
IronSkillet Documentation

Release 0.0.5

Scott Shoaf

Feb 15, 2023

GETTING STARTED

1	IronSkillet Overview	1
2	Requirements and Caveats	5
3	GUI Visual Guide: PAN-OS	7
4	Config Validations: PAN-OS	57
5	IronSkillet Players	59
6	Default Loadable Configurations	61
7	PAN-OS XML Snippets	79
8	Panorama XML Snippets	91
9	Formula-based Excel Spreadsheet	105
10	Creating Loadable Configurations	107
11	Loading the XML templates	111
12	VM-50 Security Profile Limits	121
13	CIS Palo Alto Firewall 9 Benchmark	123
14	New PAN-OS Version Updates	223
15	Release and Update History	227

IRONSKILLET OVERVIEW

Welcome to the IronSkillet day one configuration templates library.

The next-generation firewall configuration templates are based on existing [best practice recommendations](#) from Palo Alto Networks.

Instead of extensive and detailed ‘how to’ documentation, the templates provide an easy to implement configuration model that is use case agnostic. The emphasis is on key security elements such as dynamic updates, security profiles, rules, and logging that should be consistent across deployments.

1.1 Why use day one templates?

Palo Alto Networks has expertise in both security prevention and its own product portfolio. Best practice documentation is designed to provide knowledge sharing of this expertise to customers and partners. This sharing helps improve security posture across various scenarios.

The templates play a complementary role by taking common best practices recommendations and compiling them into pre-built day one configurations that can be readily loaded into Panorama or a next-generation firewall. The benefits include:

- Faster time to implement
- Reduce configuration errors
- Improve security posture

1.2 Supported releases

IronSkillet is currently supported on the three most recent releases. Earlier releases of Ironskillet are supported based on community best efforts.

Available and currently supported releases:

- 11.0
- 10.2
- 10.1

Available but end of support releases:

- 10.0
- 9.1
- 9.0

- 8.1
- 8.0

1.3 Using the templates

The templates are available on GitHub specific to each PAN-OS software version.

View *github repo*: | [11.0](#) | [10.2](#) | [10.1](#) | [10.0](#) | [9.1](#) | [9.0](#) |

Note: versions 8.0, 8.1, 9.0, 9.1 and 10.0 are still available but no longer will be updated

Use the branch specific to the software release for your deployment.

The library consists of a set of XML and set configuration templates grouped by:

- `panos` for stand-alone next-gen firewall deployments
- `panorama` for Panorama system and managed device configurations

The templates in each device-type folder include:

- `snippets` rolled up playlist for easy skillet viewing
- `full config file` to use for bootstrap or full import + load into a device
- `set commands` for traditional CLI configuration

The playlists (new in 10.1) in each device-type folder consist of:

- **full config** for full configuration of IronSkillet
- **security profiles only** for configuring only the profiles for panos or panorama
- **device hardening** for configuring only security policies for panos or panorama
- **alert only** for configuring only the alert security profiles for panos

There are also validation skillets for analysis of existing configurations

- `full assessment` to see what IronSkillet elements are missing
- `9.x upgrade from 8.1` to check for new skillet additions
- `10.x upgrade from 9.x` to check for new skillet additions

Validation insights currently require applications such as panHandler (<https://panhandler.readthedocs.io>) for analysis and results output.

1.3.1 Quick start using IronSkillet players

User can opt to use one of the *IronSkillet Players* to render and load configurations. These apps and tools are a great starting point to begin using IronSkillet.

1.3.2 Quick start using loadable configurations

The repo contains a set of ready-to-go loadable configurations that use IronSkillet placeholder values. Formats include both XML and set commands.

The XML file can be imported and loaded easily to Panorama or a firewall. The set command model requires ‘copy-and-paste’ from the CLI.

More information for loading and editing these configurations can be found at: [Default Loadable Configurations](#).

1.3.3 Excel set command spreadsheet

Also included for easy loading is an Excel formula-based spreadsheet with set commands. A variable value worksheet can be edited to update the spreadsheet using localized values for various configuratino attributes.

More information for using the spreadsheet can be found at: [Formula-based Excel Spreadsheet](#).

1.3.4 Jinja-based XML snippet and set command templates

Scripting or automation-centric users may prefer to use the base template files. These are variable-based templates using a Jinja `{{ variable }}` notation.

The XML snippets with metadata are designed to use API-based configuration loading into Panorama or the firewall and can be coupled with workflow tools for repeatable deployments.

Sample utilities are provided in the `tools` directory to create loadable configurations using these base templates.

See the sections [Creating Loadable Configurations](#) and [Loading the XML templates](#) for more information.

Note: Day one templates are not complete configuration templates. To insert the device into the network requires interface, zone, routing, and other settings outside the scope of the day one templates. Also not included are use-case specific items such as whitelist security rules, userID settings, and decryption policies that can be deployment and use case specific.

1.4 What is next after loading a template?

Based on the deployment scenario, the next steps may include:

- GUI configuration of additional configuration elements specific to the deployment use case
- API/scripted loading of additional configuration elements

In cases where the use case configuration has been merged with the templates, no further actions may be required. A key example would be interface, NAT, zone, and security rule additions for a simple Internet gateway deployments.

1.5 Where can I find complete reference use case configurations?

The initial release of the templates are use case agnostic. However, as the community creates and shared reference configurations, they will be shared across the community as an extension of the iron-skillet configurations.

REQUIREMENTS AND CAVEATS

Please read before using the IronSkillet configuration templates.

2.1 Requirements

Using IronSkillet branch version panos_v10.0 requires the following to properly load into Panorama and/or the NGFW

- Running software version 10.0
 - [Upgrade the firewall to 10.0](#)
 - [Upgrade Panorama to 10.0](#)
- Active subscription for Threat Prevention
 - [Activate the subscription licenses](#)
- Updated application and antivirus content
 - [Install content and software updates](#)

Note: The links are specific to PAN-OS v10.0 and users may switch to 9.1, 9.0, or 8.1 based on deployed release

Note: Threat Prevention and the antivirus content update are both required to gain access to the Palo Alto Networks provided External Dynamic Lists (EDLs) used in the security policies.

Note: URL Filtering, DNS Cloud Service, and Wildfire subscriptions are not required to load the configuration but are highly recommended as part of the best practice to utilize IronSkillet elements such as the URL Filtering, Spyware, and Wildfire security profiles and associated profile groups

2.2 Caveats

Please review the following to understand any limitations or recommendations regarding the IronSkillet templates

- Be sure to edit or the default administrative superuser account if not part of initial configuration
 - If the default account information is used, the user is notified at login
 - To change or add superuser accounts see [Configure a Firewall Administrator](#)
- The current version only supports IPv4 management interface configuration
 - IPv6 to be considered based on customer demand
- IronSkillet loaded into a VM-50 will utilize the full profile capacity
 - See the section *VM-50 Security Profile Limits* for more information
- The Panorama full configuration template is based on a fully shared model
 - All [device-group configuration](#) at the Shared top of tree
 - Additional Panorama [template stacks](#) should include the IronSkillet template

GUI VISUAL GUIDE: PAN-OS

IronSkillet is delivered as a configuration template without a step-by-step configuration guide. This was the intent to have a rapid deployment option without massive GUI clicks.

However, users still want to know what exactly they configured in the event they want to make changes or compare IronSkillet manually to their existing configuration.

So based on popular demand here is the GUI-based visual guide to all of the IronSkillet configuration elements.

This is based on PAN-OS 10.x with callouts for any features not supported in the prior releases. Also note that based on software release, there may be other items configured or ‘checked’ as defaults and not part of IronSkillet. These items are not referenced in this guide.

IronSkillet includes a mix of day one best practices for configuration types such as:

- **Device management hardening:** general operations of the NGFW
- **Security traffic hardening:** control of traffic flows that impacts device monitoring
- **Logging and alerts:** data collection and external notifications
- **Security objects and policies:** policy-related config settings and dynamic updates
- **Decryption objects and policies:** certification checks and sample no-decrypt policy

This visual guide is based on the [IronSkillet full configuration file](#)

This file uses default value settings and can be readily imported and loaded as a candidate configuration allowing the user to follow along with this guide.

Note: Documentation links for release 10.0 are provided for additional information.

3.1 Device

The device tab is used for device management, hardening, system logging, and other device related configuration elements.

It also includes security function related configuration such as dynamic updates for anti-virus, vulnerability, spyware DNS and Wildfire signatures as well as Wildfire submission file size configuration.

3.1.1 Setup

Management

See also

General configuration information in the Admin Guide: [Device - Setup - Management](#)

Device > Setup > Management > General Settings

General Settings

Hostname

IronSkillet_fw

Domain

Accept DHCP server provided Hostname

☐

Accept DHCP server provided Domain

☐

Login Banner

You have accessed a protected system.
Log off immediately if you are not an authorized user.

Force Admins to Acknowledge Login Banner

☐

SSL/TLS Service Profile

Time Zone

UTC

Locale

en

Time

Sat Jun 27 19:17:16 PDT 2020

Geo Location

Automatically Acquire Commit Lock

☒

Changes to General Settings:

- **Hostname:** name of the device; IronSkillet defaults to 'sample'
- **Login Banner:** display text presented to users at login
- **Time Zone:** set to UTC so all devices map to a common universal timezone
- **Automatically Acquire Commit Lock:** block a commit across multiple web sessions

Device > Setup > Management > Authentication Settings

Authentication Settings	
Authentication Profile	
Certificate Profile	
Idle Timeout (min)	10
API Key Lifetime (min)	525600
API Keys Last Expired	
Failed Attempts	5
Lockout Time (min)	30
Max Session Count (number)	0
Max Session Time (min)	0

Changes to Authentication Settings:

- **Idle Timeout:** close the session after 10 minutes of inactivity
- **API Key Lifetime (9.0):** time to expire an existing API key; 'infinite' pre 9.0
- **Failed Attempts:** Lockout the account after 5 failed attempts
- **Lockout Time:** Lockout the account for 30 minutes after 5 failed attempts

Device > Setup > Management > Logging and Reporting Settings

Logging and Reporting Settings	
Log Storage	Total: 15.22 GB Unallocated: 0 MB
Number of Versions for Config Audit	100
Max Rows in CSV Export	1048576
Max Rows in User Activity Report	5000
Average Browse Time (sec)	60
Page Load Threshold (sec)	20
Send HOSTNAME in Syslog	FQDN
Report Runtime	02:00
Report Expiration Period (days)	
Stop Traffic when LogDb Full	<input type="checkbox"/>
Enable Threat Vault Access	<input checked="" type="checkbox"/>
Enable Log on High DP Load	<input checked="" type="checkbox"/>
Support UTF-8 For Log Output	<input type="checkbox"/>
Log Collector Status	Show Status

Changes to Logging and Reporting Settings:

- **Max Rows in CSV Export:** increase row count to 1,048,576
- **Enable Log on High DP Load:** a system log entry is generated when the packet processing load on the firewall is at 100% CPU utilization

Log Suppression (CLI only)

Log suppression, when enabled, is a feature that instructs the Palo Alto Networks device to combine multiple similar logs into a single log entry on the Monitor > Logs > Traffic page.

Disabled to ensure unique log entries even if similar session types

```
set deviceconfig setting logging log-suppression no
```

Device > Setup > Management > Minimum Password Complexity

Minimum Password Complexity

Enabled ☒

Minimum Length 12

Minimum Uppercase Letters 1

Minimum Lowercase Letters 1

Minimum Numeric Letters 1

Minimum Special Characters 1

Block Repeated Characters 0

Block Username Inclusion (including reversed) ☒

New Password Differs By Characters 3

Require Password Change on First Login ☐

Prevent Password Reuse Limit 24

Block Password Change Period (days) 0

Required Password Change Period (days) 0

Expiration Warning Period (days) 0

Post Expiration Admin Login Count 0

Post Expiration Grace Period (days) 0

Enable minimum password requirements for local accounts. With this feature, you can ensure that local administrator accounts on the firewall will adhere to a defined set of password requirements.

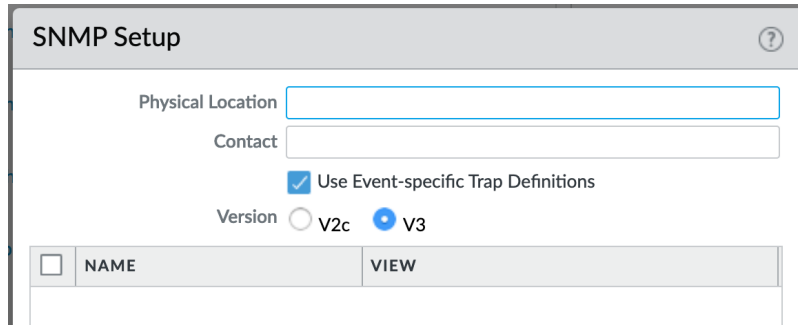
Note: password expiration has been removed based on NIST standards although users can still opt to set an expiration and notification period

Operations

See also

General configuration information in the Admin Guide: [Device - Setup - Operations](#)

Device > Setup > Operations > SNMP Setup



The image shows a web-based configuration window titled "SNMP Setup". It contains the following fields and options:

- Physical Location**: A text input field.
- Contact**: A text input field.
- Use Event-specific Trap Definitions**: A checked checkbox.
- Version**: Two radio buttons, "V2c" and "V3". The "V3" button is selected.
- Table**: A table with two columns, "NAME" and "VIEW". The "NAME" column has a checkbox in its header. The table is currently empty.

If used, ensure SNMP version is V3

Services

See also

General configuration information in the Admin Guide: [Device - Setup - Services](#)

Device > Setup > Services > Services

Services

Update Server

updates.paloaltonetworks.com

Verify Update Server Identity

☒

DNS Servers

Primary DNS Server

8.8.8.8

Secondary DNS Server

8.8.4.4

Minimum FQDN Refresh Time (sec)

30

FQDN Stale Entry Timeout (min)

1440

Proxy Server

Primary NTP Server Address

0.pool.ntp.org

Primary NTP Server Authentication Type

None

Secondary NTP Server Address

1.pool.ntp.org

Secondary NTP Server Authentication Type

None

Key configuration elements:

- **DNS:** Primary and Secondary server IP addresses; for all DNS queries that the firewall initiates in support of FQDN address objects, logging, and firewall management
- **NTP:** Primary and Secondary server FQDNs; use to synchronize the clock on the firewall

Interfaces

See also

General configuration information in the Admin Guide: [Device - Setup - Interfaces](#)

Device > Setup > Interfaces > Management

Management Interface Settings

IP Type

☐ Static
 ☒ DHCP Client

MTU

1500

Client Options

☒ Send Hostname
 ☐ Send Client ID

[Show DHCP Client Runtime Info](#)

Administrative Management Services

☐ HTTP
 ☒ HTTPS
 ☐ Telnet
 ☒ SSH

Network Services

☐ HTTP OCSP
 ☒ Ping
 ☐ SNMP
 ☐ User-ID
 ☐ User-ID Syslog Listener-SSL
 ☐ User-ID Syslog Listener-UDP

This example shows a static IP address, netmask, and gateway configuration. IronSkillet also gives the option of using the DHCP Client which removes the IP data fields.

- **Administrative Management Services:** limit to HTTPS and SSH
- **Network Services:** only allow Ping unless other services are required

Note: Additional recommendations include restricting access to only authorized IP addresses

Content-ID**See also**

General configuration information in the Admin Guide: [Device - Setup - Content-ID](#)

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

Content-ID Settings

Allow forwarding of decrypted content

☒

Extended Packet Capture Length (packets)

5

Forward segments exceeding TCP App-ID inspection queue

☐

Forward segments exceeding TCP content inspection queue

☐

Forward datagrams exceeding UDP content inspection queue

☐

Allow HTTP partial response

☒

Enable allow forwarding of decrypted content: From version 10.1 and forwards enable the firewall to forward SSL traffic for WildFire analysis.

Disable Forward segments exceeding TCP App-ID inspection queue: In newer releases disabled by default; explicit disable in IronSkillet template Disable this option to prevent the firewall from forwarding TCP segments and skipping App-ID inspection when the App-ID inspection queue is full.

Disable Forward segments exceeding TCP content inspection queue: Disable this option to prevent the firewall from forwarding TCP segments and skipping content inspection when the content inspection queue is full.

Disable Forward segments exceeding UDP content inspection queue: Disable this option to prevent the firewall from forwarding UDP segments and skipping content inspection when the content inspection queue is full.

Device > Setup > Content-ID > X-Forwarded-For Headers

Note: IronSkillet only includes pre 10.0 release configuration. In 10.0 XFF moves from a global to policy or user configuration.

X-Forwarded-For Headers

Use X-Forwarded-For Header in User-ID

☒

Strip X-Forwarded-For Header

☒

Header field option that preserves the IP address of the user who made the GET request

Enable Use X-Forwarded-For Header in User-ID

Select this option to specify that User-ID reads IP addresses from the X-Forwarded-For (XFF) header in client requests for web services when the firewall is deployed between the Internet and a proxy server that would otherwise hide client IP addresses. User-ID matches the IP addresses it reads with usernames that your policies reference so that

those policies can control and log access for the associated users and groups. If the header has multiple IP addresses, User-ID uses the first entry from the left.

Enable Strip X-Forwarded-For Header

Select this option to remove the X-Forwarded-For (XFF) header, which contains the IP address of a client requesting a web service when the firewall is deployed between the Internet and a proxy server. The firewall zeroes out the header value before forwarding the request: the forwarded packets don't contain internal source IP information.

Wildfire

See also

General configuration information in the Admin Guide: [Device - Setup - Wildfire](#)

Device > Setup > Wildfire > General Settings

General Settings ⚙️

WildFire Public Cloud wildfire.paloaltonetworks.com

WildFire Private Cloud

Use Proxy Settings for Private Cloud ☐

File Size Limits

pe: 16 MB
 apk: 30 MB
 pdf: 3072 KB
 ms-office: 16384 KB
 jar: 5 MB
 flash: 5 MB
 MacOSX: 10 MB
 archive: 50 MB
 linux: 50 MB
 script: 20 KB

Report Benign Files ☐

Report Grayware Files ☒

Key configuration elements:

- **WildFire Public Cloud:** where to send file samples for analysis; defaults to the US-based url and can be changed to various regional sites
- **File Size Limits:** recommended maximum file sizes to send to WildFire
- **Report Grayware Files:** shows verdicts in the Wildfire submissions logs

See also

The [wildfire global cloud documentation](#) has additional information for public cloud fqdn options


Session

Configure session age-out times, decryption certificate settings, and global session-related settings such as firewalling IPv6 traffic and rematching Security policy to existing sessions when the policy changes.

See also

General configuration information in the Admin Guide: [Device - Setup - Session](#)

Device > Setup > Session > Session Settings

Session Settings 

Rematch Sessions	<input checked="" type="checkbox"/>
ICMPv6 Token Bucket Size	100
ICMPv6 Error Packet Rate (per sec)	100
IPv6 Firewalling	<input checked="" type="checkbox"/>
Enable Jumbo Frame	<input type="checkbox"/>
DHCP Broadcast Session	<input type="checkbox"/>
Global MTU	1500
NAT64 IPv6 Minimum Network MTU	1280
NAT Oversubscription Rate	Platform Default
ICMP Unreachable Packet Rate (per sec)	200
Accelerated Aging	<input checked="" type="checkbox"/>
Accelerated Aging Threshold	80
Accelerated Aging Scaling Factor	2
Packet Buffer Protection	<input checked="" type="checkbox"/>
Latency Based Activation	<input type="checkbox"/>
Latency Alert (ms)	50
Latency Activate (ms)	200
Latency Max Tolerate (ms)	500
Block Countdown Threshold (ms)	500
Alert (%)	50
Activate (%)	80
Block Countdown Threshold (%)	80
Block Hold Time (sec)	60
Block Duration (sec)	3600
Multicast Route Setup Buffering	<input type="checkbox"/>
Multicast Route Setup Buffer Size	1000

Key configuration elements:

- **Rematch Sessions:** cause the firewall to apply newly configured security policies to sessions that are already in progress

Device > Setup > Session > TCP Settings

TCP Settings

Forward segments exceeding TCP out-of-order queue

☐

Allow Challenge ACK

☐

Drop segments with null timestamp option

☒

Asymmetric Path

drop

Urgent Data Flag

Clear

Drop segments without flag

☒

Strip MPTCP option

☒

SIP TCP cleartext

Always enabled

TCP Retransmit Scan

☐

Prevent TCP and MPTCP evasions

- set **Forward segments exceeding TCP out-of-order queue** to ‘no’
- set **Drop segments with null timestamp option** to ‘yes’
- set **urgent data flag** to ‘clear’
- set **drop segments without flag** to ‘yes’
- set **Strip MPTCP option** to ‘yes’

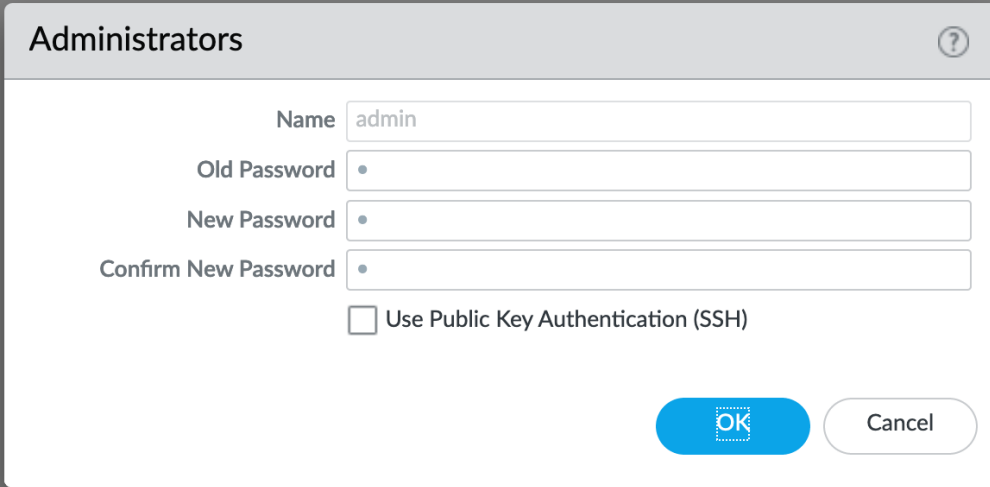
3.1.2 Administrators

IronSkillet default admin

See also

General configuration information in the Admin Guide: [Device - Administrators](#)

Device > Administrators : admin

A dialog box titled "Administrators" with a question mark icon in the top right corner. It contains four input fields: "Name" with the text "admin", "Old Password" with a single dot, "New Password" with a single dot, and "Confirm New Password" with a single dot. Below these fields is a checkbox labeled "Use Public Key Authentication (SSH)" which is currently unchecked. At the bottom right are two buttons: a blue "OK" button and a white "Cancel" button with a grey border.

The default reference configuration uses the default admin/admin login credentials. This should be changed immediately.

Note: As of release 9.0.4 the user is forced to change the admin password based on a minimum character length of 8 as part of a default password complexity profile. Once IronSkillet is loaded, this complexity profile is more complex overriding the default profile.

3.1.3 Response Pages

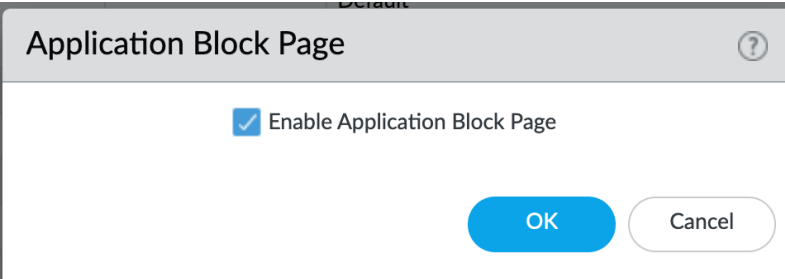
Response pages are the web pages that display when a user tries to access a URL.

See also

General configuration information in the Admin Guide: [Device - Response Pages](#)

IronSkillet Enable Block Page

Device > Response Pages > Application Block Page

A dialog box titled "Application Block Page" with a question mark icon in the top right corner. It contains a single checkbox labeled "Enable Application Block Page" which is checked. At the bottom right are two buttons: a blue "OK" button and a white "Cancel" button with a grey border.

Response pages display when a user attempts to access a URL that is not permitted by policy or content (threat) inspection. It is recommended to enable the **Application Block Page** setting so that users are aware of why an application

is not working.

3.1.4 Log Settings

See also

General configuration information in the Admin Guide: [Device - Log Settings](#)

There are multiple sections that can be configured for device log forwarding (System, Configuration, User-ID, and HIP Match)

Options include sending all logs, logs by severity, and custom attributes using the filter builder. Iron Skillet recommended settings include forwarding critical system logs to email and using Syslog for all system logs

Configuration, User-ID, and HIP Match should forward all logs to syslog or another logging platform such as Panorama or Cortex Data Lake.

It is recommended to forward all logs to Panorama if the firewall is being managed by Panorama. This setting is unchecked as the Iron Skillet configuration assumes a standalone configuration

Note: Since log settings are operational and may vary across user environments, these are focused as ‘reference configurations’ as part of a recommended day one starter configuration.

System

System event log actions

Device > Log Settings > System

System							
<input type="checkbox"/>	NAME	DESCRIPTION	FILTER	PANORAMA	SNMP TRAP	EMAIL	SYSLOG
<input type="checkbox"/>	System_Log_Forwarding		All Logs	<input type="checkbox"/>			Sample_Syslog_Profile
<input type="checkbox"/>	Email_Critical_System_Logs	Email Critical System Logs	(severity eq critical)	<input type="checkbox"/>		Sample_Email_Profile	

Email_Critical_System_Logs: Send output as an email using a configured email profile. Only email severity=critical events

System_Log_Forwarding: As reference, forward all system logs as syslog using a configured syslog profile

Profiles configurations are in the section [Server Profiles](#).

Configuration

Configuration event log actions

Device > Log Settings > Configuration

Configuration								
<input type="checkbox"/>	NAME	DESCRIPTION	FILTER	PANORAMA	SNMP TRAP	EMAIL	SYSLOG	
<input type="checkbox"/>	Configuration_Log_Forward...		All Logs	<input type="checkbox"/>			Sample_Syslog_Profile	

Configuration_Log_Forwarding: As reference, forward all configuration logs as syslog using a configured syslog profile

Profiles configurations are in the section *Server Profiles*.

User-ID

User-ID event log actions

Device > Log Settings > User-ID

User-ID								
<input type="checkbox"/>	NAME	DESCRIPTION	FILTER	PANORAMA	SNMP TRAP	EMAIL	SYSLOG	
<input type="checkbox"/>	User-ID_Log_Forwarding		All Logs	<input type="checkbox"/>			Sample_Syslog_Profile	

User-ID_Log_Forwarding: As reference, forward all user ID logs as syslog using a configured syslog profile

Profiles configurations are in the section *Server Profiles*.

Host Information Profile (HIP) Match

GlobalProtect HIP event log actions

Device > Log Settings > HIP Match

HIP Match								
<input type="checkbox"/>	NAME	DESCRIPTION	FILTER	PANORAMA	SNMP TRAP	EMAIL	SYSLOG	
<input type="checkbox"/>	HIP_Log_Forwarding		All Logs	<input type="checkbox"/>			Sample_Syslog_Profile	

HIP_Log_Forwarding: As reference, forward all HIP logs as syslog using a configured syslog profile

GlobalProtect (GP)

GlobalProtect event log actions

Device > Log Settings > GlobalProtect

GlobalProtect							
<input type="checkbox"/>	NAME	DESCRIPTION	FILTER	PANORAMA	SNMP TRAP	EMAIL	SYSLOG
<input type="checkbox"/>	GP_Log_Forwarding		All Logs	<input type="checkbox"/>			Sample_Syslog_Profile

GP_Log_Forwarding: As reference, forward all GP logs as syslog using a configured syslog profile

IP-Tag

GlobalProtect HIP event log actions

Device > Log Settings > IP-Tag

GlobalProtect							
<input type="checkbox"/>	NAME	DESCRIPTION	FILTER	PANORAMA	SNMP TRAP	EMAIL	SYSLOG
<input type="checkbox"/>	GP_Log_Forwarding		All Logs	<input type="checkbox"/>			Sample_Syslog_Profile

IP_Tag: As reference, forward all IP-Tag logs as syslog using a configured syslog profile

Profiles configurations are in the section *Server Profiles*.

3.1.5 Server Profiles

See also

General configuration information in the Admin Guide: [Device - Server Profiles](#)

Note: Since are operational and may vary across user environments, these are focused as ‘reference configurations’ as part of a recommended day one starter configuration.

Note: These values will need to be adjusted to the actual customer environment settings. You will want to verify that the Email Relay and Syslog machine can receive messages from the firewalls management interface (default **Service Route Configuration – Device > Setup > Services**).

Configuration of server profiles used by the log setting configurations.

Syslog

Device > Server Profiles > Syslog

Syslog Server Profile

Name

Servers

Custom Log Format

NAME	SYSLOG SERVER	TRANSPORT	PORT	FORMAT	FACILITY
Sample_Syslog	192.0.2.2	UDP	514	BSD	LOG_USER

+ Add

- Delete

Enter the IP address or FQDN of the Syslog server

OK

Cancel

Sample Syslog Profile using standard port 514.

