Center for Internet Security®

CIS Palo Alto Firewall 7 Benchmark

v1.0.0 - 03-30-2017

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Table of Contents

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Palo Alto Firewalls running PAN-OS version 7.1.x. This guide was tested against PAN-OS v7.1.5. 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 benchmark was created using a consensus review process comprised of subject matter experts. 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://community.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

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

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 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:

Author
Ryan Firth CISSP, CCNP, CISA, GCIH, GLEG

Contributor
Jordan Rakoske
Philippe Langlois
Adam Winnington
Raymond Winder PAN-ACE, GCED, GCIH, BS
Samshodh Sunku, Palo Alto
Derek Ho

Editor
Rob VandenBrink
Karen Scarfone

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 'Login Banner' is set (Scored)

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 `Login Banner` is set appropriately.

Remediation:

Navigate to `Device > Setup > Management > General Settings`.

Set `Login Banner` as appropriate.

Default Value:

Not configured

References:

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

1.1.2 Ensure 'Enable Log on High DP Load' is enabled (Scored)

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.

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. https://live.paloaltonetworks.com/docs/DOC-4075

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 (Scored)

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 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 > Management > Management Interface Settings`.

Verify `Permitted IP Addresses` is limited to those necessary for device management.

Remediation:

Navigate to `Device > Setup > Management > Management Interface Settings`.

Set `Permitted IP Addresses` to only those necessary for device management.

Default Value:

Not enabled

References:

1. https://live.paloaltonetworks.com/docs/DOC-8432

CIS Controls:

11.6 Use Dedicated Systems To Perform Network Device Administration
Network engineers shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated 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.

11.7 Manage Network Infrastructure Using Segregation
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 (Scored)

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`.

Verify `Permitted IP Addresses` is limited to those necessary for device management.

Remediation:

Navigate to `Network > Network Profiles > Interface Management`.

Set `Permitted IP Addresses` to only include those necessary for device management.

Default Value:

Not enabled

References:

1. https://live.paloaltonetworks.com/docs/DOC-8432

CIS Controls:

11.6 Use Dedicated Systems To Perform Network Device Administration
Network engineers shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated 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.

11.7 Manage Network Infrastructure Using Segregation
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 (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

Management access over clear text 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 `Device > Setup > Management > Management Interface Settings`.

Verify that the `HTTP` and `Telnet` options are both unchecked.

Remediation:

Navigate to `Device > Setup > Management > Management Interface Settings`.

Set the `HTTP` and `Telnet` boxes to unchecked.

Default Value:

Not set.

References:

1. https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-a-Layer-3-Interface-to-act-as-a-Management-Port/ta-p/59024

CIS Controls:

3.4 Use Only Secure Channels For Remote System Administration
Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

14.2 Encrypt All Sensitive Information Over Less-trusted Networks

All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.

16.13 User/Account Authentication Must Be Performed Over Encrypted Channels

Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

1.2.4 Ensure valid certificate is set for browser-based administrator interface (Not Scored)

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.

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 there is an appropriately named Certificate Profile for Management Interface Access:

Navigate to `Device > Certificate Management > Certificate Profile`

Verify that the Authentication Profile field contains the Certificate Profile created for Management Interface Access:

Navigate to `Device > Setup > Management (tab) > Authentication Settings > Authentication Profile (field)`

Remediation:

If a new administrative certificate is needed, acquire a certificate that meets the stated criteria and set it:

Navigate to `Device > Certificate Management > Certificates`

Set an appropriately named Certificate Profile for Management Interface Access:

Navigate to `Device > Certificate Management > Certificate Profile`

Set the Authentication Profile field so it contains the Certificate Profile created for Management Interface Access:

Navigate to `Device > Setup > Management (tab) > Authentication Settings > Authentication Profile (field)`

Default Value:

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

CIS Controls:

3.4 Use Only Secure Channels For Remote System Administration
Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

14.2 Encrypt All Sensitive Information Over Less-trusted Networks
All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.

16.13 User/Account Authentication Must Be Performed Over Encrypted Channels
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 password criteria such as complexity and restrictions.

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

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.

Audit:

Navigate to `Device > Setup > Management > Minimum Password Complexity`.

Verify `Enabled` is checked

Remediation:

Navigate to `Device > Setup > Management > Minimum Password Complexity`.

Set `Enabled` to be checked

Default Value:

Not enabled.

References:

1. https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-setup-management#48340

CIS Controls:

5.3 Change Default Passwords On All New Devices
Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.

5.7 User Accounts Shall Use Long Passwords
Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

16.12 Use Long Passwords For All User Accounts
Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

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

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.

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`

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.

Default Value:

Not enabled.

References:

1. https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-setup-management#48340

CIS Controls:

5.3 Change Default Passwords On All New Devices
Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.

5.7 User Accounts Shall Use Long Passwords
Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

16.12 Use Long Passwords For All User Accounts
Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

1.3.3 Ensure 'Prevent Password Reuse Limit' is set to 24 or more passwords (Scored)

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.

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. https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-setup-management#48340

CIS Controls:

5 Controlled Use of Administration Privileges
Controlled Use of Administration Privileges

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

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.

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`

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.

Default Value:

Not enabled.

References:

1. 2. https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-setup-management#48340

CIS Controls:

5 Controlled Use of Administration Privileges
Controlled Use of Administration Privileges

1.3.5 Ensure 'Password Profiles' do not exist (Scored)

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. https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-password-profiles

CIS Controls:

5 Controlled Use of Administration Privileges
Controlled Use of Administration Privileges

1.3.6 Ensure 'Minimum Uppercase Letters' is greater than or equal to 1 (Scored)

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. https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-setup-management#48340

CIS Controls:

5 Controlled Use of Administration Privileges
Controlled Use of Administration Privileges

1.3.7 Ensure 'Minimum Lowercase Letters' is greater than or equal to 1 (Scored)

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. https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-setup-management#48340

CIS Controls:

5 Controlled Use of Administration Privileges
Controlled Use of Administration Privileges

1.3.8 Ensure 'Minimum Numeric Letters' is greater than or equal to 1 (Scored)

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. https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-setup-management#48340

CIS Controls:

5 Controlled Use of Administration Privileges
Controlled Use of Administration Privileges

1.3.9 Ensure 'Minimum Special Characters' is greater than or equal to 1 (Scored)

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.

