Palo Alto Firewall Security Configuration Benchmark – v.1.1

GIAC (GSNA) Gold Certification

Author: Ryan Firth, RyanQFirth+pan@gmail.com
Advisor: Rob VandenBrink
Version 1.0 Accepted: February 13th, 2015
Latest revision (v.1.1): April 15th, 2015

Abstract

Security configuration benchmarks provide invaluable guidance when auditing, evaluating, or configuring network infrastructure devices. Contributions by CIS (Center for Internet Security), DISA (Defense Information Systems Agency), the NSA, NIST, and SANS provide benchmark guides for a variety of network devices, operating systems, and other IT equipment. It is also common for technology companies themselves to provide these guides for their products, such as Microsoft’s Security Baselines.

Although best practice recommendations are found in abundance on the Palo Alto Networks website, a single security configuration benchmark does not currently exist for Palo Alto firewalls. This paper will combine best practice guidance from Palo Alto, other reputable sources, and real-world experience to provide a comprehensive security benchmark for auditing a Palo Alto firewall running PAN-OS 6.1 software.

The intention of this paper is to produce a version 1 draft from which to start a living CIS project—the CIS Palo Alto Firewall Benchmark. Through a formal CIS benchmark project, many other experts will join in to provide input, scrutinize proposals, discuss, and ultimately settle on sound benchmark recommendations useful for a wide variety of organizations interested in securing and/or auditing their Palo Alto firewalls. Once published, the CIS Palo Alto Firewall Benchmark will supersede the recommendations in this paper.
# Table of Contents

1. **INTRODUCTION** ........................................................................................................... 5

2. **PAN-OS 6.1 BENCHMARK** ............................................................................................ 6

   2.1. **DEVICE SETUP** ....................................................................................................... 6

       2.1.1. General Settings ................................................................................................. 6

       2.1.1.1. Require an appropriate login banner ................................................................. 6

       2.1.2. Logging and Reporting Settings ........................................................................ 7

       2.1.2.1. Enable Log on High DP Load ........................................................................... 7

       2.1.3. Management Interface Settings ......................................................................... 8

       2.1.3.1. Forbid HTTP and telnet services for device management ............................... 8

       2.1.3.2. Limit Permitted IP Addresses to those necessary for device management ....... 9

       2.1.3.3. Require all interface management profiles where telnet, SSH, HTTP, HTTPS, or SNMP is enabled to permit only IP addresses necessary for device management ................... 10

       2.1.4. Minimum Password Requirements ..................................................................... 11

       2.1.4.1. Require minimum password complexity rules .................................................. 11

       2.1.4.2. Forbid the use of password profiles ................................................................. 13

       2.1.5. Authentication Settings (For Device Management) ............................................ 14

       2.1.5.1. Require an idle timeout value of 10 minutes for device management .............. 14

       2.1.5.2. Forbid the use of Authentication Settings for Failed Attempts and Lockout Time. Require an Authentication Profile with Failed Attempts to 3, and lockout time of 15 minutes applied to all but one Superuser account .......................................................... 15

       2.1.6. SNMP Polling ....................................................................................................... 17

       2.1.6.1. Require SNMP V3 (If SNMP polling is configured) .......................................... 17

       2.1.7. Device Services .................................................................................................... 18

       2.1.7.1. Require verification of update server identity ...................................................... 18

       2.1.7.2. Require redundant NTP services ..................................................................... 19

2.2. **USER IDENTIFICATION** ............................................................................................. 21

   2.2.1. User Identification - General ............................................................................... 21

       2.2.1.1. Require IP-to-username mapping for user traffic ............................................. 21

       2.2.2. Securing User-ID Probing ................................................................................... 22

       2.2.2.1. Disable WMI probing if not required ................................................................. 22

       2.2.2.2. Forbid User-ID on external and other non-trusted zones .................................. 24

       2.2.2.3. Require the use of User-ID’s Include/Exclude Networks section, if User-ID is enabled. Include only trusted internal networks ............................................................... 25

   2.2.3. User-ID Agent ......................................................................................................... 26
2.2.3.1. Require a dedicated service account for User-ID with minimal permissions (If a User-ID Agent or Integrated User-ID Agent is utilized) ............................................................................................................................ 26

2.2.3.2. Forbid Interactive Login rights for the User-ID service account .................................................................................................................. 27

2.2.3.4. Require security policies restricting User-ID Agent traffic from crossing into untrusted zones ................................................................. 28

2.3. HIGH AVAILABILITY ........................................................................................................................................................................ 30

2.3.1.1. Require a fully-synchronized High Availability peer .......................................................................................................................... 30

2.3.1.2. For High Availability, require Link Monitoring, Path Monitoring, or both .......................................................................................... 31

2.3.1.3. Forbid simultaneously enabling the Preemptive option, and configuring the Passive Link State to shutdown simultaneously. (For an HA pair) .................................................................................. 32

2.4. DYNAMIC UPDATES ........................................................................................................................................................................ 33

2.4.1. Scheduled Downloads ........................................................................................................................................................................... 33

2.4.1.1. Require the Antivirus Update Schedule is set to Download and install hourly ................................................................................. 33

2.4.1.2. Require the Applications and Threats Update Schedule is set to Download and Install Daily .................................................................. 34

2.4.1.3. Require the WildFire Update Schedule is set to Download and Install every 15 minutes ................................................................ 36

2.5. WILDFIRE .................................................................................................................................................................................................... 37

2.5.1. WildFire General Settings .................................................................................................................................................................... 37

2.5.1.1. Increase WildFire file size upload limits .............................................................................................................................................. 37

2.5.2. WildFire configuration ........................................................................................................................................................................... 38

2.5.2.1. Require WildFire File Blocking profiles to include any application, any file type, and action set to forward .......................................................................................................................... 38

2.5.2.2. Require a WildFire File Blocking profile for all security policies allowing Internet traffic flows .......................................................... 38

2.5.2.3. Require forwarding of decrypted content ........................................................................................................................................... 39

2.5.2.4. Require all WildFire Session Information Settings to be enabled ..................................................................................................... 40

2.5.3. WildFire alerting and verification ........................................................................................................................................................... 41

2.5.3.1. Require sending an alert for malware detected through WildFire ..................................................................................................... 41

2.5.3.2. Verify WildFire file submission and alerting is functioning as expected .............................................................................................. 43

2.6. SECURITY PROFILES ........................................................................................................................................................................ 45

2.6.1. Antivirus .................................................................................................................................................................................................. 45

2.6.1.1. Require an Antivirus profile configured to block on all decoders except imap and pop3 ................................................................. 45

2.6.1.2. Require a securely configured Antivirus profile applied to all applicable security policies ................................................................ 46

2.6.2. Anti-Spyware ....................................................................................................................................................................................... 48

2.6.2.1. Require an Anti-Spyware profile configured to block on all severity levels, categories, and threats ...................................................... 48

2.6.2.2. Require DNS Sinkhoking on all Anti-spyware profiles in use .......................................................................................................... 51

2.6.2.3. Require Passive DNS Monitoring enabled on all Anti-Spyware profiles in use ............................................................................. 51

2.6.2.4. Require a securely configured Anti-Spyware profile applied to all security policies permitting traffic to the Internet .............................................................................................................. 53

Author Name, email@address
2.6.3. 
Vulnerability Protection

2.6.3.1. 
Require a Vulnerability Protection profile configured to block at least high and critical vulnerabilities, and set to default on medium, low, and informational vulnerabilities.

