National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Fortinet FortiMail Version 7.4

Report Number:	**CCEVS-VR-VID11454-2024**
Dated:	**July 24, 2024**
Version:	**1.0**

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

Department of Defense
ATTN:NIAP, Suite 6982
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6982

Acknowledgements

Validation Team

Daniel Faigin

The Aerospace Corporation

Farid Ahmed

Kurt Bahnsen

Anne Gugel

Robert Wojcik

Johns Hopkins University APL

Common Criteria Testing Laboratory

Justin Fisher

Pascal Patin

Kofi Owusu

Srilekha Vangala

Leidos Inc.

Columbia, MD

Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Fortinet FortiMail Version 7.4 (the Target of Evaluation, or 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 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 in 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 evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. 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.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in July 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by Leidos. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant and meets the assurance requirements defined in the following documents:

- collaborative Protection Profile for Network Devices, Version 2.2e [CPP_ND_V2.2E] *[5]*
- *Evaluation Activities for Network Device cPP,* Version 2.2, December 2019 *[8]*

The TOE is Fortinet FortiMail Version 7.4. Any shorthand references to “FortiMail” in this VR are meant to refer to the TOE.

The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the aforementioned Protection Profiles. 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 (CCEVS) and the conclusions of the testing laboratory in the ETR 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 the evaluation demonstrated the product satisfies all of the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) specified in the ST. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile, and when installed, configured and operated as described in the evaluated guidance documentation, satisfies all the SFRs specified in the ST ([6]).

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 and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation evaluating products against Protection Profiles 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 IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

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)—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The Protection Profile(s) (PP)/PP-Modules 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 Version 7.4
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e [CPP_ND_V2.2E
Security Target	Fortinet FortiMail Version 7.4 Security Target, Version 1.0, 19 April 2024
Evaluation Technical Report	Evaluation Technical Report for Fortinet FortiMail Version 7.4 (Proprietary) Version 1.0, 29 May 2024
Sponsor & Developer	Fortinet, Inc. 899 Kifer Road Sunnyvale, CA 94086
Completion Date	July 18 2024
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	*collaborative Protection Profile for Network Devices,* Version 2.2e, 23 March 2020

Item	Identifier
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 Conformant
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Evaluation Personnel	Tony Apted Justin Fisher Kofi Owusu Pascal Patin
Validation Personnel	Farid Ahmed Kurt Bahnsen Daniel Faigin Anne Gugel Robert Wojcik

3 TOE Architecture

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

The FortiMail TOE is a network device with both physical models (standalone dedicated hardware chassis) and a virtual model running on an environmental hypervisor and physical platform. The TOE software includes a modified version of Linux kernel 5.10.180 without general-purpose functionality, OpenSSL 1.1.1w cryptographic library, as well as specialized software needed to run the actual FortiMail functionality. The FortiMail virtual network device runs on an environmental hypervisor (VMware ESXi v8.0) and was tested on an Intel Xeon E5-2620v4, 8 Cores, 2.10GHz.

3.1 Physical Boundary

The TOE consists of one of the following FortiMail appliances as well as its firmware.:

Model	CPU	Storage	RAM
FML-200F	Intel Celeron G3900 Skylake, 2.80 GHZ	2x 2TB HDD	64GB
FML-400F	Intel i3-6100 Skylake, 3.7 GHz	2x 4TB HDD	64GB
FML-900F	Intel E3-1275V6 Kaby Lake, 3.80GHz	4X 4TB HDD	64GB
FML-2000F	Intel Xeon Silver 4210R Cascade Lake, 2.4GHz	10X 20TB	1TB
FML-3000F	Intel Xeon Silver 4210R Cascade Lake, 2.4GHz (dual CPU)	10X 20TB	1TB
VM	1 vCPU	50GB minimum 1TB Maximum	1GB

In the evaluated configuration, the virtual appliance was tested on VMware ESXi 8.0 on a physical system with an Intel Xeon E6-2620v4.

The TOE interfaces are as follows:

- CLI: Administrative CLI via direct serial connection or SSH.
- GUI: Administrative web GUI via HTTPS.
- Logs: Forwarding of TOE audit events to a remote audit server, which is a Fortinet FortiAnalyzer (FAZ), via TLS.

