NETSCOUT

nGenius 5000 & 7000 Series Packet Flow Switches with PFOS 6.0.6

Common Criteria Guide

Version 1.0

April 2022

Document prepared by

www.lightshipsec.com

Table of Contents

List of Tables

1 About this Guide

1.1 Overview

1 This guide provides supplemental instructions to achieve the Common Criteria evaluated configuration of the nGenius 5000 & 7000 Series Packet Flow Switches with PFOS 6.0.6 (PFS) and related information.

2 This document has been developed as part of the NETSCOUT nGenius 5000 & 7000 Series Packet Flow Switches with PFOS 6.0.6 Common Criteria (CC) documentation suite. The scope of the security functions under evaluation is defined in the Security Target (ST) (Ref. [ST]).

1.2 Audience

3 This guide is intended for system administrators and the various stakeholders involved in the Common Criteria evaluation. It is assumed that readers will use this guide in conjunction with the related documents listed in Table 2.

1.3 About the Common Criteria Evaluation

4 The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) is an international standard for security certification of IT products and systems. More information is available at https://www.commoncriteriaportal.org/

1.3.1 Protection Profile Conformance

5 The Common Criteria evaluation was performed against the requirements of the Network Device collaborative Protection Profile (NDcPP) v2.2E available at https://www.niap-ccevs.org/Profile/PP.cfm

1.3.2 Evaluated Software and Hardware

6 The Target of Evaluation (TOE) included the following hardware and software:

a) **Hardware.**

   i) nGenius 5010-16X PFS

   ii) nGenius 5100 PFS

   iii) nGenius 5110 PFS

   iv) nGenius 7010 PFS

   v) nGenius 7100 PFS

   vi) nGenius 7110 PFS

   vii) nGenius 5120 PFS

   viii) nGenius 7120 PFS

b) **Software.** Packet Flow Operating Software (PFOS) 6.0.6 Build 6.0.6.4

1.3.3 Evaluated Functions

7 The following functions have been evaluated under Common Criteria:

a) **Protected Communications.** The TOE provides secure communication channels:

i) **CLI.** Administrator access to the CLI via direct serial connection or SSH.

ii) **GUI.** Administrator access to the Web GUI over HTTPS.

iii) **Logs.** Secure transmission of log events to a Syslog server via SSH.

iv) **OCSP Responder.** X.509v3 certificate revocation checking via OCSP

b) **Secure Administration.** The TOE enables secure management of its security functions, including:

i) Administrator authentication with passwords (local users)

ii) Configurable password policies

iii) Role Based Access Control

iv) Access banners

v) Management of critical security functions and data

vi) Protection of cryptographic keys and passwords

c) **Trusted Update.** The TOE ensures the authenticity and integrity of software updates via published hash.

d) **System Monitoring.** The TOE generates logs of security relevant events. The TOE stores logs locally and is capable of sending log events to a remote audit server.

e) **Self-Test.** The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions.

f) **Cryptographic Operations.** The cryptographic algorithms used in the above functions have been validated for correct implementation.

8 **NOTE:** No claims are made regarding any other security functionality.

9 **NOTE:** The Security Administrator has full access and permissions to the TOE.

1.3.4 Evaluation Assumptions

10 The following assumptions were made in performing the Common Criteria evaluation. The guidance shown in the table below should be followed to uphold these assumptions in the operational environment.

Table 1: Evaluation Assumptions

Assumption	Guidance
Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	Ensure that the device is hosted in a physically secure environment, such as a locked server room.
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.	Do not install other software on the device hardware.
The TOE does not provide any protection of traffic that traverses it. It is assumed that	The Common Criteria evaluation focused on

Assumption	Guidance
protection of this traffic will be covered by other security and assurance measures in the operational environment.	the management plane of the device.
Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.	Ensure that administrators are trustworthy – e.g. implement background checks or similar controls.
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.	Apply updates regularly according to your organization's policies.
The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.	Administrators should take care to not disclose credentials and ensure private keys are stored securely.
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 should sanitize the device before disposal or transfer out of the organization's control.

1.4 Conventions

11 The following conventions are used in this guide:

a) `CLI Command <replaceable>` - This style indicates to you that you can type the word or phrase on the command line and press [Enter] to invoke a command. Text within <> is replaceable. For example:

Use the `cat <filename>` command to view the contents of a file

b) [key] or [key-combo] – key or key combination on the keyboard is shown in this style. For example:

The [Ctrl]-[Alt]-[Backspace] key combination exits your graphical session and returns you to the graphical login screen or the console.

c) **GUI > Reference** – denotes a sequence of GUI screen interactions. For example:

Select **File > Save** to save the file.

d) [REFERENCE] *Section* – denotes a document and section reference from Table 2. For example:

Follow [ADMIN] *Configuring Users* to add a new user.

