National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Palo Alto Networks WF-500 WildFire 10.1

Report Number: CCEVS-VR-VID11286-2022
Dated: August 4, 2022
Version: 1.0

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

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

Acknowledgements

Validation Team

Jenn Dotson

Randy Heimann

Lisa Mitchell

Linda Morrison

Chris Thorpe

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report 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 Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 3 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 Palo Alto Networks WF-500 appliance running WildFire 10.1 (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 applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of the Palo Alto Networks WF-500 WildFire 10.1 was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in August 2022.

The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, release 5 ([1], [2], [3], [4]) and activities specified in the following document:

- Evaluation Activities for Network Device cPP, Version 2.2, December 2019 ([6])

The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The product is a network appliance that receives samples sent to it by Palo Alto Networks Firewalls, and automatically detects and prevents zero-day exploits and malware with its on-premises analysis. The focus of the evaluation was on the product's conformance to the security functionality specified in the following document:

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

The security functions specified in this Protection Profile include protection of communications between the TOE and external IT entities, identification and authentication of administrators, auditing of security-relevant events, and ability to verify the source and integrity of updates to the TOE.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the Security Target ([7]). The information in this VR is largely derived from the Assurance Activities Report (AAR) ([12]) and the associated test report produced by the Leidos evaluation team ([11]).

The validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associated test report. The validation team found that the evaluation showed that the TOE satisfies all the security functional and assurance requirements stated in the ST. The evaluation also showed that the TOE is conformant to the claimed Protection Profile and that the evaluation activities specified in [6] had been performed appropriately. 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.

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 and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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 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).

The following table provides information needed to completely identify the product and its evaluation.

Table 1: Evaluation Details

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Evaluated Product:	Palo Alto Networks WF-500 WildFire 10.1
Sponsor & Developer:	Palo Alto Networks, Inc. 3000 Tannery Way Santa Clara, CA 95054
CCTL:	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date:	August 4, 2022
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM:	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
Protection Profiles:	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020
Disclaimer:	The information contained in this Validation Report is not an endorsement either expressed or implied of the TOE
Evaluation Personnel:	Anthony Apted, Greg Beaver, Justin Fisher, Kofi Owusu, Pascal Patin, Allen Sant
Validation Personnel:	Jenn Dotson, Randy Heimann, Lisa Mitchell, Linda Morrison, Chris Thorpe

3 Assumptions & Clarification of Scope

Assumptions

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

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

That information has not been reproduced here and the NDcPP22e 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 NDcPP22e as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

Clarification of scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the collaborative Protection Profile for Network Devices and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guides, additional customer documentation for the specific Network Device models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP22e and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

4 Architectural Information

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

The TOE is a hardware and software solution. The software comes pre-installed on the device and can be updated by downloading a new version from the Palo Alto Networks support site. The system consists of the following items: system software, database, linux-derived operating system, and the hardware. The database is a repository for audit logs, user logs, and system/configuration data. The system software contains necessary items to support the functionality of the device such as using OpenSSL/OpenSSH, and items necessary for management interfaces (CLI). The WildFire 10.1.6 software runs on top of the PAN-OS 10.1.6 operating system. PAN-OS 10.1 is an operating system derived from Linux kernel version 4.18.0 to enforce domain separation, memory management, disk access, file I/O, and communications with the underlying hardware components including memory, network I/O, CPUs, and hard disks. Only services and libraries required by the system software and DB are enabled in the OS.

The following diagram demonstrates the software and hardware architecture of the TOE.

