CIS Palo Alto Networks NDM STIG Benchmark

v1.0.0 - 09-09-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

Target Technology Details

Palo Alto Networks NDM Secure Technical Implementation Guide (STIG)

Version: 3 Release: 3 Benchmark

Date: 02 Apr 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Palo Alto Networks NDM and are looking to comply with the STIG guidance

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Palo Alto Networks NDM

Recommendations

1 STIG RULES

Palo Alto Networks

Palo Alto Networks NDM Secure Technical Implementation Guide (STIG)

Version: 3 Release: 3 Benchmark

Date: 02 Apr 2025

CLASSIFICATION unclassified

1.1 PANW-NM-000015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Palo Alto Networks security platform must enforce the limit of three consecutive invalid logon attempts.

```
GROUP ID: V-228639
RULE ID: SV-228639r1082941
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced.

Audit:

Go to Device >> Authentication Profile.

Check the authentication profile used for the local account used for the account of last resort.

If the "Failed Attempts (#)" field is not set to "3", this is a finding.

Remediation:

Configure the authentication profile associated with the account of last resort with lockout settings of three failed attempts, which is the only local login account.

1. Go to Device >> Authentication Profile.
2. Select the configured authentication profile or select "Add" (in the bottom-left corner of the pane) to create a new one.
3. In the "Authentication Profile" field, enter the name of the authentication profile that will be used to control each person's authentication process.
4. The "Lockout Time (min)" field is the lockout duration; this must be set to "15".
5. In the "Failed Attempts" field, enter "3".
6. Select "OK".

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

1.2 PANW-NM-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Palo Alto Networks security platform must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the device.

```
GROUP ID: V-228640
RULE ID: SV-228640r960843
```

Rationale:

Display of the DoD-approved use notification before granting access to the network device ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users.

Audit:

View the logon screen of the Palo Alto Networks security platform. A white text box at the bottom of the screen will contain the configured text.

If it is blank (there is no white text box) or the wording is not one of the approved banners, this is a finding.

This is the approved verbiage for applications that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

```
"I've read & consent to terms in IS user agreem't."
```

Remediation:

1. Go to Device >> Setup >> Management >> General Settings ("Edit" icon) >> Login Banner
2. Type in the required text
3. Select "OK".
4. Commit changes by selecting "Commit" in the upper-right corner of the screen.
5. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53::AC-8 a
- NIST SP 800-53A::AC-8.1 (ii)
- NIST SP 800-53 Revision 4::AC-8 a
- NIST SP 800-53 Revision 5::AC-8 a

1.3 PANW-NM-000024 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Palo Alto Networks security platform must generate audit records when successful/unsuccessful attempts to access privileges occur.

```
GROUP ID: V-228642
RULE ID: SV-228642r960885
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

By default, the Configuration Log contains the administrator username, client (Web or CLI), and date and time for any changes to configurations and for configuration commit actions. The System Log also shows both successful and unsuccessful attempts for configuration commit actions.

The System Log and Configuration Log can be configured to send log messages by severity level to specific destinations; the Panorama management console, an SNMP console, an e-mail server, or a syslog server. Since both the System Log and Configuration Log contain information concerning the use of privileges, both must be configured to send messages to a syslog server at a minimum.

Audit:

Go to Device >> Log Settings >> System

If any severity level does not have a Syslog Profile, this is a finding.

Remediation:

Create a syslog server profile.

1. Go to Device >> Server Profiles >> Syslog
2. Select "Add"
3. In the "Syslog Server Profile", enter the name of the profile; select "Add".
4. In the "Servers" tab, enter the required information.
5. Name: Name of the syslog server
6. Server: Server IP address where the logs will be forwarded to
7. Port: Default port 514
8. Facility: Select from the drop down list
9. Select "OK".
10. Go to Device >> Log Settings >> System
11. For each severity level, select which destinations should receive the log messages. Note: The "Syslog Profile" field must be completed.
12. Commit changes by selecting "Commit" in the upper-right corner of the screen.
13. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

1.4 PANW-NM-000029 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Palo Alto Networks security platform must produce audit log records containing information (FQDN, unique hostname, management IP address) to establish the source of events.

```
GROUP ID: V-228643
RULE ID: SV-228643r960900
```

Rationale:

In order to compile an accurate risk assessment and provide forensic analysis, it is essential for security personnel to know the source of the event. The source may be a component, module, or process within the device or an external session, administrator, or device. Associating information about where the source of the event occurred provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured device.

The device must have a unique hostname that can be used to identify the device; fully qualified domain name (FQDN), hostname, or management IP address is used in audit logs to identify the source of a log message.

Audit:

Go to Device >> Setup >> Management

In the "General Settings" window, if the "hostname" field does not contain a unique identifier, this is a finding.

Go to Device >> Setup >> Management

In the "Logging and Reporting Settings" pane, if the "Send Hostname in Syslog" does not show either "FQDN", "hostname", "ipv4-address", or "ipv6-address", this is a finding.

Remediation:

Set a unique hostname.

1. Go to Device >> Setup >> Management
2. in the "General Settings" window, select the "Edit" icon (the gear symbol in the upper-right corner of the pane).
3. In the "General Settings" window, in the "hostname" field; enter a unique hostname.
4. Select "OK".

Configure the device to send the FQDN, hostname, ipv4-address, or ipv6-address with log messages.

1. Device >> Setup >> Management
2. Click the "Edit" icon in the "Logging and Reporting Settings" section.
3. Select the "Log Export and Reporting" tab.
4. Select one of the following options from the "Send Hostname in the Syslog" drop-down list:
5. FQDN — (the default) Concatenates the hostname and domain name defined on the sending device.
6. hostname — Uses the hostname defined on the sending device.
7. ipv4-address —Uses the IPv4 address of the interface used to send logs on the device. By default, this is the management interface of the device.
8. ipv6-address —Uses the IPv6 address of the interface used to send logs on the device. By default, this is the management interface of the device.
9. Note that the last two selections must be consistent with the IP address used by the management interface.
10. Select "OK".
11. Commit changes by selecting "Commit" in the upper-right corner of the screen. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-000133 Ensure that audit records containing information that establishes the source of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 d

1.5 PANW-NM-000046 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Palo Alto Networks security platform must be configured to prohibit the use of all unnecessary and/or nonsecure functions, ports, protocols, and/or services, as defined in the PPSM CAL and vulnerability assessments.

```
GROUP ID: V-228645
RULE ID: SV-228645r1043177
```

Rationale:

In order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable unused or unnecessary physical and logical ports/protocols on information systems.

Network devices are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., email and web services); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the network device must support the organizational requirements providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues.

The Palo Alto Networks security platform uses a hardened operating system in which unnecessary services are not present. The device has a DNS, NTP, update, and e-mail client installed. Note that these are client applications and not servers; additionally, each has a valid purpose. However, local policy may dictate that the update service, e-mail client, and statistics (reporting) service capabilities not be used. DNS can be either "Server" or "Proxy"; both are allowed unless local policy declares otherwise. NTP and SNMP are necessary functions.

Audit:

Go to Device >> Setup >> Services

In the "Services" window, view which services are configured.

Note: DNS can be either "Server" or "Proxy"; both are allowed unless local policy declares otherwise.

Note: The Palo Alto Networks security platform cannot be a DNS server, only a client or proxy.

NTP is a necessary service.

Note: The Palo Alto Networks security platform cannot be an NTP server, only a client.

Go to Device >> Setup >> Management

In the "Management Interface Settings" window, view the enabled services.

Note: Which management services are enabled. HTTPS, SSH, ping, and SNMP, are normally allowed.

If User-ID, User-ID Syslog Listener-SSL, User-ID Syslog Listener-UDP, or HTTP OCSP is present, verify with the ISSO that this has been authorized.

