CIS Palo Alto Firewall 11 Benchmark

v1.0.0 - 05-31-2023

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/

Table of Contents

Overview

All CIS Benchmarks focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

In the end, the CIS Benchmarks are designed as a key **component** of a comprehensive cybersecurity program.

This document provides prescriptive guidance for establishing a secure configuration posture for Palo Alto Firewalls running PAN-OS version 11.x. This guide was tested against PAN-OS v11.x.
To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

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 PAN-OS on a Palo Alto Firewall

Consensus Guidance

This CIS Benchmark was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

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 for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

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

Impact Statement

Any security, functionality, or operational consequences that can result from following 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.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) '4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount
  - acts as a defense in depth measure
  - may negatively inhibit the utility or performance of the technology.

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Recommendations

1 Device Setup

The Device Setup section covers requirements for login banners, logging, management interfaces, password strength, device management authentication, SNMP polling, and device services.

1.1 General Settings

The General settings section includes banner and logging requirement settings.

1.1.1 Ensure System Logging to a Remote Host

Logging to a remote host permits longer log retention than on-device logging. This allows more flexible approaches to log processing, both in real time and retrospectively. Real time log processing often includes log entries being used to trigger scripts or other events. Finally, logging to an external host provides a second copy of all logs. In the event that the firewall is compromised or logs are lost for whatever reason, a second copy of the logs are available.

Logging all infrastructure to a single central destination also allows the configuration of SIEM services, which facilitates correlation of firewall logs with logs of other infrastructure components. For these reasons, most regulatory frameworks require remote, centralized logging for all critical infrastructure components.

1.1.1.1 Syslog logging should be configured (Automated)

Profile Applicability:

- Level 1

Description:

Syslog logging is a standard logging protocol that is widely supported. It is recommended for a level 1 deployment only, as syslog does not support encryption.

Rationale:

Sending all system logs to a remote host is recommended to provide protected, long term storage and archiving. This also places a copy of the logs in a second location, in case the primary (on the firewall) logs are compromised. Storing logs on a remote host also allows for more flexible log searches and log processing, as well as many methods of triggering events or scripts based on specific log events or combinations of events. Finally, remote logging provides many organizations with the opportunity to combine logs from disparate infrastructure in a SIEM (Security Information and Event Management) system.

Logging to an external system is also usually required by most regulatory frameworks.

Impact:

Failure to properly store and archive logs for critical infrastructure leaves an organization without the tools required to establish trends in events or activity, or to retrospectively analyze security or operational events beyond the log timespan stored on the firewall. Not having remote logs also puts many organizations outside of compliance with many regulatory frameworks. Finally, not logging to a remote host leaves organizations without recourse in the event of a compromise of logs on the primary device. It is imperative that organizations log critical infrastructure appropriately, store and archive these logs in a central location, and have a robust set of tools to analyze logs both in real time and after the fact.

Audit:

Navigate to `Device > Server Profiles > Syslog`
Ensure that a valid Syslog profile is configured, and that it points to a valid Syslog host.
Navigate to `Device > Log Settings`
Under `System`, verify that at least one Syslog entry exists and that at least one entry has "All Logs" selected. Each Syslog entry must have a valid Syslog Profile attached.
Under `Configuration`, verify that at least one Syslog entry exists and that at least one entry has "All Logs" selected. Each Syslog entry must have a valid Syslog Profile attached.
Under `User-ID`, verify that at least one Syslog entry exists and that at least one entry has "All Logs" selected. Each Syslog entry must have a valid Syslog Profile attached.
Under `HIP Match` (Host Information Profile), verify that at least one Syslog entry exists and that at least one entry has "All Logs" selected. Each Syslog entry must have a valid Syslog Profile attached.
Under `IP-Tag`, verify that at least one Syslog entry exists and that at least one entry has "All Logs" selected. Each Syslog entry must have a valid Syslog Profile attached.

Remediation:

Navigate to `Device > Server Profiles > Syslog`
Choose `Add`
Assign a Name to the Profile. Choose `Add`, and assign a server name in the Name field, add an IP address or FQDN in the `Syslog Server` field. Edit other fields as appropriate for your server.
Repeat if multiple Syslog destinations are required.
Navigate to `Device > Log Settings`
Under `System`, add an entry. Define a `Name` and a `Filter setting`. Under `Forward Methods`, add a `Syslog Profile` in the `Syslog` section. Ensure that at least one of the Log Settings Configuration entries has its `Filter` setting at `All Logs`
Under `Configuration`, add an entry. Define a `Name` and a `Filter setting`. Under `Forward Methods`, add a `Syslog Profile` in the `Syslog` section. Ensure that at least one of the Log Settings Configuration entries has its `Filter` setting at `All Logs`
Under `User-ID`, add an entry. Define a `Name` and a `Filter setting`. Under `Forward Methods`, add a `Syslog Profile` in the `Syslog` section. Ensure that at least one of the Log Settings Configuration entries has its `Filter` setting at `All Logs`
Under `HIP Match` (Host Information Profile), add an entry. Define a `Name` and a `Filter setting`. Under `Forward Methods`, add a `Syslog Profile` in the `Syslog` section. Ensure that at least one of the Log Settings Configuration entries has its `Filter` setting at `All Logs`
Under `IP-Tag`, add an entry. Define a `Name` and a `Filter setting`. Under `Forward Methods`, add a `Syslog Profile` in the `Syslog` section. Ensure that at least one of the Log Settings Configuration entries has its `Filter` setting at `All Logs`

Default Value:

By default, no external logging is defined

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Configure Syslog Monitoring" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/use-syslog-for-monitoring/configure-syslog-monitoring.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.1 Establish and Maintain an Audit Log Management Process Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

1.1.1.2 SNMPv3 traps should be configured (Automated)

Profile Applicability:

- Level 2

Description:

SNMP v3 can be used for remote logging, and is the recommended protocol in higher security situations as it fully supports encryption of logs.

Rationale:

Sending all system logs to a remote host is recommended to provide protected, long term storage and archiving. This also places a copy of the logs in a second location, in case the primary (on the firewall) logs are compromised. Storing logs on a remote host also allows for more flexible log searches and log processing, as well as many methods of triggering events or scripts based on specific log events or combinations of events. Finally, remote logging provides many organizations with the opportunity to combine logs from disparate infrastructure in a SIEM (Security Information and Event Management) system.

Logging to an external system is also usually required by most regulatory frameworks.

Impact:

Failure to properly store and archive logs for critical infrastructure leaves an organization without the tools required to establish trends in events or activity, or to retrospectively analyze security or operational events beyond the log timespan stored on the firewall. Not having remote logs also puts many organizations outside of compliance with many regulatory frameworks. Finally, not logging to a remote host leaves organizations without recourse in the event of a compromise of logs on the primary device. It is imperative that organizations log critical infrastructure appropriately, store and archive these logs in a central location, and have a robust set of tools to analyze logs both in real time and after the fact. Not encrypting log data as it transits the network allows an attacker to mount a "MiTM" (Monkey in the Middle) attack, which allows them to intercept and/or modify logs as they transit from the source to the destination.

Audit:

Navigate to `Device > Server Profiles > SNMP Traps`
Ensure that a valid SNMP profile is configured, that version `V3` is selected, and that it points to a valid SNMPv3 host.
`User`, `EngineID` and `Password` fields should be completed appropriately
Navigate to `Device > Log Settings`
Under `System`, verify that at least one SNMP entry exists, corresponding to an SNMPv3 Server Profile and that at least one entry has "All Logs" selected.
Under `Configuration`, verify that at least one SNMP entry exists, corresponding to an SNMPv3 Server Profile and that at least one entry has "All Logs" selected.
Under `User-ID`, verify that at least one SNMP entry exists, corresponding to an SNMPv3 Server Profile and that at least one entry has "All Logs" selected.
Under `HIP Match` (Host Information Profile), verify that at least one SNMP entry exists, corresponding to an SNMPv3 Server Profile and that at least one entry has "All Logs" selected.
Under `IP-Tag`, verify that at least one SNMP entry exists, corresponding to an SNMPv3 Server Profile and that at least one entry has "All Logs" selected.

Remediation:

Navigate to `Device > Server Profiles > SNMP Trap`
Choose `Add`
Assign a `Name` to the Profile, and specify `version` V3. Choose `Add`, and assign a server name in the `Name` field, add an IP address or FQDN in the `SNMP Manager` field. Edit the `Password` fields as appropriate for your server.
Repeat if multiple Syslog destinations are required.
Navigate to `Device > Log Settings`
Under `System`, add an entry. Define a `Name` and a `Filter setting`. Under `Forward Methods`, add a `SNMP Profile` in the `SNMP` section. Ensure that at least one of the Log Settings Configuration entries has its `Filter` setting at `All Logs`
Under `Configuration`, add an entry. Define a `Name` and a `Filter setting`. Under `Forward Methods`, add a `SNMP Profile` in the `SNMP` section. Ensure that at least one of the Log Settings Configuration entries has its `Filter` setting at `All Logs`
Under `User-ID`, add an entry. Define a `Name` and a `Filter setting`. Under `Forward Methods`, add a `SNMP Profile` in the `SNMP` section. Ensure that at least one of the Log Settings Configuration entries has its `Filter` setting at `All Logs`
Under `HIP Match` (Host Information Profile), add an entry. Define a `Name` and a `Filter setting`. Under `Forward Methods`, add a `SNMP Profile` in the `SNMP` section. Ensure that at least one of the Log Settings Configuration entries has its `Filter` setting at `All Logs`
Under `IP-Tag`, add an entry. Define a `Name` and a `Filter setting`. Under `Forward Methods`, add a `SNMP Profile` in the `SNMP` section. Ensure that at least one of the Log Settings Configuration entries has its `Filter` setting at `All Logs`

Default Value:

By default, no external logging is defined

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Forward Traps to an SNMP Manager" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/snmp-monitoring-and-traps/forward-traps-to-an-snmp-manager#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.1 <u>Establish and Maintain an Audit Log Management Process</u>** Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	🟢	🟠	🔵
v7	**6.2 <u>Activate audit logging</u>** Ensure that local logging has been enabled on all systems and networking devices.	🟢	🟠	🔵

1.1.2 Ensure 'Login Banner' is set (Automated)

Profile Applicability:

- Level 1

Description:

Configure a login banner, ideally approved by the organization's legal team. This banner should, at minimum, prohibit unauthorized access, provide notice of logging or monitoring, and avoid using the word "welcome" or similar words of invitation.

Rationale:

Through a properly stated login banner, the risk of unintentional access to the device by unauthorized users is reduced. Should legal action take place against a person accessing the device without authorization, the login banner greatly diminishes a defendant's claim of ignorance.

Audit:

Navigate to `Device > Setup > Management > General Settings`.
Verify that `Login Banner` is set appropriately for your organization.

Remediation:

Navigate to `Device > Setup > Management > General Settings`.
Set `Login Banner` as appropriate for your organization.

Default Value:

Not configured

References:

1. "How to Configure the Device Login Banner" - https://live.paloaltonetworks.com/docs/DOC-7964

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	14.1 <u>Establish and Maintain a Security Awareness Program</u> Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	11 <u>Secure Configuration for Network Devices, such as Firewalls, Routers and Switches</u> Secure Configuration for Network Devices, such as Firewalls, Routers and Switches			

1.1.3 Ensure 'Enable Log on High DP Load' is enabled (Automated)

Profile Applicability:

- Level 1

Description:

Enable the option 'Enable Log on High DP Load' feature. When this option is selected, a system log entry is created when the device's packet processing load reaches 100% utilization.

Rationale:

When the device's packet processing load reaches 100%, a degradation in the availability of services accessed through the device can occur. Logging this event can help with troubleshooting system performance.

Impact:

Sustained attacks, especially volumetric DOS and DDOS attacks will often affect CPU utilization. This setting will generate an event that is easily monitored for and alerted on. While setting CPU utilization watermarks in a Network Management System is a standard practice, this setting does not depend on even having an NMS, it doesn't require anything other than standard logging to implement.

Audit:

Navigate to `Device > Setup > Management > Logging and Reporting Settings > Log Export and Reporting`.
Verify `Enable Log on High DP Load` is checked.

Remediation:

Navigate to `Device > Setup > Management > Logging and Reporting Settings > Log Export and Reporting`.
Set the `Enable Log on High DP Load` box to checked.

Default Value:

Not enabled

References:

1. "What is Enable Log on High DP Load" - https://live.paloaltonetworks.com/docs/DOC-4075

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.1 Establish and Maintain an Audit Log Management Process** Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	**6.2 Activate audit logging** Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

1.2 Management Interface Settings

The Management Interface settings include restrictions on how management interfaces are accessed, secured, and used.

1.2.1 Ensure 'Permitted IP Addresses' is set to those necessary for device management (Automated)

Profile Applicability:

- Level 1

Description:

Permit only the necessary IP addresses to be used to manage the device.

Rationale:

Management access to the device should be restricted to the IP addresses or subnets used by firewall administrators. Permitting management access from other IP addresses increases the risk of unauthorized access through password guessing, stolen credentials, or other means.

Audit:

Navigate to `Device > Setup > Interfaces > Management`.
Verify that `Permitted IP Addresses` is limited only to those necessary for device management.

Remediation:

Navigate to `Device > Setup > Interfaces > Management`.
Set `Permitted IP Addresses` to only those necessary for device management for the SSH and HTTPS protocols. If no profile exists, create one that has these addresses set.

Default Value:

Not enabled (all addresses that can reach the interface are permitted)

References:

1. "How to Allow Certain IP Addresses on the Management Interface" - https://live.paloaltonetworks.com/docs/DOC-8432
2. "PAN-OS Administrator's Guide 9.0 (English) - Best Practices for Securing Administrative Access": https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure** Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	**6.7 Centralize Access Control** Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	**11.6 Use Dedicated Machines For All Network Administrative Tasks** Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.		●	●
v7	**11.7 Manage Network Infrastructure Through a Dedicated Network** Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.		●	●

1.2.2 Ensure 'Permitted IP Addresses' is set for all management profiles where SSH, HTTPS, or SNMP is enabled (Automated)

Profile Applicability:

- Level 1

Description:

For all management profiles, only the IP addresses required for device management should be specified.

Rationale:

If a Permitted IP Addresses list is either not specified or is too broad, an attacker may gain the ability to attempt management access from unintended locations, such as the Internet. The "Ensure 'Security Policy' denying any/all traffic exists at the bottom of the security policies ruleset" recommendation in this benchmark can provide additional protection by requiring a security policy specifically allowing device management access.

Audit:

Navigate to `Network > Network Profiles > Interface Management`.
In each profile, for each of the target protocols (SNMP, HTTPS, SSH), verify that `Permitted IP Addresses` is limited to those necessary for device management.

Remediation:

Navigate to `Network > Network Profiles > Interface Management`.
In each profile, for each of the target protocols (SNMP, HTTPS, SSH), set `Permitted IP Addresses` to only include those necessary for device management. If no profile exists, create one that has these options set.

Default Value:

Not enabled

References:

1. "How to Allow Certain IP Addresses on the Management Interface" - https://live.paloaltonetworks.com/docs/DOC-8432
2. "PAN-OS Administrator's Guide 9.0 (English) - Best Practices for Securing Administrative Access": https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	🟢	🟠	🔵
v8	6.7 <u>Centralize Access Control</u> Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		🟠	🔵
v7	11.6 <u>Use Dedicated Machines For All Network Administrative Tasks</u> Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.		🟠	🔵
v7	11.7 <u>Manage Network Infrastructure Through a Dedicated Network</u> Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.		🟠	🔵

1.2.3 Ensure HTTP and Telnet options are disabled for the management interface (Automated)

Profile Applicability:

- Level 1

Description:

HTTP and Telnet options should not be enabled for device management.

Rationale:

Management access over cleartext services such as HTTP or Telnet could result in a compromise of administrator credentials and other sensitive information related to device management. Theft of either administrative credentials or session data is easily accomplished with a "Man in the Middle" attack.

Audit:

Navigate to `Device > Setup > Interfaces > Management`.
Verify that the `HTTP` and `Telnet` options are both unchecked.

Remediation:

Navigate to `Device > Setup > Interfaces > Management`.
Set the `HTTP` and `Telnet` boxes to unchecked.

Default Value:

Not set. (HTTP and Telnet are disabled by default)

References:

1. "How to Configure a Layer 3 Interface to act as a Management Port" - https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-a-Layer-3-Interface-to-act-as-a-Management-Port/ta-p/59024
2. "PAN-OS Administrator's Guide 9.0 (English) - Best Practices for Securing Administrative Access": https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.		●	●
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

1.2.4 Ensure HTTP and Telnet options are disabled for all management profiles (Automated)

Profile Applicability:

- Level 1

Description:

HTTP and Telnet options should not be enabled for device management.

Rationale:

Management access over cleartext services such as HTTP or Telnet could result in a compromise of administrator credentials and other sensitive information related to device management.

Audit:

Navigate to `Network > Network Profiles > Interface Management`.
For each Interface Management profile verify that the `HTTP` and `Telnet` options are both unchecked.

Remediation:

Navigate to `Network > Network Profiles > Interface Management`.
For each Profile, set the `HTTP` and `Telnet` boxes to unchecked.

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Best Practices for Securing Administrative Access": https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html#
2. "PAN-OS Administrator's Guide 9.0 (English) - Use Interface Management Profiles to Restrict Access": https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces/use-interface-management-profiles-to-restrict-access.html#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	**14.4 Encrypt All Sensitive Information in Transit** Encrypt all sensitive information in transit.		●	●
v7	**16.5 Encrypt Transmittal of Username and Authentication Credentials** Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

1.2.5 Ensure valid certificate is set for browser-based administrator interface (Automated)

Profile Applicability:

- Level 2

Description:

In most cases, a browser HTTPS interface is used to administer the Palo Alto appliance. The certificate used to secure this session should satisfy the following criteria:

1. A valid certificate from a trusted source should be used. While a certificate from a trusted Public Certificate Authority is certainly valid, one from a trusted Private Certificate Authority is absolutely acceptable for this purpose.
2. The certificate should have a valid date. It should not have a "to" date in the past (it should not be expired), and should not have a "from" date in the future.
3. The certificate should use an acceptable cipher and encryption level.

Rationale:

If a certificate that is self-signed, expired, or otherwise invalid is used for the browser HTTPS interface, administrators in most cases will not be able to tell if their session is being eavesdropped on or injected into by a "Man in the Middle" attack.

Impact:

If the default self-signed certificate is used, an administrator will not be able to clearly tell if their HTTPS session is being hijacked or not. Using a trusted certificate ensures that the session is both encrypted and trusted.

Audit:

Verify that the certificate used to secure HTTPS sessions meets the criteria by reviewing the appropriate certificate:
Navigate to `Device > Certificate Management > Certificates`
Verify that this Certificate is properly applied to the Management Interface:
Navigate to `Device > Setup > Management > General Settings > SSL/TLS Service Profile`

Remediation:

Create or acquire a certificate that meets the stated criteria and set it:
Navigate to `Device > Certificate Management > Certificates`
Import an appropriate Certificate for your administrative session, from a trusted Certificate Authority.
Navigate to `Device > Certificate Management > SSL/TLS Service Profile`
Choose or import the certificate you want to use for the web based administrative session.
Navigate to `Device > Setup > Management > General Settings > SSL/TLS Service Profile`
Choose the Service Profile that you have configured

Default Value:

A self-signed certificate is installed by default for the administrative interface.

References:

1. "How to Configure a Certificate for Secure Web GUI Access" - https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-configure-a-certificate-for-secure-web-gui-access/ta-p/68653
2. "PAN-OS Administrator's Guide 9.0 (English) - Best Practices for Securing Administrative Access": https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html#

Additional Information:

Verify that the clock is both accurate and reliable on both the Palo Alto and on the administrative workstations before setting the SSL/TLS Service Profile. Inaccurate or mismatched clocks will result in certificate errors and can result in loss of HTTPS administrative access.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

1.3 Minimum Password Requirements

The Minimum Password Requirements Section contains criteria for local passwords such as complexity and restrictions. The best practice is to use named accounts, and if possible a back-end authentication solution such as Active Directory or (best case) a two-factor authentication solution. However, local credentials will always exist, if only to account for failure of a back-end authentication solution.

It's recommended that a majority of the following recommendations be followed. This will vary from organization to organization, but at a minimum 5 of the following 10 password complexity recommendations on should be followed, as well as the first one that enables password complexity.

1.3.1 Ensure 'Minimum Password Complexity' is enabled (Automated)

Profile Applicability:

- Level 1

Description:

This checks all new passwords to ensure that they meet basic requirements for strong passwords.

Rationale:

Password complexity recommendations are derived from the USGCB (United States Government Configuration Baseline), Common Weakness Enumeration, and benchmarks published by the CIS (Center for Internet Security). Password complexity adds entropy to a password, in comparison to a simple password of the same length. A complex password is more difficult to attack, either directly against administrative interfaces or cryptographically, against captured password hashes. However, making a password of greater length will generally have a greater impact in this regard, in comparison to making a shorter password more complex.

Impact:

Simple passwords make an attacker's job very easy. There is a reasonably short list of commonly used admin passwords for network infrastructure, not enforcing password lengths and complexity can lend itself to making an attacker's brute force attack successful.

Audit:

Navigate to `Device > Setup > Management > Minimum Password Complexity`.
Verify `Enabled` is checked
Ensure that the various password settings to values that are appropriate to your organization. Non-zero values should be set for Minimum Uppercase, Lowercase and Special Characters. "Block Username Inclusion" should be enabled.

Remediation:

Navigate to `Device > Setup > Management > Minimum Password Complexity`.
Set `Enabled` to be checked
Set that the various password settings to values that are appropriate to your organization. It is suggested that there at least be some special characters enforced, and that a minimum length be set. Ensure that non-zero values are set for Minimum Uppercase, Lowercase and Special Characters. "Block Username Inclusion" should be enabled.
Operationally, dictionary words should be avoided for all passwords - passphrases are a much better alternative.

Default Value:

Not enabled.

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Best Practices for Securing Administrative Access" - https://docs.paloaltonetworks.com/pan-os-9-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

1.3.2 Ensure 'Minimum Length' is greater than or equal to 12 (Automated)

Profile Applicability:

- Level 1

Description:

This determines the least number of characters that make up a password for a user account.

Rationale:

A longer password is much more difficult to attack, either directly against administrative interfaces or cryptographically, against captured password hashes. Making a password of greater length will generally have a greater impact in this regard, in comparison to making a shorter password more complex. Passphrases are a commonly used recommendation, to make longer passwords more palatable to end users. Administrative staff however generally use "password safe" applications, so a long and complex password is more easily implemented for most infrastructure administrative interfaces.

Impact:

Longer passwords are much more difficult to attack. This is true of attacks against the administrative interfaces themselves, or of decryption attacks against captured hashes. A longer password will almost always have a more positive impact than a shorter but more complex password.

Audit:

Navigate to `Device > Setup > Management > Minimum Password Complexity`. Verify `Minimum Length` is greater than or equal to `12`

Remediation:

Navigate to `Device > Setup > Management > Minimum Password Complexity`. Set `Minimum Length` to greater than or equal to `12`

Default Value:

Not enabled.

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Best Practices for Securing Administrative Access" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**5.2 Use Unique Passwords** Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	**4.2 Change Default Passwords** Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	●	●	●

1.3.3 Ensure 'Minimum Uppercase Letters' is greater than or equal to 1 (Automated)

Profile Applicability:

- Level 1

Description:

This checks all new passwords to ensure that they contain at least one English uppercase character (A through Z).

Rationale:

This is one of several settings that, when taken together, ensure that passwords are sufficiently complex as to thwart brute force and dictionary attacks.