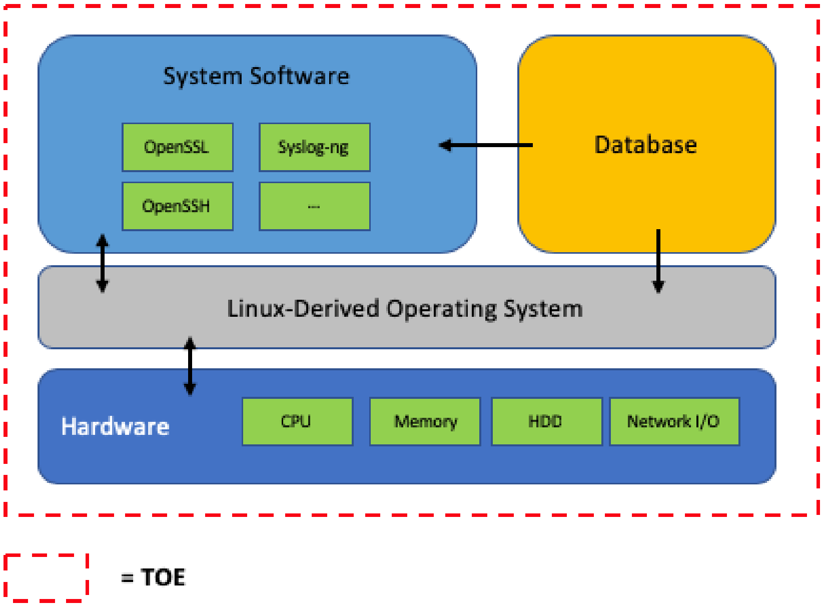

Figure 1 - TOE Architecture

4.1 Physical Boundaries

The TOE consists of the following components:

- Palo Alto Networks WF-500 hardware appliance
- WildFire 10.1 (running on top of PAN-OS 10.1): The software component that runs on the appliance

5 Security Policy

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

5.1 Security Audit

The TOE is designed to be able to generate logs for a variety of security relevant events including the events specified in NDcPP. The TOE can be configured to store the logs locally or can be configured to send the logs to a designated external log server.

5.2 Cryptographic Support

The TOE implements NIST validated cryptographic algorithms that provide key management, random bit generation, encryption/decryption, digital signature and cryptographic hashing and keyed-hash message authentication features in support of cryptographic protocols such as TLS and SSH. In order to utilize these features, the TOE must be configured in FIPS-CC mode.

5.3 Identification and Authentication

The TOE requires that all users that access the TOE be successfully identified and authenticated before they can have access to any security functions that are available in the TOE. The TOE offers functions through connections using SSH for administrators.

The TOE supports the local definition and authentication of administrators with username, password, SSH keys, and role that it uses to authenticate the operator. These items are associated with an operator and an authorized role for access to the TOE. The TOE uses X.509 certificates to support TLS authentication.

5.4 Security Management

The TOE provides access to the security management features using a Command Line Interface (CLI). CLI commands are transmitted over SSH for both local and remote connections. Security management commands are limited to administrators and only available after the operator has successfully authenticated themselves to the TOE. The TOE provides access to these services via direct RJ-45 Ethernet connection and remotely using an SSHv2 client. The product also includes a console port, but once FIPS-CC mode is enabled, the console port is disabled.

5.5 Protection of the TSF

The TOE implements features designed to protect itself, and to ensure the reliability and integrity of its security functions.

Stored passwords and cryptographic keys are protected so that unauthorized access does not result in sensitive data being lost, and the TOE also contains various self-tests so that it can detect if there are any errors with the system or if malicious activity has occurred. The TOE provides its own timing mechanism to ensure that reliable time information is present. The TOE uses digital signature mechanisms when performing trusted updates to ensure installation of software is valid and authenticated properly.

5.6 TOE Access

The TOE provides the ability for both TOE and user-initiated locking of the interactive sessions for the TOE termination of an interactive session after a period of inactivity is observed. Additionally, the TOE is able to display an advisory message regarding unauthorized use of the TOE before establishing a user session.

5.7 Trusted Path/Channels

The TOE protects interactive communication with remote administrators using SSH. Communications with other devices and services (such as a Syslog server) are protected using TLS and X.509 certificates to support TLS authentication.

6 Documentation

Palo Alto 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 each TOE model is as follows:

- WildFire Administrator's Guide Version 10.1, Last Revised: November 24, 2021 [8]
- WF-500 WildFire Appliance Hardware Reference Guide, February 29, 2016 [9]
- Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 10.1, Version 1.0, August 1, 2022 [10]

This is also provided for initial setup purposes. To use the product in the evaluated configuration, the product must be configured as specified in these guides.

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 or operate the device as evaluated. Consumers are encouraged to download the CC configuration guide (CCECG above) from the NIAP website.

7 Evaluated Configuration

The TOE is the Palo Alto Networks WF-500 with WildFire Version 10.1, as configured in accordance with the guidance documentation listed in Section 6 of this Validation Report. Specifically, version 10.1.6-h4 was used for testing. The WF-500 is the only TOE appliance model.

The TOE includes a "FIPS-CC" mode of operation. This mode must be enabled for the TOE to meet the claimed requirements.