CIS Controls:

5 Controlled Use of Administration Privileges
Controlled Use of Administration Privileges

1.3.10 Ensure 'Block Username Inclusion' is enabled (Scored)

Profile Applicability:

- Level 1

Description:

This checks all new passwords to ensure that they block username inclusion (in either forward or reverse order.)

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 `Block Username Inclusion (Including reversed)` is checked

Remediation:

Navigate to `Device > Setup > Management > Minimum Password Complexity`

Set `Block Username Inclusion (Including reversed)` to checked

Impact:

If username inclusion is allowed in passwords, they become much easier to compromise. This prevents the use of the default (and trivial) admin / admin password combination.

Default Value:

Not enabled.

CIS Controls:

5.3 Change Default Passwords On All New Devices
Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.

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

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.

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

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.

Default Value:

Not enabled.

CIS Controls:

5 Controlled Use of Administration Privileges
Controlled Use of Administration Privileges

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 (Scored)

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

CIS Controls:

16.4 Automatically Log Off Users After Standard Period Of Inactivity
Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

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

Profile Applicability:

- Level 1

Description:

Configure an Authentication Profile with Failed Attempts and 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. 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.

Audit:

Navigate to `Device > Authentication Profile`.

Verify `Failed Attempts` is set to the organization-defined value.

Verify `Lockout Time` is set to the organization-defined value.

Remediation:

Navigate to `Device > Authentication Profile`.

Set `Failed Attempts` to the organization-defined value.

Set `Lockout Time` to the organization-defined value.

Default Value:

Not configured

References:

1. PAN-OS 7.1 Administrator's Guide pg.63

CIS Controls:

16.7 Configure Account Lockouts
Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.

1.5 SNMP Polling Settings

SNMP polling sets out requirements for using SNMP.

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

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.

Audit:

Navigate to `Device > Setup > Operations > Miscellaneous > SNMP Setup`

Verify `V3` is selected.

Remediation:

Navigate to `Device > Setup > Operations > Miscellaneous > SNMP Setup`

Select `V3`.

Default Value:

Not configured

References:

1. "How to Setup SNMPv3 Polling" - https://live.paloaltonetworks.com/docs/DOC-4037
2. "Using the Simple Network Management Protocol (SNMP)" - https://live.paloaltonetworks.com/docs/DOC-4627

CIS Controls:

3.4 Use Only Secure Channels For Remote System Administration
Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

14.2 Encrypt All Sensitive Information Over Less-trusted Networks
All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.

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 (Scored)

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.

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.

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. https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/install-content-and-software-updates

CIS Controls:

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

1.6.2 Ensure redundant NTP servers are configured appropriately (Scored)

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 is selected, only SHA1 should be used as MD5 is considered severely compromised.

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 7.1 (English)" - https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/71/pan-os/pan-os.pdf
3. https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-Authenticated-NTP/ta-p/54495

CIS Controls:

6.1 Use At Least Two Synchronized Time Sources For All Servers And Network Equipment
Include at least two synchronized time sources from which all servers and network equipment 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 (Not Scored)

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.

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.

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 > Authentication > SSL/TLS Profile`

Ensure that a valid certificate is applied to the GlobalProtect Gateway:

Navigate to `Network > GlobalProtect > Gateways > Authentication > SSL/TLS Profile`

Remediation:

Create a CSR and install a certificate from a public CA 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 Profile`

Default Value:

Not configured

References:

1. https://www.paloaltonetworks.com/documentation/71/globalprotect/globalprotect-admin-guide/set-up-the-globalprotect-infrastructure/globalprotect-certificate-best-practices
2. https://www.paloaltonetworks.com/documentation/71/globalprotect/globalprotect-admin-guide/set-up-the-globalprotect-infrastructure/deploy-server-certificates-to-the-globalprotect-components

CIS Controls:

14.2 Encrypt All Sensitive Information Over Less-trusted Networks
All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.

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 (Scored)

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 `Monitor > 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. "User-ID Best Practices - PAN-OS 5.0, 6.0" - https://live.paloaltonetworks.com/docs/DOC-6591
3. "How to Configure Group Mapping settings?" - https://live.paloaltonetworks.com/docs/DOC-4994
4. "PAN-OS Administrator's Guide 7.0 (English)" - https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os
5. https://paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/tech-briefs/techbrief-user-id.pdf

CIS Controls:

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.

2.2 Ensure that WMI probing is disabled (Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

By default, WMI probing 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 security log monitoring, mitigates this risk.

Audit:

Navigate to `Device > User Identification > User Mapping > Palo Alto Networks User ID Agent Setup > Client Probing`.

Verify that `Enable Probing` is not checked.

Remediation:

Navigate to `Device > User Identification > User Mapping > Palo Alto Networks User ID Agent Setup > Client Probing`.

Set `Enable Probing` so it is unchecked.

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.

Default Value:

Not configured

References:

1. "R7-2014-16: Palo Alto Networks User-ID Credential Exposure" - http://bit.ly/1GcbmD4
2. "Best Practices for Securing User-ID Deployments" - https://live.paloaltonetworks.com/docs/DOC-7912
3. "User-ID Best Practices - PAN-OS 5.0, 6.0" - https://live.paloaltonetworks.com/docs/DOC-6591

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

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

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 on an untrusted interface.

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.

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.

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" - http://bit.ly/1GcbmD4
3. "Best Practices for Securing User-ID Deployments" - https://live.paloaltonetworks.com/docs/DOC-7912
4. "User-ID Best Practices - PAN-OS 5.0, 6.0" - https://live.paloaltonetworks.com/docs/DOC-6591

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

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

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 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.

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`.

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`.

Default Value:

Not configured

References:

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

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services 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 (Scored)

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.

Audit:

Navigate to `Active Directory Users and Computers`.

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 - PAN-OS 5.0, 6.0” - https://live.paloaltonetworks.com/docs/DOC-6591
3. “Configure User Mapping Using the Windows User-ID Agent” - https://www.paloaltonetworks.com/documentation/61/pan-os/pan-os/user-id/configure-user-mapping-using-the-windows-user-id-agent
4. “Configure User Mapping Using the PAN-OS Integrated User-ID Agent” - https://www.paloaltonetworks.com/documentation/61/pan-os/pan-os/user-id/configure-user-mapping-using-the-pan-os-integrated-user-id-agent.html

CIS Controls:

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 (Scored)

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

CIS Controls:

5 Controlled Use of Administration Privileges
Controlled Use of Administration Privileges

2.7 Ensure remote access capabilities for the User-ID service account are forbidden. (Not Scored)

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. https://community.rapid7.com/docs/DOC-2881

CIS Controls:

16 Account Monitoring and Control
Account Monitoring and Control

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

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 > 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 > Services > Services Features > Service Route Configuration > Customize.