Audit:

Navigate to `Device > Setup > Management > Minimum Password Complexity`
Verify `Minimum Uppercase Letters` is greater than or equal to `1`

Remediation:

Navigate to `Device > Setup > Management > Minimum Password Complexity`
Set `Minimum Uppercase Letters` to greater than or equal to `1`

Default Value:

Not enabled.

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Best Practices for Securing Administrative Access" - https://docs.paloaltonetworks.com/pan-os-9-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.2 <u>Change Default Passwords</u> Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	🟢	🟠	🔵
v7	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

1.3.4 Ensure 'Minimum Lowercase Letters' is greater than or equal to 1 (Automated)

Profile Applicability:

- Level 1

Description:

This checks all new passwords to ensure that they contain at least one English lowercase character (a through z).

Rationale:

This is one of several settings that, when taken together, ensure that passwords are sufficiently complex as to thwart brute force and dictionary attacks.

Audit:

Navigate to `Device > Setup > Management > Minimum Password Complexity`
Verify `Minimum Lowercase Letters` is greater than or equal to `1`

Remediation:

Navigate to `Device > Setup > Management > Minimum Password Complexity`
Set `Minimum Lowercase Letters` to greater than or equal to `1`

Default Value:

Not enabled.

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Best Practices for Securing Administrative Access" - https://docs.paloaltonetworks.com/pan-os-9-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**5.2 Use Unique Passwords** Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.2 <u>Change Default Passwords</u> Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	●	●	●
v7	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

1.3.5 Ensure 'Minimum Numeric Letters' is greater than or equal to 1 (Automated)

Profile Applicability:

- Level 1

Description:

This checks all new passwords to ensure that they contain at least one base 10 digit (0 through 9).

Rationale:

This is one of several settings that, when taken together, ensure that passwords are sufficiently complex as to thwart brute force and dictionary attacks.

Audit:

Navigate to `Device > Setup >` Management > Minimum Password Complexity`
Verify `Minimum Numeric Letters` is greater than or equal to `1`

Remediation:

Navigate to `Device > Setup > Management > Minimum Password Complexity`
Set `Minimum Numeric Letters` to greater than or equal to `1`

Default Value:

Not enabled.

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Best Practices for Securing Administrative Access" - https://docs.paloaltonetworks.com/pan-os-9-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.2 <u>Change Default Passwords</u> Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	🟢	🟠	🔵
v7	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

1.3.6 Ensure 'Minimum Special Characters' is greater than or equal to 1 (Automated)

Profile Applicability:

- Level 1

Description:

This checks all new passwords to ensure that they contain at least one non-alphabetic character (for example, !, $, #, %).

Rationale:

This is one of several settings that, when taken together, ensure that passwords are sufficiently complex as to thwart brute force and dictionary attacks.

Audit:

Navigate to `Device > Setup > Management > Minimum Password Complexity`
Verify `Minimum Special Characters` is greater than or equal to `1`

Remediation:

Navigate to `Device > Setup > Management > Minimum Password Complexity`
Set `Minimum Special Characters` to greater than or equal to `1`

Default Value:

Not enabled.

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Best Practices for Securing Administrative Access" - https://docs.paloaltonetworks.com/pan-os-9-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	16 Account Monitoring and Control Account Monitoring and Control			

1.3.7 Ensure 'Required Password Change Period' is less than or equal to 90 days (Automated)

Profile Applicability:

- Level 1

Description:

This defines how long a user can use a password before it expires.

Rationale:

The longer a password exists, the higher the likelihood that it will be compromised by a brute force attack, by an attacker gaining general knowledge about the user and guessing the password, or by the user sharing the password.

Impact:

Failure to change administrative passwords can result in a slow "creep" of people who have access. Especially in a situation with high staff turnover (for instance, in a NOC or SOC situation), administrative passwords need to be changed frequently.

Administrative credentials should not be shared across multiple devices. In a NOC/SOC situation, it's important to not share administrative credentials between operators (names accounts should be used), and in particular administrative credentials should never be shared across different customer infrastructures.

Audit:

Navigate to `Device > Setup > Management > Minimum Password Complexity`.
Verify `Required Password Change Period (days)` is less than or equal to `90`

Remediation:

Navigate to `Device > Setup > Management > Minimum Password Complexity`.
Set `Required Password Change Period (days)` to less than or equal to `90`

Default Value:

Not enabled.

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Best Practices for Securing Administrative Access" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html

Additional Information:

This guidance is currently under some debate in the community. If the password length is sufficient and password complexity is enforced, then in many organizations it is likely that the password change period can be increased to 6, 9 or even 12 months.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**5.3 Disable Dormant Accounts** Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	●	●	●
v7	**4.2 Change Default Passwords** Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	●	●	●
v7	**16 Account Monitoring and Control** Account Monitoring and Control			

1.3.8 Ensure 'New Password Differs By Characters' is greater than or equal to 3 (Automated)

Profile Applicability:

- Level 1

Description:

This checks all new passwords to ensure that they differ by at least three characters from the previous password.

Rationale:

This is one of several settings that, when taken together, ensure that passwords are sufficiently complex as to thwart brute force and dictionary attacks.

Impact:

This prevents the use of passwords that fall into a predictable pattern. Especially in situations that involve staff turnover, having a pattern to password changes should be avoided.

Audit:

Navigate to `Device > Setup > Management > Minimum Password Complexity`
Verify `New Password Differs By Characters` is set to greater than or equal to `3`

Remediation:

Navigate to `Device > Setup > Management > Minimum Password Complexity`
Set `New Password Differs By Characters` to `3` or more

Default Value:

Not enabled.

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Best Practices for Securing Administrative Access" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**5.2 Use Unique Passwords** Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	**4.2 Change Default Passwords** Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	●	●	●
v7	**16 Account Monitoring and Control** Account Monitoring and Control			

1.3.9 Ensure 'Prevent Password Reuse Limit' is set to 24 or more passwords (Automated)

Profile Applicability:

- Level 1

Description:

This determines the number of unique passwords that have to be most recently used for a user account before a previous password can be reused.

Rationale:

The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced. While current guidance emphasizes password length above frequent password changes, not enforcing password re-use guidance adds the temptation of using a small pool of passwords, which can make an attacker's job easier across an entire infrastructure.

Audit:

Navigate to `Device > Setup > Management > Minimum Password Complexity`. Verify `Prevent Password Reuse Limit` is greater than or equal to `24`

Remediation:

Navigate to `Device > Setup > Management > Minimum Password Complexity`. Set `Prevent Password Reuse Limit` to greater than or equal to `24`

Default Value:

Not enabled.

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Best Practices for Securing Administrative Access" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.2 <u>Change Default Passwords</u> Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	●	●	●
v7	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

1.3.10 Ensure 'Password Profiles' do not exist (Automated)

Profile Applicability:

- Level 1

Description:

Password profiles that are weaker than the recommended minimum password complexity settings must not exist.

Rationale:

As password profiles override any 'Minimum Password Complexity' settings defined in the device, they generally should not exist. If these password profiles do exist, they should enforce stronger password policies than what is set in the 'Minimum Password Complexity' settings.

Audit:

Navigate to `Device > Password Profiles`.
Verify Password Profiles weaker than the recommended minimum password complexity settings do not exist.

Remediation:

Navigate to `Device > Password Profiles`.
Ensure Password Profiles weaker than the recommended minimum password complexity settings do not exist.

Default Value:

Not configured

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Best Practices for Securing Administrative Access" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.2 <u>Change Default Passwords</u> Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	●	●	●
v7	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

1.4 Authentication Settings (for Device Mgmt)

The Authentication Settings Section contains Idle Timeout values and requirements for Authentication Profiles.

1.4.1 Ensure 'Idle timeout' is less than or equal to 10 minutes for device management (Automated)

Profile Applicability:

- Level 1

Description:

Set the Idle Timeout value for device management to 10 minutes or less to automatically close inactive sessions.

Rationale:

An unattended computer with an open administrative session to the device could allow an unauthorized user access to the firewall's management interface.

Audit:

Navigate to `Device > Setup > Management > Authentication Settings`.
Verify `Idle Timeout` is less than or equal to `10`.

Remediation:

Navigate to `Device > Setup > Management > Authentication Settings`.
Set `Idle Timeout` to less than or equal to `10`.

Default Value:

Not configured

References:

1. "How to Change the Admin Session Timeout Value" - https://live.paloaltonetworks.com/docs/DOC-5557
2. "PAN-OS Administrator's Guide 9.0 (English) - Device - Setup - Management" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-setup-management#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

1.4.2 Ensure 'Failed Attempts' and 'Lockout Time' for Authentication Profile are properly configured (Automated)

Profile Applicability:

- Level 1

Description:

Configure values for Failed Login Attempts and Account Lockout Time set to organization-defined values (for example, 3 failed attempts and a 15 minute lockout time). Do not set Failed Attempts and Lockout Time in the Authentication Settings section; any Failed Attempts or Lockout Time settings within the selected Authentication Profile do not apply in the Authentication Settings section.

Rationale:

Without a lockout limit, an attacker can continuously guess administrators' passwords. From the other point of view, if lockout settings are configured in the Authentication Settings section it may be possible for an attacker to continuously lock out all administrative accounts from accessing the device. This potential situation indicates the importance of using named administrative accounts, instead of the default, single shared "admin" account.

Audit:

Navigate to `Device > Authentication Profile`.
Verify `Failed Attempts` is set a non-zero organization-defined value.
Verify `Lockout Time` is set to a non-zero organization-defined value.

Remediation:

Navigate to `Device > Authentication Profile`.
Set `Failed Attempts` to the non-zero organization-defined value.
Set `Lockout Time` to the non-zero organization-defined value.

Default Value:

Not configured

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Device - Setup - Management" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-setup-management#
2. "PAN-OS Administrator's Guide 9.0 (English) - Authentication Profile" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-authentication-profile.html

Additional Information:

Both values must be set. If either value is not set, account lockout does not occur.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> 　Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16 <u>Account Monitoring and Control</u> 　Account Monitoring and Control			

1.5 SNMP Polling Settings

SNMP polling sets out requirements for using SNMP.

1.5.1 Ensure 'V3' is selected for SNMP polling (Automated)

Profile Applicability:

- Level 1

Description:

For SNMP polling, only SNMPv3 should be used.

Rationale:

SNMPv3 utilizes AES-128 encryption, message integrity, user authorization, and device authentication security features. SNMPv2c does not provide these security features. If an SNMPv2c community string is intercepted or otherwise obtained, an attacker could gain read access to the firewall. Note that SNMP write access is not possible.

Impact:

Any clear-text administrative protocol (such as SNMPv2) can expose valuable information to any attacker that is in a position to eavesdrop on that protocol.

Audit:

Navigate to `Device > Setup > Operations > Miscellaneous > SNMP Setup`
Verify `V3` is selected.

Remediation:

Navigate to `Device > Setup > Operations > Miscellaneous > SNMP Setup`
Select `V3`.
In order to be usable, the `User` and `View` sections of this dialog should also be completed. These settings need to match the settings in the organization's NMS (Network Management System)

Default Value:

Not configured

References:

1. "How to Setup SNMPv3 Polling" - https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-SNMPv3-Polling/ta-p/58225

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.10 <u>Encrypt Sensitive Data in Transit</u>** Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	**9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u>** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	**14.4 <u>Encrypt All Sensitive Information in Transit</u>** Encrypt all sensitive information in transit.		●	●

1.6 Device Services Settings

The Device Services Settings section contains requirements for verifying the update server's identity, enabling redundant NTP services, and using a valid certificate for securing VPN remote access.

1.6.1 Ensure 'Verify Update Server Identity' is enabled (Automated)

Profile Applicability:

- Level 1

Description:

This setting determines whether or not the identity of the update server must be verified before performing an update session. Note that if an SSL Forward Proxy is configured to intercept the update session, this option may need to be disabled (because the SSL Certificate will not match).

Rationale:

Verifying the update server identity before package download ensures the packages originate from a trusted source. Without this, it is possible to receive and install an update from a malicious source.

Impact:

This setting protects the device from an "evilgrade" attack, where a successful DNS attack can redirect the firewall to an attacker-controlled update server, which can then serve a modified update.

Audit:

Navigate to `Device > Setup > Services > Services`.
Verify that the `Verify` Update Server Identity box is checked.

Remediation:

Navigate to `Device > Setup > Services > Services`.
Set the `Verify Update Server Identity` box to checked.

Default Value:

Not configured

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Install Content Updates" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content-updates/install-content-and-software-updates.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**7.3 Perform Automated Operating System Patch Management** Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	**3.4 Deploy Automated Operating System Patch Management Tools** Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	**3.5 Deploy Automated Software Patch Management Tools** Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●
v7	**11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches** Secure Configuration for Network Devices, such as Firewalls, Routers and Switches			

1.6.2 Ensure redundant NTP servers are configured appropriately (Automated)

Profile Applicability:

- Level 1

Description:

These settings enable use of primary and secondary NTP servers to provide redundancy in case of a failure involving the primary NTP server.

Rationale:

NTP enables the device to maintain an accurate time and date when receiving updates from a reliable NTP server. Accurate timestamps are critical when correlating events with other systems, troubleshooting, or performing investigative work. Logs and certain cryptographic functions, such as those utilizing certificates, rely on accurate time and date parameters. In addition, rules referencing a Schedule object will not function as intended if the device's time and date are incorrect.

For additional security, authenticated NTP can be utilized. If Symmetric Key authentication is selected, only SHA1 should be used, as MD5 is considered severely compromised.

Most organizations will maintain a pair of internal NTP servers for all internal time services. These servers will either be self-contained atomic clocks, or will collect time from a known reliable source (often GPS or a well-known internet server pool will be used).

Audit:

Navigate to `Device > Setup > Services > Services`.
Verify `Primary NTP Server Address` is set appropriately.
Verify `Secondary NTP Server Address` is set appropriately.

Remediation:

Navigate to `Device > Setup > Services > Services`.
Set `Primary NTP Server Address` appropriately.
Set `Secondary NTP Server Address` appropriately.

Default Value:

Not configured

References:

1. "The NIST Authenticated NTP Service" - http://www.nist.gov/pml/div688/grp40/authntp.cfm

2. "PAN-OS Administrator's Guide 9.0 (English) - Global Services Settings" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-setup-services/global-services-settings.html
3. "How to Configure Authenticated NTP" - https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-Authenticated-NTP/ta-p/54495

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.4 Standardize Time Synchronization** Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	**6.1 Utilize Three Synchronized Time Sources** Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

1.6.3 Ensure that the Certificate Securing Remote Access VPNs is Valid (Manual)

Profile Applicability:

- Level 1

- Level 2

Description:

The Certificate used to secure Remote Access VPNs should satisfy the following criteria:

- It should be a valid certificate from a trusted source. In almost cases this means a trusted Public Certificate Authority, as in most cases remote access VPN users will not have access to any Private Certificate Authorities for Certificate validation.
- The certificate should have a valid date. It should not have a "to" date in the past (it should not be expired), and should not have a "from" date in the future.
- The key length used to encrypt the certificate should be 2048 bits or more.
- The hash used to sign the certificate should be SHA-2 or better.
- When the Certificate is applied, the TLS version should be 1.1 or higher (1.2 is recommended)

Rationale:

If presented with a certificate error, the end user in most cases will not be able to tell if their session is using a self-signed or expired certificate, or if their session is being eavesdropped on or injected into by a "Man in the Middle" attack. This means that self-signed or invalid certificates should never be used for VPN connections.

Impact:

Not using a trusted Certificate, issued by a trusted Public Certificate Authority means that clients establishing VPN sessions will always see an error indicating an untrusted Certificate. This means that they will have no method of validating if their VPN session is being hijacked by a "Monkey in the Middle" (MitM) attack. It also "trains" them to bypass certificate warnings for other services, making MitM attacks easier for those other services as well.

Audit:

Verify that the certificate being used to secure the VPN meets the criteria listed above:
Navigate to `Device > Certificate Management > Certificates`
Ensure that a valid certificate is applied to the HTTPS portal:
Navigate to `Network > GlobalProtect > Portals > Portal Configuration > (Select the Portal being assessed) > Authentication > SSL/TLS Profile`
Ensure that a valid certificate is applied to the GlobalProtect Gateway:
Navigate to `Network > GlobalProtect > Gateways > (Select the Gateway being Assessed) > Authentication > SSL/TLS Service Profile`
Ensure that the correct Certificate is selected.
Ensure that the Minimum TLS version is configured to be 1.1 or higher (TLSv1.2 is recommended).

Remediation:

Create a CSR and install a certificate from a public CA (Certificate Authority) here:
Navigate to `Device > Certificate Management > Certificates`
Apply a valid certificate to the HTTPS portal:
Navigate to `Network > GlobalProtect > Portals > Portal Configuration > Authentication > SSL/TLS Profile`
Apply a valid certificate to the GlobalProtect Gateway:
Navigate to `Network > GlobalProtect > Gateways > Authentication > SSL/TLS Service Profile`
Configure the Service Profile to use the correct certificate
Ensure that the Minimum TLS version is set to 1.1 or 1.2 (1.2 is recommended).

Default Value:

Not configured

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - GlobalProtect Certificate Best Practices" - https://docs.paloaltonetworks.com/globalprotect/9-0/globalprotect-admin/get-started/enable-ssl-between-globalprotect-components/globalprotect-certificate-best-practices.html
2. "PAN-OS Administrator's Guide 9.0 (English) - Deploy Server Certificates to the GlobalProtect Components" - https://docs.paloaltonetworks.com/globalprotect/9-0/globalprotect-admin/get-started/enable-ssl-between-globalprotect-components/deploy-server-certificates-to-the-globalprotect-components.html#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**13.9 Deploy Port-Level Access Control** Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.			●
v7	**14.4 Encrypt All Sensitive Information in Transit** Encrypt all sensitive information in transit.		●	●

2 User Identification

The User Identification section covers requirements for IP address mapping and User-ID functionality.

2.1 Ensure that IP addresses are mapped to usernames (Automated)

Profile Applicability:

- Level 2

Description:

Configure appropriate settings to map IP addresses to usernames. Mapping userids to IP addresses is what permits the firewall to create rules based on userids and groups rather than IP addresses and subnets, as well as log events by userids rather than IP addresses or DNS names. The specifics of how to achieve IP-to-username mapping is highly dependent on the environment. It can be enabled by integrating the firewall with a domain controller, Exchange server, captive portal, Terminal Server, User-ID Agent, XML API, or syslog data from a variety of devices.

Rationale:

Understanding which user is involved in a security incident allows appropriate personnel to move quickly between the detection and reaction phases of incident response. In environments with either short DHCP lease times, or where users may move frequently between systems, the ability to analyze or report, or alert on events based on user accounts or user groups is a tremendous advantage. For forensics tasks when DHCP lease information may not be available, the Source User information may be the only way to tie together related data.

Audit:

To validate if this recommendation has been met, look at the `Source User` column in the URL Filtering or Traffic logs (`Monitor > Logs > URL Filtering` and `Logs > Traffic Logs`, respectively.)
User traffic originating from a trusted zone should identify a username.

Remediation:

To Set User-ID Agents:
Navigate to `Device > User Identification > User-ID Agents`
Set the Name, IP Address and Port of the User-ID Agent`
Enable User Identification for each monitored zone that will have user accounts:
Navigate to `Network > Zone, for each relevant zone enable User Identification`
To Set Terminal Services Agents:
Navigate to `Device > Terminal Services Agents`
Set the Name, IP Address and Port of the Terminal Services Agent
Enable User Identification for each monitored zone that will have Terminal Servers:
Navigate to `Network > Zone, enable User Identification`

References:

1. "Best Practices for Securing User-ID Deployments" - https://live.paloaltonetworks.com/docs/DOC-7912
2. "How to Configure Group Mapping settings?" - https://live.paloaltonetworks.com/docs/DOC-4994
3. "PAN-OS Administrator's Guide 9.0 (English) - User-ID" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id
4. https://paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/tech-briefs/techbrief-user-id.pdf

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

2.2 Ensure that WMI probing is disabled (Automated)

Profile Applicability:

- Level 2

Description:

Disable WMI probing if it is not required for User-ID functionality in the environment.

Rationale:

WMI probing normally requires a domain administrator account. A malicious user could capture the encrypted password hash for offline cracking or relayed authentication attacks. Relying on other forms of user identification, such as using UserID Agents or security log monitoring, mitigates this risk.

In addition, it is easy to mis-configure this feature such that it is enabled on untrusted interfaces. This can result in a domain administrator account and the associated password hash being sent to untrusted hosts on the internet, where malicious users can then capture that hash for offline cracking.

Impact:

While this removes the exposure of having the WMI user account password being compromised, it also reduces the effectiveness of user identification during operation of the firewall (applying rules and policies). This trade-off should be weighed carefully for all installations.

Audit:

Navigate to `Device > User Identification > User Mapping > Palo Alto Networks User ID Agent Setup`.
Verify that `Enable Probing` is not checked.

Remediation:

Navigate to `Device > User Identification > User Mapping > Palo Alto Networks User ID Agent Setup`.
Set `Enable Probing` so it is unchecked.

Default Value:

Not configured

References:

1. "R7-2014-16: Palo Alto Networks User-ID Credential Exposure" - https://blog.rapid7.com/2014/10/14/palo-alto-networks-userid-credential-exposure/

2. "Best Practices for Securing User-ID Deployments" -
   https://live.paloaltonetworks.com/docs/DOC-7912
3. "PAN-OS Administrator's Guide 9.0 (English) - Client Probing" -
   https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/user-id-concepts/user-mapping/client-probing

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

2.3 Ensure that User-ID is only enabled for internal trusted interfaces (Automated)

Profile Applicability:

- Level 1

Description:

Only enable the User-ID option for interfaces that are both internal and trusted. There is rarely a legitimate need to allow WMI probing (or any user-id identification) on an untrusted interface. The exception to this is identification of remote-access VPN users, who are identified as they connect.

Rationale:

PAN released a customer advisory in October of 2014 warning of WMI probing on untrusted interfaces with User-ID enabled. This can result in theft of the password hash for the account used in WMI probing.

Impact:

If WMI probing is enabled without limiting the scope, internet hosts that are sources or destinations of traffic will be probed, and the password hash of the configured Domain Admin account can be captured by an outside attacker on such a host.

Audit:

Navigate to `Network > Network Profiles > Interface Management`.
Verify that `User-ID` is only enabled for interfaces that are both internal and trusted.

Remediation:

Navigate to `Network > Network Profiles > Interface Management`.
Set `User-ID` to be checked only for interfaces that are both internal and trusted; uncheck it for all other interfaces.

Default Value:

By default, WMI probing and all User-ID functions are disabled.

References:

1. "Customer advisory: Security Impact of User-ID Misconfiguration" - https://live.paloaltonetworks.com/docs/DOC-8125
2. "R7-2014-16: Palo Alto Networks User-ID Credential Exposure" - https://blog.rapid7.com/2014/10/14/palo-alto-networks-userid-credential-exposure/

3. "Best Practices for Securing User-ID Deployments" - https://live.paloaltonetworks.com/docs/DOC-7912
4. "User-ID Best Practices" - https://live.paloaltonetworks.com/docs/DOC-6591
5. "PAN-OS Administrator's Guide 9.0 (English) - Client Probing" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/user-id-concepts/user-mapping/client-probing

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure** Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	**6.2 Activate audit logging** Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	**16 Account Monitoring and Control** Account Monitoring and Control			
v7	**16.13 Alert on Account Login Behavior Deviation** Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

2.4 Ensure that 'Include/Exclude Networks' is used if User-ID is enabled (Automated)

Profile Applicability:

- Level 1

Description:

If User-ID is configured, use the Include/Exclude Networks section to limit the User-ID scope to operate only on trusted networks. There is rarely a legitimate need to allow WMI probing or other User identification on an untrusted network.

