Palo Alto Networks

Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 11.0

Revision Date: August 11, 2023

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Table of Contents

1 Introduction

The WildFire appliance provides an on-premise WildFire private cloud, enabling the analysis of suspicious files in a sandbox environment without requiring the deployed Palo Alto Networks firewall to send files out of network. The WildFire appliance can be configured to host a WildFire private cloud where the firewall is configured to submit samples to the local WildFire appliance for analysis. The WildFire appliance sandboxes all files locally and analyzes them for malicious behaviors using the same engine the WildFire public cloud uses.

This guidance only covers the WildFire physical appliance. The Palo Alto Networks next-generation firewalls appliances were evaluated separately, and the documentation is provided in separate documents. Any information about them provided here is only for completeness.

The Palo Alto next-generation firewalls are network firewall appliances and virtual appliances on specified hardware used to manage enterprise network traffic flow using function-specific processing for networking, security, and management. The next-generation firewalls let the administrator specify security policies based on an accurate identification of each application seeking access to the protected network. The next-generation firewall uses packet inspection and a library of applications to distinguish between applications that have the same protocol and port, and to identify potentially malicious applications that use non-standard ports.

This document provides administrative guidance for the WildFire appliance and is a supplement to the Palo Alto Networks WildFire Administrator's Guide Version 11.0. This document describes procedures on how to prepare and operate the WildFire appliance to meet its Common Criteria evaluated configuration and is referred to as the operational user guide in the Network Device collaborative Protection Profile (NDcPP) v2.2e that meets all the required guidance assurance activities from the NDcPP.

1.1 Common Criteria (CC) Evaluated Configuration

The following sections describe the scope of evaluation, required configuration, assumptions, and operational environment that the system must be in to ensure a secure deployment. To ensure the system is in the CC evaluated configuration, the administrators must do the following:

- Configure all the required settings and default policies as documented in this guide.
- Disable all the features that would violate the NDcPP requirements or would make the system vulnerable to attacks as documented in this guide.
- Ensure all the environmental assumptions in section 2 are met.
- Ensure that your operational environment is consistent with section 2.
- Follow the guidance in this document.

After FIPS-CC mode has been enabled, the user is required to register and license the device as needed for the capabilities to be operational.

The operational guidance and evaluated configuration only relate to the functionality in the claimed Protection Profile. No other functionality is assured by the CC evaluation process.

Scope of Evaluation

The list below identifies features or protocols that are not evaluated or must be disabled, and the rationale why. Note that this does not mean the features cannot be used in the evaluated configuration (unless explicitly stated so). It means that the features were not evaluated and/or validated by an independent third party and the functional correctness of the implementation is vendor assertion. Evaluated functionality is scoped exclusively to the security functional requirements specified in the Security Target. In particular, only the following protocols implemented by the TOE have been tested, and only to the extent specified by the security functional requirements: TLS and SSH. The features below are out of scope.

Feature	Description
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	CRL (not OCSP) is to be used in the evaluated configuration.
External Authentication Servers	The NDcPP does not require external authentication servers.
Shell and Console Access	The shell and console access are 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.

Table 1: Feature Table

1.2 TOE References

Model	Description	Version
Physical WF-500 and WF-500-B	Palo Alto Networks WildFire WF-500 and WF-500-B Appliances	11.0.2

Table 2: TOE Reference

Documentation References

The Palo Alto Networks System documentation set includes online help and PDF files.

The following product guidance documents are provided online or by request:

- WildFire Administrator's Guide Version 11.0, Last Revised: See Below
  https://docs.paloaltonetworks.com/advanced-wildfire/wildfire-appliance

- WF-500 WildFire Appliance Hardware Reference Guide, Last Revised: See Below
  https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/hardware/wf-500/wf-500-hardware-reference-guide.pdf

- WF-500-B WildFire Appliance Hardware Reference Guide, Last Revised: See Below
  https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/hardware/wf-500-b/wf-500-b-appliance-hardware-reference.pdf

- Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for WildFire 11.0 [This Document]

The most up-to-date versions of the documentation can be accessed on the Palo Alto Networks Support web site (https://support.paloaltonetworks.com) or Technical Documentation (https://docs.paloaltonetworks.com/).

2 Operational Environment

This section describes the non-TOE components in the environment and assumptions made about the environment.

2.1 Non-TOE Components

The operational environment includes the following:

- Syslog server,
- Palo Alto Networks firewalls appliances
- Workstation
    - SSHv2 client

2.2 Environmental Security Objectives

The assumptions state the specific conditions that are expected to be met by the operational environment and/or administrators.

Table 3: Environment Security Objectives and Responsibility

Environment Security Objective	Operational Environment Security Objective Definition	Administrator Responsibility
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	Administrators must ensure the system is installed and maintained within a secure physical location. This can include a secured building with key card access or within the physical control of an authorized administrator in a mobile environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	Administrators must not add any general-purpose computing capabilities (e.g., compilers or user applications) to the system.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.	Administrators must configure the security devices that are managed by the TOE to secure the network.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.	Administrators must be properly trained in the usage and proper operation of the system and all the enabled functionality. These administrators must follow the provided guidance.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	Administrators must regularly update the system to address any known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.	Administrators must protect their access credentials where ever they may be.

Environment Security Objective	Operational Environment Security Objective Definition	Administrator Responsibility
OE.RESIDUAL_INFORMATION	The Security Administrator ensures 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.	Administrators must follow the proper electronic equipment disposal policy to ensure all sensitive information are wiped off the TOE prior to deactivation and removal from the network.

3 Before Installation You Must

Before you install your appliance in the evaluated configuration, Palo Alto Networks requires that the administrators **must** consider the following:

- Verify the delivery of Palo Alto Networks appliances from the trusted carrier and check the shipping containers for any sign of tampering. If tampering is found, please contact Support.
- Install the Palo Alto Networks appliances in a lockable rack within a secure location that prevents access by unauthorized personnel.
- Allow only trained and qualified personnel to install, replace, administer, or service the Palo Alto Networks appliances.
- Always connect the management interface to a secure internal management network that is protected from unauthorized access. This management interface is physically separate from the data interface.
- Identify the specific management workstation IP addresses that can be allowed to access appliances. Restrict access to the appliance to only those specific hosts using the Permitted IP feature in the Management Interface Settings.
- Connect the management interface of any managed devices to the same protected internal network as the TOE. This allows the administrators to securely control the device from the TOE and aggregate the event data generated on the managed device's network segment.
- By default, several ports are open to allow the TOE to take advantage of additional features and functionality. The following table lists these ports.

Ports	Description	Protocol	Direction	Open the port to …
22	SSH	TCP	Bidirectional	Allow a secure remote connection to the appliance.
161, 162	SNMP	UDP	Bidirectional (161); Outbound (162)	Provide access if you enabled SNMP polling (inbound) and SNMP traps (outbound).
514 6514	SYSLOG SYSLOG over TLS	UDP TCP	Outbound Outbound	Send logs to a remote syslog server. The remote syslog server must allow port 6514 to be opened.
443 10443	TLS	TCP TCP	Bidirectional	Firewall connection for sample submission

Table 4: Port and Description

4 Required Auditable Events

This section lists and describes the audit events generated by the TOE to meet the NDcPP auditing requirements. In addition, this section describes the format, syntax, and content of these audit logs.

The audit trail generated by the TOE consists of several logs, which are locally stored in the file system on the hard disk. The two main logs are the following:

- Configuration logs — Record events such as when an administrator configures the security policies, and when an administrator configures which events are audited.
- System logs — Record user login and logout, system and session information.

The TOE generates an audit event for each user interaction with the CLI command executed. Each event includes at least a timestamp, the username of the user whose action generated the event, a source IP, and message describing the event. The common fields are described in the tables below. The TOE has an internal log database that can be used to store and review audit records locally. Once the audit log is full, the newest audit data will overwrite the oldest audit data.