Click on the protocol in use (IPv4and/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

CIS Controls:

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 (Scored)

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

Audit:

Navigate to `Device > High Availability > General`.

Click `General`. Click `Data Link (HA2)`. Verify the correct interface is selected. Verify the `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 > General`.

Click `General`. Click `Data Link (HA2)`. Select the correct interface . Select the `protocol (IPv4 or IPv6)`. Select the correct Transport. Set the `Enable Session Synchronization` box to be checked .

`Save Configuration`.

Default Value:

Not Configured

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

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.

Audit:

To verify Link Monitoring from GUI:

Navigate to `Device > High Availability > Link and Path Monitoring`. Click `Link Monitoring`.

Verify the correct interfaces are in the `Link Group` and `Group Failure Conditions`

Click `Link Monitoring`.

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`.

Click `Path Monitoring`.

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

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

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.

Audit:

To ensure `Active/Passive Settings` are configured correctly:

Navigate to `Device > High Availability > 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 > 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. https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/high-availability

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 (Scored)

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 7.0 (English) for High Availability” - https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/high-availability

CIS Controls:

12 Boundary Defense
Boundary Defense

4.2 Ensure 'Applications and Threats Update Schedule' is set to download and install updates daily (Scored)

Profile Applicability:

- Level 1

Description:

Set the Applications and Threats Update Schedule to download and install updates daily.

Rationale:

New Applications and Threats file versions may be released at any time. With a daily 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`.

Remediation:

Navigate to `Device > Dynamic Updates > Application and Threats Update Schedule`.

Set `Action` to `Download and Install`.

Set `Recurrence` to `Daily`.

Default Value:

Not Configured

References:

1. “Tips for Managing Content Updates” - https://live.paloaltonetworks.com/docs/DOC- 1578
2. “PAN-OS Administrator's Guide 7.0 (English) for High Availability” - https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/high-availability

CIS Controls:

12 Boundary Defense
Boundary Defense

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 about 15 minutes.

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 (Scored)

Profile Applicability:

- Level 1

Description:

Increase WildFire file size limits to the maximum file size supported by the environment. An organization with bandwidth constraints or heavy usage of unique files under a supported file type may require lower settings.

Rationale:

Increasing file size limits allows the devices to forward more files for WildFire analysis. This increases the chances of identifying, and later preventing, threats in larger files.

Audit:

Navigate to `Device > Setup > WildFire`.

Click the `General Settings` edit icon.

Verify the maximum size for each file type.

Remediation:

Navigate to `Device > Setup > WildFire`.

Click the `General Settings` edit icon.

Set the maximum size for each file type.

Default Value:

Not Configured

References:

1. “WildFire Administrator's Guide 7.0 (English)” - https://www.paloaltonetworks.com/documentation/70/wildfire/wf_admin
2. “How to Configure WildFire” - https://live.paloaltonetworks.com/docs/DOC-3252

CIS Controls:

8.5 Deploy Network-based Anti-malware Tools
Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.

5.2 Ensure forwarding is enabled for all applications and file types in WildFire file blocking profiles (Scored)

Profile Applicability:

- Level 1

Description:

Set Applications and File Types fields to any in WildFire file blocking profiles. With a WildFire license, seven file types are supported, while only PE (Portable Executable) files are supported without a license. For web traffic, the action "continue-and-forward" can be selected. This still forwards the file to the Wildfire service, but also presents the end user with a confirmation message before they receive the file.
If there is a "continue-and-forward" rule, there should still be an "any traffic / any application / forward" rule after that in the list.

Rationale:

Selecting 'Any' application and file type ensures WildFire is analyzing as many files as possible.

Audit:

Navigate to `Objects > Security Profiles > File Blocking`.

Verify an appropriate rule exists with `Applications` set to `any`, `File Type` set to `any`, and `Action` set to `forward`.

Remediation:

Navigate to `Objects > Security Profiles > File Blocking`.

Set a rule so that `Applications` is set to `any`, `File Type` is set to `any`, and `Action` is set to `forward`.

Default Value:

Not Configured

References:

1. 7.0 WF Admin guide - https://www.paloaltonetworks.com/documentation/70/wildfire/wf_admin

CIS Controls:

8.5 Deploy Network-based Anti-malware Tools

Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.

5.3 Ensure a WildFire file blocking profile is enabled for all security policies allowing Internet traffic flows (Scored)

Profile Applicability:

- Level 1

Description:

Apply a WildFire file blocking profile to all security policies allowing Internet traffic flows. In the following example, the "WildFire" blocking profile is included in the "Inside to Outside" profile group. In a production setting, both inbound and outbound traffic should be inspected and have a Wildfire blocking policy applied.

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 industrywide is roughly 40-60% effective. In a targeted attack, the success of signature-based-only analysis drops even further.

Audit:

To verify File Blocking Profile:

Navigate to `Objects > Security Profiles > File Blocking > File Blocking Profile`.

To verify File Blocking Rules:

Navigate to `Policies > Security > Security Policy Rule > Actions > Profile Setting > File Blocking`.

Verify a WildFire file blocking profile exists with `Source Zone INSIDE`, `Address any`, and `User any`; with `Destination Zone OUTSIDE`, `Address any`, `Service any`, and `Application` set to all denied applications; and with `Action` set to `Deny`.

Verify a WildFire file blocking profile exists with `Source Zone INSIDE`, `Address any`, and `User any`; with `Destination Zone OUTSIDE`, `Address any`, `Application any`, and `Service` set to all denied service ports; and with `Action` set to `Deny`.

Remediation:

To Set File Blocking Profile:

Navigate to `Objects > Security Profiles > File Blocking > File Blocking Profile`.

To Set File Blocking Rules:

Navigate to `Policies > Security > Security Policy Rule > Actions > Profile Setting > File Blocking`.

Set a WildFire file blocking profile with `Source Zone INSIDE`, `Address any`, and `User any`; with `Destination Zone OUTSIDE`, `Address any`, `Service any`, and `Application` set to all denied applications; and with `Action` set to `Deny`.