Rationale:

The Include/Exclude Networks feature allow users to configure boundaries for the User-ID service. By using the feature to limit User-ID probing to only trusted internal networks, the risks of privileged information disclosure through sent probes can be reduced. Note that if an entry appears in the Include/Exclude Networks section, an implicit exclude-all-networks policy will take effect for all other networks.

Impact:

Not restricting the networks subject to User Identification means that the administrative credentials (userid and password hash) used for this task will transit untrusted networks, or be sent to untrusted hosts. Capturing these credentials exposes them to offline cracking attacks.

Audit:

Navigate to `Device > User Identification > User Mapping > Include/Exclude Networks`.
Verify that all trusted internal networks have a Discovery value of `Include`.
Verify that all untrusted external networks have a Discovery value of `Exclude`. Note that any value in the trusted networks list implies that all other networks are untrusted.

Remediation:

Navigate to `Device > User Identification > User Mapping > Include/Exclude Networks`.
Set all trusted internal networks to have a Discovery value of `Include`.
Set all untrusted external networks to have a Discovery value of `Exclude`. Note that any value in the trusted networks list implies that all other networks are untrusted.

Default Value:

Not configured

References:

1. Best Practices for Securing User-ID Deployments -
   https://live.paloaltonetworks.com/docs/DOC-7912

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**12.2 Establish and Maintain a Secure Network Architecture** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		🟠	🔵
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		🟠	🔵

2.5 Ensure that the User-ID Agent has minimal permissions if User-ID is enabled (Manual)

Profile Applicability:

- Level 1

Description:

If the integrated (on-device) User-ID Agent is utilized, the Active Directory account for the agent should only be a member of the Event Log Readers group, Distributed COM Users group, and Domain Users group. If the Windows User-ID agent is utilized, the Active Directory account for the agent should only be a member of the Event Log Readers group, Server Operators group, and Domain Users group.

Rationale:

As a principle of least privilege, user accounts should have only minimum necessary permissions. If an attacker compromises a User-ID service account with domain admin rights, the organization is at far greater risk than if the service account were only granted minimum rights.

Impact:

Using accounts with full administrative privileges when those rights are not required is always a bad idea. This is particularly true for service accounts of this type, which in many organizations do not see strong passwords or frequent password changes. In addition, service passwords are stored in the Windows Registry, and are recoverable with the user of appropriate malicious tools. The principal of least privilege means that any compromised accounts of this type have less value to an attacker, and expose fewer assets based on their rights.

Audit:

Navigate to `Active Directory Users and Computers` for the Active Directory under consideration.
Verify that the service account for the User-ID agent is not a member of any groups other than Event Log Readers, Distributed COM Users, and Domain Users (for the integrated, on-device User-ID agent) or Event Log Readers, Server Operators, and Domain Users (for the Windows User-ID agent.)

Remediation:

Navigate to `Active Directory Users and Computers`.
Set the service account for the User-ID agent so that it is only a member of the Event Log Readers, Distributed COM Users, and Domain Users (for the integrated, on-device User-ID agent) or the Event Log Readers, Server Operators, and Domain Users groups (for the Windows User-ID agent.)

Default Value:

Not configured

References:

1. "Best Practices for Securing User-ID Deployments" - https://live.paloaltonetworks.com/docs/DOC-7912
2. "User-ID Best Practices" - https://live.paloaltonetworks.com/docs/DOC-6591
3. "PAN-OS Administrator's Guide 9.0 (English) - Configure User Mapping Using the Windows User-ID Agent" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-mapping-using-the-windows-user-id-agent.html
4. "PAN-OS Administrator's Guide 9.0 (English) - Configure User Mapping Using the PAN-OS Integrated User-ID Agent" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-mapping-using-the-pan-os-integrated-user-id-agent.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	9 Limitation and Control of Network Ports, Protocols, and Services Limitation and Control of Network Ports, Protocols, and Services			

2.6 Ensure that the User-ID service account does not have interactive logon rights (Automated)

Profile Applicability:

- Level 1

Description:

Restrict the User-ID service account from interactively logging on to systems in the Active Directory domain.

Rationale:

In the event of a compromised User-ID service account, restricting interactive logins forbids the attacker from utilizing services such as RDP against computers in the Active Directory domain of the organization. This reduces the impact of a User-ID service account compromise.

Audit:

Navigate to `Active Directory Group Policies`.
Verify that Group Policies restricts the interactive logon privilege for the User-ID service account.
or
Navigate to `Active Directory Managed Service Accounts`.
Verify that Managed Service Accounts restricts the interactive logon privilege for the User-ID service account.

Remediation:

Navigate to `Active Directory Group Policies`.
Set Group Policies to restrict the interactive logon privilege for the User-ID service account.
or
Navigate to `Active Directory Managed Service Accounts`.
Set Managed Service Accounts to restrict the interactive logon privilege for the User-ID service account.

Default Value:

Not configured

References:

1. "Best Practices for Securing User-ID Deployments" - https://live.paloaltonetworks.com/docs/DOC-7912
2. "PAN-OS Administrator's Guide 9.0 (English) - Configure User Mapping Using the Windows User-ID Agent" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-

os-admin/user-id/map-ip-addresses-to-users/configure-user-mapping-using-the-windows-user-id-agent.html

3. "PAN-OS Administrator's Guide 9.0 (English) - Configure User Mapping Using the PAN-OS Integrated User-ID Agent" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-mapping-using-the-pan-os-integrated-user-id-agent.html

4. "User-ID Best Practices" - https://live.paloaltonetworks.com/docs/DOC-6591

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.5 <u>Establish and Maintain an Inventory of Service Accounts</u> Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.		🟠	🔵
v7	4 <u>Controlled Use of Administrative Privileges</u> Controlled Use of Administrative Privileges			

2.7 Ensure remote access capabilities for the User-ID service account are forbidden. (Automated)

Profile Applicability:

- Level 1

Description:

Restrict the User-ID service account's ability to gain remote access into the organization. This capability could be made available through a variety of technologies, such as VPN, Citrix GoToMyPC, or TeamViewer. Remote services that integrate authentication with the organization's Active Directory may unintentionally allow the User-ID service account to gain remote access.

Rationale:

In the event of a compromised User-ID service account, restricting the account's ability to remotely access resources within the organization's internal network reduces the impact of a service account compromise.

Audit:

Auditing is operating-system dependent. For instance, in Windows Active Directory, this account should not be included in any group that grants the account access to VPN or Wireless access. In addition, domain administrative accounts should not have remote desktop (RDP) access to all domain member workstations.

Remediation:

Remove this account from all groups that might grant remote access to the network, or to any network services or hosts. Remediation is operating-system dependent. For instance, in Windows Active Directory, this account should be removed from any group that grants the account access to VPN or Wireless access. In addition, domain administrative accounts by default have remote desktop (RDP) access to all domain member workstations - this should be explicitly denied for this account.

Default Value:

Not configured

References:

1. "Best Practices for Securing User-ID Deployments" - https://live.paloaltonetworks.com/docs/DOC-7912
2. "User-ID Best Practices" - https://live.paloaltonetworks.com/docs/DOC-6591
3. "PAN-OS Administrator's Guide 9.0 (English) - Configure User Mapping Using the Windows User-ID Agent" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-

os-admin/user-id/map-ip-addresses-to-users/configure-user-mapping-using-the-windows-user-id-agent.html

4. "PAN-OS Administrator's Guide 9.0 (English) - Configure User Mapping Using the PAN-OS Integrated User-ID Agent" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-mapping-using-the-pan-os-integrated-user-id-agent.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4 Controlled Use of Administrative Privileges Controlled Use of Administrative Privileges			

2.8 Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones (Automated)

Profile Applicability:

- Level 1

Description:

Create security policies to deny Palo Alto User-ID traffic originating from the interface configured for the UID Agent service that are destined to any untrusted zone.

Rationale:

If User-ID and WMI probes are sent to untrusted zones, the risk of privileged information disclosure exists. The information disclosed can include the User-ID Agent service account name, domain name, and encrypted password hashes sent in User-ID and WMI probes. To prevent this exposure, msrpc traffic originating from the firewall to untrusted networks should be explicitly denied. This security policy should be in effect even for environments not currently using WMI probing to help guard against possible probe misconfigurations in the future.

This setting is a "fail safe" to prevent exposure of this information if any of the other WMI User control settings are misconfigured.

Audit:

Navigate to `Device > Setup > Services > Services Features > Service Route Configuration > Customize`.
Click on the protocol in use (`IPv4` and/or `IPv6`).
Click `UID Agent`.
Click on the address object for the UID Agent's IP address.
Verify `SOURCE/NAME` is set to '`Deny msrpc to untrusted`'.
Verify `SOURCE/ZONE` is set to '`INSIDE`'.
Verify `SOURCE/Address` is set to the Address object for the UID Agent.
Verify `DESTINATION/ZONE` is set to '`GUEST`' and '`OUTSIDE`'.
Verify `DESTINATION/Address` is set to '`any`'.
Verify `DESTINATION/Application` is set to '`msrpc`'.
Verify `DESTINATION/Service` is set to '`application-default`'.
Verify `DESTINATION/Action` is set to '`Block`' (red circle with diagonal line).

Remediation:

Navigate to `Device > Setup > Services > Services Features > Service Route Configuration > Customize`.
Click on the protocol in use (`IPv4` and/or `IPv6`).
Click `UID Agent`.
Click on the address object for the UID Agent's IP address.
Set `SOURCE/NAME` to '`Deny msrpc to untrusted`'.
Set `SOURCE/ZONE` to '`INSIDE`'.
Set `SOURCE/Address` to the Address object for the UID Agent.
Set `DESTINATION/ZONE` to '`GUEST`' and '`OUTSIDE`'.
Set `DESTINATION/Address` to '`any`'.
Set `DESTINATION/Application` to '`msrpc`'.
Set `DESTINATION/Service` to '`application-default`'.
Set `DESTINATION/Action` to '`Block`' (red circle with diagonal line).

References:

1. "Best Practices for Securing User-ID Deployments" - https://live.paloaltonetworks.com/docs/DOC-7912
2. "User-ID Best Practices" - https://live.paloaltonetworks.com/docs/DOC-6591
3. "PAN-OS Administrator's Guide 9.0 (English) - Configure User Mapping Using the Windows User-ID Agent" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-mapping-using-the-windows-user-id-agent.html
4. "PAN-OS Administrator's Guide 9.0 (English) - Configure User Mapping Using the PAN-OS Integrated User-ID Agent" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-mapping-using-the-pan-os-integrated-user-id-agent.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	14 Controlled Access Based on the Need to Know Controlled Access Based on the Need to Know			

3 High Availability

The High Availability section includes requirements for High Availability peer synchronization and monitoring.

3.1 Ensure a fully-synchronized High Availability peer is configured (Automated)

Profile Applicability:

- Level 1

Description:

Ensure a High Availability peer is fully synchronized and in a passive or active state.

Rationale:

To ensure availability of both the firewall and the resources it protects, a High Availability peer is required. In the event a single firewall fails, or when maintenance such as a software update is required, the HA peer can be used to automatically fail over session states and maintain overall availability

Impact:

Not configuring High Availability (HA) correctly directly impacts the Availability of the system. With HA in place, standard maintenance such as OS updates, network and power cabling can be accomplished with no outage or a minimum impact.

Audit:

Navigate to `Device > High Availability > HA Communications`.
In the `HA Communications.` `>Data Link (HA2)` section, verify that the correct interface is selected. Verify the desired `protocol (IPv4 or IPv6)` is selected. Verify the correct Transport is selected. Verify the `Enable Session Synchronization` box is checked.

Remediation:

Navigate to `Device > High Availability > HA Communications`.
Click `HA Communications.` Click `Data Link (HA2)`. Select the correct interface. Select the desired `protocol (IPv4 or IPv6)`. Select the correct Transport. Set the `Enable Session Synchronization` box to be checked.
Choose `Save Configuration`.

Default Value:

Not Configured

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - High Availability" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-high-availability.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	11 <u>Secure Configuration for Network Devices, such as Firewalls, Routers and Switches</u> Secure Configuration for Network Devices, such as Firewalls, Routers and Switches			

3.2 Ensure 'High Availability' requires Link Monitoring and/or Path Monitoring (Automated)

Profile Applicability:

- Level 1

Description:

Configure Link Monitoring and/or Path Monitoring under High Availability options. If Link Monitoring is utilized, all links critical to traffic flow should be monitored.

Rationale:

If Link or Path Monitoring is not enabled, the standby router will not automatically take over as active if a critical link fails on the active firewall. Services through the firewall could become unavailable as a result.

Impact:

Not configuring High Availability (HA) correctly directly impacts the Availability of the system. With HA in place, standard maintenance such as OS updates, network and power cabling can be accomplished with no outage or a minimum impact.

Without Link and Path monitoring in particular, failover will only occur when the primary device fails completely. Link and path monitoring permits failover if a critical interface loses link (either due to cabling or an upstream switch failover), or if a route or path fails (indicating an upstream issue that affects local Layer 3).

Audit:

To verify Link Monitoring from GUI:
Navigate to `Device > High Availability > Link and Path Monitoring`.
In the `Link Monitoring` section, verify the correct interfaces are in the `Link Group` and `Group Failure Conditions`
Under the `Link Monitoring` section, verify `Failure Condition` is set to `Any`.
Verify `Enabled button` is `checked`.
To verify Path Monitoring from GUI:
Navigate to `Device > High Availability > Link and Path Monitoring`.
In the `Path Monitoring` section, verify `Option` is set correctly.
Verify `Failure Condition` is set to `Any`.
Verify `Name, IP Address, Failure Condition` is set correctly.
Verify `Default setting` is set to `Any`.
Verify `Enabled button` is `checked`.

Remediation:

To set Link Monitoring from GUI:
Navigate to `Device > High Availability > Link and Path Monitoring`.
Click `Link Monitoring`.
Set the correct interfaces to the `Link Group` and `Group Failure Conditions`.
Click `Link Monitoring`.
Set Failure Condition to `Any`.
Check Enabled button.
To set Path Monitoring from GUI:
Navigate to `Device > High Availability > Link and Path Monitoring`.
Click `Path Monitoring`.
Set `Option` correctly.
Set `Failure Condition` to `Any`.
Set `Name, IP Address, Failure Condition` correctly.
Set `Default setting` to `Any`.
Check Enabled button.

Default Value:

Not Configured

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - High Availability" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-high-availability.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches Secure Configuration for Network Devices, such as Firewalls, Routers and Switches			

3.3 Ensure 'Passive Link State' and 'Preemptive' are configured appropriately (Manual)

Profile Applicability:

- Level 1

Description:

Set the Passive Link State to auto, and uncheck the Preemptive option to disable it.

Rationale:

Simultaneously enabling the 'Preemptive' option and setting the 'Passive Link State' option to 'Shutdown' could cause a 'preemptive loop' if Link and Path Monitoring are both configured. This will negatively impact the availability of the firewall and network services, should a monitored failure occur.

Impact:

Incorrectly configuring this setting will adversely affect availability, rather than positively affect it.

Audit:

To ensure `Active/Passive Settings` are configured correctly:
Navigate to `Device > High Availability > General > Active/Passive Settings`.
Verify `Passive Link State` is set to `auto`.
To ensure `Election Settings` are configured correctly:
Navigate to `Device > High Availability > Election Settings`.
Verify `Preemptive` is disabled.

Remediation:

To set `Active/Passive Settings` correctly:
Navigate to `Device > High Availability > General > Active/Passive Settings`.
Set `Passive Link State` to `auto`.
To set `Election Settings` correctly:
Navigate to `Device > High Availability > Election Settings`.
Set `Preemptive` to be disabled.

Default Value:

Not Configured

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - High Availability" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-high-availability.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	11 <u>Secure Configuration for Network Devices, such as Firewalls, Routers and Switches</u> Secure Configuration for Network Devices, such as Firewalls, Routers and Switches			

4 Dynamic Updates

The Dynamic Updates section covers requirements for scheduled downloads for antivirus updates and for applications and threats updates.

4.1 Ensure 'Antivirus Update Schedule' is set to download and install updates hourly (Automated)

Profile Applicability:

- Level 1

Description:

Set Antivirus Update Schedule to download and install updates hourly.

Rationale:

New antivirus definitions may be released at any time. With an hourly update schedule, the firewall can ensure threats with new definitions are quickly mitigated. A daily update schedule could leave an organization vulnerable to a known virus for nearly 24 hours, in a worst-case scenario. Setting an appropriate threshold value reduces the risk of a bad definition file negatively affecting traffic.

Audit:

Navigate to `Device > Dynamic Updates > Antivirus Update Schedule`.
Verify that `Action` is set to `Download and Install`.
Verify that `Recurrence` is set to `Hourly`.

Remediation:

Navigate to `Device > Dynamic Updates > Antivirus Update Schedule`.
Set `Action` to `Download and Install`.
Set `Recurrence` to `Hourly`.

Default Value:

Not Configured

References:

1. "Tips for Managing Content Updates" - https://live.paloaltonetworks.com/docs/DOC-1578
2. "PAN-OS Administrator's Guide 9.0 (English) -Dynamic Content Updates" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content-updates/dynamic-content-updates.html
3. "PAN-OS Administrator's Guide 9.0 (English) - Install Content Updates" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content-updates/install-content-and-software-updates.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 <u>Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	🟢	🟠	🔵
v7	3.4 <u>Deploy Automated Operating System Patch Management Tools</u> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	🟢	🟠	🔵
v7	3.5 <u>Deploy Automated Software Patch Management Tools</u> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	🟢	🟠	🔵

4.2 Ensure 'Applications and Threats Update Schedule' is set to download and install updates at daily or shorter intervals (Automated)

Profile Applicability:

- Level 1

Description:

Set the Applications and Threats Update Schedule to download and install updates at daily or shorter intervals.

Rationale:

New Applications and Threats file versions may be released at any time. With a frequent update schedule, the firewall can ensure threats with new signatures are quickly mitigated, and the latest application signatures are applied.

Audit:

Navigate to `Device > Dynamic Updates > Application and Threats Update Schedule`.
Verify that `Action` is set to `Download and Install`.
Verify that `Recurrence` is set to `Daily`, `Hourly` or `Every 30 Minutes`

Remediation:

Navigate to `Device > Dynamic Updates > Application and Threats Update Schedule`.
Set `Action` to `Download and Install`.
Set `Recurrence` to `Daily`, `Hourly` or `Every 30 Minutes`

Default Value:

This setting is by default set to `Weekly`.

References:

1. "Tips for Managing Content Updates" - https://live.paloaltonetworks.com/docs/DOC-1578
2. "PAN-OS Administrator's Guide 9.0 (English) -Dynamic Content Updates" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content-updates/dynamic-content-updates.html
3. "PAN-OS Administrator's Guide 9.0 (English) - Install Content Updates" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content-updates/install-content-and-software-updates.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**7.3 Perform Automated Operating System Patch Management** Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	**3.4 Deploy Automated Operating System Patch Management Tools** Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	**3.5 Deploy Automated Software Patch Management Tools** Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

5 Wildfire

WildFire is a cloud-based virtual malware detection, analysis, and blocking service that is native to Palo Alto next generation firewalls. The service detects and blocks targeted and unknown malware, exploits, and outbound command and control activity by observing malicious behavior in real time, rather than using pre-existing signatures. Post-analysis, WildFire generates protections that are shared globally in real-time.

The WildFire section covers requirements related to WildFire file size upload limits, file blocking profiles, decrypted content forwarding, session information settings, malicious file alerts, and update downloads.

5.1 Ensure that WildFire file size upload limits are maximized (Automated)

Profile Applicability:

- Level 1

Description:

The default file size limits on the firewall are designed to include the majority of malware in the wild (which is smaller than the default size limits) and to exclude large files that are very unlikely to be malicious and that can impact WildFire file-forwarding capacity.

Rationale:

Because the firewall has a specific capacity reserved to forward files for WildFire analysis, forwarding high numbers of large files can cause the firewall to skip forwarding of some files. This condition occurs when the maximum file size limits are configured for a file type that is traversing the firewall at a high rate. In this case, a potentially malicious file might not get forwarded for WildFire analysis. Consider this possible condition if you would like to increase the size limit for files other than PEs beyond their default size limit.

Impact:

Using larger file filtering can cause the system to skip files in the event multiple larger files are sent.

Audit:

Navigate to `Device > Setup > WildFire`.
Navigate to the `General Settings` sections.
Verify the maximum size for each file type at the defaults or larger, to a size that is as large enough to account for "large" files, but not large enough to affect performance of the hardware.

Remediation:

Navigate to `Device > Setup > WildFire`.
Click the `General Settings` edit icon.
Set the maximum size for each file type are larger than the defaults, to a size that is as large enough to account for "large" files, but not large enough to affect performance of the hardware.
In PAN-OS 9.x and higher, the default file sizes for WildFire are:

- pe (Portable Executable) - 16MB
- apk (Android Application)- 10MB
- pdf (Portable Document Format) - 3072KB

- ms-office (Microsoft Office) — 16384KB
- jar (Packaged Java class file) — 5MB
- flash (Adobe Flash) — 5MB
- MacOSX (DMG/MAC-APP/MACH-O PKG files) — 10MB
- archive (RAR and 7z files) — 50MB
- linux (ELF files) — 50MB
- script (JScript, VBScript, PowerShell, and Shell Script)- 20KB

In PAN-OS 9.x and higher, the maximum file sizes for Wildfire are:

- pe (Portable Executable) - 50MB
- apk (Android Application)- 50MB
- pdf (Portable Document Format) - 51200KB
- ms-office (Microsoft Office) — 51200KB
- jar (Packaged Java class file) — 20MB
- flash (Adobe Flash) — 10MB
- MacOSX (DMG/MAC-APP/MACH-O PKG files) — 50MB
- archive (RAR and 7z files) — 50MB
- linux (ELF files) — 50MB
- script (JScript, VBScript, PowerShell, and Shell Script)- 4096KB

Default Value:

In PAN-OS 9.x, the default file sizes for WildFire are:

- pe (Portable Executable) - 16MB
- apk (Android Application)- 10MB
- pdf (Portable Document Format) - 3072KB
- ms-office (Microsoft Office) — 16384KB
- jar (Packaged Java class file) — 5MB
- flash (Adobe Flash) — 5MB
- MacOSX (DMG/MAC-APP/MACH-O PKG files) — 10MB
- archive (RAR and 7z files) — 50MB
- linux (ELF files) — 50MB
- script (JScript, VBScript, PowerShell, and Shell Script)- 20KB

References:

1. "How to Configure WildFire" - https://live.paloaltonetworks.com/docs/DOC-3252
2. https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-deployment-best-practices/wildfire-best-practices

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**10.1 Deploy and Maintain Anti-Malware Software** Deploy and maintain anti-malware software on all enterprise assets.	🟢	🟠	🔵
v7	**8 Malware Defenses** Malware Defenses			

5.2 Ensure a WildFire Analysis profile is enabled for all security policies (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that all files traversing the firewall are inspected by WildFire by setting a Wildfire file blocking profile on all security policies.

Rationale:

Traffic matching security policies that do not include a WildFire file blocking profile will not utilize WildFire for file analysis. Wildfire analysis is one of the key security measures available on this platform. Without Wildfire analysis enabled, inbound malware can only be analyzed by signature - which industry wide is roughly 40-60% effective. In a targeted attack, the success of signature-based-only analysis drops even further.

Audit:

To verify WildFire Analysis Profile:

- Navigate to `Objects > Security Profiles > WildFire Analysis Profile` verify that a profile exists.