Note: The sample IP address 192.0.2.2 is a non-routable address

Email Server

Device > Server Profiles > Email

Email Server Profile

Name

Sample_Email_Profile

Servers

Custom Log Format

	NAME	EMAIL DISPLAY NAME	FROM	TO	ADDITIO... RECIPIENT	EMAIL GATEWAY	PROTOCOL	PORT	TLS VERSION	AUTHENT... METHOD	CERTIFIC... PROFILE
<input type="checkbox"/>	Sample_E...	Threat_Al...	sentfrom...	sendto@y...		192.0.2.1	SMTP	25			

+ Add

- Delete

Enter the IP address or FQDN of the Email gateway

OK

Cancel

Sample email server profile for critical alert events including the new option for Protocol, IronSkillet using SMTP.

Note: the from/to and gateway values are reference only. The gateway address is non-routable.

3.1.6 Dynamic Updates

See also

General configuration information in the Admin Guide: [Device - Dynamic Updates](#)

IronSkillet Dynamic Updates

Dynamic updates allow the firewall to periodically check for content updates. Without this schedule configured, no new signature, vulnerabilities, malicious domains, or GlobalProtect files will be locally loaded into the firewall.

Device > Dynamic Updates : schedules

VERSION ^	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE
> Antivirus	Last checked: 2020/06/26 08:04:04 PDT		Schedule: Every hour at 4 minutes past the hour (Download and Install)			
> Applications and Threats	Last checked: 2020/06/26 08:02:04 PDT		Schedule: Every 30 minutes at 2 minutes past half-hour (Download and Install)			
> GlobalProtect Clientless VPN	Last checked: 2020/06/26 07:50:04 PDT		Schedule: Every hour at 50 minutes past the hour (Download and Install)			
> GlobalProtect Data File	Schedule: Every hour at 40 minutes past the hour (Download and Install)					
> WildFire	Last checked: 2020/06/26 08:00:16 PDT		Schedule: Real-time			

Updates are configured with minimum time values to ensure new content loads are applied when available. They are also installed at the time of download.

Time schedules are varied around the hour to avoid download/install overlap between update types.

Antivirus

Includes new and updated antivirus signatures, including signatures discovered by WildFire. You must have a Threat Prevention subscription to get these updates. New antivirus signatures are published daily.

Applications and Threats

Includes new and updated application and threat signatures. This update is available if you have a Threat Prevention subscription (and in this case you will get this update instead of the Applications update). New Applications and Threats updates are published weekly. This means that the latest content update always includes the application and threat signatures released in previous versions.

WildFire

Provides real-time malware and antivirus signatures created as a result of the analysis done by the WildFire public cloud. Without the WildFire subscription, you must wait 24 to 48 hours for the WildFire signatures to roll into the Applications and Threat update.

GlobalProtect Clientless VPN

Contains new and updated application signatures to enable Clientless VPN access to common web applications from the GlobalProtect portal. You must have a GlobalProtect subscription to receive these updates. In addition, you must create a schedule for these updates before GlobalProtect Clientless VPN will function.

GlobalProtect Data File

Contains the vendor-specific information for defining and evaluating host information profile (HIP) data returned by GlobalProtect apps. You must have a GlobalProtect gateway subscription in order to receive these updates. In addition, you must create a schedule for these updates before GlobalProtect will function.

3.2 Network

3.2.1 Network Profiles

See also

General configuration information in the Admin Guide: [Network - Network Profiles](#)

Zone Protection

IronSkillet includes ‘non volumetric’ recommendations that are device and deployment specific. This is configured as the Recommended_Zone_Protection profile and should be added to configured zones. IronSkillet also provides an Alert_Only_Zone_Protection profile for users to monitor zones without blocking traffic.

Note: IronSkillet does not include zone configurations so the user must apply this profile when configured zones.

Network > Network Profiles > Zone Protection Profile > Recommended_Zone_Protection/Alert_Only_Zone_Protection > Reconnaissance Protection

Zone Protection Profile ?

Name Recommended_Zone_Protection

Description

Flood Protection

Reconnaissance Protection

Packet Based Attack Protection

Protocol Protection

Ethernet SGT Protection

SCAN	ENABLE	ACTION	INTERVAL (SEC)	THRESHOLD (EVENTS)
TCP Port Scan	<input checked="" type="checkbox"/>	alert	2	100
Host Sweep	<input checked="" type="checkbox"/>	alert	10	100
UDP Port Scan	<input checked="" type="checkbox"/>	alert	2	100

Q

0 items → X

TCP Port Scan, Host Sweep, and UDP Port Scan are enabled in alert-only mode to monitoring without blocking.

Note: Active blocking requires network tuning.

Network > Network Profiles > Zone Protection Profile > Recommended_Zone_Protection > Packet Based Attack Protection > IP Drop

Zone Protection Profile ⓘ

Name:

Description:

Flood Protection | Reconnaissance Protection | **Packet Based Attack Protection** | Protocol Protection | Ethernet SGT Protection

IP Drop | TCP Drop | ICMP Drop | IPv6 Drop | ICMPv6 Drop

☒ Spoofed IP address
☐ Strict IP Address Check
☐ Fragmented traffic

IP Option Drop

☐ Strict Source Routing
☐ Loose Source Routing
☐ Timestamp
☐ Record Route

☐ Security
☐ Stream ID
☐ Unknown
☒ Malformed

OK Cancel

IP Drop settings enabled for a spoofed IP address and malformed packets.

Network > Network Profiles > Zone Protection Profile > Alert_Only_Zone_Protection > Packet Based Attack Protection > IP Drop

Zone Protection Profile ⓘ

Name:

Description:

Flood Protection | Reconnaissance Protection | **Packet Based Attack Protection** | Protocol Protection | Ethernet SGT Protection

IP Drop | TCP Drop | ICMP Drop | IPv6 Drop | ICMPv6 Drop

☐ Spoofed IP address
☐ Strict IP Address Check
☐ Fragmented traffic

IP Option Drop

☐ Strict Source Routing
☐ Loose Source Routing
☐ Timestamp
☐ Record Route

☐ Security
☐ Stream ID
☐ Unknown
☐ Malformed

OK Cancel

No IP Drop settings have been enabled for the Alert Only profile.

Network > Network Profiles > Zone Protection Profile > Recommended_Zone_Protection > Packet Based Attack Protection > TCP Drop

Zone Protection Profile

Name

Recommended_Zone_Protection

Description

Flood Protection

Reconnaissance Protection

Packet Based Attack Protection

Protocol Protection

Ethernet SGT Protection

IP Drop

TCP Drop

ICMP Drop

IPv6 Drop

ICMPv6 Drop

☐ Mismatched overlapping TCP segment

☐ Split Handshake

☒ TCP SYN with Data

☒ TCP SYNACK with Data

Reject Non-SYN TCP

global

Asymmetric Path

global

Strip TCP Options

☒ TCP Timestamp

☐ TCP Fast Open

Multipath TCP (MPTCP) Options

global

OK

Cancel

TCP Drop settings enabled for TCP SYN with Data, SYNACK with Data. Also to strip TCP Timestamp.

Network > Network Profiles > Zone Protection Profile > Alert_Only_Zone_Protection > Packet Based Attack Protection > TCP Drop

Zone Protection Profile

Name

Alert_Only_Zone_Protection

Description

Flood Protection

Reconnaissance Protection

Packet Based Attack Protection

Protocol Protection

Ethernet SGT Protection

IP Drop

TCP Drop

ICMP Drop

IPv6 Drop

ICMPv6 Drop

☐ Mismatched overlapping TCP segment

☐ Split Handshake

☒ TCP SYN with Data

☒ TCP SYNACK with Data

Reject Non-SYN TCP

global

Asymmetric Path

global

Strip TCP Options

☐ TCP Timestamp

☐ TCP Fast Open

Multipath TCP (MPTCP) Options

global

OK

Cancel

Default TCP Drop settings are set here with nothing more enabled for the Alert Only profile.

Note: These are explicit enables in the template to ensure not disabled across software versions.

3.3 Objects

This section includes various profiles, objects, and tags used primarily in security and decryption policies.

3.3.1 Tags

See also

General configuration information in the Admin Guide: [Objects - Tags](#)

IronSkillet Tag Objects

Object > Tags : directionals and version

<input type="checkbox"/>	NAME ^	COMMENTS
<input type="checkbox"/>	empty	
<input type="checkbox"/>	Inbound	Inbound from the Internet
<input type="checkbox"/>	Internal	Internal to Internal
<input type="checkbox"/>	iron-skillet-version	version 0.0.1 for 10.0: version of this IronSkillet template file
<input type="checkbox"/>	Outbound	Outbound to the Internet
<input type="checkbox"/>	Sanctioned	

Reference tags used in security policies along with an 'IronSkillet' version tag.

- **Outbound:** traffic from internal to external
- **Inbound:** traffic from external to internal
- **Internal:** internal-only traffic

Note: The iron-skillet-version tag is used for release tracking only.

3.3.2 Custom Objects

See also

General configuration information in the Admin Guide: [Objects - Custom Objects](#)

User generated objects as placeholders.

IronSkillet Custom Objects

Object > Custom Objects > URL Category

<input type="checkbox"/>	NAME	TYPE
<input type="checkbox"/>	Black-List	URL List
<input type="checkbox"/>	White-List	URL List
<input type="checkbox"/>	Custom-No-Decrypt	URL List

Placeholder for custom url categories used in security rules and url profiles. Using these categories prevents the need to modify the default template.

- **Block:** placeholder to be used in block rules and objects to override default template behavior
- **Allow:** placeholder to be used in permit rules and objects to override default template behavior
- **Custom-No-Decrypt:** to be used in the decryption no-decrypt rule to specify URLs that should no be decrypted

3.3.3 Security Profiles

See also

General configuration information in the Admin Guide: [Objects - Security Profiles](#)

Security profiles in IronSkillet are explicitly named using one or more of the following:

- **Outbound:** traffic originating inside the network accessing external sites
- **Inbound:** traffic originating outside the network accessing internal sites
- **Internal:** traffic originating inside the network access other internal sites
- **Alert-Only:** alert-only for any traffic sessions; not recommended when blocking required

AntiVirus

Antivirus profiles to protect against worms, viruses, and trojans and to block spyware downloads.

Outbound, Inbound, and Internal AntiVirus (AV) profiles.

Object > Security Profiles > Antivirus : Blocking

- reset-both for all decoder actions: Antivirus and Wildfire
- Includes reset-both for Dynamic Classification actions
- Includes enable for all file types

<input type="checkbox"/>	NAME	LOCATION	PACKET CAPTURE	Decoders				Application Exceptions		WildFire Inline ML		SIGNATURE EXCEPTIONS	WILDFIRE INLINE ML EXCEPTIONS
				PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION	APPLICATION	ACTION	MODEL	ACTION SETTING		
<input type="checkbox"/>	Outbound-AV		<input type="checkbox"/>	http	reset-both	reset-both	reset-both			Windows Executables	enable (inherit per-protocol actions)	0	0
				http2	reset-both	reset-both	reset-both			PowerShell Script 1	enable (inherit per-protocol actions)		
				smtp	reset-both	reset-both	reset-both			PowerShell Script 2	enable (inherit per-protocol actions)		
				imap	reset-both	reset-both	reset-both			Executable Linked Format	enable (inherit per-protocol actions)		
				pop3	reset-both	reset-both	reset-both			MSOffice	enable (inherit per-protocol actions)		
				ftp	reset-both	reset-both	reset-both			Shell	enable (inherit per-protocol actions)		
				smb	reset-both	reset-both	reset-both						
<input type="checkbox"/>	Inbound-AV		<input type="checkbox"/>	http	reset-both	reset-both	reset-both			Windows Executables	enable (inherit per-protocol actions)	0	0
				http2	reset-both	reset-both	reset-both			PowerShell Script 1	enable (inherit per-protocol actions)		
				smtp	reset-both	reset-both	reset-both			PowerShell Script 2	enable (inherit per-protocol actions)		
				imap	reset-both	reset-both	reset-both			Executable Linked Format	enable (inherit per-protocol actions)		
				pop3	reset-both	reset-both	reset-both			MSOffice	enable (inherit per-protocol actions)		
				ftp	reset-both	reset-both	reset-both			Shell	enable (inherit per-protocol actions)		
				smb	reset-both	reset-both	reset-both						
<input type="checkbox"/>	Internal-AV		<input type="checkbox"/>	http	reset-both	reset-both	reset-both			Windows Executables	enable (inherit per-protocol actions)	0	0
				http2	reset-both	reset-both	reset-both			PowerShell Script 1	enable (inherit per-protocol actions)		
				smtp	reset-both	reset-both	reset-both			PowerShell Script 2	enable (inherit per-protocol actions)		
				imap	reset-both	reset-both	reset-both			Executable Linked Format	enable (inherit per-protocol actions)		
				pop3	reset-both	reset-both	reset-both			MSOffice	enable (inherit per-protocol actions)		
				ftp	reset-both	reset-both	reset-both			Shell	enable (inherit per-protocol actions)		
				smb	reset-both	reset-both	reset-both						

These are all explicitly set to reset-both for all decoders.

Object > Security Profiles > Antivirus : Alert-Only

- alert for all decoder actions: Antivirus and Wildfire
- Includes alert for Dynamic Classification actions
- Includes enable (alert only) for all file types

<input type="checkbox"/>	NAME	LOCATION	PACKET CAPTURE	Decoders				Application Exceptions		WildFire Inline ML		SIGNATURE EXCEPTIONS	WILDFIRE INLINE ML EXCEPTIONS
				PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION	APPLICATION	ACTION	MODEL	ACTION SETTING		
<input type="checkbox"/>	Alert-Only-AV		<input type="checkbox"/>	http	alert	alert	alert			Windows Executables	alert-only (override more strict actions to alert)	0	0
				http2	alert	alert	alert			PowerShell Script 1	alert-only (override more strict actions to alert)		
				smtp	alert	alert	alert			PowerShell Script 2	alert-only (override more strict actions to alert)		
				imap	alert	alert	alert			Executable Linked Format	alert-only (override more strict actions to alert)		
				pop3	alert	alert	alert			MSOffice	alert-only (override more strict actions to alert)		
				ftp	alert	alert	alert			Shell	alert-only (override more strict actions to alert)		
				smb	alert	alert	alert						

Sets all decoders to alert mode.

Anti-Spyware

Anti-Spyware profiles to block attempts from spyware on compromised hosts trying to phone-home or beacon out to external command-and-control (C2) servers.

Object > Security Profiles > Antivirus : Outbound-AS

Rules: Outbound Anti-Spyware (AS) and Inbound-AS profiles

Anti-Spyware Profile

Name

Outbound-AS

Description

Signature Policies

Signature Exceptions

DNS Policies

DNS Exceptions

<input type="checkbox"/>	POLICY NAME	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	Block-Critical-High-Medium	critical high medium	reset-both	single-packet
<input type="checkbox"/>	Default-Low-Info	low informational	default	disable

Rules block critical, high, and medium severity events. For low and informational, default is used.

Note: Only Outbound-AS is shown with Inbound-AS having an identical configuration.

Exceptions: Checking Default Actions

To see the actions for 'default', click into Exceptions and enable 'Show all signatures'. The Action column shows default actions for each ID.

Anti-Spyware Profile ?

Name:

Description:

Signature Policies | **Signature Exceptions** | DNS Policies | DNS Exceptions

10302 items → ×

ENAB...	ID	THREAT NAME	IP ADDRESS EXEMPTIONS	POLICY	CATEGORY	SEVERITY	ACTION ^	PACKET CAPTURE
<input type="checkbox"/>	18250	Microsoft Phishing Site Detection		Block-Critical-High-Medium	phishing-kit	critical	default (reset-both)	disable
<input type="checkbox"/>	18575	Bartblaze PHP Webshell Traffic Detection		Block-Critical-High-Medium	webshell	medium	default (alert)	disable
<input type="checkbox"/>	18864	FTSRAT Command and Control Traffic Detection		Block-Critical-High-Medium	spyware	critical	default (reset-both)	disable
<input type="checkbox"/>	18412	CrimsonRAT.Gen Command And Control Traffic		Block-Critical-High-Medium	spyware	critical	default (reset-both)	disable
<input type="checkbox"/>	18295	Floriensh4x bc0de PHP Webshell Upload Detection		Block-Critical-High-Medium	webshell	critical	default (reset-both)	disable
<input type="checkbox"/>	18896	BabyShark Command and Control Traffic Detection		Block-Critical-High-Medium	spyware	critical	default (reset-both)	disable
<input type="checkbox"/>	18555	Microsoft Phishing Site		Block-Critical-	phishing-kit	critical	default (reset-	disable

☒ Show all signatures Page 1 of 344 | Displaying 1 - 30/ 10302 threats

DNS Signature: Sinkhole Malicious Domains

Anti-Spyware Profile ?

Name:

Description:

Signature Policies | Signature Exceptions | **DNS Policies** | DNS Exceptions

DNS Policies 9 items → ×

SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
▼ : Palo Alto Networks Content			
<input type="checkbox"/> default-paloalto-dns		sinkhole	single-packet
▼ : DNS Security			
<input type="checkbox"/> Command and Control Domains	default (high)	sinkhole	single-packet
<input type="checkbox"/> Dynamic DNS Hosted Domains	default (informational)	default (allow)	single-packet
<input type="checkbox"/> Grayware Domains	default (low)	sinkhole	single-packet

DNS Sinkhole Settings

Sinkhole IPv4:

Sinkhole IPv6:

The profile also sinkholes malicious domains based on the sinkhole settings. The settings map to the address objects and sinkhole redirects can be dropped as part of the security policies if no sinkhole server is used.

Note: As of 9.0, instead of only leveraging a list of locally stored malicious domains (Content DNS Signatures), Palo Alto Networks also provides a DNS Security service subscription for cloud-based domain lookups.

DNS Security Service: Sinkhole Malicious Domains by Category

Anti-Spyware Profile

Name

Outbound-AS

Description

Signature Policies

Signature Exceptions

DNS Policies

DNS Exceptions

DNS Policies

<input type="checkbox"/>	Command and Control Domains	default (high)	sinkhole	single-packet
<input type="checkbox"/>	Dynamic DNS Hosted Domains	default (informational)	default (allow)	single-packet
<input type="checkbox"/>	Grayware Domains	default (low)	sinkhole	single-packet
<input type="checkbox"/>	Malware Domains	default (medium)	sinkhole	single-packet
<input type="checkbox"/>	Parked Domains	default (informational)	default (allow)	disable
<input type="checkbox"/>	Phishing Domains	default (low)	sinkhole	single-packet
<input type="checkbox"/>	Proxy Avoidance and Anonymizers	default (low)	sinkhole	single-packet
<input type="checkbox"/>	Newly Registered Domains	default (informational)	default (allow)	single-packet

DNS Sinkhole Settings

Sinkhole IPv4

sinkhole.paloaltonetworks.com

Sinkhole IPv6

2600:5200::1

OK

Cancel

In 10.0 and later, the DNS Security Service includes the ability to set actions by category. IronSkillet sets explicitly ‘sinkhole’ actions for each malicious category (Command-and-Control, Malware) leaving the others as default. Severities are also left as default.

Object > Security Profiles > Antivirus : Internal-AS

The Internal profile shifts the medium severity to ‘default’ instead of reset both slightly lowering the security posture for internal-only sessions.

Anti-Spyware Profile

Name

Internal-AS

Description

Signature Policies

Signature Exceptions

DNS Policies

DNS Exceptions

<input type="checkbox"/>	POLICY NAME	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	Block-Critical-High-Medium	critical high medium	reset-both	single-packet
<input type="checkbox"/>	Default-Low-Info	low informational	default	disable

The DNS Signatures and Security Service configurations are the same as Outbound-AS and Inbound-AS.

Object > Security Profiles > Antivirus : Alert-Only

This is a non-blocking alert-only configuration that can be used for testing/demonstration purposes.

Anti-Spyware Profile

Name:

Description:

Signature Policies | Signature Exceptions | DNS Policies | DNS Exceptions

<input type="checkbox"/>	POLICY NAME	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	Alert-All	any	alert	disable

All DNS Security Service domain actions are set to 'allow' with no blocking posture.

Anti-Spyware Profile

Name:

Description:

Signature Policies | Signature Exceptions | **DNS Policies** | DNS Exceptions

DNS Policies

<input type="checkbox"/>	Command and Control Domains	default (high)	allow	single-packet
<input type="checkbox"/>	Dynamic DNS Hosted Domains	default (informational)	allow	single-packet
<input type="checkbox"/>	Grayware Domains	default (low)	allow	single-packet
<input type="checkbox"/>	Malware Domains	default (medium)	allow	single-packet
<input type="checkbox"/>	Parked Domains	default (informational)	default (allow)	disable
<input type="checkbox"/>	Phishing Domains	default (low)	allow	single-packet
<input type="checkbox"/>	Proxy Avoidance and Anonymizers	default (low)	allow	single-packet
<input type="checkbox"/>	Newly Registered Domains	default (informational)	allow	single-packet

DNS Sinkhole Settings

Sinkhole IPv4:

Sinkhole IPv6:

OK Cancel

Vulnerability

Vulnerability protection profiles to stop attempts to exploit system flaws or gain unauthorized access to systems.

Object > Security Profiles > Vulnerability Protection : Outbound-VP

Vulnerability Protection Profile ?

Name

Description

Rules | Exceptions

<input type="checkbox"/>	RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	Block-Critical-High-Medium	any	any	any	critical high medium	reset-both	single-packet
<input type="checkbox"/>	Default-Low-Info	any	any	any	low informational	default	disable

IronSkillet adds two rules:

- (1) reset-both for critical/high/medium severity events
- (2) the use of default actions for low and informational severities.

Vulnerability Protection Profile ?

Name

Description

Rules | Exceptions | **Inline Cloud Analysis**

☒ Enable cloud inline analysis

Available Analysis Engines

2 items → ×

MODEL	DESCRIPTION	ACTION
SQL Injection	Detects a common hacking technique where an attacker inserts SQL queries into an applications' request	reset-both
Command Injection	Detects a common hacking technique that allows an attacker to execute arbitrary operating system (OS)	reset-both

IronSkillet in 11.0 also enables cloud inline analysis and sets analysis engines to reset-both.

Object > Security Profiles > Vulnerability Protection : Inbound-VP

Vulnerability Protection Profile ?

Name

Description

Rules | Exceptions

<input type="checkbox"/>	RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	Block-Critical-High-Medium	any	any	any	critical high medium	reset-both	single-packet
<input type="checkbox"/>	Default-Low-Info	any	any	any	low informational	default	disable

Currently identical to the above Outbound profile to block critical/high/medium and use 'default' for low and informational severities.

Vulnerability Protection Profile ?

Name

Description

Rules | Exceptions | **Inline Cloud Analysis**

☒ Enable cloud inline analysis

Available Analysis Engines

MODEL	DESCRIPTION	ACTION
SQL Injection	Detects a common hacking technique where an attacker inserts SQL queries into an applications' request	reset-both
Command Injection	Detects a common hacking technique that allows an attacker to execute arbitrary operating system (OS)	reset-both

For IronSkillet 11.0 the cloud inline analysis settings for the Inbound-VP profile are also identical to the Outbound profile.

Object > Security Profiles > Vulnerability Protection : Internal-VP

Vulnerability Protection Profile ?

Name

Description

Rules | Exceptions

<input type="checkbox"/>	RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	Block-Critical-High	any	any	any	critical high	reset-both	single-packet
<input type="checkbox"/>	Default-Medium-Low-Info	any	any	any	low informational medium	default	disable

As with the Anti-spyware internal profile, medium is set as 'default' along with low and informational. This adds some trust to internal-only communications.

Vulnerability Protection Profile ?

Name

Description

Rules | Exceptions | **Inline Cloud Analysis**

☒ Enable cloud inline analysis

Available Analysis Engines

2 items → ×

MODEL	DESCRIPTION	ACTION
SQL Injection	Detects a common hacking technique where an attacker inserts SQL queries into an applications' request	reset-both
Command Injection	Detects a common hacking technique that allows an attacker to execute arbitrary operating system (OS)	reset-both

For IronSkillet 11.0 the cloud inline analysis settings for the Internal-VP profile are identical to the Outbound and Inbound profiles.

Object > Security Profiles > Vulnerability Protection : Alert-Only-VP

Vulnerability Protection Profile ?

Name

Description

Rules | Exceptions

<input type="checkbox"/>	RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	Alert-All	any	any	any	any	alert	disable

Alert-Only provides a monitoring-only profile for vulnerability events. It is designed for use in demonstration or test deployments without active blocking.

Vulnerability Protection Profile ?

Name
 Description

Rules | Exceptions | **Inline Cloud Analysis**

☒ Enable cloud inline analysis

Available Analysis Engines

2 items
→
×

MODEL	DESCRIPTION	ACTION
SQL Injection	Detects a common hacking technique where an attacker inserts SQL queries into an applications' request	alert
Command Injection	Detects a common hacking technique that allows an attacker to execute arbitrary operating system (OS)	alert

For IronSkillet 11.0 the cloud inline analysis settings are activated while the analysis engines are set to alert mode.

URL Filtering

URL filtering profiles to restrict users access to specific websites and/or website categories, such as shopping or gambling.

Object > Security Profiles > URL-Filtering

<input type="checkbox"/>	NAME	LOCATION	SITE ACCESS	USER CREDENTIAL SUBMISSION	HTTP HEADER INSERTION
<input type="checkbox"/>	default	Predefined	Allow Categories (58) Alert Categories (5) Continue Categories (0) Block Categories (10) Override Categories (0)	Allow Categories (73) Alert Categories (0) Continue Categories (0) Block Categories (0)	
<input type="checkbox"/>	Outbound-URL		Allow Categories (0) Alert Categories (70) Continue Categories (0) Block Categories (5) Override Categories (0)	Allow Categories (0) Alert Categories (0) Continue Categories (0) Block Categories (75)	
<input type="checkbox"/>	Alert-Only-URL		Allow Categories (0) Alert Categories (75) Continue Categories (0) Block Categories (0) Override Categories (0)	Allow Categories (0) Alert Categories (75) Continue Categories (0) Block Categories (0)	

IronSkillet provides only 2 profiles for URL excluding the Inbound and Internal used in the other profiles. The IronSkillet assumption is that only outbound requests may be accessing malicious sites. In IronSkillet 10.1 added advanced URL Filtering changes, specifically updated real-time-detection categories to alert for all profiles.

Object > Security Profiles > URL-Filtering : HTTP Header Logging

The screenshot shows the 'URL Filtering Profile' configuration window. The 'Name' field is 'Sample-URL' and the 'Description' field is empty. The 'URL Filtering Settings' tab is selected, showing options for 'Log container page only' (checked), 'Safe Search Enforcement' (unchecked), and 'HTTP Header Logging' (checked). Under 'HTTP Header Logging', 'User-Agent', 'Referer', and 'X-Forwarded-For' are all checked. 'OK' and 'Cancel' buttons are at the bottom right.

User-Agent, Referer and X-Forwarded-For HTTP Header Logging options have all been toggled on, added in IronSkillet 10.2.

Object > Security Profiles > URL-Filtering : Advanced URL Filtering

The screenshot shows the 'URL Filtering Profile' configuration window. The 'Name' field is 'Sample-URL' and the 'Description' field is empty. The 'Inline Categorization' tab is selected, showing options for 'Enable local inline categorization' (checked) and 'Enable cloud inline categorization' (checked). The 'Exceptions' section shows a list with a header 'CUSTOM URL CATEGORY/EDL' and an expand/collapse arrow. At the bottom of the exceptions list are '+ Add' and '- Delete' buttons. 'OK' and 'Cancel' buttons are at the bottom right.

Advanced URL Filtering inline local and cloud categorization have all been toggled on, added in Ironskillet 10.2.

Object > Security Profiles > URL-Filtering : Outbound-URL**Categories: Site Access**

IronSkillet only blocks known malicious categories and not high risk categories such as copyright-infringement mentioned in our Best Practice Assessment (BPA).

Categories blocked in the Outbound profiles:

- Malware
- Command-and-Control
- Phishing
- Ransomware
- Grayware
- Block [custom object users can edit]

All other categories have their action set as 'alert' instead of the default 'allow' for logging purposes.

URL Filtering Profile

Name

Outbound-URL

Description

Categories

URL Filtering Settings

User Credential Detection

HTTP Header Insertion

Dynamic Classification

hack

75 items

<input type="checkbox"/>	CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
<input type="checkbox"/>	command-and-control	block	block
<input type="checkbox"/>	grayware	block	block
<input type="checkbox"/>	malware	block	block
<input type="checkbox"/>	phishing	block	block
<input type="checkbox"/>	abortion	alert	block
<input type="checkbox"/>	abused-drugs	alert	block
<input type="checkbox"/>	adult	alert	block
<input type="checkbox"/>	alcohol-and-tobacco	alert	block

* indicates a custom URL category, + indicates external dynamic list

[Check URL Category](#)

For releases 10.0 and later, Dynamic Classification is configured for local machine learning and blocking based on web page analysis.