1. Go to Device >> Setup >> Operations tab>> Miscellaneous
2. Select SNMP Setup.
3. In the "SNMP Setup" window, check if SNMP V3 is selected.
4. If unauthorized services are configured, this is a finding.

Remediation:

Go to Device >> Setup >> Services

In the "Services" window, select the "Edit" icon (the gear symbol in the upper-right corner of the pane).

Note: DNS can be either "Server" or "Proxy"; both are allowed unless local policy declares otherwise.

Note: The Palo Alto Networks security platform cannot be a DNS server, only a client or proxy.

NTP is a necessary service.

Note: The Palo Alto Networks security platform cannot be an NTP server, only a client.

1. Go to Device >> Setup >> Management
2. In the "Management Interface Settings" window, select the "Edit" icon (the gear symbol in the upper-right corner of the pane).
3. In the "Management Interface Settings" window, select HTTP OCSP, HTTPS, SSH, SNMP, User-ID, User-ID Syslog Listener-SSL, User-ID Syslog Listener-UDP if these protocols will be used.
4. Select "OK".

Note: SNMP Versions 1 and 2 are not considered secure; use SNMP Version 3.

1. Device >> Setup >> Operations tab>> Miscellaneous
2. Select SNMP Setup.
3. In the "SNMP Setup" window, select V3.
4. Select "OK".
5. Commit changes by selecting "Commit" in the upper-right corner of the screen.
6. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (iii)
- NIST SP 800-53 Revision 4::CM-7 b
- NIST SP 800-53 Revision 5::CM-7 b

1.6 PANW-NM-000048 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Palo Alto device must be configured with only one local account to be used as the account of last resort in the event the authentication server is unavailable.

```
GROUP ID: V-268323
RULE ID: SV-268323r1084266
```

Rationale:

Authentication for administrative (privileged level) access to the device is required at all times. An account can be created on the device's local database for use when the authentication server is down or connectivity between the device and the authentication server is not operable. This account is referred to as the account of last resort since it is intended to be used as a last resort and when immediate administrative access is absolutely necessary.

The account of last resort logon credentials must be stored in a sealed envelope and kept in a safe. The safe must be periodically audited to verify the envelope remains sealed. The signature of the auditor and the date of the audit must be added to the envelope as a record. Administrators must secure the credentials and disable the root account (if possible) when not needed for system administration functions.

Audit:

Navigate to Device >> Administrators.

Review the user list.

If there is an authentication profile/user account configured (and enabled) for any account other than the emergency administration account, this is a finding.

Remediation:

Remove local users other than the designated account of last resort.

Using the Console UI:

1. Navigate to Device >> Administrators.
2. Select and delete local users other than the account of last resort.

Note: To protect against brute-force attacks, delete the default admin account by creating a new superuser administrator account, logging out, and logging back in using the new account.

Additional Information:

CCI-001358 Establish privileged user accounts in accordance with a role-based access scheme; or an attribute-based access scheme.

- NIST SP 800-53::AC-2 (7) (a)
- NIST SP 800-53A::AC-2 (7).1 (i)
- NIST SP 800-53 Revision 4::AC-2 (7) (a)
- NIST SP 800-53 Revision 5::AC-2 (7) (a)

CCI-002111 The organization identifies and selects the organization-defined information system account types of information system accounts which support organizational missions/business functions.

- NIST SP 800-53 Revision 4::AC-2 a

1.7 PANW-NM-000051 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Palo Alto Networks security platform must implement replay-resistant authentication mechanisms for network access to privileged accounts.

```
GROUP ID: V-228647
RULE ID: SV-228647r960993
```

Rationale:

A replay attack may enable an unauthorized user to gain access to the application. Authentication sessions between the authenticator and the application validating the user credentials must not be vulnerable to a replay attack. An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message.

Techniques used to address this include protocols using nonces (e.g., numbers generated for a specific one-time use) or challenges (e.g., TLS, WS_Security). Additional techniques include time-synchronous or challenge-response one-time authenticators. Of the three authentication protocols on the Palo Alto Networks security platform, only Kerberos is inherently replay-resistant. If LDAP is selected, TLS must also be used. If RADIUS is used, the device must be operating in FIPS mode.

Audit:

Ask the Administrator which form of centralized authentication server is being used.

Navigate to the appropriate window to view the configured server(s).

- For RADIUS, go to Device >> Server Profiles >> RADIUS
- For LDAP, go to Device >> Server Profiles >> LDAP
- For Kerberos, go to Device >> Server Profiles >> Kerberos

If Kerberos is used, this is a not finding.
If LDAP is used, view the LDAP Server Profile; if the SSL checkbox is not checked, this is a finding.
If RADIUS is used, use the command line interface to determine if the device is operating in FIPS mode. Enter the CLI command "show fips-mode" or the command show fips-cc (for more recent releases).
If FIPS mode is set to "off", this is a finding.

Remediation:

To configure the Palo Alto Networks security platform to use an LDAP server with SSL/TLS.

1. Go to Device >> Server-Profiles >> LDAP
2. Select "Add" (lower left of window).
3. Populate the required fields.
4. Enter the name of the profile in the "Name" field.

In the server box:

1. Enter the name of the server in the "Name" field.
2. Enter the IP Address of the server.
3. Enter the Port number the firewall should use to connect to the LDAP server (default=389 for LDAP; 636 for LDAP over SSL).
4. Enter the LDAP Domain name to prepend to all objects learned from the server. The value entered here depends on the specific deployment. If using Active Directory, enter the NetBIOS domain name, not a FQDN (for example, enter acme, not acme.com). Note that if collecting data from multiple domains, it is necessary to create separate server profiles. If using a global catalog server, leave this field blank.
5. Select the Type of LDAP server connecting to. The correct LDAP attributes in the group mapping settings will automatically be populated based on the selection.
6. In the Base field, select the DN that corresponds to the point in the LDAP tree where the firewall is to begin its search for user and group information.
7. Select (check) the SSL checkbox.
8. Select "OK".
9. Commit changes by selecting "Commit" in the upper-right corner of the screen. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (8)
- NIST SP 800-53 Revision 5::IA-2 (8)

1.8 PANW-NM-000053 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

If multifactor authentication is not available and passwords must be used, the Palo Alto Networks security platform must enforce a minimum 15-character password length.

```
GROUP ID: V-228648
RULE ID: SV-228648r1018774
```

Rationale:

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password.

The shorter the password, the lower the number of possible combinations that needs to be tested before the password is compromised. Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Audit:

1. Go to Device >> Setup >> Management.
2. View the "Minimum Password Complexity" window.

If the "Minimum Length" field is not "15", this is a finding.

Remediation:

1. Go to Device >> Setup >> Management.
2. In the "Minimum Password Complexity" window, select the "Edit" icon (the gear symbol in the upper-right corner of the pane).
3. In the "Minimum Length" field, enter "15".
4. Check the "Enabled" box, then select "OK".
5. Commit changes by selecting "Commit" in the upper-right corner of the screen.
6. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000205 The information system enforces minimum password length.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (i)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

1.9 PANW-NM-000055 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

If multifactor authentication is not available and passwords must be used, the Palo Alto Networks security platform must enforce password complexity by requiring that at least one uppercase character be used.

```
GROUP ID: V-228650
RULE ID: SV-228650r1018775
```

Rationale:

Use of a complex passwords helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password is, the greater the number of possible combinations that needs to be tested before the password is compromised.

Audit:

1. Go to Device >> Setup >> Management.
2. View the "Minimum Password Complexity" window.

If the "Minimum Uppercase Letters" field is not "1", this is a finding.

