National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Palo Alto Networks WF-500-B Appliance running WildFire 11.1

Report Number: CCEVS-VR-VID11479-2025
Dated: 29 October 2025
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 Meade, MD 20755-6982

Acknowledgements

Validation Team

Lisa Mitchell

Linda Morrison

Jaemond Reyes

Sheldon Durrant

Randy Heimann

The MITRE Corporation

Common Criteria Testing Laboratory

Leidos Inc.

Columbia, MD

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 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 Palo Alto Networks WF-500-B Appliance running WildFire 11.1 (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 TOE was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in October 2025.

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 documents:

- *Evaluation Activities for Network Device cPP*, Version 3.0e, 6 December 2023 [6]
- *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021 [7]

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 TOE provides detection and prevention of zero-day malware using a combination of dynamic and static analysis to detect threats and create protections to block malware. The WF-500-B appliance extends the capabilities of Palo Alto Networks' Next Generation Firewalls by receiving network traffic samples to identify and block targeted and unknown malware. The focus of the evaluation was on the product's conformance to the security functionality specified in the following documents:

- *collaborative Protection Profile for Network Devices*, Version 3.0e, 6 December 2023 ([NDcPP], [5])
- *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021 ([SSHPKG], [7])

The security functions specified in this collaborative Protection Profile and Functional Package 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 Functional Package, and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the Security Target [8]. The information in this VR is largely derived from the Assurance Activities Report (AAR) ([12]) and the associated test report ([13]) produced by the Leidos evaluation team.

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 Functional Package, and that the evaluation activities specified in [6] and [7] had been performed appropriately. 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) ([16]) 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 Identifiers

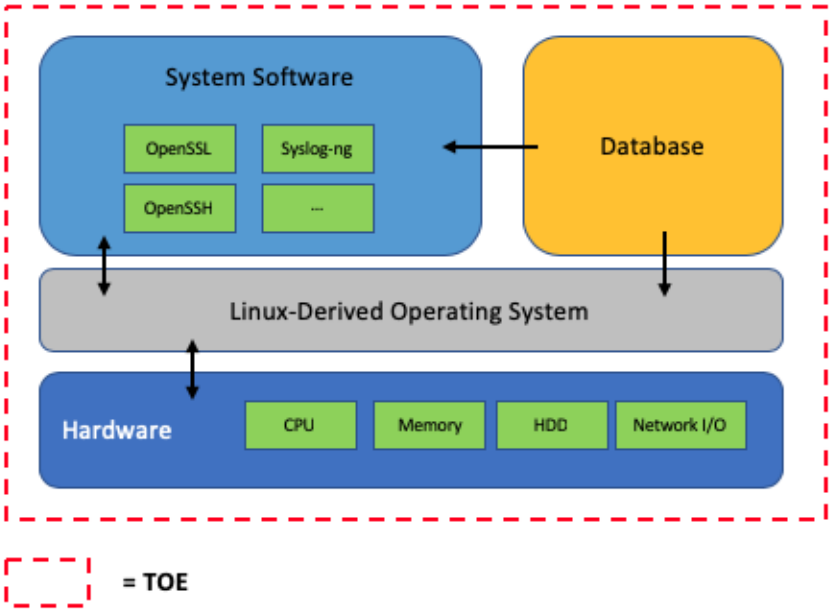
Evaluated Product:	Palo Alto Networks WF-500-B Appliance running WildFire 11.1
Sponsor & Developer:	Palo Alto Networks, Inc. 3000 Tannery Way Santa Clara, CA 95054
CCTL:	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date:	29 October 2025
ST:	*Palo Alto Networks WF-500-B Appliance running WildFire 11.1 Security Target, Version 1.0, October 22, 2025*
ETR:	*Evaluation Technical Report for Palo Alto Networks WF-500-B Appliance WildFire 11.1, Version 1.0, October 22, 2025*
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 3.0e, 6 December 2023 *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021
Conformance Result:	CC Part 2 extended; CC Part 3 conformant

Evaluation Personnel:	Justin Fisher Anthony Apted Greg Beaver Josh Marciante Allen Sant
Validation Personnel:	Lisa Mitchell Linda Morrison Jaemond Reyes Sheldon Durrant Randy Heimann

3 TOE Architecture

The TOE is a hardware and software solution consisting of the Palo Alto Networks WF-500-B hardware appliance running WildFire 11.1 software. 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 11.1 software runs on top of the PAN-OS 11.1 operating system. PAN-OS 11.1 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.