1.5 Related Documents

12 This guide supplements the below documents.

Table 2: Related Documents

Reference	Document
[ST]	NETSCOUT nGenius 5000 & 7000 Series Packet Flow Switches with PFOS 6.0.6 Security Target, v1.6 | April 2022
[INSTALL]	nGenius PFS 5000 Series Packet Flow Switches Quick Connection Guide PFOS Installation Guide for Qualified PFS Devices
[USER]	NETSCOUT Packet Flow Operating Software (PFOS) 6.x User Guide v6.0.6, 733-1485 | December 2021
[CLI]	NETSCOUT Packet Flow Operating Software (PFOS) 6.x CLI Reference Guide v6.0.6, 733-1486 | December 2021
[REL]	NETSCOUT Packet Flow Operating Software (PFOS) 6.x Release Notes v6.0.6, 733-1488 | April 2022 Rev.C

13 **NOTE:** The information in this guide supersedes related information in other documentation.

2 Secure Acceptance and Update

2.1 Obtaining the TOE

14 Your PFS 5000 appliance will be delivered via commercial courier. Perform the following checks upon receipt (return the device if either of the checks fail):

a) Confirm that the correct device has been delivered

b) Inspect the packaging to confirm that there are no signs of tampering

15 Refer to [USER] *Upgrading PFOS* on requirements for obtaining the TOE software.

2.2 Verifying the TOE

16 Refer to [USER] section *Managing With PFOS* subsection *System Status* on steps to verify the currently installed version of TOE software.

17 TOE software is verified by means of a published hash as follows:

a) Published hashes are provided by NETSCOUT and are available on the NETSCOUT support website.

b) Verification is done manually by the Security Administrator by comparing the SHA256 checksum published on the NETSCOUT support website.

2.3 Power-on Self-Tests

18 On start-up, the system will run a series of self-tests:

a) **POST.** The system runs Power-On diagnostic Self-Test (POST) every time it starts until disabled.

b) **FIPS Self-tests.** The TOE checks the integrity of the system files at the startup.

19 Any failure of the POST test writes a diagnostic code to the console (an LCD K/V/M or a terminal connected to the serial port) and sounds a beep code on the system speaker. Depending on the severity of the error, the boot-up may halt.

a) If an error occurs, power down the system, check all cables and retry the power on sequence.

b) If a hardware error persists, record the error codes or symptoms, and if possible, take a screen shot of the errors. Contact NETSCOUT Customer Support for assistance.

20 The TOE runs FIPS-Approved power-up self-tests (during power-up or reboot of the TOE) and conditional self-tests. If any of the self-tests fail to produce the expected outcome, failure of any of these tests will cause the module startup to fail and write a failure message to the appropriate log file.

21 All of the above errors result in a critical error state and an administrator must reboot the TOE to run the self tests again by using the appliance's power button. Once the self-tests successfully pass, the appliance will start up successfully. The log messages displaying the error messages can then be viewed via the Syslog viewer.

2.4 Updating the TOE

22 Follow instructions at [USER] *Upgrading PFOS* to update the TOE. Verify the integrity and authenticity of TOE software prior to installation per instructions above at 2.2.

23 The TOE supports delayed activation of a newly loaded software image. More information on performing an update with this feature can be found in [REL] section *3 – Upgrading Software and Firmware.*

3 Configuration Guidance

3.1 Installation

24 Follow the instructions of [INSTALL] and [USER] augmented by the configuration steps in the following sections.

3.2 Administrative Roles (RBAC)

25 The TOE consists of the following administrative roles for the purposes of providing role-based access control:

a) **Security Administrator.** This role provides full access and permissions to the TOE for local and remote administration of all security functions.