Remediation:

1. Go to Device >> Setup >> Management.
2. In the "Minimum Password Complexity" window, select the "Edit" icon (the gear symbol in the upper-right corner of the pane).
3. In the "Minimum Uppercase Letters" field, enter "1".
4. Check the "Enabled" box, then select "OK".
5. Commit changes by selecting "Commit" in the upper-right corner of the screen.
6. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000192 The information system enforces password complexity by the minimum number of upper case characters used.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

1.10 PANW-NM-000056 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

If multifactor authentication is not available and passwords must be used, the Palo Alto Networks security platform must enforce password complexity by requiring that at least one lowercase character be used.

```
GROUP ID: V-228651
RULE ID: SV-228651r1018776
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that needs to be tested before the password is compromised.

Audit:

1. Go to Device >> Setup >> Management.
2. View the "Minimum Password Complexity" window.

If the "Minimum Lowercase Letters" field is not "1", this is a finding.

Remediation:

1. Go to Device >> Setup >> Management.
2. In the "Minimum Password Complexity" window, select the "Edit" icon (the gear symbol in the upper-right corner of the pane).
3. In the "Minimum Lowercase Letters" field, enter "1".
4. Check the "Enabled" box, then select "OK".
5. Commit changes by selecting "Commit" in the upper-right corner of the screen.
6. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000193 The information system enforces password complexity by the minimum number of lower case characters used.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

1.11 PANW-NM-000057 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

If multifactor authentication is not available and passwords must be used, the Palo Alto Networks security platform must enforce password complexity by requiring that at least one numeric character be used.

```
GROUP ID: V-228652
RULE ID: SV-228652r1018777
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that needs to be tested before the password is compromised.

Audit:

1. Go to Device >> Setup >> Management.
2. View the "Minimum Password Complexity" window.

If the "Minimum Numeric Letters" field is not "1", this is a finding.

Remediation:

1. Go to Device >> Setup >> Management.
2. In the "Minimum Password Complexity" window, select the "Edit" icon (the gear symbol in the upper-right corner of the pane).
3. In the "Minimum Numeric Letters" field, enter "1".
4. Check the "Enabled" box, then select "OK".
5. Commit changes by selecting "Commit" in the upper-right corner of the screen.
6. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000194 The information system enforces password complexity by the minimum number of numeric characters used.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

1.12 PANW-NM-000058 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

If multifactor authentication is not available and passwords must be used, the Palo Alto Networks security platform must enforce password complexity by requiring that at least one special character be used.

```
GROUP ID: V-228653
RULE ID: SV-228653r1018778
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that needs to be tested before the password is compromised.

Audit:

1. Go to Device >> Setup >> Management.
2. View the "Minimum Password Complexity" window.

If the "Minimum Special Letters" field is not "1", this is a finding.

Remediation:

1. Go to Device >> Setup >> Management.
2. In the "Minimum Password Complexity" window, select the "Edit" icon (the gear symbol in the upper-right corner of the pane).
3. In the "Minimum Special Letters" field, enter "1".
4. Check the "Enabled box", then select "OK".
5. Commit changes by selecting "Commit" in the upper-right corner of the screen.
6. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-001619 The information system enforces password complexity by the minimum number of special characters used.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

1.13 PANW-NM-000059 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

If multifactor authentication is not available and passwords must be used, the Palo Alto Networks security platform must require that when a password is changed, the characters are changed in at least 8 of the positions within the password.

```
GROUP ID: V-228654
RULE ID: SV-228654r1043189
```

Rationale:

If the application allows the user to consecutively reuse extensive portions of passwords, this increases the chances of password compromise by increasing the window of opportunity for attempts at guessing and brute-force attacks.

The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. In other words, characters may be the same within the two passwords; however, the positions of the like characters must be different.

Audit:

1. Go to Device >> Setup >> Management.
2. View the "Minimum Password Complexity" window.

If the "New Password Differs by Characters" field is not "8", this is a finding.

Remediation:

1. Go to Device >> Setup >> Management.
2. In the "Minimum Password Complexity" window, select the "Edit" icon (the gear symbol in the upper-right corner of the pane).
3. In the "New Password Differs by Characters" field, enter "8".
4. Check the "Enabled box", then select "OK".
5. Commit changes by selecting "Commit" in the upper-right corner of the screen.
6. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000195 The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.

- NIST SP 800-53::IA-5 (1) (b)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (b)

1.14 PANW-NM-000061 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Palo Alto Networks security platform must prohibit the use of unencrypted protocols for network access to privileged accounts.

```
GROUP ID: V-228655
RULE ID: SV-228655r961029
```

Rationale:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Network devices can accomplish this by making direct function calls to encryption modules or by leveraging operating system encryption capabilities.

Audit:

1. Go to Device >> Setup >> Management
2. View the "Management Interface Settings" pane.

If either Telnet or HTTP is listed in the "Services" field, this is a finding.

Remediation:

1. Go to Device >> Setup >> Management
2. In the "Management Interface Settings" window, select the "Edit" icon (the gear symbol in the upper-right corner of the pane). In the "Management Interface Settings" window, make sure that HTTP and Telnet are not checked (enabled).
3. If they are not checked, select either "OK" or "Cancel".
4. If either one is checked, select the check box to disable it, then select "OK".
5. If any changes were made, commit changes by selecting "Commit" in the upper-right corner of the screen.
6. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-000197 For password-based authentication, transmit passwords only over cryptographically-protected channels.

- NIST SP 800-53::IA-5 (1) (c)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (c)
- NIST SP 800-53 Revision 5::IA-5 (1) (c)

1.15 PANW-NM-000069 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Palo Alto Networks security platform must terminate management sessions after 10 minutes of inactivity except to fulfill documented and validated mission requirements.

```
GROUP ID: V-228658
RULE ID: SV-228658r961068
```

Rationale:

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. This does not mean that the device terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Device management sessions are normally ended by the Administrator when he or she has completed the management activity. The session termination takes place from the web client by selecting "Logout" (located at the bottom-left of the GUI window) or using the command line commands "exit" or "quit" at Operational mode.

Audit:

1. Go to Device >> Setup >> Management.
2. View the "Authentication Settings" pane.
3. If the "Idle Timeout (min)" field is not "10" or less, ask the Administrator to produce documentation signed by the Authorizing Official that the configured value exists to support mission requirements.

If this documentation is not made available, this is a finding.

Remediation:

1. Go to Device >> Setup >> Management.
2. In the "Authentication Settings" pane, select the "Edit" icon (the gear symbol in the upper-right corner of the pane).
3. In the "Idle Timeout (min)" field, enter "10", then select "OK".
4. Commit changes by selecting "Commit" in the upper-right corner of the screen.
5. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

1.16 PANW-NM-000075 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Administrators in the role of Security Administrator, Cryptographic Administrator, or Audit Administrator must not also have the role of Audit Administrator.

```
GROUP ID: V-228659
RULE ID: SV-228659r961863
```

Rationale:

The Palo Alto Networks security platform has both pre-configured and configurable Administrator roles. Administrator roles determine the functions that the administrator is permitted to perform after logging in. Roles can be assigned directly to an administrator account, or define role profiles, which specify detailed privileges, and assign those to administrator accounts.

There are three preconfigured roles designed to comply with Common Criteria requirements - Security Administrator, Audit Administrator, and Cryptographic Administrator. Of the three, only the Audit Administrator can delete audit records. The Palo Alto Networks security platform can use both pre-configured and configurable Administrator roles.

Audit:

For the roles of Security Administrator, Cryptographic Administrator, or Audit Administators, verify the same individual does not have more than one of these roles.

If the Palo Alto Networks security platform has any accounts where the same person is in the role of Security Administrator, Cryptographic Administrator, or Audit Administrator, this is a finding.

Remediation:

Do not assign or configure more than one account to the same Administrator. Also, neither the Security Administrator nor the Cryptographic Administrator can be have the role of Audit Administrator.

Note that the system allows each account to have only one role assigned. However, individuals, either accidentally or intentionally, may have more than one account.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

1.17 PANW-NM-000092 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Palo Alto Networks security platform must automatically lock the account until the locked account is released by an administrator when three unsuccessful logon attempts in 15 minutes are exceeded.