To verify File Blocking Rules:

- For each Security Policy were the action is set to Allow, edit the Rule and navigate to `Actions > Profile Setting. Ensure that the WildFire Analysis` is set to `Allow` and verify that a profile is set.

If **Group Profiles** are used:

- Navigate to `Policies > Security`
- For each Security Policy were the action is set to Allow, edit the Rule and navigate to `Actions > Profile Setting.` Ensure that the `Profile Type` is set to `Group.`
- Navigate to Objects > Security Profile Groups. Open the Security Profile Group used above, and ensure that the Wildfire Analysis Profile is set.

Remediation:

To Set File Blocking Profile:

- Navigate to `Objects > Security Profiles > WildFire Analysis Profile.`

- Create a WildFire profile that has 'Application Any', 'File Types Any', and 'Direction Both'

To Set WildFire Analysis Rules:

- Navigate to `Policies > Security`.
- For each Security Policy Rule where the action is "Allow", Navigate to `Actions > Profile Setting > WildFire Analysis` and set a WildFire Analysis profile.

Group Profiles can also be used. To take this approach:

- Navigate to `Objects > Security Profile Groups`. Create a Security Profile Group, and ensure that (among other settings) the `Wildfire Analysis Profile` is set to the created profile.
- Navigate to `Policies > Security`. For each Security Policy Rule where the action is "Allow", Navigate to `Actions > Profile Setting`. Modify the `Profile Type` to `Group`, and set the `Group Profile` to the created Security Profile Group.

Default Value:

Not Configured

References:

1. "Wildfire Administrator's Guide 9.0 (English)" - https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8 Malware Defenses Malware Defenses			

5.3 Ensure forwarding of decrypted content to WildFire is enabled (Automated)

Profile Applicability:

- Level 1

Description:

Allow the firewall to forward decrypted content to WildFire. Note that SSL Forward-Proxy must also be enabled and configured for this setting to take effect on inside-to-outside traffic flows.

Rationale:

As encrypted Internet traffic continues to proliferate, WildFire becomes less effective unless it is allowed to act on decrypted content. For example, if a user downloads a malicious pdf over SSL, WildFire can only provide analysis if 1) the session is decrypted by the firewall and 2) forwarding of decrypted content is enabled. In today's internet, roughly 70-80% of all user traffic is encrypted. If Wildfire is not configured to analyze encrypted content, the effectiveness of Wildfire is drastically reduced.

Audit:

Navigate to `Device > Setup > Content-ID > Content-ID Settings`.
Verify that `Allow forwarding of decrypted content` is checked.

Remediation:

Navigate to `Device > Setup > Content-ID > Content-ID Settings`.
Set `Allow forwarding of decrypted content` to be checked.
Note that SSL Forward Proxy must be configured for this setting to be effective.

Default Value:

Not Configured

References:

1. "WildFire Fails Forwarding File to Cloud for Encrypted Traffic" - https://live.paloaltonetworks.com/docs/DOC-6845
2. "Wildfire Administrator's Guide 9.0 (English) - Forward Decrypted SSL Traffic for Wildfire Analysis" - https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/submit-files-for-wildfire-analysis/forward-decrypted-ssl-traffic-for-wildfire-analysis.html#
3. "Wildfire Administrator's Guide 9.0 (English) - Wildfire Best Practices" - https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/wildfire-deployment-best-practices/wildfire-best-practices.html#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**10.1 Deploy and Maintain Anti-Malware Software** Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v8	**10.5 Enable Anti-Exploitation Features** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	**8 Malware Defenses** Malware Defenses			
v7	**12.9 Deploy Application Layer Filtering Proxy Server** Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.			●
v7	**12.10 Decrypt Network Traffic at Proxy** Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.			●

5.4 Ensure all WildFire session information settings are enabled (Automated)

Profile Applicability:

- Level 1

Description:

Enable all options under Session Information Settings for WildFire.

Rationale:

Permitting the firewall to send all of this information to WildFire creates more detailed reports, thereby making the process of tracking down potentially infected devices more efficient. This could prevent an infected system from further infecting the environment. Environments with security policies restricting sending this data to the WildFire cloud can instead utilize an on-premises WildFire appliance. In addition, risk can be analyzed in the context of the destination host and user account, either during analysis or during incident response.

Audit:

Navigate to `Device > Setup > WildFire > Session Information Settings`. Verify that every option is enabled.

Remediation:

Navigate to `Device > Setup > WildFire > Session Information Settings`. Set every option to be enabled.

Default Value:

All Session Information Settings are enabled by default. These include:

- Source IP
- Source port
- Destination IP
- Destination port
- Virtual System
- Application
- User
- URL
- File name
- Email sender
- Email recipient
- Email subject

References:

1. "Wildfire Administrator's Guide 9.0 (English)" -
   https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin.html#
2. "Wildfire Administrator's Guide 9.0 (English) - Wildfire Best Practices" -
   /https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/wildfire-deployment-best-practices/wildfire-best-practices.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**10.1 Deploy and Maintain Anti-Malware Software** Deploy and maintain anti-malware software on all enterprise assets.	🟢	🟠	🔵
v7	**6.2 Activate audit logging** Ensure that local logging has been enabled on all systems and networking devices.	🟢	🟠	🔵
v7	**8.6 Centralize Anti-malware Logging** Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.		🟠	🔵

5.5 Ensure alerts are enabled for malicious files detected by WildFire (Automated)

Profile Applicability:

- Level 1

Description:

Configure WildFire to send an alert when a malicious or greyware file is detected. This alert could be sent by whichever means is preferable, including email, SNMP trap, or syslog message.

Alternatively, configure the WildFire cloud to generate alerts for malicious files. The cloud can generate alerts in addition to or instead of the local WildFire implementation. Note that the destination email address of alerts configured in the WildFire cloud portal is tied to the logged in account, and cannot be modified. Also, new systems added to the WildFire cloud portal will not be automatically set to email alerts.

Rationale:

WildFire analyzes files that have already been downloaded and possibly executed. A WildFire verdict of malicious indicates that a computer could already be infected. In addition, because WildFire only analyzes files it has not already seen that were not flagged by the firewall's antivirus filter, files deemed malicious by WildFire are more likely to evade detection by desktop antivirus products.

Audit:

Navigate to `Objects > Log Forwarding`.
Verify that the `WildFire` log type is configured to generate alerts using the desired alerting mechanism(s).

Remediation:

From GUI, configure some combination of the following Server Profiles:
Configure the Email Server:
Select `Device > Server Profiles > Email`
Click `Add`
Enter a name for the Profile.
Select the virtual system from the Location drop down menu (if applicable)
Click `Add`
Configure the Syslog Server:
Select `Device > Server Profiles > Syslog > Add`
Enter `Name, Display Name, Syslog Server, Transport, Port, Format, Facility`
Click `OK`
Click `Commit` to save the configuration
Configure the SMTP Server:
Select `Device > Server Profiles > Email`
Select `Add, Name, Display Name, From, To, Additional Recipients, Gateway IP or Hostname`
Click `OK`
Click `Commit` to save the configuration
Navigate to `Objects, Log Forwarding`
Choose `Add`, set the log type to "wildfire", add the filter "(verdict neq benign)", then add log destinations for SNMP, Syslog, Email or HTTP as required.

Default Value:

Not Configured

References:

1. "WildFire Email Alerts: Subscribe or Add Additional Recipients" - https://live.paloaltonetworks.com/docs/DOC-7740
2. "Wildfire Administrator's Guide 9.0 (English)" - https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.5 <u>Central Log Management</u> Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		🟠	🔵
v7	8 <u>Malware Defenses</u> Malware Defenses			
v7	8.6 <u>Centralize Anti-malware Logging</u> Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.		🟠	🔵

5.6 Ensure 'WildFire Update Schedule' is set to download and install updates in real-time (Automated)

Profile Applicability:

- Level 1

Description:

Set the WildFire update schedule to download and install updates in real-time.

Rationale:

WildFire definitions may contain signatures to block immediate, active threats to the environment. With updates in real-time, the firewall can ensure threats with new definitions are quickly mitigated.

Audit:

Navigate to `Device > Dynamic Updates > WildFire Update Schedule`.
Verify that `Recurrence` is set to `Real-time`.

Remediation:

Navigate to `Device > Dynamic Updates > WildFire Update Schedule`.
Set `Recurrence` is set to `Real-time`.

Default Value:

Not Configured

References:

1. "Wildfire What's New in 10.0 (English)" - https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/wildfire-features-in-panos-100/wildfire-real-time-signature-updates
2. "How to Configure WildFire" - https://live.paloaltonetworks.com/docs/DOC-3252
3. "Tips for Managing Content Updates" - https://live.paloaltonetworks.com/docs/DOC-1578

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**10.2 <u>Configure Automatic Anti-Malware Signature Updates</u>** Configure automatic updates for anti-malware signature files on all enterprise assets.	●	●	●
v7	**3.4 <u>Deploy Automated Operating System Patch Management Tools</u>** Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	**3.5 <u>Deploy Automated Software Patch Management Tools</u>** Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

5.7 Choosing Wildfire public cloud region (Manual)

Profile Applicability:

- Level 2

Description:

By default, all relevant files are uploaded to Wildfire datacenter located in US. Palo Alto Networks has been adding more WildFire regional clouds around the world. From having just 3 regional clouds back in PanOS 8.x, now to more than 10 regional clouds all over the world.

Rationale:

Depending on regulations, files is only allowed to be uploaded to local country / region. Besides, uploading to local country or even nearest country decreases file uploading speed.

Refer to the available regions in the references below.

Impact:

With default values, all relevant files are uploaded to wildfire.paloaltonetworks.com which is located in US.

Audit:

Navigate to `Device > Setup > WildFire`.
Navigate to the `General Settings sections`.
Verify that `WildFire Public Cloud` is set to your appropriate region.

Remediation:

Navigate to `Device > Setup > WildFire`.
Navigate to the `General Settings sections`.
Click the `General Settings` edit icon.
Change the `WildFire Public Cloud` to your appropriate region.

Default Value:

wildfire.paloaltonetworks.com

References:

1. "List of Available Wildfire Regions" - https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/wildfire-deployments/wildfire-global-cloud
2. "Announcements as More Regions are Added" - https://docs.paloaltonetworks.com/wildfire

6 Security Profiles

The Security Profiles section covers requirements for several types of profiles, including antivirus, anti-spyware, Vulnerability Protection Profiles, URL filtering, URL logging, data filtering, and Zone Protection Profiles.

6.1 Ensure that antivirus profiles are set to reset-both on all decoders except 'imap' and 'pop3' (Automated)

Profile Applicability:

- Level 1

Description:

Configure antivirus profiles to a value of 'reset-both' for all decoders except imap and pop3 under both Action and WildFire Action. If required by the organization's email implementation, configure imap and pop3 decoders to 'alert' under both Action and WildFire Action.

Rationale:

Antivirus signatures produce low false positives. By blocking any detected malware through the specified decoders, the threat of malware propagation through the firewall is greatly reduced. It is recommended to mitigate malware found in pop3 and imap through a dedicated antivirus gateway. Due to the nature of the pop3 and imap protocols, the firewall is not able to block only a single email message containing malware. Instead, the entire session would be terminated, potentially affecting benign email messages.

Audit:

Navigate to `Objects > Security Profiles > Antivirus`
Verify that antivirus profiles have all decoders set to `reset-both` for both `Action` and `Wildfire Action`. If `imap` and `pop3` are required in the organization, verify that the `imap` and `pop3` decoders are set to `alert` for both `Action` and `Wildfire Action`.

Remediation:

Navigate to `Objects > Security Profiles > Antivirus`.
Set antivirus profiles to have all decoders set to `reset-both` for both `Action` and `Wildfire Action`. If `imap` and `pop3` are required in the organization, set the `imap` and `pop3` decoders to `alert` for both `Action` and `Wildfire Action`.

Default Value:

Not Configured

References:

1. "Threat Prevention Deployment Tech Note" - https://live.paloaltonetworks.com/docs/DOC-3094
2. "PAN-OS Administrator's Guide 9.0 (English) - Security Profiles" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles.html

3. "KB on reset-server, reset-client or silent drop" -
   https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000
   CITaCAK

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8 Malware Defenses Malware Defenses			

6.2 Ensure a secure antivirus profile is applied to all relevant security policies (Manual)

Profile Applicability:

- Level 1

Description:

Create a secure antivirus profile and apply it to all security policies that could pass HTTP, SMTP, IMAP, POP3, FTP, or SMB traffic. The antivirus profile may be applied to the security policies directly or through a profile group.

Rationale:

By applying a secure antivirus profile to all applicable traffic, the threat of malware propagation through the firewall is greatly reduced. Without an antivirus profile assigned to any potential hostile zone, the first protection in the path against malware is removed, leaving in most cases only the desktop endpoint protection application to detect and remediate any potential malware.

Impact:

Not having an AV Profile on a Security Policy allows signature-based malware to transit the security boundary without blocks or alerts. In most cases this leaves only the Endpoint Security application to block or alert malware.

Audit:

Navigate to `Policies > Security` .
For each policy, navigate to `[Policy Name] > Actions`
Verify there is a secure `Antivirus profile` applied to all security policies passing traffic - regardless of protocol. This can be set by Profiles or by Profile Group.

Remediation:

Navigate to `Policies > Security` .
For each policy, navigate to `[Policy Name] > Actions`
Set an `Antivirus profile` or a `Profile Group` containing an AV profile for each security policy passing traffic - regardless of protocol.

Default Value:

No Antivirus Profiles are enabled on any default or new Security Policy

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Security Policies " - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-policy.html
2. "PAN-OS Administrator's Guide 9.0 (English) - Security Profiles" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8 Malware Defenses Malware Defenses			

6.3 Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats (Automated)

Profile Applicability:

- Level 1

Description:

If a single rule exists within the anti-spyware profile, configure it to block on any spyware severity level, any category, and any threat. If multiple rules exist within the anti-spyware profile, ensure all spyware categories, threats, and severity levels are set to be blocked. Additional rules may exist for packet capture or exclusion purposes.

Rationale:

Requiring a blocking policy for all spyware threats, categories, and severities reduces the risk of spyware traffic from successfully exiting the organization. Without an anti-spyware profile assigned to any potential hostile zone, the first protection in the path against malware is removed, leaving in most cases only the desktop endpoint protection application to detect and remediate any potential spyware.

Audit:

Navigate to `Objects > Security Profiles > Anti-Spyware`.
Verify a rule exists within the anti-spyware profile that is configured to perform the `reset-both` on any `Severity` level, any `Category`, and any `Threat Name`.

Remediation:

Navigate to `Objects > Security Profiles > Anti-Spyware`.
Set a rule within the anti-spyware profile that is configured to perform the `reset-both` on any `Severity` level, any `Category`, and any `Threat Name`.

Default Value:

Two Anti-Spyware Security Profiles are configured by default "strict" and "default".

References:

1. "PAN OS Administrator's Guide 11.0 (English) - Anti-Spyware Profile" - https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/objects/objects-security-profiles-anti-spyware-profile

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**10.1 <u>Deploy and Maintain Anti-Malware Software</u>** Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	**8 <u>Malware Defenses</u>** Malware Defenses			

6.4 Ensure DNS sinkholing is configured on all anti-spyware profiles in use (Automated)

Profile Applicability:

- Level 1

Description:

Configure DNS sinkholing for all anti-spyware profiles in use. All internal requests to the selected sinkhole IP address must traverse the firewall. Any device attempting to communicate with the DNS sinkhole IP address should be considered infected.

Rationale:

DNS sinkholing helps to identify infected clients by spoofing DNS responses for malware domain queries. Without sinkholing, the DNS server itself may be seen as infected, while the truly infected device remains unidentified. In addition, sinkholing also ensures that DNS queries that might be indicators of compromise do not transit the internet, where they could be potentially used to negatively impact the "ip reputation" of the organization's internet network subnets.

Audit:

Navigate to `Objects > Security Profiles > Anti-Spyware`.
Within each anti-spyware profile, under its `DNS Policies` tab, verify the `Signature Source` List:
`default-paloalto-dns` should have as its `Policy Action` set to `sinkhole`
If licensed, the `DNS Security` should have as its `Policy Action` set to `sinkhole`
Verify the '`Sinkhole IPv4`' IP address is correct. This should be set to `sinkhole.paloaltnetworks.com`, or if an internal host is set then that host IP or FQDN should be in that field
Verify the '`Sinkhole IPv6`' IP address is correct. This should be set to `IPv6 Loopback IP (::1)`, or if an internal DNS Sinkhole host is set then that host IP or FQDN should be in that field
Navigate to `Policies > Security Policies`
For each outbound security Policy, in the `Actions` tab, verify that the `Anti-Spyware` setting includes the Spyware Profile created, either explicitly or as a `Group Profile`
To verify correct operation of DNS Security, from an internal station make a DNS request to each of the following hosts:

- `test-malware.testpanw.com` to test `Malware` DNS Signature checks
- `test-c2.testpanw.com` to test `C2` DNS Signature checks

- `test-dga.testpanw.com` to test `DGA` (Domain Generation Algorithm) DNS attack checks
- `test-dnstun.testpanw.com` to test `DNS Tunneling` attack checks

  Each of these DNS requests should be redirected to the configured DNS Sinkhole server IP address

  Each of these DNS requests should appear in the firewall logs, under `Monitor > Logs > Threat`. If configured, each of these requests should generate an alert in the organization's SIEM.

Remediation:

Navigate to `Objects > Security Profiles > Anti-Spyware`.
Within each anti-spyware profile, under its `DNS Policies` tab, set the `Signature Source List`:
`default-paloalto-dns` should have as its `Policy Action` set to `sinkhole`
If licensed, the `DNS Security` should have as its `Policy Action` set to `sinkhole`
Verify the '`Sinkhole IPv4`' IP address is correct. This should be set to `sinkhole.paloaltnetworks.com`, or if an internal host is set then that host IP or FQDN should be in that field
Verify the '`Sinkhole IPv6`' IP address is correct. This should be set to `IPv6 Loopback IP (::1)`, or if an internal DNS Sinkhole host is set then that host IP or FQDN should be in that field
Navigate to `Policies > Security Policies`
For each outbound security Policy, in the `Actions` tab, set the `Anti-Spyware` setting to include the Spyware Profile created, either explicitly or as a `Group Profile`

Default Value:

Not Configured

References:

1. "How to Deal with Conficker using DNS Sinkhole" - https://live.paloaltonetworks.com/docs/DOC-6628
2. "Threat Prevention Deployment Tech Note" - https://live.paloaltonetworks.com/docs/DOC-3094
3. "PAN OS Administrator's Guide 11.0 (English) - Anti-Spyware Profile" - https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/objects/objects-security-profiles-anti-spyware-profile

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.7 <u>Use Behavior-Based Anti-Malware Software</u> Use behavior-based anti-malware software.		🟠	🔵
v7	8 <u>Malware Defenses</u> Malware Defenses			
v7	8.7 <u>Enable DNS Query Logging</u> Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.		🟠	🔵

6.5 Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the Internet (Automated)

Profile Applicability:

- Level 1

Description:

Create one or more anti-spyware profiles and collectively apply them to all security policies permitting traffic to the Internet. The anti-spyware profiles may be applied to the security policies directly or through a profile group.

Rationale:

By applying secure anti-spyware profiles to all applicable traffic, the threat of sensitive data exfiltration or command-and-control traffic successfully passing through the firewall is greatly reduced. Anti-spyware profiles are not restricted to particular protocols like antivirus profiles, so anti-spyware profiles should be applied to all security policies permitting traffic to the Internet. Assigning an anti-spyware profile to each trusted zone will quickly and easily identify trusted hosts that have been infected with spyware, by identifying the infection from their outbound network traffic. In addition, that outbound network traffic will be blocked by the profile.

Audit:

Navigate to `Objects > Security Profiles > Anti-Spyware`.
Also navigate to `Policies > Security`.
Verify there are one or more anti-spyware profiles that collectively apply to all inside to outside traffic from any address to any address and any application and service.

Remediation:

Navigate to `Objects > Security Profiles > Anti-Spyware`.
Also navigate to `Policies > Security`.
Set one or more anti-spyware profiles to collectively apply to all inside to outside traffic from any address to any address and any application and service.

Default Value:

Not Configured

References:

1. "Threat Prevention Deployment Tech Note" - https://live.paloaltonetworks.com/docs/DOC-3094
2. "PAN-OS Administrator's Guide 9.0 (English) - Security Profiles" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**10.1 Deploy and Maintain Anti-Malware Software** Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	**8 Malware Defenses** Malware Defenses			

6.6 Ensure a Vulnerability Protection Profile is set to block attacks against critical and high vulnerabilities, and set to default on medium, low, and informational vulnerabilities (Automated)

Profile Applicability:

- Level 1

Description:

Configure a Vulnerability Protection Profile set to block attacks against any critical or high vulnerabilities, at minimum, and set to default on any medium, low, or informational vulnerabilities. Configuring an alert action for low and informational, instead of default, will produce additional information at the expense of greater log utilization.

Rationale:

A Vulnerability Protection Profile helps to protect assets by alerting on, or blocking, network attacks. The default action for attacks against many critical and high vulnerabilities is to only alert on the attack - not to block.

Impact:

Not configuring a Vulnerability Protection Profile means that network attacks will not be logged, alerted on or blocked.

Audit:

Navigate to `Objects > Security Profiles > Vulnerability Protection`.
Verify a Vulnerability Protection Profile is set to block attacks against any critical or high vulnerabilities (minimum), and set to default on attacks against any medium, low, or informational vulnerabilities.

Remediation:

Navigate to `Objects > Security Profiles > Vulnerability Protection`.
Set a Vulnerability Protection Profile to block attacks against any critical or high vulnerabilities (minimum), and to default on attacks against any medium, low, or informational vulnerabilities.

Default Value:

Two Vulnerability Protection Profiles are configured by default - "strict" and "default".

References:

1. "Threat Prevention Deployment Tech Note" -
   https://live.paloaltonetworks.com/docs/DOC-3094

2. "PAN-OS Administrator's Guide 9.0 (English) - Security Profiles" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v7	**12.7 Deploy Network-Based Intrusion Prevention Systems** Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.			●

6.7 Ensure a secure Vulnerability Protection Profile is applied to all security rules allowing traffic (Automated)

Profile Applicability:

- Level 1

Description:

For any security rule allowing traffic, apply a securely configured Vulnerability Protection Profile. Careful analysis of the target environment should be performed before implementing this configuration, as outlined by PAN's "Threat Prevention Deployment Tech Note" in the references section.

Rationale:

A Vulnerability Protection Profile helps to protect assets by alerting on, or blocking network attacks. By applying a secure Vulnerability Protection Profile to all security rules permitting traffic, all network traffic traversing the firewall will be inspected for attacks. This protects both organizational assets from attack and organizational reputation from damage.

Note that encrypted sessions do not allow for complete inspection.

Impact:

Not configuring a Vulnerability Protection Profile means that network attacks will not be logged, alerted on or blocked.

Audit:

Navigate to `Policies > Security`.
For each Policy, under the `Actions` tab, select `Vulnerability Protection`.
Verify either the 'Strict' or the 'Default' profile is selected, or a custom profile that complies with the organization's policies, legal and regulatory requirements.

Remediation:

Navigate to `Policies > Security`.
For each Policy, under the `Actions` tab, select `Vulnerability Protection`.
Set it to use either the 'Strict' or the 'Default' profile, or a custom profile that complies with the organization's policies, legal and regulatory requirements.