Configuration Logs

Field	Description
Generate Time	Time and date that the appliance generated the audit record.
Administrator	User name of the user that triggered the audit event.
Host	IP address of the host used by the user.
Client	CLI
Command	The command executed such as view, set, or commit.
Result	The result of the command.
Configuration Path	If applicable, the configuration path of the command. For the CLI, it is the actual command executed.
Full Path	If applicable, the full configuration path of the command.
Before Change	If applicable, the old configuration values or settings.
After Change	The new configuration values or settings.
Sequence Number	The sequence number of the command.
Device SN	The device serial number that the command executed on.
Device Name	The device name that the command executed on.

Table 5: Configuration Logs

System Logs

Field	Description
Generate Time	Time and date that the appliance generated the audit record.
Type	The event type such as general, tls, ssh, auth, etc.
Severity	The severity of the event.
Event	The high-level identification of the event.
Object	If applicable, the object accessed or modified as part of the event.
Description	The detailed description of the event. This may include IP address, result of event, etc.
Device SN	The device serial number that the event occurred on.
Device Name	The device name that the event occurred on.

Table 6: System Logs

SFR	Required Audit Event [Required Content]	Actual Audit Event - '*Description*' Only	Type
FAU_GEN.1	Start-up and shut-down of audit functions ***Note**: The audit function cannot be disabled. To stop the audit function, you must shutdown the whole system.*	Startup *The system is starting up.* Shutdown *System restart requested by <Username>* *The system is shutting down due to CLI Initiated.*	System
FAU_GEN.1	Administrator login and logout [Username]	See FIA_UIA	System
FAU_GEN.1	Changes to TSF data related to configuration changes [What has changed]	See FMT_SMF	Config

FAU_GEN.1	Generating/import of, changing, deleting of cryptographic keys [Unique key name or reference]	See FMT_SMF.1 **Note:** Some config logs need to be exported from device (via SCP or sent to Syslog server) to see detailed message(s)	System/ Config
FAU_GEN.1	Resetting passwords [Username]	On CLI (SSH): *Password changed for user <Username>*	System
FCS_SSHS_EXT.1	Failure to establish an SSH session. Reason for failure.	Failure *Unable to negotiate with <IP Address> from <Source IP> port 22: no matching mac found: client <Client Cipher> server <Server Cipher>* *Unable to negotiate with <IP Address> from <Source IP> port 22: no matching cipher found: client <Client Cipher> server <Server Cipher>* *Unable to negotiate with <IP Address> from <Source IP> port 22: unable to negotiate a key exchange method: client <Client Cipher> server <Server Cipher>*	System
FCS_TLSC_EXT.1 FCS_TLSC_EXT.2	Failure to establish a TLS session. Reason for failure.	Failure *2019/05/28 16:34:09 info general general 0 Failed to establish SSL connection to <Server>: <IP Address> Port:3978 Retry: 5000* *Syslog SSL error while writing stream; tls_error='SSL routines: SSL3_WRITE_BYTES:sslhandshake failure'* *Syslog SSL error while writing stream; tls_error='SSL routine:SSL3_GET_SERVER_CERTIFICATE: certificate verify failed'*	System
FCS_TLSS_EXT.1 FCS_TLSS_EXT.2	Failure to establish a TLS session. Reason for failure.	Failure *SSL handshake failed - (NONE)* *No shared cipher for peer <IP Address>* *Certificate not trusted for peer <IP Address>* *Invalid Extended Key Usage Purpose for peer <IP Address>* *Certificate digest, key size, or key do not meet FIPS-CC requirements for peer <IP Address>*	System
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded. [Origin of the attempt (e.g., IP address).]	On CLI (SSH): *Failed authentication for user <username>. Reason: Invalid username/password. From: <IP Address>* *ssh: euid 0 user <Username>: LOGIN_EXCEED_MAXTRIES*	System

FIA_UIA_EXT.1 FIA_UAU_EXT.2	All use of the identification and authentication mechanism. [Provided user identity, origin of the attempt (e.g., IP address).]	CLI (SSH): *User <Username> logged in via CLI from <IP Address>* *Failed authentication for user '<Username>'. Reason: Invalid username/password. From: <IP address>* Public-Key *Accepted publickey for <Username> from <IP Address> port <Source Port> ssh2: RSA <fingerprint>* *ssh: euid 0 user <Username>: CONNECTION_ABANDON* *User <Username> logged out via CLI from <IP Address>*	System
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate and reason for failure.	*Src Host/IP : <IP/hostname> Dst Host/IP: <IP/hostname> - <Reason>* *<Reason> can be any of the following example:* *OCSP/CRL validation of the X.509v3 certificate failed or not configured.* *Client cert expired or revoked for peer <IP Address>* *Certificate unknown for peer <IP Address>*	System
	Identification of certificates added, replaced or removed as trust anchor[1] in the TOE's trust store	*Admin | request/upload | config certificate wf* *{* *certificate* *{* *RSA 3072 CC keys* *{* *subject-hash ebcd3885; issuer-hash ebcd3885; not-valid-before "May 9 22:30:59 2018 GMT"; issuer "/CN=Root CA"; not-valid-after "May 9 22:30:59 2019 GMT"; common-name "Root CA"; expiry-epoch 1557441059; ca yes; subject "/CN=Root CA"; public-key…* *Admin | Upload | config certificate import <Name>* *Import <Name>* *{* *private-key ********;* *}* *Admin | delete | config certificate wf* *{* *certificate* *{* *RSA 3072 CC keys* *{* *subject-hash ebcd3885; issuer-hash ebcd3885; not-valid-before "May 9 22:30:59 2018 GMT"; issuer "/CN=Root CA"; not-valid-after "May 9 22:30:59 2019 GMT"; common-name "Root CA"; expiry-epoch 1557441059; ca yes; subject "/CN=Root CA"; public-key…*	Config
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	*Installed wf software version <Software Version>*	System

[1] Importing CA certificate(s) or generating CA certificate(s) internally will implicitly set them as trust anchor.

FMT_SMF.1	All management activities of TSF Data	Startup *The system is starting up.* Reboot/Shutdown *System restart requested by <Username>* *The system is shutting down due to CLI Initiated.* Ability to administer the TOE locally and remotely ssh: session open from <client IP> to <WildFire IP> for uid 0 user <user> on tty /dev/pts/0 User <user> logged in via CLI from <IP Address> Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates See FPT_TUD_EXT.1 Set Time See FPT_STM_EXT.1 · Ability to configure the access banner; 1,2019/08/28 10:39:15,009707001137,CONFIG,0,0,2019/08/28 10:39:15,10.54.96.101,,set,admin,CLI,Succeeded, deviceconfig system,,"system { login-banner ""FIPS APPROVED OPERATORS ONLY""; } ",41,0x8000000000000000,0,0,0,0,,WF-500,0, · Ability to configure the session inactivity time before session termination or locking; 1,2019/08/28 10:39:31,009707001137,CONFIG,0,0,2019/08/28 10:39:31,10.54.96.101,,set,admin,CLI,Succeeded, deviceconfig setting management,,management { idle-timeout 1400; } ,42,0x8000000000000000,0,0,0,0,,WF-500,0, · Ability to configure the authentication failure parameters for FIA_AFL.1; <Date>, <WF Serial Number>, CONFIG, 0, 0, <Date>, <Src IP Address>, set, <user>, CLI, Succeeded, deviceconfig setting management admin-lockout · Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1; See access banner note above · Ability to configure the cryptographic functionality; See below in this section · Ability to set the time which is used for time-	System/ Config

FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	Installed wf software version <version>	System
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1) [For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).]	*System time changed from <Old Date> <Old Time> to <New Date> <New Time> by <Username> from host <IP Address>*	System
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	CLI (SSH): *Session for user <Username> via CLI from <IP Address> timed out* Note that the auditable events for FTA_SSL_EXT.1 and FTA_SSL.3 are the same because the same logical interface is used for both local and remote access. Whether the access is local or remote is distinguished by whether the user's IP address is local or remote.	System
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	CLI (SSH): *Session for user <Username> via CLI from <IP Address> timed out* Note that the auditable events for FTA_SSL_EXT.1 and FTA_SSL.3 are the same because the same logical interface is used for both local and remote access. Whether the access is local or remote is distinguished by whether the user's IP address is local or remote.	System
FTA_SSL.4	The termination of an interactive session.	CLI (SSH): *User <Username> logged out via CLI from <IP Address>*	System

FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions [Identification of the initiator and target of failed trusted channels establishment attempt.]	on TLS Initiation 1,2019/06/19 09:14:17,009707000480,SYSTEM,tls,0,2019/06/19 09:14:17,,tls-session-established,,0,0,general,medium,"SSL negotiation finished successfully for peer 192.168.1.150:41874",697196,0x8000000000000000,0,0,0,0,,wf1 Termination *1,2019/06/19 12:02:53,009707000480,SYSTEM,tls,0,2019/06/19 12:02:53,,tls-session-terminated,,0,0,general,medium,"close notify for peer ",700075,0x8000000000000000,0,0,0,0,,wf1* Failure 1,2019/06/19 09:13:40,009707000480,SYSTEM,tls,0,2019/06/19 09:13:40,,tls-session-establishment-failed,,0,0,general,medium,"<reason for failure> 192.168.1.150:41856",697184,0x8000000000000000,0,0,0,0,,wf1	System

FTP_TRP.1/ Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	CLI (SSH) Initiation *ssh: session open from <Source IP Address> to <IP Address> for uid <ID> user <Username> on tty* Termination *ssh: session close from <Source IP Address> to <IP Address> for uid <ID> user <Username> on tty* Failure *Unable to negotiate with <IP Address> from <Source IP> port 22: no matching mac found* *Unable to negotiate with <IP Address> from <Source IP> port 22: no matching cipher found* *1,2019/03/26 09:56:36,009707000480,SYSTEM,ssh,0,2019/03/26 09:56:36,,ssh-session-establishment-failed,,0,0,general,medium,"Unable to negotiate with 192.168.1.150 from 192.168.1.205 port 22: unable to negotiate a key exchange method: client diffie-hellman-group1-sha1,ext-info-c server ecdh-sha2-nistp256,ecdh-sha2-nis.",685,0xc000000000000000,0,0,0,0,,WF-500*	System

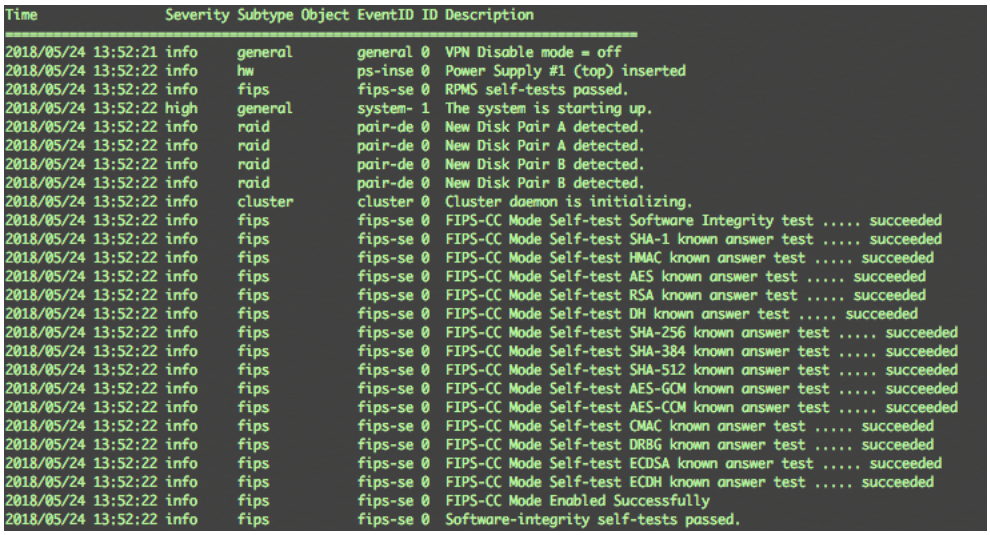
Table 7: Required Audit Events

The auditable administrative actions are identified in the above table for FMT_SMF.1.

Examples of the audit log events for the configuration and system:

Time	Host	Command	Admin	Client	Result
2018/05/15 14:40:34	10.54.98.61	request	admin	CLI	Succeeded
2018/05/15 14:46:17	10.54.98.61	set	admin	CLI	Succeeded
2018/05/15 14:46:28	10.54.98.61	set	admin	CLI	Succeeded
2018/05/15 14:46:36	10.54.98.61	set	admin	CLI	Succeeded
2018/05/15 14:46:37	10.54.98.61	commit	admin	CLI	Failed
2018/05/15 14:46:42	10.54.98.61	commit	admin	CLI	Submitted
2018/05/15 15:06:20	10.54.98.61	set	admin	CLI	Succeeded
2018/05/15 15:06:28	10.54.98.61	set	admin	CLI	Succeeded
2018/05/15 15:06:46	10.54.98.61	set	admin	CLI	Succeeded
2018/05/15 15:06:47	10.54.98.61	commit	admin	CLI	Submitted
2018/05/15 15:59:21	10.54.98.61	set	admin	CLI	Succeeded
2018/05/15 16:02:02	10.54.98.61	set	admin	CLI	Succeeded
2018/05/15 16:02:10	10.54.98.61	commit	admin	CLI	Submitted

Figure 1 - Configuration Logs



```
Time                Severity Subtype Object EventID ID Description
=============================================================================
2018/05/24 13:52:21 info     general       general 0  VPN Disable mode = off
2018/05/24 13:52:22 info     hw            ps-inse 0  Power Supply #1 (top) inserted
2018/05/24 13:52:22 info     fips          fips-se 0  RPMS self-tests passed.
2018/05/24 13:52:22 high     general       system- 1  The system is starting up.
2018/05/24 13:52:22 info     raid          pair-de 0  New Disk Pair A detected.
2018/05/24 13:52:22 info     raid          pair-de 0  New Disk Pair A detected.
2018/05/24 13:52:22 info     raid          pair-de 0  New Disk Pair B detected.
2018/05/24 13:52:22 info     raid          pair-de 0  New Disk Pair B detected.
2018/05/24 13:52:22 info     cluster       cluster 0  Cluster daemon is initializing.
2018/05/24 13:52:22 info     fips          fips-se 0  FIPS-CC Mode Self-test Software Integrity test ..... succeeded
2018/05/24 13:52:22 info     fips          fips-se 0  FIPS-CC Mode Self-test SHA-1 known answer test ..... succeeded
2018/05/24 13:52:22 info     fips          fips-se 0  FIPS-CC Mode Self-test HMAC known answer test ..... succeeded
2018/05/24 13:52:22 info     fips          fips-se 0  FIPS-CC Mode Self-test AES known answer test ..... succeeded
2018/05/24 13:52:22 info     fips          fips-se 0  FIPS-CC Mode Self-test RSA known answer test ..... succeeded
2018/05/24 13:52:22 info     fips          fips-se 0  FIPS-CC Mode Self-test DH known answer test ..... succeeded
2018/05/24 13:52:22 info     fips          fips-se 0  FIPS-CC Mode Self-test SHA-256 known answer test ..... succeeded
2018/05/24 13:52:22 info     fips          fips-se 0  FIPS-CC Mode Self-test SHA-384 known answer test ..... succeeded
2018/05/24 13:52:22 info     fips          fips-se 0  FIPS-CC Mode Self-test SHA-512 known answer test ..... succeeded
2018/05/24 13:52:22 info     fips          fips-se 0  FIPS-CC Mode Self-test AES-GCM known answer test ..... succeeded
2018/05/24 13:52:22 info     fips          fips-se 0  FIPS-CC Mode Self-test AES-CCM known answer test ..... succeeded
2018/05/24 13:52:22 info     fips          fips-se 0  FIPS-CC Mode Self-test CMAC known answer test ..... succeeded
2018/05/24 13:52:22 info     fips          fips-se 0  FIPS-CC Mode Self-test DRBG known answer test ..... succeeded
2018/05/24 13:52:22 info     fips          fips-se 0  FIPS-CC Mode Self-test ECDSA known answer test ..... succeeded
2018/05/24 13:52:22 info     fips          fips-se 0  FIPS-CC Mode Self-test ECDH known answer test ..... succeeded
2018/05/24 13:52:22 info     fips          fips-se 0  FIPS-CC Mode Enabled Successfully
2018/05/24 13:52:22 info     fips          fips-se 0  Software-integrity self-tests passed.
```

Figure 2 - System Logs

5 Identification and Authentication

This section and subsequent sections describe the required guidance assurance activities as specified in the NDcPP. Before any configuration can be performed on the TOE, the user must login. Other than viewing the login banner and pinging (i.e., ICMP echo request and reply) the TOE, no other action is provided to the users until they are successfully logged in. After that, the actions available will be based on the role and privileges assigned to that user.