```
GROUP ID: V-228660
RULE ID: SV-228660r961863
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

This should not be configured in Device >> Setup >> Management >> Authentication Settings; instead, an authentication profile should be configured with lockout settings of three failed attempts and a lockout time of zero minutes. The Lockout Time is the number of minutes that a user is locked out if the number of failed attempts is reached (0-60 minutes, default 0). 0 means that the lockout is in effect until it is manually unlocked.

Audit:

Go to Device >> Administrators.

If there is no authentication profile configured for each account (aside from the emergency administration account), this is a finding.

Note which authentication profile is used for each account.

Go to Device >> Authentication Profile.

Check the authentication profile used for each account (noted in the previous step).

If the Lockout Time is not set to "0" (zero), this is a finding.

Remediation:

This should not be configured in Device >> Setup >> Management >> Authentication Settings; instead, an authentication profile should be configured with lockout settings of three failed attempts and a lockout time of zero minutes.

1. Go to Device >> Authentication Profile
2. Select the configured authentication profile, or select "Add" (in the bottom-left corner of the pane) to create a new one.
3. In the "Authentication Profile" field, enter the name of the authentication profile that will be used to control each person's authentication process.
4. The "Lockout Time (min)" field is the lockout duration; this must be set to "0". This will keep the lockout in effect until it is manually unlocked.
5. In the "Failed Attempts" field, enter "3".
6. Select "OK".

Apply the authentication profile to the Administrator accounts.

1. Go to Device >> Administrators
2. Select each configured account, or select "Add" (in the bottom-left corner of the pane) to create a new one.
3. In the "Authentication Profile" field, enter the configured authentication profile.
4. Select "OK".

This authentication profile should not be applied to the emergency administration account since it has special requirements.
Commit changes by selecting "Commit" in the upper-right corner of the screen.
Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

1.18 PANW-NM-000096 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Palo Alto Networks security platform must generate an immediate alert when allocated audit record storage volume reaches 75% of repository maximum audit record storage capacity.

```
GROUP ID: V-228661
RULE ID: SV-228661r961863
```

Rationale:

If security personnel are not notified immediately upon storage volume utilization reaching 75%, they are unable to plan for storage capacity expansion. This could lead to the loss of audit information. Note that while the network device must generate the alert, notification may be done by a management server.

Audit:

Go to Device >> Log Settings >> Alarms

If the Traffic Log DB, Threat Log DB, Configuration Log DB, System Log DB, Alarm DB, and HIP Match Log DB fields are not "75", this is a finding.

Remediation:

1. Go to Device >> Log Settings >> Alarms
2. Select the "Edit" icon (the gear symbol in the upper-right corner of the pane).

In the "Alarm Settings" window:

1. Select the "Enable Alarms" box.
2. In the "Traffic Log DB" field, enter "75".
3. In the "Threat Log DB" field, enter "75".
4. In the "Configuration Log DB" field, enter "75".
5. In the "System Log DB" field, enter "75".
6. In the "Alarm DB" field, enter "75".
7. In the "HIP Match Log DB" field, enter "75".
8. Select "OK".
9. Commit changes by selecting "Commit" in the upper-right corner of the screen. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

CCI-001855 Provide a warning to organization-defined personnel, roles, and/or locations within an organization-defined time period when allocated audit log storage volume reaches an organization-defined percentage of repository maximum audit log storage capacity.

- NIST SP 800-53 Revision 4::AU-5 (1)
- NIST SP 800-53 Revision 5::AU-5 (1)

1.19 PANW-NM-000097 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Palo Alto Networks security platform must have alarms enabled.

```
GROUP ID: V-228662
RULE ID: SV-228662r997675
```

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without a real-time alert, security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Alerts provide organizations with urgent messages. Real-time alerts provide these messages immediately (i.e., the time from event detection to alert occurs in seconds or less).

Audit:

Go to Device >> Log Settings >> Alarms.

If the "Enable Alarms" box is not checked, this is a finding.

Remediation:

1. Go to Device >> Log Settings >> Alarms.
2. Select the "Edit" icon (the gear symbol in the upper-right corner of the pane).
3. In the "Alarm Settings" window; select the "Enable Alarms" box.
4. Select "OK".
5. Commit changes by selecting "Commit" in the upper-right corner of the screen.
6. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-001858 Provide an alert in an organization-defined real-time-period to organization-defined personnel, roles, and/or locations when organization-defined audit failure events requiring real-time alerts occur.

- NIST SP 800-53 Revision 4::AU-5 (2)
- NIST SP 800-53 Revision 5::AU-5 (2)

CCI-003831 Alert organization-defined personnel or roles upon detection of unauthorized access, modification, or deletion of audit information.

- NIST SP 800-53 Revision 5::AU-9 b

1.20 PANW-NM-000098 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Palo Alto Networks security platform must compare internal information system clocks at least every 24 hours with an authoritative time server.

```
GROUP ID: V-228663
RULE ID: SV-228663r1018780
```

Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Network Time Protocol (NTP) is used to synchronize the system clock of a computer to reference time source. The Palo Alto Networks security platform can be configured to use specified NTP servers. For synchronization with the NTP server(s), NTP uses a minimum polling value of 64 seconds and a maximum polling value of 1024 seconds. These minimum and maximum polling values are not configurable on the firewall.

Audit:

Go to Device >> Setup >> Services.

In the "Services" window, the names or IP addresses of the Primary NTP Server and Secondary NTP Server must be present.

If the "Primary NTP Server" and "Secondary NTP Server" fields are blank, this is a finding.

Remediation:

1. Go to Device >> Setup >> Services.
2. Select the "Edit" icon (the gear symbol in the upper-right corner of the pane).
3. In the "Services" window, in the NTP tab, in the "Primary NTP Server Address" field and the "Secondary NTP Server Address" field, enter the IP address or hostname of the NTP servers.

In the "Authentication Type" field, select one of the following:

- **Symmetric Key**; this option uses symmetric key exchange, which are shared secrets. Enter the key ID, algorithm, authentication key, and confirm the authentication key; for the algorithm, select "SHA1".
- **Autokey**; this option uses auto key, or public key cryptography.
- Commit changes by selecting "Commit" in the upper-right corner of the screen.
- Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

CCI-004923 Compare the internal system clocks on an organization-defined frequency with organization-defined authoritative time source.

- NIST SP 800-53 Revision 5::SC-45 (1) (a)

CCI-001891 The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.

- NIST SP 800-53 Revision 4::AU-8 (1) (a)

1.21 PANW-NM-000099 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Palo Alto Networks security platform must synchronize internal information system clocks to the authoritative time source when the time difference is greater than one second.

```
GROUP ID: V-228664
RULE ID: SV-228664r1018781
```

Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

The Palo Alto Networks security platform can be configured to use specified Network Time Protocol (NTP) servers. NTP is used to synchronize the system clock of a computer to reference time source. Sources outside of the configured acceptable allowance (drift) may be inaccurate. When properly configured, NTP will synchronize all participating computers to within a few milliseconds of the reference time source.

Audit:

Go to Device >> Setup >> Services.

In the "Services" window, the names or IP addresses of the Primary NTP Server and Secondary NTP Server must be present.

If the "Primary NTP Server" and "Secondary NTP Server" fields are blank, this is a finding.

Remediation:

1. Go to Device >> Setup >> Services.
2. Select the "Edit" icon (the gear symbol in the upper-right corner of the pane).
3. In the "Services" window, in the "Primary NTP Server Address" field and the "Secondary NTP Server Address" field, enter the IP address or hostname of the NTP servers.