2.6.3.2. 
Require a securely configured Vulnerability Protection Profile applied to all security policies allowing traffic.

2.6.4. 
URL Filtering

2.6.4.1. 
Require the use of PAN-DB URL Filtering

2.6.4.2. 
Require a URL Filtering profile with the action of “block” or “override” on the following categories: adult, hacking, malware, phishing, proxy-avoidance-and-anonymizers

2.6.4.3. 
Forbid a utilized URL Filtering profile with any category set to “allow”.

2.6.4.4. 
Require all HTTP Header Logging options enabled

2.6.4.5. 
Require a securely configured URL Filtering profile applied to all security policies allowing traffic to the Internet.

2.6.5. 
Data Filtering

2.6.5.1. 
Require a Data Filtering policy set to alert after a threshold of Credit Card or Social Security numbers are detected

2.6.6. 
Zone Protection profiles

2.6.6.1. 
Require a Zone Protection Profile with an enabled SYN Flood Action of SYN Cookies attached to all untrusted zones.

2.6.6.2. 
Require a Zone Protection Profile with tuned Flood Protection settings enabled for all flood types attached to all untrusted zones.

2.6.6.3. 
Require all zones have Zone Protection Profiles with all Reconnaissance Protection settings tuned and enabled, and NOT set to allow for any scan type.

2.6.6.4. 
Require all zones have Zone Protection Profiles that drop Spoofed IP address, mismatched overlapping TCP segment, Malformed, Strict Source Routing, and Loose Source Routing IP options.

2.7. 
SECURITY POLICIES

2.7.1. 
Security Policies - General

2.7.1.1. 
Require specific application policies when allowing traffic from an untrusted zone to a more trusted zone.

2.7.1.2. 
Forbid using the Service setting of any in a security policy.

2.7.1.3. 
Require a security policy denying any/all traffic at the bottom of the security policies ruleset.

2.8. 
DECRIPTION

2.8.1. 
SSL Forward Proxy

2.8.1.1. 
Require an SSL Forward Proxy policy for traffic destined to the Internet for all URL categories except financial-services and health-and-medicine.

2.8.2. 
SSL Inbound Inspection

2.8.2.1. 
Require SSL Inbound Inspection for all untrusted traffic destined for servers using SSL.

3. 
AUDIT CHECKLIST

4. 
REFERENCES
1. Introduction

This security configuration benchmark was created and tested against Palo Alto Networks’ PAN-OS 6.1 software. The recommendations herein were compiled and derived from Palo Alto Networks (PAN) documentation, knowledge base, other guidance found in the PAN Community website (https://live.paloaltonetworks.com), and practical, real-world experience. Where appropriate, guidance from well-established security organizations were incorporated, such as NIST, MITRE, and SANS.

This benchmark is intended for firewall administrators, IT auditors, and other security professionals responsible for the configuration, assessment, deployment, or management of a PAN firewall. Configuration and day-to-day management of a PAN firewall primarily occurs through the web GUI, which can be granularly controlled to provide read-only access for IT auditors. Because of this, this guide will primarily focus on configuration and auditing through the web GUI. The order of topics roughly follows the flow and logical groupings of the web interface.

Only recommendations providing a clear, practical security benefit and minimum due care are provided in this document. For example, although incorporating two-factor authentication is superior to password-only authentication, recommendations around the latter is considered minimum due care. For non-security related topics, or additional configuration information, administrator’s guides found in the documentation section of live.paloaltonetworks.com is a helpful place to start. (https://www.paloaltonetworks.com/documentation.html)

Recommendations in this benchmark are considered generally acceptable best practice for most environments. As with almost any best practices guide, careful testing and consideration should be exercised when deciding if a recommendation is appropriate for a specific environment. PAN firewalls have a flexible and powerful feature set making them useful in a wide variety of environments and situations. Therefore, creating a one size fits all security guide is not possible. IT auditors should weigh the overall design, architectural

Author Name, email@address
considerations, and other security controls in place when reporting findings based on this benchmark.

By utilizing the guidance contained in this document, you assume total responsibility of the consequences. The author, contributors, and Palo Alto Networks are not liable for any damages incurred directly or indirectly from the use of this document.

Acknowledgements:

Albert Estevez, BD Solutions Architect at Palo Alto Networks for timely feedback, coordination, validation, and support throughout the creation of this benchmark.

Others at Palo Alto Networks and the PAN and SANS communities for the support and feedback.

2. PAN-OS 6.1 Benchmark

2.1. Device Setup

2.1.1. General Settings

2.1.1.1. Require an appropriate login banner

Location:

Device > Setup > Management > General Settings

Recommendation:

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 should not contain 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.

**References:**

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

**2.1.2. Logging and Reporting Settings**

**2.1.2.1. Enable Log on High DP Load**

Location:

Author Name, email@address
Device > Setup > Management > Logging and Reporting Settings

**Recommendation:**

Enable the *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.

![Logging and Reporting Settings](image)

**Rationale:**

When the device’s packet processing load reaches 100%, a degradation in the availability of services accessed through the device can occur.

**References:**

“What is "Enable Log on High DP Load" in PAN-OS 5.0?” - [https://live.paloaltonetworks.com/docs/DOC-4075](https://live.paloaltonetworks.com/docs/DOC-4075)

**2.1.3. Management Interface Settings**

**2.1.3.1. Forbid HTTP and telnet services for device management**

**Location:**

Device > Setup > Management > Management Interface Settings

**Recommendation:**

HTTP and Telnet options should not be checked.
Rationale:

Management access over clear-text services such as telnet or HTTP could result in a compromise of administrator credentials.

References:

“What could Cause a Large Number of Auth-Fail Events in the System Logs?” - https://live.paloaltonetworks.com/docs/DOC-3703

“How to Configure In-Band Management” - https://live.paloaltonetworks.com/docs/DOC-1153

2.1.3.2. Limit Permitted IP Addresses to those necessary for device management.

Location:

Device > Setup > Management > Management Interface Settings

Recommendation:

Permit only the IP addresses necessary for management of 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 or stolen credentials.