The TOE's operational environment includes the following:

- Remote audit server
- Platform (hardware and firmware) on which the virtual appliance TOE is hosted. In the tested configuration, this included the following:
  - VMware ESXi 8.0
  - Intel Xeon E5-2620V4, 8 Cores, 2.10GHz processor (Broadwell) processor
- Access to a Certification Authority and corresponding revocation checking mechanism for certificate management.
- A remote management workstation with a supported web browser for remote administrative access:
  - The tested configuration used Google Chrome 117.0.5938.150

The TOE runs in FIPS-CC mode of operation. Non FIPS-CC mode of operation is excluded from the evaluated configuration.

4 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST and the Final ETR.

4.1 Security Audit

The TOE generates audit records of security-relevant activity. Audit data is stored locally and the TOE also has the ability to export all audit records to an external audit server over a TLS protected channel. The TOE manages the audit storage by overwriting previous audit records when the local storage space for audit data is full in order to capture new events.

4.2 Cryptographic Support

The TOE implements cryptographic functions in support of trusted communications, key pair generation for X.509 certificate requests, and self-testing. For trusted communications, the TOE implements TLS as a server with HTTPS, and TLS as a client without HTTPS. The TOE's TLS client supports mutual authentication. The TOE relies on platform hardware to generate entropy that is used to seed its DRBG to ensure that generated keys have the advertised security strength.

4.3 Identification and Authentication

The TOE uses a local password-based mechanism and additionally for SSH, an SSH public key-based mechanism for administrator authentication. The TOE enforces restrictions on the length and character composition of administrator passwords. Excessive failed authentication attempts on a remote administrative interface will cause a lockout that is resolved by a waiting period. The TOE also uses X.509 certificates for authentication of TLS connections. The TOE has a mechanism by which a certificate signing request can be generated so that it may obtain a certificate for its own use from a trusted CA.

4.4 Security Management

The TOE has a web-based remote management interface as well as a local/remote console. Most functionality can be administered over both interfaces. The TOE uses a single Security Administrator role to authorize the use of management functions.

4.5 Protection of the TSF

The TOE protects sensitive data from unauthorized access. It enforces integrity of its own contents through the use of self-tests to ensure that the TSF has not been modified. Firmware updates are obtained through the operational environment (e.g. downloaded from the vendor's support site); updates have a digital signature that is verified prior to application.

4.6 TOE Access

The TOE controls access through enforcement of idle session timeout on its management interfaces. These interfaces also display a configurable pre-authentication warning banner that advises against unauthorized use of the TOE.

4.7 Trusted Path/Channels

The TOE implements a TLS trusted channel between itself and trusted external audit servers. The TOE also implements SSH and TLS/HTTPS trusted paths for secure remote administration.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the NDcPP to which it claims conformance for assumptions about the use of the TOE. The NDcPP defines several assumptions that only apply to the TOE in certain circumstances; within the context of this ST, the A.COMPONENTS_RUNNING assumption does not apply because the TOE is a standalone device, and the assumptions for vNDs all apply because the TOE includes a virtual network device model.

The assumptions drawn from the PP are:

- The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security 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 cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does 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. For vNDs, this assumption applies to the physical platform on which the VM runs.
- 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). In the case of vNDs, the virtualization system (VS) is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.
- 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 ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
- 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 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. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
- 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.

- The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
- 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.
- The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
- The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
- For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

5.2 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 shows only that the evaluated configuration meets the security claims made, with a certain level of assurance, achieved through performance by the evaluation team of the evaluation activities specified in the following documents:
  - *Evaluation Activities for Network Device cPP, Version 2.2,* December 2019 ([8])
- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in the Fortinet FortiMail Security Target, Version 1.0, 19 April 2024 ([6]). Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- 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 TOE must be installed, configured and managed as described in the documentation referenced in Section 6 of this VR.

6 Documentation

The vendor offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- *Fortinet FortiMail 7.4 FIPS 140-3 and Common Criteria Technote, Version 0.2, July 17, 2024. [9]*
- *Fortinet FortiMail 7.4.1 CLI Reference, February 7, 2024. [13]*
- *Fortinet FortiMail 7.4.1 Administration Guide,* April 12, 2024. *[7]*

To use the product in the evaluated configuration, the product must be installed and configured as specified in *Fortinet FortiMail 7.4 FIPS 140-3 and Common Criteria Technote*. This document provides references to other documentation for specific steps to place the TOE into its evaluated configuration.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure the TOE as evaluated. Consumers can download the CCECG from the NIAP website and the remaining referenced documentation is available online via links provided in the Security Target or from Section 1.3 of the CCECG.