URL Filtering Profile

Name

Outbound-URL

Description

Categories

URL Filtering Settings

User Credential Detection

HTTP Header Insertion

Dynamic Classification

Available Classification Engines

2 items

ENGINES	DESCRIPTION	POLICY ACTION
Phishing Detection	Machine Learning engine to dynamically identify credential phishing pages	block
Javascript Exploit Detection	Machine Learning engine to dynamically detect Javascript based exploitation attacks	block

Categories: User Credential Submission

If you block all the URL categories in a URL Filtering profile for user credential submission, you don't need to check credentials. IronSkillet takes this approach blocking all categories under User Credential Submission.

The Alert-Only-URL profile sets all actions to alert for logging purposes, including Dynamic Classification and User Credential Submission. No categories are blocked.

File Blocking

This set of profiles allow the NGFW to explicitly block files transiting the firewall by type and direction.

Object > Security Profiles > File-Blocking

<input type="checkbox"/>	NAME	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
<input type="checkbox"/>	basic file blocking	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf	both	block
		Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
		Log all other file types	any	both	alert	
<input type="checkbox"/>	strict file blocking	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
		Block encrypted files	any	encrypted-rar, encrypted-zip	both	block
		Log all other file types	any	both	alert	
<input type="checkbox"/>	Outbound-FB	Alert-All	any	any	both	alert
		Block	any	7z, bat, chm, class, cpl, dll, hlp, hta, jar, ocx, pif, scr, torrent, vbe, wsf	both	block
<input type="checkbox"/>	Inbound-FB	Alert-All	any	any	both	alert
		Block	any	7z, bat, chm, class, cpl, dll, hlp, hta, jar, ocx, pif, scr, torrent, vbe, wsf	both	block
<input type="checkbox"/>	Internal-FB	Alert-All	any	any	both	alert
		Block	any	7z, bat, chm, class, cpl, hlp, hta, jar, ocx, pif, scr, torrent, vbe, wsf	both	block
<input type="checkbox"/>	Alert-Only-FB	Alert-Only	any	any	both	alert

IronSkillet defines a day one perspective without variations in file blocking based on URL category, direction, or application. File types that are not blocked are set as 'alert' for logging purposes.

The set of blocked file types represents the most common malicious file types that typically are not expected to cross a security zone boundary. Other types are ignored (eg. exe) since these can be used for legitimate, although not recommended, business purposes.

Note: Supported WildFire file types, even if blocked, will be sent to WildFire for analysis if Wildfire is license and configured in the device.

External Dynamic Lists

EDL's are text files that allow the firewall to import objects and enforce policies based on contents of the EDL. In order to enforce policies on the entries included in the EDL, the list must be referenced in a supported policy rule or profile. Added in 10.2 Ironskillet are Bulletproof IP addresses and Tor exit IP addresses.

Object > External Dynamic Lists

<input type="checkbox"/>	NAME	LOCATION	DESCRIPTION	SOURCE	CERTIFICATE PROFILE	FREQUENCY
<input type="checkbox"/>	Palo Alto Networks BulletProof IP Addresses		IP addresses that are provided by bulletproof hosting providers. Because bulletproof hosting providers place few, if any, restrictions on content, attackers can use these services to host and distribute malicious, illegal, and unethical material.	Palo Alto Networks - Bulletproof IP addresses		
<input type="checkbox"/>	Palo Alto Networks Tor exit IP Addresses		IP addresses supplied by multiple providers and validated with Palo Alto Networks threat intelligence data as active Tor exit nodes. Traffic from Tor exit nodes are disproportionately associated with malicious activity.	Palo Alto Networks - Tor exit IP addresses		

WildFire Analysis

WildFire™ analysis profiles to specify for file analysis to be performed locally on the WildFire appliance or in the WildFire cloud. IronSkillet uses the cloud option.

Object > Security Profiles > WildFire Analysis

<input type="checkbox"/>	NAME	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
<input type="checkbox"/>	default	default	any	any	both	public-cloud
<input type="checkbox"/>	Outbound-WF	Forward-All	any	any	both	public-cloud
<input type="checkbox"/>	Inbound-WF	Forward-All	any	any	both	public-cloud
<input type="checkbox"/>	Internal-WF	Forward-All	any	any	both	public-cloud
<input type="checkbox"/>	Alert-Only-WF	Forward-All	any	any	both	public-cloud

All profiles are set to send all file types for all applications in any direction to WildFire for analysis.

This configuration is for file analysis submissions only. WildFire signatures and protections are configured in the Anti-Virus profile. Below is the reference example for the Outbound-AV profile.

Antivirus Profile ?

Name

Outbound-AV

Description

Action

Virus Exception

Dynamic Classification

☐ Enable Packet Capture

Decoders

DECODER ^	ACTION	WILDFIRE ACTION	DYNAMIC CLASSIFICATION ACTION
ftp	reset-both	reset-both	reset-both
http	reset-both	reset-both	reset-both
http2	reset-both	reset-both	reset-both
imap	reset-both	reset-both	reset-both
pop3	reset-both	reset-both	reset-both
smb	reset-both	reset-both	reset-both
smtp	reset-both	reset-both	reset-both

Based on the dynamic updates configuration, the device will check for new WildFire content updates based on world-wide analysis to download the latest signatures. These signatures are moved to the antivirus signature set on a daily basis for customers not subscribing to the WildFire service.

3.3.4 Security Profile Groups

See also

General configuration information in the Admin Guide: [Objects - Security Profile Groups](#)

In addition to individual profiles, you can combine profiles that are often applied together, and create Security Profile groups. These can be referenced in a security profile without the need to explicitly reference each profile.

IronSkillet Security Profile Groups

Object > Security Profile Groups : all groups

<input type="checkbox"/>	NAME	ANTIVIRUS PROFILE	ANTI-SPYWARE PROFILE	VULNERABILITY PROTECTION PROFILE	URL FILTERING PROFILE	FILE BLOCKING PROFILE	DATA FILTERING PROFILE	WILDFIRE ANALYSIS PROFILE
<input type="checkbox"/>	Outbound	Outbound-AV	Outbound-AS	Outbound-VP	Outbound-URL	Outbound-FB		Outbound-WF
<input type="checkbox"/>	Inbound	Inbound-AV	Inbound-AS	Inbound-VP		Inbound-FB		Inbound-WF
<input type="checkbox"/>	Internal	Internal-AV	Internal-AS	Internal-VP		Internal-FB		Internal-WF
<input type="checkbox"/>	Alert-Only	Alert-Only-AV	Alert-Only-AS	Alert-Only-VP	Alert-Only-URL	Alert-Only-FB		Alert-Only-WF
<input type="checkbox"/>	default	Outbound-AV	Outbound-AS	Outbound-VP	Outbound-URL	Outbound-FB		Outbound-WF

Each profile group is associated to the set of profiles reference the same direction or 'alert' mode.

The default profile, based on the Outbound security profiles, is created so that new security policies can easily reference this default profile group.

IronSkillet does not reference the security profile objects since IronSkillet does not have explicit allow rules.

3.3.5 Log Forwarding

See also

General configuration information in the Admin Guide: [Objects - Log Forwarding](#)

Sets up log forwarding profiles referenced in security policies.

IronSkillet Log Forwarding

Object > Log Forwarding : default

<input type="checkbox"/>	NAME	LOG TYPE	FILTER	PANORAMA	EMAIL	SYSLOG
<input type="checkbox"/>	default	traffic	All Logs	<input type="checkbox"/>		Sample_Syslog_Profile
		threat	All Logs	<input type="checkbox"/>		Sample_Syslog_Profile
		wildfire	All Logs	<input type="checkbox"/>		Sample_Syslog_Profile
		url	All Logs	<input type="checkbox"/>		Sample_Syslog_Profile
		data	All Logs	<input type="checkbox"/>		Sample_Syslog_Profile
		tunnel	All Logs	<input type="checkbox"/>		Sample_Syslog_Profile
		auth	All Logs	<input type="checkbox"/>		Sample_Syslog_Profile
		wildfire	(verdict neq benign)	<input type="checkbox"/>	Sample_Email_Profile	

IronSkillet sets all log events to be sent to Syslog. Any malicious or phishing WildFire verdicts are emailed using the Threat Alert email profile. The Panorama associated configuration sends log to Panorama. Users can modify the default logging profile to send logs to additional locations as required.

The 'default' naming is used so that new security rules will automatically pick up this logging profile.

3.3.6 Decryption

Decryption profiles enable you to block and control specific aspects of SSL and SSH traffic that you have specified for decryption, as well as traffic that you have explicitly excluded from decryption. After you create a decryption profile, you can then add that profile to a decryption policy; any traffic matched to the decryption policy is additionally enforced based on the profile settings.

Decryption Profile

See also

General configuration information in the Admin Guide: [Objects - Decryption Profile](#)

Object > Decryption > Decryption Profile : Recommended_Decryption_Profile

The Recommended_Decryption_Profile is provided to set several baseline, recommended profile elements.

Decryption Profile > SSL Decryption : SSL Forward Proxy

Decryption Profile

Name
Recommended_Decryption_Profile

SSL Decryption
No Decryption
SSH Proxy

SSL Forward Proxy
SSL Inbound Inspection
SSL Protocol Settings

Server Certificate Verification

- ☒ Block sessions with expired certificates
- ☒ Block sessions with untrusted issuers
- ☒ Block sessions with unknown certificate status
- ☒ Block sessions on certificate status check timeout
- ☐ Restrict certificate extensions [Details](#)
- ☐ Append certificate's CN value to SAN extension

Unsupported Mode Checks

- ☒ Block sessions with unsupported versions
- ☒ Block sessions with unsupported cipher suites
- ☐ Block sessions with client authentication

Failure Checks

- ☐ Block sessions if resources not available
- ☐ Block sessions if HSM not available
- ☐ Block downgrade on no resource

Client Extension

- ☐ Strip ALPN

Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.

If using SSL Forward Proxy, block sessions with invalid certs and versions.

Decryption Profile > SSL Decryption : SSL Protocol Settings

Decryption Profile

Name
Recommended_Decryption_Profile

SSL Decryption
No Decryption
SSH Proxy

SSL Forward Proxy
SSL Inbound Inspection
SSL Protocol Settings

Protocol Versions

Min Version
TLSv1.2

Max Version
TLSv1.3

Key Exchange Algorithms

☐ RSA
☒ DHE
☒ ECDHE

Encryption Algorithms

☐ 3DES
☒ AES128-CBC
☒ AES128-GCM
☒ CHACHA20-POLY1305

☐ RC4
☒ AES256-CBC
☒ AES256-GCM

Authentication Algorithms

☐ MD5
☐ SHA1
☒ SHA256
☒ SHA384

Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.

Protocol versions: Set the minimum protocol version to TLSv1.2. Any TLSv1.1 errors can help find outdated TLS endpoints

In 10.0, the max protocol version is set to TLSv1.3.

Encryption Algorithms: 3DES and RC4 not recommended and unavailable when TLSv1.2 is the minimum version.

Authentication Algorithms: MD5 not recommended and unavailable when TLSv1.2 is the minimum version

Decryption Profile > No Decryption

Decryption Profile ?

Name

SSL Decryption **No Decryption** SSH Proxy

Server Certificate Verification

☒ Block sessions with expired certificates
 ☒ Block sessions with untrusted issuers

Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.

Even without decrypting, the recommended profile can block session with invalid certs or untrusted issuers.

3.4 Policies

3.4.1 Security

See also

General configuration information in the Admin Guide: [Policies - Security](#)

IronSkillet Security Policies

IronSkillet only provides suggested block rules and no traffic passing allow rules. When admins add new security rules, they should reference the security profile groups and logging profile configured under Objects.

Policies > Security : Block Malicious IPs

	NAME	TAGS	Source			Destination		APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	ZONE	ADDRESS					
1	Outbound Block Rule	Outbound	any	any	any	any	<div>Palo Alto Netw...</div> <div>Palo Alto Netw...</div> <div>Palo Alto Netw...</div>	any	any	Deny	none	<div></div> <div></div>
2	Inbound Block Rule	Inbound	any	<div>Palo Alto Netw...</div> <div>Palo Alto Netw...</div> <div>Palo Alto Netw...</div>	any	any	any	any	any	Deny	none	<div></div> <div></div>
3	Intrazone-default	none	any	any	any	(intrazone)	any	any	any	Allow	<div></div>	<div></div> <div></div>
4	Interzone-default	none	any	any	any	any	any	any	any	Drop	none	<div></div> <div></div>

Inbound and Outbound Block Rules Recommended Deny rules using the Palo Alto Networks predefined external dynamic lists (EDLs).

From Objects > External Dynamic Lists:

<input type="checkbox"/>	NAME	LOCATION	DESCRIPTION	SOURCE
▼ Dynamic IP Lists				
<input type="checkbox"/>	Palo Alto Networks - Bulletproof IP addresses	Predefined	IP addresses that are provided by bulletproof hosting providers. Because bulletproof hosting providers place few, if any, restrictions on content, attackers can use these services to host and distribute malicious, illegal, and unethical material.	Palo Alto Networks - Bulletproof IP addresses
<input type="checkbox"/>	Palo Alto Networks - High risk IP addresses	Predefined	IP addresses that have recently been featured in threat activity advisories distributed by high-trust organizations. However, Palo Alto Networks does not have direct evidence of maliciousness for these IP addresses.	Palo Alto Networks - High risk IP addresses
<input type="checkbox"/>	Palo Alto Networks - Known malicious IP addresses	Predefined	IP addresses that are currently used almost exclusively by malicious actors for malware distribution, command-and-control, and for launching various attacks.	Palo Alto Networks - Known malicious IP addresses

These external dynamic lists (EDLs) require a threat subscription and content update. Before configuring these security rules, the user needs to ensure that the EDLs show up under Objects - External Dynamic Lists. If not present, either the subscription is not valid or the content update has not been performed.

3.4.2 Decryption

See also

General configuration information in the Admin Guide: [Policies - Decryption](#)

IronSkillet Decryption Policies

The IronSkillet decryption policies contain two rules: (1) An optional no-decrypt URL category rule to bypass recommended URL categories when SSL decrypt is enabled and (2) a default NO-Decrypt rule that only provides cert validation checks according to the Recommended_Decryption_Profile.

Neither of the two rules perform any decryption but rather validate the encrypted sessions (SSL/SSH) meet particular integrity and encryption standards.

Policies > Decryption : no decrypt

	NAME	Source			Destination		URL CATEGORY	SERVICE	ACTION
		ZONE	ADDRESS	USER	ZONE	ADDRESS			
1	NO-Decrypt URL Cat...	any	any	any	any	any	financial-services government health-and-med... Custom-No-Decr...	any	no-decrypt

SSL Decryption is highly recommended to gain visibility to traffic sessions yet is not part of the IronSkillet configuration template due to various requirements around certificates and application testing before full implementations. Included is a reference decryption rule for 'no decrypt' URL categories.

3.5 Monitor

3.5.1 Manage Custom Reports

See also

General configuration information in the Admin Guide: [Monitor - Custom Reports](#)

IronSkillet Custom Reports

IronSkillet includes a small set of custom reports aimed at SecOps practices and discovering malicious behavior. These can be used as a reference for additional custom reports.

Monitor > Manage Custom Reports

<input type="checkbox"/>	NAME	DESCRIPTION	DATABASE	TIME FRAME	ROWS	SORT BY	GROUP BY	SCHEDUL...
<input type="checkbox"/>	Host-visit malicious sites plus		URL Log	Last 7 Calendar Days	500	Count	src	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Hosts visit malicious sites		URL Log	Last 7 Calendar Days	500	Count	src	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Hosts visit questionable sites		URL Log	Last 7 Calendar Days	500	Count	src	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Host-visit quest sites plus	Detail of hosts visiting questionable URLs	URL Log	Last 7 Calendar Days	500	Count	src	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Wildfire malicious verdicts	Files uploaded or downloaded that were later found to be malicious. This is a summary. Act on real-time email.	WildFire Submissions	Last 30 Calendar Days	500	Count		<input checked="" type="checkbox"/>
<input type="checkbox"/>	Wildfire verdicts SMTP	Links sent from emails found to be malicious.	WildFire Submissions	Last 30 Calendar Days	500	Count		<input checked="" type="checkbox"/>
<input type="checkbox"/>	Clients sinkholed		Traffic Log	Last 30 Calendar Days	500	Count	from	<input checked="" type="checkbox"/>

Monitor > Management > Custom Reports > Host-visit malicious sites plus

Custom Report

Report Setting

Load Template → Run Now

Name	Host-visit malicious sites plus	Available Columns	Selected Columns
Description		App Category	Source Zone
Database	URL Log	App Container	Source User
	<input checked="" type="checkbox"/> Scheduled	App Sub Category	Category
Time Frame	Last 7 Calendar Days	App Technology	Action
Sort By	Count	Application	Count
Group By	Source Address		
	Top 500		
	50 Groups		

Query Builder

(category eq command-and-control) or (category eq hacking) or (category eq malware) or (category eq phishing) or (category eq grayware)

Filter Builder

A weekly report to identify over the past seven days the following categories:

- Command-and-control
- Hacking
- Malware
- Phishing

Monitor > Management > Custom Reports > Host-visit malicious sites

Custom Report

Report Setting

Load Template → Run Now

Name	Hosts visit malicious sites	Available Columns	Selected Columns
Description		Action	Source Zone
Database	URL Log	App Category	Source User
	<input checked="" type="checkbox"/> Scheduled	App Container	Count
Time Frame	Last 7 Calendar Days	App Sub Category	
Sort By	Count	App Technology	
Group By	Source Address		
	Top 500		
	50 Groups		

Query Builder

(category eq command-and-control) or (category eq hacking) or (category eq malware) or (category eq phishing) or (category eq grayware)

Filter Builder

Same categories as previous report with fewer columns to simplify output

Monitor > Management > Custom Reports > Hosts visit questionable sites

Custom Report
?

Report Setting

Load Template
Run Now

Name	Hosts visit questionable sites		Available Columns	Selected Columns
Description			Action	Source Zone
Database	URL Log		App Category	Source User
	<input checked="" type="checkbox"/> Scheduled		App Container	Count
Time Frame	Last 7 Calendar Days		App Sub Category	
Sort By	Count	Top 500	App Technology	
Group By	Source Address	50 Groups	Top Up Down Bottom	

Query Builder

(category eq dynamic-dns) and (category eq parked) and (category eq questionable) and (category eq unknown)

Filter Builder

A weekly report to identify over the past seven days the following categories

- Dynamic-dns
- Parked
- Questionable
- Unknown

Monitor > Management > Custom Reports > Host-visit quest sites plus

Custom Report
?

Report Setting

Load Template → Run Now

Name: Host-visit quest sites plus Description: Detail of hosts visiting questionable URLs Database: URL Log <input checked="" type="checkbox"/> Scheduled Time Frame: Last 7 Calendar Days Sort By: Count Top 500 Group By: Source Address 50 Groups	Available Columns App Category App Container App Sub Category App Technology Application	Selected Columns Source Zone Source User Category Action Count
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------

Query Builder

(category eq dynamic-dns) and (category eq parked) and (category eq questionable) and (category eq unknown)

Filter Builder

Note: ‘questionable’ was concatenated to meet name length requirements

Same categories as previous report with more columns as an extended view

Monitor > Management > Custom Reports > Wildfire malicious verdicts

Custom Report
?

Report Setting

Load Template → Run Now

Name: Wildfire malicious verdicts Description: Files uploaded or downloaded that were later found to Database: WildFire Submissions <input checked="" type="checkbox"/> Scheduled Time Frame: Last 30 Calendar Days Sort By: Count Top 500 Group By: None 10 Groups	Available Columns App Category App Sub Category App Technology Client to Server Day	Selected Columns File Digest App Container Application Verdict File Type
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------

Query Builder

(app neq smtp) and (category neq benign)

Filter Builder

Report viewing all grayware and malicious verdicts

- Minus smtp (SMTP in separate report)
- Minus benign (only grayware and malicious)

Monitor > Management > Custom Reports > Wildfire verdicts SMTP

Custom Report

Report Setting

Load Template

Run Now

Name

Wildfire verdicts SMTP

Description

Links sent from emails found to be malicious.

Database

WildFire Submissions

☒ Scheduled

Time Frame

Last 30 Calendar Days

Sort By

Count

Top 500

Group By

None

10 Groups

Available Columns

App Category

App Sub Category

App Technology

Client to Server

Count

Selected Columns

File Digest

App Container

Application

Verdict

File Type

Top

Up

Down

Bottom

Query Builder

(app eq smtp) and (category neq benign)

Filter Builder

Report viewing all grayware and malicious verdicts

- Only SMTP traffic
- Minus benign (only grayware and malicious)

Monitor > Management > Custom Reports > Clients sinkholed

Custom Report

Report Setting

Load Template → Run Now

Name

Clients sinkholed

Description

Database

Traffic Log

☒ Scheduled

Time Frame

Last 30 Calendar Days

Sort By

Count

Top 500

Group By

Source Zone

50 Groups

Available Columns

Action

Action_source

App Category

App Container

App Sub Category

Selected Columns

Source Address

Source User

Count

Top

Up

Down

Bottom

Query Builder

(rule eq 'DNS Sinkhole Block')

Filter Builder

The importance here is we are viewing the verdict based on a rule. Reason being that if you go to threat log and say (action eq sinkhole) it will give you the DNS server and not the culprit. This rule allows for identification of the compromised client.

3.5.2 PDF Reports

See also

General configuration information in the Admin Guide: [Monitor - PDF Reports](#)

Report Groups

The set of recommended reports and grouped as 'Possible Compromise' for review and email distribution.

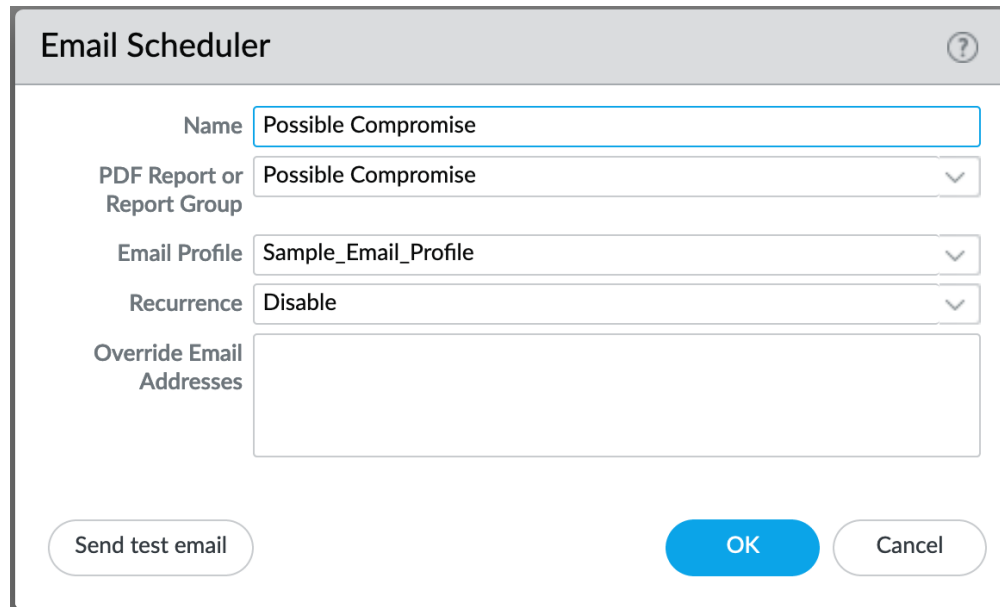
Monitor > PDF Reports > Report Groups

<input type="checkbox"/>	NAME	TITLE PAGE	TITLE	WIDGETS
<input type="checkbox"/>	Possible Compromise	<input checked="" type="checkbox"/>	Possible Compromise	<div>Clients sinkholed</div> <div>Wildfire malicious verdicts</div> <div>Wildfire verdicts SMTP</div> <div>Hosts visit malicious sites</div> <div>Host-visit malicious sites plus</div> <div>Hosts visit questionable sites</div> <div>Host-visit quest sites plus</div>

Email Scheduler

The report group 'Possible Compromise' is set up to be emailed using the referenced email profile as part of the device settings.

Monitor > PDF Reports > Email Scheduler



The 'Email Scheduler' dialog box is shown with the following configuration:

Field	Value
Name	Possible Compromise
PDF Report or Report Group	Possible Compromise
Email Profile	Sample_Email_Profile
Recurrence	Disable
Override Email Addresses	

Buttons at the bottom: Send test email, OK, Cancel.

It is up to the user to finalize configuration by setting the recurrence for how often the email should be generated and sent.

CONFIG VALIDATIONS: PAN-OS

Validation skillets allow for assessment of the config files or system state with pass/fail outputs based on validation skillet test rules. Each test result is mapped to its respective section in the Visual Guide for manual review and remediation.

The following validations are provided with IronSkillet

4.1 Full Configuration Assessment

View validation test file: | [9.0](#) | [9.1](#) | [10.0](#) |

Looks at a firewall xml configuration file to determine what elements recommended by IronSkillet are missing from the analyzed config file. Types of validation tests include the following based on IronSkillet recommendations with some elements version specific:

- dynamic updates configured
- use of snmpv3
- dns and ntp configured
- login banner configured
- timezone set to UTC
- auto acquire commit lock enabled
- X-Forward-For settings
- http range disabled
- inspection queue related settings
- max rows for CSV export
- API key lifetime
- admin attempts, timeout, and lockout
- Wildfire file size limits configured
- enable application block page
- disable log suppression
- prevent TCP evasions
- configure password complexity
- recommended zone protection profile

- inclusion of IronSkillet named profiles and groups
- logging configuration
- EDL block rules
- report and email scheduler related configuration

4.2 Upgrade to Newer Release Deltas [10.x]

View validation test file: | 10.0 |

Looks at a firewall xml configuration file to determine what elements recommended by IronSkillet are missing from a recently upgraded PAN-OS version to 10.x. Types of validation tests include the following based on IronSkillet recommendations:

- Wildfire dynamic updates set to realtime
- AV profile using ‘reset-both’ for Dynamic Classification and all file types enabled
- Anti-spyware profile DNS Security using ‘sinkhole’ action for malicious categories
- URL-Filtering profile using ‘block for Dynamic Classification, all engines
- Recommended decryption profile max version set to TLSv1.3

4.3 Upgrade to Newer Release Deltas [9.x]

View validation test file: | 9.0 | 9.1 |

Looks at a firewall xml configuration file to determine what elements recommended by IronSkillet are missing from a recently upgraded PAN-OS version to 9.x. Types of validation tests include the following based on IronSkillet recommendations:

- addition of panw-bulletproof-ip-list to the EDL block rules
- API key lifetime configured
- WF file size limits for script
- IPv4 sinkhole address object is using FQDN
- default-paloalto-cloud is used for the DNS security service setting in the anti-spyware profile
- new URL categories such as newly-registered-domain, grayware and cryptocurrency have been added

IRONSKILLET PLAYERS

IronSkillet configuration files can be rendered and loaded with various apps and tools.

5.1 SLI

The Skillet Line Interfacing tool is a CLI interface that can be used to load and work with skillets including IronSkillet. Please refer to the README document found within the following [SLI](#) repository. This will walk you through the installation and basic usage of SLI in the context of skillets.

5.2 panHandler

panHandler is a multi-skillet player easily installed as a Docker container. This recommended application supports configuration and validation skillets provided as part of IronSkillet.

Visit the Skillet District in the Live Community to [Install and Get Started with panHandler](#)

5.3 Expedition

Expedition (the Migration Tool) allows user not only migrate configurations from other vendors but also integrates best practice capabilities such as IronSkillet and the Best Practice Assessment.

Visit the [Expedition site](#) in Live for more information including the Installer.

5.4 Customer Support Portal

The Palo Alto Networks [Customer Support Portal](#) allows users to create a loadable XML Day One configuration. Users can generate the Day One configuration when registering a NGFW or Panorama. The IronSkillet configuration is also accessible using the portal Tools menu.

DEFAULT LOADABLE CONFIGURATIONS

The default loadable configurations have been created using the iron-skillet default and sample values. These configurations can be loaded into Panorama or a firewall for day one purposes.

Warning: Before committing the default configuration, be sure to edit the superuser name and password to avoid unauthorized access

Note: The values for syslog IP address, the email profile, and the config export IP address are sample information and should be updated specific to the user's environment.

Each directory corresponds to variations in the configuration specific to the Panorama and firewall management IP addresses:

- sample-cloud options: management interfaces for Panorama and PAN-OS use DHCP
- sample-mgmt-dhcp: PAN-OS default to DHCP while Panorama uses a static IP interface
- sample-mgmt-static: both PAN-OS and Panorama use static IP Interfaces for management

Included for each type are a set command .conf file and xml full configuration file. Both include the same configurations. Also in each directory is the config_variables.yaml file to see what values were used to create the full configuration.

Note: Panorama can be configured using shared elements and device-specific elements. The default loadable configuration are specific to the shared model only.

6.1 SET commands

This model uses traditional CLI 'copy-and-paste' to load in the configuration line by line. Users can elect to edit default values for their specific deployment as each line is added or load the configuration as-is and then edit using the instructions below for *GUI variable edits* or *CLI variable edits* to the default configuration.

Note: The set command conf file includes options for standard/static or dhcp management interfaces. Only load the commands specific to the interface type to be used.

Adding the configuration with set commands

- get the conf file specific to the deployment type

- log into the CLI and enter *configure* for configuration mode
- copy set commands from the *.conf* file and paste into the terminal

Note: It is recommended that the user only grab 30-40 set commands per paste to avoid any buffer issues resulting in errors.