Set a WildFire file blocking profile with `Source Zone INSIDE`, `Address any`, and `User any`; with `Destination Zone OUTSIDE`, `Address any`, `Application any`, and `Service` set to all denied service ports; and with `Action` set to `Deny`.

Default Value:

Not Configured

References:

1. 7.0 WF Admin guide - https://www.paloaltonetworks.com/documentation/70/wildfire/wf_admin

CIS Controls:

8.5 Deploy Network-based Anti-malware Tools
Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.

5.4 Ensure forwarding of decrypted content to WildFire is enabled (Scored)

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.

Default Value:

Not Configured

References:

1. "WildFire Fails Forwarding File to Cloud for Encrypted Traffic" - https://live.paloaltonetworks.com/docs/DOC-6845
2. 7.0 WF Admin guide - https://www.paloaltonetworks.com/documentation/70/wildfire/wf_admin

CIS Controls:

12.5 Design Network Perimeters To Leverage Proxy

Design and implement network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server. The proxy should support decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a black list, and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites. Organizations should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter.

5.5 Ensure all WildFire session information settings are enabled (Scored)

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:

Not Configured

References:

1. "WildFire Administrator's Guide 6.1 (English)" - https://live.paloaltonetworks.com/docs/DOC-8251

CIS Controls:

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.

8.5 Deploy Network-based Anti-malware Tools

Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.

5.6 Ensure alerts are enabled for malicious files detected by WildFire (Scored)

Profile Applicability:

- Level 1

Description:

Configure WildFire to send an alert when a malicious 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.

Remediation:

From GUI: `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: `Name, Display Name, Syslog Server, Transport, Port, Format, Facility`

Click `OK`.

Click `Commit` to save the configuration

Configure the SMTP Server: `Name, Display Name, From, To, Additional Recipients, Gateway IP or Hostname` Click `OK` Click `Commit` to save the configuration

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 6.1 (English)" - https://live.paloaltonetworks.com/docs/DOC-8251

CIS Controls:

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.

8.5 Deploy Network-based Anti-malware Tools
Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.

5.7 Ensure 'WildFire Update Schedule' is set to download and install updates every 15 minutes (Scored)

Profile Applicability:

- Level 1

Description:

Set the WildFire update schedule to download and install updates every 15 minutes.

Rationale:

WildFire definitions may contain signatures to block immediate, active threats to the environment. With a 15 minute update schedule, the firewall can ensure threats with new definitions are quickly mitigated.

Audit:

Navigate to `Device > Dynamic Updates > WildFire Update Schedule`.

Verify that `Action` is set to `Download and Install`.

Verify that `Recurrence` is set to `Every 15 Minutes`.

Remediation:

Navigate to `Device > Dynamic Updates > WildFire Update Schedule`.

Set `Action` to `Download and Install`.

Set `Recurrence` to `Every 15 Minutes`.

Default Value:

Not Configured

References:

1. “WildFire Administrator's Guide 6.1 (English)” - https://live.paloaltonetworks.com/docs/DOC-8251
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

4. “PAN-OS Administrator's Guide 6.1 (English)” - https://live.paloaltonetworks.com/docs/DOC-8246

CIS Controls:

12 Boundary Defense
Boundary Defense

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 at least one antivirus profile is set to block on all decoders except 'imap' and 'pop3' (Scored)

Profile Applicability:

- Level 1

Description:

Configure at least one antivirus profile to a value of 'block' for all decoders except imap and pop3 under both Action and WildFire Action. 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 at least one antivirus profile has all decoders except `imap` and `pop3` set to `block` for both `Action` and `Wildfire Action`, and that the `imap` and `pop3` decoders are set to `alert` for both `Action` and `Wildfire Action`.

Remediation:

Navigate to `Objects > Security Profiles > Antivirus.`

Set at least one antivirus profile to have all decoders except `imap` and `pop3` set to `block` for both `Action` and `Wildfire Action`, and the `imap` and `pop3` decoders set 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

CIS Controls:

8.5 Deploy Network-based Anti-malware Tools
Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.

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

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.

Audit:

Navigate to `Objects > Security Profiles > Antivirus Policies > Security`.

Verify there is an `Antivirus profile` applied to all security policies passing traffic - regardless of protocol.

Verify each Decoder contains `Action` set to Block and `Wildfire Action` set to Block.

Verify the `Source Zone` is INSIDE and `Source Address` is ANY.

Verify the `Destination Zone` is OUTSIDE and `Destination Address` is ANY.

Verify `Application` is ANY.

Verify `Service` is ANY.

Verify `Action` is checked.

Verify `Profile` is Block All-AV

Remediation:

Navigate to `Objects > Security Profiles > Antivirus Policies > Security`.

Set an `Antivirus profile` for all security policies passing traffic - regardless of protocol.

Ensure each Decoder contains `Action` set to Block and `Wildfire Action` set to Block.

Set the `Source Zone` to INSIDE and `Source Address` to ANY.

Set the `Destination Zone` to OUTSIDE and `Destination Address` to ANY.

Set `Application` to ANY.

Set `Service` to ANY.

Set `Action` to checked.

Set `Profile` to Block All-AV.

CIS Controls:

8.5 Deploy Network-based Anti-malware Tools
Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.

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

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 `Block Action` 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 `Block Action` on `any Severity` level, `any Category`, and `any Threat Name`.

Default Value:

Not Configured

References:

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

CIS Controls:

8.5 Deploy Network-based Anti-malware Tools

Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.

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

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 the anti-spyware profile, under its `DNS Signatures` tab, verify that `Action on DNS queries` is set to `sinkhole`.

Verify the '`Sinkhole IPv4`' IP address is correct.

Verify the '`Sinkhole IPv6`' IP address is correct.

Remediation:

Navigate to `Objects > Security Profiles > Anti-Spyware`.

Within the anti-spyware profile, under its `DNS Signatures` tab, set `Action on DNS queries` to `sinkhole`.

Set '`Sinkhole IPv4`' to the correct IP address.

Set '`Sinkhole IPv6`' to the correct IP address.

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 Version 7.0" - https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/70/pan-os/pan-os.pdf

CIS Controls:

8.5 Deploy Network-based Anti-malware Tools
Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.

8.6 Enabled DNS Query Logging
Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains.

6.5 Ensure passive DNS monitoring is set to enabled on all anti-spyware profiles in use (Scored)

Profile Applicability:

- Level 1

Description:

Enable passive DNS monitoring within all anti-spyware profiles in use.