7 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary document:

- *Fortinet FortiMail Version 7.4 Common Criteria Test Report and Procedures for Network Device collaborative PP, Version 2.2e, Version 1.0, 09 May 2023.* ([12])

A non-proprietary description of the tests performed and their results is provided in the following document:

- *Assurance Activities Report for Fortinet FortiMail Version 7.4, Version 1.1, July 17, 2024.* ([11])

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the following specifications:

- *collaborative Protection Profile for Network Devices,* Version 2.2e, 23 March 2020

The evaluation team devised a test plan based on the test activities specified in the PP. The test plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the test plan and documented the results in the team test report listed above.

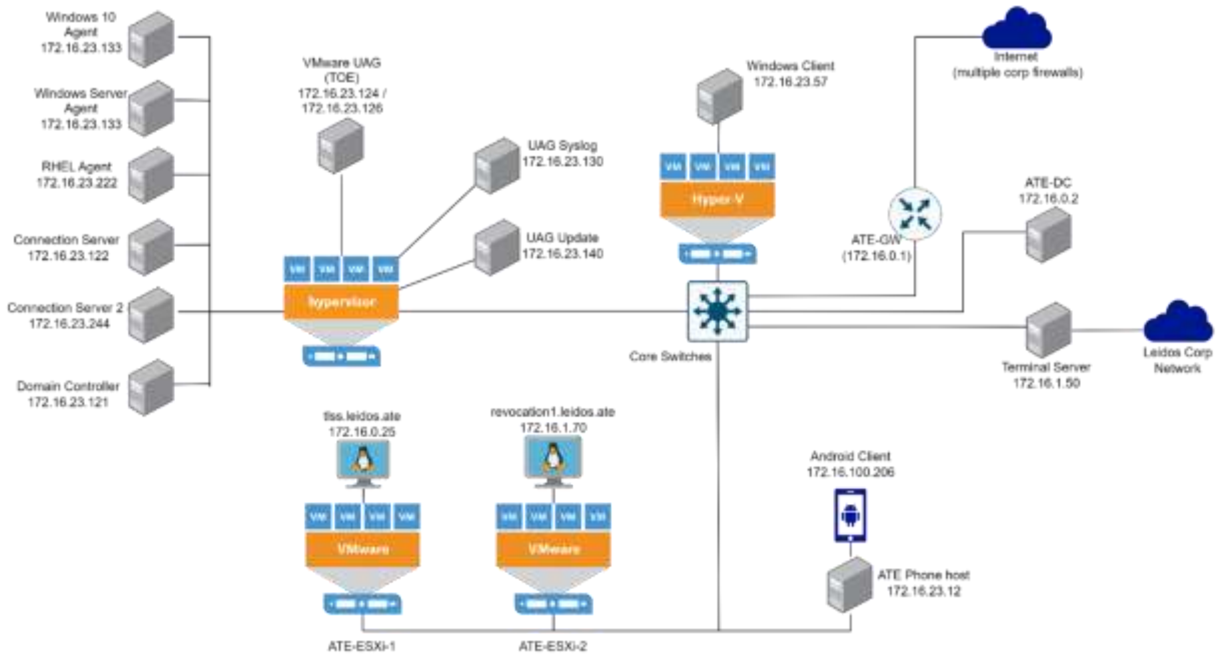
Independent testing took place at Leidos CCTL facilities in Columbia, Maryland, from May 2, 2022 to July 1, 2024.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the team test plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *collaborative Protection Profile for Network Devices* were fulfilled.