7.1 Excluded Functionality

All product functionality that is not claimed by the Security Target as part of achieving exact conformance to the NDcPP is excluded from the evaluation scope. The product also has the following exclusions:

- Telnet and HTTP Management Protocols: Telnet and HTTP are disabled by default and cannot be enabled in the evaluated configuration. Telnet and HTTP are insecure protocols which allow for plaintext passwords to be transmitted. Use SSH and HTTPS only as the management protocols to manage the TOE.
- Online Certificate Status Protocol (OCSP): Use of OCSP is not covered by the evaluation. Only Certificate Revocation Lists (CRLs) are to be used for certificate revocation checking in the evaluated configuration.
- External Authentication Servers: The NDcPP does not require external authentication servers. The WildFire device optionally supports RADIUS authentication but this is not claimed in the evaluated configuration.
- Shell and Console Access: The shell and console access is only allowed for pre-operational installation, configuration, and post-operational maintenance and trouble shooting.
- Any features not associated with SFRs in claimed NDcPP: NDcPP forbids adding additional requirements to the Security Target (ST). If additional functionalities are mentioned in the ST, it is for completeness only.

8 Independent Testing

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

- *Palo Alto Networks WF-500 WildFire 10.1 Common Criteria Test Report and Procedures For Network Device collaborative PP Version 2.2e* [11]

A non-proprietary description of the tests performed by the evaluation team is provided in the following document:

- Assurance Activities Report for Palo Alto Networks WF-500 WildFire 10.1 [12]

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 *collaborative Protection Profile for Network Devices* [5].

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *Evaluation Activities for Network Device cPP* [6]. 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.

The evaluators received the TOE in the form that normal 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* [5] were fulfilled.

8.1 Test Configuration

The evaluated version of the TOE consists of Palo Alto WildFire version 10.1.6-h4 running on a WF-500 hardware appliance.

The TOE must be configured in accordance with the *WildFire Administrator's Guide* [8], *WF-500 WildFire Appliance Hardware Reference Guide* [9], and *Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 10.1* [10].

Per Policy Letter #22, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

8.2 Vulnerability Analysis

The evaluation team applied each AVA CEM work unit. The evaluation team searched the National Vulnerability Database (http://web.nvd.nist.gov/view/vuln/search) and several other public vulnerability repositories. Searches were performed on 7/13/2022 and repeated again on 8/3/2022.

The keyword searches included the following terms:

- Intel xeon e5-2620 (TOE processor)
- Sandy bridge (processor microarchitecture)

- PAN-OS 10.1 (TOE software platform)
- WildFire 10.1 (TOE software)
- Palo Alto Wildfire (vendor and product)
- Palo Alto Networks Wildfire (vendor and product variation)
- WF-500 (TOE hardware).

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.

Additionally, the evaluators performed fuzz testing of the TOE as specified in Section A.1.4 of Evaluation Activities for Network Device cPP, Version 2.2, December 2019. The evaluators observed the TOE did not react adversely to the packets directed at the TOE or respond to the packets. This testing did not discover any vulnerabilities in the TOE.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the following documents, in conjunction with Version 3.1, Revision 5 of the CC and CEM:

- *Evaluation Activities for Network Device cPP*, Version 2.2, December 2019 [6]

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

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 claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 2: TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing – conformance
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 10.1, Version 1.0, August 1, 2022. No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The ST for this product’s evaluation is *Palo Alto Networks WF-500 WildFire 10.1 Security Target*, Version 1.0, August 1, 2022 [7].

13 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

AAR	Assurance Activities Report
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PCL	Product Compliant List
PP	Protection Profile
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VR	Validation Report

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, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 5, April 2017

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017

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

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

[7] Palo Alto Networks WF-500 WildFire 10.1 Security Target Version 1.0, August 1, 2022

[8] WildFire Administrator’s Guide Version 10.1, Last Revised: November 24, 2021

[9] WF-500 WildFire Appliance Hardware Reference Guide, February 29, 2016

[10] Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 10.1, Version 1.0, August 1, 2022

[11] Palo Alto Networks WF-500 WildFire 10.1 Common Criteria Test Report and Procedures For Network Device collaborative PP Version 2.2e, Version 1.1, August 1, 2022

[12] Assurance Activities Report for Palo Alto Networks WF-500 WildFire 10.1, Version 1.0, August 3, 2022

[13] Palo Alto Networks WF-500 WildFire 10.1 Vulnerability Assessment, Version 1.1, August 3, 2022