3.3 Administration Interfaces

26 Only the following administration interfaces may be used:

a) **CLI / Console.** Directly connected via RJ45 to female DB9 cable to the RJ45 console port.

   i) Session termination is supported and may be configured via `config access-policy`

   ii) Account lockouts are enforced and may be configured via `config access-policy login user-lockout-duration`

   iii) Banner messages are supported and may be configured via `system banner <text>`

b) **CLI / SSH.** Remote access to the CLI interface via SSH.

c) **GUI / HTTPS.** Web based Graphical User Interface.

   i) The TOE supports the addition of OCSP responder to configure and manage instructions on configuring certificates and generate signing requests.

   ii) Banner messages are supported and may be configured via `CLI command` described above.

   iii) Session termination is supported and may be configured via **Global Settings > Access Control > Session Limit**

   iv) Account lockouts are enforced and may be configured via **Global Settings > Access Control > User Lockout**

27 Terminating a local or remote session can be achieved by clicking the ‘Logout’ button in the Web UI or typing “exit” at the command line. Sessions that are not properly terminated are addressed with the idle timeout function which terminates inactive sessions after 30 minutes by default.

3.4 Cryptography

28 Enable FIPS mode per instructions at [USER] *FIPS Mode*

29 **Note:** This ensures that the TOE is configured to use approved algorithms. No further configuration is required to achieve the Common Criteria cryptographic configuration.

30 To install a leaf certificate:

a) Upload a server/leaf (example: leaf.crt) certificate to the ‘Certificate’ section under File Management

b) Upload an intermediate+root ca bundle (example: bundle.crt) to the ‘Certificate Authority’ section under File Management

3.5 Default Passwords

31 The following accounts have default credentials:

a) **admin.** Default account. Follow the instructions at [USER] *Change a Password* to set a new password for this account.

3.6 Setting Time

32 The use of NTP has not been evaluated. Set the time manual per instructions at [USER] *Manual Time Setting.*

3.7 Audit Logging

33 The Common Criteria evaluation confirmed that the log events listed at Annex A: Log Reference are generated by the TOE.

34 A syslog server must be configured to store the logs as follows:

a) Define at least one Syslog server per [USER] section *Configuring the System and Ports* subsection *Send System Logs to Remote Server over SSH Tunnel.*

b) The TOE establishes a secure channel with the Syslog Server using SSH.

c) The TOE attempts to reconnect the session until a certain number of attempts are made, then initiates a new session with a new handshake.

35 The TOE stores logs locally and sends them to syslog in real-time. When the local logs space is full, the TOE will overwrite the oldest logs.

36 Additional journal logs can be found on the TOE by navigating to the following on the WebUI:
System Administration > File Management > Download File from Chassis > Download Individual File(s) and selecting the ***‘Journal’*** directory.

3.8 Administrator Authentication

37 The minimum administrator passwords length may be set to between 9 and 15 characters. Passwords may include special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”

3.9 Certificate Management

38 Detailed information on certificate management by the TOE can be found in [USER] section *Maintenance* subsection *Maintaining Certificate Files*.

39 Certificate revocation checking is conducted via the Online Certificate Status Protocol (OCSP) as described in [USER] Section *3-Configuring the System and Ports* subsection *System Settings > Features > Common Criteria Mode > Online Certificate Status Protocol.*

3.10 Key Management

40 **SSH.** Detailed information on SSH key management by the TOE can be found in [USER] section *Maintenance* subsection *Maintaining SSH Public Key Files*.

41 **TLS.** More information on TLS key management by the TOE can be found in [USER] section *Maintenance* subsection *Maintaining Certificate Files.*

42 Key destruction methods are described in [USER] section *Maintenance* subsection *Maintaining SSH Public Key Files* and [CLI] section *General CLI Commands* subsection *delete ssh-key.*

Annex A: Log Reference

3.11 Format

43 Each audit record includes the following fields:

a) Timestamp

b) Severity Level (info, warn)

c) Message (including user if applicable and indication of success or failure)

3.12 Events

44 The TOE generates the following log events.

Table 3: Audit Events

Requirement	Auditable Events	Example Event
FAU_GEN.1	Start-up and shutdown of the audit functions	Oct 8 11:48:38 10.19.7.10 98 <5>1 2020-10-08T15:48:34+00:00 10.19.7.10 PFS5010 - - - Sys. Reboot is issued by admin for mgmt-1
	Administrative login	GUI: Oct 8 11:32:10 10.19.7.10 137 <29>1 2020-10-08T15:31:54+00:00 10.19.7.10 PFS5010 - - - SysAccCtl. Logged in User:admin,IP:172.16.200.42,Context:webui,AccessType:HTTPS SSH: Oct 8 11:36:17 10.19.7.10 133 <29>1 2020-10-08T15:36:13+00:00 10.19.7.10 PFS5010 - - - SysAccCtl. Logged in User:admin,IP:172.16.200.42,Context:cli,AccessType:SSH
	Administrative logout	GUI: Oct 8 11:37:04 10.19.7.10 138 <29>1 2020-10-08T15:37:00+00:00 10.19.7.10 PFS5010 - - - SysAccCtl. Logged out User:admin,IP:172.16.200.42,Context:webui,AccessType:HTTPS SSH: Oct 8 11:37:51 10.19.7.10 134 <29>1 2020-10-08T15:37:47+00:00 10.19.7.10 PFS5010 - - - SysAccCtl. Logged out

