitive>
11. Common Criteria NDcPP Assurance Activity Report Fortinet FortiMail Appliances, Version 1.3, January 2019. (AAR) <Evaluation Sensitive>
12. Fortinet FortiMail Appliances v6.0 Evaluation Technical Report, Version 1.3, January 2019. (ASE-ETR) <Evaluation Sensitive>
13. VID10899 Fortinet FortiMail Appliances Equivalency Analysis, Version 1.0, July 2018. <evaluation sensitive>
14. Vulnerability Assessment for Fortinet FortiMail Appliances Version 1.2, January 2019. <evaluation sensitive>