Default Value:

Not Configured

References:

1. "Threat Prevention Deployment Tech Note" -
   https://live.paloaltonetworks.com/docs/DOC-3094
2. "PAN-OS Administrator's Guide 9.0 (English) - Security Policies" -
   https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-policy.html
3. "PAN-OS Administrator's Guide 9.0 (English) - Security Profiles" -
   https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v7	**8 Malware Defenses** Malware Defenses			
v7	**12.6 Deploy Network-based IDS Sensor** Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.		●	●

6.8 Ensure that PAN-DB URL Filtering is used (Automated)

Profile Applicability:

- Level 1

Description:

Configure the device to use PAN-DB URL Filtering instead of BrightCloud.

Rationale:

Standard URL filtering provides protection against inappropriate and malicious URLs and IP addresses. PAN-DB URL Filtering is slightly less granular than the BrightCloud URL filtering. However, the PAN-DB Filter offers additional malware protection and PAN threat intelligence by using the Wildfire service as an additional input, which is currently not available in the BrightCloud URL Filtering license. This makes the PAN-DB filter more responsive to specific malware "campaigns".

Impact:

Not having an effective URL Filtering configuration can leave an organization open to legal action, internal HR issues, non-compliance with regulatory policies or productivity loss.

Audit:

Navigate to `Device > Licenses`.
Click on `PAN-DB URL Filtering`.
Verify `Active` is set to `Yes`.

Remediation:

Navigate to `Device > Licenses`.
Click on `PAN-DB URL Filtering`.
Set `Active` to `Yes`.

Default Value:

Not Configured

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - URL Filtering" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/url-filtering.html
2. "PAN-OS Administrator's Guide 9.0 (English) - URL Filtering Best Practices": https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/url-filtering/url-filtering-best-practices.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**9.3 Maintain and Enforce Network-Based URL Filters** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
v7	**7.4 Maintain and Enforce Network-Based URL Filters** Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.		●	●
v7	**7.5 Subscribe to URL-Categorization service** Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.		●	●

6.9 Ensure that URL Filtering uses the action of "block" or "override" on the URL categories (Automated)

Profile Applicability:

- Level 1

Description:

Ideally, deciding which URL categories to block, and which to allow, is a joint effort between IT and another entity of authority within an organization—such as the legal department or administration. For most organizations, blocking or requiring an override on the following categories represents a minimum baseline: adult, hacking, command-and-control, copyright-infringement, extremism, malware, phishing, proxy-avoidance-and-anonymizers, and parked. Some organizations may add "unknown" and "dynamic-dns" to this list, at the expense of some support calls on those topics.

Rationale:

Certain URL categories pose a technology-centric threat, such as command-and-control, copyright-infringement, extremism, malware, phishing, proxy-avoidance-and-anonymizers, and parked. Users visiting websites in these categories, many times unintentionally, are at greater risk of compromising the security of their system. Other categories, such as adult, may pose a legal liability and will be blocked for those reasons.

Impact:

Not having an effective URL Filtering configuration can leave an organization open to legal action, internal HR issues, non-compliance with regulatory policies or productivity loss.

Audit:

Navigate to `Objects > Security Profiles > URL Filtering`.
Verify that all URL categories designated by the organization are listed, and the action is set to `Block`.

Remediation:

Navigate to `Objects > Security Profiles > URL Filtering`.
Set a URL filter so that all URL categories designated by the organization are listed. Navigate to the `Actions` tab.

Set the action to `Block`.

Default Value:

Not Configured

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Security Profiles" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles.html
2. "PAN-OS Administrator's Guide 9.0 (English) - URL Filtering" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/url-filtering.html
3. "PAN-OS Admin Guide 9.0 (English) - URL Filtering Best Practices": https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/url-filtering/url-filtering-best-practices.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.		●	●
v7	7.5 Subscribe to URL-Categorization service Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.		●	●

6.10 Ensure that access to every URL is logged (Automated)

Profile Applicability:

- Level 1

Description:

URL filters should not specify any categories as `Allow Categories`.

Rationale:

Setting a URL filter to have one or more entries under Allow Categories will cause no log entries to be produced in the URL Filtering logs for access to URLs in those categories. For forensic, legal, and HR purposes, it is advisable to log access to every URL. In many cases failure to log all URL access is a violation of corporate policy, legal requirements or regulatory requirements.

Impact:

Not having an effective URL Filtering configuration can leave an organization open to legal action, internal HR issues, non-compliance with regulatory policies or productivity loss.

Audit:

Navigate to `Objects > Security Profiles > URL Filtering`.
Verify that the for all allowed categories, that the `Site Access` action is set to `alert`

Remediation:

Navigate to `Objects > Security Profiles > URL Filtering`.
For each permitted category, set the `Site Access` action to `alert`

Default Value:

A default URL Filtering Security Profile is configured, with the following categories set to "block": abused-drugs adult gambling hacking malware phishing questionable weapons 3 Categories are set to `alert` in the default policy, and 58 Categories are set to `allow` (which means they are not logged)

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - URL Filtering Best Practices": https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/url-filtering/url-filtering-best-practices.html
2. "PAN-OS Administrator's Guide 9.0 (English) - URL Filtering" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/url-filtering.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.5 Collect Detailed Audit Logs** Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		🟠	🔵
v8	**9.3 Maintain and Enforce Network-Based URL Filters** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		🟠	🔵
v7	**6.2 Activate audit logging** Ensure that local logging has been enabled on all systems and networking devices.	🟢	🟠	🔵
v7	**6.3 Enable Detailed Logging** Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		🟠	🔵
v7	**7.6 Log all URL requests** Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.		🟠	🔵

6.11 Ensure all HTTP Header Logging options are enabled (Automated)

Profile Applicability:

- Level 1

Description:

Enable all options (User-Agent, Referrer, and X-Forwarded-For) for HTTP header logging.

Rationale:

Logging HTTP header information provides additional information in the URL logs, which may be useful during forensic investigations. The User-Agent option logs which browser was used during the web session, which could provide insight to the vector used for malware retrieval. The Referrer option logs the source webpage responsible for referring the user to the logged webpage. The X-Forwarded-For option is useful for preserving the user's source IP address, such as if a user traverses a proxy server prior to the firewall. Un-checking the Log container page only box produces substantially more information about web activity, with the expense of producing far more entries in the URL logs. If this option remains checked, a URL filter log entry showing details of a malicious file download may not exist.

Impact:

Not having an effective URL Filtering configuration can leave an organization open to legal action, internal HR issues, non-compliance with regulatory policies or productivity loss.

Audit:

Navigate to `Objects > Security Profiles > URL Filtering > URL Filtering Profile > URL Filtering Settings`.
Verify these four settings:
a. `Log container page only` box is un-checked
b. `User-Agent` box is checked
c. `Referrer` box is checked
d. `X-Forwarded-For` box is checked

Remediation:

Navigate to `Objects > Security Profiles > URL Filtering > URL Filtering Profile > URL Filtering Settings`.
Set the following four settings:
a. `Log container page only` box is un-checked
b. Check the `User-Agent` box
c. Check the `Referrer` box
d. Check the `X-Forwarded-For` box

Default Value:

Not Configured

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - URL Filtering Best Practices":
   https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/url-filtering/url-filtering-best-practices.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.5 Collect Detailed Audit Logs** Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v8	**9.3 Maintain and Enforce Network-Based URL Filters** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
v7	**6.2 Activate audit logging** Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	**6.3 Enable Detailed Logging** Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	**7.6 Log all URL requests** Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.		●	●

6.12 Ensure secure URL filtering is enabled for all security policies allowing traffic to the Internet (Automated)

Profile Applicability:

- Level 1

Description:

Apply a secure URL filtering profile to all security policies permitting traffic to the Internet. The URL Filtering profile may be applied to the security policies directly or through a profile group.

Rationale:

URL Filtering policies dramatically reduce the risk of users visiting malicious or inappropriate websites. In addition, a complete URL history log for all devices is invaluable when performing forensic analysis in the event of a security incident. Applying complete and approved URL filtering to outbound traffic is a frequent requirement in corporate policies, legal requirements or regulatory requirements.

Impact:

Not having an effective URL Filtering configuration can leave an organization open to legal action, internal HR issues, non-compliance with regulatory policies or productivity loss.

Audit:

To Verify URL Filtering:
For each Security Policy that transits traffic to the public internet, navigate to `Policies > Security > Security Profiles > [Policy Name] > Actions`.
Verify there is a URL Filtering profile that complies with the policies of the organization is applied to all Security Policies that transit traffic to the public internet.

Remediation:

To Set URL Filtering:
For each Security Profile that transits traffic to the internet, navigate to `Policies > Security > Security Profiles > [Policy Name] > Actions`.
Set a URL Filtering profile that complies with the policies of the organization is applied to all Security Policies that transit traffic to the public internet.

Default Value:

Not Configured

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - URL Filtering Best Practices":
   https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/url-filtering/url-filtering-best-practices.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**9.3 Maintain and Enforce Network-Based URL Filters** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
v7	**7.4 Maintain and Enforce Network-Based URL Filters** Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.		●	●
v7	**7.5 Subscribe to URL-Categorization service** Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.		●	●

6.13 Ensure alerting after a threshold of credit card or Social Security numbers is detected is enabled (Automated)

Profile Applicability:

- Level 1

Description:

This guideline is highly specific to an organization. While blocking of credit card or Social Security numbers will not occur with the recommended settings below, careful tuning is also recommended.

Rationale:

Credit card and Social Security numbers are sensitive, and should never traverse an organization's Internet connection in clear text. Passing sensitive data within an organization should also be avoided whenever possible. Detecting and blocking known sensitive information is a basic protection against a data breach or data loss. Not implementing these defenses can lead to loss of regulatory accreditation (such as PCI, HIPAA etc.), or can lead to legal action from injured parties or regulatory bodies.

Audit:

Navigate to `Objects > Custom Objects > Data Patterns`.
Verify an appropriate `Data Pattern` has been created that accounts for sensitive information within your organization. In most cases this will include Credit Card Numbers, and your jurisdiction's equivalent of Social Insurance Numbers. In many cases these can simply be picked from the list of `Predefined Patterns`.
Navigate to `Objects > Security Profiles > Data Filtering`.
Verify an appropriate `Data Filtering Profile` has been created, using the created `Data Patterns`. Ensure that an `Alert Threshold` is set that generates alerts appropriately. A typical starting value for `Alert Threshold` is `20`, but this should be adjusted after appropriate testing.

Remediation:

Navigate to `Objects > Custom Objects > Data Patterns`.
Create an appropriate `Data Pattern` that accounts for sensitive information within your organization. In most cases this will include Credit Card Numbers, and your jurisdiction's equivalent of Social Insurance Numbers. In many cases these can simply be picked from the list of `Predefined Patterns`.
Navigate to `Objects > Security Profiles > Data Filtering`.
Create appropriate `Data Filtering Profile`, using the created `Data Patterns`. Ensure that an `Alert Threshold` is set that generates alerts appropriately. A typical starting value for `Alert Threshold` is `20`, but this should be adjusted after appropriate testing.

Default Value:

Not Configured

References:

1. "What are the Data Filtering Best Practices?" - https://live.paloaltonetworks.com/docs/DOC-2513
2. "PAN-OS Administrator's Guide 9.0 (English) - Setting up Data Filtering" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/set-up-data-filtering.html#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure** Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	**8.5 Collect Detailed Audit Logs** Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	**6.2 Activate audit logging** Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	**6.3 Enable Detailed Logging** Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	**13.3 Monitor and Block Unauthorized Network Traffic** Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●
v6	**6.5 Ensure Network Boundary Devices Log Verbosely** Configure network boundary devices, including firewalls, network-based IPS, and inbound and outbound proxies, to verbosely log all traffic (both allowed and blocked) arriving at the device.			

6.14 Ensure a secure Data Filtering profile is applied to all security policies allowing traffic to or from the Internet (Automated)

Profile Applicability:

- Level 1

Description:

Create a secure Data Filtering profile and apply it to all security policies permitting traffic to or from the Internet. The Data Filtering profile may be applied to security policies directly or through a profile group.

Rationale:

A Data Filtering profile helps prevent certain types of sensitive information from traversing an organization's Internet connection, especially in clear text. Detecting and blocking known sensitive information is a basic protection against a data breach or data loss. Not implementing these defenses can lead to loss of regulatory accreditation (such as PCI, HIPAA etc.), or can lead to legal action from injured parties or regulatory bodies.

Before starting, be very aware that Data Filtering will often block data that you didn't anticipate, false positives will definitely occur. Even the prebuilt filters will frequently match on unintended data in files or websites. Work very closely with your user community to ensure that required data is blocked or alerted on, but a minimum of false positive blocks occur. As false positives occur, ensure that your user community has a clear and timely procedure to get the configuration updated.

Audit:

Navigate to `Objects > Custom Objects > Data Patterns`. Verify that the patterns defined match the various data that you wish to monitor or make blocking decisions on.
Navigate to `Objects > Security Profiles > Data Filtering`
For each `Filtering Profile`, verify that the `Data Patterns` defined matches the data you wish to monitor, with appropriate values for `Alert Threshold` (typically 20), `Block Threshold` (typically 0) and `Log Severity`.
Finally, navigate to `Policies > Security`. Open all appropriate policies, for each Policy choose the `Actions` tab, and verify that the appropriate `Data Filtering Policy` is applied (either as an individual `Profile` or as part of a `Group Profile`)

Remediation:

Navigate to `Objects > Custom Objects > Data Patterns`. Add patterns to match the various data that you wish to monitor or make blocking decisions on.
Navigate to `Objects > Security Profiles > Data Filtering`
Add a `Filtering Profile` that matches the data you wish to monitor, with appropriate values for `Alert Threshold` (typically 20), `Block Threshold` (typically 0) and `Log Severity`
Finally, apply the Filtering Profile to a Security Profile.
Navigate to `Policies > Security`. Edit all appropriate policies, and for each Policy choose the `Actions` tab, and add the appropriate `Data Filtering Policy` (either as an individual `Profile` or as part of a `Group Profile`)

Default Value:

Not Configured

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Setting up Data Filtering" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/set-up-data-filtering.html#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	13.3 Monitor and Block Unauthorized Network Traffic Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

6.15 Ensure that a Zone Protection Profile with an enabled SYN Flood Action of SYN Cookies is attached to all untrusted zones (Automated)

Profile Applicability:

- Level 1

Description:

Enable the SYN Flood Action of SYN Cookies for all untrusted zones. The Alert, Activate, and Maximum settings for SYN Flood Protection depend highly on the environment and device used. Perform traffic analysis on the specific environment and firewall to determine accurate thresholds. Do not rely on default values to be appropriate for an environment.

Setting these values for all interfaces is an approach that should be considered by many organizations, as traffic floods can result from internal testing or malware as well.

As a rough ballpark for most environments, an Activate value of 50% of the firewall's maximum "New sessions per second"/CPS is a conservative setting. The following is a list of maximum new sessions per second for each platform:

PA-4xx series = 73,000 CPS

PA-8xx series = 13,100 CPS

PA-14xx series = 140,000 CPS

PA-32xx series = 84,000 CPS

PA-34xx series = 268,000 CPS

PA-52xx series = 500,000 CPS

PA-54xx series = 3,600,000 CPS

PA-70xx series = 6,000,000 CPS

Rationale:

Protecting resources and the firewall itself against DoS/DDoS attacks requires a layered approach. Firewalls alone cannot mitigate all DoS attacks, however, many attacks can be successfully mitigated. Utilizing SYN Cookies helps to mitigate SYN flood attacks, where the CPU and/or memory buffers of the victim device become overwhelmed by incomplete TCP sessions. SYN Cookies are preferred over Random Early Drop.

Impact:

Not configuring a Network Zone Protection Profile on untrusted interfaces leaves an organization exposed to common attacks and reconnaissance from those untrusted networks. Not configuring a Zone Protection Profile for internal networks leaves an organization vulnerable to malware, software or hardware causes of traffic flooding from internal sources.

Audit:

From GUI:
Navigate to `Network > Network Profiles > Zone Protection > Zone Protection Profile > Flood Protection` tab.
Verify the SYN box is `checked`. Verify the Action dropdown is `SYN Cookies`. Verify Alert is `20000` (or appropriate for org). Verify Activate is `25000` (50% of maximum for firewall model). Verify Maximum is `1000000` (or appropriate for org).
Navigate to `Network > Zones`. Open the zone facing any untrusted network. Verify that `Zone Protection` has the `Zone Protection Profile` set to the Profile created.

Remediation:

From GUI:
Navigate to `Network > Network Profiles > Zone Protection > Zone Protection Profile > Flood Protection` tab.
Check the SYN box. Set the Action dropdown to `SYN Cookies` Set Alert to `20000` (or appropriate for org). Set Activate to `25000` (50% of maximum for firewall model). Set Maximum to `1000000` (or appropriate for org)
Navigate to `Network > Zones`. Open the zone facing any untrusted network, if one does not exist create it. Set `Zone Protection` to the `Zone Protection Profile` created.

Default Value:

Not Configured

References:

1. "Understanding DoS Protection" - https://live.paloaltonetworks.com/docs/DOC-5078
2. "Syn Cookie Operation" - https://live.paloaltonetworks.com/docs/DOC-1542
3. "How to Determine if Configured DoS Classify TCP SYN Cookie Alarm, Activate and Maximal Rate is Triggered" - https://live.paloaltonetworks.com/docs/DOC-6801
4. "Threat Prevention Deployment Tech Note" - https://live.paloaltonetworks.com/docs/DOC-3094
5. "What are the Differences between DoS Protection and Zone Protection?" - https://live.paloaltonetworks.com/docs/DOC-4501
6. "Application DDoS Mitigation" - https://live.paloaltonetworks.com/docs/DOC-7158

7. PANOS 9.0 Admin Guide - Zone Protection . Flood Protection:
   https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-
   help/network/network-network-profiles/network-network-profiles-zone-
   protection/flood-protection.html#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 <u>Define and Maintain Role-Based Access Control</u> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	13.3 <u>Monitor and Block Unauthorized Network Traffic</u> Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

6.16 Ensure that a Zone Protection Profile with tuned Flood Protection settings enabled for all flood types is attached to all untrusted zones (Automated)

Profile Applicability:

- Level 2

Description:

Enable all Flood Protection options in the Zone Protection Profile attached to all untrusted zones. The Alert, Activate, and Maximum settings for Flood Protection depend highly on the environment and device used. Perform traffic analysis on the specific environment and firewall to determine accurate thresholds. Do not rely on default values to be appropriate for an environment.

Setting these values for all interfaces is an approach that should be considered by many organizations, as traffic floods can result from internal testing or malware as well.

Rationale:

Without flood protection, it may be possible for an attacker, through the use of a botnet or other means, to overwhelm network resources. Flood protection does not completely eliminate this risk; rather, it provides a layer of protection. Without a properly configured zone protection profile applied to untrusted interfaces, the protected / trusted networks are susceptible to large number of attacks. While many of these involve denial of service, some of these attacks are designed to evade IPS systems (fragmentation attacks for instance) or to evade basic firewall protections (source routing and record route attacks).

Impact:

Not configuring and applying a Network Zone Protection Profile leaves an organization exposed to common attacks and reconnaissance from untrusted networks.

Not configuring a Zone Protection Profile for internal networks leaves an organization vulnerable to malware, software or hardware causes of traffic flooding from internal sources.

Audit:

In the GUI:
Navigate to `Network > Network Profiles > Zone Protection > Flood Protection`. Ensure that all settings are enabled with at least the default values.
Navigate to `Network > Zones`, select each untrusted zone in turn, and ensure that the Zone Protection Profile is set.

Remediation:

In the GUI:
Navigate to `Network > Network Profiles > Zone Protection > Flood Protection`.
Set all settings to "enabled" with at least the default values.
Navigate to `Network > Zones`, select each untrusted zone in turn, and set the Zone Protection Profile.

Default Value:

Not Configured

References:

1. "Understanding DoS Protection" - https://live.paloaltonetworks.com/docs/DOC-5078
2. "Threat Prevention Deployment Tech Note" - https://live.paloaltonetworks.com/docs/DOC-3094
3. "What are the Differences between DoS Protection and Zone Protection?" - https://live.paloaltonetworks.com/docs/DOC-4501
4. PANOS 9.0 Admin Guide - Network Profiles / Zone Protection / Flood Protection : https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-zone-protection/flood-protection.html#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	13.3 Monitor and Block Unauthorized Network Traffic Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

6.17 Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned, and set to appropriate actions (Automated)

Profile Applicability:

- Level 1

Description:

Enable all three scan options in a Zone Protection profile. Do not configure an action of Allow for any scan type. The exact interval and threshold values must be tuned to the specific environment. Less aggressive settings are typically appropriate for trusted zones, such as setting an action of alert for all scan types.

Attach appropriate Zone Protection profiles meeting these criteria to all zones. Separate Zone Protection profiles for trusted and untrusted zones is a best practice.

Rationale:

Port scans and host sweeps are common in the reconnaissance phase of an attack. Bots scouring the Internet in search of a vulnerable target may also scan for open ports and available hosts. Reconnaissance Protection will allow for these attacks to be either alerted on or blocked altogether.

Impact:

Not configuring a Network Zone Protection Profile leaves an organization exposed to common attacks and reconnaissance from untrusted networks.

Audit:

Navigate to `Network > Network Profiles > Zone Protection > Zone Protection Profile > Reconnaissance Protection`.
Verify that `TCP Port Scan` is `enabled`, its Action is set to `block-ip`, its Interval is set to `5`, and its Threshold is set to `20`. For `block-ip`, ensure the "Track By" is set to `source` and "Duration" is set to `600` seconds.
Verify that `Host Sweep` is `enabled`, its Action is set to `block`, its Interval is set to `10`, and its Threshold is set to `30`.
Verify that `UDP Port Scan` is `enabled`, its Action is set to `alert`, its Interval is set to `10`, and its Threshold is set to `20`.

Remediation:

Navigate to `Network > Network Profiles > Zone Protection > Zone Protection Profile > Reconnaissance Protection`.
Set `TCP Port Scan` to `enabled`, its Action to `block-ip`, its Interval to `5`, and its Threshold to `20`. For `block-ip`, set the "Track By" is set to `source` and "Duration" is set to `600` seconds.
Set `Host Sweep` to `enabled`, its Action to `block`, its Interval to `10`, and its Threshold to `30`.
Set `UDP Port Scan` to `enabled`, its Action to `alert`, its Interval to `10`, and its Threshold to `20`.

Default Value:

Not Configured

References:

1. "Host Sweep Triggering Method in Zone Protection Profile" - https://live.paloaltonetworks.com/docs/DOC-8703
2. "Understanding DoS Protection" - https://live.paloaltonetworks.com/docs/DOC-5078
3. "Threat Prevention Deployment Tech Note" - https://live.paloaltonetworks.com/docs/DOC-3094
4. "What are the Differences between DoS Protection and Zone Protection?" - https://live.paloaltonetworks.com/docs/DOC-4501
5. PANOS 9.0 Admin Guide - Network Profiles / Zone Protection / Reconnaissance Protection: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-zone-protection/reconnaissance-protection.html#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	12 <u>Boundary Defense</u> Boundary Defense			
v7	12.4 <u>Deny Communication over Unauthorized Ports</u> Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	13.3 Monitor and Block Unauthorized Network Traffic Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

6.18 Ensure all zones have Zone Protection Profiles that drop specially crafted packets (Automated)

Profile Applicability:

- Level 1

Description:

For all zones, attach a Zone Protection Profile that is configured to drop packets with a spoofed IP address or a mismatched overlapping TCP segment, and packets with malformed, strict source routing, or loose source routing IP options set.

Rationale:

Using specially crafted packets, an attacker may attempt to evade or diminish the effectiveness of network security devices. Enabling the options in this recommendation lowers the risk of these attacks.

Impact:

Not configuring a Network Zone Protection Profile leaves an organization exposed to common attacks and reconnaissance from untrusted networks.