The TOE in its evaluated configuration requires the following components in its operational environment:

- Syslog server
- Palo Alto Networks Firewall appliances
- Workstation
    - SSHv2 client

Additional detail regarding the evaluated configuration is provided in Section 8 below.

4 Security Policy

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

4.1 Security Audit

The TOE is designed to be able to generate logs for a variety of security relevant events including the events specified in the claimed Protection Profile and Functional Package. 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 TOE implements NIST-validated cryptographic algorithms that provide key management, random bit generation, encryption/decryption, digital signature generation and verification, cryptographic hashing, and keyed-hash message authentication features in support of higher-level cryptographic protocols, including SSH and TLS.

4.3 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. In the evaluated configuration, the syslog connection implements OCSP for status verification for the certificate. The connection to the firewalls can use either CRLs or OCSP.

4.4 Security Management

The TOE provides access to its security management features using the CLI. CLI commands are transmitted over SSH for secure 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 using an SSHv2 client. The product also includes a console port, but once FIPS-CC mode is enabled, the console port is disabled.

4.5 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 implements 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 TOE provides the ability for both TOE and user-initiated termination of interactive sessions and 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 TOE protects interactive communication with administrators using SSH. Communication with other devices and services (such as a Syslog server) are protected using TLS and X.509 certificates to support TLS authentication.

5 Assumptions and Clarification of Scope

5.1 Assumptions

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

- *collaborative Protection Profile for Network Device*, Version 3.0e, 6 December 2023 [NDcPP]
- *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021 [SSHPKG]

That information has not been reproduced here and the NDcPP/SSHPKG should be consulted if there is interest in that material.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP/SSHPKG as described for this TOE in the ST. 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.

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 NDcPP with the SSHPKG 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.
- The evaluation of security functionality of the product was limited to the functionality specified in *Palo Alto Networks WF-500-B Appliance running WildFire 11.1 Security Target*, Version 1.0, October 22, 2025 [8]. Section 2.4 of [8] lists the specific features that were excluded from the evaluation.
- The TOE appliance consists of software and hardware and does 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 6 of this Validation Report.

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:

- Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 11.1, Revision Date: October 22, 2025 [9]
- *WildFire Appliance Administration*, Version 11.1, 23 August 2023 [10]
- *WF-500-B Appliance Hardware Reference*, March 21, 2023 [11].

These are 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 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 IT Product Testing

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

- *Palo Alto WildFire 11.1 Common Criteria Test Report and Procedures for Network Device collaborative PP Version 3.0e*, Version 1.0, October 22, 2025 [13]

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

- *Assurance Activities Report for Palo Alto Networks WF-500-B Appliance running WildFire 11.1*, Version 1.0, October 22, 2025 [12]

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

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] and *Functional Package for Secure Shell (SSH)* [7].

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *Evaluation Activities for Network Device cPP* [6] and *Functional Package for Secure Shell (SSH)* [7]. 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 August 2024 to September 2025.

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.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The evaluated version of the TOE consists of Palo Alto WildFire 11.1running on the WF-500-B appliance.

Evaluated functionality is scoped exclusively to the security functional requirements specified in ST. The TOE must be deployed as described in the ST and be configured in accordance with the *Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 11.1* [9].

Per NIAP Scheme 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 Excluded Functionality

The following functionality is excluded from the evaluation.