In the "Authentication Type" field, select one of the following:

- **None (default)**; this option disables NTP authentication.
- **Symmetric Key**; this option uses symmetric key exchange, which are shared secrets. Enter the key ID, algorithm, authentication key, and confirm the authentication key.
- **Autokey**; this option uses auto key, or public key cryptography.
- Commit changes by selecting "Commit" in the upper-right corner of the screen.
- Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

CCI-004926 Synchronize the internal system clocks to the authoritative time source when the time difference is greater than organization-defined time period.

- NIST SP 800-53 Revision 5::SC-45 (1) (b)

CCI-004923 Compare the internal system clocks on an organization-defined frequency with organization-defined authoritative time source.

- NIST SP 800-53 Revision 5::SC-45 (1) (a)

CCI-002046 The information system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than the organization-defined time period.

- NIST SP 800-53 Revision 4::AU-8 (1) (b)

1.22 PANW-NM-000100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Palo Alto Networks security platform must be configured to synchronize internal information system clocks with the primary and secondary time sources located in different geographic regions using redundant authoritative time sources.

```
GROUP ID: V-228665
RULE ID: SV-228665r1018782
```

Rationale:

The loss of connectivity to a particular authoritative time source will result in the loss of time synchronization (free-run mode) and increasingly inaccurate time stamps on audit events and other functions. Multiple time sources provide redundancy by including a secondary source. Time synchronization is usually a hierarchy; clients synchronize time to a local source while that source synchronizes its time to a more accurate source.

DOD-approved solutions consist of a combination of a primary and secondary time source using a combination or multiple instances of the following: a time server designated for the appropriate DOD network (NIPRNet/SIPRNet); United States Naval Observatory (USNO) time servers; and/or the Global Positioning System (GPS). The secondary time source must be located in a different geographic region from the primary time source.

Audit:

Go to Device >> Setup >> Services.

If there is only one NTP Server configured, this is a finding.

Ask the firewall administrator where the Primary NTP Server and Secondary NTP Server are located; if they are not in different geographic regions, this is a finding.

Remediation:

1. Go to Device >> Setup >> Services.
2. Select the "Edit" icon (the gear symbol in the upper-right corner of the pane).
3. In the "Services" window, in the "Primary NTP Server Address" field and the "Secondary NTP Server Address" field, enter the IP address or hostname of the NTP servers.

In the "Authentication Type" field, select one of the following:

- **None (default)**; this option disables NTP authentication.
- **Symmetric Key**; this option uses symmetric key exchange, which are shared secrets. Enter the key ID, algorithm, authentication key, and confirm the authentication key.
- **Autokey**; this option uses auto key, or public key cryptography.
- Commit changes by selecting "Commit" in the upper-right corner of the screen.
- Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

CCI-004928 Identify a secondary authoritative time source that is in a different geographic region than the primary authoritative time source.

- NIST SP 800-53 Revision 5::SC-45 (2) (a)

CCI-004922 Synchronize system clocks within and between systems or system components.

- NIST SP 800-53 Revision 5::SC-45

CCI-001893 The information system identifies a secondary authoritative time source that is located in a different geographic region than the primary authoritative time source.

- NIST SP 800-53 Revision 4::AU-8 (2)

1.23 PANW-NM-000101 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Palo Alto Networks security platform must record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).

```
GROUP ID: V-228666
RULE ID: SV-228666r961443
```

Rationale:

If time stamps are not consistently applied and there is no common time reference, it is difficult to perform forensic analysis. Time stamps generated by the application include date and time and must be expressed in Coordinated Universal Time (UTC), also known as Zulu time, a modern continuation of Greenwich Mean Time (GMT).

Audit:

Go to Device >> Setup >> Management

In the "General Settings" window, if the time zone is not set to "GMT" or "UTC", this is a finding.

Remediation:

1. Go to Device >> Setup >> Management
2. In the "General Settings" window, select the "Edit" icon (the gear symbol in the upper-right corner of the pane).
3. In the "General Settings" window, in the "Time Zone" field, select "GMT" or "UTC" from the list of time zones.
4. Select "OK".
5. Commit changes by selecting "Commit" in the upper-right corner of the screen. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-001890 Record time stamps for audit records that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

- NIST SP 800-53 Revision 4::AU-8 b
- NIST SP 800-53 Revision 5::AU-8 b

1.24 PANW-NM-000110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Palo Alto Networks security platform must accept and verify Personal Identity Verification (PIV) credentials.

```
GROUP ID: V-228667
RULE ID: SV-228667r997687
```

Rationale:

The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

DOD has mandated the use of the CAC to support identity management and personal authentication for systems covered under HSPD 12 and as a primary component of layered protection for national security systems.

Audit:

Go to Device >> Certificate Management >> Certificates.

If no DOD Certification Authority (CA) certificates and subordinate certificates are imported, this is a finding.

Go to Device >> Setup >> Management.

In the Authentication Settings pane, if the Certificate Profile field is blank, this is a finding.

View the Certificate Profile, if it does not list the DOD CA certificates and subordinate certificates, this is a finding.

If the Use OCSP checkbox is not selected, this is a finding.

Remediation:

Import the DOD CA certificates and subordinate certificates for all of the certificate authorities.

1. Go to Device >> Certificate Management >> Certificates.
2. Select the Import icon at the bottom of the pane.
3. In the Import Certificate window, complete the required information.
4. Select "OK".

Create a certificate profile.

1. Go to Device >> Setup >> Management.
2. In the Authentication Settings pane, select the select the "Edit" icon (the gear symbol in the upper-right corner).
3. In the Authentication Settings window, complete the required information.
4. In the Authentication Profile field, select "None".
5. In the Certificate Profile field, select "New Certificate Profile". This will change the Authentication Settings window to the Certificate Profile window.
6. Leave the username field blank.
7. Leave the domain field blank.
8. In the Certificate Profile window, complete the required fields.
9. In the CA Certificates section, select "Add" to import the DOD certificate authorities.
10. Select the Use OCSP checkbox.
11. When importing the top level DOD CA Certificate, for the Default OCSP URL field, add the DOD/DISA OCSP URL.
12. Select "OK".
13. Select "OK" again.
14. Commit changes by selecting "Commit" in the upper-right corner of the screen.
15. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

CCI-001953 Accept Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)
- NIST SP 800-53 Revision 5::IA-2 (12)

CCI-004068 For public key-based authentication, implement a local cache of revocation data to support path discovery and validation.

- NIST SP 800-53 Revision 5::IA-5 (2) (b) (2)

1.25 PANW-NM-000117 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Palo Alto Networks security platform must only allow the use of secure protocols that implement cryptographic mechanisms to protect the integrity of maintenance and diagnostic communications for nonlocal maintenance sessions.

```
GROUP ID: V-228669
RULE ID: SV-228669r961554
```

Rationale:

This requires the use of secure protocols instead of their unsecured counterparts, such as SSH instead of telnet, SCP instead of FTP, and HTTPS instead of HTTP. Note that HTTP OCSP is permitted to support OCSP where used. If unsecured protocols (lacking cryptographic mechanisms) are used for sessions, the contents of those sessions will be susceptible to manipulation, potentially allowing alteration and hijacking of maintenance sessions.

Audit:

Go to Device >> Setup >> Management

In the "Management Interface Settings" window, view the enabled services.

Note: Which management services are enabled.

If Telnet or HTTP is selected, this is a finding.