Rationale:

Enabling passive DNS monitoring improves PAN's threat prevention and threat intelligence capabilities. This is performed without source information delivered to PAN to ensure sensitive DNS information of the organization is not compromised.

Audit:

Navigate to `Objects > Security Profiles > Anti-Spyware > Anti-Spyware profile > DNS signatures`.

For each anti-spyware profile in use, verify the `Enable Passive DNS Monitoring` box is checked under the `DNS Signatures` tab.

Remediation:

Navigate to `Objects > Security Profiles > Anti-Spyware > Anti-Spyware profile > DNS signatures`.

For each anti-spyware profile in use, set the `Enable Passive DNS Monitoring` box under the `DNS Signatures` tab to be checked.

Default Value:

Not Configured

References:

1. "What Information is Submitted to the Palo Alto Networks when Enabling the Passive DNS Feature" - https://live.paloaltonetworks.com/docs/DOC-7256
2. "PAN-OS Administrator's Guide 7.0" - https://www.paloaltonetworks.com/documentation/70/wildfire/wf_admin

CIS Controls:

8.5 Deploy Network-based Anti-malware Tools
Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.

8.6 Enabled DNS Query Logging
Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains.

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

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

CIS Controls:

8.5 Deploy Network-based Anti-malware Tools
Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.

6.7 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 (Scored)

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.

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.

References:

1. “Threat Prevention Deployment Tech Note” - https://live.paloaltonetworks.com/docs/DOC-3094
2. “PAN-OS Administrator's Guide 6.1 (English)” - https://live.paloaltonetworks.com/docs/DOC-8246

CIS Controls:

8.5 Deploy Network-based Anti-malware Tools
Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.

12.4 Deploy Network-based IPS Devices To Complement IDS Sensors
Network-based IPS devices should be deployed to complement IDS by blocking known bad signatures or the behavior of potential attacks. As attacks become automated, methods such as IDS typically delay the amount of time it takes for someone to react to an attack. A properly configured network-based IPS can provide automation to block bad traffic. When evaluating network-based IPS products, include those using techniques other than signature-based detection (such as virtual machine or sandbox-based approaches) for consideration.

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

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.

Audit:

Navigate to `Policies > Security`.

Under the `Actions` tab, select `Vulnerability Protection`.

Verify either the 'Strict' or the 'Default' profile is selected.

Remediation:

Navigate to `Policies > Security`.

Under the `Actions` tab, select `Vulnerability Protection`.

Set it to use either the 'Strict' or the 'Default' profile.

Default Value:

Not Configured

References:

1. “Threat Prevention Deployment Tech Note” - https://live.paloaltonetworks.com/docs/DOC-3094
2. “PAN-OS Administrator's Guide 6.1 (English)” - https://live.paloaltonetworks.com/docs/DOC-8246

CIS Controls:

8.5 Deploy Network-based Anti-malware Tools
Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.

12.3 Deploy Network-based IDS Sensors on DMZ Systems
Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.

6.9 Ensure that PAN-DB URL Filtering is used (Scored)

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".

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

CIS Controls:

7.6 Deploy, Use, And Maintain Network-based URL Filters
The organization shall maintain and enforce network based URL filters that limit a system's ability to connect to websites not approved by the organization. The organization shall 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. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.

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

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, malware, phishing, and proxy-avoidance-and-anonymizers.

Rationale:

Certain URL categories pose a technology-centric threat, such as malware, phishing, hacking, and proxy-avoidance-and-anonymizers. 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.

Audit:

Navigate to `Objects > Security Profiles > URL Filtering`.

Verify that all URL categories designated by the organization are listed in `Block Categories` or `Override Categories`.

Remediation:

Navigate to `Objects > Security Profiles > URL Filtering`.

Set a URL filter so that all URL categories designated by the organization are listed in `Block Categories` or `Override Categories`.

Default Value:

Not Configured

References:

1. "PAN-OS Administrator's Guide 6.1 (English)" - https://live.paloaltonetworks.com/docs/DOC-8246

CIS Controls:

7.6 Deploy, Use, And Maintain Network-based URL Filters

The organization shall maintain and enforce network based URL filters that limit a system's ability to connect to websites not approved by the organization. The organization shall 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. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.

6.11 Ensure that access to every URL is logged (Scored)

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.

Audit:

Navigate to `Objects > Security Profiles > URL Filtering`.

Verify that the `Allow Categories` column is blank.

Remediation:

Navigate to `Objects > Security Profiles > URL Filtering`.

Set the `Allow Categories` column so that it is blank.

Default Value:

Not Configured

References:

1. "PAN-OS Administrator's Guide 6.1 (English)" - https://live.paloaltonetworks.com/docs/DOC-8246

CIS Controls:

7.4 Log All URL Requests From Systems
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 all HTTP Header Logging options are enabled (Scored)

Profile Applicability:

- Level 1

Description:

Enable all options (User-Agent, Referer, 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 Referer 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.

Audit:

Navigate to `Objects > Security Profiles > URL Filtering > URL Filtering Profile > Settings`.

Verify `Log container page only` box is un-checked

Verify `User-Agent` box is checked

Verify `Referer` box is checked

Verify `X-Forwarded-For` box is checked

Remediation:

Navigate to `Objects > Security Profiles > URL Filtering > URL Filtering Profile > Settings`.

Un-check `Log container page only`

Check the `User-Agent` box

Check the `Referer` box

Check the `X-Forwarded-For` box

Default Value:

Not Configured

References:

1. "PAN-OS Administrator's Guide 6.1 (English)" - https://live.paloaltonetworks.com/docs/DOC-8246

CIS Controls:

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.

7.4 Log All URL Requests From Systems
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.

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

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.

Audit:

To Verify URL Filtering:

Navigate to `Policies > Security > Security Profiles > URL Filtering`.

Navigate to `Objects > Security Profiles > URL Filtering`.

Verify there is a URL Filtering profile applied to:

SOURCE: Name: Inside to Outside Zone: INSIDE Address: Any DESTINATION: Zone: OUTSIDE Address: ANY Application: ANY Service: ANY

Remediation:

To Set URL Filtering:

Navigate to `Policies > Security > Security Profiles > URL Filtering`.