**References:**

“Allowing Specific IP Addresses to Access the Palo Alto Network Device” - https://live.paloaltonetworks.com/docs/DOC-8042

2.1.3.3. **Require all interface management profiles where telnet, SSH, HTTP, HTTPS, or SNMP is enabled to permit only IP addresses necessary for device management.**

**Location:**

Network > Network Profiles > Interface Mgmt

**Recommendation:**

For all interface management profiles with enabled protocols providing device management, only IP addresses necessary for device management should be specified.
Rationale:

If a Permitted IP Addresses list is either not specified or too broad, an attacker may gain the ability to attempt management access from unintentional locations, such as the Internet. In the example above, if the Ping-SSH-HTTPS profile were missing a Permitted IP Addresses list, then applied to an outside interface, it may be possible for anyone on the Internet to attempt device management access. The “Require a security policy denying any/all traffic 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.

References:

“Allowing Specific IP Addresses to Access the Palo Alto Network Device” - https://live.paloaltonetworks.com/docs/DOC-8042

2.1.4. Minimum Password Requirements

2.1.4.1. Require minimum password complexity rules

Location:

Device > Setup > Management > Minimum Password Complexity

Recommendation:

Minimum Password Complexity – Enabled

Minimum Length – 12
Minimum Uppercase Letters – 1
Minimum Lowercase Letters – 1
Minimum Numeric Letters – 1
Minimum Special Characters – 1
Block Username Inclusion (including reversed) – Enabled
New Password Differs By Characters – 3
Prevent Password Reuse Limit – 24
Required Password Change Period (days) – 90

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).

References:

Author Name, email@address
“CIS Microsoft Windows Server 2012 R2 benchmark” -

“Common Weakness Enumeration CWE-255: Credentials Management” -
http://cwe.mitre.org/data/definitions/255.html


2.1.4.2. **Forbid the use of password profiles**

**Location:**
Device > Password Profiles

**Recommendation:**
Do not use password profiles.

[Image of a screen showing Password Profiles]

**Rationale:**
Password profiles override recommended settings in the *Minimum Password Complexity* section. See the section in this benchmark titled “Require minimum password complexity rules”.

**References:**
“Defining Granular Admin Role Profiles” -
https://live.paloaltonetworks.com/docs/DOC-5177
2.1.5. Authentication Settings (For Device Management)

2.1.5.1. Require an idle timeout value of 10 minutes for device management.

Location:
Device > Setup > Management > Authentication Settings

Recommendation:
Set the Idle Timeout value for device management to 10 minutes.

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

This mirrors recommendation 1.1.2.4 (Require Timeout for Login Sessions) in the CIS Cisco Firewall Benchmark v3.0.2.

References:
“CIS Cisco Firewall Benchmark v3.0.2” - https://benchmarks.cisecurity.org/en-us/?route=downloads.form.firewall.302

“How to Change the Admin Session Timeout Value” - https://live.paloaltonetworks.com/docs/DOC-5557
2.1.5.2. **Forbid the use of Authentication Settings for Failed Attempts and Lockout Time.** Require an Authentication Profile with Failed Attempts to 3, and lockout time of 15 minutes applied to all but one Superuser account.

**Locations:**

Device > Setup > Management > Authentication Settings

Device > Authentication Profile

**Recommendation:**

Do not set Failed Attempts and Lockout Time in the Authentication Settings section. Note that any Failed Attempts or Lockout Time settings within the selected Authentication Profile does not apply in the Authentication Settings section.

Instead, configure an Authentication Profile with lockout settings of 3 Failed Attempts and Lockout Time of 15 minutes.
This authentication profile should be applied to all user accounts, with the exception of one Superuser account. This account should be monitored, have an extremely secure password, and used only in very limited circumstances, such as if a primary administrator account is being continuously locked out.

**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.
2.1.6. SNMP Polling

2.1.6.1. Require SNMP V3 (If SNMP polling is configured)

**Location:**
Device > Setup > Operations > Miscellaneous > SNMP Setup

**Recommendation:**
For SNMP polling, only SNMP V3 should be used.

**Rationale:**

Author Name, email@address
SNMP V3 utilizes AES-128 encryption, message integrity, user authorization, and device authentication. SNMP V2c does not provide these security features. If an SNMP V2c community string is intercepted or otherwise obtained, an attacker could gain read access to the firewall. Note that SNMP write access is not possible.

**References:**

“How to Setup SNMPv3 Polling” - [https://live.paloaltonetworks.com/docs/DOC-4037](https://live.paloaltonetworks.com/docs/DOC-4037)


### 2.1.7. Device Services

#### 2.1.7.1. Require verification of update server identity

**Location:**

Device > Setup > Services > Services

**Recommendation:**

Enable the *Verify Update Server Identity* option.

Note that if an SSL Forward Proxy is configured to intercept the update session, this option may need to be disabled.
Rationale:

While updates are cryptographically signed, verifying the update server identity provides additional protection by ensuring update packages originate from a trusted source.

Reference:

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

2.1.7.2. Require redundant NTP services

Location:

Device > Setup > Services > Services

Recommendation:

A primary and secondary NTP server should be configured.
Enhanced Security Recommendation:

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

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.

References:


2.2. User Identification

2.2.1. User Identification - General

2.2.1.1. Require IP-to-username mapping for user traffic

Locations:

Device > User Identification
Monitor > Logs > URL Filtering
Monitor > Logs > Traffic Logs

Recommendation:

Configure appropriate settings to map IP addresses to usernames. The specifics of how to achieve IP-to-username mapping is highly dependent on the environment. This is enabled by integrating PAN firewalls with a domain controller, Exchange server, captive portal, Terminal Server, User-ID Agent, XML API, or syslog data from a variety of devices.

To validate if this recommendation has been met, look at the Source User column in the URL Filtering or Traffic logs. User traffic originating from a trusted zone should identify a username.

URL Filtering logs:

<table>
<thead>
<tr>
<th>Zone</th>
<th>URL</th>
<th>Source User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust</td>
<td></td>
<td>johndoe</td>
</tr>
</tbody>
</table>

Traffic logs:

Author Name, email@address
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.

References:

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

“User-ID Best Practices - PAN-OS 5.0, 6.0” -
https://live.paloaltonetworks.com/docs/DOC-6591

“How to Configure Group Mapping settings?” -
https://live.paloaltonetworks.com/docs/DOC-4994

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

2.2.2. Securing User-ID Probing

2.2.2.1. Disable WMI probing if not required.

Location:

Author Name, email@address
Device > User Identification > User Mapping > Palo Alto Networks User ID Agent

**Setup**

**Recommendation:**

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

![Palo Alto Networks User ID Agent Setup](image)

**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.

**References:**


2.2.2.2. **Forbid User-ID on external and other non-trusted zones**

**Location:**

Network > Network Profiles > Interface Mgmt

Network > Interfaces

**Recommendation:**

Only enable the User-ID option for interfaces that are both internal and trusted.