Remediation:

1. Go to Device >> Setup >> Management.
2. In the "Management Interface Settings" window, select the "Edit" icon (the gear symbol in the upper-right corner).
3. In the "Management Interface Settings" window, make sure that Telnet or HTTP are not selected.
4. Select "OK".
5. Commit changes by selecting "Commit" in the upper-right corner of the screen.
6. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-002890 Implement organization-defined cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4::MA-4 (6)
- NIST SP 800-53 Revision 5::MA-4 (6)

1.26 PANW-NM-000118 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Palo Alto Networks security platform must not use SNMP Versions 1 or 2.

```
GROUP ID: V-228670
RULE ID: SV-228670r961557
```

Rationale:

SNMP Versions 1 and 2 are not considered secure. Without the strong authentication and privacy that is provided by the SNMP Version 3 User-based Security Model (USM), an unauthorized user can gain access to network management information used to launch an attack against the network. SNMP Versions 1 and 2 cannot authenticate the source of a message nor can they provide encryption. Without authentication, it is possible for nonauthorized users to exercise SNMP network management functions. It is also possible for nonauthorized users to eavesdrop on management information as it passes from managed systems to the management system.

Audit:

Go to Device >> Setup >> Operations; in the Miscellaneous pane, select SNMP Setup.

In the SNMP Setup window, check if SNMP V3 is selected.

If V3 is not selected, this is a finding.

Go to Device >> Server Profiles >> SNMP Trap.

View the list of configured SNMP servers; if the Version is not "v3", this is a finding.

Remediation:

Go to Device >> Setup >> Operations; in the Miscellaneous pane, select SNMP Setup.

In the SNMP Setup window, complete the required fields.

For the Version, select V3.

1. Configure a view and assign it to a user.
2. In the upper half of the SNMP Setup window, select "Add".
3. In the Views window, complete the required fields; obtain the values for the OID and Mask fields from product documentation or vendor support.
4. In the Option field, select "include".
5. Select "OK".
6. In the lower half of the SNMP Setup window, select "Add".
7. Complete the required fields.
8. Select "OK".
9. Obtain the engineID of the Palo Alto device by issuing an SNMPv3 GET from the management workstation against the OID of the Palo Alto device.
10. Configure the SNMPv3 Trap Server profile; go to Device >> Server Profiles >> SNMP Trap; select "Add".
11. In the SNMP Trap Server Profile window, complete the required fields.
12. Select "OK".
13. Commit changes by selecting "Commit" in the upper-right corner of the screen.
14. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-003123 Implement organization-defined cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4::MA-4 (6)
- NIST SP 800-53 Revision 5::MA-4 (6)

1.27 PANW-NM-000128 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Palo Alto Networks security platform must off-load audit records onto a different system or media than the system being audited.

```
GROUP ID: V-228671
RULE ID: SV-228671r961860
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration. Off-loading is a common process in information systems with limited audit storage capacity.

The Palo Alto Networks security platform has multiple log types; at a minimum, the Traffic, Threat, System, and Configuration logs must be sent to a Syslog server.

Audit:

To view a syslog server profile,

Go to Device >> Server Profiles >> Syslog

If there are no Syslog Server Profiles present, this is a finding.

Select each Syslog Server Profile.

If no server is configured, this is a finding.

View the log-forwarding profile to determine which logs are forwarded to the syslog server.

Go to Objects >> Log forwarding

If no Log Forwarding Profile is present, this is a finding.

The "Log Forwarding Profile" window has five columns.

If there are no Syslog Server Profiles present in the Syslog column for the Traffic Log Type, this is a finding.

If there are no Syslog Server Profiles present for each of the severity levels of the Threat Log Type, this is a finding.

Go to Device >> Log Settings >> System Logs

The list of Severity levels is displayed.

If any of the Severity levels does not have a configured Syslog Profile, this is a finding.

Go to Device >> Log Settings >> Config Logs

If the "Syslog" field is blank, this is a finding.

Remediation:

To create a syslog server profile:

1. Go to Device >> Server Profiles >> Syslog
2. Select "Add".
3. In the Syslog Server Profile, enter the name of the profile.
4. Select "Add".
5. In the "Servers" tab, enter the required information.
6. Name: Name of the syslog server
7. Server: Server IP address where the logs will be forwarded to
8. Port: Default port 514
9. Facility: Select from the drop-down list.
10. Select "OK".

After creating the Server Profiles that define where to logs, enable log forwarding.

The way to enable forwarding depends on the log type:
Traffic Logs—Enable forwarding of Traffic logs by creating a Log Forwarding Profile (Objects >> Log Forwarding) and adding it to the security policies to trigger the log forwarding. Only traffic that matches a specific rule within the security policy will be logged and forwarded.
Configure the log-forwarding profile to select the logs to be forwarded to syslog server.

1. Go to Objects >> Log forwarding
2. The Log Forwarding Profile window appears. Note that it has five columns. In the Syslog column, select the syslog server profile for forwarding threat logs to the configured server(s).
3. Select "OK".

When the Log Forwarding Profile window disappears, the screen will show the configured log-forwarding profile.
Threat Logs—Enable forwarding of Threat logs by creating a Log Forwarding Profile (Objects >> Log Forwarding) that specifies which severity levels to forward and then adding it to the security policies, which triggers the log forwarding. A Threat log entry will only be created (and therefore forwarded) if the associated traffic matches a Security Profile (Antivirus, Anti-spyware, Vulnerability, URL Filtering, File Blocking, Data Filtering, or DoS Protection).
Configure the log-forwarding profile to select the logs to be forwarded to syslog server.

1. Go to Objects >> Log forwarding
2. The Log Forwarding Profile window appears. Note that it has five columns. In the "Syslog" column, select the syslog server profile for forwarding threat logs to the configured server(s).
3. Select "OK".

When the Log Forwarding Profile window disappears, the screen will show the configured log-forwarding profile.
System Logs—Enable forwarding of System logs by specifying a Server Profile in the log settings configuration.

1. Go to Device >> Log Settings >> System Logs
2. The list of severity levels is displayed.
3. Select a Server Profile for each severity level to forward.
4. Select each severity level in turn; with each selection, the "Log Systems - Setting" window will appear.
5. In the "Log Systems - Setting" window, in the "Syslog drop-down" box, select the configured Server Profile.
6. Select "OK".

Config Logs—Enable forwarding of Config logs by specifying a Server Profile in the log settings configuration.

1. Go to Device >> Log Settings >> Config Logs
2. Select the "Edit" icon (the gear symbol in the upper-right corner of the pane).
3. In the "Log Settings Config" window, in the "Syslog drop-down" box, select the configured Server Profile.
4. Select "OK".

For Traffic Logs and Threat Logs, use the log forwarding profile in the security rules.

1. Go to Policies >> Security Rule
2. Select the rule for which the log forwarding needs to be applied.
3. Apply the security profiles to the rule.
4. Go to Actions >> Log forwarding
5. Select the log forwarding profile from drop-down list.
6. Commit changes by selecting "Commit" in the upper-right corner of the screen. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4::AU-4 (1)
- NIST SP 800-53 Revision 5::AU-4 (1)

1.28 PANW-NM-000131 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Palo Alto Networks security platform must use automated mechanisms to alert security personnel to threats identified by authoritative sources (e.g., CTOs) and IAW CJCSM 6510.01B.

