National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Palo Alto Networks WF-500 WildFire 8.1.11

Report Number:	**CCEVS-VR-VID11032-2020**
Dated:	**30 January 2020**
Version:	**1.0**

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

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

Acknowledgements

Validation Team

Paul Bicknell, Senior Validator
Jenn Dotson, ECR Team
Sheldon Durrant, ECR Team
Linda Morrison, Lead Validator
The MITRE Corporation

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Palo Alto Networks WF-500 WildFire 8.1.11 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This Validation Report (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 Security Target (ST).

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 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. 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 of the Palo Alto Networks WF-500 WildFire 8.1.11 (WildFire) was performed by the Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in January, 2020. 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 the assurance activities specified in *Evaluation Activities for Network Device cPP*, Version 2.1, September 2018 [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 on specified hardware used to identify threats and shield computing infrastructure from network vulnerabilities, exploits, and known and zero-day attacks. The focus of the evaluation was on the product's conformance to the security functionality specified in the collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018 [5]

The security functions specified in the *collaborative Protection Profile for Network Devices*, Version 2.1 [NDcPP] 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 PP and, when installed, configured, and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the ST [7]. The technical information included in this VR is derived from the ST and analysis performed by the Validation team.

The Validation team provided guidance on technical issues and evaluation processes and reviewed the evaluation outputs produced by the Evaluation team, specifically, the Assurance Activity Report (AAR) [12] and associated test report [11]. 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 PP and that the evaluation activities specified in [6] had been performed appropriately. 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 (ETR) [13] 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), evaluate products against Protection Profiles (PP) with defined Assurance Activities (AA), which are interpretations of Common Methodology for IT Security Evaluation (CEM) work units specific to the technology described by the PP and in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of Information Technology (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, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The PP to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product:	Palo Alto Networks WF-500 WildFire 8.1.11
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:	23 January 2020
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 2.1, 24 September 2018
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 Kevin Steiner

Validation Personnel:	Paul Bicknell Jenn Dotson Sheldon Durrant Linda Morrison

3 Architectural Information

Note: The following architectural information is from the description provided in the ST.

The TOE is a hardware and software solution that is consists of the following components:

- Palo Alto Networks WF-500 hardware appliance
- WildFire 8.1.11: The software component that runs on the appliance

The operational environment includes the following:

- Syslog server
- Another Wildfire appliance for High Availability (HA)
- Palo Alto Networks Firewall or Panorama appliances
- Workstation
- SSHv2 client

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, operating system derived from kernel version 3.10.88, 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 operating system provides a customized Linux kernel 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.

4 Security Policy

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

4.1 Security Audit

The Palo Alto Networks WF-500 WildFire 8.1.11 is designed 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.

4.2 Cryptographic Support

The Palo Alto Networks WF-500 WildFire 8.1.11 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 IPsec, TLS, and SSH. In order to utilize these features, the TOE must be configured in FIPS-CC mode.

4.3 Identification and Authentication

The Palo Alto Networks WF-500 WildFire 8.1.11 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 Palo Alto Networks WF-500 WildFire 8.1.11 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.

4.4 Security Management

The Palo Alto Networks WF-500 WildFire 8.1.11 provides access to the security management features using the 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 himself or herself 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 enabled, the console port is disabled.

4.5 Protection of the TSF

The Palo Alto Networks WF-500 WildFire 8.1.11 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.

4.6 TOE Access

The Palo Alto Networks WF-500 WildFire 8.1.11 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.

4.7 Trusted Path/Channels

The Palo Alto Networks WF-500 WildFire 8.1.11 protects interactive communication with remote administrators using SSH and protects communication between itself and other WildFire devices using IPsec. Communication with other devices and services (such as a Syslog server) are protected using TLS.

5 Assumptions, Threats and Clarification of Scope

5.1 Assumptions

The assumptions are drawn directly from the NDcPP.

5.2 Threats

The threats are drawn directly from the NDcPP.

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 evaluation activities specified in *Evaluation Activities for Network Device cPP* [6] and performed by the Evaluation team).
- This evaluation covers only the specific device model and software version identified in this document, and not any earlier or later versions released or in process. Only the WF-500 on-premise hardware appliance was evaluated; per NIAP TD0407, cloud deployments of WildFire are not within the evaluation scope.
- The evaluation of security functionality of the product was limited to the functionality specified in the Security Target [7], in the NDcPP and applicable Technical Decisions. Any additional security related functional capabilities included in the product were not covered by this evaluation.
    - In a deployment architecture, the WildFire appliance receives traffic samples from other Palo Alto firewall and Panorama devices to analyze them for potential malware and zero-day exploitation. However, since these devices are in the TOE's operational environment, these capabilities (i.e. stateful inspection filtering, IPsec VPN gateway, IPS/IDS threat prevention) were not subject to evaluation. Only the trusted communication channels from WildFire to these external devices are claimed.
- The TOE appliances consist of software and hardware and do not rely on the operational environment for any supporting security functionality.
- 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 7 of this Validation Report.