Navigate to `Objects > Security Profiles > URL Filtering`.

Ensure there is a URL Filtering profile set to:

SOURCE: Name: Inside to Outside Zone: INSIDE Address: Any DESTINATION: Zone: OUTSIDE Address: ANY Application: ANY Service: ANY

Default Value:

Not Configured

References:

1. "PAN-OS Administrator's Guide 6.1 (English)" - https://live.paloaltonetworks.com/docs/DOC-8246

CIS Controls:

7.6 Deploy, Use, And Maintain Network-based URL Filters
The organization shall maintain and enforce network based URL filters that limit a system's ability to connect to websites not approved by the organization. The organization shall 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. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.

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

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.

Configure a Data Pattern with the following values:

CC# - 10

SSN# - 20

SSN# (without dash) – 1

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:

From GUI:

Navigate to `Objects > Security Profiles > Data Patterns`.

Verify an appropriate Data Pattern has been created with CC# set to `10`, SSN# set to `20`, and SSN# (without dash) set to `1`.

Navigate to `Objects > Security Profiles > Data Filtering`.

Verify an appropriate Data Filtering Profile has been created: Data Pattern: `CC-and-SS-Weight` Applications: `ANY` File Types: `ANY` Direction: `Both` Alert Threshold: `20` Block Threshold: `0`

Remediation:

From GUI:

Navigate to `Objects > Security Profiles > Data Patterns`.

Create an appropriate Data Pattern with CC# set to `10`, SSN# set to `20`, and SSN# (without dash) set to `1`.

Navigate to `Objects > Security Profiles > Data Filtering`.

Create an appropriate Data Filtering Profile: Data Pattern: `CC-and-SS-Weight` Applications: `ANY` File Types: `ANY` Direction: `Both` Alert Threshold: `20` Block Threshold: `0`

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 6.1 (English)" - https://live.paloaltonetworks.com/docs/DOC-8246

CIS Controls:

13.3 Use Automated Tools On Network Perimeters For Sensitive Information Detection
Deploy an automated tool on network perimeters that monitors for sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.

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

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:

Audit:

From GUI: Navigate to `Objects > Security Profiles > Data Filtering`.

Verify a Data Filtering Profile exists: Applies to all security policies allowing traffic from Internet The Shared and Data Capture boxes are checked Data Pattern is `CC-and-SS-Weight` Applications are `Any` File Types are `Any` Direction is `Both` Alert Threshold is `20` Block Threshold is `0`

Verify a Data Threshold Profile is applied to all Security Policies permitting traffic to the Internet.

Remediation:

From GUI:

Navigate to `Objects > Security Profiles > Data Filtering`

Create a Data Filtering Profile: Applies to all security policies allowing traffic from Internet `Check` the Shared and Data Capture boxes Data Pattern set to `CC-and-SS-Weight` Applications set to `Any` File Types set to `Any` Direction set to `Both` Alert Threshold set to `20` Block Threshold set to `0`

Configure a Data Threshold Profile to be applied to all Security Policies permitting traffic to the Internet.

Default Value:

Not Configured

References:

1. “PAN-OS Administrator's Guide 6.1 (English)” - https://live.paloaltonetworks.com/docs/DOC-8246

CIS Controls:

13.3 Use Automated Tools On Network Perimeters For Sensitive Information Detection
Deploy an automated tool on network perimeters that monitors for sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.

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

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.

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 new sessions per second maximum for each platform:

PA-200 = 1,000 CPS

PA-500 = 7,500 CPS

PA-2000 series = 15,000 CPS

PA-3000 series = 50,000 CPS

PA-5000 series = 120,000 CPS

PA-7050 = 720,000 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.

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).

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)

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

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

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.

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).

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

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

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.

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`.

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`.

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. "PAN-OS Administrator's Guide 6.1 (English)" - https://live.paloaltonetworks.com/docs/DOC-8246

6.19 Ensure all zones have Zone Protection Profiles that drop specially crafted packets (Scored)

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.

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. “PAN-OS Administrator's Guide 6.1 (English)” - https://live.paloaltonetworks.com/docs/DOC-8246

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 (Scored)

Profile Applicability:

- Level 1

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. 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.

Audit:

Navigate to `Policies > Security`.

Verify a Security Policy exists with: Source: `Zone` set to `OUTSIDE` `Address` set to `any` `Destination` Destination: `Zone` set to `DMZ` `Address` set to `Application` set to `web-browsing` `Service` set to `application-default`

Remediation:

Navigate to `Policies > Security`.

Set a Security Policy with: Source: `Zone` set to `OUTSIDE` `Address` set to `any` `Destination` Destination: `Zone` set to `DMZ` `Address` set to `Application` set to `web-browsing` `Service` set to `application-default`

Default Value:

Not Configured

References:

1. “PAN-OS Administrator's Guide 6.1 (English)” - https://live.paloaltonetworks.com/docs/DOC-8246

CIS Controls:

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 (Scored)

Profile Applicability:

- Level 1

Description:

Create security policies specifying application-default for the Service setting, or 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`.

Verify a Security Policy exists with:

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

Destination: `Zone` set to `DMZ Address` set to `<DMZ IP Address> Application` set to `web-browsing Service` set to `application-default` and NOT to `any`

Remediation:

Navigate to `Policies > Security`.

Set a Security Policy that has:

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

Destination: `Zone` set to `DMZ Address` set to `<DMZ IP Address>` `Application` set to `web-browsing` `Service` set to `application-default` and NOT to `any`

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 7.0" - https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os.html

7.3 Ensure 'Security Policy' denying any/all traffic exists at the bottom of the security policies ruleset (Scored)

Profile Applicability:

- Level 2

Description:

EXTREME CAUTION MUST BE USED BEFORE IMPLEMENTING THIS RECOMMENDATION, AS CERTAIN TRAFFIC PERMITTED BY DEFAULT WILL BE DENIED UNLESS SPECIFICALLY ALLOWED. Create a security rule at the bottom of the security policies ruleset denying any traffic, regardless of source, destination, or application. Ensure this policy is set to log at session end, just before pre-defined intrazone-default and interzone-default rules.

Rationale:

In incident response, logging denied traffic is often just as important as logging permitted traffic. The logs for denied traffic can be used to establish a pattern of failed attack attempts before the final attack succeeds. This can be used in attribution and identification of the attacker, but can also be used to help identify which defenses need shoring up to defend against future attacks. Viewing denied traffic can also be useful for understanding how security policies are affecting traffic.