7.1 Test Configuration

This section identifies the devices used for testing the TOE and describes the test configuration. The test configuration is described below:


Windows 10 Agent 172.16.23.133
Windows Server Agent 172.16.23.133
RHEL Agent 172.16.23.222
Connection Server 172.16.23.122
Connection Server 2 172.16.23.244
Domain Controller 172.16.23.121
VMware UAG (TOE) 172.16.23.124 / 172.16.23.126
UAG Syslog 172.16.23.130
UAG Update 172.16.23.140
VM
hypervisor
Windows Client 172.16.23.57
Hyper-V
Internet (multiple corp firewalls)
ATE-GW (172.16.0.1)
ATE-DC 172.16.0.2
Core Switches
Terminal Server 172.16.1.50
Leidos Corp Network
tlss.leidos.ate 172.16.0.25
revocation1.leidos.ate 172.16.1.70
VMware
Android Client 172.16.100.206
ATE Phone host 172.16.23.12
ATE-ESXi-1
ATE-ESXi-2

The following components were used to create the test configurations:

VMware Hypervisor
Purpose: TOE host
IP / MAC: 172.16.23.232 / 78:AC:44:41:B7:68
ESXi Version: 7.0

Hyper-V
Purpose: Hosting server
IP / MAC: 172.16.50.10 / DC:F4:01:E8:60
Version: Windows Server Datacenter 10.0.1836

ATE Phone Host server
Purpose: Virtualization server
IP / MAC: 172.16.23.12 / 8C:AE:4C:E1:70:84
Version: Windows 10 Professional

VMware Connection Server
Purpose: Client device to TOE
IP / MAC: 172.16.23.122 / 00:50:56:88:36:BC
Version: 2209.1

VMware Connection Server 2
Purpose: Secondary client device to TOE
IP / MAC: 172.16.23.224 / 00:50:56:A7:A7:17
Version: 2209.1

Domain Controller
Purpose: Domain Controller for local network
IP / MAC: 172.16.23.224 / 00:50:56:88:26:bc
Version: Windows Server 2019

VMware Windows Client
Purpose: Client device to TOE

IP / MAC: 172.16.23.57 / 8C:AE:4C:E1:70:84
Version: 2209.1

VMware Android Client
Purpose: Client device to TOE
IP / MAC: 172.16.100.206 / BE:C6:70:E3:22:8B
Phone model: Galaxy S10 5G
OS: Android 11

Windows 10 Agent
Purpose: Networked device for TOE
IP / MAC: 172.16.23.131 / 00:50:56:88:69:92
Version: 2209.1
ESXi Version: 7.0.2

Windows Server Agent
Purpose: Networked device for TOE
IP / MAC: 172.16.23.133 / 00:0C:29:52:6B:B4
Version: 2209.1
ESXi Version: 7.0.2

RHEL Agent
Purpose: Networked device for TOE
IP / MAC: 172.16.23.222 / 00:0C:29:A):F4:04
Version: 2209.1
ESXi Version: 7.0.2

ATE-GW (Physical)
Purpose: Main router/gateway
IP/ MAC: 172.16.0.1 / ac:1f:6b:95:0c:1d
OS: PfSense 2.4.4-RELEASE-p2

ATE-DC (Physical)
Purpose: Main Domain Controller (DC) for Test environment/DNS server
IP /MAC: 172.16.0.2 / 00:22:19:58:EB:8D
OS: Windows Server 2016 version 1607
Protocols used: RDP, DNS

ATE-ESXi-1 (Physical)
Purpose: Virtualization server
IP/ MAC: 172.16.1.62 / 10:7b:44:92:77:bf
OS: VMware ESXi, 6.5.0, 5969303

Terminal Server (Physical)
Purpose: Provide tester access to the Test Environment from corporate network.
IP/MAC: 172.16.1.50 / D4:BE:D9:B4:FE:66
OS: Windows server 2016 version 1607
Protocols used: RDP

TLSS.leidos.ate (VM)
Purpose: Hosts TLS Test Tools
IP/MAC: 172.16.0.25 / 00:50:56:b1:66:0b
OS: Ubuntu 18.04.5
Protocols Used: TLS
Relevant Software:
Proprietary Python TLS test tools
OpenSSL 1.1.1

Wireshark 2.6.10

Revocation server

Purpose: CRL distribution

IP/MAC: 172.16.1.70 / 00:50:56:B1:A0:FC

OS: Ubuntu 18.04.5

Relevant Software:

Apache 2.4.29

UAG-Update

Purpose: Update repository

IP/MAC: 172.16.23.140 / 00:50:56:A7:97:9A

OS: Photon 3

Relevant Software:

Apache 2.4.55

UAG-Syslog

Purpose: Syslog machine

IP/MAC: 172.16.23.140 / 00:50:56:A7:FB:B2

OS: Photon 3

Relevant Software:

Syslog-ng 3.37.1

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The Target of Evaluation (TOE) is Fortinet FortiMail version 7.4. The specific tested firmware version is v7.4.3.