6.2 XML configuration file

The full configuration file can be imported and loaded using the management GUI.

Instead of using scripting tools, the instructions below allow a user to `Import` and `Load` a candidate configuration that can be manually edited by *GUI variable edits* or *CLI variable edits*.

Warning: Loading a full configuration file will replace the existing candidate configuration. Save a copy of the existing configuration prior to loading the iron-skillet xml configuration file. Edit any local values before committing as a running configuration.

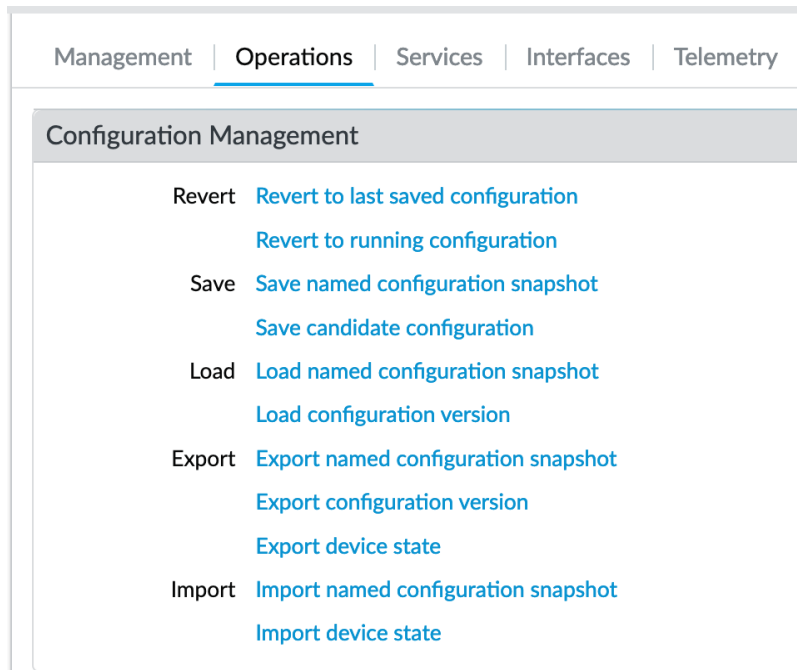
6.2.1 Import the configuration file using the GUI

1. Click on the `Device` tab
2. Select `Setup` in the left nav bar
3. Click on the `Operations` tab
4. Then `Import` named configuration snapshot choosing the day one config xml file

Note: You should perform a `Save` named configuration snapshot as backup prior to loading the new configuration

6.2.2 Load the configuration

1. Still under the `Operations` tab, use `Load` named configuration snapshot choosing the day one config xml file
2. Ensure no errors loading the configuration.



Note: If you see `{{ text }}` related import or load errors ensure you have the template file imported from the `loadable_configs` directory and not the `templates` directory.

6.3 GUI variable edits

After loading the configurations using `set` or `xml` commands, users can edit specific values instead of using the iron-skillet defaults.

The complete list of variables used by iron-skillet can be found at [Creating Loadable Configurations](#).

6.3.1 GUI variable edits: Firewall

The steps below are for a stand-alone NGFW platform without Panorama.

Device tab edits

The following edits are found under the `Device` tab




From here the following edits can be made:

Hostname


1. Go to Device → Setup → Management

2. Click the gear icon to edit the hostname

Management	Operations	Services	Interfaces	Telemetry	Content-ID
<div>General Settings </div> <div> <div>Hostname</div> <div>IronSkillet_fw</div> </div> <div> <div>Domain</div> <div></div> </div> <div> <div>Accept DHCP server provided Hostname</div> <div><input type="checkbox"/></div> </div>					

DNS and NTP servers

1. Go to Device → Setup → Services
2. Click the gear icon to edit the server values
3. Choose the Services (DNS) and NTP tabs accordingly

Services	
Update Server	updates.paloaltonetworks.com
Verify Update Server Identity	<input checked="" type="checkbox"/>
DNS Servers	
Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4
Minimum FQDN Refresh Time (sec)	30
FQDN Stale Entry Timeout (min)	1440
Proxy Server	
Primary NTP Server Address	0.pool.ntp.org
Primary NTP Server Authentication Type	None
Secondary NTP Server Address	1.pool.ntp.org
Secondary NTP Server Authentication Type	None

Static Management Interface

For a static management interface configuration, edit the IP address, subnet mask, default gateway.

1. Go to Device → Setup → Interfaces
2. Click on the Management link
3. Edit the management interface attributes

Management | Operations | Services | **Interfaces** |

INTERFACE NAME	ENABLED
Management	<input checked="" type="checkbox"/>

Superuser Administrator

The sample configuration uses the default admin/admin username and password setting. It is recommended to remove this user and add a new superuser or at a minimum change the admin user password.

1. Go to Device → Administrators
2. Select and delete the admin user account
3. Choose to Add a new user entering the username and password in the pop-up window

<input type="checkbox"/>	NAME	ROLE	
<input type="checkbox"/>	admin	Superuser	

Syslog IP Address

Syslog is used to send traffic, threat and other log updates to an external system.

1. Go to Device → Server Profiles → Syslog
2. Click on the Sample_Syslog_Profile link and edit the IP address

<input type="checkbox"/>	NAME	LOCATION	NAME	SYSLOG SERVER
<input type="checkbox"/>	Sample_Syslog_Profile		Sample_Syslog	192.0.2.2

Email Server Profile

The email profile is used to send key alerts to select recipients.

1. Go to Device → Server Profiles → Email
2. Click on the Sample_Email_Profile link and edit the from, to, and gateway values in the pop-up window.

<input type="checkbox"/>	NAME	LOCATION	Servers						
			NAME	EMAIL DISPLAY NAME	FROM	TO	ADDITION... RECIPIENT	EMAIL GATEWAY	PROTOCOL
<input type="checkbox"/>	Sample_E...		Sample_E...	Threat_Ale...	sentfrom@...	sendto@yo...		192.0.2.1	SMTP

Anti-Spyware Security Profiles

The templates define multiple named Anti-Spyware profiles all appended with `-AS`. Each of these profiles must be updated with new sinkhole address if non-default values are required.

These values should match the sinkhole IP addresses configured under `Addresses`.

1. Go to Objects \rightarrow Security Profiles \rightarrow Anti-Spyware

<input type="checkbox"/>	NAME	LOCATION	COUNT	POLICY NAME	THREAT NAME	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	default	Predefined	Policies: 4	simple-critical	any	critical	default	disable
				simple-high	any	high	default	disable
				simple-medium	any	medium	default	disable
				simple-low	any	low	default	disable
<input type="checkbox"/>	strict	Predefined	Policies: 5	simple-critical	any	critical	reset-both	disable
				simple-high	any	high	reset-both	disable
				simple-medium	any	medium	reset-both	disable
				simple-informational	any	informational	default	disable
				simple-low	any	low	default	disable
<input type="checkbox"/>	Outbound-AS		Policies: 2	Block-Critical-High-Medium	any	critical,high,medi...	reset-both	single-packet
				Default-Low-Info	any	low,informational	default	disable
<input type="checkbox"/>	Inbound-AS		Policies: 2	Block-Critical-High-Medium	any	critical,high,medi...	reset-both	single-packet
				Default-Low-Info	any	low,informational	default	disable
<input type="checkbox"/>	Internal-AS		Policies: 2	Block-Critical-High-Medium	any	critical,high,medi...	reset-both	single-packet
				Default-Low-Info	any	low,informational	default	disable
<input type="checkbox"/>	Alert-Only-AS		Policies: 1	Alert-All	any	any	alert	disable
<input type="checkbox"/>	Exception-AS							

2. Click on one of the template specific profiles ending in `-AS`
3. Click on the DNS Signatures tab and update the IPv4 and IPv6 sinkhole addresses

Anti-Spyware Profile

Name

Outbound-AS

Description

Signature Policies

Signature Exceptions

DNS Policies

DNS Exceptions

DNS Policies

Q

6 items

\rightarrow

\times

<input type="checkbox"/>	SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
	\vee : Palo Alto Networks Content			
<input type="checkbox"/>	default-paloalto-dns		sinkhole	disable
	\vee : DNS Security			
<input type="checkbox"/>	Benign Domains	default (none)	default (allow)	disable

DNS Sinkhole Settings

Sinkhole IPv4

sinkhole.paloaltonetworks.com

Sinkhole IPv6

2600:5200::1

6.3.2 GUI variable edits: Panorama

The steps below are for edits to the Panorama configuration. Variable edits in the GUI will include both the Panorama system edits and managed firewall device-group and template configurations.

The are four areas to be edited:

- Panorama platform settings
- iron-skillet template for shared device and network items
- sample template stack for device-specific items
- Shared device-group for shared objects and policies

Panorama tab edits

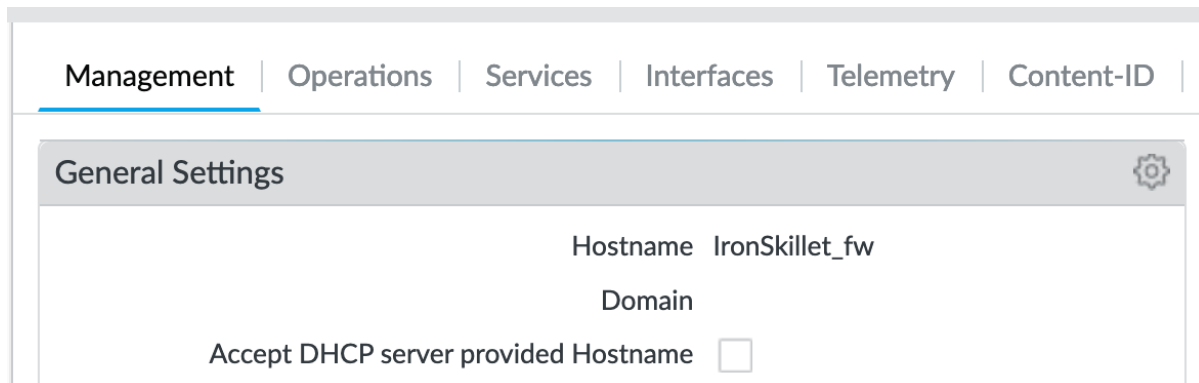
The following edits are found under the Panorama tab



From here the following edits can be made:


Panorama > Hostname

1. Go to Panorama → Setup → Management
2. Click the gear icon to edit the Panorama hostname



Panorama > DNS and NTP servers

1. Go to Panorama → Setup → Services
2. Click the gear icon to edit the server values
3. Choose the Services (DNS) and NTP tabs accordingly

Services 

Update Server updates.paloaltonetworks.com
Verify Update Server Identity ☒
DNS Servers
Primary DNS Server 8.8.8.8
Secondary DNS Server 8.8.4.4
Minimum FQDN Refresh Time (sec) 30
FQDN Stale Entry Timeout (min) 1440
Proxy Server
Primary NTP Server Address 0.pool.ntp.org
Primary NTP Server Authentication Type None
Secondary NTP Server Address 1.pool.ntp.org
Secondary NTP Server Authentication Type None

Panorama > Management Interface

This configuration is specific to the Panorama management interface when statically defined.

1. Go to Panorama → Setup → Interfaces
2. Click on the Management link
3. Edit the management interface attributes

Management	Operations	Services	Interfaces	Telemetry	WildFire	HSM
INTERFACE NAME	ENABLED	SPEED	PUBLIC IP ADDRESS	IP ADDRESS	SERVICES ENABLED	
Management	<input checked="" type="checkbox"/>	auto-negotiate		192.168.55.110	Ping	
					SSH	
					Device Management and Device Log Collection	
					Collector Group Communication	
					Syslog Forwarding	
					Device Deployment	

Panorama > Superuser Administrator

The sample configuration uses the default admin/admin username and password setting. It is recommended to remove this user and add a new superuser or at a minimum change the admin user password.

1. Go to Panorama → Administrators
2. Select and delete the admin user account
3. Choose to Add a new user entering the username and password in the pop-up window

<input type="checkbox"/>	NAME	ROLE	A F
<input type="checkbox"/>	admin	Superuser	

Panorama > Syslog IP Address

Syslog is used to send traffic, threat and other log updates to an external system.

1. Go to Panorama → Server Profiles → Syslog
2. Click on the Sample_Syslog_Profile link and edit the IP address

<input type="checkbox"/>	NAME	LOCATION	NAME	SYSLOG SERVER
<input type="checkbox"/>	Sample_Syslog_Profile		Sample_Syslog	192.0.2.2

Panorama > Email Server Profile

The email profile is used to send key alerts to select recipients.

1. Go to Panorama → Server Profiles → Email
2. Click on the Sample_Email_Profile link and edit the from, to, and gateway values in the pop-up window.

<input type="checkbox"/>	NAME	LOCATION	Servers						
			NAME	EMAIL DISPLAY NAME	FROM	TO	ADDITION... RECIPIENT	EMAIL GATEWAY	PROTOCOL
<input type="checkbox"/>	Sample_E...		Sample_E...	Threat_Ale...	sentfrom@...	sendto@yo...		192.0.2.1	SMTP

Panorama > Config Bundle Export Server

1. Go to Panorama → Scheduled Config Export
2. Click on the Recommended_Config_Export link
3. In the pop-up window, edit the Hostname value

Scheduled Config Export ?

Name

Description

☒ Enable

Scheduled Export Start Time (Daily) 00:00 - 23:59

Protocol ☒ SCP ☐ FTP

Hostname

Port

Path

Username

Password

Confirm Password

Panorama > Template Stack

1. Go to Panorama -> Template
2. Click on the `sample_stack` link and edit the name

Template Stack ?

Name

Default VSYS The default virtual system template configuration is pushed to firewalls with a single virtual system.

Description

TEMPLATES
<input type="checkbox"/> iron-skillet

The Template at the top of the Stack has the highest priority in the presence of overlapping config

Devices **FILTERS**

<input type="checkbox"/> Platforms <input type="checkbox"/> Device Groups <input type="checkbox"/> Tags <input type="checkbox"/> HA Status	<input type="text" value=""/> 0 items <input type="button" value="↔"/> <input type="button" value="✕"/>
-----------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------

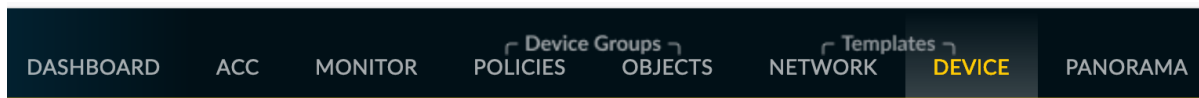
Select All Deselect All ☐ Group HA Peers ☐ Filter Selected (0)

Panorama > Device-Group

1. Go to Panorama → Device-Groups
2. Click on the `sample_devicegroup` link and edit the name

Templates > Device tab edits

The following edits are found under the *Device* tab



Note: The edits are grouped by the *iron-skillet* template edits and *sample_stack* template stack edits

**** iron-skillet template edits****

Note: Make sure the template selected in the GUI is *iron-skillet* before completing the steps below

DNS and NTP servers

1. Go to Device → Setup → Services
2. Click the gear icon to edit the server values

3. Choose the Services (DNS) and NTP tabs accordingly

Services ⚙️

Update Server

updates.paloaltonetworks.com

Verify Update Server Identity

☒

DNS Servers

Primary DNS Server

8.8.8.8

Secondary DNS Server

8.8.4.4

Minimum FQDN Refresh Time (sec)

30

FQDN Stale Entry Timeout (min)

1440

Proxy Server

Primary NTP Server Address

0.pool.ntp.org

Primary NTP Server Authentication Type

None

Secondary NTP Server Address

1.pool.ntp.org

Secondary NTP Server Authentication Type

None

Superuser Administrator

The sample configuration uses the default admin/admin username and password setting. It is recommended to remove this user and add a new superuser or at a minimum change the admin user password.

1. Go to Device → Administrators
2. Select and delete the `admin` user account
3. Choose to Add a new user entering the username and password in the pop-up window

<input type="checkbox"/>	NAME	ROLE	A F
<input type="checkbox"/>	admin	Superuser	

Syslog IP Address

Syslog is used to send traffic, threat and other log updates to an external system.

1. Go to Device → Server Profiles → Syslog
2. Click on the Sample_Syslog_Profile link and edit the IP address

<input type="checkbox"/>	NAME	LOCATION	NAME	SYSLOG SERVER
<input type="checkbox"/>	Sample_Syslog_Profile		Sample_Syslog	192.0.2.2

Email Server Profile

The email profile is used to send key alerts to select recipients.

1. Go to Device -> Server Profiles -> Email
2. Click on the Sample_Email_Profile link and edit the from, to, and gateway values in the pop-up window.

<input type="checkbox"/>	NAME	LOCATION	Servers						
			NAME	EMAIL DISPLAY NAME	FROM	TO	ADDITION... RECIPIENT	EMAIL GATEWAY	PROTOCOL
<input type="checkbox"/>	Sample_E...		Sample_E...	Threat_Ale...	sentfrom@...	sendto@yo...		192.0.2.1	SMTP


** iron-skillet template edits**

Note: Make sure the template selected in the GUI is *sample_stack* (or the updated name) before completing the steps below

Hostname

1. Go to Device -> Setup -> Management
2. Click the gear icon to edit the hostname

Management | Operations | Services | Interfaces | Telemetry | Content-ID |

General Settings 

Hostname IronSkillet_fw

Domain

Accept DHCP server provided Hostname ☐

Static Management Interface

For a static management interface configuration, edit the IP address, subnet mask, default gateway.

1. Go to Device -> Setup -> Interfaces
2. Click on the Management link
3. Edit the management interface attributes

Management | Operations | Services | Interfaces |

INTERFACE NAME	ENABLED
Management	<input checked="" type="checkbox"/>

** Shared device-group edits**

Note: Make sure the device-group selected in the GUI is *Shared* before completing the steps below

Anti-Spyware Security Profiles

The templates define multiple named Anti-Spyware profiles all appended with `-AS`. Each of these profiles must be updated with new sinkhole address if non-default values are required.

These values should match the sinkhole IP addresses configured under *Addresses*.

1. Go to Objects → Security Profiles → Anti-Spyware

<input type="checkbox"/>	NAME	LOCATION	COUNT	POLICY NAME	THREAT NAME	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	default	Predefined	Policies: 4	simple-critical	any	critical	default	disable
				simple-high	any	high	default	disable
				simple-medium	any	medium	default	disable
				simple-low	any	low	default	disable
<input type="checkbox"/>	strict	Predefined	Policies: 5	simple-critical	any	critical	reset-both	disable
				simple-high	any	high	reset-both	disable
				simple-medium	any	medium	reset-both	disable
				simple-informational	any	informational	default	disable
				simple-low	any	low	default	disable
<input type="checkbox"/>	Outbound-AS		Policies: 2	Block-Critical-High-Medium	any	critical,high,medi...	reset-both	single-packet
				Default-Low-Info	any	low,informational	default	disable
<input type="checkbox"/>	Inbound-AS		Policies: 2	Block-Critical-High-Medium	any	critical,high,medi...	reset-both	single-packet
				Default-Low-Info	any	low,informational	default	disable
<input type="checkbox"/>	Internal-AS		Policies: 2	Block-Critical-High-Medium	any	critical,high,medi...	reset-both	single-packet
				Default-Low-Info	any	low,informational	default	disable
<input type="checkbox"/>	Alert-Only-AS		Policies: 1	Alert-All	any	any	alert	disable
<input type="checkbox"/>	Exception-AS							

2. Click on one of the template specific profiles ending in `-AS`
3. Click on the DNS Signatures tab and update the IPv4 and IPv6 sinkhole addresses

Anti-Spyware Profile

Name

Outbound-AS

Description

Signature Policies

Signature Exceptions

DNS Policies

DNS Exceptions

DNS Policies

6 items

→

×

<input type="checkbox"/>	SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
▼	: Palo Alto Networks Content			
<input type="checkbox"/>	default-paloalto-dns		sinkhole	disable
▼	: DNS Security			
<input type="checkbox"/>	Benign Domains	default (none)	default (allow)	disable

DNS Sinkhole Settings

Sinkhole IPv4

sinkhole.paloaltonetworks.com

▼

Sinkhole IPv6

2600:5200::1

▼

6.4 CLI variable edits

After loading the configurations using `set` or `xml` commands, users can edit specific values instead of using the iron-skillet defaults.

The complete list of variables used by iron-skillet can be found at [Creating Loadable Configurations](#).

6.4.1 CLI variable edits: Firewall

This section is specific to a non-Panorama managed NGFW.

Instead of using the GUI to make template edits for each variable value, below are steps using `SET` commands to make the same candidate configuration changes.

The `{{ text }}` values denotes where a variable is used in the template.

Hostname

```
set deviceconfig system hostname {{ hostname }}
```

DNS and NTP Servers

```
set deviceconfig system dns-setting servers primary {{ DNS 1 }} secondary {{ DNS 2 }}
set deviceconfig system ntp-servers primary-ntp-server ntp-server-address {{ NTP 1 }}
set deviceconfig system ntp-servers secondary-ntp-server ntp-server-address {{ NTP 2 }}
↪ }
```

Static management interface

```
set deviceconfig system ip-address {{ ip address }} netmask {{ mask }} default-
↪ gateway {{ gateway }}
```

Superuser admin account

```
set mgt-config users {{ username }} permissions role-based superuser yes
set mgt-config users {{ username }} password
```

When the password command is entered, the user will be prompted for a password.

Syslog and Email Server Profiles

```
set shared log-settings syslog Sample_Syslog_Profile server Sample_Syslog server {{
  ↳ip address }}
set shared log-settings email Sample_Email_Profile server Sample_Email_Profile from {
  ↳{ from }}
set shared log-settings email Sample_Email_Profile server Sample_Email_Profile to {{
  ↳to }}
set shared log-settings email Sample_Email_Profile server Sample_Email_Profile_
  ↳gateway {{ address }}
```

Address Objects

```
set address Sinkhole-IPv4 ip-netmask {{ IPv4 address }}
set address Sinkhole-IPv6 ip-netmask {{ IPv6 address }}
```

Anti-Spyware Security Profiles

The same commands are used across all of the template security profiles ending in -AS.

```
set profiles spyware {{ profile name }} botnet-domains sinkhole ipv4-address {{ IPv4
  ↳address }}
set profiles spyware {{ profile name }} botnet-domains sinkhole ipv6-address {{ IPv6
  ↳address }}
```

6.4.2 CLI variable edits: Panorama

This section is specific to configuration of a Panorama management system.

Instead of using the GUI to make template edits for each variable value, below are steps using SET commands to make the same candidate configuration changes.

The {{ text }} values denotes where a variable is used in the template.

Note: The initial configurations are specific to the Panorama platform itself. The managed firewall configurations are added under the template and device-group configurations.

Panorama > Hostname

```
set deviceconfig system hostname {{ hostname }}
```

Panorama > DNS and NTP Servers

```
set deviceconfig system dns-setting servers primary {{ DNS 1 }} secondary {{ DNS 2 }}
set deviceconfig system ntp-servers primary-ntp-server ntp-server-address {{ NTP 1 }}
set deviceconfig system ntp-servers secondary-ntp-server ntp-server-address {{ NTP 2 }}
  ↳}
```


Panorama > Static management interface

```
set deviceconfig system ip-address {{ ip address }} netmask {{ mask }} default-
↪gateway {{ gateway }}
```

Panorama > Superuser admin account

```
set mgt-config users {{ username }} permissions role-based superuser yes
set mgt-config users {{ username }} password
```

When the password command is entered, the user will be prompted for a password.

Panorama > Syslog and Email Server Profiles

```
set panorama log-settings syslog Sample_Syslog_Profile server Sample_Syslog server {{
↪ip address }}
set panorama log-settings email Sample_Email_Profile server Sample_Email_Profile from
↪{{ from }}
set panorama log-settings email Sample_Email_Profile server Sample_Email_Profile to {
↪{ to }}
set panorama log-settings email Sample_Email_Profile server Sample_Email_Profile
↪gateway {{ address }}
```

Panorama > Config Bundle Export Schedule

```
set deviceconfig system config-bundle-export-schedule Recommended_Config_Export
↪protocol scp hostname {{ ip address }}
```

Note: The configuration for Panorama has some element in the iron-skilllet shared template and others specific to the device captured as a template-stack called `sample_stack`. The same is true for device-group items that are either shared or contained in a device-specific group, namely reports.

Template > Hostname

```
set template-stack sample_stack config deviceconfig system hostname {{ hostname }}
```

Template > DNS and NTP Servers

```
set template iron-skilllet config deviceconfig system dns-setting servers primary {{
↪DNS 1 }} secondary {{ DNS 2 }}
set template iron-skilllet config deviceconfig system ntp-servers primary-ntp-server
↪ntp-server-address {{ NTP 1 }}
set template iron-skilllet config deviceconfig system ntp-servers secondary-ntp-server
↪ntp-server-address {{ NTP 2 }}
```

Template > Static management interface

This is to be configured for a firewall with a static management interface.

```
set template-stack sample_stack config deviceconfig system ip-address {{ ip address }}
set template-stack sample_stack config deviceconfig system netmask {{ mask }}
set template-stack sample_stack config deviceconfig system default-gateway {{ gateway
↪ }}
```

Template > Superuser admin account

```
set template iron-skillet config mgt-config users {{ username }} permissions role-  
↳based superuser yes  
set template iron-skillet config mgt-config users {{ username }} password
```

When the password command is entered, the user will be prompted for a password.

Template > Syslog and Email Server Profiles

```
set template iron-skillet config shared log-settings syslog Sample_Syslog_Profile_␣  
↳server Sample_Syslog server {{ ip address }}  
set template iron-skillet config shared log-settings email Sample_Email_Profile_␣  
↳server Sample_Email_Profile from {{ from }}  
set template iron-skillet config shared log-settings email Sample_Email_Profile_␣  
↳server Sample_Email_Profile to {{ to }}  
set template iron-skillet config shared log-settings email Sample_Email_Profile_␣  
↳server Sample_Email_Profile gateway {{ address }}
```

Device-Group > Address Objects

```
set shared address Sinkhole-IPv4 ip-netmask {{ IPv4 address }}  
set shared address Sinkhole-IPv6 ip-netmask {{ IPv6 address }}
```

Device-Group Anti-Spyware Security Profiles

The same commands are used across all of the templated security profiles ending in -AS.

```
set shared profiles spyware {{ profile name }} botnet-domains sinkhole ipv4-address {  
↳{ IPv4 address }}  
set shared sample profiles spyware {{ profile name }} botnet-domains sinkhole ipv6-  
↳address {{ IPv6 address }}
```

PAN-OS XML SNIPPETS

The configuration snippet descriptions and the associated GitHub repository link for each xml snippet.

Note: The template version is found in the template xml file as a tag attribute

Note: The set commands utilize the same configuration settings

7.1 Playlist Includes Model

Starting with IronSkillet 10.1, the xml snippets are included in sub-skillets in the [ironskillet-components](#) submodule. These sub-skillets are referenced in playlists through skillet includes, and allows for easy re-use of individual snippets. It also allows for subsets of the configuration to be run, as reflected in the new playlist options for panos and panorama configuration. An overview of the IronSkillet playlists available can be found in the playlist folder in the IronSkillet repo.

See the [Playlist Includes tutorial](#) in the SkilletBuilder documentation for more information on how this works.

7.2 General Device Configuration

This section provides templated configurations for general device settings.

7.2.1 Management Users

View xml snippet: | [9.0](#) | [9.1](#) | [10.0](#) | [10.1](#) |

Management configuration superuser access

- Administrative user name
- Password hash stored in the configuration file

7.2.2 Password Complexity

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

Administrative user password complexity profile

- Attributes including minimum length, characters, and history

7.2.3 Security-related Device Settings

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

General device settings that effect security posture. Found in Device > Setup in the GUI.

- Wildfire: set optimal file size limits for Wildfire uploads and show verdict responses for grayware, malware and phishing
- Session rematch: the firewall will go through all the existing sessions and apply the new security policy to any matching traffic
- Notify User: user should be notified when web-application is blocked; enables the application response page
- Log Suppression: disabled to ensure unique log entries even if similar session types
- Prevent TCP and UDP buffer overflow and multi-part HTTP download evasions
 - Disable ‘tcp-bypass-exceed-queue’
 - Disable ‘udp-bypass-exceed-queue’
- Enable high DP load logging
- Prevent App-ID buffer overflow evasion
 - set bypass-exceed-queue to ‘no’
- Prevent TCP and MPTCP evasions
 - set urgent data to ‘clear’
 - set drop zero flag to ‘yes’
 - set bypass-exceed-oo-queue to ‘no’
 - set check-timestamp-option to ‘yes’
 - set strip-mptcp-option to yes
- Set an API key lifetime instead of a permanent/static value
 - default set to 525,600 minutes (1 year)
- set export of csv log file to maximum of 1,048,576

7.2.4 System Configuration

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

View dns xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

View mgmt IP config xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

System configuration settings for dynamic updates and network services (eg. DNS, NTP).

- Update schedule settings
 - Check every 30 minutes for new threat signatures
 - Hourly checks for new AV signatures
 - Check realtime for new Wildfire signatures
 - Recommended time delays and thresholds for checks and installs
- Use SNMPv3
- Set default DNS and NTP values
- Set timezone to UTC
- Provide a standard login banner warning for unauthorized users

Note: The management config types include static or dhcp-client. This is specific to each deployment and can be selected as part of the tools to build `loadable_configs`. Since management interface is in the template config, this option must be included for deployment.