Palo Alto firewalls do not log denied traffic by default. Therefore, to acquire visibility to denied traffic, a “deny and log” policy must be created at the end of the security policy ruleset.

Audit:

Navigate to `Policies > Security`.

Verify a Security Policy exists with: Name set to '`Deny and Log Any`' Source: `Zone` set to `Any Address` set to A`ny` Destination: `Zone` set to `Any Address` set to `Any Application` set to `Any Service` set to `Any Action`set to `Block Profile` set to `None`

Remediation:

Navigate to `Policies > Security`.

Set a Security Policy with: Name set to 'Deny and Log Any' Source: Zone set to Any Address set to Any Destination: Zone set to Any Address set to Any Application set to Any Service set to Any Action set to Block Profile set to None

Default Value:

Not Configured

References:

1. "Dynamic Protocols on Palo Alto Networks Devices that Do Not Require Security Policies to Operate" - https://live.paloaltonetworks.com/docs/DOC-8114
2. "Security Policy Guidelines" - https://live.paloaltonetworks.com/docs/DOC-3469

CIS Controls:

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.

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 (Scored)

Profile Applicability:

- Level 1

Description:

Configure SSL Forward Proxy for all traffic destined to the Internet. Include all categories except financial-services and health-and-medicine.

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.

Audit:

Navigate to `Policies > Decryption`.

Verify `SSL Forward Proxy` is set for all traffic destined to the Internet. Include all categories except financial-services and health-and-medicine.

Remediation:

Navigate to `Policies > Decryption`.

Set `SSL Forward Proxy` for all traffic destined to the Internet. Include all categories except financial-services and health-and-medicine.

Default Value:

Not Configured

References:

1. “How to Implement SSL Decryption” - https://live.paloaltonetworks.com/docs/DOC- 1412
2. “PAN-OS Administrator's Guide 6.1 (English)” - https://live.paloaltonetworks.com/docs/DOC-8246

CIS Controls:

12.5 Design Network Perimeters To Leverage Proxy
Design and implement network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server. The proxy should support decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a black list, and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites. Organizations should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter.

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

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.

Audit:

Navigate to `Policies > Decryption`.

Verify `SSL Inbound Inspection` is set appropriately for all untrusted traffic destined for servers using SSL or TLS.

Remediation:

Navigate to `Policies > Decryption`.

Set `SSL Inbound Inspection` appropriately for all untrusted traffic destined for servers using SSL or TLS.

Default Value:

Not Configured

CIS Controls:

12.5 Design Network Perimeters To Leverage Proxy
Design and implement network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server. The proxy should support decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a black list, and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other

sites. Organizations should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter.

8.3 Ensure that the Certificate used for Decryption is Trusted (Not Scored)

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. There are two 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. A 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 members 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 > Setup > Certificate Management > Certificates`.

Verify the Certificate Profile needed for the SSL Forward Proxy:

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

Verify that the decryption profile includes the settings described in the SSL Forward Proxy guidance in this document:

Navigate to `Objects > Decryption Profile`.

Verify that the Decryption Policy is applied to the appropriate interfaces and has the categories assigned to it that comply with your organization's internal policies, regulatory requirements and legal requirements.

Navigate to `Policies > Decryption`.

Source: all internal user subnets

Destination: all target zones (typically this is the public internet)

Excluded URL categories: include Health Care, Personal Banking and any other category that exposes PII, PHI or that exposes any information that might be described in your organization's internal policies, regulatory framework, privacy requirements or legal requirements as protected.

Decryption Policy Rule: include the SSL Forward Proxy defined above, and the Decryption Profile defined above

Remediation:

Set the CA Certificate(s):

Navigate to `Device > Setup > Certificate Management > Certificates`.

Set the Certificate Profile needed for the SSL Forward Proxy:

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

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

Navigate to `Objects > Decryption Profile`.

Set the Decryption Policy to be applied to the appropriate interfaces and to have the categories assigned to it that comply with your organization's internal policies, regulatory requirements and legal requirements.

Navigate to `Policies > Decryption`.

Source: all internal user subnets.

Destination: all target zones (typically this is the public internet).

Excluded URL categories: include Health Care, Personal Banking and any other category that exposes PII, PHI or that exposes any information that might be described in your organization's internal policies, regulatory framework, privacy requirements or legal requirements as protected.

Decryption Policy Rule: include the SSL Forward Proxy defined above, and the Decryption Profile defined above.

Default Value:

Decryption is not enabled by default.

References:

1. https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Implement-and-Test-SSL-Decryption/ta-p/59719
2. https://www.paloaltonetworks.com/documentation/61/pan-os/pan-os/certificate-management
3. https://live.paloaltonetworks.com/t5/Management-Articles/SSL-certificates-resource-list/ta-p/53068
4. http://palo-alto.wikia.com/wiki/Certificates

CIS Controls:

12.5 Design Network Perimeters To Leverage Proxy
Design and implement network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server. The proxy should support decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a black list, and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites. Organizations should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter.

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Device Setup**		
1.1	**General Settings**		
1.1.1	Ensure 'Login Banner' is set (Scored)	☐	☐
1.1.2	Ensure 'Enable Log on High DP Load' is enabled (Scored)	☐	☐
1.2	**Management Interface Settings**		
1.2.1	Ensure 'Permitted IP Addresses' is set to those necessary for device management (Scored)	☐	☐
1.2.2	Ensure 'Permitted IP Addresses' is set for all management profiles where SSH, HTTPS, or SNMP is enabled (Scored)	☐	☐
1.2.3	Ensure HTTP and Telnet options are disabled for the Management Interface (Scored)	☐	☐
1.2.4	Ensure valid certificate is set for browser-based administrator interface (Not Scored)	☐	☐
1.3	**Minimum Password Requirements**		
1.3.1	Ensure 'Minimum Password Complexity' is enabled (Scored)	☐	☐
1.3.2	Ensure 'Minimum Length' is greater than or equal to 12 (Scored)	☐	☐
1.3.3	Ensure 'Prevent Password Reuse Limit' is set to 24 or more passwords (Scored)	☐	☐
1.3.4	Ensure 'Required Password Change Period' is less than or equal to 90 days (Scored)	☐	☐
1.3.5	Ensure 'Password Profiles' do not exist (Scored)	☐	☐
1.3.6	Ensure 'Minimum Uppercase Letters' is greater than or equal to 1 (Scored)	☐	☐
1.3.7	Ensure 'Minimum Lowercase Letters' is greater than or equal to 1 (Scored)	☐	☐
1.3.8	Ensure 'Minimum Numeric Letters' is greater than or equal to 1 (Scored)	☐	☐
1.3.9	Ensure 'Minimum Special Characters' is greater than or equal to 1 (Scored)	☐	☐
1.3.10	Ensure 'Block Username Inclusion' is enabled (Scored)	☐	☐
1.3.11	Ensure 'New Password Differs By Characters' is greater than or equal to 3 (Scored)	☐	☐
1.4	**Authentication Settings (for Device Mgmt)**		
1.4.1	Ensure 'Idle timeout' is less than or equal to 10 minutes for device management (Scored)	☐	☐
1.4.2	Ensure 'Failed Attempts' and 'Lockout Time' for	☐	☐