Feature	Description
Telnet Protocol	Telnet is disabled by default and cannot be enabled in the evaluated configuration. Telnet is insecure protocols which allow for plaintext passwords to be transmitted. Use SSH only as the management protocols to manage the TOE.
HTTP	HTTP is disabled by default and cannot be enabled in the evaluated configuration.
External Authentication Servers	The WildFire appliance supports the optional use of RADIUS as an authentication server, but this is not claimed in the TOE's evaluated configuration.
WildFire Cloud	Other deployments of WildFire are cloud-based and not within the scope of this evaluation.
Shell and Console Access	The shell and console access is only allowed for pre-operational installation, configuration, and post-operational maintenance and troubleshooting.
Any features not associated with SFRs in claimed [NDcPP] and [SSHPKG]	[NDcPP] and [SSHPKG] forbids adding additional requirements to the Security Target (ST). If additional functionalities are mentioned in the ST, it is for completeness only.

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 3.0e, December 6, 2023 [6]
- *Functional Package for Secure Shell (SSH) Version 1.0*, May 13, 2021 [7].

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.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Palo Alto Wildfire v11.1 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validation team 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 the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST and Guidance documents. Additionally, the evaluation team performed the assurance activities specified in the NDcPP/SSHPKG related to the examination of the information contained in the TSS.

The validation team 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.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validation team 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.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validation team 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 the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDcPP/SSHPKG and recorded the results in a Test Report, summarized in the AAR.

The validation team 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.

9.6 Vulnerability Analysis

The evaluation team performed a vulnerability analysis following the processes described in the claimed Protection Profiles 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].

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)
- Tipping Point Zero Day Initiative (https://www.zerodayinitiative.com/advisories/published/)
- Palo Alto Networks Security Advisories (https://security.paloaltonetworks.com/).

The evaluators performed these searches most recently on October 2, 2025.

The evaluation team applied the search criteria specified in [6] as follows:

- The list of software and hardware components that comprise the TOE:
    - Processor:
        - Intel Xeon Silver 4316
    - The processor is based on the following microarchitecture:
        - Ice Lake

  - Software:
    - WildFire 11.1
    - PAN-OS 11.1
    - Palo Alto Networks Crypto Module 11
    - Linux 4.18.0
    - OpenSSL
    - OpenSSH

- "Palo Alto WildFire", "Palo Alto Networks WildFire", and "WF-500-B" as variations of the TOE name.

The evaluation team 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. 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 performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the instructions in the Guidance documents defined in Section 6 and any additional guidance that it references. 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 ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness. Specifically, Section 8.2 defines functionality that was excluded from or not allowed in the evaluated configuration.

Evaluation activities are strictly bound by the assurance activities described in the Evaluation Activities for Network Device cPP, Version 3.0e and Functional Package for Secure Shell (SSH) v1.0. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

Per NIAP Scheme 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.

11 Security Target

The ST for this product's evaluation is Palo Alto Networks WF-500-B Appliance running WildFire 11.1 Security Target, Version 1.0, October 22, 2025 [8].

12 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
CCECG	Common Criteria Evaluated Configuration Guide
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface
CM	Configuration Management
CPU	Central Processing Unit
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
PC	Personal Computer
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

13 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, 00 April 2017

[5] collaborative Protection Profile for Network Devices, Version 3.0e, December 6, 2023

[6] Evaluation Activities for Network Device cPP, Version 3.0e, December 6, 2023

[7] Functional Package for Secure Shell (SSH), Version 1.0, May 13, 2021

[8] Palo Alto Networks WF-500-B Appliance running WildFire 11.1 Security Target, Version 1.0, October 22, 2025

[9] Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 11.1, Revision Date: October 22, 2025

[10] WildFire Appliance Administration, Version 11.1, 23 August 2023

[11] WF-500-B Appliance Hardware Reference, March 21, 2023

[12] Assurance Activities Report for Palo Alto Networks WF-500-B Appliance running WildFire 11.1, Version 1.0, October 22, 2025

[13] Palo Alto Wildfire 11.1 Common Criteria Test Report and Procedures for Network Device collaborative PP Version 3.0e, Version 1.0, October 22, 2025

[14] Palo Alto Networks WF-500-B Appliance running WildFire 11.1 Vulnerability Assessment, Version 1.0, October 22, 2025

[15] Palo Alto Networks Flaw Remediation Procedures, Version 0.1, November 14, 2023

[16] Evaluation Technical Report for Palo Alto Networks WF-500-B Appliance WildFire 11.1, Version 1.0, October 22, 2025