7.3 Logging

Logging best practice configurations for logging output and forwarding profiles.

Warning: Configure logging profiles before security rules The template creates a log forwarding profile call default. This profile is referenced in the template security rules and should be configured before the security rules.

Note: Logging can be deployment dependent The destination in the logging profile is templated to an unroutable syslog server address. This can vary based on actual deployment scenarios.

7.3.1 Log forwarding profile

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

View email xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

Log forward profile referenced in security rules to determine where to forward log related events.

- Forward all log activity to syslog (see the reference syslog configuration in shared_log_settings.xml)
- Email malicious and phishing Wildfire verdicts to the address in the email profile (see shared_log_settings.xml)

7.3.2 Device log settings

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

View email profile xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

View email system critical xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

Device event logging including sample profiles for email and syslog forwarding.

- Reference syslog profile that can be edited for a specific IP address and UDP/TCP port
- Reference email profile that can be edited for specific email domain and user information
- System, configuration, user, HIP, and correlation log forwarding to syslog
- Email critical system events to the email profile

Note: When to use email alerts The purpose of select email alert forwarding is ensure not to under alert or over alert yet provide critical messages for key events. Under alerting reduces visibility to key events while over alerting creates too much noise in the system. The templates are set with a median view to capture key events without too much ‘log fatigue’ noise

7.4 Referenced Objects

Address, External Dynamic List (EDL), and tag objects that are referenced in security rules by name.

7.4.1 Tags

View xml snippet: | 9.0 | 9.0 | 10.0 | 10.1 |

Tags used in security rules and related objects.

- Inbound - inbound (untrust to trust) elements
- Outbound - outbound (trust to untrust) elements
- Internal - internal (trust) segmentation elements

Tag showing IronSkillet loaded and the associated template version.

7.5 Security Profiles and Groups

The key elements for security posture are security profiles and the security rules. The templates ensure best practice profiles and profile groups are available and can be referenced in any security rules. The template security rules focus on 'top of the list' block rules to reduce the attack surface.

Warning: Profiles and subscriptions All of the template security profiles other than file blocking require Threat Prevention, URL Filtering, and Wildfire subscriptions. Ensure that the device is properly licensed before applying these configurations.

7.5.1 Custom URL Category

View xml snippet: | [9.0](#) | [9.1](#) | [10.0](#) | [10.1](#) |

Placeholder for custom url categories used in security rules and url profiles. Using these categories prevents the need to modify the default template.

- Block: placeholder to be used in block rules and objects to override default template behavior
- Allow: placeholder to be used in permit rules and objects to override default template behavior
- Custom-No-Decrypt: to be used in the decryption no-decrypt rule to specify URLs that should not be decrypted

7.5.2 File Blocking

View xml snippet: | [9.0](#) | [9.1](#) | [10.0](#) | [10.1](#) |

Security profile for actions specific to file blocking (FB).

Note: File blocking and file types The Block file type recommendation is based on common malicious file types with minimal impact in a Day 1 deployment. Although PE is considered the highest risk file type it is also used for legitimate purposes so blocking PE files will be deployment specific and not included in the template.

- Day 1 Block file types: 7z, bat, chm, class, cpl, dll, hlp, hta, jar, ocx, pif, scr, torrent, vbe, wsf
- The profiles will alert on all other file types for logging purposes

Profiles:

- Outbound-FB: For outbound (trust to untrust) security rules
- Inbound-FB: For inbound (untrust to trust) security rules
- Internal-FB: For internal network segmentation rules
- Alert-Only-FB: No file blocking, only alerts for logging purposes
- Exception-FB: For exception requirements in security rules to avoid modifying the default template profiles

7.5.3 Anti-Spyware

View xml snippet: | [9.0](#) | [9.1](#) | [10.0](#) | [10.1](#) |

Security profile for actions specific to anti-spyware (AS).

Note: Sinkhole addresses The profiles use IPv4 and IPv6 addresses for DNS sinkholes. IPv4 is currently provided by Palo Alto Networks. IPv6 is a bogon address. In 9.0 the IPv4 address is replaced by an FQDN

[9.x] Support for DNS Cloud subscription service

- In addition to the current malicious domain push to the device, also include domain lookups using the cloud service

[10.x] Support for DNS Cloud subscription domain categories and actions

- set malicious categories to sinkhole

Profiles:

- Outbound-AS : For outbound (trust to untrust) security rules
 - Block severity = Critical, High, Medium
 - Default severity = Low, Informational
 - DNS Sinkhole for IPv4 and IPv6
 - Single packet capture for Critical, High, Medium severity
- Inbound-AS : For inbound (untrust to trust) security rules
 - Block severity = Critical, High, Medium
 - Default severity = Low, Informational
 - DNS Sinkhole for IPv4 and IPv6
 - Single packet capture for Critical, High, Medium severity
- Internal-AS : For internal network segmentation rules
 - Block severity = Critical, High
 - Default severity = Medium, Low, Informational
 - DNS Sinkhole for IPv4 and IPv6
 - Single packet capture for Critical, High, Medium severity
- Alert-Only-AS : No blocking, only alerts for logging purposes
 - Alert all severities and malicious domain events
 - No packet capture
- Exception-AS : For exception requirements in security rules to avoid modifying the default template profiles

7.5.4 URL Filtering

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

Security profile for actions specific to URL filtering (URL).

Note: Only BLOCK categories will be listed for each profile below. All other URL categories will be set to ALERT in the templates for logging purposes. The complete list of categories can be found in the url filtering template.

[10.x] Support for local machine learning based on web content

- block malicious content using dynamic classification

Profiles:

- Outbound-URL : For outbound (trust to untrust) security rules
 - URL Categories
 - Site Access: Block command-and-control, malware, phishing, Black List (custom URL category)
 - User Credential Submission: Block all categories
 - Alert category = includes White List (custom URL category)
 - URL Filtering Settings: HTTP Header Logging (user agent, referer, X -Forwarded-For)
 - dynamic classification to block malicious web content
- Alert-Only-URL : No blocking, only alerts for logging purposes
 - Alert all categories including custom categories Black List and White List
- Exception-URL : For exception requirements in security rules to avoid modifying the default template profiles
 - URL Categories
 - Site Access: Block command-and-control, malware, phishing, Black List (custom URL category)
 - User Credential Submission: Block all categories
 - Alert category = includes White List (custom URL category)
 - URL Filtering Settings: HTTP Header Logging (user agent, referer, X -Forwarded-For)
 - dynamic classification to block malicious web content

Note: 9.0 includes new URL categories for risk and newly created domains. In future best practices, these categories may be used to provide additional security protections when combined with existing URL categories. For now, these categories are only set to *alert*.

7.5.5 Anti-Virus

View xml snippet: | [9.0](#) | [9.1](#) | [10.0](#) | [10.1](#) |

Security profile for actions specific to AntiVirus (AV) and Wildfire signatures. All decoders using 'reset-both' as actions except for the Alert-Only profile.

[10.x] Support for WF-based local machine learning to block malicious content for exe and powershell files.

Profiles:

- Outbound-AV: For outbound (trust to untrust) security rules
- Inbound-AV: For inbound (untrust to trust) security rules
- Internal-AV: For internal network segmentation rules
- Alert-Only-AV: No blocking, only alerts for logging purposes
- Exception-AV: For exception requirements in security rules to avoid modifying the default template profiles

Note: Email response codes with SMTP not IMAP or POP3 Reset-both is used for SMTP, IMAP, and POP3. SMTP '541' response messages are returned to notify that the session was blocked. IMAP and POP3 do not have the same response model. In live deployments, instead of DoS concerns with retries, the endpoints typically stop resending after a small number of sends with timeouts.

Note: 9.0 includes support for http/2. If you are upgrading from a previous version ensure that this decoder matches the actions for standard http.

7.5.6 Vulnerability Protection

View xml snippet: | [9.0](#) | [9.1](#) | [10.0](#) | [10.1](#) |

Profiles:

- Outbound-VP : For outbound (trust to untrust) security rules
 - Block severity = Critical, High, Medium
 - Alert severity = Low, Informational
 - Single packet capture for Critical, High, Medium severity
- Inbound-VP : For inbound (untrust to trust) security rules
 - Block severity = Critical, High, Medium
 - Alert severity = Low, Informational
 - Single packet capture for Critical, High, Medium severity
- Internal-VP : For internal network segmentation rules
 - Block severity = Critical, High
 - Alert severity = Medium, Low, Informational
 - Single packet capture for Critical, High, Medium severity
- Alert-Only-VP : No blocking, only alerts for logging purposes

- Alert all severities
- No packet capture
- Exception-VP: For exception requirements in security rules to avoid modifying the default template profiles

Note: A separate branch is being used as a placeholder for [Brute-Force-Exceptions](#). This provides a way to include Support recommended exceptions by ThreatID value. These can be loaded using console SET commands or using API-based tools

7.5.7 Wildfire Analysis

View xml snippet: | [9.0](#) | [9.1](#) | [10.0](#) | [10.1](#) |

Security profile for actions specific to Wildfire upload and analysis (WF).

Note: `Public Cloud` is the default All template profiles are configured to upload all file types in any direction to the public cloud for analysis.

Profiles:

- Outbound-WF: For outbound (trust to untrust) security rules
- Inbound-WF: For inbound (untrust to trust) security rules
- Internal-WF: For internal network segmentation rules
- Alert-Only-WF: No blocking, only alerts for logging purposes
- Exception-WF: For exception requirements in security rules to avoid modifying the default template profiles

7.5.8 Security Profile Groups

View xml snippet: | [9.0](#) | [9.1](#) | [10.0](#) | [10.1](#) |

Security profile groups based on use case

- Inbound: For rules associated to inbound (untrust to trust) sessions
- Outbound: For rules associated to outbound (trust to untrust) sessions
- Internal: For rules associated to trust-domain network segmentation
- Alert Only: Provides visibility and logging without a blocking posture

7.6 Security Rules

7.6.1 Recommended Block Rules

View xml snippet: | [9.0](#) | [9.1](#) | [10.0](#) | [10.1](#) |

Recommended block rules for optimal security posture with associated default log-forwarding profile

- Outbound Block Rule: Block destination IP address match based on the Palo Alto Networks predefined externals dynamic lists
- Inbound Block Rule: Block source IP address match based on the Palo Alto Networks predefined externals dynamic lists

Note: Security rules in the template are block only The template only uses block rules. Allow rules are zone, direction and use case dependent. Additional templating work will provide recommended use case security rules.

7.6.2 Default Security Rules

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

Configuration for the default interzone and intrazone default rules

- Intrazone
 - Enable logging at session-end using the default logging profile
 - Use the Internal security profile-group
- Interzone
 - Explicit drop of traffic between zones
 - Enable logging at session-end using the default logging profile

7.7 Decryption

7.7.1 Profiles

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

Recommended_Decryption_Profile. Referenced by the default decryption rule.

- SSL Forward Proxy
 - Server Cert Verification : Block sessions with expired certs, Block sessions with untrusted issuers, Block sessions with unknown cert status
 - Unsupported Mode Checks : Block sessions with unsupported versions, Blocks sessions with unsupported cipher suites
- SSL No Proxy
 - Server Cert Verification : Block sessions with expired certs, Block sessions with untrusted issuers
- SSH Proxy
 - Unsupported Mode Checks : Block sessions with unsupported versions, Block sessions with unsupported algorithms
- SSL Protocol Settings:
 - Minimum Version: TLSv1.2; Max version TLSv1.3; Any TLSv1.1 errors can help find outdated TLS endpoints

- Key Exchange Algorithms: RSA not recommended and unchecked
- Encryption Algorithms: 3DES and RC4 not recommended and unavailable when TLSv1.2 is the min version
- Authentication Algorithms: MD5 not recommended and unavailable when TLSv1.2 is the min version

7.7.2 Decryption Rules

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

Recommended SSL decryption pre-rules for no-decryption.

- NO decrypt rule for select URL categories; Initially disabled in the Day 1 template until SSL decryption to be enabled

7.8 Zone Protection

7.8.1 Profile

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

Recommended_Zone_Protection profile for standard, non-volumetric best practices. This profile should be attached to all interfaces within the network.

Note: Recon Protection Default values enabled in alert-only mode; active blocking posture requires network tuning

Packet Based Attack Protection

- IP Drop: Spoofed IP Address, Malformed
- TCP Drop: Remove TCP timestamp, No TCP Fast Open, Multipath TCP (MPTCP) Options = Global

7.9 Reports

7.9.1 Reports

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

Series of reports to look for traffic anomalies, where to apply or remove rules, etc. Reports are grouped by topic per the report group section below.

Note: Zones and Subnets in report queries The repo contains a separate folder for custom reports that use a placeholder zone called 'internet' for match conditions in reports. This value **MUST** be changed to match the actual public zone used in a live network. Additional zones and/or subnets to be used or excluded in the reports would be added in the query values.

7.9.2 Report Groups

View xml snippet: | [9.0](#) | [9.1](#) | [10.0](#) | [10.1](#) |

Report groups allow you to create sets of reports that the system can compile and send as a single aggregate PDF report with an optional title page and all the constituent reports included.

Template report groups include:

Simple (included in Day One template)

- Possible Compromise: malicious sites and verdicts, sinkhole sessions

Custom

- User Group Activity (eg. Employee, Student, Teacher): user-id centric reports grouped by user type
- Inbound/Outbound/Internal Rule Tuning: Used rules, app ports, unknown apps, geo information
- Inbound/Outbound/Internal Threat Tuning: Allowed threats traversing the device
- File Blocking Tuning: View of upload/download files and types with associated rule
- URL Tuning: Views by categories, especially questionable and unknown categories
- Inbound/Outbound/Internal Threats Blocked: Threat reports specific to blocking posture; complement to threat tuning
- Non-Working Traffic: View of dropped, incomplete, or insufficient data sessions

7.9.3 Email Scheduler

View xml snippet: | [9.0](#) | [9.1](#) | [10.0](#) | [10.1](#) |

Schedule and email recipients for each report group. The template uses a sample email profile configured in `shared_log_settings`.

PANORAMA XML SNIPPETS

The configuration snippet descriptions and the associated GitHub repository link for each xml snippet.

Panorama can be configured using shared elements and device-specific elements. For xml configurations the use of shared or device-specific configurations is based on the xpath location of the snippets. Set commands also denote shared or device-specific configurations. The provided xml snippets have variations in the .meta-cnc.yaml files specifying shared or device-specific placement in the configuration while the set commands and default loadable configuration are shared only.

Grouping of XML snippets

The xml template directories are group according to the user environment:

- *snippets_panorama*: A full Panorama configuration using shared device-group and template configurations
- *snippets_panorama_dgtemplate_shared*: used to add shared device-group and baseline template content without Panorama system elements
- *snippets_panorama_not_shared*: a full Panorama configuration with the device-group and stack containing all configuration elements. Nothing is shared.
- *snippets_panorama_dgstack_notshared*: used to add additional device-groups and stack, each with full configuration elements. Nothing is shared.

Note: The template version is found in the template xml file as a tag attribute

Note: The set commands utilize the same configuration settings

8.1 Playlist Includes Model

Starting with IronSkillet 10.1, the xml snippets are included in sub-skilllets in the [ironskillet-components](#) submodule. These sub-skilllets are referenced in playlists through skilllet includes, and allows for easy re-use of individual snippets. It also allows for subsets of the configuration to be run, as reflected in the new playlist options for panos and panorama configuration. An overview of the IronSkillet playlists available can be found in the playlist folder in the IronSkillet repo.

See the [Playlist Includes tutorial](#) in the SkilletBuilder documentation for more information on how this works.

Note: If using the xpaths for IronSkillet 10.1 XML snippets directly from ironskillet-components, you may need to change xpath to match a panorama notshared configuration. The shared xpath is used as the default in the sub-skillets. XML snippets that change xpaths between the panorama shared and panorama notshared versions are marked with an asterisk (10.1*).

8.2 General Device Configuration

This section provides templated configurations for general device settings.

8.2.1 Panorama Admin Users

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

Management configuration superuser access

- Administrative user name
- Password hash stored in the configuration file

8.2.2 Panorama Password Complexity

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

Administrative user password complexity profile

- Attributes including minimum length, characters, and history

8.2.3 Panorama settings

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

System configuration settings for dynamic updates and network services (eg. DNS, NTP).

- Update schedule settings
 - Check every 30 minutes for new threat signatures
 - Hourly checks for new AV signatures
 - Check realtime for new Wildfire signatures
 - Recommended time delays and thresholds for checks and installs
- Use SNMPv3
- Set default DNS and NTP values
- Set timezone to UTC
- Provide a standard login banner warning for unauthorized users

Note: The Panorama deployment types include `standard` or `cloud` for AWS, Azure, or GCP environments. This is an option in the tools `build_my_config` utility to use the proper config option in the template.

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

Panorama management settings

- Set 'enable reporting on groups' to 'yes'
- Disable sharing unused objects with devices
- Set an API key lifetime instead of a permanent/static value
 - default set to 525,600 minutes (1 year)
- set export of csv log file to maximum of 1,048,576
- Administrative lockout and access
 - failed attempts and lockout time
 - idle timeout
 - auto acquire commit lock

8.2.4 Security-related Device Settings

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1* |

General device settings that effect security posture. Found in Device > Setup in the GUI.

- Wildfire: set optimal file size limits for Wildfire uploads and show verdict responses for grayware, malware and phishing
- Session rematch: the firewall will go through all the existing sessions and apply the new security policy to any matching traffic
- Notify User: user should be notified when web-application is blocked; enables the application response page
- Log Suppression: disabled to ensure unique log entries even if similar session types
- Prevent TCP and UDP buffer overflow and multi-part HTTP download evasions
 - Disable 'tcp-bypass-exceed-queue'
 - Disable 'udp-bypass-exceed-queue'
- Enable high DP load logging
- Prevent App-ID buffer overflow evasion
 - set bypass-exceed-queue to 'no'
- Prevent TCP and MPTCP evasions
 - set urgent data to 'clear'
 - set drop zero flag to 'yes'
 - set bypass-exceed-oo-queue to 'no'
 - set check-timestamp-option to 'yes'
 - set strip-mptcp-option to yes
- Set an API key lifetime instead of a permanent/static value

- default set to 525,600 minutes (1 year)
- set export of csv log file to maximum of 1,048,576

8.2.5 System Configuration

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1* |

System configuration settings for dynamic updates and network services (eg. DNS, NTP).

- Update schedule settings
 - Check every 30 minutes for new threat signatures
 - Hourly checks for new AV signatures
 - Check realtime for new Wildfire signatures
 - Recommended time delays and thresholds for checks and installs
- Use SNMPv3
- Set default DNS and NTP values
- Set timezone to UTC
- Provide a standard login banner warning for unauthorized users

Note: The management config types include static or dhcp-client. This is specific to each deployment and can be selected as part of the tools to build `loadable_configs`. Since management interface is in the template config, this option must be included for deployment.

8.3 Logging

Logging best practice configurations for logging output and forwarding profiles. Also Panorama-specific settings for Panorama as a log collector

Warning: Configure logging profiles before security rules The template creates a log forwarding profile call default. This profile is referenced in the template security rules and should be configured before the security rules.

Note: Logging can be deployment dependent The destination in the logging profile is templated to an unroutable syslog server address. This can vary based on actual deployment scenarios.

8.3.1 Log forwarding profile

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1* |

Log forward profile referenced in security rules to determine where to forward log related events.

- Forward all log activity to Panorama (see the reference syslog configuration in shared_log_settings.xml)
- Email malicious and phishing Wildfire verdicts to the address in the email profile (see shared_log_settings.xml)

8.3.2 Device log settings

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1* |

Device event logging including sample profiles for email and syslog forwarding.

- Reference syslog profile that can be edited for a specific IP address and UDP/TCP port
- Reference email profile that can be edited for specific email domain and user information
- System, configuration, user, HIP, and correlation log forwarding to syslog
- Email critical system events to the email profile

Note: When to use email alerts The purpose of select email alert forwarding is ensure not to under alert or over alert yet provide critical messages for key events. Under alerting reduces visibility to key events while over alerting creates too much noise in the system. The templates are set with a median view to capture key events without too much ‘log fatigue’ noise

8.3.3 Panorama log settings

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

Panorama event logging including sample profiles for email and syslog forwarding.

- Reference syslog profile that can be edited for a specific IP address and UDP/TCP port
- Reference email profile that can be edited for specific email domain and user information
- System, configuration, user, HIP, and correlation log forwarding to Panorama
- Traffic and threat related log configuration forwarding to Panorama

8.3.4 Panorama log collector group

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

After you configure Log Collectors and firewalls, you must assign them to a Collector Group so that the firewalls can send logs to the Log Collectors.

This is a placeholder default log collector group providing proper log forwarding and real-time email alerting configuration. In many cases deployments under-alert or over-alert real time losing visibility to something drastic because it is never sent to lost in then noise of too many emails.

- Syslog all logs using the sample syslog profile
- Email alerts for critical system logs and Wildfire malware/phishing verdicts that require immediate attention

8.4 Referenced Objects

Address, External Dynamic List (EDL), and tag objects that are referenced in security rules by name.

8.4.1 Tags

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1* |

Tags used in security rules and related objects.

- Inbound - inbound (untrust to trust) elements
- Outbound - outbound (trust to untrust) elements
- Internal - internal (trust) segmentation elements

8.5 Security Profiles and Groups

The key elements for security posture are security profiles and the security rules. The templates ensure best practice profiles and profile groups are available and can be referenced in any security rules. The template security rules focus on 'top of the list' block rules to reduce the attack surface.

Warning: Profiles and subscriptions All of the template security profiles other than file blocking require Threat Prevention, URL Filtering, and Wildfire subscriptions. Ensure that the device is properly licensed before applying these configurations.

8.5.1 Custom URL Category

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1* |

Placeholder for custom url categories used in security rules and url profiles. Using these categories prevents the need to modify the default template.

- Block: placeholder to be used in block rules and objects to override default template behavior
- Allow: placeholder to be used in permit rules and objects to override default template behavior
- Custom-No-Decrypt: to be used in the decryption no-decrypt rule to specify URLs that should not be decrypted

8.5.2 File Blocking

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1* |

Security profile for actions specific to file blocking (FB).

Note: File blocking and file types The Block file type recommendation is based on common malicious file types with minimal impact in a Day 1 deployment. Although PE is considered the highest risk file type it is also used for legitimate purposes so blocking PE files will be deployment specific and not included in the template.

- Day 1 Block file types: 7z, bat, chm, class, cpl, dll, hlp, hta, jar, ocx, pif, scr, torrent, vbe, wsf
 - The profiles will alert on all other file types for logging purposes
-

Profiles:

- Outbound-FB: For outbound (trust to untrust) security rules
- Inbound-FB: For inbound (untrust to trust) security rules
- Internal-FB: For internal network segmentation rules
- Alert-Only-FB: No file blocking, only alerts for logging purposes
- Exception-FB: For exception requirements in security rules to avoid modifying the default template profiles

8.5.3 Anti-Spyware

View xml snippet: | [9.0](#) | [9.1](#) | [10.0](#) | [10.1*](#) |

Security profile for actions specific to anti-spyware (AS).

Note: Sinkhole addresses The profiles use IPv4 and IPv6 addresses for DNS sinkholes. IPv4 is currently provided by Palo Alto Networks. IPv6 is a bogon address. In 9.0 the IPv4 address is replaced by an FQDN

[9.x] Support for DNS Cloud subscription service

- In addition to the current malicious domain push to the device, also include domain lookups using the cloud service

[10.x] Support for DNS Cloud subscription domain categories and actions

- set malicious categories to sinkhole

Profiles:

- Outbound-AS : For outbound (trust to untrust) security rules
 - Block severity = Critical, High, Medium
 - Default severity = Low, Informational
 - DNS Sinkhole for IPv4 and IPv6
 - Single packet capture for Critical, High, Medium severity
- Inbound-AS : For inbound (untrust to trust) security rules
 - Block severity = Critical, High, Medium
 - Default severity = Low, Informational
 - DNS Sinkhole for IPv4 and IPv6
 - Single packet capture for Critical, High, Medium severity
- Internal-AS : For internal network segmentation rules
 - Block severity = Critical, High
 - Default severity = Medium, Low, Informational
 - DNS Sinkhole for IPv4 and IPv6
 - Single packet capture for Critical, High, Medium severity

- Alert-Only-AS : No blocking, only alerts for logging purposes
 - Alert all severities and malicious domain events
 - No packet capture
- Exception-AS : For exception requirements in security rules to avoid modifying the default template profiles

8.5.4 URL Filtering

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1* |

Security profile for actions specific to URL filtering (URL).

Note: Only BLOCK categories will be listed for each profile below. All other URL categories will be set to ALERT in the templates for logging purposes. The complete list of categories can be found in the url filtering template.

[10.x] Support for local machine learning based on web content

- block malicious content using dynamic classification

Profiles:

- Outbound-URL : For outbound (trust to untrust) security rules
 - URL Categories
 - Site Access: Block command-and-control, malware, phishing, Black List (custom URL category)
 - User Credential Submission: Block all categories
 - Alert category = includes White List (custom URL category)
 - URL Filtering Settings: HTTP Header Logging (user agent, referer, X -Forwarded-For)
 - dynamic classification to block malicious web content
- Alert-Only-URL : No blocking, only alerts for logging purposes
 - Alert all categories including custom categories Black List and White List
- Exception-URL : For exception requirements in security rules to avoid modifying the default template profiles
 - URL Categories
 - Site Access: Block command-and-control, malware, phishing, Black List (custom URL category)
 - User Credential Submission: Block all categories
 - Alert category = includes White List (custom URL category)
 - URL Filtering Settings: HTTP Header Logging (user agent, referer, X -Forwarded-For)
 - dynamic classification to block malicious web content

Note: 9.0 includes new URL categories for risk and newly created domains. In future best practices, these categories may be used to provide additional security protections when combined with existing URL categories. For now, these categories are only set to *alert*.

8.5.5 Anti-Virus

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1* |

Security profile for actions specific to AntiVirus (AV) and Wildfire signatures. All decoders using 'reset-both' as actions except for the Alert-Only profile.

[10.x] Support for WF-based local machine learning to block malicious content for exe and powershell files.

Profiles:

- Outbound-AV: For outbound (trust to untrust) security rules
- Inbound-AV: For inbound (untrust to trust) security rules
- Internal-AV: For internal network segmentation rules
- Alert-Only-AV: No blocking, only alerts for logging purposes
- Exception-AV: For exception requirements in security rules to avoid modifying the default template profiles

Note: **Email response codes with SMTP not IMAP or POP3** Reset-both is used for SMTP, IMAP, and POP3. SMTP '541' response messages are returned to notify that the session was blocked. IMAP and POP3 do not have the same response model. In live deployments, instead of DoS concerns with retries, the endpoints typically stop resending after a small number of sends with timeouts.

Note: 9.0 includes support for http/2. If you are upgrading from a previous version ensure that this decoder matches the actions for standard http.

8.5.6 Vulnerability Protection

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1* |

Profiles:

- Outbound-VP : For outbound (trust to untrust) security rules
 - Block severity = Critical, High, Medium
 - Alert severity = Low, Informational
 - Single packet capture for Critical, High, Medium severity
- Inbound-VP : For inbound (untrust to trust) security rules
 - Block severity = Critical, High, Medium
 - Alert severity = Low, Informational
 - Single packet capture for Critical, High, Medium severity
- Internal-VP : For internal network segmentation rules
 - Block severity = Critical, High
 - Alert severity = Medium, Low, Informational
 - Single packet capture for Critical, High, Medium severity
- Alert-Only-VP : No blocking, only alerts for logging purposes

- Alert all severities
- No packet capture
- Exception-VP: For exception requirements in security rules to avoid modifying the default template profiles

Note: A separate branch is being used as a placeholder for [Brute-Force-Exceptions](#). This provides a way to include Support recommended exceptions by ThreatID value. These can be loaded using console SET commands or using API-based tools

8.5.7 Wildfire Analysis

View xml snippet: | [9.0](#) | [9.1](#) | [10.0](#) | [10.1*](#) |

Security profile for actions specific to Wildfire upload and analysis (WF).

Note: `Public Cloud` is the default All template profiles are configured to upload all file types in any direction to the public cloud for analysis.

Profiles:

- Outbound-WF: For outbound (trust to untrust) security rules
- Inbound-WF: For inbound (untrust to trust) security rules
- Internal-WF: For internal network segmentation rules
- Alert-Only-WF: No blocking, only alerts for logging purposes
- Exception-WF: For exception requirements in security rules to avoid modifying the default template profiles

8.5.8 Security Profile Groups

View xml snippet: | [9.0](#) | [9.1](#) | [10.0](#) | [10.1*](#) |

Security profile groups based on use case

- Inbound: For rules associated to inbound (untrust to trust) sessions
- Outbound: For rules associated to outbound (trust to untrust) sessions
- Internal: For rules associated to trust-domain network segmentation
- Alert Only: Provides visibility and logging without a blocking posture

8.6 Security Rules

8.6.1 Recommended Block Rules

View xml snippet: | [9.0](#) | [9.1](#) | [10.0](#) | [10.1*](#) |

Recommended block rules for optimal security posture with associated default log-forwarding profile

- Outbound Block Rule: Block destination IP address match based on the Palo Alto Networks predefined external dynamic lists
- Inbound Block Rule: Block source IP address match based on the Palo Alto Networks predefined external dynamic lists

Note: Security rules in the template are block only The template only uses block rules. Allow rules are zone, direction and use case dependent. Additional templating work will provide recommended use case security rules.