**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 credential theft of the account used in WMI probing.

**References:**


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

“User-ID Best Practices - PAN-OS 5.0, 6.0” -
https://live.paloaltonetworks.com/docs/DOC-6591

2.2.2.3. Require the use of User-ID’s Include/Exclude Networks section, if User-ID is enabled. Include only trusted internal networks.

Location:
Device > User Identification > User Mapping > Include/Exclude Networks

Recommendation:
If User-ID is configured, use the Include/Exclude Networks section to specify trusted, internal subnets.

<table>
<thead>
<tr>
<th>Include/Exclude Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>Internal</td>
</tr>
<tr>
<td>Guest</td>
</tr>
</tbody>
</table>

Rationale:
To help ensure only corporate assets are probed, only trusted networks should be included. Note that if an entry appears in the Include/Exclude Networks section, an implicit exclude-all-networks will take effect for all other networks. WMI probes to non-trusted subnets can result in credential theft of the account used in WMI probing.

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

Author Name, email@address
2.2.3. User-ID Agent

2.2.3.1. Require a dedicated service account for User-ID with minimal permissions (If a User-ID Agent or Integrated User-ID Agent is utilized)

Locations:

Device > User Identification > User Mapping > Server Monitoring

Windows Server 2008 or later > Active Directory Users and Computers

Recommendations:

A) 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.

B) 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 a far greater risk than if the service account were only granted minimum rights.

References:

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

“User-ID Best Practices - PAN-OS 5.0, 6.0” -
https://live.paloaltonetworks.com/docs/DOC-6591

“Configure User Mapping Using the Windows User-ID Agent” -

“Configure User Mapping Using the PAN-OS Integrated User-ID Agent” -

2.2.3.2. **Forbid Interactive Login rights for the User-ID service account**

**Location:**

Windows domain controller

**Recommendation:**

Restrict the User-ID service account from interactively logging on to a system in the Active Directory domain. Most commonly, this can be achieved through Active Directory’s Group Policy or Managed Service Accounts functions.

**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.

Author Name, email@address
Directory domain of the organization. This reduces the impact of a User-ID service account compromise.

References:

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

2.2.3.3. Forbid all remote access capabilities for the User-ID service account.

Location:
Remote access systems, such as VPN, Citrix GoToMyPC, or TeamViewer

Recommendation:
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.

References:

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

2.2.3.4. Require security policies restricting User-ID Agent traffic from crossing into untrusted zones.

Locations:

Author Name, email@address
Device > Setup > Services > Services Features > Service Route Configuration

Policies > Security

**Recommendation:**

Create security policies to deny msrpc traffic originating from the interface configured for the UID Agent service and destined to all untrusted zones. The firewall’s management interface is used by the UID Agent service by default.
Author Name, email@address

(Address object created for the UID Agent’s IP address)

Rationale:

WMI probes to non-trusted subnets can result in credential theft of the account used in WMI probing. To help ensure only corporate assets are probed, 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 future probe misconfigurations.

References:


“MSRPC traffic to unknown IP addresses on Internet originating from the Management interface” - https://live.paloaltonetworks.com/docs/DOC-8690

2.3. High Availability

2.3.1.1. Require a fully-synchronized High Availability peer

Location:

Dashboard > Widgets > System > High Availability

Recommendation:

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.

Reference:

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

2.3.1.2.  For High Availability, require Link Monitoring, Path Monitoring, or both

Location:

Device > High Availability > Link and Path Monitoring

Recommendation:

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.

References:

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

2.3.1.3. Forbid simultaneously enabling the Preemptive option, and configuring the Passive Link State to *shutdown* simultaneously. (For an HA pair)

Location:

Device > High Availability > Active/Passive Settings

Device > High Availability > Election Settings

Recommendation:
Either set the Passive Link State to shutdown, or uncheck the Preemptive option. It is preferred to disable preemption and set the Passive Link State to auto.

![Active/Passive Settings](image)

**Rationale:**

If the firewall is set both to preempt and to shut down the links on the passive firewall, a preemption loop could occur if Link and Path Monitoring is configured. This will negatively impact the availability of the firewall and network services, should a monitored failure occur.

**References:**


### 2.4. Dynamic Updates

#### 2.4.1. Scheduled Downloads

**2.4.1.1. Require the Antivirus Update Schedule is set to Download and Install hourly.**

**Location:**

Device > Dynamic Updates

**Recommendation:**

Set the Antivirus Update Schedule to Download and Install hourly.
The threshold value is highly contingent on the organization. In the event of an error in the antivirus definitions, a longer threshold value provides time for PAN to correct the faulty definition. A shorter threshold time provides more up-to-date antivirus definitions.

**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 worse-case scenario. Setting an appropriate threshold value reduces the risk of a bad definition file negatively affecting traffic.

**References:**

“Tips for Managing Content Updates” - https://live.paloaltonetworks.com/docs/DOC-1578


**2.4.1.2. Require the Applications and Threats Update Schedule is set to Download and Install Daily.**

**Location:**

Device > Dynamic Updates
**Recommendation:**

Set the Applications and Threats Update Schedule to *Download and Install* daily.

The threshold value is highly contingent on the organization. In the event of an error in an Applications and Threats version, a longer threshold value provides time for PAN to correct the faulty version. A shorter threshold time provides a more up-to-date Applications and Threats version.

**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. Setting an appropriate threshold value reduces the risk of a bad Applications and Threats file version from negatively affecting traffic.

**References:**

“Tips for Managing Content Updates” - [https://live.paloaltonetworks.com/docs/DOC-1578](https://live.paloaltonetworks.com/docs/DOC-1578)

2.4.1.3. **Require the WildFire Update Schedule is set to Download and Install every 15 minutes.**

Location:

Device > Dynamic Updates

**Recommendation:**

Set the WildFire Update Schedule to *Download and Install* every 15 minutes.

![WildFire Update Schedule](image)

**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.

**References:**

- “How to Configure WildFire” - [https://live.paloaltonetworks.com/docs/DOC-3252](https://live.paloaltonetworks.com/docs/DOC-3252)
- “Tips for Managing Content Updates” - [https://live.paloaltonetworks.com/docs/DOC-1578](https://live.paloaltonetworks.com/docs/DOC-1578)
2.5. WildFire

2.5.1. WildFire General Settings

2.5.1.1. Increase WildFire file size upload limits

Location:

Device > Setup > Wildfire > General Settings

Recommendation:

Increase WildFire file size limits to the maximum supported by the environment. An organization with bandwidth constraints or heavy usage of unique files under a supported file type may require lower settings. Devices without a WildFire license will only forward PE (Portable Executable) files for WildFire analysis.