Audit:

Navigate to `Network > Network Profiles > Zone Protection > Zone Protection Profile > Packet Based Attack Protection > TCP/IP Drop`.
Verify `Spoofed IP address` is checked.
Verify `Mismatched overlapping TCP segment` is checked.
Under `IP Option Drop`, verify that `Strict Source Routing`, `Loose Source Routing`, and `Malformed` are all checked. Additional options may also be checked.

Remediation:

Navigate to `Network > Network Profiles > Zone Protection > Zone Protection Profile > Packet Based Attack Protection > TCP/IP Drop`.
Set `Spoofed IP address` to be checked.
Set `Mismatched overlapping TCP segment` to be checked.
Under `IP Option Drop`, set `Strict Source Routing`, `Loose Source Routing`, and `Malformed` to all be checked. Additional options may also be set if desired.

Default Value:

Not Configured

References:

1. "Understanding DoS Protection" - https://live.paloaltonetworks.com/docs/DOC-5078
2. "Threat Prevention Deployment Tech Note" - https://live.paloaltonetworks.com/docs/DOC-3094
3. "What are the Differences between DoS Protection and Zone Protection?" - https://live.paloaltonetworks.com/docs/DOC-4501
4. PANOS 9.0 Admin Guide - Network Profiles / Zone Protection / Packet Based Attack Protection: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-zone-protection/packet-based-attack-protection.html#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	12 Boundary Defense Boundary Defense			
v7	13.3 Monitor and Block Unauthorized Network Traffic Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

6.19 Ensure that User Credential Submission uses the action of "block" or "continue" on the URL categories (Automated)

Profile Applicability:

- Level 1

Description:

Ideally user names and passwords user within an organization are not used with third party sites. Some sanctioned SAS applications may have connections to the corporate domain, in which case they will need to be exempt from the user credential submission policy through a custom URL category.

Rationale:

Preventing users from having the ability to submit their corporate credentials to the Internet could stop credential phishing attacks and the potential that a breach at a site where a user reused credentials could lead to a credential stuffing attack.

Impact:

Not preventing users from submitting their corporate credentials to the Internet can leave them open to phishing attacks or allow for credential reuse on unauthorized sites. Using internal email accounts provides malicious actors with intelligence information, which can be used for phishing, credential stuffing and other attacks. Using internal passwords will often provide authenticated access directly to sensitive information. Not only that, but a pattern of credential re-use can expose personal information from multiple online sources.

Audit:

Navigate to `Objects > Security Profiles > URL Filtering`.
Choose the `Categories` tab. Verify that the `User Credential Submitting` action on all enabled URL categories is set to either `block` or `continue`.
Under the `User Credential Detection` tab ensure the `User Credential Detection` is set to a value appropriate to your organization, and is not set to `Disabled`. Verify that the `Log Severity` value is set to a value appropriate to your organization and your logging or SIEM solution.

Remediation:

Navigate to `Objects > Security Profiles > URL Filtering`.
Choose the `Categories` tab. Set the `User Credential Submitting` action on all enabled URL categories is either `block` or `continue`, as appropriate to your organization and the category.
Under the `User Credential Detection` tab set the `User Credential Detection` value to a setting appropriate to your organization, any value except `Disabled`. Set the `Log Severity` to a value appropriate to your organization and your logging or SIEM solution.

Default Value:

Not Configured

References:

1. PAN OS 9.0 Admin Guide - URL Filtering / User Credential Detection: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/objects/objects-security-profiles-url-filtering/user-credential-detection.html#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	7 Email and Web Browser Protections Email and Web Browser Protections			

6.20 Ensure that 'Wildfire Inline ML Action' on antivirus profiles are set to reset-both on all decoders except 'imap' and 'pop3' (Manual)

Profile Applicability:

- Level 1

Description:

Configure 'Wildfire Inline ML Action' on antivirus profiles to a value of 'reset-both' for all decoders except imap and pop3 under 'Wildfire Inline ML Action'. If required by the organization's email implementation, configure imap and pop3 decoders to 'alert' under 'Wildfire Inline ML Action'.

Rationale:

Starting from PanOS 10, Wildfire supports real-time detection and blocking. As more attacks are designed to bypass signature-based protection, real-time signatureless-based protection is needed. Antivirus signatures produce low false positives. By blocking any detected malware through the specified decoders, the threat of malware propagation through the firewall is greatly reduced. It is recommended to mitigate malware found in pop3 and imap through a dedicated antivirus gateway. Due to the nature of the pop3 and imap protocols, the firewall is not able to block only a single email message containing malware. Instead, the entire session would be terminated, potentially affecting benign email messages.

Audit:

Navigate to `Objects > Security Profiles > Antivirus`
Verify that antivirus profiles have all decoders set to `reset-both` for `Wildfire Inline ML Action`. If imap and pop3 are required in the organization, verify that the imap and pop3 decoders are set to `alert` for `Wildfire Inline ML Action`.

Remediation:

Navigate to `Objects > Security Profiles > Antivirus`
Set antivirus profiles to have all decoders set to `reset-both` for `Wildfire Inline ML Action`. If imap and pop3 are required in the organization, set the imap and pop3 decoders are set to `alert` for `Wildfire Inline ML Action`.

Default Value:

Not Configured

References:

1. "PAN-OS Administrator's Guide 10.2 (English) - Security Profiles" - https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/threat-prevention/wildfire-inline-ml/configure-wildfire-inline-ml

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●

6.21 Ensure that 'Wildfire Inline ML' on antivirus profiles are set to enable for all file types (Automated)

Profile Applicability:

- Level 1

Description:

Configure 'Wildfire Inline ML' on antivirus profiles to a value of 'enable' for all file types.

Rationale:

Starting from PanOS 10, Wildfire supports real-time detection and blocking. As more attacks are designed to bypass signature-based protection, real-time signatureless-based protection is needed. With this new functionality, common file types used for malware delivery such as Windows Executables, PowerShell Script, MSOffice, Shell, and Executable Linked Format (ELF) can be inspected using Wildfire and malicious files are blocked in real-time.

Audit:

Navigate to `Objects > Security Profiles > Antivirus`
Go to `Wildfire Inline ML` tab. Verify that all `Action Setting` are set to `enable` `(inherit per-protocol actions)`.

Remediation:

Navigate to `Objects > Security Profiles > Antivirus`
Go to `Wildfire Inline ML` tab. Set `enable (inherit per-protocol actions)` for all `Model` on `Action Setting`.

Default Value:

Not Configured

References:

1. "PAN-OS Administrator's Guide 10.2 (English) - Security Profiles" - https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/threat-prevention/wildfire-inline-ml/configure-wildfire-inline-ml

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**10.1 Deploy and Maintain Anti-Malware Software** Deploy and maintain anti-malware software on all enterprise assets.	●	●	●

6.22 Ensure that 'Inline Cloud Analysis' on Vulnerability Protection profiles are enabled if 'Advanced Threat Prevention' is available (Automated)

Profile Applicability:

- Level 1

Description:

Enable 'Inline Cloud Analysis' on Vulnerability Protection profiles to combat zero-day threats.

Rationale:

Starting from PanOS 11, Palo Alto Networks now operates new inline deep learning detection engines in the Advanced Threat Prevention cloud to analyze traffic for command injection and SQL injection vulnerabilities in real-time to protect users against zero-day threats. By operating cloud-based detection engines, you can access a wide array of detection mechanisms that are updated and deployed automatically without requiring the user to download update packages or operate process intensive, firewall-based analyzers which can sap resources.

It is recommended to set the action as 'alert' during initial deployment and monitor it's false positive, configure the exclusion URL and IP before moving to 'reset-both' action.

Audit:

Navigate to `Objects > Security Profiles > Vulnerability Protection`
Go to `Inline Cloud Analysis` tab. Verify that it is enabled and all `Model` action is set as `alert`.

Remediation:

Navigate to `Objects > Security Profiles > Vulnerability Protection`
Go to `Inline Cloud Analysis` tab. Tick the checkbox for `Enable cloud inline analysis`. Verify that all `Model` action is set as `alert`.
Note that, firewall device certificate is used to authenticate to the Advanced Threat Prevention inline cloud analysis service. This step is required before 'Inline Cloud Analysis' can be used. Refer to reference for detailed guide.

Default Value:

Not Configured

References:

1. "Configuring Vulnerability Protection Inline Cloud Analysis Guide (English)" - https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/content-inspection-features/vuln-protection-inline-cloud-analysis

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●

6.23 Ensure that 'Cloud Inline Categorization' on URL Filtering profiles are enabled if 'Advanced Threat Prevention' is available (Automated)

Profile Applicability:

- Level 1

Description:

Enable both 'Local Inline Categorization' and 'Cloud Inline Categorization' on URL Filtering profiles to evaluate suspicious web page contents in real-time to protect users against zero-day threats.

Rationale:

Starting from PanOS 10, Palo Alto Networks Advanced URL Filtering now operates a series of inline cloud-based deep learning detectors that evaluate suspicious web page contents in real-time to protect users against zero-day threats. This includes cloaked websites, multi-step attacks, CAPTCHA challenges, and previously unseen one-time-use URLs.

Audit:

Navigate to `Objects > Security Profiles > URL Filtering`
Go to `Inline Categorization` tab. Verify that it is enabled for both `Enable local inline categorization` and `Enable cloud inline categorization`.

Remediation:

Navigate to `Objects > Security Profiles > URL Filtering`
Go to `Inline Categorization` tab. Tick the checkbox for both `Enable local inline categorization` and `Enable cloud inline categorization`.
Note that:

1. Firewall device certificate is used to authenticate to the Advanced Threat Prevention inline cloud analysis service. This step is required before 'Inline Cloud Analysis' can be used. Refer to reference for detailed guide.
2. 'Local Inline Categorization' can be enabled with just the URL Filtering license (no Advanced Threat Prevention is needed).

Default Value:

Not Configured

References:

1. "Configuring Cloud Inline Categorization for URL Filtering Guide (English)" - https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-new-features/url-filtering-features/cloud-inline-categorization
2. "PAN-OS Administrator's Guide 11.0 (English) - Inline Categorization" - https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/objects/objects-security-profiles-url-filtering/inline-categorization

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**9.3 Maintain and Enforce Network-Based URL Filters** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●

6.24 Ensure that 'Inline Cloud Analysis' on Anti-Spyware profiles are enabled if 'Advanced Threat Prevention' is available (Automated)

Profile Applicability:

- Level 1

Description:

Enable 'Inline Cloud Analysis' on Anti-Spyware profiles to detect and protection against advanced, highly-evasive zero-day command-and-control (C2) threats.

Rationale:

Starting from PanOS 10, Palo Alto Networks now operates a series of ML-based detection engines in the Advanced Threat Prevention cloud to analyze traffic for advanced C2 (command-and-control) and spyware threats in real-time to protect users against zero-day threats. By operating cloud-based detection engines, you can access a wide array of detection mechanisms that are updated and deployed automatically without requiring the user to download update packages or operate process intensive, firewall-based analyzers which can sap resources.

The cloud-based detection engine logic is continuously monitored and updated using C2 traffic datasets from WildFire, with additional support through manual updates by Palo Alto Networks threat researchers, who provide human intervention for highly accurized detection enhancements.

Audit:

Navigate to `Objects > Security Profiles > Anti-Spyware`
Go to `Inline Cloud Analysis` tab. Verify that it is enabled and all `Model` action is set as `reset-both`.

Remediation:

Navigate to `Objects > Security Profiles > Anti-Spyware`
Go to `Inline Cloud Analysis` tab. Tick the checkbox for `Enable cloud inline analysis`. Verify that all `Model` action is set as `reset-both`.
Note that, firewall device certificate is used to authenticate to the Advanced Threat Prevention inline cloud analysis service. This step is required before `Inline Cloud Analysis` can be used. Refer to reference for detailed guide.

Default Value:

Not Configured

References:

1. "Configuring Inline Cloud Analysis Guide (English)" -
   https://docs.paloaltonetworks.com/advanced-threat-
   prevention/administration/configure-threat-prevention/configure-inline-cloud-
   analysis#idcf1fc426-b522-4e84-9098-ac82f2d784ae

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●

6.25 Ensure that 'DNS Policies' is configured on Anti-Spyware profiles if 'DNS Security' license is available (Manual)

Profile Applicability:

- Level 1

Description:

DNS security is an extensible cloud-based service capable of generating DNS signatures using advanced predictive analytics and machine learning. DNS Security protects from sophisticated DNS-based attacks.

Rationale:

DNS traffic are normally allowed on firewall. With this in mind, attackers leverage on this attack surface to evade detections or extract out data. Starting from PanOS 9, Palo Alto Networks has launched DNS Security services to combat against evasive malwares and to detect DNS tunneling activities.

For DNS Security to be effective, "Threat Prevention" or "Advanced Threat Prevention" license must be purchased in addition of "DNS Security" license.

Audit:

Navigate to `Objects > Security Profiles > Anti-Spyware`
Go to `DNS Policies` tab. Verify that policy action is set to `sinkhole` for all DNS Security categories.
On `Command and control Domains` category, verify that the packet capture option to `extended-capture`. Navigate to `Objects > Security Profiles > Anti-Spyware`
Go to `DNS Policies` tab. Configure policy action to `sinkhole` for all DNS Security categories.
On `Command and control Domains` category, set the packet capture option to `extended-capture`

Remediation:

Navigate to `Objects > Security Profiles > Anti-Spyware`
Go to `DNS Policies` tab. Configure policy action to `sinkhole` for all DNS Security categories.
On `Command and control Domains` category, set the packet capture option to `extended-capture`.

Default Value:

Not Configured

References:

1. "PAN-OS Administrator's Guide 11.0 (English) - Configuring DNS Security" - https://docs.paloaltonetworks.com/dns-security/administration/configure-dns-security/enable-dns-security#tabs-id066476b2-c4dd-4fc0-b7e4-f4ba32e19f60
2. "DNS Security Best Practices" - https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/threat-prevention/best-practices-for-securing-your-network-from-layer-4-and-layer-7-evasions

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.6 Collect DNS Query Audit Logs** Collect DNS query audit logs on enterprise assets, where appropriate and supported.		●	●
v8	**10.1 Deploy and Maintain Anti-Malware Software** Deploy and maintain anti-malware software on all enterprise assets.	●	●	●

7 Security Policies

The Security Policies section covers requirements for application and service security policies.

7.1 Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone (Automated)

Profile Applicability:

- Level 1

- Level 2

Description:

When permitting traffic from an untrusted zone, such as the Internet or guest network, to a more trusted zone, such as a DMZ segment, create security policies specifying which specific applications are allowed.

**Enhanced Security Recommendation: ** Require specific application policies when allowing `any` traffic, regardless of the trust level of a zone. Do not rely solely on port permissions. This may require SSL interception, and may also not be possible in all environments.

Rationale:

To avoid unintentionally exposing systems and services, rules allowing traffic from untrusted zones to trusted zones should be as specific as possible. Application-based rules, as opposed to service/port rules, further tighten what traffic is allowed to pass. Similarly, traffic from trusted to untrusted networks should have a security policy set, with application-based rules. A "catch-all" rule that allows all applications will also allow malware traffic. The goal should be to understand both inbound and outbound traffic, permit what is known, and block all other traffic.

Impact:

Setting application based rules on both inbound and outbound traffic ensures that the traffic on the protocol and port being specified is actually the application that you expect. For outbound traffic, the days of "we trust our users" is well past us, that statement also implies that we trust the malware on the user workstations, which is obviously not the case.
For traffic from trusted to less trusted interfaces, the applications should be characterized over time, with the end goal being that all applications in in the rules, and a final "block all" rule is in place. Not having this goal gives both attackers and malware the leeway they need to accomplish their goals.
Trusting only Port permissions to control traffic exposes an organization to "tunneling" style attacks that can exfiltrate data or facilitate Command and Control (C2) sessions.

Audit:

Navigate to `Policies > Security`.
For all Security Policies that transit from a less trusted to a more trusted interface, that the appropriate `Application` and `Service` values are set. For instance, for a web server exposed to the internet from a DMZ:
`Source` tab: `Zone` set to `OUTSIDE` / `Address` set to `Any`
`Destination` tab: `Zone` set to `DMZ` / `Address` set to `[DMZ Host Object]`
`Application` tab: set to `web-browsing`
`Service/URL Category` tab: set `Service` to ether:

-
    `application-default`
    or:
-
    `service-http` and/or `service-https`

**Enhanced Security Recommendation: **
Assess this setting for Policies on all Interfaces, for traffic in all directions. Ensure that for each Security Policy that the appropriate settings are set for both `Application` and `Service`

Remediation:

Navigate to `Policies > Security`.
For all `Security Policies` that transit from a less trusted to a more trusted interface, set the `Application` and `Service` values to match the exposed application. For instance, for a web server exposed to the internet from a DMZ:
`Source` tab: `Zone` set to `OUTSIDE` / `Address` set to `Any`
`Destination` tab: `Zone` set to `DMZ` / `Address` set to `[DMZ Host Object]`
`Application` tab: set to `web-browsing`
`Service/URL Category` tab: set `Service` to ether:

-
    `application-default`
    or:
-
    `service-http` and/or `service-https`

**Enhanced Security Recommendation: **
Set these values for Policies on all Interfaces, for traffic in all directions. For each `Security Policy`, set the `Application` and `Service` values to match the exposed application.

Default Value:

Not Configured

References:

1. "PAN-OS Administrator's Guide 9.0 (English) - Security Policies / Applications and Usage " - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/policies/policies-security/applications-and-usage.html#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	🟢	🟠	🔵
v7	14 Controlled Access Based on the Need to Know Controlled Access Based on the Need to Know			

7.2 Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist (Automated)

Profile Applicability:

- Level 1

Description:

Create security policies specifying application-default for the Service setting, in addition to the specific ports desired. The Service setting of `any` should not be used for any policies that allow traffic.

Rationale:

App-ID requires a number of packets to traverse the firewall before an application can be identified and either allowed or dropped. Due to this behavior, even when an application is defined in a security policy, a service setting of `any` may allow a device in one zone to perform ports scans on IP addresses in a different zone. In addition, this recommendation helps to avoid an App-ID cache pollution attack.

Because of how App-ID works, configuring the service setting to "Any" allows some initial traffic to reach the target host before App-ID can recognize and appropriately restrict the traffic. Setting the Service Setting to application specific at least restricts the traffic to the target applications or protocols for that initial volume of traffic.

Audit:

Navigate to `Policies > Security`.
For each exposed host, verify that a Security Policy exists with:

- `Source` tab: `Zone` set to `OUTSIDE` Address set to `any`

- `Destination` tab: `Zone` set to `DMZ` / `Address` set to `<DMZ Host Object>`

- `Application` tab: `Application` set to `web-browsing` (or appropriate application)

- `Service` tab: `Service` set to `application-default`. The value of `any` should never be used

Remediation:

Navigate to `Policies > Security`.
For each exposed host, set a Security Policy exists with:

- `Source` tab: `Zone` set to `OUTSIDE` Address set to `any`

- Destination **tab:** Zone **set to** DMZ / Address **set to** <DMZ Host Object>
- Application **tab:** Application **set to** web-browsing (or appropriate application)
- Service **tab:** Service **set to** application-default. The value of any should never be used

Default Value:

Not Configured

References:

1. "Security Policy Guidelines" - https://live.paloaltonetworks.com/docs/DOC-3469
2. "Security Bulletin: App-ID Cache Pollution" - http://researchcenter.paloaltonetworks.com/2012/12/app-id-cache-pollution-response/
3. "PAN-OS Administrator's Guide 9.0 (English) - Security Policy Overview " - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/policies/policies-security/security-policy-overview.html#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

7.3 Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists (Automated)

Profile Applicability:

- Level 1

Description:

Create a pair of security rules at the top of the security policies ruleset to block traffic to and from IP addresses known to be malicious.

Note: This recommendation (as written) requires a Palo Alto Networks "Threat Prevention License". Third Party and Open Source Threat Intelligence Feeds can also be used for this purpose.

Rationale:

Creating rules that block traffic to/from known malicious sites from Trusted Threat Intelligence Sources protects you against IP addresses that Palo Alto Networks has proven to be used almost exclusively to distribute malware, initiate command-and-control activity, and launch attacks.

Impact:

While not foolproof, simply blocking traffic from known malicious hosts allows more resources to be devoted to analyzing traffic from other sources for malicious content. This approach is a recommended part of most "Defense in Depth" recommendations, allowing defenders to focus more deeply on traffic from uncategorized sources.

Audit:

Navigate to `Policies > Security`
Verify a Security Policy exists similar to:

- General tab: `Name` set to `Deny to Malicious IP`

- Source tab: `Source Zone` set to `Any,`

- Destination tab: `Destination Zone` set to `Any,` `Destination Address` set to `Palo Alto Networks - Known malicious IP addresses,` `Palo Alto Networks - High risk IP addresses,` `Palo Alto Networks - Tor exit IP addresses,` `Palo Alto Networks - Bulletproof IP addresses`

- Application tab: `Application` set to `Any`

-
    Service/URL Category tab: Service set to Any
-
    Actions tab: Action set to Block, Profile Type set to None

Verify a Security Policy exists similar to:

-
    General tab: Name set to Deny from Malicious IP
-
    Source tab: Source Zone set to Any, Source Address set to Palo Alto Networks - Known malicious IP addresses, Palo Alto Networks - High risk IP addresses, Palo Alto Networks - Tor exit IP addresses, Palo Alto Networks - Bulletproof IP addresses
-
    Destination tab: Destination Zone set to Any
-
    Application tab: Application set to Any
-
    Service/URL Category tab: Service set to Any
-
    Actions tab: Action set to Block, Profile Type set to None

Note: This recommendation requires a Palo Alto Networks "Threat Prevention License"

Remediation:

Navigate to Policies > Security
Create a Security Policy similar to:

-
    General tab: Name set to Deny to Malicious IP
-
    Source tab: Source Zone set to Any,
-
    Destination tab: Destination Zone set to Any, Destination Address set to Palo Alto Networks - Known malicious IP addresses, Palo Alto Networks - High risk IP addresses, Palo Alto Networks - Tor exit IP addresses, Palo Alto Networks - Bulletproof IP addresses
-
    Application tab: Application set to Any
-
    Service/URL Category tab: Service set to Any
-
    Actions tab: Action set to Block, Profile Type set to None

Create a Security Policy similar to:

- General **tab:** Name set to Deny from Malicious IP

- Source **tab:** Source Zone set to Any, Source Address set to Palo Alto Networks - Known malicious IP addresses, Palo Alto Networks - High risk IP addresses, Palo Alto Networks - Tor exit IP addresses, Palo Alto Networks - Bulletproof IP addresses

- Destination **tab:** Destination Zone set to Any

- Application **tab:** Application set to Any

- Service/URL Category **tab:** Service set to Any

- Actions **tab:** Action set to Block, Profile Type set to None

Note: This recommendation requires a Palo Alto Networks "Threat Prevention License"

Default Value:

Not Configured

References:

1. "PAN-OS 11.0 Admin Guide: Built-in External Dynamic Lists": https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/built-in-edls

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	12.3 <u>Deny Communications with Known Malicious IP Addresses</u> Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries,.		●	●

7.4 Ensure that logging is enabled on built-in default security policies (Manual)

Profile Applicability:

- Level 1

Description:

Enable logging on built-in default security policies "intrazone-default" and "interzone-default"

Rationale:

By default, these default security policies does not have logging enabled. This enables SOC or security analyst to do further investigations on security incidents especially on threat hunting or incident response activities.

Audit:

Navigate to `Policies > Security`
Go to default policies `intrazone-default` and `interzone-default`. On `Actions` tab, verify that log setting has `Log at Session End` is enabled.