5.1 Logging into the TOE

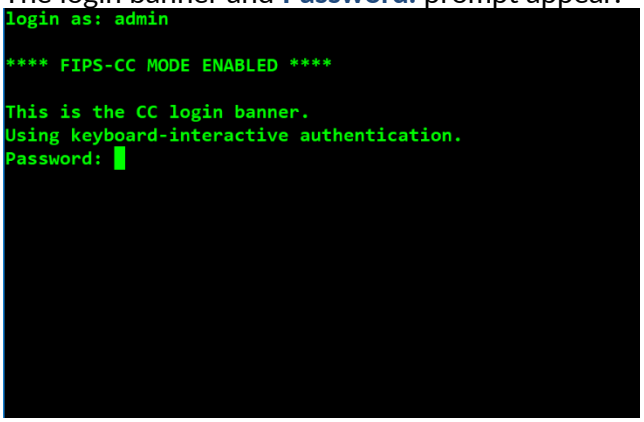
5.1.1 User Login to CLI Remotely/Locally

1. Direct an SSHv2 connection to the appliance at ***hostname***, where hostname corresponds to the host name of the appliance. SSHv2 on the TOE is enabled by default, and you can also use the IP address of the appliance. SSH is used for both local and remote administration. If connecting locally, use the Ethernet management port to connect to the appliance and follow section 6.1 to configure IP restriction. Restrict network access to only local IP addresses in your secure, internal management network. The Ethernet management port must be used because once FIPS-CC mode is enabled, the console port is disabled.

   The **login as:** command prompt appears.

2. Type your username and press **Enter**.

   The login banner and **Password:** prompt appear.



3. Type your password and press **Enter**.

The command prompt appears if the authentication is successful.
If authentication fails, the following error message is displayed:

```
Access denied
```

5.1.2 User Logout

1. For CLI sessions accessed locally or via remote SSH, type **exit** and press enter.
    a. The connection to the appliance will be closed.

6 Evaluated Configuration

This section describes the required steps to put the TOE in the CC evaluated configuration.

To ensure the TOE is configured in the evaluated configuration for Common Criteria, the following configuration actions **must** be taken:

- The administrator **must** enable FIPS-CC mode.
- The administrator **must** change the default password on the TOE.
- The administrator **must** restrict all cryptographic mechanisms to NDcPP-Approved algorithms and key sizes.

The TOE by default only supports SSH for management. Telnet and HTTP are not enabled for management and **must** not be enabled. The TOE is required to support only the cipher suites, version, and protocols claimed in the Security Target. TLS connection settings are configured automatically when FIPS-CC mode is enabled. For the other settings such as SSH, please follow the guide in this section. While not required by the NDcPP, the administrator should configure the Permitted IP feature to restrict which computers can access the TOE and from specific IP addresses.

6.1 Restrict Management Access (Recommended)

By default, port 22 (SSH), which is used to access the command line, is enabled for any IP address. To configure (whitelist) the permitted IP, use the following command:

set deviceconfig system permitted-ip <IP/Netmask> and **delete deviceconfig system permitted-ip <IP/Netmask>**.

6.2 Enable FIPS-CC Mode (Required)

The administrator must enable FIPS-CC mode to restrict the TLS version and cipher suites (including elliptical curves) to the Approved ones claimed in the Security Target. The TOE supports checking of identifiers as noted in RFC 6125 and IPv4 addresses in SAN or CN. See sections below for instructions on how to set these identifiers.

There are additional features such as enabling the FIPS power-up self-tests, enabling FIPS mode, and enforcing other TLS required checks such as the ones specified in section 6 of RFC 6125. To be in the evaluated configuration, the administrator must enable FIPS-CC Mode. In FIPS-CC mode, the module supports various cryptographic algorithms including an approved DRBG. For specific details regarding the algorithms, see the CAVP certificate information:

- AES – Cert. #A3453
- CVL – Cert. #A3453
- DRBG – Cert. #A3453
- ECDSA – Cert. #A3453

- HMAC – Cert. #A3453
- RSA – Cert. #A3453
- SHA – Cert. #A3453
- KAS – Cert. #A3453

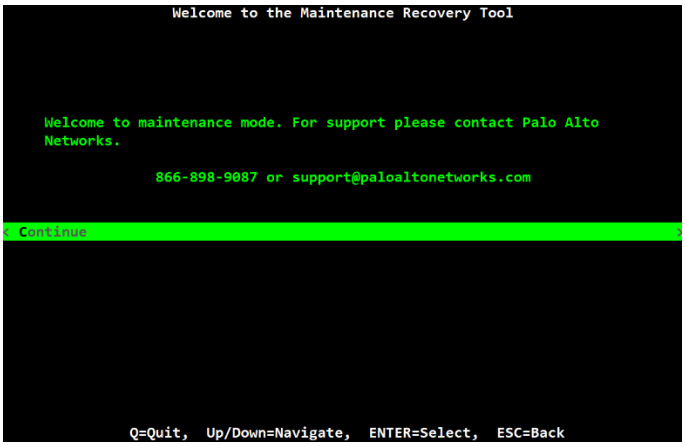
> **NOTE:** The administrator must still configure the SSH algorithms, except for the key exchange method, MAC algorithm, and rekeying interval.

To enable FIPS-CC mode, first boot the TOE into the maintenance mode. From there, change the operational mode from normal mode to FIPS-CC mode.

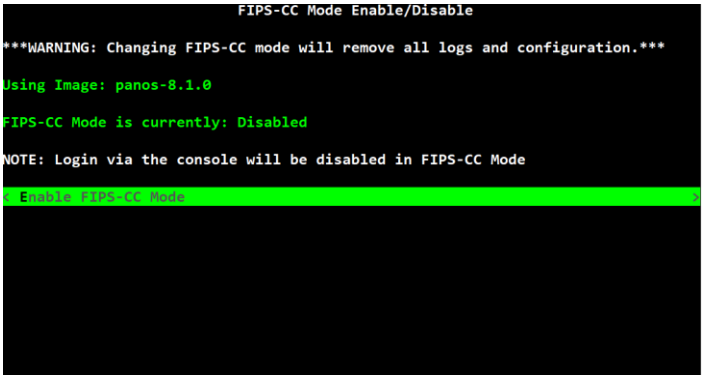
1. Using SSH, login with Administrator Role.
2. Enter the following command: **debug system maintenance-mode**
3. Type **y** to confirm. The SSH session will disconnect.

> **WARNING:** When the TOE is in maintenance mode, it is no longer in the evaluated configuration.

4. It will take approximately 2 to 3 minutes for the TOE to boot up into maintenance mode. During this time, the SSH management session will be disabled.



5. Using the local console, select **Continue** and press the Enter key.
6. Using the down arrow, select **Set FIPS-CC Mode** and press the Enter key.
7. Select **Enable FIPS-CC Mode** and press the Enter key.



Note: Image name will be different; this is shown as an example

8. When prompted, select **Reboot**.
9. After the TOE passes all the FIPS power-up self-tests and switches to FIPS-CC mode, the administrator will see the following status: *FIPS-CC mode enabled successfully*.

WARNING: Enabling FIPS-CC Mode will completely zeroize the TOE and the KEK (i.e., Master Key); all configurations and logs will be erased permanently.