8.6.2 Default Security Rules

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1* |

Configuration for the default interzone and intrazone default rules

- Intrazone
 - Enable logging at session-end using the default logging profile
 - Use the Internal security profile-group
- Interzone
 - Explicit drop of traffic between zones
 - Enable logging at session-end using the default logging profile

8.7 Decryption

8.7.1 Profiles

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1* |

Recommended_Decryption_Profile. Referenced by the default decryption rule.

- SSL Forward Proxy
 - Server Cert Verification : Block sessions with expired certs, Block sessions with untrusted issuers, Block sessions with unknown cert status
 - Unsupported Mode Checks : Block sessions with unsupported versions, Blocks sessions with unsupported cipher suites
- SSL No Proxy
 - Server Cert Verification : Block sessions with expired certs, Block sessions with untrusted issuers
- SSH Proxy
 - Unsupported Mode Checks : Block sessions with unsupported versions, Block sessions with unsupported algorithms
- SSL Protocol Settings:
 - Minimum Version: TLSv1.2; Max version TLSv1.3; Any TLSv1.1 errors can help find outdated TLS endpoints

- Key Exchange Algorithms: RSA not recommended and unchecked
- Encryption Algorithms: 3DES and RC4 not recommended and unavailable when TLSv1.2 is the min version
- Authentication Algorithms: MD5 not recommended and unavailable when TLSv1.2 is the min version

8.7.2 Decryption Rules

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1* |

Recommended SSL decryption pre-rules for no-decryption.

- NO decrypt rule for select URL categories; Initially disabled in the Day 1 template until SSL decryption to be enabled

8.8 Zone Protection

8.8.1 Profile

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1* |

Recommended_Zone_Protection profile for standard, non-volumetric best practices. This profile should be attached to all interfaces within the network.

Note: Recon Protection Default values enabled in alert-only mode; active blocking posture requires network tuning

Packet Based Attack Protection

- IP Drop: Spoofed IP Address, Malformed
- TCP Drop: Remove TCP timestamp, No TCP Fast Open, Multipath TCP (MPTCP) Options = Global

8.9 Reports

8.9.1 Reports

View xml snippet: | 9.0 | 9.1 | 10.0 | 10.1 |

Series of reports to look for traffic anomalies, where to apply or remove rules, etc. Reports are grouped by topic per the report group section below.

Note: Zones and Subnets in report queries The repo contains a separate folder for custom reports that use a placeholder zone called 'internet' for match conditions in reports. This value **MUST** be changed to match the actual public zone used in a live network. Additional zones and/or subnets to be used or excluded in the reports would be added in the query values.

Note: To generate reports that include PA-7000 Series log data not forwarding to Panorama, use Remote Device Data as the Data Source. This is only viewable from the `All` device group option and not a specific device group.

8.9.2 Report Groups

View xml snippet: | [9.0](#) | [9.1](#) | [10.0](#) | [10.1](#) |

Report groups allow you to create sets of reports that the system can compile and send as a single aggregate PDF report with an optional title page and all the constituent reports included.

Template report groups include:

Simple (included in Day One template)

- Possible Compromise: malicious sites and verdicts, sinkhole sessions

Custom

- User Group Activity (eg. Employee, Student, Teacher): user-id centric reports grouped by user type
- Inbound/Outbound/Internal Rule Tuning: Used rules, app ports, unknown apps, geo information
- Inbound/Outbound/Internal Threat Tuning: Allowed threats traversing the device
- File Blocking Tuning: View of upload/download files and types with associated rule
- URL Tuning: Views by categories, especially questionable and unknown categories
- Inbound/Outbound/Internal Threats Blocked: Threat reports specific to blocking posture; complement to threat tuning
- Non-Working Traffic: View of dropped, incomplete, or insufficient data sessions

8.9.3 Email Scheduler

View xml snippet: | [9.0](#) | [9.1](#) | [10.0](#) | [10.1](#) |

Schedule and email recipients for each report group. The template uses a sample email profile configured in `shared_log_settings`.

FORMULA-BASED EXCEL SPREADSHEET

For users who want to customize their configuration before loading without the use of python utilities, this is a preferred model for configuration.

The spreadsheets can be found at:

PAN-OS | [9.0](#) | [9.1](#) | [10.0](#) | [10.1](#) |

Panorama | [9.0](#) | [9.1](#) | [10.0](#) | [10.1](#) |

The `values` worksheet can be updated with user-specific values. Formulas embedded in the `set` commands worksheet will use the user added values.

Once the spreadsheet is updated, the traditional copy-and-paste model can be used to load the configuration using the CLI.

<p>Warning: The <code>set</code> commands use formulas referencing cells in the <code>values</code> worksheet. Use caution if making changes to the base spreadsheet to avoid incorrect references to cell values.</p>

CREATING LOADABLE CONFIGURATIONS

The base templates are designed for variable substitution. The variables provide flexibility for templates configurations to be modified specific to each deployment.

A jinja model for variables is used with the form `{{ variable }}`

Warning: The configuration templates for device and Panorama system include jinja ‘if’ conditionals. These are used by the `create_loadable_configs.py` tool to determine what IP information should be added regarding the management interface.

If the tool or jinja formats will not be used, remove the `{% text %}` statements. The user will also have to manually replace the variables in order for the config to load and commit

10.1 Variables list and descriptions

The table below lists the template variables along with placeholder or recommended settings.

Variable name	Default value	Description
ADMINISTRATOR_USERNAME	admin	superuser id; prompted when using <code>build_my_config</code> tool
ADMINISTRATOR_PASSWORD	admin [change first]	superuser password; prompted and hashed in <code>build_my_config</code>
FW_NAME	sample	used for hostname and device-group/template in Panorama
STACK	sample_stack	Panorama sample template name
DEVICE_GROUP	sample_devicegroup	Panorama sample device-group name
DNS_1	8.8.8.8 (Google)	primary DNS server
DNS_2	8.8.4.4 (Google)	secondary DNS server
NTP_1	0.pool.ntp.org	primary NTP server
NTP_2	1.pool.ntp.org	secondary NTP server
SINKHOLE_IPV4	72.5.65.111	IPv4 sinkhole address (Palo Alto Networks)
SINKHOLE_IPV6	2600:5200::1	IPv6 sinkhole address (IPv6 bogon)
EMAIL_PROFILE_GATEWAY	192.0.2.1	email profile gateway address; NET-1 default
EMAIL_PROFILE_FROM	sentfrom@yourdomain.com	from address for email alerts
EMAIL_PROFILE_TO	sendto@yourdomain.com	to address for email alerts
SYSLOG_SERVER	192.0.2.2	syslog IP address; NET-1 unroutable default
CONFIG_EXPORT_IP	192.0.2.3	config bundle export target from Panorama; NET-1 default
MGMT_TYPE	dhcp-client	Firewall mgmt IP type (dhcp-client or static)
MGMT_IP	192.168.55.10	Firewall mgmt IP if type=static
MGMT_MASK	255.255.255.0	Firewall netmask if type=static
MGMT_DG	192.168.55.2	Firewall default gateway if type=static

continues on next page

Table 1 – continued from previous page

Variable name	Default value	Description
CONFIG_PANORAMA_IP	yes	For build_my_config, determine if Panorama IP to be added
PANORAMA_TYPE	standard	Used in order to set mgmt interface for standard or cloud
PANORAMA_IP	192.168.55.7	Panorama IP if to be added to my_config
PANORAMA_MASK	255.255.255.0	Panorama netmask if to be added to my_config
PANORAMA_DG	192.168.55.2	Panorama default gateway if to be added to my_config
API_KEY_LIFETIME	525600	Panorama and device API key lifetime in minutes
INCLUDE_PAN_EDL	yes	Include the panw edl object security rules
config_mgmt_intf	no	Include management interface config snippet
config_admin_user	no	Include addition of admin user account
config_dns	no	Include DNS configuration element

10.2 Create Loadable Configuration using the SLI tool (10.1 onwards)

The tools folder in the iron-skilllet repo contains a simple bash script the runs a series of SLI commands in order to create both XML and set command versions of the loadable configs with variable substitution.

This tools folder can be found at:

Release branch | [10.1](#) |

Command to create the loadable config using SLI:

```
$ sli template -n {template_name} {out_directory}
```

This command takes in a full panos skilllet file generated from the playlists directory and renders it with jinja variable substitution thus outputting a final loadable config file in the specified directory. This is done for all 5 loadable_config directories.

10.3 Create Loadable Configuration python utility (pre 10.1)

The tools folder in the iron-skilllet repo contains a simple python utility for variable substitution.

This tools folder can be found at:

Release branch | [9.0](#) | [9.1](#) | [10.0](#) |

The directions below detail how to use the utility in a python virtual environment on Mac or Linux. Similar instructions can work for Windows with python and pip installed.

Note: This tool is designed for Python 3.6 or layer.

Note: The examples below show PAN-OS 9.0 and other releases can be used by changing the release/branch version.

10.3.1 Install the repo and tools

The initial step is to clone the repo to a local machine with releaselbranch panos_v10.0.

Clone using ssh:

```
$ git clone -b panos_v10.0 git@github.com:PaloAltoNetworks/iron-skillet.git
```

Clone using https:

```
$ git clone -b panos_v10.0 https://github.com/PaloAltoNetworks/iron-skillet.git
```

After the repo is cloned locally, the following steps are used to setup and activate the python virtual environment.

Note: The example below shows python version 3.6 in the second step. If using another 3.x version, replace with the respective version

```
$ cd iron-skillet/tools
$ python3.6 -m venv env
$ source env/bin/activate
(env)$ pip install -r requirements.txt
```

The virtual environment name is `env` and if active will likely be shown to the left of the command prompt. If successful, the iron-skillet templates and tools are now ready to use.

10.3.2 Update the variable values

Inside the tools directory, update the `config_variables.yaml` file then run `create_loadable_configs.py`. The example shows the `vi` text editor but any text editor may be used.

```
(env)$ cd iron-skillet/tools [if not in the tools directory]
(env)$ vi config_variables.yaml
```

Edit the `config_variables.yaml` file for your local deployment and save.

Key variables to edit include:

- management interface type: static or dhcp-client based on firewall deployment
- Panorama deployment type: standard or cloud based on Panorama deployment

10.3.3 Run the application

Ensure the variable values are correct and run the application.

```
(env)$ python3 create_loadable_configs.py
>>> Enter the name of the output directory:
>>> Enter the superuser administrator account username:
>>> Enter the superuser administrator account password:
```

This will run the python utility and output set commands and full xml config files. Loadable configs are stored in the `loadable_configs` directory. The config folder prefix is based on the output directory name used when running the script.

Warning: You will be prompted for a username/password that will be used in the configuration file. A hash is created for the password so it is unreadable and the default admin/admin is removed. Remember the user/password information before committing to a running firewall or Panorama.

LOADING THE XML TEMPLATES

The template are xml file format that have to be loaded into the device as a full config or with modular partial loading. Multiple options including GUI, CLI, and API can be utilized. The sections below give details for template loading using various models specific to the users expertise and current operational environment.

Note: Sample configuration files are in the `loadable_configs` directory. Samples include a static management interface, basic dhcp-client management interface, and additional dhcp-client options for cloud deployments. These configurations are loadable and can be manually edited although user-specific configurations can be created using the ``create_loadable_configs`` utility in the tools folder.

11.1 Loading Configuration Snippets using Panhandler

11.1.1 panHandler overview

Panhandler is container-based UI used to aggregate and load configuration templates. PanHandler simplifies input of user data and using the NGFW API to push configuration snippets.

11.1.2 installing and using PanHandler

PanHandler is an easily distributed and loadable Docker container. Instructions for using PanHandler can be reviewing the [PanHandler Docs](#)

11.2 Loading Configuration Snippets using SLI

11.2.1 SLI overview

The Skillet Line Interfacing tool is a CLI interface that can be used to load and work with skilletts including IronSkillet.

11.2.2 installing and using SLI

Please refer to the README document found within the following [SLI](#) repository. This will walk you through the installation and basic usage of SLI in the context of skillet.

For more information on SLI commands and their use within the IronSkillet tools directory please refer to the following [link](#).

11.3 Preparing the configuration files

The template files in the panos and panorama directories are xml format. These templates are using a jinja variable model in the xml as `{{ variable name }}`. In order to have a loadable configuration, the recommended practice is to use `create_loadable_configs.py` in the tools folder.

The *Creating Loadable Configurations* documentation section details how to use this tool.

The output of the tool will be a set of xml snippet and full configuration files stored in the `loadable_configs` folder.

11.4 Load full configuration file

Either at the time of VM instantiation or post deploy, a full xml can be loaded into the system as a candidate configuration. This provides the simplicity of loading a new configuration but will replace any configuration currently in the device.

In comparison, a load config partial requires additional steps but merges into the existing configuration instead of replacing.

The steps below are for for a full configuration load and replace.

11.4.1 Edit the full xml configuration file

Since this will replace the existing configuration, the user is required to modify the xml file with admin accounts, management IP, and other initial configuration values. The template uses `{{ text }}` markers in the config file to denote values that MUST be changed.

Warning: During a commit, the device will show an error with the variable `{{ text }}` values in the error message. These values must be modified offline and the file imported for a successful load and commit.

Note: The user is recommended to use the `create_loadable_configs.py` tool to have a loadable configuration file

11.4.2 Import the configuration file using the GUI

1. Log into the firewall and click on the `Device` tab
2. Select `Setup` in the left nav bar
3. Click on the `Operations` tab
4. Then `Import` named configuration snapshot choosing the day one config xml file

Note: You should perform a `Save` named configuration snapshot as backup prior to loading the new configuration

11.4.3 Load and commit the configuration

1. Still under the `Operations` tab, use `Load` named configuration snapshot choosing the day one config xml file
2. Ensure no errors loading the configuration.
3. Once loaded use the GUI to verify the configuration elements have been loaded then `commit`

Note: As referenced above, you may see `{{ text }}` related errors during the commit. If this happens, you will need to edit the pre-imported xml file and then repeat the steps above to import, load, and commit the configuration.

11.5 Using Load Config Partial

The configuration file uses the xml format. Therefore each configuration element sits in the xml tree and is referenced by its `xpath`.

Using this concept, a template configuration file can be imported into Panorama or the firewall with only the referenced elements merged into the existing configuration. This is more modular than loading a full configuration file that replaces the existing configuration.

The syntax used for loading the templates is:

```
load config partial from {{filename}} from-xpath {{xpath}} to-xpath {{xpath}} mode merge
```

where:

`{{filename}}` is the xml file loaded into the device

`{{xpath}}` denotes what part of the configuration is being merged from the day one file to the candidate configuration.

11.5.1 Edit the configuration xml file

Since this will replace the existing configuration, the user is required to modify the xml file with admin accounts, management IP, and other initial configuration values. The template uses `{{ text }}` markers in the config file to denote values that MUST be changed.

Warning: During a commit, the device will show an error with the variable `{{ text }}` values in the error message. These values must be modified offline and the file imported for a successful load and commit.

Note: The user is recommended to use the `create_loadable_configs.py` tool to have a loadable configuration file

11.5.2 Import the Day One configuration: GUI

1. Log into the firewall and click on the `Device` tab
2. Select `Setup` in the left nav bar
3. Click on the `Operations` tab
4. Then Import named configuration snapshot choosing the day one config xml file

Note: You can perform a `Save` named configuration snapshot as backup prior to loading the new configuration

11.5.3 Load the configuration elements: CLI

1. Log into the PAN-OS command line interface
2. Enter `configure` to go into configuration mode
3. Paste in each of the `load config partial` commands, in order
4. Once complete use the GUI to verify the configuration elements have been loaded then `commit`

11.5.4 PAN-OS load config partial commands

Cut-and-paste from the table below into the PAN-OS command line while in configuration mode.

You can paste multiple items. The system will pause during each load config partial, return a status message, then move to the next load. When complete, ensure the final load is entered and a status message received.

PAN-OS 8.x

```
load config partial from iron_skillet_panos_full.xml from-xpath /config/  
→shared/log-settings to-xpath /config/shared/log-settings mode merge  
load config partial from iron_skillet_panos_full.xml from-xpath /config/  
→devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/  
→tag to-xpath /config/devices/entry[@name='localhost.localdomain']/vsys/  
→entry[@name='vsys1']/tag mode merge
```

```

load config partial from iron_skillet_panos_full.xml from-xpath /config/
↳devices/entry[@name='localhost.localdomain']/deviceconfig/system to-xpath
↳/config/devices/entry[@name='localhost.localdomain']/deviceconfig/system
↳mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
↳devices/entry[@name='localhost.localdomain']/deviceconfig/setting to-xpath
↳/config/devices/entry[@name='localhost.localdomain']/deviceconfig/setting
↳mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
↳devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
↳address to-xpath /config/devices/entry[@name='localhost.localdomain']/vsys/
↳entry[@name='vsys1']/address mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
↳devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
↳external-list to-xpath /config/devices/entry[@name='localhost.localdomain']/
↳vsys/entry[@name='vsys1']/external-list mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
↳devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
↳profiles to-xpath /config/devices/entry[@name='localhost.localdomain']/vsys/
↳entry[@name='vsys1']/profiles mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
↳devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
↳profile-group to-xpath /config/devices/entry[@name='localhost.localdomain']/
↳vsys/entry[@name='vsys1']/profile-group mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
↳devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
↳rulebase to-xpath /config/devices/entry[@name='localhost.localdomain']/vsys/
↳entry[@name='vsys1']/rulebase mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /
↳config/devices/entry[@name='localhost.localdomain']/network/profiles/
↳zone-protection-profile to-xpath /config/devices/entry[@name='localhost.
↳localdomain']/network/profiles/zone-protection-profile mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
↳shared/reports to-xpath /config/shared/reports mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
↳shared/report-group to-xpath /config/shared/report-group mode merge
load config partial from iron_skillet_panos_full.xml from-xpath /config/
↳shared/email-scheduler to-xpath /config/shared/email-scheduler mode merge

```

PAN-OS 9.0 and later

```

load config partial from-xpath /config/shared/log-settings to-xpath /config/
↳shared/log-settings mode merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/vsys/entry[@name='vsys1']/tag to-xpath /config/devices/
↳entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/tag mode
↳merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/deviceconfig/system to-xpath /config/devices/
↳entry[@name='localhost.localdomain']/deviceconfig/system mode merge from
↳iron_skillet_panos_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/deviceconfig/setting to-xpath /config/devices/
↳entry[@name='localhost.localdomain']/deviceconfig/setting mode merge from
↳iron_skillet_panos_full.xml

```

```
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/vsys/entry[@name='vsys1']/address to-xpath /config/devices/
↳entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/address mode_
↳merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/vsys/entry[@name='vsys1']/external-list to-xpath /config/
↳devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
↳external-list mode merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/vsys/entry[@name='vsys1']/profiles to-xpath /config/devices/
↳entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/profiles_
↳mode merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/vsys/entry[@name='vsys1']/profile-group to-xpath /config/
↳devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
↳profile-group mode merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/vsys/entry[@name='vsys1']/rulebase to-xpath /config/devices/
↳entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/rulebase_
↳mode merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/network/profiles/zone-protection-profile to-xpath /
↳config/devices/entry[@name='localhost.localdomain']/network/profiles/
↳zone-protection-profile mode merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/shared/reports to-xpath /config/shared/
↳reports mode merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/shared/report-group to-xpath /config/
↳shared/report-group mode merge from iron_skillet_panos_full.xml
load config partial from-xpath /config/shared/email-scheduler to-xpath /
↳config/shared/email-scheduler mode merge from iron_skillet_panos_full.xml
```

Note: The filename is specific to the iron-skillet templates but can be renamed if the base file is renamed. Simply use a text editor to replace the template filename with the update name.

Note: For subsequent updates, specific load config partial commands can be used.

11.5.5 PAN-OS config elements used in load config partial

Each xpath in the load config partial gives an indication of each element loaded. Below is a simple explanation of the configuration elements with key items in the xml load.

xpath	suffix description
log settings	settings syslog/email profiles and system, configuration logging
tag	referenced tags used in security rules
system	dynamic updates, dns and ntp server settings
setting	Wildfire max file sizes, disable log suppression
address	named references for sinkholes values used in security rules
external list	EDLs referenced in security rules, eg. IPv4/v6 bogons
profiles	Threat, URL Filtering, Wildfire, and decryption profile configurations
profile-group	Group settings for the security profiles, eg. Inbound, Outbound, Alert-All
rulebase	template security and decryption rules
zone protection	recommended zone protection profile
reports	traffic and threat reports
report groups	grouping of reports for viewing and scheduling
email scheduler	email schedule for report groups

11.5.6 Panorama load config partial commands

Cut-and-paste from the table below into the PAN-OS command line while in configuration mode.

You can paste multiple items. The system will pause during each load config partial, return a status message, then move to the next load. When complete, ensure the final load is entered and a status message received.

Panorama 8.x

```
load config partial from iron_skillet_panorama_full.xml from-xpath /config/
↳devices/entry[@name='localhost.localdomain']/deviceconfig/system to-xpath
↳/config/devices/entry[@name='localhost.localdomain']/deviceconfig/system
↳mode merge
load config partial from iron_skillet_panorama_full.xml from-xpath /config/
↳devices/entry[@name='localhost.localdomain']/deviceconfig/setting to-xpath
↳/config/devices/entry[@name='localhost.localdomain']/deviceconfig/setting
↳mode merge
load config partial from iron_skillet_panorama_full.xml from-xpath /config/
↳panorama/log-settings to-xpath /config/panorama/log-settings mode merge
load config partial from iron_skillet_panorama_full.xml from-xpath /config/
↳devices/entry[@name='localhost.localdomain']/template to-xpath /config/
↳devices/entry[@name='localhost.localdomain']/template mode merge
load config partial from iron_skillet_panorama_full.xml from-xpath /config/
↳devices/entry[@name='localhost.localdomain']/device-group to-xpath /config/
↳devices/entry[@name='localhost.localdomain']/device-group mode merge
load config partial from iron_skillet_panorama_full.xml from-xpath /config/
↳shared to-xpath /config/shared mode merge
load config partial from iron_skillet_panorama_full.xml from-xpath /config/
↳devices/entry[@name='localhost.localdomain']/log-collector-group to-xpath
↳/config/devices/entry[@name='localhost.localdomain']/log-collector-group
↳mode merge
```

Panorama 9.0 and later

```
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localhost.localdomain']/deviceconfig/system to-xpath /config/devices/
↳entry[@name='localhost.localdomain']/deviceconfig/system mode merge from
↳iron_skillet_panorama_full.xml
```

```
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/deviceconfig/setting to-xpath /config/devices/
↳entry[@name='localhost.localdomain']/deviceconfig/setting mode merge from_
↳iron_skillet_panorama_full.xml
load config partial from-xpath /config/panorama/log-settings to-xpath /config/
↳panorama/log-settings mode merge from iron_skillet_panorama_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/template to-xpath /config/devices/entry[@name='localhost.
↳localdomain']/template mode merge from iron_skillet_panorama_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/device-group to-xpath /config/devices/entry[@name='localhost.
↳localdomain']/device-group mode merge from iron_skillet_panorama_full.xml
load config partial from-xpath /config/shared to-xpath /config/shared mode_
↳merge from iron_skillet_panorama_full.xml
load config partial from-xpath /config/devices/entry[@name='localhost.
↳localdomain']/log-collector-group to-xpath /config/devices/
↳entry[@name='localhost.localdomain']/log-collector-group mode merge from_
↳iron_skillet_panorama_full.xml
```

Note: The filename is specific to the iron-skillet templates but can be renamed if the base file is renamed. Simply use a text editor to replace the template filename with the update name.

Note: For subsequent updates, specific `load config partial` commands can be used.

11.5.7 Panorama config elements used in load config partial

Each xpath in the load config partial gives an indication of each element loaded. Below is a simple explanation of the configuration elements with key items in the xml load.

This uses an aggregate template loading module with multiple configuration elements contained under the template, device-group, and shared parts of the xml tree. The hierarchical nature of Panorama simplifies the configuration loading.

xpath	suffix description
panorama system	panorama specific dynamic updates, dns and ntp server settings
panorama settings	enable reporting on groups and sharing of unused objects
panorama log settings	syslog/email profiles and system, configuration logging
template	test template configuration with device settings and zone profile
device-group	reports, report groups, and email scheduler
shared	profile object, rules, and other device-group ‘top of tree’ items
log collector	settings for Panorama when used as a log collector

11.6 Loading Configuration Snippets using skilletCLI

11.6.1 SkilletCLI overview

This open-source utility provides a command line interface to Palo Alto “skillets”, curated configuration templates designed to be imported into firewalls or Panorama.

11.6.2 installing and using SkilletCLI

Usage information for SkilletCLI is found in the repo [SkilletCLI](#)

VM-50 SECURITY PROFILE LIMITS

IronSkillet includes a broad set of security profiles to simplify the usage in security policies. However, the VM-50 limits the number of security profiles that can be configured to 38 resulting in possible commit errors if this limit is exceeded.

Note: If > 49 profiles, the user may see an error message that the number of profiles (39) exceeds capacity (38). This is an error in the message output and the user will have to remove enough profiles for the 38 count limit.

Note: Make sure the firewall is licensed. An unlicensed firewall will allow only 20 profiles, far below what is configured with IronSkillet.

The *delete* commands below can be used to delete security profiles and profile groups from an IronSkillet template load that may not be required for a basic VM-50 configuration yet allow for a reduced number of profiles.

Copy/paste all or part of these commands into the console before any of the profiles or profiles groups are referenced by other items in the configuration. This will leave the Outbound, Inbound, and Alert-Only profiles in the configuration.

This frees up space for nine other security profiles not part of IronSkillet.

```
delete profile-group Internal
delete profiles virus Internal-AV
delete profiles spyware Internal-AS
delete profiles vulnerability Internal-VP
delete profiles file-blocking Internal-FB
delete profiles wildfire-analysis Internal-WF
delete profiles virus Exception-AV
delete profiles spyware Exception-AS
delete profiles vulnerability Exception-VP
delete profiles url-filtering Exception-URL
```


CIS PALO ALTO FIREWALL 9 BENCHMARK

13.1 Terms of Use

This documentation is text taken from the Center for Information Security specific to the Palo Alto Networks firewall
Official benchmark content: https://www.cisecurity.org/benchmark/palo_alto_networks/

Mirroring the terms of use from the official document: <https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

13.2 Web documentation notes

The information captured here is a summary of each benchmark that excludes some of the section specific intro text. For the complete set of content, please reference the office benchmark document.

The official document also includes references to the intended audience, consensus guidance, scoring, and current acknowledgements for key contributors.

Associated CIS Controls are captured in the benchmark document and currently omitted from this web documentation with an emphasis on audit and remediation.

13.3 1.1.1.1 Syslog logging should be configured

13.3.1 Scored/Not Scored

Scored

13.3.2 Profile Applicability

Level 1

13.3.3 Description

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

13.3.4 Rationale

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

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

13.3.5 Audit

Navigate to Device > Server Profiles > Syslog

Ensure that a valid Syslog profile is configured, and that it points to a valid Syslog host.

Navigate to Device > Log Settings

Under System, verify that at least one Syslog entry exists and that at least one entry has “All Logs” selected. Each Syslog entry must have a valid Syslog Profile attached.

Under Configuration, verify that at least one Syslog entry exists and that at least one entry has “All Logs” selected. Each Syslog entry must have a valid Syslog Profile attached.

Under User-ID, verify that at least one Syslog entry exists and that at least one entry has “All Logs” selected. Each Syslog entry must have a valid Syslog Profile attached.

Under HIP Match (Host Information Profile), verify that at least one Syslog entry exists and that at least one entry has “All Logs” selected. Each Syslog entry must have a valid Syslog Profile attached.

Under IP-Tag, verify that at least one Syslog entry exists and that at least one entry has “All Logs” selected. Each Syslog entry must have a valid Syslog Profile attached.

13.3.6 Remediation

Navigate to Device > Server Profiles > Syslog

Choose Add

Assign a Name to the Profile. Choose Add, and assign a server name in the Name field, add an IP address or FQDN in the Syslog Server field. Edit other fields as appropriate for your server.

Repeat if multiple Syslog destinations are required.