Rationale:

Increasing file size limits will allow the device to forward more files for WildFire analysis than default settings. This increases the chances of identifying, and later preventing, threats in larger files.

References:


2.5.2. WildFire configuration

2.5.2.1. Require WildFire File Blocking profiles to include *any* application, *any* file type, and action set to *forward*

**Location:**

Objects > Security Profiles > File Blocking

**Recommendation:**

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.

![File Blocking Profile](image)

**Rationale:**

Selecting *any* application and file type ensures WildFire is analyzing as many files as possible.

**References:**


“How to Configure WildFire” - [https://live.paloaltonetworks.com/docs/DOC-3252](https://live.paloaltonetworks.com/docs/DOC-3252)

2.5.2.2. Require a WildFire *File Blocking* profile for all security policies allowing Internet traffic flows.

**Locations:**

Objects > Security Profiles > File Blocking

Author Name, email@address
Policies > Security

**Recommendation:**

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.

![File Blocking Profile](image)

**Rationale:**

Traffic matching security policies that do not include a WildFire file blocking profile will not utilize WildFire for file analysis.

**References:**

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

2.5.2.3. **Require forwarding of decrypted content**

**Location:**

Device > Setup > Content-ID > Content-ID Settings

**Recommendation:**

Author Name, email@address
Allow the firewall to forward decrypted content to WildFire by enabling the setting, *Allow forwarding of decrypted content*. Note that SSL Forward-Proxy must also be configured for this setting to take effect on inside-to-outside traffic flows.

![Content-ID Settings](image)

**Rationale:**

As encrypted Internet traffic continues to proliferate, WildFire’s ability to help protect an environment 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) *Allow forwarding of decrypted content* is enabled.

**References:**


### 2.5.2.4. Require all WildFire Session Information Settings to be enabled

**Location:**

Device > Setup > WildFire > Session Information Settings

**Recommendation:**

Under *Session Information Settings*, all options should be enabled.
### Rationale:

Permitting the firewall to send this information to WildFire creates more detailed reports, thereby making the process of tracking down potentially infected devices quicker and more efficient. This quicker reaction time could prevent an infected system from otherwise further infecting the environment. Environments with security policies restricting sending this data to the WildFire cloud can instead utilize an on-premises WildFire appliance.

### References:

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

### 2.5.3. WildFire alerting and verification

#### 2.5.3.1. Require sending an alert for malware detected through WildFire

**Location:**

Objects > Log Forwarding

Author Name, email@address
https://wildfire.paloaltonetworks.com/

Recommendation:

Configure WildFire to send an alert when a malicious file is detected. In the following example, an email will be sent upon detection of a malicious file. SNMP traps or syslog messages could be used instead, so long as an appropriate member of the IT staff is quickly made aware of the malicious file.

In addition, or instead of, configure the WildFire cloud to email alerts for malicious files. Note that the destination email address of alerts configured in the WildFire portal is tied to the logged in account, and cannot be modified. New systems added to the WildFire 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 and not flagged by the firewall’s
antivirus filter, files deemed malicious by WildFire are more likely to evade desktop antivirus products.

References:

“WildFire Email Alerts: Subscribe or Add Additional Recipients” - https://live.paloaltonetworks.com/docs/DOC-7740


2.5.3.2. Verify WildFire file submission and alerting is functioning as expected

Location:

CLI

https://wildfire.paloaltonetworks.com/wildfire/dashboard

Recommendation:

From the command line, run the command “show wildfire status”. At minimum, the Device registered field should display yes and Status set to Idle. The command “show wildfire statistics” should also display counter values appropriate to the environment.
In addition, the WildFire dashboard will display activity up to the last 24 hours. Benign files will only appear if the setting is enabled under Device > Setup > WildFire.

As a final end-to-end test, PAN provides a unique fake malicious file, which can be downloaded here: http://wildfire.paloaltonetworks.com/publicapi/test/pe This file should be seen as an unknown executable to WildFire, triggering an upload and analysis. Once WildFire determines the file is malicious, the configured alert should fire.

Rationale:

Although an administrator may believe WildFire is configured properly, additional steps should be taken to verify it is functioning as expected.
References:

“Wildfire Configuration, Testing and Monitoring” -
https://live.paloaltonetworks.com/docs/DOC-3300

“How to Check the Connectivity to Wildfire and Upload Status of Files” -
https://live.paloaltonetworks.com/docs/DOC-2670

“How to Test WildFire with a Fake Malicious File” -
https://live.paloaltonetworks.com/docs/DOC-7321

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

2.6. Security Profiles

2.6.1. Antivirus

2.6.1.1. Require an Antivirus profile configured to block on all decoders except imap and pop3.

Location:
Objects > Security Profiles > Antivirus

Recommendation:

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.

Author Name, email@address
Rationale:

Antivirus signatures produce low false positives. By blocking any detected virus through the specified decoders, the threat of virus propagation through the firewall is greatly reduced. It is recommended to mitigate viruses 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.

References:

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

2.6.1.2. Require a securely configured Antivirus profile applied to all applicable security policies.

Locations:

Author Name, email@address
Objects > Security Profiles > Antivirus

Policies > Security

**Recommendation:**

Create an Antivirus profile in accordance with this benchmark, and apply it to all security policies that could pass http, smtp, imap, pop3, ftp, or smb traffic. The Antivirus profile may be applied directly or through a profile group.

**Rationale:**

By applying a secure Antivirus profile to all applicable traffic, the threat of virus propagation through the firewall is greatly reduced.

**References:**
2.6.2. Anti-Spyware

2.6.2.1. Require an Anti-Spyware profile configured to block on all severity levels, categories, and threats.

Location:

Objects > Security Profiles > Anti-Spyware

Recommendations:

A) If a single rule exists within the Anti-Spyware Profile, configure it to block on any severity level, any category, and any threat.
B) If multiple rules exist within the Anti-Spyware profile, ensure any category, any threat, and all severity levels are set to Block. 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 malware and spyware traffic from successfully exiting the organization.

References:

Author Name, email@address
“Threat Prevention Deployment Tech Note” -
https://live.paloaltonetworks.com/docs/DOC-3094

2.6.2.2. **Require DNS Sinkholing on all Anti-spyware profiles in use.**

Location:

Objects > Security Profiles > Anti-Spyware

Recommendation:

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.

![DNS Sinkholing Configuration](image)

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.

References:

Author Name, email@address
“How to Deal with Conficker using DNS Sinkhole” -
https://live.paloaltonetworks.com/docs/DOC-6628

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

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

2.6.2.3. **Require Passive DNS Monitoring enabled on all Anti-Spyware profiles in use.**

   **Location:**
   
   Objects > Security Profiles > Anti-Spyware Policies > Security
   
   **Recommendation:**
   
   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.