Requirement	Auditable Events	Example Event
		User:admin,IP:172.16.200.42,Context:cli,AccessType:SSH
	Changes to TSF data related to configuration changes	Users: Oct 8 11:39:16 10.19.7.10 124 <29>1 2020-10-08T15:39:13+00:00 10.19.7.10 PFS5010 - - - SysCfgChg. Acc Ctl user travis is modified: password Chgd by admin Syslog: Oct 8 11:29:48 10.19.7.10 147 <29>1 2020-10-08T15:11:13+00:00 10.19.7.10 PFS5010 - - - SysCfgChg. Syslog server created: "ip: 10.19.7.2 port:514 proto:tcp level:debug" by admin
	Generating/import of cryptographic keys	Oct 8 15:43:34 10.19.7.10 114 <29>1 2020-10-08T19:43:22+00:00 10.19.7.10 PFS5010 - - - Sys. Certificate File root-ca.key uploaded by user admin Oct 8 15:43:34 10.19.7.10 114 <29>1 2020-10-08T19:43:22+00:00 10.19.7.10 PFS5010 - - - Sys. Certificate File root-ca.crt uploaded by user admin Oct 8 15:45:10 10.19.7.10 111 <29>1 2020-10-08T19:44:58+00:00 10.19.7.10 PFS5010 - - - Sys. Certificate File int1.key uploaded by user admin Oct 8 15:45:10 10.19.7.10 111 <29>1 2020-10-08T19:44:58+00:00 10.19.7.10 PFS5010 - - - Sys. Certificate File int1.crt uploaded by user admin Oct 8 15:46:02 10.19.7.10 120 <29>1 2020-10-08T19:45:51+00:00 10.19.7.10 PFS5010 - - - Sys. Certificate File syslog-client.key uploaded by user admin Oct 8 15:46:02 10.19.7.10 120 <29>1 2020-10-08T19:45:51+00:00 10.19.7.10 PFS5010 - - - Sys. Certificate File syslog-client.crt

Requirement	Auditable Events	Example Event
		uploaded by user admin
	Deleting of cryptographic keys	Oct 13 15:52:40 10.19.7.10 PFS5010: Sys. ssh public key file id_rsa2.pub is deleted by user admin
	Resetting Passwords	Oct 8 11:39:16 10.19.7.10 124 <29>1 2020-10-08T15:39:13+00:00 10.19.7.10 PFS5010 - - - SysCfgChg. Acc Ctl user travis is modified: password Chgd by admin
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Covered under FCS_TLSS_EXT.1 and FIA_X509_EXT.1
FCS_SSHC_EXT.1	Failure to establish an SSH session	2001-01-10T21:20:23+00:00 PFS5010 - - - - ssh_client root@10.100.1.156: Permission denied (publickey,password,keyboard-interactive).
FCS_SSHS_EXT.1	Failure to establish an SSH session	2021-05-19T13:51:40+00:00 10.19.7.10 PFS5010 - - - SysAccCtl. Login failed User:admin,IP:172.16.200.18,Context: cli,AccessType:SSH,reason:noauth
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Oct 13 17:05:34 10.19.7.10 PFS5010: SysAccCtl. SSL_do_handshake() failed, error 193 - No shared cipher client: 172.16.200.42
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Oct 14 13:47:32 10.19.7.10 PFS5010: SysAccCtl. User:travis,IP:172.16.200.42,Context:webui,AccessType:HTTPS,reason: User blocked Oct 14 13:47:32 10.19.7.10 PFS5010: SysAccCtl. User:travis,IP:172.16.200.42,Context:webui,AccessType:HTTPS,reason: IP blocked
FIA_UIA_EXT.1	All use of identification and	Oct 9 15:58:41 10.19.7.10 PFS5010: SysAccCtl. Logged in