6.3 Change Default Admin Password (Required)

1. Login as **admin** with the default password **paloalto**.
2. Enter configuration mode using the **configure** command
3. Enter the following command
   set mgt-config users <user> password
4. Enter the new password, and then confirm the new password
5. Enter the new password
6. Commit the changes using the **commit** command

6.4 Configure SSH Encryption[2] Algorithms (Required)

In FIPS-CC mode, the TOE supports all AES key sizes including 192 for CBC and CTR. The NDcPP does not allow this 192 bits key size for SSH. Use the following steps to configure 128 and 256 bits only:

1. Using SSH, login with Administrator Role.
2. Enter configuration mode using **configure** command.
3. Enter the following commands:
   - **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> ciphers aes128-cbc**

[2] The MAC algorithms are configured by default when FIPS-CC mode is enabled. To further restrict them (e.g., use HMAC-SHA2-512 only), use the command **set deviceconfig system ssh mac mgmt**.

- **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> ciphers aes128-ctr**
- **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> ciphers aes128-gcm**
- **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> ciphers aes256-cbc**
- **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> ciphers aes256-ctr**
- **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> ciphers aes256-gcm**

4. Enter **set deviceconfig system ssh mgmt server-profiles <Profile_Name>** to apply the profile to the management interface.
5. Enter **commit** to save the changes.
6. Enter **run set ssh service-restart mgmt** to restart the SSH server.
7. Type **y** to confirm.

6.5 Configure SSH Rekey Interval (Required)

When FIPS-CC mode is enabled, the SSH rekeying will occur approximately at 1 hour of time or after 1 GB of data has been transmitted, whichever occurs first. To change the SSH rekeying interval, please follow the instructions below.

1. Using SSH, login with Administrator Role.
2. Enter configuration mode using **configure** command.
3. Enter the following commands:
   - **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> session-rekey interval <10-3600 seconds>**
   - **set deviceconfig system ssh profiles mgmt-profiles server-profiles <Profile_Name> session-rekey data <10-4000 MB>**

   WARNING: The data limit must be 1024 MB or less in the evaluated configuration.
4. Enter **set deviceconfig system ssh mgmt server-profiles <Profile_Name>** to apply the profile to the management interface.
5. Enter **commit** to save the changes.
6. Enter **run set ssh service-restart mgmt** to restart the SSH server.
7. Type **y** to confirm.

6.6 Configure SSH Public-Key Authentication

Perform the following steps on a remote workstation:

1. Log in as a privileged user.
2. Generate the SSH keypair.

   Note: Currently, only RSA keypair is supported and only generate RSA 2048 bits or higher.

3. Enter **ssh-keygen -t rsa -b 3072**
4. Enter an optional passphrase, if desired.

> **NOTE:** ECDSA keypair is not supported at the moment.

On the TOE CLI:

1. Login with Administrator Role.
2. Enter configuration mode.
3. Enter the following commands: **set mgt-config users <Username> public-key <Value>**. The **<Value>** must be Base64 encoded (e.g., linux$: base64 id_rsa.pub).
4. Remember to commit the settings: **commit**.
5. To delete the public key, use the following command:

   delete mgt-config users <Username> public-key <Value>

   commit

On the same remote workstation:

1. Log into the remote machine as a privileged user.
2. Attempt to log in as 'admin2' using the SSH public-key authentication.
   a. Enter **ssh admin2@<IP Address>**
   b. Verify access is allowed without entering the password.

> **NOTE:** The passphrase is different from the password. The passphrase, if set above, is used to protect the SSH private key and will be prompted each time the private key is accessed.

> **NOTE:** If StrictHostKeyChecking is enabled on the SSH client, the user may need to add the SSH server (TOE) host key to the known hosts. Use this command if prompted to do so: **ssh-keygen -f "/home/user/.ssh/known_hosts" -R <IP Address>**

6.7 Secure Connection Settings

The sections below provide details for the various secure connections that can be set and utilized. By default, the WildFire appliance must have the following setting set to "True".

admin@WF-500> **show ssl-conn-on-cert fail-all-conns**[3]

Fail connection on cert set to True

If this is not set to true for some reason, use the following command:

admin@WF-500> **set ssl-conn-on-cert fail-all-conns True**

By setting to True, WF will enforce checking the certificate validity during the TLS handshake. If the certificate fails the validity check, the TLS session will not be established.

6.7.1 Syslog Server Connection Settings (Required)

The TOE can be configured to forward generated audit records to an external syslog server in real-time. When configured, the TOE automatically converts the audit records to syslog format before forwarding them to the external syslog server. Audit records are converted and forwarded to the external syslog as they are locally written to the log files. The TOE automatically attempts to re-connect to the external syslog server should the TLSv1.2 channel be broken.

Syslog over TLS connection fails if the syslog server certificate meets any of the following criteria:

- The server certificate has been revoked or modified.
- The server certificate is not signed by the CA with CA flag set to TRUE.
- The server certificate is not signed by a trusted CA in the certificate chain.
- The server certificate Common Name (CN) or Subject Alternative Name (SAN) does not match the expected hostname (i.e., reference identifier).
- The server certificate is expired.

Configure a Syslog Server Profile:

1. Login to the CLI, and enter configuration mode
2. Setup connection to the Syslog server:
    a) admin@WF-500# **set shared log-settings syslog <enter name> server <enter name> format IETF port <6514 default for SSL> server <IPv4 address or FQDN for SAN/CN verification of Syslog server> transport <SSL> facility LOG_USER**
3. Create a log setting rule (i.e., which logs to forward – system/configuration logs)
    a) admin@WF-500# **set shared log-settings <system or config> match-list <name for this filter> send-syslog <syslog setting name> filter "All Logs"**

[3] To configure just the syslog connection, use **fail-syslog-conns**.

4. Create a certificate profile with the CA of the Syslog server to ensure connection is established successfully
    a) Ensure CA certificate has been imported into the WildFire device (see below for directions)
    b) admin@WF-500# **set shared certificate-profile <name of profile> CA <name of CA>**
5. Commit this configuration, and the logs will begin forwarding to the Syslog server

The TOE automatically checks the revocation status based on CRL information located in the certificate for Syslog connections. The connection is dropped if the revocation status cannot be determined, which is the default behavior and cannot be turned off.

Generate or import certificates:

1. Login with Administrator Role.
2. Enter **request certificate generate** and add the additional items as applicable (see below).
    a) For generation of CSRs, see "CSR Generation" below
3. Example for creating a CA[4]:
    a) admin@WF-500> **request certificate generate ca yes digest sha384 algorithm RSA rsa-nbits 3072 certificate-name <cert name> name <IP address or FQDN of certificate> passphrase <passphrase for encrypting private key>**

CLI options present when initiating generate command:

admin@WF-500> **request certificate generate**

+ ca	CA for the certificate
+ country-code	Country code
+ days-till-expiry	Number of days till expiry
+ digest	Digest Algorithm
+ email	Email address of the contact person
+ filename	file name for the certificate
+ for-use-by	Purpose of this certificate
+ locality	Locality
+ ocsp-responder-url	ocsp-responder-url
+ organization	Organization
+ signed-by	CA for the signing certificate
+ state	State/province
* algorithm	algorithm
* certificate-name	Name of the certificate object

[4] Enter 'configure' mode and type commit before you can use the CA certificate.

* name	IP or FQDN to appear on the certificate
* passphrase	Pass-phrase for encrypting private key
> alt-email	Subject alternate Email type
> hostname	Subject alternate name DNS type
> ip	Subject alternate name IP type

Summarize this command options below:

1. ca	yes | no (yes if this is a CA certificate)
2. country-code	enter the country code (e.g., US)
3. days-till-expiry	enter the number of days before expiration
4. digest	sha256 | sha384 | sha512
5. email	enter the email address
6. filename	enter the file name
7. for-use-by	enter if use for server or web interface
8. locality	enter the city or county (e.g., Santa Clara)
9. ocsp-responder-url	enter the OCSP responder URI
10. organization	enter the company (e.g., Palo Alto Networks)
11. signed-by	enter the CA who signed this or **external** if this is a CSR
12. state	enter the state or province (e.g., CA)
13. algorithm	RSA | ECDSA
14. certificate-name	enter the name of the certificate for device
15. name	enter IP or FQDN to appear on the certificate
16. passphrase	enter passphrase for encrypting private key
17. alt-email	enter Subject alternate name (SAN) email type
18. hostname	enter Subject alternate name (SAN) DNS type
19. ip	enter Subject alternate name (SAN) IP type

NOTE: In the evaluated configuration, the 'country-code', 'organization', and 'name' fields are used for identification of the WF-500.