References:

“What Information is Submitted to the Palo Alto Networks when Enabling the Passive DNS Feature” - https://live.paloaltonetworks.com/docs/DOC-7256


2.6.2.4. Require a securely configured Anti-Spyware profile applied to all security policies permitting traffic to the Internet.

Locations:

Objects > Security Profiles > Anti-Spyware

Policies > Security

Recommendation:

Create an Anti-Spyware profile in accordance with this benchmark, and apply it to all security policies permitting traffic to the Internet. The Anti-Spyware profile may be applied directly or through a profile group.

Rationale:

By applying a secure Anti-Spyware profile 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, therefore, should be applied to all security policies permitting traffic to the Internet.
2.6.3. Vulnerability Protection

2.6.3.1. Require a Vulnerability Protection profile configured to block at least high and critical vulnerabilities, and set to default on medium, low, and informational vulnerabilities.

Location:

Objects > Security Profiles > Vulnerability Protection

Recommendation:

Configure a Vulnerability Protection Profile set to block any critical or high threats, at minimum, and set to default on any medium, low, or informational threats. 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 on many critical and high threats are configured to only alert on the attack.

References:


Author Name, email@address
2.6.3.2. **Require a securely configured Vulnerability Protection Profile applied to all security policies allowing traffic.**

**Location:**

Policies > Security

**Recommendation:**

For any security rule allowing traffic, apply a securely configured vulnerability profile. This benchmark provides recommendations on configuring a secure vulnerability profile. Careful analysis of the target environment should be performed before implementing this configuration, as outlined by PAN’s “Threat Prevention Deployment Tech Note” found in the references section of this rule.

<table>
<thead>
<tr>
<th>Name</th>
<th>Count</th>
<th>Rule Name</th>
<th>Threat Name</th>
<th>Host Type</th>
<th>Severity</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>I-Inside-Default</td>
<td>1</td>
<td>critical-high</td>
<td>any</td>
<td>any</td>
<td>medium-high,informational</td>
<td>block</td>
</tr>
</tbody>
</table>

**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 attack. Note that encrypted sessions do not allow for complete inspection.

**References:**

“Threat Prevention Deployment Tech Note” -
[https://live.paloaltonetworks.com/docs/DOC-3094](https://live.paloaltonetworks.com/docs/DOC-3094)

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

Author Name, email@address
2.6.4. URL Filtering

2.6.4.1. Require the use of PAN-DB URL Filtering

Location:
Device > Licenses

Recommendation:
Configure the device to use PAN-DB URL Filtering.

Rationale:
URL Filtering provides protection against malicious URLs and IP addresses, as well as protection against websites posing a liability risk, such as pornography. PAN-DB URL Filtering offers additional malware protection and PAN threat intelligence not available in the BrightCloud URL Filtering license.

References:

2.6.4.2. Require a URL Filtering profile with the action of “block” or “override” on the following categories: adult, hacking, malware, phishing, proxy-avoidance-and-anonymizers

Location:
Objects > Security Profiles > URL Filtering

Author Name, email@address
**Recommendation:**

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, 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.

**References:**


2.6.4.3. **Forbid a utilized URL Filtering profile with any category set to “allow”**.

**Location:**

Author Name, email@address
Objects > Security Profiles > URL Filtering

**Recommendation:**

Do not set a URL category action to *allow* for any category.

**Rationale:**

For URL categories, the “allow” setting will not produce a log entry in the URL Filtering logs. For forensic purposes, it is advisable to log access to every URL, regardless of category.

**References:**

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

2.6.4.4. Require all HTTP Header Logging options enabled

**Location:**

Objects > Security Profiles > URL Filtering > URL Filtering Profile > Settings

**Recommendation:**

Enable *User-Agent*, *Referer*, and *X-Forwarded-For* options under *HTTP Header Logging*.
Enhanced Security Recommendation:

Uncheck the *Log container page only* option.

**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.

Unchecking 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.

**References:**

“PAN-OS Administrator's Guide 6.1 (English)” -
[https://live.paloaltonetworks.com/docs/DOC-8246](https://live.paloaltonetworks.com/docs/DOC-8246)
2.6.4.5. Require a securely configured URL Filtering profile applied to all security policies allowing traffic to the Internet.

Locations:

Policies > Security
Objects > Security Profiles > URL Filtering

Recommendation:

Create a URL Filtering profile in accordance with this benchmark, and apply it to all security policies permitting traffic to the Internet. The URL Filtering profile may be applied 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.

Reference:

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

2.6.5. Data Filtering

2.6.5.1. Require a Data Filtering policy set to alert after a threshold of Credit Card or Social Security numbers are detected.

Location:

Objects > Security Profiles > Data Filtering

Recommendation:

Author Name, email@address
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

Apply this Data Pattern to a Data Filtering policy with the following values:

- Applications – any
- File Types – any
- Direction – both
- Alert Threshold – 20
- Block Threshold – 0
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.

References:


2.6.5.2. Require a securely configured Data Filtering profile applied to all security policies allowing traffic to or from the Internet.

Location:
Objects > Security Profiles > Data Filtering
Policies > Security

**Recommendation:**

Create a Data Filtering profile in accordance with this benchmark, and apply it to all security policies permitting traffic to or from the Internet. The Data Filtering profile may be applied directly or through a profile group.

**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.

**Reference:**

Author Name, email@address
2.6.6. Zone Protection profiles

2.6.6.1. Require a Zone Protection Profile with an enabled SYN Flood Action of SYN Cookies attached to all untrusted zones.

Location:

Network > Network Profiles > Zone Protection > Zone Protection Profile > Flood Protection

Network > Zones

Recommendation:

The Alert, Activate, and Maximum settings for SYN Flood Protection depend highly on the environment and device used. Traffic analysis should be performed on the specific environment and firewall to determine accurate thresholds.

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.

References:


“How to Determine if Configured DoS Classify TCP SYN Cookie Alarm, Activate and Maximal Rate is Triggered” - https://live.paloaltonetworks.com/docs/DOC-6801


Author Name, email@address
“What are the Differences between DoS Protection and Zone Protection?” - 
https://live.paloaltonetworks.com/docs/DOC-4501

“Application DDoS Mitigation” - https://live.paloaltonetworks.com/docs/DOC-7158

2.6.6.2. **Require a Zone Protection Profile with tuned Flood Protection settings enabled for all flood types attached to all untrusted zones.**

**Location:**

Network > Network Profiles > Zone Protection > Zone Protection Profile > Flood Protection

Network > Zones

**Recommendation:**

Enable all Flood Protection options in the Zone Profile attached to 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.

![Zone Protection Profile](image-url)
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.

References:


“What are the Differences between DoS Protection and Zone Protection?” - https://live.paloaltonetworks.com/docs/DOC-4501

2.6.6.3. **Require all zones have Zone Protection Profiles with all Reconnaissance Protection settings tuned and enabled, and NOT set to allow for any scan type.**

Location:

Network > Network Profiles > Zone Protection > Zone Protection Profile > Reconnaissance Protection

Network > Zones

Recommendation:

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 this 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.