Requirement	Auditable Events	Example Event
	authentication mechanism.	User:admin,IP:172.16.200.42,Context:webui,AccessType:HTTPS
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	GUI: Oct 8 13:52:39 10.19.7.10 138 <29>1 2020-10-08T17:52:28+00:00 10.19.7.10 PFS5010 - - - SysAccCtl. Logged out User:admin,IP:172.16.200.42,Context:webui,AccessType:HTTPS SSH: Oct 8 13:08:17 10.19.7.10 130 <29>1 2020-10-08T17:08:14+00:00 10.19.7.10 PFS5010 - - - SysAccCtl. Logged out User:admin,IP:10.19.7.2,Context:cli,AccessType:SSH
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	Oct 21 08:50:10 10.19.7.10 123 <29>1 2020-10-21T12:50:06+00:00 10.19.7.10 PFS5010 - - - Sys. Certificate File server-rsa2.cert.crt uploaded by user admin Oct 21 08:50:30 10.19.7.10 118 <29>1 2020-10-21T12:50:25+00:00 10.19.7.10 PFS5010 - - - Sys. Certificate File server-rsa2.key uploaded by user admin Oct 21 08:50:55 10.19.7.10 119 <29>1 2020-10-21T12:50:50+00:00 10.19.7.10 PFS5010 - - - Sys. Certificate server-rsa2.cert.crt installed by user admin
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	See FPT_TUD_EXT.1
FMT_SMF.1	All management activities of TSF data.	Syslog: Oct 8 11:29:48 10.19.7.10 147 <29>1 2020-10-08T15:11:13+00:00 10.19.7.10 PFS5010 - - - SysCfgChg. Syslog server created: "ip: 10.19.7.2 port:514 proto:tcp level:debug" by admin Users: Oct 8 14:20:09 10.19.7.10 137 <29>1 2020-10-08T18:19:57+00:00 10.19.7.10 PFS5010 - - - SysCfgChg. Acc Ctl

Requirement	Auditable Events	Example Event
		user travis is modified: password Set, role:created by admin Banner: Oct 8 14:31:29 10.19.7.10 99 <29>1 2020-10-08T18:31:17+00:00 10.19.7.10 PFS5010 - - - SysCfgChg. System Banner changed by admin
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	May 18 17:55:20 10.100.1.156 173 <29>1 2001-02-25T06:06:12+00:00 10.19.7.10 PFS5010 - - - Sys. VXOS software pkg vxos_core_PFS5k_6.0.3.31-989f4123 is set to be installed on nextboot by user admin on mgmt-1
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)	Oct 8 13:52:19 10.19.7.10 142 <29>1 2020-10-08T17:52:08+00:00 10.19.7.10 PFS5010 - - - SysCfgChg. Sytem clock Chgd from 2020-10-07 17:52:14 to 2020-10-08 17:52:08 by admin
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	Oct 12 14:30:10 10.19.7.10 PFS5010: SysCfgChg. System CLI idle timeout changed from 'PT5M0S.0' to 'PT10M0S.0' by admin Oct 12 14:31:06 10.19.7.10 PFS5010: SysAccCtl. Logged in User:admin,IP:172.16.200.42,Context:cli,AccessType:HTTP Oct 12 14:41:07 10.19.7.10 PFS5010: SysAccCtl. Logged out User:admin,IP:172.16.200.42,Context:cli,AccessType:HTTP, reason:Idle-Timeout
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	Oct 12 14:30:10 10.19.7.10 PFS5010: SysCfgChg. System CLI idle timeout changed from 'PT5M0S.0' to 'PT10M0S.0' by admin Oct 12 15:02:34 10.19.7.10 PFS5010: SysAccCtl. Logged in