Navigate to Device > Log Settings

Under System, add an entry. Define a Name and a Filter setting. Under Forward Methods, add a Syslog Profile in the Syslog section. Ensure that at least one of the Log Settings Configuration entries has it's Filter setting at All Logs

Under Configuration, add an entry. Define a Name and a Filter setting. Under Forward Methods, add a Syslog Profile in the Syslog section. Ensure that at least one of the Log Settings Configuration entries has it's Filter setting at All Logs

Under User-ID, add an entry. Define a Name and a Filter setting. Under Forward Methods, add a Syslog Profile in the Syslog section. Ensure that at least one of the Log Settings Configuration entries has it's Filter setting at All Logs

Under HIP Match (Host Information Profile), add an entry. Define a Name and a Filter setting. Under Forward Methods, add a Syslog Profile in the Syslog section. Ensure that at least one of the Log Settings Configuration entries has it's Filter setting at All Logs

Under IP-Tag, add an entry. Define a Name and a Filter setting. Under Forward Methods, add a Syslog Profile in the Syslog section. Ensure that at least one of the Log Settings Configuration entries has it's Filter setting at All Logs

13.3.7 Impact

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

13.3.8 Default Value

By default no external logging is defined

13.3.9 References

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

13.4 1.1.1.2 SNMPv3 traps should be configured

13.4.1 Scored/Not Scored

(Scored)

13.4.2 Profile Applicability

Level 2

13.4.3 Description

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

13.4.4 Rationale

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

13.4.5 Audit

Navigate to Device > Server Profiles > SNMP Traps

Ensure that a valid SNMP profile is configured, that version V3 is selected, and that it points to a valid SNMPv3 host. User, EngineID and Password fields should be completed appropriately

Navigate to Device > Log Settings

Under System, verify that at least one SNMP entry exists, corresponding to an SNMPv3 Server Profile and that at least one entry has “All Logs” selected.

Under Configuration, verify that at least one SNMP entry exists, corresponding to a SNMPv3 Server Profile and that at least one entry has “All Logs” selected.

Under User-ID, verify that at least one SNMP entry exists, corresponding to a SNMPv3 Server Profile and that at least one entry has “All Logs” selected.

Under HIP Match (Host Information Profile), verify that at least one SNMP entry exists, corresponding to a SNMPv3 Server Profile and that at least one entry has “All Logs” selected.

Under IP-Tag, verify that at least one SNMP entry exists, corresponding to a SNMPv3 Server Profile and that at least one entry has “All Logs” selected.

13.4.6 Remediation

Navigate to Device > Server Profiles > SNMP Trap

Choose Add Assign a Name to the Profile, and specify version V3.

Choose Add, and assign a server name in the Name field, add an IP address or FQDN in the SNMP Manager field. Edit the Password fields as appropriate for your server.

Repeat if multiple Syslog destinations are required.

Navigate to Device > Log Settings

Under System, add an entry. Define a Name and a Filter setting. Under Forward Methods, add a SNMP Profile in the SNMP section. Ensure that at least one of the Log Settings Configuration entries has its Filter setting at All Logs

Under Configuration, add an entry. Define a Name and a Filter setting. Under Forward Methods, add a SNMP Profile in the SNMP section. Ensure that at least one of the Log Settings Configuration entries has its Filter setting at All Logs

Under User-ID, add an entry. Define a Name and a Filter setting. Under Forward Methods, add a SNMP Profile in the SNMP section. Ensure that at least one of the Log Settings Configuration entries has its Filter setting at All Logs

Under HIP Match (Host Information Profile), add an entry. Define a Name and a Filter setting. Under Forward Methods, add a SNMP Profile in the SNMP section. Ensure that at least one of the Log Settings Configuration entries has its Filter setting at All Logs

Under IP-Tag, add an entry. Define a Name and a Filter setting. Under Forward Methods, add a SNMP Profile in the SNMP section. Ensure that at least one of the Log Settings Configuration entries has its Filter setting at All Logs

13.4.7 Impact

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

13.4.8 Default Value

By default no external logging is defined

13.4.9 References

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

13.5 1.1.2 Ensure ‘Login Banner’ is set

13.5.1 Scored/Not Scored

(Scored)

13.5.2 Profile Applicability

Level 1

13.5.3 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.

13.5.4 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 ignorance.

13.5.5 Audit

Navigate to Device > Setup > Management > General Settings.

Verify that Login Banner is set appropriately for your organization.

13.5.6 Remediation

Navigate to Device > Setup > Management > General Settings.

Set Login Banner as appropriate for your organization.

13.5.7 Default Value

Not configured

13.5.8 References

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

13.6 1.1.3 Ensure ‘Enable Log on High DP Load’ is enabled

13.6.1 Scored/Not Scored

(Scored)

13.6.2 Profile Applicability

Level 1

13.6.3 Description

Enable the option ‘Enable Log on High DP Load’ feature. When this option is selected, a system log entry is created when the utilization.

13.6.4 Rationale

services accessed through the device can occur. Logging this event can help with troubleshooting system performance.

13.6.5 Audit

Navigate to Device > Setup > Management > Logging and Reporting Settings > Log Export and Reporting.

Verify Enable Log on High DP Load is checked.

13.6.6 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.

13.6.7 Impact

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

13.6.8 Default Value

Not enabled

13.6.9 References

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

13.7 1.2.1 Ensure 'Permitted IP Addresses' is set to those necessary for device management

13.7.1 Scored/Not Scored

(Scored)

13.7.2 Profile Applicability

Level 1

13.7.3 Description

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

13.7.4 Rationale

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

13.7.5 Audit

Navigate to Device > Setup > Interfaces > Management.

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

13.7.6 Remediation

Navigate to Device > Setup > Interfaces > Management.

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

13.7.7 Default Value

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

13.7.8 References

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

13.8 1.2.2 Ensure 'Permitted IP Addresses' is set for all management profiles where SSH, HTTPS, or SNMP is enabled

13.8.1 Scored/Not Scored

(Scored)

13.8.2 Profile Applicability

Level 1

13.8.3 Description

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

13.8.4 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.

13.8.5 Audit

Navigate to Network > Network Profiles > Interface Management.

In each profile, for each of the target protocols (SNMP, HTTPS, SSH), verify that Permitted IP Addresses is limited to those necessary for device management.

13.8.6 Remediation

Navigate to Network > Network Profiles > Interface Management.

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

13.8.7 Default Value

Not enabled

13.8.8 References

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

13.9 1.2.3 Ensure HTTP and Telnet options are disabled for the management interface

13.9.1 Scored/Not Scored

(Scored)

13.9.2 Profile Applicability

Level 1

13.9.3 Description

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

13.9.4 Rationale

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

13.9.5 Audit

Navigate to Device > Setup > Interfaces > Management.

Verify that the HTTP and Telnet options are both unchecked.

13.9.6 Remediation

Navigate to Device > Setup > Interfaces > Management.

Set the HTTP and Telnet boxes to unchecked.

13.9.7 Default Value

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

13.9.8 References

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

13.10 1.2.4 Ensure HTTP and Telnet options are disabled for all management profiles

13.10.1 Scored/Not Scored

(Scored)

13.10.2 Profile Applicability

Level 1

13.10.3 Description

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

13.10.4 Rationale

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

13.10.5 Audit

Navigate to Network > Network Profiles > Interface Management.

For each Interface Management profile verify that the HTTP and Telnet options are both unchecked.

13.10.6 Remediation

Navigate to Network > Network Profiles > Interface Management.

For each Profile, set the HTTP and Telnet boxes to unchecked.

13.10.7 References

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

13.11 1.2.5 Ensure valid certificate is set for browser-based administrator interface

13.11.1 Scored/Not Scored

(Not Scored)

13.11.2 Profile Applicability

Level 2

13.11.3 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.

13.11.4 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.

13.11.5 Audit

Verify that the certificate used to secure HTTPS sessions meets the criteria by reviewing the appropriate certificate:

Navigate to Device > Certificate Management > Certificates

Verify that this Certificate is properly applied to the Management Interface:

Navigate to Device > Setup > Management > General Settings > SSL/TLS Service Profile

13.11.6 Remediation

Create or acquire a certificate that meets the stated criteria and set it:

Navigate to Device > Certificate Management > Certificates

Import an appropriate Certificate for your administrative session, from a trusted Certificate Authority.

Navigate to Device > Certificate Management > SSL/TLS Service Profile

Choose or import the certificate you want to use for the web based administrative session.

Navigate to Device > Setup > Management > General Settings > SSL/TLS Service Profile

Choose the Service Profile that you have configured

13.11.7 Impact

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

13.11.8 Default Value

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

13.11.9 References

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

13.11.10 Notes

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

13.12 1.3.1 Ensure ‘Minimum Password Complexity’ is enabled

13.12.1 Scored/Not Scored

(Scored)

13.12.2 Profile Applicability

Level 1

13.12.3 Description

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

13.12.4 Rationale

Password complexity recommendations are derived from the USGCB (United States Government Configuration Base-line), 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.

13.12.5 Audit

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

Verify Enabled is checked Ensure that the various password settings to values that are appropriate to your organization. Non-zero values should be set for Minimum Uppercase, Lowercase and Special Characters. “Block Username Inclusion” should be enabled.

13.12.6 Remediation

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

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

13.12.7 Impact

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

13.12.8 Default Value

Not enabled.

13.12.9 References

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

13.13 1.3.2 Ensure 'Minimum Length' is greater than or equal to 12

13.13.1 Scored/Not Scored

(Scored)

13.13.2 Profile Applicability

Level 1

13.13.3 Description

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

13.13.4 Rationale

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

13.13.5 Audit

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

Verify Minimum Length is greater than or equal to 12

13.13.6 Remediation

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

Set Minimum Length to greater than or equal to 12

13.13.7 Impact

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

13.13.8 Default Value

Not enabled.

13.13.9 References

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

13.14 1.3.3 Ensure ‘Minimum Uppercase Letters’ is greater than or equal to 1

13.14.1 Scored/Not Scored

(Scored)

13.14.2 Profile Applicability

Level 1

13.14.3 Description

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

13.14.4 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.

13.14.5 Audit

Navigate to Device > Setup > Management > Minimum Password Complexity

Verify Minimum Uppercase Letters is greater than or equal to 1

13.14.6 Remediation

Navigate to Device > Setup > Management > Minimum Password Complexity

Set Minimum Uppercase Letters to greater than or equal to 1

13.14.7 Default Value

Not enabled.

13.14.8 References

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

13.15 1.3.4 Ensure 'Minimum Lowercase Letters' is greater than or equal to 1

13.15.1 Scored/Not Scored

(Scored)

13.15.2 Profile Applicability

Level 1

13.15.3 Description

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

13.15.4 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.

13.15.5 Audit

Navigate to Device > Setup > Management > Minimum Password Complexity

Verify Minimum Lowercase Letters is greater than or equal to 1

13.15.6 Remediation

Navigate to Device > Setup > Management > Minimum Password Complexity

Set Minimum Lowercase Letters to greater than or equal to 1

13.15.7 Default Value

Not enabled.

13.15.8 References

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

13.16 1.3.5 Ensure ‘Minimum Numeric Letters’ is greater than or equal to 1

13.16.1 Scored/Not Scored

(Scored)

13.16.2 Profile Applicability

Level 1

13.16.3 Description

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

13.16.4 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.

13.16.5 Audit

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

Verify Minimum Numeric Letters is greater than or equal to 1

13.16.6 Remediation

Navigate to Device > Setup > Management > Minimum Password Complexity

Set Minimum Numeric Letters to greater than or equal to 1

13.16.7 Impact

nan

13.16.8 Default Value

Not enabled.

13.16.9 References

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

13.16.10 Notes

nan

13.17 1.3.6 Ensure 'Minimum Special Characters' is greater than or equal to 1

13.17.1 Scored/Not Scored

(Scored)

13.17.2 Profile Applicability

Level 1

13.17.3 Description

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

13.17.4 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.

13.17.5 Audit

Navigate to Device > Setup > Management > Minimum Password Complexity

Verify Minimum Special Characters is greater than or equal to 1

13.17.6 Remediation

Navigate to Device > Setup > Management > Minimum Password Complexity

Set Minimum Special Characters to greater than or equal to 1

13.17.7 Default Value

Not enabled.

13.17.8 References

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

13.18 1.3.7 Ensure 'Required Password Change Period' is less than or equal to 90 days

13.18.1 Scored/Not Scored

(Scored)

13.18.2 Profile Applicability

Level 1

13.18.3 Description

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

13.18.4 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.

13.18.5 Audit

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

Verify Required Password Change Period (days) is less than or equal to 90

13.18.6 Remediation

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

Set Required Password Change Period (days) to less than or equal to 90

13.18.7 Impact

Failure to change administrative passwords can result in a slow “creep” of people who have access. Especially in a situation with high staff turnover (for instance, in a NOC or SOC situation), administrative passwords need to be changed frequently. Administrative credentials should not be shared across multiple devices. In a NOC/SOC situation, it’s important to not share administrative credentials between operators (names accounts should be used), and in particular administrative credentials should never be shared across different customer infrastructures.

13.18.8 Default Value

Not enabled.

13.18.9 References

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

13.18.10 Notes

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

13.19 1.3.8 Ensure ‘New Password Differs By Characters’ is greater than or equal to 3

13.19.1 Scored/Not Scored

(Scored)

13.19.2 Profile Applicability

Level 1

13.19.3 Description

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

13.19.4 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.

13.19.5 Audit

Navigate to Device > Setup > Management > Minimum Password Complexity

Verify New Password Differs By Characters is set to greater than or equal to 3

13.19.6 Remediation

Navigate to Device > Setup > Management > Minimum Password Complexity

Set New Password Differs By Characters to 3 or more

13.19.7 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.

13.19.8 Default Value

Not enabled.

13.19.9 References

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

13.20 1.3.9 Ensure 'Prevent Password Reuse Limit' is set to 24 or more passwords

13.20.1 Scored/Not Scored

(Scored)

13.20.2 Profile Applicability

Level 1

13.20.3 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.

13.20.4 Rationale

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

13.20.5 Audit

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

Verify Prevent Password Reuse Limit is greater than or equal to 24

13.20.6 Remediation

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

Set Prevent Password Reuse Limit to greater than or equal to 24

13.20.7 Default Value

Not enabled.

13.20.8 References

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

13.21 1.3.10 Ensure 'Password Profiles' do not exist

13.21.1 Scored/Not Scored

(Scored)

13.21.2 Profile Applicability

Level 1

13.21.3 Description

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

13.21.4 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.

13.21.5 Audit

Navigate to Device > Password Profiles.

Verify Password Profiles weaker than the recommended minimum password complexity settings do not exist.

13.21.6 Remediation

Navigate to Device > Password Profiles.

Ensure Password Profiles weaker than the recommended minimum password complexity settings do not exist.

13.21.7 Default Value

Not configured

13.21.8 References

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

13.22 1.4.1 Ensure 'Idle timeout' is less than or equal to 10 minutes for device management

13.22.1 Scored/Not Scored

(Scored)

13.22.2 Profile Applicability

Level 1

13.22.3 Description

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

13.22.4 Rationale

An unattended computer with an open administrative session to the device could allow an

13.22.5 Audit

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

13.22.6 Remediation

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

13.22.7 Default Value

Not configured

13.22.8 References

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

13.23 1.4.2 Ensure ‘Failed Attempts’ and ‘Lockout Time’ for Authentication Profile are properly configured

13.23.1 Scored/Not Scored

(Scored)

13.23.2 Profile Applicability

Level 1

13.23.3 Description

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

13.23.4 Rationale

From the other point of view, if lockout settings are configured in the Authentication Settings section it may be possible for an attacker to continuously lock out all administrative accounts from accessing the device. This potential situation indicates the importance of using named administrative accounts, instead of the default, single shared “admin” account.

13.23.5 Audit

Navigate to Device > Authentication Profile.

Verify Failed Attempts is set a non-zero organization-defined value.

Verify Lockout Time is set to a non-zero organization-defined value.

13.23.6 Remediation

Navigate to Device > Authentication Profile.

Set Failed Attempts to the non-zero organization-defined value.

Set Lockout Time to the non-zero organization-defined value.

13.23.7 Default Value

Not configured

13.23.8 References

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

13.23.9 Notes

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

13.24 1.5.1 Ensure ‘V3’ is selected for SNMP polling

13.24.1 Scored/Not Scored

(Scored)

13.24.2 Profile Applicability

Level 1

13.24.3 Description

For SNMP polling, only SNMPv3 should be used.

13.24.4 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.

13.24.5 Audit

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

Verify V3 is selected.

13.24.6 Remediation

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

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

13.24.7 Impact

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

13.24.8 Default Value

Not configured

13.24.9 References

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

13.25 1.6.1 Ensure 'Verify Update Server Identity' is enabled

13.25.1 Scored/Not Scored

(Scored)

13.25.2 Profile Applicability

Level 1

13.25.3 Description

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

13.25.4 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.

13.25.5 Audit

Navigate to Device > Setup > Services > Services.

Verify that the Verify Update Server Identity box is checked.

13.25.6 Remediation

Navigate to Device > Setup > Services > Services.

Set the Verify Update Server Identity box to checked.

13.25.7 Impact

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

13.25.8 Default Value

Not configured

13.25.9 References

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

13.26 1.6.2 Ensure redundant NTP servers are configured appropriately

13.26.1 Scored/Not Scored

(Scored)

13.26.2 Profile Applicability

Level 1

13.26.3 Description

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

13.26.4 Rationale

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

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

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

13.26.5 Audit

Navigate to Device > Setup > Services > Services.

Verify Primary NTP Server Address is set appropriately.

Verify Secondary NTP Server Address is set appropriately.

13.26.6 Remediation

Navigate to Device > Setup > Services > Services.

Set Primary NTP Server Address appropriately.

Set Secondary NTP Server Address appropriately.

13.26.7 Default Value

Not configured

13.26.8 References

1. "The NIST Authenticated NTP Service" - <http://www.nist.gov/pml/div688/grp40/authntp.cfm>
2. "PAN-OS Administrator's Guide 9.0 (English) - Global Services Settings" - <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-setup-services/global-services-settings.html>
3. "How to Configure Authenticated NTP" - <https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-Authenticated-NTP/ta-p/54495>

13.27 1.6.3 Ensure that the Certificate Securing Remote Access VPNs is Valid

13.27.1 Scored/Not Scored

(Not Scored)

13.27.2 Profile Applicability

Level 1, Level 2

13.27.3 Description

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

It should be a valid certificate from a trusted source. In almost cases this means a trusted Public Certificate Authority, as in most cases remote access VPN users will not have access to any Private Certificate Authorities for Certificate validation.

The certificate should have a valid date. It should not have a “to” date in the past (it should not be expired), and should not have a “from” date in the future.

The key length used to encrypt the certificate should be 2048 bits or more.

The hash used to sign the certificate should be SHA-2 or better.

When the Certificate is applied, the TLS version should be

13.27.4 Rationale

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

13.27.5 Audit

Verify that the certificate being used to secure the VPN meets the criteria listed above:

Navigate to Device > Certificate Management > Certificates

Ensure that a valid certificate is applied to the HTTPS portal:

Navigate to Network > GlobalProtect > Portals > Portal Configuration > (Select the Portal being assessed) > Authentication > SSL/TLS Profile

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

Navigate to Network > GlobalProtect > Gateways > (Select the Gateway being Assessed) > Authentication > SSL/TLS Service Profile Ensure that the correct Certificate is selected.

Ensure that the Minimum TLS version is configured to be 1.1 or higher (TLSv1.2 is recommended).

13.27.6 Remediation

Create a CSR and install a certificate from a public CA (Certificate Authority) here:

Navigate to Device > Certificate Management > Certificates

Apply a valid certificate to the HTTPS portal:

Navigate to Network > GlobalProtect > Portals > Portal Configuration > Authentication > SSL/TLS Profile

Apply a valid certificate to the GlobalProtect Gateway:

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

Configure the Service Profile to use the correct certificate

Ensure that the Minimum TLS version is set to 1.1 or 1.2 (1.2 is recommended).

13.27.7 Impact

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

13.27.8 Default Value

Not configured

13.27.9 References

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

13.28 2.1 Ensure that IP addresses are mapped to usernames

13.28.1 Scored/Not Scored

(Scored)

13.28.2 Profile Applicability

Level 2

13.28.3 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.

13.28.4 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.

13.28.5 Audit

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

13.28.6 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

13.28.7 References

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

13.29 2.2 Ensure that WMI probing is disabled

13.29.1 Scored/Not Scored

(Scored)

13.29.2 Profile Applicability

Level 2

13.29.3 Description

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

13.29.4 Rationale

WMI probing normally requires a domain administrator account. A malicious user could capture the encrypted password hash for offline cracking or relayed authentication attacks. Relying on other forms of user identification, such as using UserID Agents or security log monitoring, mitigates this risk. In addition, it is easy to mis-configure this feature such that it is enabled on untrusted interfaces. This can result in a domain administrator account and the associated password hash being sent to untrusted hosts on the internet, where malicious users can then capture that hash for offline cracking.

13.29.5 Audit

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

Verify that Enable Probing is not checked.

13.29.6 Remediation

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

Set Enable Probing so it is unchecked.

13.29.7 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.

13.29.8 Default Value

Not configured

13.29.9 References

1. “R7-2014-16: Palo Alto Networks User-ID Credential Exposure” - <https://blog.rapid7.com/2014/10/14/palo-alto-networks-userid-credential-exposure/>
2. “Best Practices for Securing User-ID Deployments” - <https://live.paloaltonetworks.com/docs/DOC-7912>
3. “PAN-OS Administrator’s Guide 9.0 (English) - Client Probing” - <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/user-id-concepts/user-mapping/client-probing>

13.30 2.3 Ensure that User-ID is only enabled for internal trusted interfaces

13.30.1 Scored/Not Scored

(Scored)

13.30.2 Profile Applicability

Level 1

13.30.3 Description

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

13.30.4 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.

13.30.5 Audit

Navigate to Network > Network Profiles > Interface Management.

Verify that User-ID is only enabled for interfaces that are both internal and trusted.

13.30.6 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.

13.30.7 Impact

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

13.30.8 Default Value

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

13.30.9 References

1. “Customer advisory: Security Impact of User-ID Misconfiguration” - <https://live.paloaltonetworks.com/docs/DOC-8125>
2. “R7-2014-16: Palo Alto Networks User-ID Credential Exposure” - <https://blog.rapid7.com/2014/10/14/palo-alto-networks-userid-credential-exposure/>
3. “Best Practices for Securing User-ID Deployments” - <https://live.paloaltonetworks.com/docs/DOC-7912>
4. “User-ID Best Practices” - <https://live.paloaltonetworks.com/docs/DOC-6591>
5. “PAN-OS Administrator’s Guide 9.0 (English) - Client Probing” - <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/user-id-concepts/user-mapping/client-probing>

13.31 2.4 Ensure that ‘Include/Exclude Networks’ is used if User-ID is enabled

13.31.1 Scored/Not Scored

(Scored)

13.31.2 Profile Applicability

Level 1

13.31.3 Description

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

13.31.4 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.

13.31.5 Audit

Navigate to Device > User Identification > User Mapping > Include/Exclude Networks.

Verify that all trusted internal networks have a Discovery value of Include.

Verify that all untrusted external networks have a Discovery value of Exclude.

Note that any value in the trusted networks list implies that all other networks are untrusted.

13.31.6 Remediation

Navigate to Device > User Identification > User Mapping > Include/Exclude Networks.

Set all trusted internal networks to have a Discovery value of Include.

Set all untrusted external networks to have a Discovery value of Exclude.

Note that any value in the trusted networks list implies that all other networks are untrusted.

13.31.7 Impact

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

13.31.8 Default Value

Not configured

13.31.9 References

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

13.32 2.5 Ensure that the User-ID Agent has minimal permissions if User-ID is enabled

13.32.1 Scored/Not Scored

(Scored)

13.32.2 Profile Applicability

Level 1

13.32.3 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.

13.32.4 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.

13.32.5 Audit

Navigate to Active Directory Users and Computers for the Active Directory under consideration.

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

13.32.6 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.)

13.32.7 Impact

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

13.32.8 Default Value

Not configured

13.32.9 References

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

13.33 2.6 Ensure that the User-ID service account does not have interactive logon rights

13.33.1 Scored/Not Scored

(Scored)

13.33.2 Profile Applicability

Level 1

13.33.3 Description

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

13.33.4 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.

13.33.5 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.

13.33.6 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.

13.33.7 Default Value

Not configured

13.33.8 References

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

13.34 2.7 Ensure remote access capabilities for the User-ID service account are forbidden.

13.34.1 Scored/Not Scored

(Not Scored)

13.34.2 Profile Applicability

Level 1

13.34.3 Description

Restrict the User-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 -ID service account to gain remote access.

13.34.4 Rationale

In the event of a compromised User-a service account compromise.

13.34.5 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.

13.34.6 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.

13.34.7 Default Value

Not configured

13.34.8 References

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

13.35 2.8 Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones

13.35.1 Scored/Not Scored

(Scored)

13.35.2 Profile Applicability

Level 1

13.35.3 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.

13.35.4 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.

13.35.5 Audit

Navigate to Device > Setup > Services > Services Features > Service Route Configuration > Customize.

Click on the protocol in use (IPv4 and/or IPv6). Click UID Agent.

Click on the address object for the UID Agent’s IP address.

Verify SOURCE/NAME is set to ‘Deny msrpc to untrusted’.

Verify SOURCE/ZONE is set to ‘INSIDE’.

Verify SOURCE/Address is set to the Address object for the UID Agent.

Verify DESTINATION/ZONE is set to 'GUEST' and 'OUTSIDE'.

Verify DESTINATION/Address is set to 'any'.

Verify DESTINATION/Application is set to 'msrpc'.

Verify DESTINATION/Service is set to 'application-default'.

Verify DESTINATION/Action is set to 'Block' (red circle with diagonal line).

13.35.6 Remediation

Navigate to Device > Setup > 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).

13.35.7 References

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

13.36 3.1 Ensure a fully-synchronized High Availability peer is configured

13.36.1 Scored/Not Scored

(Scored)

13.36.2 Profile Applicability

Level 1

13.36.3 Description

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

13.36.4 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

13.36.5 Audit

Navigate to Device > High Availability > General.

In the General. >Data Link (HA2) section, verify that the correct interface is selected.

Verify the desired protocol (IPv4 or IPv6) is selected.

Verify the correct Transport is selected.

Verify the Enable Session Synchronization box is checked.

13.36.6 Remediation

Navigate to Device > High Availability > General.

Click General. Click Data Link (HA2).

Select the correct interface.

Select the desired protocol (IPv4 or IPv6).

Select the correct Transport.

Set the Enable Session Synchronization box to be checked.

Choose Save Configuration.

13.36.7 Impact

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

13.36.8 Default Value

Not Configured

13.36.9 References

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

13.37 3.2 Ensure ‘High Availability’ requires Link Monitoring and/or Path Monitoring

13.37.1 Scored/Not Scored

(Scored)

13.37.2 Profile Applicability

Level 1

13.37.3 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.

13.37.4 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.

13.37.5 Audit

To verify Link Monitoring from GUI: Navigate to Device > High Availability > Link and Path Monitoring.

In the Link Monitoring section, verify the correct interfaces are in the Link Group and Group Failure Conditions

Under the Link Monitoring section, verify Failure Condition is set to Any.

Verify Enabled button is checked.

To verify Path Monitoring from GUI:

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

In the Path Monitoring section, verify Option is set correctly.

Verify Failure Condition is set to Any.

Verify Name, IP Address, Failure Condition is set correctly.

Verify Default setting is set to Any.

Verify Enabled button is checked.

13.37.6 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.

13.37.7 Impact

Not configuring High Availability (HA) correctly directly impacts the Availability of the system. With HA in place, standard maintenance such as OS updates, network and power cabling can be accomplished with no outage or a minimum impact. Without Link and Path monitoring in particular, failover will only occur when the primary device fails completely. Link and path monitoring permits failover if a critical interface loses link (either due to cabling or an upstream switch failover), or if a route or path fails (indicating an upstream issue that affects local Layer 3).

13.37.8 Default Value

Not Configured

13.37.9 References

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

13.38 3.3 Ensure ‘Passive Link State’ and ‘Preemptive’ are configured appropriately

13.38.1 Scored/Not Scored

(Scored)

13.38.2 Profile Applicability

Level 1

13.38.3 Description

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

13.38.4 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.

13.38.5 Audit

To ensure Active/Passive Settings are configured correctly:

Navigate to Device > High Availability > General > Active/Passive Settings.

Verify Passive Link State is set to auto.

To ensure Election Settings are configured correctly:

Navigate to Device > High Availability > Election Settings.

Verify Preemptive is disabled.

13.38.6 Remediation

To set Active/Passive Settings correctly:

Navigate to Device > High Availability > General > Active/Passive Settings.

Set Passive Link State to auto.

To set Election Settings correctly:

Navigate to Device > High Availability > Election Settings.

Set Preemptive to be disabled.

13.38.7 Impact

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

13.38.8 Default Value

Not Configured

13.38.9 References

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

13.39 4.1 Ensure ‘Antivirus Update Schedule’ is set to download and install updates hourly

13.39.1 Scored/Not Scored

(Scored)

13.39.2 Profile Applicability

Level 1

13.39.3 Description

Set Antivirus Update Schedule to download and install updates hourly.

13.39.4 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.

13.39.5 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.

13.39.6 Remediation

Navigate to Device > Dynamic Updates > Antivirus Update Schedule.

Set Action to Download and Install.

Set Recurrence to Hourly.

13.39.7 Default Value

Not Configured

13.39.8 References

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

13.40 4.2 Ensure ‘Applications and Threats Update Schedule’ is set to download and install updates at daily or shorter intervals

13.40.1 Scored/Not Scored

(Scored)

13.40.2 Profile Applicability

Level 1

13.40.3 Description

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

13.40.4 Rationale

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

13.40.5 Audit

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

13.40.6 Remediation

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

Set Action to Download and Install.

Set Recurrence to Daily, Hourly or Every 30 Minutes

13.40.7 Default Value

This setting is by default set to Weekly.