References:


“What are the Differences between DoS Protection and Zone Protection?” - https://live.paloaltonetworks.com/docs/DOC-4501

2.6.6.4. Require all zones have Zone Protection Profiles that drop *Spoofed IP address, mismatched overlapping TCP segment, Malformed, Strict Source Routing, and Loose Source Routing* IP options.

**Location:**

Network > Network Profiles > Zone Protection > Zone Protection Profile > Packet Based Attack Protection > TCP/IP Drop

Network > Zones

**Recommendation:**

For all zones, attach a Zone Protection Profile that is configured to drop *Spoofed IP address, mismatched overlapping TCP segment, Malformed, Strict Source Routing, and Loose Source Routing* IP options
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.

References:


“What are the Differences between DoS Protection and Zone Protection?” - https://live.paloaltonetworks.com/docs/DOC-4501


2.7. Security Policies

2.7.1. Security Policies - General

2.7.1.1. Require specific application policies when allowing traffic from an untrusted zone to a more trusted zone.

Location:

Policies > Security

Recommendation:

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.

References:


2.7.1.2. Forbid using the Service setting of any in a security policy.

Location:

Policies > Security

Recommendation:

Create security policies specifying application-default for the Service setting, or the specific ports desired. The Service setting of any should not be used.

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.

**References:**


### 2.7.1.3. **Require a security policy denying any/all traffic at the bottom of the security policies ruleset.**

**Location:**

Policies > Security

**Recommendation:**

EXTREME CAUTION MUST BE USED BEFORE IMPLEMENTING THIS RECOMMENDATION, AS CERTAIN TRAFFIC PERMITTED BY DEFAULT WILL BE DENIED UNLESS SPECIFICALLY ALLOWED. SEE THE “REFERENCES” SECTION FOR MORE INFORMATION.

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:

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. Viewing denied traffic can be extremely useful for understanding how security policies are affecting traffic, security investigations, general security analysis, or a host of additional use cases.

References:


2.8. Decryption

2.8.1. SSL Forward Proxy

2.8.1.1. Require an SSL Forward Proxy policy for traffic destined to the Internet for all URL categories except financial-services and health-and-medicine.

Location:

Policies > Decryption

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Source Zone</th>
<th>Source Address</th>
<th>Destination Zone</th>
<th>Destination Address</th>
<th>URL Category</th>
<th>Action</th>
<th>Type</th>
<th>Decryption Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Internet Decryption</td>
<td>INSIDE</td>
<td>any</td>
<td>OUTSIDE</td>
<td>any</td>
<td>abortion</td>
<td>decrypt</td>
<td>ssl-forward-proxy</td>
<td>Default-Decrypt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>abused-drugs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>adult</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>alcohol-and-t...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>auctions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>business-and...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>computer-and...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>more...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.

**References:**

“How to Implement SSL Decryption” - [https://live.paloaltonetworks.com/docs/DOC-1412](https://live.paloaltonetworks.com/docs/DOC-1412)


**2.8.2. SSL Inbound Inspection**

**2.8.2.1. Require SSL Inbound Inspection for all untrusted traffic destined for servers using SSL.**

**Location:**

Policies > Decryption

**Recommendation:**

Author Name, email@address
Configure SSL Inbound Inspection for all untrusted traffic destined for servers using SSL.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source Zone</th>
<th>Source Address</th>
<th>Destination Zone</th>
<th>Destination Address</th>
<th>URL Category</th>
<th>Action</th>
<th>Type</th>
<th>Decryption Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inspect Webservers</td>
<td>GUEST</td>
<td>any</td>
<td>DMZ</td>
<td>203.0.113.0/24</td>
<td>any</td>
<td>decrypt</td>
<td>ssl-inbound-inspection</td>
<td>Default-Decrypt</td>
</tr>
</tbody>
</table>

**Rationale:**

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

**References:**

“How to Implement SSL Decryption” - [https://live.paloaltonetworks.com/docs/DOC-1412](https://live.paloaltonetworks.com/docs/DOC-1412)

## Audit checklist

<table>
<thead>
<tr>
<th>Section</th>
<th>Recommendation</th>
<th>Page</th>
<th>Objective Met? (Yes, No, Partial, Other)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2.1.</strong></td>
<td><strong>Device Setup</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.1.1.</td>
<td>Require an appropriate login banner</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>2.1.2.1.</td>
<td>Enable Log on High DP Load</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>2.1.3.1.</td>
<td>Forbid HTTP and telnet services for device management</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>2.1.3.2.</td>
<td>Limit Permitted IP Addresses to those necessary for device management.</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>2.1.3.3.</td>
<td>Require all interface management profiles where telnet, SSH, HTTP, HTTPS, or SNMP is enabled to permit only IP addresses necessary for device management.</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>2.1.4.1.</td>
<td>Require minimum password complexity rules</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>2.1.4.2.</td>
<td>Forbid the use of password profiles</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>2.1.5.1.</td>
<td>Require an idle timeout value of 10 minutes for device management.</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>2.1.5.2.</td>
<td>Forbid the use of Authentication Settings for Failed Attempts and Lockout Time. Require an Authentication Profile with Failed Attempts to 3, and lockout time of 15 minutes applied to all but one Superuser account.</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>2.1.6.1.</td>
<td>Require SNMP V3 (If SNMP polling is configured)</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>2.1.7.1.</td>
<td>Require verification of update server identity</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>2.1.7.2.</td>
<td>Require redundant NTP services</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td><strong>2.2.</strong></td>
<td><strong>User Identification</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.1.1.</td>
<td>Require IP-to-username mapping for user traffic</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>2.2.2.1.</td>
<td>Disable WMI probing if not required.</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.2.2.</td>
<td>Forbid User-ID on external and other non-trusted zones</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.2.3.</td>
<td>Require the use of User-ID's Include/Exclude Networks section, if User-ID is enabled. Include only trusted internal networks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.3.1.</td>
<td>Require a dedicated service account for User-ID with minimal permissions (If a User-ID Agent or Integrated User-ID Agent is utilized)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.3.2.</td>
<td>Forbid Interactive Login rights for the User-ID service account</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.3.4.</td>
<td>Require security policies restricting User-ID Agent traffic from crossing into untrusted zones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3.</td>
<td>High Availability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3.1.1.</td>
<td>Require a fully-synchronized High Availability peer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3.1.2.</td>
<td>For High Availability, require Link Monitoring, Path Monitoring, or both</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3.1.3.</td>
<td>Forbid simultaneously enabling the Preemptive option, and configuring the Passive Link State to shutdown simultaneously. (For an HA pair)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4.</td>
<td>Dynamic Updates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4.1.1.</td>
<td>Require the Antivirus Update Schedule is set to Download and Install hourly.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4.1.2.</td>
<td>Require the Applications and Threats Update Schedule is set to Download and Install Daily.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4.1.3.</td>
<td>Require the WildFire Update Schedule is set to Download and Install every 15 minutes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5.</td>
<td>WildFire</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5.1.1.</td>
<td>Increase WildFire file size upload limits</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5.2.1.</td>
<td>Require WildFire File Blocking profiles to include any application, any file type, and action set to forward</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5.2.2.</td>
<td>Require a WildFire File Blocking profile for all security policies allowing Internet traffic flows.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5.2.3.</td>
<td>Require forwarding of decrypted content</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5.2.4.</td>
<td>Require all WildFire Session Information Settings to be enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5.3.1.</td>
<td>Require sending an alert for malware detected through WildFire</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 2.5.3.2. Verify WildFire file submission and alerting is functioning as expected