Requirement	Auditable Events	Example Event
		User:admin,IP:10.19.7.2,Context:cli ,AccessType:SSH Oct 12 15:12:36 10.19.7.10 PFS5010: SysAccCtl. Logged out User:admin,IP:10.19.7.2,Context:cli ,AccessType:SSH, reason:Idle-Timeout
FTA_SSL.4	The termination of an interactive session.	WebGUI: Oct 12 15:23:52 10.19.7.10 PFS5010: SysAccCtl. Logged in User:admin,IP:172.16.200.42,Cont ext:cli,AccessType:HTTP Oct 12 15:23:58 10.19.7.10 PFS5010: SysAccCtl. Logged out User:admin,IP:172.16.200.42,Cont ext:cli,AccessType:HTTP SSH: Oct 12 15:29:41 10.19.7.10 PFS5010: SysAccCtl. Logged in User:admin,IP:10.19.7.2,Context:cli ,AccessType:SSH Oct 12 15:29:44 10.19.7.10 PFS5010: SysAccCtl. Logged out User:admin,IP:10.19.7.2,Context:cli ,AccessType:SSH
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Failure of trusted channel May 18 18:24:34 10.100.1.156 743 <30>1 2001-01-15T00:04:17+00:00 PFS5010 sshd 4293 - [journald PRIORITY="6" SYSLOG_FACILITY="3" _UID="0" _GID="0" _CA P_EFFECTIVE="3fffffffff" _SYSTEMD_SLICE="system.slice" _BOOT_ID="bc9cd9b1602b4aacbe 6dc9f9e759ede5" _MACHINE_ID="94744b4e327e42 a1a3db54a02b904354" _TR ANSPORT="stdout" SYSLOG_IDENTIFIER="sshd" _COMM="sshd" _EXE="/usr/sbin/sshd" _SYSTEMD_CGROUP="/system.sl ice/sshd.service" _SYSTEMD_UNIT="sshd.service " _PID="4293" _HOSTNAME="PFS5010"

Requirement	Auditable Events	Example Event
		_CMDLINE="sshd: /usr/sbin/sshd -e [listener\] 1 of 10-100 startup" MESSAGE="Disconnecting authenticating user admin 10.100.1.156 port 46524: Too many authentication failures [preauth\]"] Disconnecting authenticating user admin 10.100.1.156 port 46524: Too many aut hentication failures [preauth]
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	May 18 17:42:04 10.100.1.156 136 <29>1 2001-02-25T05:51:27+00:00 10.19.7.10 PFS5010 - - - SysAccCtl. Logged in User:admin,IP:10.100.1.156,Context:web ui,AccessType:HTTPS May 18 17:42:31 10.100.1.156 137 <29>1 2001-02-25T05:51:58+00:00 10.19.7.10 PFS5010 - - - SysAccCtl. Logged out User:admin,IP:10.100.1.156,Context:we bui,AccessType:HTTPS May 18 17:42:52 10.100.1.156 153 <28>1 2001-02-25T05:52:21+00:00 10.19.7.10 PFS5010 - - - SysAccCtl. Login failed User:admin,IP:10.100.1.156,Context: webui,AccessType:HTTPS,reason:noauth May 18 17:43:07 10.100.1.156 762 <30>1 2001-02-25T05:52:37+00:00 PFS5010 sshd 4300 - [journald PRIORITY="6" _UID="0" _GID="0" _CAP_EFFECTIVE="3fffffffff" _SYSTEMD_SLICE="system.slice" _BOOT_ID="51b8a5cd746046038d035db6d7884b24" _MACHINE_ID="94744b4e327e42a1a3db54a02b904354" _HOSTNAME="PFS5010" _TRANSPORT="stdout" SYSLOG_FACILITY="3" SYSLOG_IDENTIFIER="sshd" _PID="4300" _COMM="sshd"

Requirement	Auditable Events	Example Event
		_EXE="/usr/sbin/sshd" _CMDLINE="sshd: /usr/sbin/sshd -e [listener\] 1 of 10-100 startup" _SYSTEMD_CGROUP="/system.slice/sshd.service" _SYSTEMD_UNIT="sshd.service" MESSAGE="Failed publickey for admin from 172.16.200.18 port 56644 ssh2: RSA SHA256:/DscqBxVTEVisTd4FyRGT3MlGiGoisthGH462ODX75E"] Failed publickey for admin from 172.16.200.18 port 56644 ssh2: RSA SHA256:/DscqBxVTEVisTd4FyRGT3MlGiGoisthGH462ODX75E May 18 17:43:09 10.100.1.156 150 <28>1 2001-02-25T05:52:39+00:00 10.19.7.10 PFS5010 - - - SysAccCtl. Login failed User:admin,IP:172.16.200.18,Context:cli,AccessType:SSH,reason:no auth May 18 17:43:11 10.100.1.156 133 <29>1 2001-02-25T05:52:42+00:00 10.19.7.10 PFS5010 - - - SysAccCtl. Logged in User:admin,IP:172.16.200.18,Context:cli,AccessType:SSH May 18 17:43:14 10.100.1.156 134 <29>1 2001-02-25T05:52:45+00:00 10.19.7.10 PFS5010 - - - SysAccCtl. Logged out User:admin,IP:172.16.200.18,Context:cli,AccessType:SSH