1. To import external CA Certificates (and optionally, private keys if you want to sign other certificates), enter the following command:
   a) admin@WF-500> **scp import certificate passphrase <cert passphrase> format pem certificate-name <name of cert> from <username>@<ip address>:/<path to cert>/<cert filename>**

b) admin@WF-500> **scp import private-key passphrase <key passphrase> format pem certificate-name <name of cert associated with private key> from <username>@<ip address>:/<path to key>/<key filename>**
c) Change to configure mode and commit.

CSR Generation: To create a CSR and prepare it for signing, the following steps must be done.

1. Create a certificate signing request using the following command:

   admin@WF-500> **request certificate generate ca no signed-by external country-code <value> organization <value> name <IP or FQDN> algorithm < ECDSA | RSA> <ecdsa or RSA>-nbits <256/384 or 2048/3072/4096> certificate-name <name> passphrase <value>**

2. Navigate to the configure settings (i.e. enter **configure**), and enter the following command to retrieve the certificate request details:

   admin@WF-500# **show shared certificate <Certificate Name>**

3. Copy the certificate request, and paste it into a new file in the location where you will be signing the certificate

   -----BEGIN CERTIFICATE REQUEST-----

   MIIBJjCBrQIBADAuMQswCQYDVQQGEwJVUzENMAsGA1UEChMEUEFOVzEQMA4GA1UE
   AxMHMS4zLjMuMjB2MBAGByqGSM49AgEGBSuBBAAiA2IABE5WKVGaODbjAZjP587G
   dFSeUIo40U+T7EkmX9cXUXH28o/k5bmG/ouFQJ+ctgqqavRmjZC0TUgPKCZpKvk5
   fPf2YBo1s3rlfBjZcCIexAEwRX+/eZpTOCijxlazXv6WLKAAMAoGCCqGSM49BAMC
   A2gAMGUCMFIj92iwC6tZKL939OWVmLvR65CqnhL55lXcQ1aih0zy7Jy8L4C6rope
   GTKqW+faBwIxAJ/IxM8yEANA6VTqanyaaXjFy49NLG7Km4i/w42/fdnslXj4OFIa
   RnNjQiIXk7rRjA==
   -----END CERTIFICATE REQUEST-----

4. Sign the certificate using the desired CA, and then import the CA that signed the CSR into the appliance.

> **NOTE:** If the CA or CA(s) are not imported first, you will get this error message: “Import of <signed certificate based on CSR> failed. Certificate chain cannot be validated, required CAs not found”. Root CA and Intermediate CA certificates cannot have spaces on their names.

> **NOTE:** Do not import CA that has been expired or revoked.

> **NOTE:** Do not import CA with duplicate Common Name with an existing CA. Please delete the old CA first. The TOE will use the first CA with the matching CN from the signed certificate (Issuer field) which may not be the CA you want to use to validate the chain.

5. Import the signed certificate back into the appliance using the SCP import command:
   admin@WF-500> **scp import certificate format pem from <path to file> certificate-name <value>**

> **NOTE:** The signed certificate that is being imported to replace the CSR must have the same name in order for the device to register it and replace it properly.

Configure the External Syslog-ng Server:

1. Login as authorized administrator.
2. Install or use syslog-ng with version 3.7 or later (recommended).
3. Edit the syslog-ng configuration file by adding the following highlighted section below.
   vi /etc/syslog-ng/syslog-ng.conf

   If the config file is in a different location, search for with **find / -name syslog-ng.conf**
   # This command assumes you have root privilege or can sudo to root.

```
source s_Wildfire {
        syslog(ip(0.0.0.0) port(6514)  # This port can be changed but must match the port configured in the TOE.
        transport("tls")
        tls(
          # Location of the private key of syslog server certificate.
          key-file("/etc/ssl/Server.Key.pem")  # Make sure the private key is not encrypted.
          # Location of the syslog server certificate.
          cert-file("/etc/ssl/Server.Cert.pem")  # Make sure the server cert has the correct EKU.

          ### The next line is needed if authentication mutual is required.
          ca-dir("/etc/ssl") # Location of the CA certificates and symbolic links. See below
            ###  openssl x509 -noout -hash -in <CA certificate>
            ###   ln -s <CA certificate> <Hash Output>.0
            ###   This is the CA that signed the client certificate and other CA(s) in the chain.
            ###   All CA certs must have basic constraints CA flag set to TRUE

          cipher-suite(AES128-SHA) # e.g., TLS Ciphersuite to be supported by the server
          ssl-options(no-sslv2, no-sslv3, no-tlsv1)  # TLS Version NOT supported by the server
                                                     # The TOE only supports TLSv1.2
          peer-verify(optional-trusted)  # required-trusted for mutual auth, optional-trusted for no mutual auth
        )
    );
};

destination d_Local {
  file("/var/log/Wildfire_messages");   # The remote syslog file location can be configured here
```

```
};

log {
    source(s_Wildfire); destination(d_Local);
};
```

4. Restart the syslog-ng server and make sure there is no error message.
   systemctl restart syslog-ng.service # This command may be different on different OS.

5. Use netstat to make sure the syslog-ng is listening.
   netstat -an | grep 6514
6. Make sure port 6514 is opened by the local firewall to allow the connection.

This section provides TLS troubleshooting tips. The following are common reasons why the TLS connection fails and how to fix it:

- ClientHello but no ServerHello from Server
  - Make sure the private key (unencrypted) and server certificate are in the right directory and are accessible (e.g., permission to read).
- 'Unknown ca'
  - On the TOE, make sure the server certificate is signed and issued by valid CA chain with one of the CA certificates (i.e., Root CA) specified as the trust anchor.
  - If mutual authentication is configured, make sure the CA certificates are in the right directory with the correct name and symbolic links.
  - For syslog connection, the syslog server cannot be signed by the Root CA. At minimum, the syslog server certificate must be signed and issued by an Intermediate CA.
  - Reboot the TOE.
- 'Unknown certificate'
  - Make sure the revocation status is accessible.
  - Make sure CRLsign is set properly on the CRL issuer.
  - If you change the server certificate and/or key on the syslog-ng server, make sure to restart the syslog server.
- 'Certificate Revoked'
  - Certificate is revoked.
  - CRL is signed by unauthorized CA[5].

[5] Make sure the CA is trusted and has the CRLsign in the Key Usage field.

This section provides CC X509v3 certificate checks when FIPS-CC mode is enabled. All required EKU checks are performed[6].

- CAs must have CA flag set to TRUE.
- Server certificate must have CA flag set to FALSE.
- Server certificate must have ServerAuth in the Extended Key Usage field. (for client certificate, ClientAuth instead of ServerAuth)
- Server certificate must have digitalSignature in the Key Usage field.
- Certificate must have proper CDP (for CRL) reference. CRL must be issued and signed by CA with CRLsign in the KU field.
- Certificate must have proper CN and SAN format that complies with section 6 of RFC 6125 if hostname/FQDN is required.
- Certificate names must not have space in them. For example, “Root CA” should be Root-CA, Root.CA or Root_CA.
- Certificate must not be expired or modified.
- The syslog server must be restarted, and TOE must be rebooted.

The administrator is responsible for maintaining the physical connection between the TOE and external syslog server. If the connection is unintentionally broken, the administrator should perform the following steps to diagnose and fix the problem:

- Check the physical network cables.
- Check that the syslog server is still running.
- Reconfigure the Log Settings.
- If all else fails, reboot the TOE and/or syslog server.

[6] Enter **show syslogng-ssl-conn-validation**. By default, every check is enforced.