Remediation:

Navigate to `Policies > Security`
Go to default policies `intrazone-default` and `interzone-default`. On `Actions` tab, enable `Log at Session End` on log setting.

Default Value:

Disabled

References:

1. "Gateway Firewall Best Practices on Default Policies Logging Configuration" - https://docs.paloaltonetworks.com/best-practices/10-2/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/define-the-initial-internet-gateway-security-policy/step-5-enable-logging-for-traffic-that-doesnt-match-any-rules
2. "Datacenter Firewall Best Practices on Default Policies Logging Configuration" - https://docs.paloaltonetworks.com/best-practices/10-2/data-center-best-practices/data-center-best-practice-security-policy/log-and-monitor-data-center-traffic/log-intra-data-center-traffic-that-matches-the-intrazone-allow-rule

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.6 <u>Collect Network Traffic Flow Logs</u> Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		🟠	🔵

8 Decryption

The Decryption section covers requirements for the SSL Forward Proxy policy and the SSL Inbound Inspection policy.

8.1 Ensure 'SSL Forward Proxy Policy' for traffic destined to the Internet is configured (Automated)

Profile Applicability:

- Level 1

Description:

Configure SSL Forward Proxy for all traffic destined to the Internet. In most organizations, including all categories except `financial-services`, `government` and `health-and-medicine` is recommended.

Rationale:

Without SSL inspection, the firewall cannot apply many of its protection features against encrypted traffic. The amount of encrypted malware traffic continues to rise, and legitimate websites using SSL encryption are hacked or tricked into delivering malware on a frequent basis. As encryption on the Internet continues to grow at a rapid rate, SSL inspection is no longer optional as a practical security measure. If proper decryption is not configured, it follows that the majority of traffic is not being fully inspected for malicious content or policy violations. This is a major exposure, allowing delivery of exploits and payloads direct to user desktops.

Impact:

Failure to decrypt outbound traffic allows attackers to mask attacks, data exfiltration and/or command and control (C2) traffic by simply using standard TLS encryption. Privacy concerns for your organization's users will dictate that some common categories should be exempted from inspection and decryption. Personal banking or healthcare information is almost always exempted, as are interactions with government entities. Exemptions and inclusions to decryption policies should be negotiated internally and governed by published Corporate Policies.

Audit:

Navigate to `Policies > Decryption`.
Verify `SSL Forward Proxy` is set for all traffic destined to the Internet.
Verify each Decryption Policy Rule:

- `Source` tab: The `Source Zone` and/or `Source Address` should include all target internal networks. `Source User` should include all target internal users

- `Destination` tab: The `Destination Zone` should include the untrusted target zone (usually the `internet`). `Destination Address` is typically `Any` for an internet destination.

- Service/URL Category tab: Verify that all URL Category entries are included except financial-services, government and health-and-medicine (this list may vary depending on your organization and its policies).
- Options tab: Verify that the Type is set to SSL Forward Proxy

Remediation:

Navigate to Policies > Decryption.
Create a Policy for all traffic destined to the Internet. This Policy should include:

- Source tab: The Source Zone and/or Source Address should include all target internal networks. Source User should include all target internal users
- Destination tab: The Destination Zone should include the untrusted target zone (usually the internet). Destination Address is typically Any for an internet destination.
- Service/URL Category tab: all URL Category entries should be included except financial-services, government and health-and-medicine (this list may vary depending on your organization and its policies).
- Options tab: Type set to SSL Forward Proxy

Default Value:

Not Configured

References:

1. "How to Implement SSL Decryption" - https://live.paloaltonetworks.com/docs/DOC-1412
2. ""PAN-OS Administrator's Guide 9.0 (English) - Decryption (English)" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/decryption.html#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	**12.9** Deploy Application Layer Filtering Proxy Server Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.			●
v7	**12.10** Decrypt Network Traffic at Proxy Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.			●

8.2 Ensure 'SSL Inbound Inspection' is required for all untrusted traffic destined for servers using SSL or TLS (Manual)

Profile Applicability:

- Level 1

Description:

Configure SSL Inbound Inspection for all untrusted traffic destined for servers using SSL or TLS.

Rationale:

Without SSL Inbound Inspection, the firewall is not able to protect SSL or TLS-enabled webservers against many threats.

Impact:

Not decrypting inbound traffic to TLS encrypted services means that inspection for many common attacks cannot occur on the firewall. This means that all defenses against these attacks are up to the host.

Audit:

Navigate to `Policies > Decryption`.
Verify `SSL Inbound Inspection` is set appropriately for all untrusted traffic destined for servers using SSL or TLS.
Navigate to `Policies > Decryption`. For each service published to the internet (or other untrusted zones), verify the following settings:

- `General` tab: `Name` set to a descriptive name

- `Source`: `Source Zone` set to the target zone (Internet in many cases). `Source Address` set to the target address space (`Any` for internet traffic)

- `Destination` tab: `Destination Zone` should be set to the appropriate zone, or `Any`. `Destination Address` set to the target host address

- `Options` tab: Type set to `SSL Inbound Inspection`

Remediation:

Navigate to `Policies > Decryption`.
Set `SSL Inbound Inspection` appropriately for all untrusted traffic destined for servers using SSL or TLS.
Navigate to `Policies > Decryption`. For each service published to the internet (or other untrusted zones), create a Policy and set the following options:

- `General` tab: `Name` set to a descriptive name

- `Source`: `Source Zone` set to the target zone (Internet in many cases). `Source Address` set to the target address space (`Any` for internet traffic)

- `Destination` tab: `Destination Zone` should be set to the appropriate zone, or `Any`. `Destination Address` set to the target host address

- `Options` tab: Type set to `SSL Inbound Inspection`

Default Value:

Not Configured

References:

1. "How to Implement SSL Decryption" - https://live.paloaltonetworks.com/docs/DOC-1412
2. "PAN-OS Administrator's Guide 9.0 (English) - Decryption (English)" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/decryption.html#

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		🟠	🔵
v7	12.9 <u>Deploy Application Layer Filtering Proxy Server</u> Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.			🔵
v7	12.10 <u>Decrypt Network Traffic at Proxy</u> Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.			🔵

8.3 Ensure that the Certificate used for Decryption is Trusted (Automated)

Profile Applicability:

- Level 1

- Level 2

Description:

The CA Certificate used for in-line HTTP Man in the Middle should be trusted by target users. For `SSL Forward Proxy` configurations, there are classes of users that need to be considered.

1: Users that are members of the organization, users of machines under control of the organization. For these people and machines, ensure that the CA Certificate is in one of the Trusted CA certificate stores. This is easily done in Active Directory, using Group Policies for instance. An MDM (Mobile Device Manager) can be used to accomplish the same task for mobile devices such as telephones or tablets. Other central management or orchestration tools can be used for Linux or "IoT" (Internet of Things) devices.

2: Users that are not member of the organization - often these are classed as "Visitors" in the policies of the organization. If a public CA Certificate is a possibility for your organization, then that is one approach. A second approach is to not decrypt affected traffic - this is easily done, but leaves the majority of "visitor" traffic uninspected and potentially carrying malicious content. The final approach, and the one most commonly seen, is to use the same certificate as is used for the hosting organization. In this last case, visitors will see a certificate warning, but the issuing CA will be the organization that they are visiting.

Rationale:

Using a self-signed certificate, or any certificate that generates a warning in the browser, means that members of the organization have no method of determining if they are being presented with a legitimate certificate, or an attacker's "man in the middle' certificate. It also very rapidly teaches members of the organization to bypass all security warnings of this type.

Audit:

Verify the CA Certificate(s):
Navigate to `Device > Certificate Management > Certificates`

- Verify that appropriate internal certificates are imported, and that all certificates in the list are valid. In particular, verify the `Subject`, `Issuer`, `CA`, `Expires`, `Algorithm` and `Usage` fields

- Alternatively, if an internal CA is implemented on the firewall, verify that target clients have the root certificate for this CA imported into their list of trusted certificate authorities.

Verify the Certificate Profile needed for the SSL Forward Proxy:

- Navigate to `Device > Certificate Management > Certificate Profile`. Verify that an appropriate profile is created.

Remediation:

Set the CA Certificate(s):
Navigate to `Device > Certificate Management > Certificates`. Import the appropriate CA Certificates from any internal Certificate Authorities.
Alternatively, generate a self-signed certificate for an internal CA on the firewall, and then import the root certificate for that CA into the trusted CA list of target clients. In an Active Directory environment this can be facilitated using a Group Policy.
Set the Certificate Profile needed for the SSL Forward Proxy:

- Navigate to `Device > Certificate Management > Certificate Profile`.

Set the decryption profile to include the settings described in the `SSL Forward Proxy` guidance in this document

Default Value:

Decryption is not enabled by default.

References:

1. "How to Implement and Test SSL Decryption" - https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Implement-and-Test-SSL-Decryption/ta-p/59719
2. "PAN-OS Administrator's Guide 9.0 (English) - Decryption (English)" - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/decryption.html#
3. "SSL Certificates Resource List on Configuring and Troubleshooting" - https://live.paloaltonetworks.com/t5/Management-Articles/SSL-certificates-resource-list/ta-p/53068
4. "Certificates" - http://palo-alto.wikia.com/wiki/Certificates

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	12.9 <u>Deploy Application Layer Filtering Proxy Server</u> Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.			●
v7	12.10 <u>Decrypt Network Traffic at Proxy</u> Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.			●

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Device Setup**		
1.1	**General Settings**		
1.1.1	**Ensure System Logging to a Remote Host**		
1.1.1.1	Syslog logging should be configured (Automated)	☐	☐
1.1.1.2	SNMPv3 traps should be configured (Automated)	☐	☐
1.1.2	Ensure 'Login Banner' is set (Automated)	☐	☐
1.1.3	Ensure 'Enable Log on High DP Load' is enabled (Automated)	☐	☐
1.2	**Management Interface Settings**		
1.2.1	Ensure 'Permitted IP Addresses' is set to those necessary for device management (Automated)	☐	☐
1.2.2	Ensure 'Permitted IP Addresses' is set for all management profiles where SSH, HTTPS, or SNMP is enabled (Automated)	☐	☐
1.2.3	Ensure HTTP and Telnet options are disabled for the management interface (Automated)	☐	☐
1.2.4	Ensure HTTP and Telnet options are disabled for all management profiles (Automated)	☐	☐
1.2.5	Ensure valid certificate is set for browser-based administrator interface (Automated)	☐	☐
1.3	**Minimum Password Requirements**		
1.3.1	Ensure 'Minimum Password Complexity' is enabled (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.3.2	Ensure 'Minimum Length' is greater than or equal to 12 (Automated)	☐	☐
1.3.3	Ensure 'Minimum Uppercase Letters' is greater than or equal to 1 (Automated)	☐	☐
1.3.4	Ensure 'Minimum Lowercase Letters' is greater than or equal to 1 (Automated)	☐	☐
1.3.5	Ensure 'Minimum Numeric Letters' is greater than or equal to 1 (Automated)	☐	☐
1.3.6	Ensure 'Minimum Special Characters' is greater than or equal to 1 (Automated)	☐	☐
1.3.7	Ensure 'Required Password Change Period' is less than or equal to 90 days (Automated)	☐	☐
1.3.8	Ensure 'New Password Differs By Characters' is greater than or equal to 3 (Automated)	☐	☐
1.3.9	Ensure 'Prevent Password Reuse Limit' is set to 24 or more passwords (Automated)	☐	☐
1.3.10	Ensure 'Password Profiles' do not exist (Automated)	☐	☐
1.4	**Authentication Settings (for Device Mgmt)**		
1.4.1	Ensure 'Idle timeout' is less than or equal to 10 minutes for device management (Automated)	☐	☐
1.4.2	Ensure 'Failed Attempts' and 'Lockout Time' for Authentication Profile are properly configured (Automated)	☐	☐
1.5	**SNMP Polling Settings**		
1.5.1	Ensure 'V3' is selected for SNMP polling (Automated)	☐	☐
1.6	**Device Services Settings**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.6.1	Ensure 'Verify Update Server Identity' is enabled (Automated)	☐	☐
1.6.2	Ensure redundant NTP servers are configured appropriately (Automated)	☐	☐
1.6.3	Ensure that the Certificate Securing Remote Access VPNs is Valid (Manual)	☐	☐
2	**User Identification**		
2.1	Ensure that IP addresses are mapped to usernames (Automated)	☐	☐
2.2	Ensure that WMI probing is disabled (Automated)	☐	☐
2.3	Ensure that User-ID is only enabled for internal trusted interfaces (Automated)	☐	☐
2.4	Ensure that 'Include/Exclude Networks' is used if User-ID is enabled (Automated)	☐	☐
2.5	Ensure that the User-ID Agent has minimal permissions if User-ID is enabled (Manual)	☐	☐
2.6	Ensure that the User-ID service account does not have interactive logon rights (Automated)	☐	☐
2.7	Ensure remote access capabilities for the User-ID service account are forbidden. (Automated)	☐	☐
2.8	Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones (Automated)	☐	☐
3	**High Availability**		
3.1	Ensure a fully-synchronized High Availability peer is configured (Automated)	☐	☐
3.2	Ensure 'High Availability' requires Link Monitoring and/or Path Monitoring (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.3	Ensure 'Passive Link State' and 'Preemptive' are configured appropriately (Manual)	☐	☐
4	**Dynamic Updates**		
4.1	Ensure 'Antivirus Update Schedule' is set to download and install updates hourly (Automated)	☐	☐
4.2	Ensure 'Applications and Threats Update Schedule' is set to download and install updates at daily or shorter intervals (Automated)	☐	☐
5	**Wildfire**		
5.1	Ensure that WildFire file size upload limits are maximized (Automated)	☐	☐
5.2	Ensure a WildFire Analysis profile is enabled for all security policies (Automated)	☐	☐
5.3	Ensure forwarding of decrypted content to WildFire is enabled (Automated)	☐	☐
5.4	Ensure all WildFire session information settings are enabled (Automated)	☐	☐
5.5	Ensure alerts are enabled for malicious files detected by WildFire (Automated)	☐	☐
5.6	Ensure 'WildFire Update Schedule' is set to download and install updates in real-time (Automated)	☐	☐
5.7	Choosing Wildfire public cloud region (Manual)	☐	☐
6	**Security Profiles**		
6.1	Ensure that antivirus profiles are set to reset-both on all decoders except 'imap' and 'pop3' (Automated)	☐	☐
6.2	Ensure a secure antivirus profile is applied to all relevant security policies (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.3	Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats (Automated)	☐	☐
6.4	Ensure DNS sinkholing is configured on all anti-spyware profiles in use (Automated)	☐	☐
6.5	Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the Internet (Automated)	☐	☐
6.6	Ensure a Vulnerability Protection Profile is set to block attacks against critical and high vulnerabilities, and set to default on medium, low, and informational vulnerabilities (Automated)	☐	☐
6.7	Ensure a secure Vulnerability Protection Profile is applied to all security rules allowing traffic (Automated)	☐	☐
6.8	Ensure that PAN-DB URL Filtering is used (Automated)	☐	☐
6.9	Ensure that URL Filtering uses the action of "block" or "override" on the <enterprise approved value> URL categories (Automated)	☐	☐
6.10	Ensure that access to every URL is logged (Automated)	☐	☐
6.11	Ensure all HTTP Header Logging options are enabled (Automated)	☐	☐
6.12	Ensure secure URL filtering is enabled for all security policies allowing traffic to the Internet (Automated)	☐	☐
6.13	Ensure alerting after a threshold of credit card or Social Security numbers is detected is enabled (Automated)	☐	☐
6.14	Ensure a secure Data Filtering profile is applied to all security policies allowing traffic to or from the Internet (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.15	Ensure that a Zone Protection Profile with an enabled SYN Flood Action of SYN Cookies is attached to all untrusted zones (Automated)	☐	☐
6.16	Ensure that a Zone Protection Profile with tuned Flood Protection settings enabled for all flood types is attached to all untrusted zones (Automated)	☐	☐
6.17	Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned, and set to appropriate actions (Automated)	☐	☐
6.18	Ensure all zones have Zone Protection Profiles that drop specially crafted packets (Automated)	☐	☐
6.19	Ensure that User Credential Submission uses the action of "block" or "continue" on the URL categories (Automated)	☐	☐
6.20	Ensure that 'Wildfire Inline ML Action' on antivirus profiles are set to reset-both on all decoders except 'imap' and 'pop3' (Manual)	☐	☐
6.21	Ensure that 'Wildfire Inline ML' on antivirus profiles are set to enable for all file types (Automated)	☐	☐
6.22	Ensure that 'Inline Cloud Analysis' on Vulnerability Protection profiles are enabled if 'Advanced Threat Prevention' is available (Automated)	☐	☐
6.23	Ensure that 'Cloud Inline Categorization' on URL Filtering profiles are enabled if 'Advanced Threat Prevention' is available (Automated)	☐	☐
6.24	Ensure that 'Inline Cloud Analysis' on Anti-Spyware profiles are enabled if 'Advanced Threat Prevention' is available (Automated)	☐	☐
6.25	Ensure that 'DNS Policies' is configured on Anti-Spyware profiles if 'DNS Security' license is available (Manual)	☐	☐
7	**Security Policies**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
7.1	Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone (Automated)	☐	☐
7.2	Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist (Automated)	☐	☐
7.3	Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists (Automated)	☐	☐
7.4	Ensure that logging is enabled on built-in default security policies (Manual)	☐	☐
8	**Decryption**		
8.1	Ensure 'SSL Forward Proxy Policy' for traffic destined to the Internet is configured (Automated)	☐	☐
8.2	Ensure 'SSL Inbound Inspection' is required for all untrusted traffic destined for servers using SSL or TLS (Manual)	☐	☐
8.3	Ensure that the Certificate used for Decryption is Trusted (Automated)	☐	☐

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Syslog logging should be configured	☐	☐
1.1.1.2	SNMPv3 traps should be configured	☐	☐
1.1.3	Ensure 'Enable Log on High DP Load' is enabled	☐	☐
1.3.2	Ensure 'Minimum Length' is greater than or equal to 12	☐	☐
1.3.3	Ensure 'Minimum Uppercase Letters' is greater than or equal to 1	☐	☐
1.3.4	Ensure 'Minimum Lowercase Letters' is greater than or equal to 1	☐	☐
1.3.5	Ensure 'Minimum Numeric Letters' is greater than or equal to 1	☐	☐
1.3.7	Ensure 'Required Password Change Period' is less than or equal to 90 days	☐	☐
1.3.8	Ensure 'New Password Differs By Characters' is greater than or equal to 3	☐	☐
1.3.9	Ensure 'Prevent Password Reuse Limit' is set to 24 or more passwords	☐	☐
1.3.10	Ensure 'Password Profiles' do not exist	☐	☐
1.4.1	Ensure 'Idle timeout' is less than or equal to 10 minutes for device management	☐	☐
1.6.1	Ensure 'Verify Update Server Identity' is enabled	☐	☐
2.3	Ensure that User-ID is only enabled for internal trusted interfaces	☐	☐
4.1	Ensure 'Antivirus Update Schedule' is set to download and install updates hourly	☐	☐
4.2	Ensure 'Applications and Threats Update Schedule' is set to download and install updates at daily or shorter intervals	☐	☐
5.4	Ensure all WildFire session information settings are enabled	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.5	Ensure alerts are enabled for malicious files detected by WildFire	☐	☐
5.6	Ensure 'WildFire Update Schedule' is set to download and install updates in real-time	☐	☐
6.10	Ensure that access to every URL is logged	☐	☐
6.11	Ensure all HTTP Header Logging options are enabled	☐	☐
6.13	Ensure alerting after a threshold of credit card or Social Security numbers is detected is enabled	☐	☐
6.17	Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned, and set to appropriate actions	☐	☐

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Syslog logging should be configured	☐	☐
1.1.1.2	SNMPv3 traps should be configured	☐	☐
1.1.3	Ensure 'Enable Log on High DP Load' is enabled	☐	☐
1.2.1	Ensure 'Permitted IP Addresses' is set to those necessary for device management	☐	☐
1.2.2	Ensure 'Permitted IP Addresses' is set for all management profiles where SSH, HTTPS, or SNMP is enabled	☐	☐
1.2.3	Ensure HTTP and Telnet options are disabled for the management interface	☐	☐
1.2.4	Ensure HTTP and Telnet options are disabled for all management profiles	☐	☐
1.2.5	Ensure valid certificate is set for browser-based administrator interface	☐	☐
1.3.1	Ensure 'Minimum Password Complexity' is enabled	☐	☐
1.3.2	Ensure 'Minimum Length' is greater than or equal to 12	☐	☐
1.3.3	Ensure 'Minimum Uppercase Letters' is greater than or equal to 1	☐	☐
1.3.4	Ensure 'Minimum Lowercase Letters' is greater than or equal to 1	☐	☐
1.3.5	Ensure 'Minimum Numeric Letters' is greater than or equal to 1	☐	☐
1.3.7	Ensure 'Required Password Change Period' is less than or equal to 90 days	☐	☐
1.3.8	Ensure 'New Password Differs By Characters' is greater than or equal to 3	☐	☐
1.3.9	Ensure 'Prevent Password Reuse Limit' is set to 24 or more passwords	☐	☐
1.3.10	Ensure 'Password Profiles' do not exist	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.4.1	Ensure 'Idle timeout' is less than or equal to 10 minutes for device management	☐	☐
1.5.1	Ensure 'V3' is selected for SNMP polling	☐	☐
1.6.1	Ensure 'Verify Update Server Identity' is enabled	☐	☐
1.6.2	Ensure redundant NTP servers are configured appropriately	☐	☐
1.6.3	Ensure that the Certificate Securing Remote Access VPNs is Valid	☐	☐
2.2	Ensure that WMI probing is disabled	☐	☐
2.3	Ensure that User-ID is only enabled for internal trusted interfaces	☐	☐
2.4	Ensure that 'Include/Exclude Networks' is used if User-ID is enabled	☐	☐
2.8	Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones	☐	☐
4.1	Ensure 'Antivirus Update Schedule' is set to download and install updates hourly	☐	☐
4.2	Ensure 'Applications and Threats Update Schedule' is set to download and install updates at daily or shorter intervals	☐	☐
5.4	Ensure all WildFire session information settings are enabled	☐	☐
5.5	Ensure alerts are enabled for malicious files detected by WildFire	☐	☐
5.6	Ensure 'WildFire Update Schedule' is set to download and install updates in real-time	☐	☐
6.4	Ensure DNS sinkholing is configured on all anti-spyware profiles in use	☐	☐
6.7	Ensure a secure Vulnerability Protection Profile is applied to all security rules allowing traffic	☐	☐
6.8	Ensure that PAN-DB URL Filtering is used	☐	☐
6.9	Ensure that URL Filtering uses the action of "block" or "override" on the <enterprise approved value> URL categories	☐	☐
6.10	Ensure that access to every URL is logged	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
6.11	Ensure all HTTP Header Logging options are enabled	☐	☐
6.12	Ensure secure URL filtering is enabled for all security policies allowing traffic to the Internet	☐	☐
6.13	Ensure alerting after a threshold of credit card or Social Security numbers is detected is enabled	☐	☐
6.17	Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned, and set to appropriate actions	☐	☐
7.2	Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist	☐	☐
7.3	Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists	☐	☐