<table>
<thead>
<tr>
<th>2.6.</th>
<th>Security Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.6.1.</td>
<td>Require an Antivirus profile configured to block on all decoders except imap and pop3.</td>
</tr>
<tr>
<td>2.6.1.2.</td>
<td>Require a securely configured Antivirus profile applied to all applicable security policies.</td>
</tr>
<tr>
<td>2.6.2.1.</td>
<td>Require an Anti-Spyware profile configured to block on all severity levels, categories, and threats.</td>
</tr>
<tr>
<td>2.6.2.2.</td>
<td>Require DNS Sinkholing on all Anti-spyware profiles in use.</td>
</tr>
<tr>
<td>2.6.2.3.</td>
<td>Require Passive DNS Monitoring enabled on all Anti-Spyware profiles in use.</td>
</tr>
<tr>
<td>2.6.2.4.</td>
<td>Require a securely configured Anti-Spyware profile applied to all security policies permitting traffic to the Internet.</td>
</tr>
<tr>
<td>2.6.3.1.</td>
<td>Require a Vulnerability Protection profile configured to block at least high and critical vulnerabilities, and set to default on medium, low, and informational vulnerabilities.</td>
</tr>
<tr>
<td>2.6.3.2.</td>
<td>Require a securely configured Vulnerability Protection Profile applied to all security policies allowing traffic.</td>
</tr>
<tr>
<td>2.6.4.1.</td>
<td>Require the use of PAN-DB URL Filtering</td>
</tr>
<tr>
<td>2.6.4.2.</td>
<td>Require a URL Filtering profile with the action of &quot;block&quot; or &quot;override&quot; on the following categories: adult, hacking, malware, phishing, proxy-avoidance-and-anonymizers</td>
</tr>
<tr>
<td>2.6.4.3.</td>
<td>Forbid a utilized URL Filtering profile with any category set to &quot;allow&quot;.</td>
</tr>
<tr>
<td>2.6.4.4.</td>
<td>Require all HTTP Header Logging options enabled</td>
</tr>
<tr>
<td>2.6.4.5.</td>
<td>Require a securely configured URL Filtering profile applied to all security policies allowing traffic to the Internet.</td>
</tr>
<tr>
<td>2.6.5.1.</td>
<td>Require a Data Filtering policy set to alert after a threshold of Credit Card or Social Security numbers are detected.</td>
</tr>
</tbody>
</table>

Author Name, email@address
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.6.6.1</td>
<td>Require a Zone Protection Profile with an enabled SYN Flood Action of SYN Cookies attached to all untrusted zones.</td>
<td>64</td>
</tr>
<tr>
<td>2.6.6.2</td>
<td>Require a Zone Protection Profile with tuned Flood Protection settings enabled for all flood types attached to all untrusted zones.</td>
<td>66</td>
</tr>
<tr>
<td>2.6.6.3</td>
<td>Require all zones have Zone Protection Profiles with all Reconnaissance Protection settings tuned and enabled, and NOT set to allow for any scan type.</td>
<td>67</td>
</tr>
<tr>
<td>2.6.6.4</td>
<td>Require all zones have Zone Protection Profiles that drop Spoofed IP address, mismatched overlapping TCP segment, Malformed, Strict Source Routing, and Loose Source Routing IP options.</td>
<td>69</td>
</tr>
<tr>
<td>2.7.1.1</td>
<td>Require specific application policies when allowing traffic from an untrusted zone to a more trusted zone.</td>
<td>70</td>
</tr>
<tr>
<td>2.7.1.2</td>
<td>Forbid using the Service setting of any in a security policy.</td>
<td>71</td>
</tr>
<tr>
<td>2.7.1.3</td>
<td>Require a security policy denying any/all traffic at the bottom of the security policies ruleset.</td>
<td>72</td>
</tr>
<tr>
<td>2.8.1.1</td>
<td>Require an SSL Forward Proxy policy for traffic destined to the Internet for all URL categories except financial-services and health-and-medicine.</td>
<td>73</td>
</tr>
<tr>
<td>2.8.2.1</td>
<td>Require SSL Inbound Inspection for all untrusted traffic destined for servers using SSL.</td>
<td>74</td>
</tr>
</tbody>
</table>
4. References


How to Determine if Configured DoS Classify TCP SYN Cookie Alarm, Activate and Maximal Rate is Triggered. (2014, March 31). Retrieved February 12, 2015, from https://live.paloaltonetworks.com/docs/DOC-6801


Author Name, email@address


Author Name, email@address


Author Name, email@address
# 5. Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Changes for this version</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/13/15</td>
<td>1.0</td>
<td>Original version</td>
</tr>
<tr>
<td>4/13/15</td>
<td>1.1</td>
<td>Updated section 2.1.7.1</td>
</tr>
<tr>
<td>4/13/15</td>
<td>1.1</td>
<td>Several links were broken in v.1.0 during Reading Room conversion.</td>
</tr>
<tr>
<td>4/13/15</td>
<td>1.1</td>
<td>Updated section 2.6.1.1</td>
</tr>
<tr>
<td>4/13/15</td>
<td>1.1</td>
<td>Updated the introduction to include an acknowledgements section.</td>
</tr>
<tr>
<td>4/13/15</td>
<td>1.1</td>
<td>Added the Revision History section</td>
</tr>
</tbody>
</table>

Author Name, email@address
<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Chicago Spring 2020</td>
<td>Chicago, IL US</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Europe Summit &amp; Training 2020</td>
<td>Munich, DE</td>
<td>Jun 08, 2020 - Jun 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Budapest June 2020</td>
<td>Budapest, HU</td>
<td>Jun 08, 2020 - Jun 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Zurich June 2020</td>
<td>Zurich, CH</td>
<td>Jun 15, 2020 - Jun 20, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London June 2020</td>
<td>OnlineGB</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s Only US</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>