6.7.2 Firewall Connection Settings (Required)

In order to connect the TOE to a firewall, the following configurations must be set on the firewall:

1. Obtain a Palo Alto Networks Firewall.
    - Ensure that the Palo Alto Networks Firewall is in FIPS-CC mode.
2. License the device, and ensure that a valid WildFire license is applied.
3. On the Firewall WebUI, navigate to **Device > Setup > WildFire** Tab.
    - Under the **General Settings**, set the IP address or FQDN of the WildFire appliance for private cloud.
4. Create a WildFire Analysis profile.
    - **Objects > Security Profiles > WildFire** Analysis > click **add.**
        i. Include the desired details (i.e., File Types, Applications), and select analysis as **private-cloud.**
5. Attach this WildFire Analysis Profile to a security rule under **Policies > Security.**
6. **Commit** the configuration.
7. Test the connection using the following command:

    admin@PA-Firewall> **request wildfire registration channel private**

8. The device should state successful if you have set the connection properly.

The administrator is responsible for maintaining the physical connection between the TOE and external Firewall. If the connection is unintentionally broken, the administrator should perform the following steps to diagnose and fix the problem:

- Check the physical network cables.
- Check that the Firewall is still running.
- Reconfigure the connection settings between the Firewall and the TOE.
- If all else fails, reboot the TOE and/or Firewall.

NOTE: The connection between the Firewall and WildFire appliance can use either a pre-defined certificate, or a custom certificate. To implement a custom certificate, use the steps below.

1. Create the necessary CAs along with the leaf certificate or import them – see "Generate or Import the Certificates" above for more details.
2. Create a certificate profile on the WF-500 that includes the CAs that will validate the Firewall's client certificate:

    admin@WF-500# **set shared certificate-profile <name> CA <Root CA, Intermediate CA(s)> username-field subject common-name <expected reference value>**

    To set the individual flags below, use **set shared certificate-profile <name> <flag> <yes|no>** where **<flag>** refers to the individual values below (e.g., "block-unknown-cert").

    + block-timeout-cert whether to block a session if cert. status can't be retrieved within timeout
    + block-unauthenticated-cert whether to block session if the certificate was not issued to the authenticating device
    + block-unknown-cert whether to block a session if cert. status is unknown

```
+ cert-status-timeout        set cert status query timeout value in seconds
+ crl-receive-timeout        set CRL receive timeout value in seconds
+ domain                     alphanumeric string [ 0-9a-zA-Z._-]
+ use-crl                    use-crl
> CA                        CA
> username-field            username-field
  <Enter>                   Finish input
```

NOTE: The full list of flags has been listed for completeness; in the evaluated configuration, use-crl is set to 'yes'. The 'block-unknown-cert' command can be set to either value; this determines whether or not the connection is blocked if the certificate's revocation status cannot be verified.

3. Create an SSL-TLS Service Profile on the WF-500 with the server's leaf certificate:
   admin@WF-500# **set shared ssl-tls-service-profile <name> certificate <WF-500 leaf cert> protocol-settings min-version tls1-1 max-version max**

4. Set the secure server connection configuration, which will incorporate the items done in previous steps as well as including the items below:
   - Disable the pre-defined certificate.
   - Create an authorization list and set it to **yes.**
   - Set the identifier that needs to be checked (e.g., the FQDN of the connecting firewall).

   admin@WF-500# **set deviceconfig setting management secure-conn-server certificate-profile <name of profile> disable-pre-defined-cert yes ssl-tls-service-profile <name of profile> check-authorization-list yes authorization-list <name of list> identifier <subject or subject-alt-name> <common-name | email, hostname, ip> <value>**

5. **Commit** the configuration.
6. Set the Firewall with the necessary certificate information; see section below for procedure.

Similar steps must be done on the Firewall in order to properly set the configuration. The settings for the Firewall can be done via the WebUI.

1. Similar to Step 1 in the previous section, you must create the required CA/leaf certificates or import them.
2. Authenticate into the Firewall's WebUI and navigate to **Device > Setup > Management.**
3. Click on **Secure Communication Settings.**
4. Change the Certificate Type from **Predefined** to **Local**; this will provide additional selectable options to configure.
5. For the **Certificate** section, select the Firewall's leaf certificate that it will use to present to the WildFire appliance.
6. The certificate profile can also be set for the client (Firewall) to verify the WildFire appliance's certificate chain. It is recommended that this is set as well to ensure mutual authentication.
   - A new window will present itself if **New Certificate Profile** is selected.
   - Provide the Certificate Profile with a name and add the applicable CA certificates.
7. Under the **Customize Communication**, select **WildFire Communication.**

8. **Commit** the configuration.

6.7.3 Set Wildfire Appliance with ECDHE Ciphersuites (Recommended)

The Administrator can configure the WildFire appliance to only offer ECDHE cipher suites if desired. The steps below detail the configuration required to achieve this behavior.

1. Create a CA with a leaf certificate (or import them) via the WildFire Appliance.
    - See directions above for how to generate/import certificates and private keys into the appliance.

2. Create an SSL-TLS Service Profile.
    - admin@WF-500# **set shared ssl-tls-service-profile <name> certificate <leaf certificate> protocol-settings min-version tls1-1 max-version max**
3. Apply the SSL-TLS Service Profile created in the previous step to the secure connection setting for the server, and disable the pre-defined certificate:
    - admin@WF-500# **set deviceconfig setting management secure-conn-server ssl-tls-service-profile <profile name from step 2> disable-pre-defined-cert yes**
4. **Commit** the configuration.
5. The WildFire appliance as a server will now present ECDHE cipher suites.

7 Management Activity

This section describes the management functions provided by the TOE to the authorized administrators.

7.1 Manage Audit Log

The TOE generates and stores read-only auditing information for user activity. The logs are presented in a standard event view that allows administrator to view/filter audit log messages based on any item in the audit columns. Administrator can delete and report on audit information and can view detailed reports of the changes that users make.

To quickly view the latest logs, enter the following command for system/configuration:

admin@WF-500> **show log <system or config> direction equal backward**

To export the logs, and view them externally, use the following command:

admin@WF-500> **scp export log <system/config> to <user>@<IP Address>:<file> start-time equal YYYY/MM/DD@HH:MM:SS end-time equal YYYY/MM/DD@HH:MM:SS**

The CLI provides the following commands that the user can utilize to view/filter the system or configuration logs:

```
admin@WF-500> show log system

      + csv-output        csv-output
      + direction         direction
      + end-time          end-time
      + eventid           eventid
      + id                id
      + object            object
      + opaque            opaque
      + query             query
      + receive_time      receive_time
      + serial            serial
      + severity          severity
      + start-time        start-time
      + subtype           subtype
        |                 Pipe through a command
        <Enter>           Finish input

admin@WF-500> show log config

      + client            client
      + cmd               cmd
      + csv-output        csv-output
      + direction         direction
      + end-time          end-time
      + query             query
      + receive_time      receive_time
      + result            result
      + serial            serial
      + start-time        start-time
        |                 Pipe through a command
        <Enter>           Finish input
```

7.2 Configure Custom TLS Server Certificate

Use the following procedures to configure the TLS server (TOE) to use a custom certificate instead of the predefined certificate. You can deploy the certificate on the TOE by generating a server certificate internally or obtaining a server certificate from your enterprise CA or a trusted third-party CA.

1. Login to the CLI with Administrator Role.
2. Enter the configuration mode by entering **configure**
3. Create an SSL-TLS-Service Profile
    a. admin@WF-500# **set shared ssl-tls-service-profile <profile name> certificate <custom certificate name> protocol-settings min-version tls1-1 max-version tls1-2**

WARNING: The minimum TLS version must be TLSv1.1 or higher.

4. Update the management setting using the following:
    a. admin@WF-500# **set deviceconfig setting management secure-conn-server ssl-tls-service-profile <profile name> disable-pre-defined-cert yes**
5. Enter **commit** to have the change applied to the configuration.

7.3 Role-Based Access Control (RBAC)

RBAC enables you to define the privileges and responsibilities of users of the device. Every administrator must have a user account that specifies a role and authentication method. By default, every TOE appliance has a predefined administrative account (**admin**) that provides full read-write access (superuser access) to all.

In the evaluated configuration, it is recommended that the users use the **admin** account to create separate accounts, and only use the **admin** account as an emergency account.