	Authentication Profile are properly configured (Scored)		
1.5	**SNMP Polling Settings**		
1.5.1	Ensure 'V3' is selected for SNMP polling (Scored)	☐	☐
1.6	**Device Services Settings**		
1.6.1	Ensure 'Verify Update Server Identity' is enabled (Scored)	☐	☐
1.6.2	Ensure redundant NTP servers are configured appropriately (Scored)	☐	☐
1.6.3	Ensure that the certificate securing Remote Access VPNs is valid (Not Scored)	☐	☐
2	**User Identification**		
2.1	Ensure that IP addresses are mapped to usernames (Scored)	☐	☐
2.2	Ensure that WMI probing is disabled (Scored)	☐	☐
2.3	Ensure that User-ID is only enabled for internal trusted interfaces (Scored)	☐	☐
2.4	Ensure that 'Include/Exclude Networks' is used if User-ID is enabled (Scored)	☐	☐
2.5	Ensure that the User-ID Agent has minimal permissions if User-ID is enabled (Scored)	☐	☐
2.6	Ensure that the User-ID service account does not have interactive logon rights (Scored)	☐	☐
2.7	Ensure remote access capabilities for the User-ID service account are forbidden. (Not Scored)	☐	☐
2.8	Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones (Scored)	☐	☐
3	**High Availability**		
3.1	Ensure a fully-synchronized High Availability peer is configured (Scored)	☐	☐
3.2	Ensure 'High Availability' requires Link Monitoring and/or Path Monitoring (Scored)	☐	☐
3.3	Ensure 'Passive Link State' and 'Preemptive' are configured appropriately (Scored)	☐	☐
4	**Dynamic Updates**		
4.1	Ensure 'Antivirus Update Schedule' is set to download and install updates hourly (Scored)	☐	☐
4.2	Ensure 'Applications and Threats Update Schedule' is set to download and install updates daily (Scored)	☐	☐
5	**Wildfire**		
5.1	Ensure that WildFire file size upload limits are maximized (Scored)	☐	☐
5.2	Ensure forwarding is enabled for all applications and file types in WildFire file blocking profiles (Scored)	☐	☐
5.3	Ensure a WildFire file blocking profile is enabled for all security policies allowing Internet traffic flows (Scored)	☐	☐

5.4	Ensure forwarding of decrypted content to WildFire is enabled (Scored)	☐	☐
5.5	Ensure all WildFire session information settings are enabled (Scored)	☐	☐
5.6	Ensure alerts are enabled for malicious files detected by WildFire (Scored)	☐	☐
5.7	Ensure 'WildFire Update Schedule' is set to download and install updates every 15 minutes (Scored)	☐	☐
6	**Security Profiles**		
6.1	Ensure at least one antivirus profile is set to block on all decoders except 'imap' and 'pop3' (Scored)	☐	☐
6.2	Ensure a secure antivirus profile is applied to all relevant security policies (Scored)	☐	☐
6.3	Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats (Scored)	☐	☐
6.4	Ensure DNS sinkholing is configured on all anti-spyware profiles in use (Scored)	☐	☐
6.5	Ensure passive DNS monitoring is set to enabled on all anti-spyware profiles in use (Scored)	☐	☐
6.6	Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the Internet (Scored)	☐	☐
6.7	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 (Scored)	☐	☐
6.8	Ensure a secure Vulnerability Protection Profile is applied to all security rules allowing traffic (Scored)	☐	☐
6.9	Ensure that PAN-DB URL Filtering is used (Scored)	☐	☐
6.10	Ensure that URL Filtering uses the action of “block” or “override” on the <enterprise approved value> URL categories (Scored)	☐	☐
6.11	Ensure that access to every URL is logged (Scored)	☐	☐
6.12	Ensure all HTTP Header Logging options are enabled (Scored)	☐	☐
6.13	Ensure secure URL filtering is enabled for all security policies allowing traffic to the Internet (Scored)	☐	☐
6.14	Ensure alerting after a threshold of credit card or Social Security numbers is detected is enabled (Scored)	☐	☐
6.15	Ensure a secure Data Filtering profile is applied to all security policies allowing traffic to or from the Internet (Scored)	☐	☐
6.16	Ensure that a Zone Protection Profile with an enabled SYN Flood Action of SYN Cookies is attached to all untrusted zones (Scored)	☐	☐
6.17	Ensure that a Zone Protection Profile with tuned Flood Protection settings enabled for all flood types is attached to	☐	☐

	all untrusted zones (Scored)		
6.18	Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned, and set to appropriate actions (Scored)	☐	☐
6.19	Ensure all zones have Zone Protection Profiles that drop specially crafted packets (Scored)	☐	☐
7	**Security Policies**		
7.1	Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone (Scored)	☐	☐
7.2	Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist (Scored)	☐	☐
7.3	Ensure 'Security Policy' denying any/all traffic exists at the bottom of the security policies ruleset (Scored)	☐	☐
8	**Decryption**		
8.1	Ensure 'SSL Forward Proxy Policy' for traffic destined to the Internet is configured (Scored)	☐	☐
8.2	Ensure 'SSL Inbound Inspection' is required for all untrusted traffic destined for servers using SSL or TLS (Scored)	☐	☐
8.3	Ensure that the Certificate used for Decryption is Trusted (Not Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
3/31/17	1.0.0	Initial Release