6 TOE Evaluated Configuration

6.1 Evaluated Configuration

The TOE is the Palo Alto Networks WF-500 WildFire Version 8.1.11, as configured in accordance with the guidance documentation listed in Section 7 of this Validation Report. 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.

6.2 Excluded Functionality

All product functionality that is not claimed by the ST as part of achieving exact conformance to the NDcPP is excluded from the evaluation scope.

7 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 the TOE is as follows:

- WildFire Administrator's Guide Version 8.1, December 5, 2018 [8]
- WF-500 Appliance Hardware Reference Guide, February 29, 2016 [9]
- Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire v8.1, Version 1.10, January 3, 2020 [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.

8 Independent Testing

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

- *Palo Alto WildFire Common Criteria Test Report and Procedures for Network Device collaborative PP Version 2.1* [11]

A non-proprietary version of the tests performed and samples of the evidence that was generated is summarized in the following document:

- *Assurance Activities Report for Palo Alto Networks WF-WildFire v8.1.11* [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 the Palo Alto Networks WF-500 WildFire 8.1.11, which claims conformance to the *collaborative Protection Profile for Network Devices* [5].

The Evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the *collaborative Protection Profile for Network Devices* [5]. 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 standard 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 the *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 8.1.11 running on a WF-500 hardware appliance.

The TOE must be deployed as described in Section 5.1 of this Validation Report and be configured in accordance with the *WildFire Administrator's Guide* [8], *WF-500 Appliance Hardware Reference Guide* [9], and *Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire v8.1* [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 performed a vulnerability analysis following the processes described in the claimed PP and using the flaw-hypothesis methodology. This included a search of public vulnerability databases and development of Type 3 flaw hypotheses in accordance with Section A.3 of [6]. These searches were performed during the evaluation on October 2 and 16, 2019, November 14, 2019, and January 13, 2020. Full results and analysis were documented in [14].

The evaluation team searched the National Vulnerability Database (http://web.nvd.nist.gov/view/vuln/search) and the Palo Alto Security Advisories page (https://securityadvisories.paloaltonetworks.com).

The keyword searches included the following terms:

- Microarchitectural (category of processor vulnerability)
- Xeon (processor type)
- Palo Alto (vendor)
- WildFire (TOE name)
- WF-500 (TOE hardware)
- PAN-OS (TOE software platform)
- TCP (required by [6]
- SSH (supported protocol)
- TLS (supported protocol)
- IPsec (supported protocol)
- Linux 3.10 (OS kernel that PAN-OS is derived from)

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 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 2.1, September 2018 [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 PP, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the ETR [13], 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 suggests that the consumer pay particular attention to the evaluated configuration of the products(s). The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST, and only the functionality implemented by the SFR's within the ST was evaluated. All other functionality provided by the product(s), to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about the effectiveness of the additional functionality.

Consumers employing the devices must follow the configuration instructions provided in the Users Guidance documentation listed in Section 7 to ensure the evaluated configuration is established and maintained.

11 Annexes

Not applicable

12 Security Target

The ST for this product's evaluation is *Palo Alto Networks WF-500 WildFire 8.1.11 Security Target*, Version 1.0, January 3, 2020 [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
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 2.1, 24 September 2018

[6] Evaluation Activities for Network Device cPP, Version 2.1, September 2018

[7] Palo Alto Networks WF-500 WildFire 8.1.11 Security Target Version 1.0, January 3, 2020

[8] WildFire Administrator's Guide Version 8.1, December 5, 2018

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

[10] Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire v8.1, Version 1.10, January 3, 2020

[11] Palo Alto WildFire Common Criteria Test Report and Procedures for Network Device collaborative PP Version 2.1, Version 1.2, January 13, 2020

[12] Assurance Activities Report for Palo Alto Networks WF-500 WildFire v8.1.11, Version 1.1, January 13, 2020.

[13] Evaluation Technical Report for Palo Alto Networks WF-500 WildFire v8.1.11, Version 1.2, January 13, 2020

[14] Palo Alto Networks WF-500 WildFire v8.1.11 Vulnerability Assessment, Version 1.3, January 13, 2020