```
GROUP ID: V-228672
RULE ID: SV-228672r997690
```

Rationale:

CJCSM 6510.01B, "Cyber Incident Handling Program", in subsection e.(6)(c) sets forth three requirements for Cyber events detected by an automated system: If the cyber event is detected by an automated system, an alert will be sent to the POC designated for receiving such automated alerts. CC/S/A/FAs that maintain automated detection systems and sensors must ensure that a POC for receiving the alerts has been defined and that the IS configured to send alerts to that POC. The POC must then ensure that the cyber event is reviewed as part of the preliminary analysis phase and reported to the appropriate individuals if it meets the criteria for a reportable cyber event or incident.

By immediately displaying an alarm message, potential security violations can be identified more quickly even when administrators are not logged on to the network device. An example of a mechanism to facilitate this would be through the utilization of SNMP traps.

The Palo Alto Networks security platform can be configured to send messages to an SNMP server and to an email server as well as a Syslog server. SNMP traps can be generated for each of the five logging event types on the firewall: traffic, threat, system, hip, config. For this requirement, only the threat logs must be sent. Note that only traffic that matches an action in a rule will be logged and forwarded. In the case of traps, the messages are initiated by the firewall and sent unsolicited to the management stations.

The use of email as a notification method may result in a very larger number of messages being sent and possibly overwhelming the email server as well as the POC. The use of SNMP is preferred over email in general, but organizations may want to use email in addition to SNMP for high-priority messages.

Audit:

Note: The actual method is determined by the organization.

Review the system/network documentation to determine who the Points of Contact are and which methods are being used.

If the selected method is SNMP, verify that the device is configured.

Go to Device >> Server Profiles.

If no SNMP servers are configured, this is a finding.

Go to Objects >> Log Forwarding.

If no Log Forwarding Profile is listed, this is a finding.

If the "Log Type" column does not include "Threat", this is a finding.

If any Severity is not listed, this is a finding.

Remediation:

For SNMP traps, follow the following steps:

1. Configure the SNMP Trap Destinations; go to Device >> Server Profiles >> SNMP Trap.
2. Select "Add".
3. In the "SNMP Trap Server Profile" window, enter the required information.
4. For SNMP Version, select "V3".
5. Enter the name of the SNMP Server Profile.
6. Select "Add".
7. Server—Specify the SNMP trap destination name (up to 31 characters).
8. Manager—Specify the IP address of the trap destination.
9. User—Specify the SNMP user.
10. EngineID—Specify the engine ID of the firewall. The input is a string in hexadecimal representation. The engine ID is any number between 5 to 64 bytes. When represented as a hexadecimal string, this is between 10 and 128 characters (2 characters for each byte) with two additional characters for 0x that must be used as a prefix in the input string.
11. Auth Password—Specify the user's authentication password (minimum 8 characters, maximum of 256 characters, and no character restrictions). Only Secure Hash Algorithm (SHA) is supported.
12. Priv Password—Specify the user's encryption password (minimum 8 characters, maximum of 256 characters, and no character restrictions). Only Advanced Encryption Standard (AES) is supported.
13. Select "OK".

Configure generating "Traps for Threat" events:

1. Go to Objects >> Log Forwarding.
2. Select "Add".
3. In the "Log Forwarding Profile" window, enter the required information.
4. Enter the name of the Log Forwarding Profile.
5. In the "Threat Settings" section, in the "SNMP Trap" field for each Severity, select the SNMP Trap Server Profile.
6. Select "OK".

Add the Log Forwarding Profile to the security policies to trigger log forwarding to the SNMP server.

1. Go to Policies >> Security.
2. Select the rule for which the log forwarding needs to be applied. Apply the security profiles to the rule.
3. Go to "Actions" (tab); in the "Log forwarding" field, select the "log forwarding" profile.
4. Commit changes by selecting "Commit" in the upper-right corner of the screen.
5. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

CCI-001274 Alert organization-defined personnel or roles using organization-defined automated mechanisms when inappropriate or unusual activities with security or privacy implications.

- NIST SP 800-53::SI-4 (12)
- NIST SP 800-53A::SI-4 (12).1 (ii)
- NIST SP 800-53 Revision 4::SI-4 (12)
- NIST SP 800-53 Revision 5::SI-4 (12)

CCI-003831 Alert organization-defined personnel or roles upon detection of unauthorized access, modification, or deletion of audit information.

- NIST SP 800-53 Revision 5::AU-9 b

1.29 PANW-NM-000136 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Palo Alto Networks security platform must employ centrally managed authentication server(s).

```
GROUP ID: V-228673
RULE ID: SV-228673r1082978
```

Rationale:

The use of authentication servers or other centralized management servers for providing centralized authentication services is required for network device management. Maintaining local administrator accounts for daily usage on each network device without centralized management is not scalable or feasible. Without centralized management, it is likely that credentials for some network devices will be forgotten, leading to delays in administration, which itself leads to delays in remediating production problems and in addressing compromises in a timely fashion.

Only the emergency administration account, also known as the account of last resort, can be locally configured on the device.

Audit:

Ask the administrator which form of centralized authentication server is being used. This requirement is not applicable to the local account of last resort.

Navigate to the appropriate window to view the configured server(s).

For RADIUS, go to Device >> Server Profiles >> RADIUS.

For LDAP, go to Device >> Server Profiles >> LDAP.

For Kerberos, go to Device >> Server Profiles >> Kerberos.

If there are no servers configured in the window that match the specified form of centralized authentication, this is a finding.

Remediation:

The device allows three different authentication protocols: RADIUS, LDAP, and Kerberos. In this explanation, LDAP is used.

To configure the Palo Alto Networks security platform to use an LDAP server, follow these steps:

1. Go to Device >> Server-Profiles >> LDAP.
2. Select "Add" (lower left of window).
3. Populate the required fields.
4. a. Enter the name of the profile in the "Name" field.
5. b. In the server box enter the name of the server in the "Name" field.
6. c. Enter the IP Address of the server.
7. d. Enter the Port number the firewall should use to connect to the LDAP server (default=389 for LDAP; 636 for LDAP over SSL).
8. e. Enter the LDAP Domain name to prepend to all objects learned from the server. The value entered here depends on the specific deployment. If using Active Directory, enter the NetBIOS domain name; not an FQDN (for example, enter acme, not acme.com). Note that if collecting data from multiple domains, it is necessary to create separate server profiles. If using a global catalog server, leave this field blank.
9. Select the Type of LDAP server that will be connected. The correct LDAP attributes in the group mapping settings will automatically be populated based on the selection.
10. In the Base field, select the DN that corresponds to the point in the LDAP tree where the firewall is to begin its search for user and group information.
11. Select the SSL checkbox.
12. Select "OK".

To create an Authentication Profile using the newly created LDAP server, follow these steps:

1. Go to Device >> Authentication Profile.
2. Select "Add" (lower left of window).
3. Populate the required fields as needed.
4. a. In the Authentication field, select "LDAP".
5. b. In the Server Profile field, select the configured LDAP server profile.
6. c. In the Login Attribute field, enter “sAMAccountName”.
7. Select "OK".

Apply the authentication profile to the Administrator accounts.

1. Go to Device >> Administrators.
2. Select each configured account or select "Add" (in the bottom-left corner of the pane) to create a new one.
3. In the "Authentication Profile" field, enter the configured LDAP authentication profile.
4. Select "OK".

Note: The name of the administrator must match the name of the user in the LDAP server.
Note: The authentication profile must not be applied to the emergency administration account since it has special requirements.
Commit changes by selecting "Commit" in the upper-right corner of the screen.
Select "OK" when the confirmation dialog appears.
Note that the emergency administration account is the only account that is configured locally on the device itself.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

CCI-000372 Verify configuration settings for organization-defined system components using organization-defined automated mechanisms.

- NIST SP 800-53::CM-6 (1)
- NIST SP 800-53A::CM-6 (1).1
- NIST SP 800-53 Revision 4::CM-6 (1)
- NIST SP 800-53 Revision 5::CM-6 (1)

1.30 PANW-NM-000141 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Palo Alto Networks security platform must use DoD-approved PKI rather than proprietary or self-signed device certificates.