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Syslog logging should be configured	☐	☐
1.1.1.2	SNMPv3 traps should be configured	☐	☐
1.1.3	Ensure 'Enable Log on High DP Load' is enabled	☐	☐
1.2.1	Ensure 'Permitted IP Addresses' is set to those necessary for device management	☐	☐
1.2.2	Ensure 'Permitted IP Addresses' is set for all management profiles where SSH, HTTPS, or SNMP is enabled	☐	☐
1.2.3	Ensure HTTP and Telnet options are disabled for the management interface	☐	☐
1.2.4	Ensure HTTP and Telnet options are disabled for all management profiles	☐	☐
1.2.5	Ensure valid certificate is set for browser-based administrator interface	☐	☐
1.3.1	Ensure 'Minimum Password Complexity' is enabled	☐	☐
1.3.2	Ensure 'Minimum Length' is greater than or equal to 12	☐	☐
1.3.3	Ensure 'Minimum Uppercase Letters' is greater than or equal to 1	☐	☐
1.3.4	Ensure 'Minimum Lowercase Letters' is greater than or equal to 1	☐	☐
1.3.5	Ensure 'Minimum Numeric Letters' is greater than or equal to 1	☐	☐
1.3.7	Ensure 'Required Password Change Period' is less than or equal to 90 days	☐	☐
1.3.8	Ensure 'New Password Differs By Characters' is greater than or equal to 3	☐	☐
1.3.9	Ensure 'Prevent Password Reuse Limit' is set to 24 or more passwords	☐	☐
1.3.10	Ensure 'Password Profiles' do not exist	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
1.4.1	Ensure 'Idle timeout' is less than or equal to 10 minutes for device management	☐	☐
1.5.1	Ensure 'V3' is selected for SNMP polling	☐	☐
1.6.1	Ensure 'Verify Update Server Identity' is enabled	☐	☐
1.6.2	Ensure redundant NTP servers are configured appropriately	☐	☐
1.6.3	Ensure that the Certificate Securing Remote Access VPNs is Valid	☐	☐
2.1	Ensure that IP addresses are mapped to usernames	☐	☐
2.2	Ensure that WMI probing is disabled	☐	☐
2.3	Ensure that User-ID is only enabled for internal trusted interfaces	☐	☐
2.4	Ensure that 'Include/Exclude Networks' is used if User-ID is enabled	☐	☐
2.8	Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones	☐	☐
4.1	Ensure 'Antivirus Update Schedule' is set to download and install updates hourly	☐	☐
4.2	Ensure 'Applications and Threats Update Schedule' is set to download and install updates at daily or shorter intervals	☐	☐
5.3	Ensure forwarding of decrypted content to WildFire is enabled	☐	☐
5.4	Ensure all WildFire session information settings are enabled	☐	☐
5.5	Ensure alerts are enabled for malicious files detected by WildFire	☐	☐
5.6	Ensure 'WildFire Update Schedule' is set to download and install updates in real-time	☐	☐
6.4	Ensure DNS sinkholing is configured on all anti-spyware profiles in use	☐	☐
6.6	Ensure a Vulnerability Protection Profile is set to block attacks against critical and high vulnerabilities, and set to default on medium, low, and informational vulnerabilities	☐	☐
6.7	Ensure a secure Vulnerability Protection Profile is applied to all security rules allowing traffic	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.8	Ensure that PAN-DB URL Filtering is used	☐	☐
6.9	Ensure that URL Filtering uses the action of "block" or "override" on the <enterprise approved value> URL categories	☐	☐
6.10	Ensure that access to every URL is logged	☐	☐
6.11	Ensure all HTTP Header Logging options are enabled	☐	☐
6.12	Ensure secure URL filtering is enabled for all security policies allowing traffic to the Internet	☐	☐
6.13	Ensure alerting after a threshold of credit card or Social Security numbers is detected is enabled	☐	☐
6.14	Ensure a secure Data Filtering profile is applied to all security policies allowing traffic to or from the Internet	☐	☐
6.15	Ensure that a Zone Protection Profile with an enabled SYN Flood Action of SYN Cookies is attached to all untrusted zones	☐	☐
6.16	Ensure that a Zone Protection Profile with tuned Flood Protection settings enabled for all flood types is attached to all untrusted zones	☐	☐
6.17	Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned, and set to appropriate actions	☐	☐
6.18	Ensure all zones have Zone Protection Profiles that drop specially crafted packets	☐	☐
7.2	Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist	☐	☐
7.3	Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists	☐	☐
8.1	Ensure 'SSL Forward Proxy Policy' for traffic destined to the Internet is configured	☐	☐
8.2	Ensure 'SSL Inbound Inspection' is required for all untrusted traffic destined for servers using SSL or TLS	☐	☐
8.3	Ensure that the Certificate used for Decryption is Trusted	☐	☐

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
5.7	Choosing Wildfire public cloud region	☐	☐
6.20	Ensure that 'Wildfire Inline ML Action' on antivirus profiles are set to reset-both on all decoders except 'imap' and 'pop3'	☐	☐
6.21	Ensure that 'Wildfire Inline ML' on antivirus profiles are set to enable for all file types	☐	☐
6.22	Ensure that 'Inline Cloud Analysis' on Vulnerability Protection profiles are enabled if 'Advanced Threat Prevention' is available	☐	☐
6.23	Ensure that 'Cloud Inline Categorization' on URL Filtering profiles are enabled if 'Advanced Threat Prevention' is available	☐	☐
6.24	Ensure that 'Inline Cloud Analysis' on Anti-Spyware profiles are enabled if 'Advanced Threat Prevention' is available	☐	☐
6.25	Ensure that 'DNS Policies' is configured on Anti-Spyware profiles if 'DNS Security' license is available	☐	☐
7.4	Ensure that logging is enabled on built-in default security policies	☐	☐

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Syslog logging should be configured	☐	☐
1.1.1.2	SNMPv3 traps should be configured	☐	☐
1.1.2	Ensure 'Login Banner' is set	☐	☐
1.1.3	Ensure 'Enable Log on High DP Load' is enabled	☐	☐
1.2.1	Ensure 'Permitted IP Addresses' is set to those necessary for device management	☐	☐
1.2.2	Ensure 'Permitted IP Addresses' is set for all management profiles where SSH, HTTPS, or SNMP is enabled	☐	☐
1.2.3	Ensure HTTP and Telnet options are disabled for the management interface	☐	☐
1.2.4	Ensure HTTP and Telnet options are disabled for all management profiles	☐	☐
1.2.5	Ensure valid certificate is set for browser-based administrator interface	☐	☐
1.3.1	Ensure 'Minimum Password Complexity' is enabled	☐	☐
1.3.2	Ensure 'Minimum Length' is greater than or equal to 12	☐	☐
1.3.3	Ensure 'Minimum Uppercase Letters' is greater than or equal to 1	☐	☐
1.3.4	Ensure 'Minimum Lowercase Letters' is greater than or equal to 1	☐	☐
1.3.5	Ensure 'Minimum Numeric Letters' is greater than or equal to 1	☐	☐
1.3.6	Ensure 'Minimum Special Characters' is greater than or equal to 1	☐	☐
1.3.7	Ensure 'Required Password Change Period' is less than or equal to 90 days	☐	☐
1.3.8	Ensure 'New Password Differs By Characters' is greater than or equal to 3	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
1.3.9	Ensure 'Prevent Password Reuse Limit' is set to 24 or more passwords	☐	☐
1.3.10	Ensure 'Password Profiles' do not exist	☐	☐
1.4.1	Ensure 'Idle timeout' is less than or equal to 10 minutes for device management	☐	☐
1.4.2	Ensure 'Failed Attempts' and 'Lockout Time' for Authentication Profile are properly configured	☐	☐
1.6.1	Ensure 'Verify Update Server Identity' is enabled	☐	☐
2.2	Ensure that WMI probing is disabled	☐	☐
2.3	Ensure that User-ID is only enabled for internal trusted interfaces	☐	☐
2.5	Ensure that the User-ID Agent has minimal permissions if User-ID is enabled	☐	☐
2.8	Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones	☐	☐
3.1	Ensure a fully-synchronized High Availability peer is configured	☐	☐
3.2	Ensure 'High Availability' requires Link Monitoring and/or Path Monitoring	☐	☐
3.3	Ensure 'Passive Link State' and 'Preemptive' are configured appropriately	☐	☐
4.1	Ensure 'Antivirus Update Schedule' is set to download and install updates hourly	☐	☐
4.2	Ensure 'Applications and Threats Update Schedule' is set to download and install updates at daily or shorter intervals	☐	☐
5.1	Ensure that WildFire file size upload limits are maximized	☐	☐
5.2	Ensure a WildFire Analysis profile is enabled for all security policies	☐	☐
5.3	Ensure forwarding of decrypted content to WildFire is enabled	☐	☐
5.4	Ensure all WildFire session information settings are enabled	☐	☐
5.5	Ensure alerts are enabled for malicious files detected by WildFire	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.6	Ensure 'WildFire Update Schedule' is set to download and install updates in real-time	☐	☐
6.1	Ensure that antivirus profiles are set to reset-both on all decoders except 'imap' and 'pop3'	☐	☐
6.2	Ensure a secure antivirus profile is applied to all relevant security policies	☐	☐
6.3	Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats	☐	☐
6.5	Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the Internet	☐	☐
6.13	Ensure alerting after a threshold of credit card or Social Security numbers is detected is enabled	☐	☐
6.14	Ensure a secure Data Filtering profile is applied to all security policies allowing traffic to or from the Internet	☐	☐
6.17	Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned, and set to appropriate actions	☐	☐
6.18	Ensure all zones have Zone Protection Profiles that drop specially crafted packets	☐	☐
6.19	Ensure that User Credential Submission uses the action of "block" or "continue" on the URL categories	☐	☐
6.20	Ensure that 'Wildfire Inline ML Action' on antivirus profiles are set to reset-both on all decoders except 'imap' and 'pop3'	☐	☐
6.21	Ensure that 'Wildfire Inline ML' on antivirus profiles are set to enable for all file types	☐	☐
6.24	Ensure that 'Inline Cloud Analysis' on Anti-Spyware profiles are enabled if 'Advanced Threat Prevention' is available	☐	☐
6.25	Ensure that 'DNS Policies' is configured on Anti-Spyware profiles if 'DNS Security' license is available	☐	☐
7.1	Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone	☐	☐
7.2	Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist	☐	☐
7.3	Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
8.3	Ensure that the Certificate used for Decryption is Trusted	☐	☐

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Syslog logging should be configured	☐	☐
1.1.1.2	SNMPv3 traps should be configured	☐	☐
1.1.2	Ensure 'Login Banner' is set	☐	☐
1.1.3	Ensure 'Enable Log on High DP Load' is enabled	☐	☐
1.2.1	Ensure 'Permitted IP Addresses' is set to those necessary for device management	☐	☐
1.2.2	Ensure 'Permitted IP Addresses' is set for all management profiles where SSH, HTTPS, or SNMP is enabled	☐	☐
1.2.3	Ensure HTTP and Telnet options are disabled for the management interface	☐	☐
1.2.4	Ensure HTTP and Telnet options are disabled for all management profiles	☐	☐
1.2.5	Ensure valid certificate is set for browser-based administrator interface	☐	☐
1.3.1	Ensure 'Minimum Password Complexity' is enabled	☐	☐
1.3.2	Ensure 'Minimum Length' is greater than or equal to 12	☐	☐
1.3.3	Ensure 'Minimum Uppercase Letters' is greater than or equal to 1	☐	☐
1.3.4	Ensure 'Minimum Lowercase Letters' is greater than or equal to 1	☐	☐
1.3.5	Ensure 'Minimum Numeric Letters' is greater than or equal to 1	☐	☐
1.3.6	Ensure 'Minimum Special Characters' is greater than or equal to 1	☐	☐
1.3.7	Ensure 'Required Password Change Period' is less than or equal to 90 days	☐	☐
1.3.8	Ensure 'New Password Differs By Characters' is greater than or equal to 3	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
1.3.9	Ensure 'Prevent Password Reuse Limit' is set to 24 or more passwords	☐	☐
1.3.10	Ensure 'Password Profiles' do not exist	☐	☐
1.4.1	Ensure 'Idle timeout' is less than or equal to 10 minutes for device management	☐	☐
1.4.2	Ensure 'Failed Attempts' and 'Lockout Time' for Authentication Profile are properly configured	☐	☐
1.5.1	Ensure 'V3' is selected for SNMP polling	☐	☐
1.6.1	Ensure 'Verify Update Server Identity' is enabled	☐	☐
1.6.2	Ensure redundant NTP servers are configured appropriately	☐	☐
2.2	Ensure that WMI probing is disabled	☐	☐
2.3	Ensure that User-ID is only enabled for internal trusted interfaces	☐	☐
2.4	Ensure that 'Include/Exclude Networks' is used if User-ID is enabled	☐	☐
2.5	Ensure that the User-ID Agent has minimal permissions if User-ID is enabled	☐	☐
2.6	Ensure that the User-ID service account does not have interactive logon rights	☐	☐
2.8	Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones	☐	☐
3.1	Ensure a fully-synchronized High Availability peer is configured	☐	☐
3.2	Ensure 'High Availability' requires Link Monitoring and/or Path Monitoring	☐	☐
3.3	Ensure 'Passive Link State' and 'Preemptive' are configured appropriately	☐	☐
4.1	Ensure 'Antivirus Update Schedule' is set to download and install updates hourly	☐	☐
4.2	Ensure 'Applications and Threats Update Schedule' is set to download and install updates at daily or shorter intervals	☐	☐
5.1	Ensure that WildFire file size upload limits are maximized	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
5.2	Ensure a WildFire Analysis profile is enabled for all security policies	☐	☐
5.3	Ensure forwarding of decrypted content to WildFire is enabled	☐	☐
5.4	Ensure all WildFire session information settings are enabled	☐	☐
5.5	Ensure alerts are enabled for malicious files detected by WildFire	☐	☐
5.6	Ensure 'WildFire Update Schedule' is set to download and install updates in real-time	☐	☐
6.1	Ensure that antivirus profiles are set to reset-both on all decoders except 'imap' and 'pop3'	☐	☐
6.2	Ensure a secure antivirus profile is applied to all relevant security policies	☐	☐
6.3	Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats	☐	☐
6.4	Ensure DNS sinkholing is configured on all anti-spyware profiles in use	☐	☐
6.5	Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the Internet	☐	☐
6.6	Ensure a Vulnerability Protection Profile is set to block attacks against critical and high vulnerabilities, and set to default on medium, low, and informational vulnerabilities	☐	☐
6.7	Ensure a secure Vulnerability Protection Profile is applied to all security rules allowing traffic	☐	☐
6.8	Ensure that PAN-DB URL Filtering is used	☐	☐
6.9	Ensure that URL Filtering uses the action of "block" or "override" on the <enterprise approved value> URL categories	☐	☐
6.10	Ensure that access to every URL is logged	☐	☐
6.11	Ensure all HTTP Header Logging options are enabled	☐	☐
6.12	Ensure secure URL filtering is enabled for all security policies allowing traffic to the Internet	☐	☐
6.13	Ensure alerting after a threshold of credit card or Social Security numbers is detected is enabled	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
6.14	Ensure a secure Data Filtering profile is applied to all security policies allowing traffic to or from the Internet	☐	☐
6.17	Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned, and set to appropriate actions	☐	☐
6.18	Ensure all zones have Zone Protection Profiles that drop specially crafted packets	☐	☐
6.19	Ensure that User Credential Submission uses the action of "block" or "continue" on the URL categories	☐	☐
6.20	Ensure that 'Wildfire Inline ML Action' on antivirus profiles are set to reset-both on all decoders except 'imap' and 'pop3'	☐	☐
6.21	Ensure that 'Wildfire Inline ML' on antivirus profiles are set to enable for all file types	☐	☐
6.22	Ensure that 'Inline Cloud Analysis' on Vulnerability Protection profiles are enabled if 'Advanced Threat Prevention' is available	☐	☐
6.23	Ensure that 'Cloud Inline Categorization' on URL Filtering profiles are enabled if 'Advanced Threat Prevention' is available	☐	☐
6.24	Ensure that 'Inline Cloud Analysis' on Anti-Spyware profiles are enabled if 'Advanced Threat Prevention' is available	☐	☐
6.25	Ensure that 'DNS Policies' is configured on Anti-Spyware profiles if 'DNS Security' license is available	☐	☐
7.1	Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone	☐	☐
7.2	Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist	☐	☐
7.3	Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists	☐	☐
7.4	Ensure that logging is enabled on built-in default security policies	☐	☐
8.1	Ensure 'SSL Forward Proxy Policy' for traffic destined to the Internet is configured	☐	☐
8.2	Ensure 'SSL Inbound Inspection' is required for all untrusted traffic destined for servers using SSL or TLS	☐	☐

Recommendation		Set Correctly	
		Yes	No
8.3	Ensure that the Certificate used for Decryption is Trusted	☐	☐

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Syslog logging should be configured	☐	☐
1.1.1.2	SNMPv3 traps should be configured	☐	☐
1.1.2	Ensure 'Login Banner' is set	☐	☐
1.1.3	Ensure 'Enable Log on High DP Load' is enabled	☐	☐
1.2.1	Ensure 'Permitted IP Addresses' is set to those necessary for device management	☐	☐
1.2.2	Ensure 'Permitted IP Addresses' is set for all management profiles where SSH, HTTPS, or SNMP is enabled	☐	☐
1.2.3	Ensure HTTP and Telnet options are disabled for the management interface	☐	☐
1.2.4	Ensure HTTP and Telnet options are disabled for all management profiles	☐	☐
1.2.5	Ensure valid certificate is set for browser-based administrator interface	☐	☐
1.3.1	Ensure 'Minimum Password Complexity' is enabled	☐	☐
1.3.2	Ensure 'Minimum Length' is greater than or equal to 12	☐	☐
1.3.3	Ensure 'Minimum Uppercase Letters' is greater than or equal to 1	☐	☐
1.3.4	Ensure 'Minimum Lowercase Letters' is greater than or equal to 1	☐	☐
1.3.5	Ensure 'Minimum Numeric Letters' is greater than or equal to 1	☐	☐
1.3.6	Ensure 'Minimum Special Characters' is greater than or equal to 1	☐	☐
1.3.7	Ensure 'Required Password Change Period' is less than or equal to 90 days	☐	☐
1.3.8	Ensure 'New Password Differs By Characters' is greater than or equal to 3	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.3.9	Ensure 'Prevent Password Reuse Limit' is set to 24 or more passwords	☐	☐
1.3.10	Ensure 'Password Profiles' do not exist	☐	☐
1.4.1	Ensure 'Idle timeout' is less than or equal to 10 minutes for device management	☐	☐
1.4.2	Ensure 'Failed Attempts' and 'Lockout Time' for Authentication Profile are properly configured	☐	☐
1.5.1	Ensure 'V3' is selected for SNMP polling	☐	☐
1.6.1	Ensure 'Verify Update Server Identity' is enabled	☐	☐
1.6.2	Ensure redundant NTP servers are configured appropriately	☐	☐
1.6.3	Ensure that the Certificate Securing Remote Access VPNs is Valid	☐	☐
2.1	Ensure that IP addresses are mapped to usernames	☐	☐
2.2	Ensure that WMI probing is disabled	☐	☐
2.3	Ensure that User-ID is only enabled for internal trusted interfaces	☐	☐
2.4	Ensure that 'Include/Exclude Networks' is used if User-ID is enabled	☐	☐
2.5	Ensure that the User-ID Agent has minimal permissions if User-ID is enabled	☐	☐
2.6	Ensure that the User-ID service account does not have interactive logon rights	☐	☐
2.7	Ensure remote access capabilities for the User-ID service account are forbidden.	☐	☐
2.8	Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones	☐	☐
3.1	Ensure a fully-synchronized High Availability peer is configured	☐	☐
3.2	Ensure 'High Availability' requires Link Monitoring and/or Path Monitoring	☐	☐
3.3	Ensure 'Passive Link State' and 'Preemptive' are configured appropriately	☐	☐
4.1	Ensure 'Antivirus Update Schedule' is set to download and install updates hourly	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.2	Ensure 'Applications and Threats Update Schedule' is set to download and install updates at daily or shorter intervals	☐	☐
5.1	Ensure that WildFire file size upload limits are maximized	☐	☐
5.2	Ensure a WildFire Analysis profile is enabled for all security policies	☐	☐
5.3	Ensure forwarding of decrypted content to WildFire is enabled	☐	☐
5.4	Ensure all WildFire session information settings are enabled	☐	☐
5.5	Ensure alerts are enabled for malicious files detected by WildFire	☐	☐
5.6	Ensure 'WildFire Update Schedule' is set to download and install updates in real-time	☐	☐
6.1	Ensure that antivirus profiles are set to reset-both on all decoders except 'imap' and 'pop3'	☐	☐
6.2	Ensure a secure antivirus profile is applied to all relevant security policies	☐	☐
6.3	Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats	☐	☐
6.4	Ensure DNS sinkholing is configured on all anti-spyware profiles in use	☐	☐
6.5	Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the Internet	☐	☐
6.6	Ensure a Vulnerability Protection Profile is set to block attacks against critical and high vulnerabilities, and set to default on medium, low, and informational vulnerabilities	☐	☐
6.7	Ensure a secure Vulnerability Protection Profile is applied to all security rules allowing traffic	☐	☐
6.8	Ensure that PAN-DB URL Filtering is used	☐	☐
6.9	Ensure that URL Filtering uses the action of "block" or "override" on the <enterprise approved value> URL categories	☐	☐
6.10	Ensure that access to every URL is logged	☐	☐
6.11	Ensure all HTTP Header Logging options are enabled	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.12	Ensure secure URL filtering is enabled for all security policies allowing traffic to the Internet	☐	☐
6.13	Ensure alerting after a threshold of credit card or Social Security numbers is detected is enabled	☐	☐
6.14	Ensure a secure Data Filtering profile is applied to all security policies allowing traffic to or from the Internet	☐	☐
6.15	Ensure that a Zone Protection Profile with an enabled SYN Flood Action of SYN Cookies is attached to all untrusted zones	☐	☐
6.16	Ensure that a Zone Protection Profile with tuned Flood Protection settings enabled for all flood types is attached to all untrusted zones	☐	☐
6.17	Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned, and set to appropriate actions	☐	☐
6.18	Ensure all zones have Zone Protection Profiles that drop specially crafted packets	☐	☐
6.19	Ensure that User Credential Submission uses the action of "block" or "continue" on the URL categories	☐	☐
6.20	Ensure that 'Wildfire Inline ML Action' on antivirus profiles are set to reset-both on all decoders except 'imap' and 'pop3'	☐	☐
6.21	Ensure that 'Wildfire Inline ML' on antivirus profiles are set to enable for all file types	☐	☐
6.22	Ensure that 'Inline Cloud Analysis' on Vulnerability Protection profiles are enabled if 'Advanced Threat Prevention' is available	☐	☐
6.23	Ensure that 'Cloud Inline Categorization' on URL Filtering profiles are enabled if 'Advanced Threat Prevention' is available	☐	☐
6.24	Ensure that 'Inline Cloud Analysis' on Anti-Spyware profiles are enabled if 'Advanced Threat Prevention' is available	☐	☐
6.25	Ensure that 'DNS Policies' is configured on Anti-Spyware profiles if 'DNS Security' license is available	☐	☐
7.1	Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone	☐	☐

Recommendation		Set Correctly	
		Yes	No
7.2	Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist	☐	☐
7.3	Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists	☐	☐
7.4	Ensure that logging is enabled on built-in default security policies	☐	☐
8.1	Ensure 'SSL Forward Proxy Policy' for traffic destined to the Internet is configured	☐	☐
8.2	Ensure 'SSL Inbound Inspection' is required for all untrusted traffic destined for servers using SSL or TLS	☐	☐
8.3	Ensure that the Certificate used for Decryption is Trusted	☐	☐

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
5.7	Choosing Wildfire public cloud region	☐	☐

Appendix: Change History

Date	Version	Changes for this version