7.3.1 View Administrator Account

The CLI provides the ability to view configured users via the following command:

admin@WF-500# **show mgt-config users**

7.3.2 Adding New Accounts

When you create a new user account, you can control which parts of the system the account can access. You can set the authentication method (password vs public-key), authentication profile (e.g., using an authentication server), and the administrator role (e.g., superuser with all privileges or superreader with read-only privilege)

1. Login to the CLI with an Administrator Role.
2. Enter **configure** to enter the configuration mode.
3. Enter the following command to create a new user account, which provides the following options:

   admin@WF-500# **set mgt-config users <user name>**

   + authentication-profile authentication-profile

   + public-key Public RSA

   > permissions permissions

   > phash phash

   password password

   <Enter> Finish input

4. The following are required when setting up the new users
   - Passwords must be a minimum of 8 characters in length
   - If a public key is assigned, it can only be RSA 2048 bits or higher, and must be correctly formatted when entering it into the CLI

> **NOTE:** If public key authentication fails, the TOE will failback to password authentication.

7.3.3 Deleting or Modifying Accounts

The administrator can modify or delete user accounts from the system at any time, with the exception of the **admin** account, which cannot be deleted.

To delete an account, enter configuration mode in the CLI, and utilize the following command:

admin@WF-500# **delete mgt-config users <username>**

Once complete, perform a **commit** to finalize the update.

7.3.4 Change User Password

All user accounts are protected with a password by default. Any user can change their own password but only a user with Administrator role (i.e., superuser) can change another user's password.

To update a password, utilize the following command via the CLI:

admin@WF-500# **set mgt-config users <username> password**

Enter the new password, and then **commit** the change once complete.

To change own password, enter command: **set password**

Passwords can be composed of uppercase, lowercase, numbers, and special characters. It is recommended that Administrators set a password with at least 3 out of the 4 options (e.g., uppercase, lowercase, and a special character) for added security.

7.4 Configure System Time

The administrator can configure time manually.

7.4.1 Configure Time Manually

1. Login with Administrator Role via CLI.
2. Use the following command to configure the time/date:

admin@WF-500> **set clock date <YYYY/MM/DD> time <hh:mm:ss>**

7.5 Configure Login Banner

The administrator can create a custom login banner that appears when users log into the appliance using SSH.

1. Login to the CLI with Administrator Role.
2. Enter configuration mode.
3. Use the following command to specify the banner verbiage:

   admin@WF-500# **set deviceconfig system login-banner <insert banner verbiage>**

   > **NOTE:** When entering the banner verbiage, it must be enclosed using quotations. Example: set deviceconfig system login-banner “This is the banner”

4. Enter **commit** to complete the configuration.

(Optionally) To disable ICMP, perform the following:

1. Login to the CLI with Administrator Role.
2. Enter configuration mode.
3. Use the following command to disable ICMP by entering **yes** as the option:

admin@WF-500# **set deviceconfig system service disable-icmp <yes | no>**

4. Enter **commit** to complete the configuration.

7.6 Configure Idle Timeout and Lockout

The administrator can configure the idle session timeout for CLI users that access the TOE locally or via remote SSH. By default, the idle timeout value is 60 minutes.

1. Login to the CLI with Administrator Role.
2. Enter configuration mode.
3. Use the following command to set the idle timeout (in minutes):
   admin@WF-500# **set deviceconfig setting management idle-timeout**
   0 never
   1 1
   <value> <1-1440>
4. Enter **commit** to complete the configuration.

The administrator can also configure the number of failed login attempts to trigger a lock-out, and also how long this user is locked-out once this number of failed attempts is hit.

The following configuration can be set via the CLI:

admin@WF-500# **set deviceconfig setting management admin-lockout failed-attempts <value>**
<0-10> Number of failed login attempts to trigger lock-out

> **WARNING:** In the evaluated configuration, the **failed-attempts** value must not be set to zero.

To configure the lock-out time or failed attempts, the following commands can be used:

admin@WF-500# **set deviceconfig setting management admin-lockout**

+ failed-attempts Number of failed login attempts to trigger lock-out

+ lockout-time Number of minutes to lock-out

<Enter> Finish input

The lockout-time ranges from 0 to 60 (minutes) while the failed attempts can be set from 0 – 10 attempts.

> **NOTE:** Setting a lockout-time of 0 means that the account is locked out indefinitely and can only be restored by administrative action. When a setting of 0 is set for the failed attempts, it means that the account will never be locked out.

It is required that an administrator be created or the default admin set using an SSH key for additional security (See Section 6.6 above). This is to prevent a denial of service through the password lockout mechanism. In the event that an administrator is locked out, they can be unlocked via the following command:

admin@WF-500> **request authentication unlock-admin user <value>**

where <value> is the username of administrator

7.7 Configure Minimum Password Length

The administrator can create a password rule to force users to create passwords that adhere to a specified length requirement. To set this length requirement, the administrator can utilize the following CLI command:

admin@WF-500> **set minimum-password-length to <8-15>**

> **NOTE:** In FIPS-CC mode, a minimum password length of 8 is required.

7.8 Verify and Update System Software

The TOE supports the ability for administrators to update their software via the CLI. If the TOE is not internet connected, the software updates can be loaded into the device by an administrator (download the update image from support.paloaltonetworks.com). Regardless of the method, the digital signature of the file image is verified during installation to ensure that the update being installed has been digitally signed by Palo Alto Networks[7].

To query the current active version of the TOE, an administrator can use the following command[8]:

admin@WF-500> **show system info**

Follow the instructions below to update the software of the device.

1. Login to the CLI with an administrator role.
2. If you have Internet access and can ping the Update server from the TOE, skip to step 4.
3. Otherwise, download the image from the Support site. Upload/import the image to the TOE with command **scp import software from <username>@<IP>:<path>/<filename>**. Skip to step 6.
4. Enter the following command to get an updated list of software available:
   admin@WF-500> **request system software check**

5. Once the software version has been identified, begin the download using the following command:
   admin@WF-500> **request system software download version <Version number>**

6. Once the download is complete, begin the installation of the file using the following command:
   admin@WF-500> **request system software install version <Version number>**

> **NOTE:** Some software updates require that the content on the device is also updated. To update content, use the following commands: **request wf-content upgrade check**, **request wf-content upgrade download latest**, and **request wf-content upgrade install file <YYYY-XXXX>** or **request wf-content upgrade install version latest**.

7. After the installation is complete, the device will need to be rebooted for the software update to be complete.

> **NOTE:** If the software update is not a valid image or is corrupt (e.g., failed signature validation), then the TOE will reject the update and provide the following message: "Server Error: Invalid Image".

[7] Palo Alto Networks public key is used to verify the signature.

[8] TOE version is identified by **sw-version:** field.

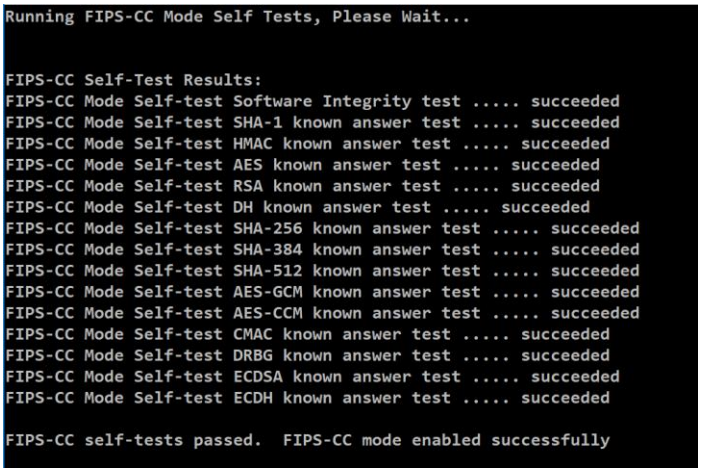
7.9 Self-Tests

The TOE performs a suite of FIPS self-tests during power-up and during operational state. If any self-test fails, the TOE will go into an error state (i.e., maintenance mode), and not operate until the error is resolved.

When this occurs, an administrator can attempt to resolve the issue by rebooting the device. If the self-tests continue to fail, please contact Palo Alto Networks Support (e-mail support@paloaltonetworks.com or call them at 866-898-9087).

The following possible failures can be detected during the self-test:

- Software Integrity failure[9]
- Known Answer Test (KAT) failures
- Pairwise Consistency failures
- RNG Continuous failures
- Entropy Continuous failures



[9] HMAC-SHA-256 key and ECDSA P-256 are used to verify integrity during power-up.