```
GROUP ID: V-228674
RULE ID: SV-228674r961863
```

Rationale:

DoD Instruction 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling mandates that certificates must be issued by the DoD PKI or by a DoD-approved PKI for authentication, digital signature, or encryption.

Audit:

Go to Device >> Certificate Management >> Certificates

Installed Certificates are listed in the "Device Certificates" tab.

If any of the have the name or identifier of a non-approved source in the "Issuer" field, this is a finding.

Remediation:

Obtain a Device Certificate from the DoD PKI or from a DoD-approved PKI:

1. Go to Device >> Certificate Management >> Certificates
2. Select "Import" (at the bottom of the pane).
3. In the "Import Certificate" pane, complete each field.
4. Select "OK".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

CCI-001159 Issue public key certificates under an organization-defined certificate policy or obtain public key certificates from an approved service provider.

- NIST SP 800-53::SC-17
- NIST SP 800-53A::SC-17.1
- NIST SP 800-53 Revision 4::SC-17
- NIST SP 800-53 Revision 5::SC-17 a

1.31 PANW-NM-000142 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Palo Alto Networks security platform must not use Password Profiles.

```
GROUP ID: V-228675
RULE ID: SV-228675r961863
```

Rationale:

Password profiles override settings made in the Minimum Password Complexity window. If Password Profiles are used they can bypass password complexity requirements.

Audit:

Go to Device >> Password Profiles

If there are configured Password Profiles, this is a finding.

Remediation:

Go to Device >> Password Profiles

If the screen is blank (no configured Password Profiles), do nothing.

If there are configured Password Profiles, identify which accounts are using them and bring this to the attention of the ISSO immediately.

Delete the Password Profiles when authorized to make changes to the device in accordance with local change management policies.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.32 PANW-NM-000143 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Palo Alto Networks security platform must not use the default admin account password.

```
GROUP ID: V-228676
RULE ID: SV-228676r961863
```

Rationale:

To assure accountability and prevent unauthenticated access, organizational administrators must be uniquely identified and authenticated for all network management accesses to prevent potential misuse and compromise of the system.

The use of a default password for any account, especially one for administrative access, can quickly lead to a compromise of the device and subsequently, the entire enclave or system. The "admin" account is intended solely for the initial setup of the device and must be disabled when the device is initially configured. The default password for this account must immediately be changed at the first login of an authorized administrator.

Audit:

Open a web browser at an authorized workstation and enter the management IP address of the Palo Alto Networks security platform.

Use HTTP Secure (HTTPS) instead of HTTP since HTTP is disabled by default.

The logon window will appear.

Enter

```
"admin" into both the "Name" and "Password" fields.
```

If anything except the logon screen with the message "Invalid username or password" appears, this is a finding.

Remediation:

1. Go to Device >> Administrators
2. Select the admin user.
3. In the "Old Password" field, enter "admin".
4. In the "New Password" field, enter the new password.
5. In the "Confirm New Password" field, enter the new password.
6. Select "OK".
7. Commit changes by selecting "Commit" in the upper-right corner of the screen.
8. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53::IA-2
- NIST SP 800-53A::IA-2.1
- NIST SP 800-53 Revision 4::IA-2
- NIST SP 800-53 Revision 5::IA-2

1.33 PANW-NM-000144 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Palo Alto Networks security platform must generate an audit log record when the Data Plane CPU utilization is 100%.

```
GROUP ID: V-228677
RULE ID: SV-228677r961863
```

Rationale:

Auditing and logging are key components of any security architecture. Logging the actions of specific events provides a means to investigate an attack; to recognize resource utilization or capacity thresholds; or to identify an improperly configured network device. If auditing is not comprehensive, it will not be useful for intrusion monitoring, security investigations, and forensic analysis.

If the Data Plane CPU utilization is 100%, this may indicate an attack or simply an over-utilized device. In either case, action must be taken to identify the source of the issue and take corrective action.

Audit:

Go to Device >> Setup >> Management

In the "Logging and Reporting Settings" pane.

If the "Enable Log on High DP Load" check box is not selected, this is a finding.

Remediation:

1. Go to Device >> Setup >> Management
2. In the "Logging and Reporting Settings" pane, select the "Edit" icon (the gear symbol in the upper-right corner of the pane).
3. In the "Log Export and Reporting" tab, select the "Enable Log on High DP Load" check box.
4. Select "OK".
5. Commit changes by selecting "Commit" in the upper-right corner of the screen.
6. Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.34 PANW-NM-000145 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Palo Alto Networks security platform must authenticate Network Time Protocol sources.

```
GROUP ID: V-228678
RULE ID: SV-228678r961506
```

Rationale:

If Network Time Protocol is not authenticated, an attacker can introduce a rogue NTP server. This rogue server can then be used to send incorrect time information to network devices, which will make log timestamps inaccurate and affected scheduled actions. NTP authentication is used to prevent this tampering by authenticating the time source.

Audit:

Go to Device >> Setup >> Services

In the "Services" window, the Primary NTP Server Authentication Type and Secondary NTP Server Authentication Type must be either Symmetric Key or Autokey. If the "Primary NTP Server Authentication Type" and "Secondary NTP Server Authentication Type" fields are "none", this is a finding.

Remediation:

1. Go to Device >> Setup >> Services
2. Select the "Edit" icon (the gear symbol in the upper-right corner of the pane).
3. In the "Services" window, in the NTP tab, in the "Primary NTP Server Address" field and the "Secondary NTP Server Address" field, enter the IP address or hostname of the NTP servers.

In the "Authentication Type" field, select one of the following:

- **Symmetric Key**; this option uses symmetric key exchange, which are shared secrets. Enter the key ID, algorithm, authentication key, and confirm the authentication key; for the algorithm, select "SHA1".
- **Autokey**; this option uses auto key, or public key cryptography.
- Commit changes by selecting "Commit" in the upper-right corner of the screen.
- Select "OK" when the confirmation dialog appears.

Additional Information:

CCI-001967 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.

- NIST SP 800-53 Revision 4::IA-3 (1)
- NIST SP 800-53 Revision 5::IA-3 (1)

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	PANW-NM-000015 (Manual)	☐	☐
1.2	PANW-NM-000016 (Manual)	☐	☐
1.3	PANW-NM-000024 (Manual)	☐	☐
1.4	PANW-NM-000029 (Manual)	☐	☐
1.5	PANW-NM-000046 (Manual)	☐	☐
1.6	PANW-NM-000048 (Manual)	☐	☐
1.7	PANW-NM-000051 (Manual)	☐	☐
1.8	PANW-NM-000053 (Manual)	☐	☐
1.9	PANW-NM-000055 (Manual)	☐	☐
1.10	PANW-NM-000056 (Manual)	☐	☐
1.11	PANW-NM-000057 (Manual)	☐	☐
1.12	PANW-NM-000058 (Manual)	☐	☐
1.13	PANW-NM-000059 (Manual)	☐	☐
1.14	PANW-NM-000061 (Manual)	☐	☐
1.15	PANW-NM-000069 (Manual)	☐	☐
1.16	PANW-NM-000075 (Manual)	☐	☐
1.17	PANW-NM-000092 (Manual)	☐	☐
1.18	PANW-NM-000096 (Manual)	☐	☐
1.19	PANW-NM-000097 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	PANW-NM-000098 (Manual)	☐	☐
1.21	PANW-NM-000099 (Manual)	☐	☐
1.22	PANW-NM-000100 (Manual)	☐	☐
1.23	PANW-NM-000101 (Manual)	☐	☐
1.24	PANW-NM-000110 (Manual)	☐	☐
1.25	PANW-NM-000117 (Manual)	☐	☐
1.26	PANW-NM-000118 (Manual)	☐	☐
1.27	PANW-NM-000128 (Manual)	☐	☐
1.28	PANW-NM-000131 (Manual)	☐	☐
1.29	PANW-NM-000136 (Manual)	☐	☐
1.30	PANW-NM-000141 (Manual)	☐	☐
1.31	PANW-NM-000142 (Manual)	☐	☐
1.32	PANW-NM-000143 (Manual)	☐	☐
1.33	PANW-NM-000144 (Manual)	☐	☐
1.34	PANW-NM-000145 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Sep 9, 2025	1.0.0	Initial CIS Release