All functional testing was performed on the following devices:

- Physical device: FML-900F
- Virtual device: virtualized on VMware ESXi 8.0, Intel Xeon E5-2620v4 processor

Additionally, to ensure full coverage of all processor microarchitectures and substrates, cryptographic algorithm validation was performed on both models listed above as well as the FML-200F, FML-400F, and FML-2000F.

8.2 Excluded Functionality

The product is designed to function as a network security appliance that filters emails and associated executable content to prevent compromise of end user systems. No NIAP PP or PP-Module exists for this functionality, so the TOE conforms to the NDcPP for its implementation of general security mechanisms. As such, the security-relevant functionality of the product is limited to the claimed requirements in this standard. The security-relevant functionality is described in [ST] sections 2.3 and 2.4. The product overview in section 2.2 is intended to provide the reader with an overall summary of the entire product so that its intended usage is clear. The subset of the product functionality that is within the evaluation scope is subsequently described in the sections of the [ST] that follow it.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for Fortinet FortiMail Version 7.4 ([10]). The reader of this VR can assume that all evaluation activities and work units received passing verdicts.

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, revision 5 ([1], [2], [3]) and CEM version 3.1, revision 5 ([4]), and the specific evaluation activities specified in:

- *Evaluation Activities for Network Device cPP,* Version 2.2, December 2019 ([8])

The evaluation determined the TOE satisfies the conformance claims made in the Fortinet FortiMail Version 7.4 Security Target, of Part 2 extended and Part 3 Conformant. The TOE satisfies the requirements specified in the PPs listed above.

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS evaluation activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed PP, and security function descriptions that satisfy the requirements.

9.2 Evaluation of the Development (ADV)

The evaluation team performed each ADV evaluation activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed PP for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance evaluation activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC evaluation activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit, to the extent possible given the evaluation evidence required by the claimed PP. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team performed each test activity and applied each ATE_IND.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and recorded the results in the Test Report, summarized in the AAR.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA evaluation activity and applied each AVA_VAN.1 CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed PP. This comprised a search of public vulnerability databases.

The evaluation team performed a search of the following public vulnerability databases:

- National Vulnerability Database (https://nvd.nist.gov/)
- US-CERT (https://www.kb.cert.org/vuls/html/search)
- Fortinet's Product Security Incident Response Team (PSIRT) (https://www.fortiguard.com/psirt)

Searches were performed several times, most recently July 1

, 2024, using search terms that referenced the TOE itself, the processors that the physical TOE models use, the OS kernel version, the cryptographic library, and the list of additional third-party software components provided by the vendor.

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the assurance activities specified in the claimed PP. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope in section 5, the evaluated functionality is scoped exclusively to the SFRs specified in the Security Target, and the only evaluated functionality was that which was described by the SFRs claimed in the Security Target. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

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

11 Security Target

The ST for this product's evaluation is *Fortinet FortiMail Version 7.4 Security Target*, Version 1.0, April 19, 2024 ([6]).

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

AAR	Assurance Activity Report
CA	Certificate Authority
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
PCL	Product Compliant List
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VR	Validation Report
VS	Virtualization System

13 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.

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

[3] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017.

[4] Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.

[5] collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020.

[6] Fortinet FortiMail Version 7.4 Security Target, Version 1.0, April 19, 2024.

[7] Fortinet FortiMail 7.4.1 Administration Guide, April 12, 2024.

[8] Evaluation Activities for Network Device cPP, Version 2.2, December 2019.

[9] Fortinet FortiMail 7.4 FIPS 140-3 and Common Criteria Technote, Version 0.2, July 17, 2024.

[10] Evaluation Technical Report for Fortinet FortiMail Version 7.4, Version 1.0, May 29, 2024.

[11] Assurance Activities Report for Fortinet FortiMail Version 7.4, Version 1.1, July 17, 2024.

[12] Fortinet FortiMail Version 7.4 Common Criteria Test Report and Procedures for Network Device collaborative PP, Version 2.2e, Version 1.0, 09 May 2023.

[13] Fortinet FortiMail 7.4.1 CLI Reference, February 7, 2024.

[14] Fortinet FortiMail 7.4.1 Vulnerability Assessment Version 1.1, July 5, 2024