13.40.8 References

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

13.41 5.1 Ensure that WildFire file size upload limits are maximized

13.41.1 Scored/Not Scored

(Scored)

13.41.2 Profile Applicability

Level 1

13.41.3 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. The recommendations account for the CPU load on smaller platforms. If an organization consistently has CPU to spare, it’s recommended to set some or all of these values to the maximum.

13.41.4 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. The default values are configured for files small enough that the majority of files are not assessed by Wildfire.

13.41.5 Audit

Navigate to Device > Setup > WildFire.

Navigate to the General Settings sections.

Verify the maximum size for each file type are larger than the defaults, to a size that is as large enough to account for “large” files, but not large enough to affect performance of the hardware.

13.41.6 Remediation

Navigate to Device > Setup > WildFire.

Click the General Settings edit icon.

Set the maximum size for each file type are larger than the defaults, to a size that is as large enough to account for “large” files, but not large enough to affect performance of the hardware.

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

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

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

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

13.41.7 Impact

With the default values known, an attacker has only to send an infected file slightly over the “maximum” size for that filetype to evade detection at the perimeter. Many of the values are significantly lower than is typical for each file size.

13.41.8 Default Value

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

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

13.41.9 References

1. “Wildfire Administrator’s Guide 9.0 (English) - Increased Wildfire File Forwarding Capacity” - <https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/wildfire-features-in-panos-90/increased-wildfire-file-forwarding-capacity>
2. “How to Configure WildFire” - <https://live.paloaltonetworks.com/docs/DOC-3252>
3. “Wildfire Administrator’s Guide 9.0 (English) - Wildfire Best Practices” - <https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/wildfire-deployment-best-practices/wildfire-best-practices.html#>
4. “Wildfire Administrator’s Guide 9.0 (English) - Forward Files for Wildfire Analysis” - <https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/submit-files-for-wildfire-analysis/forward-files-for-wildfire-analysis.html#>

13.42 5.2 Ensure forwarding is enabled for all applications and file types in WildFire file blocking profiles

13.42.1 Scored/Not Scored

(Scored)

13.42.2 Profile Applicability

Level 1

13.42.3 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 the “web browsing” application, the action “continue” 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. Selecting “continue” for any other application will block the file (because the end user will not see the prompt). If there is a “continue” rule, there should still be an “any traffic / any application / forward” rule after that in the list.

13.42.4 Rationale

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

13.42.5 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.

13.42.6 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.

13.42.7 Default Value

Predefined Security Profiles exist for “basic” and “strict” File Blocking.

13.42.8 References

1. ““Wildfire Administrator’s Guide 9.0 (English) -WildFire Best Practices” - <https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/wildfire-deployment-best-practices/wildfire-best-practices.html#>

13.43 5.3 Ensure a WildFire Analysis profile is enabled for all security policies

13.43.1 Scored/Not Scored

(Scored)

13.43.2 Profile Applicability

Level 1

13.43.3 Description

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

13.43.4 Rationale

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

13.43.5 Audit

To verify WildFire Analysis Profile:

Navigate to Objects > Security Profiles > WildFire Analysis Profile

verify that a profile exists.

To verify File Blocking Rules:

For each Security Policy where the action is set to Allow, edit the Rule and navigate to Actions > Profile Setting.

Ensure that the WildFire Analysis is set to Allow and verify that a profile is set.

If Group Profiles are used: Navigate to Policies > Security

For each Security Policy where the action is set to Allow, edit the Rule and navigate to Actions > Profile Setting.

Ensure that the Profile Type is set to Group.

Navigate to Objects > Security Profile Groups.

Open the Security Profile Group used above, and ensure that the Wildfire Analysis Profile is set.

13.43.6 Remediation

To Set File Blocking Profile:

Navigate to Objects > Security Profiles > WildFire Analysis Profile.

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

To Set WildFire Analysis Rules:

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

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

Navigate to Objects > Security Profile Groups. Create a Security Profile Group, and ensure that (among other settings) the Wildfire Analysis Profile is set to the created profile.

Navigate to Policies > Security. For each Security Policy Rule where the action is “Allow”, Navigate to Actions > Profile Setting. Modify the Profile Type to Group, and set the Group Profile to the created Security Profile Group.

13.43.7 Default Value

Not Configured

13.43.8 References

1. “Wildfire Administrator’s Guide 9.0 (English)” - <https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin.html>

13.44 5.4 Ensure forwarding of decrypted content to WildFire is enabled

13.44.1 Scored/Not Scored

(Scored)

13.44.2 Profile Applicability

Level 1

13.44.3 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.

13.44.4 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.

13.44.5 Audit

Navigate to Device > Setup > Content-ID > Content-ID Settings.

Verify that Allow forwarding of decrypted content is checked.

13.44.6 Remediation

Navigate to Device > Setup > Content-ID > Content-ID Settings.

Set Allow forwarding of decrypted content to be checked.

Note that SSL Forward Proxy must be configured for this setting to be effective.

13.44.7 Default Value

Not Configured

13.44.8 References

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

13.45 5.5 Ensure all WildFire session information settings are enabled

13.45.1 Scored/Not Scored

(Scored)

13.45.2 Profile Applicability

Level 1

13.45.3 Description

Enable all options under Session Information Settings for WildFire.

13.45.4 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.

13.45.5 Audit

Navigate to Device > Setup > WildFire > Session Information Settings.

Verify that every option is enabled.

13.45.6 Remediation

Navigate to Device > Setup > WildFire > Session Information Settings.

Set every option to be enabled.

13.45.7 Default Value

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

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

13.45.8 References

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

13.46 5.6 Ensure alerts are enabled for malicious files detected by WildFire

13.46.1 Scored/Not Scored

(Scored)

13.46.2 Profile Applicability

Level 1

13.46.3 Description

Configure WildFire to send an alert when a malicious or greyware file is detected. This alert could be sent by whichever means is preferable, including email, SNMP trap, or syslog message. Alternatively, configure the WildFire cloud to generate alerts for malicious files. The cloud can generate alerts in addition to or instead of the local WildFire implementation. Note that the destination email address of alerts configured in the WildFire cloud portal is tied to the logged in account, and cannot be modified. Also, new systems added to the WildFire cloud portal will not be automatically set to email alerts.

13.46.4 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 fievade detection by desktop antivirus products.

13.46.5 Audit

Navigate to Objects > Log Forwarding.

Verify that the WildFire log type is configured to generate alerts using the desired alerting mechanism(s).

13.46.6 Remediation

From GUI, configure some combination of the following Server Profiles:

Configure the Email Server:

Select Device > Server Profiles > Email

Click Add Enter a name for the Profile. Select the virtual system from the Location drop down menu (if applicable)
Click Add

Configure the Syslog Server:

Select Device > Server Profiles > Syslog > Add Enter Name, Display Name, Syslog Server, Transport, Port, Format, Facility Click OK Click Commit to save the configuration

Configure the SMTP Server:

Select Device > Server Profiles > Email Select Add, Name, Display Name, From, To, Additional Recipients, Gateway IP or Hostname Click OK Click Commit to save the configuration

Navigate to Objects, Log Forwarding Choose Add, set the log type to “wildfire”, add the filter “(verdict neq benign)”, then add log destinations for SNMP, Syslog, Email or HTTP as required.

13.46.7 Default Value

Not Configured

13.46.8 References

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

13.47 5.7 Ensure ‘WildFire Update Schedule’ is set to download and install updates every minute

13.47.1 Scored/Not Scored

(Scored)

13.47.2 Profile Applicability

Level 1

13.47.3 Description

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

13.47.4 Rationale

WildFire definitions may contain signatures to block immediate, active threats to the environment. With a 1 minute update schedule, the firewall can ensure threats with new definitions are quickly mitigated.

13.47.5 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 Minute.

13.47.6 Remediation

Navigate to Device > Dynamic Updates > WildFire Update Schedule.

Set Action to Download and Install.

Set Recurrence to Every Minute.

13.47.7 Default Value

Not Configured

13.47.8 References

1. “Wildfire Administrator’s Guide 9.0 (English)” - <https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin.html>
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>

13.48 6.1 Ensure that antivirus profiles are set to block on all decoders except ‘imap’ and ‘pop3’

13.48.1 Scored/Not Scored

(Scored)

13.48.2 Profile Applicability

Level 1

13.48.3 Description

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

13.48.4 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.

13.48.5 Audit

Navigate to Objects > Security Profiles > Antivirus

Verify that antivirus profiles have all decoders set to block for both Action and Wildfire Action.

If imap and pop3 are required in the organization, verify that the imap and pop3 decoders are set to alert for both Action and Wildfire Action.

13.48.6 Remediation

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

13.48.7 Default Value

Not Configured

13.48.8 References

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

13.49 6.2 Ensure a secure antivirus profile is applied to all relevant security policies

13.49.1 Scored/Not Scored

(Scored)

13.49.2 Profile Applicability

Level 1

13.49.3 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.

13.49.4 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.

13.49.5 Audit

Navigate to Policies > Security. For each policy, navigate to [Policy Name] > Actions

Verify there is a secure Antivirus profile applied to all security policies passing traffic - regardless of protocol. This can be set by Profiles or by Profile Group.

13.49.6 Remediation

Navigate to Policies > Security.

For each policy, navigate to [Policy Name] > Actions

Set an Antivirus profile or a Profile Group containing an AV profile for each security policy passing traffic - regardless of protocol.

13.49.7 Impact

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

13.49.8 Default Value

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

13.49.9 References

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

13.50 6.3 Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats

13.50.1 Scored/Not Scored

(Scored)

13.50.2 Profile Applicability

Level 1

13.50.3 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.

13.50.4 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.

13.50.5 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.

13.50.6 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.

13.50.7 Default Value

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

13.50.8 References

1. “PAN-OS Administrator’s Guide 9.0 (English) - Security Profiles”: <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-policy.html>

13.51 6.4 Ensure DNS sinkholing is configured on all anti-spyware profiles in use

13.51.1 Scored/Not Scored

(Scored)

13.51.2 Profile Applicability

Level 1

13.51.3 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.

13.51.4 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.

13.51.5 Audit

Navigate to Objects > Security Profiles > Anti-Spyware.

Within the each anti-spyware profile, under its DNS Signatures tab, verify the DNS Signature Source List:

Palo Alto Networks Content DNS Signatures should have as its Action on DNS Queries set to sinkhole

If licensed, the Palo Alto Networks Cloud DNS Security should have as its Action on DNS Queries set to sinkhole

Verify the ‘Sinkhole IPv4’ IP address is correct. This should be set to sinkhole.paloaltnetworks.com, or if an internal host is set then that host IP or FQDN should be in that field Verify the ‘Sinkhole IPv6’ IP address is correct. This should be set to IPv6 Loopback IP (::1), or if an internal DNS Sinkhole host is set then that host IP or FQDN should be in that field

Navigate to Policies > Security Policies

For each outbound security Policy, in the Actions tab, verify that the Anti-Spyware setting includes the Spyware Profile created, either explicitly or as a Group Profile

To verify correct operation of DNS Security, from an internal station make a DNS request to each of the following hosts:

test-malware.testpanw.com to test Malware DNS Signature checks

test-c2.testpanw.com to test C2 DNS Signature checks

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

test-dnstun.testpanw.com to test DNS Tunneling attack checks

Each of these DNS requests should be redirected to the configured DNS Sinkhole server IP address. Each of these DNS requests should appear in the firewall logs, under Monitor > Logs > Threat. If configured, each of these requests should generate an alert in the organization's SIEM.

13.51.6 Remediation

Navigate to Objects > Security Profiles > Anti-Spyware.

Within each anti-spyware profile, under its DNS Signatures tab, set the DNS Signature Source List: Palo Alto Networks Content DNS Signatures should have as its Action on DNS Queries set to sinkhole.

If licensed, the Palo Alto Networks Cloud DNS Security should have as its Action on DNS Queries set to sinkhole. Verify the 'Sinkhole IPv4' IP address is correct. This should be set to sinkhole.paloaltonetworks.com, or if an internal host is set then that host IP or FQDN should be in that field.

Verify the 'Sinkhole IPv6' IP address is correct. This should be set to IPv6 Loopback IP (::1), or if an internal DNS Sinkhole host is set then that host IP or FQDN should be in that field. Navigate to Policies > Security Policies. For each outbound security Policy, in the Actions tab, set the Anti-Spyware setting to include the Spyware Profile created, either explicitly or as a Group Profile.

13.51.7 Default Value

Not Configured

13.51.8 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. "PANOS Administrator's Guide 9.0 (English) - Security Profiles": <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles.html>
4. "PAN-OS Administrator's Guide 9.0 (English) - DNS Security" - <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/dns-security.html#>

13.52 6.5 Ensure passive DNS monitoring is set to enabled on all anti-spyware profiles in use

13.52.1 Scored/Not Scored

(Scored)

13.52.2 Profile Applicability

Level 1

13.52.3 Description

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

13.52.4 Rationale

Rationale: and threat intelligence capabilities. This is performed without source information delivered to PAN to ensure sensitive DNS information of the organization is not compromised.

13.52.5 Audit

Navigate to Device > Setup > Telemetry.

Ensure that Passive DNS Monitoring is enabled

13.52.6 Remediation

Navigate to Device > Setup > Telemetry.

Set Passive DNS Monitoring to enabled

13.52.7 Default Value

Not Configured

13.52.8 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 9.0 (English) - DNS Security” - <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/dns-security.html#>

13.53 6.6 Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the Internet

13.53.1 Scored/Not Scored

(Scored)

13.53.2 Profile Applicability

Level 1

13.53.3 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.

13.53.4 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.

13.53.5 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.

13.53.6 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.

13.53.7 Default Value

Not Configured

13.53.8 References

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

13.54 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

13.54.1 Scored/Not Scored

(Scored)

13.54.2 Profile Applicability

Level 1

13.54.3 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.

13.54.4 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.

13.54.5 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.

13.54.6 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.

13.54.7 Impact

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

13.54.8 Default Value

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

13.54.9 References

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

13.55 6.8 Ensure a secure Vulnerability Protection Profile is applied to all security rules allowing traffic

13.55.1 Scored/Not Scored

(Scored)

13.55.2 Profile Applicability

Level 1

13.55.3 Description

For any security rule allowing traffic, apply a securely configured Vulnerability Protection Profile. Careful analysis of the target environment should be performed before cition.

13.55.4 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.

13.55.5 Audit

Navigate to Policies > Security.

For each Policy, under the Actions tab, select Vulnerability Protection.

Verify either the ‘Strict’ or the ‘Default’ profile is selected, or a custom profile that complies with the organization’s policies, legal and regulatory requirements.

13.55.6 Remediation

Navigate to Policies > Security.

For each Policy, under the Actions tab, select Vulnerability Protection.

Set it to use either the 'Strict' or the 'Default' profile, or a custom profile that complies with the organization's policies, legal and regulatory requirements.

13.55.7 Impact

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

13.55.8 Default Value

Not Configured

13.55.9 References

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

13.56 6.9 Ensure that PAN-DB URL Filtering is used

13.56.1 Scored/Not Scored

(Scored)

13.56.2 Profile Applicability

Level 1

13.56.3 Description

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

13.56.4 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”.

13.56.5 Audit

Navigate to Device > Licenses.

Click on PAN-DB URL Filtering. Verify Active is set to Yes.

13.56.6 Remediation

Navigate to Device > Licenses.

Click on PAN-DB URL Filtering. Set Active to Yes.

13.56.7 Impact

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

13.56.8 Default Value

Not Configured

13.56.9 References

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

13.57 6.10 Ensure that URL Filtering uses the action of “block” or “override” on the URL categories

13.57.1 Scored/Not Scored

(Scored)

13.57.2 Profile Applicability

Level 1

13.57.3 Description

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

13.57.4 Rationale

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

13.57.5 Audit

Navigate to Objects > Security Profiles > URL Filtering.

Verify that all URL categories designated by the organization are listed, and the action is set to Block.

13.57.6 Remediation

Navigate to Objects > Security Profiles > URL Filtering.

Set a URL filter so that all URL categories designated by the organization are listed.

Navigate to the Actions tab. Set the action to Block.

13.57.7 Impact

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

13.57.8 Default Value

Not Configured

13.57.9 References

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

13.58 6.11 Ensure that access to every URL is logged

13.58.1 Scored/Not Scored

(Scored)

13.58.2 Profile Applicability

Level 1

13.58.3 Description

URL filters should not specify any categories as Allow Categories.

13.58.4 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.

13.58.5 Audit

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

13.58.6 Remediation

Navigate to Objects > Security Profiles > URL Filtering.

For each permitted category, set the Site Access action to alert

13.58.7 Impact

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

13.58.8 Default Value

A default URL Filtering Security Profile is configured, with the following categories set to “block”:

- abused-drugs
- adult
- gambling
- hacking
- malware
- phishing
- questionable
- weapons

3 Categories are set to alert in the default policy, and 58 Categories are set to allow (which means they are not logged)

13.58.9 References

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

13.59 6.12 Ensure all HTTP Header Logging options are enabled

13.59.1 Scored/Not Scored

(Scored)

13.59.2 Profile Applicability

Level 1

13.59.3 Description

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

13.59.4 Rationale

Logging HTTP header information provides additional information in the URL logs, which may be useful during forensic investigations. The User-Agent option logs which browser was used during the web session, which could provide insight to the vector used for malware retrieval. The Referrer option logs the source webpage responsible for referring the user to the logged webpage. The X-Forwarded-For option is useful for preserving the -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.

13.59.5 Audit

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

Verify these four settings:

- a. Log container page only box is un-checked
- b. User-Agent box is checked
- c. Referrer box is checked
- d. X-Forwarded-For box is checked

13.59.6 Remediation

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

Set the following four settings:

- a. Log container page only box is un-checked
- b. Check the User-Agent box
- c. Check the Referrer box
- d. Check the X-Forwarded-For box

13.59.7 Impact

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

13.59.8 Default Value

Not Configured

13.59.9 References

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

13.60 6.13 Ensure secure URL filtering is enabled for all security policies allowing traffic to the Internet

13.60.1 Scored/Not Scored

(Scored)

13.60.2 Profile Applicability

Level 1

13.60.3 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.

13.60.4 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.

13.60.5 Audit

To Verify URL Filtering:

For each Security Policy that transits traffic to the public internet, navigate to Policies > Security > Security Profiles > [Policy Name] > Actions.

Verify there is a URL Filtering profile that complies with the policies of the organization is applied to all Security Policies that transit traffic to the public internet.

13.60.6 Remediation

To Set URL Filtering:

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

13.60.7 Impact

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

13.60.8 Default Value

Not Configured

13.60.9 References

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

13.61 6.14 Ensure alerting after a threshold of credit card or Social Security numbers is detected is enabled

13.61.1 Scored/Not Scored

(Scored)

13.61.2 Profile Applicability

Level 1

13.61.3 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.

13.61.4 Rationale

Credit card and Social Security numbers are sensitive, and should never traverse 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.

13.61.5 Audit

Navigate to Objects > Security Objects > Data Patterns.

Verify an appropriate Data Pattern has been created that accounts for sensitive information within your organization. In most cases this will include Credit Card Numbers, and your jurisdiction's equivalent of Social Insurance Numbers. In many cases these can simply be picked from the list of Predefined Patterns.

Navigate to Objects > Security Profiles > Data Filtering.

Verify an appropriate Data Filtering Profile has been created, using the created Data Patterns.

Ensure that an Alert Threshold is set that generates alerts appropriately. A typical starting value for Alert Threshold is 20, but this should be adjusted after appropriate testing.

13.61.6 Remediation

Navigate to Objects > Security Objects > Data Patterns.

Create an appropriate Data Pattern that accounts for sensitive information within your organization. In most cases this will include Credit Card Numbers, and your jurisdiction's equivalent of Social Insurance Numbers. In many cases these can simply be picked from the list of Predefined Patterns.

Navigate to Objects > Security Profiles > Data Filtering.

Create appropriate Data Filtering Profile, using the created Data Patterns. Ensure that an Alert Threshold is set that generates alerts appropriately. A typical starting value for Alert Threshold is 20, but this should be adjusted after appropriate testing.

13.61.7 Default Value

Not Configured

13.61.8 References

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

13.62 6.15 Ensure a secure Data Filtering profile is applied to all security policies allowing traffic to or from the Internet

13.62.1 Scored/Not Scored

(Scored)

13.62.2 Profile Applicability

Level 1

13.62.3 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.

13.62.4 Rationale

A Data Filtering profile helps prevent certain types of sensitive information from traversing known sensitive information is a basic protection against a data breach or data loss. Not implementing these defenses can lead to loss of regulatory accreditation (such as PCI, HIPAA etc.), or can lead to legal action from injured parties or regulatory bodies. Before starting, be very aware that Data Filtering will often block data that you didn't anticipate, false positives will definitely occur. Even the prebuilt filters will frequently match on unintended data in files or websites. Work very closely with your user community to ensure that required data is blocked or alerted on, but a minimum of false positive blocks occur. As false positives occur, ensure that your user community has a clear and timely procedure to get the configuration updated.

13.62.5 Audit

Navigate to Objects > Custom Objects > Data Patterns.

Verify that the patterns defined match the various data that you wish to monitor or make blocking decisions on.

Navigate to Objects > Security Profiles > Data Filtering

For each Filtering Profile, verify that the Data Patterns defined matches the data you wish to monitor, with appropriate values for Alert Threshold (typically 20), Block Threshold (typically 0) and Log Severity.

Finally, navigate to Policies > Security.

Open all appropriate policies, for each Policy choose the Actions tab, and verify that the appropriate Data Filtering Policy is applied (either as an individual Profile or as part of a Group Profile)

13.62.6 Remediation

Navigate to Objects > Custom Objects > Data Patterns.

Add patterns to match the various data that you wish to monitor or make blocking decisions on.

Navigate to Objects > Security Profiles > Data Filtering

Add a Filtering Profile that matches the data you wish to monitor, with appropriate values for Alert Threshold (typically 20), Block Threshold (typically 0) and Log Severity Finally, apply the Filtering Profile to a Security Profile.

Navigate to Policies > Security.

Edit all appropriate policies, and for each Policy choose the Actions tab, and add the appropriate Data Filtering Policy (either as an individual Profile or as part of a Group Profile)

13.62.7 Default Value

Not Configured

13.62.8 References

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

13.63 6.16 Ensure that a Zone Protection Profile with an enabled SYN Flood Action of SYN Cookies is attached to all untrusted zones

13.63.1 Scored/Not Scored

(Scored)

13.63.2 Profile Applicability

Level 1

13.63.3 Description

Enable the SYN Flood Action of SYN Cookies for all untrusted zones. The Alert, Activate, and Maximum settings for SYN Flood Protection depend highly on the environment and device used. Perform traffic analysis on the specific environment and firewall to determine accurate thresholds. Do not rely on default values to be appropriate for an environment. Setting these values for all interfaces is an approach that should be considered by many organizations, as traffic floods can result from internal testing or malware as well. 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

13.63.4 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.

13.63.5 Audit

From GUI:

Navigate to Network > Network Profiles > Zone Protection > Zone Protection Profile > Flood Protection tab.

Verify the SYN box is checked.

Verify the Action dropdown is SYN Cookies.

Verify Alert is 20000(or appropriate for org).

Verify Activate is 25000(50% of maximum for firewall model).

Verify Maximum is 1000000(or appropriate for org).

Navigate to Network > Zones >.

Open the zone facing any untrusted network.

Verify that Zone Protection has the Zone Protection Profile set to the Profile created.

13.63.6 Remediation

From GUI:

Navigate to Network > Network Profiles > Zone Protection > Zone Protection Profile > Flood Protection tab.

Check the SYN box.

Set the Action dropdown to SYN Cookies

Set Alert to 20000(or appropriate for org).

Set Activate to 25000(50% of maximum for firewall model).

Set Maximum to 1000000(or appropriate for org)

Navigate to Network > Zones >.

Open the zone facing any untrusted network, if one does not exist create it.

Set Zone Protection to the Zone Protection Profile created.

13.63.7 Impact

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

13.63.8 Default Value

Not Configured

13.63.9 References

1. “Understanding DoS Protection” - <https://live.paloaltonetworks.com/docs/DOC-5078>
2. “Syn Cookie Operation” - <https://live.paloaltonetworks.com/docs/DOC-1542>
3. “How to Determine if Configured DoS Classify TCP SYN Cookie Alarm, Activate and Maximal Rate is Triggered” - <https://live.paloaltonetworks.com/docs/DOC-6801>
4. “Threat Prevention Deployment Tech Note” - <https://live.paloaltonetworks.com/docs/DOC-3094>
5. “What are the Differences between DoS Protection and Zone Protection?” - <https://live.paloaltonetworks.com/docs/DOC-4501>
6. “Application DDoS Mitigation” - <https://live.paloaltonetworks.com/docs/DOC-7158>
7. PANOS 9.0 Admin Guide - Zone Protection . Flood Protection: <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-zone-protection/flood-protection.html#>

13.64 6.17 Ensure that a Zone Protection Profile with tuned Flood Protection settings enabled for all flood types is attached to all untrusted zones

13.64.1 Scored/Not Scored

(Scored)

13.64.2 Profile Applicability

Level 2

13.64.3 Description

Enable all Flood Protection options in the Zone Protection Profile attached to all untrusted zones. The Alert, Activate, and Maximum settings for Flood Protection depend highly on the environment and device used. Perform traffic analysis on the specific environment and firewall to determine accurate thresholds. Do not rely on default values to be appropriate for an environment. Setting these values for all interfaces is an approach that should be considered by many organizations, as traffic floods can result from internal testing or malware as well.

13.64.4 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).

13.64.5 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.

13.64.6 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.

13.64.7 Impact

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

13.64.8 Default Value

Not Configured

13.64.9 References

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

13.65 6.18 Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned, and set to appropriate actions

13.65.1 Scored/Not Scored

(Scored)

13.65.2 Profile Applicability

Level 1

13.65.3 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.

13.65.4 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.

13.65.5 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.

13.65.6 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.

13.65.7 Impact

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

13.65.8 Default Value

Not Configured

13.65.9 References

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

13.66 6.19 Ensure all zones have Zone Protection Profiles that drop specially crafted packets

13.66.1 Scored/Not Scored

(Scored)

13.66.2 Profile Applicability

Level 1

13.66.3 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.

13.66.4 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.

13.66.5 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.

13.66.6 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.

13.66.7 Impact

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

13.66.8 Default Value

Not Configured

13.66.9 References

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

13.67 6.20 Ensure that User Credential Submission uses the action of “block” or “continue” on the URL categories

13.67.1 Scored/Not Scored

(Scored)

13.67.2 Profile Applicability

Level 1

13.67.3 Description

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

13.67.4 Rationale

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

13.67.5 Audit

Navigate to Objects > Security Profiles > URL Filtering.

Choose the Categories tab. Verify that the User Credential Submitting action on all enabled URL categories is set to either block or continue.

Under the User Credential Detection tab ensure the User Credential Detection is set to a value appropriate to your organization, and is not set to Disabled.

Verify that the Log Severity value is set to a value appropriate to your organization and your logging or SIEM solution.

13.67.6 Remediation

Navigate to Objects > Security Profiles > URL Filtering.

Choose the Categories tab. Set the User Credential Submitting action on all enabled URL categories is either block or continue, as appropriate to your organization and the category.

Under the User Credential Detection tab set the User Credential Detection value to a setting appropriate to your organization, any value except Disabled. Set the Log Severity to a value appropriate to your organization and your logging or SIEM solution.

13.67.7 Impact

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

13.67.8 Default Value

Not Configured

13.67.9 References

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

13.68 7.1 Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone

13.68.1 Scored/Not Scored

(Scored)

13.68.2 Profile Applicability

Level 1 Level 2

13.68.3 Description

When permitting traffic from an untrusted zone, such as the Internet or guest network, to a more trusted zone, such as a DMZ segment, create security policies specifying which specific applications are allowed. ****Enhanced Security Recommendation:** ** Require specific application policies when allowing any traffic, regardless of the trust level of a zone. Do not rely solely on port permissions. This may require SSL interception, and may also not be possible in all environments.

13.68.4 Rationale

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

13.68.5 Audit

Navigate to Policies > Security.

For all Security Policies that transit from a less trusted to a more trusted interface, that the appropriate Application and Service values are set.

For instance, for a web server exposed to the internet from a DMZ:

Source tab: Zone set to OUTSIDE / Address set to Any

Destination tab: Zone set to DMZ / Address set to [DMZ Host Object]

Application tab: set to web-browsing

Service/URL Category tab: set Service to ether:

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

****Enhanced Security Recommendation:** **

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

13.68.6 Remediation

Navigate to Policies > Security.

For all Security Policies that transit from a less trusted to a more trusted interface, set the Application and Service values to match the exposed application. For instance, for a web server exposed to the internet from a DMZ:

Source tab: Zone set to OUTSIDE / Address set to Any

Destination tab: Zone set to DMZ / Address set to [DMZ Host Object]

Application tab: set to web-browsing

Service/URL Category tab: set Service to ether:

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

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

13.68.7 Impact

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

13.68.8 Default Value

Not Configured

13.68.9 References

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

13.69 7.2 Ensure ‘Service setting of ANY’ in a security policy allowing traffic does not exist

13.69.1 Scored/Not Scored

(Scored)

13.69.2 Profile Applicability

Level 1

13.69.3 Description

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

13.69.4 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.

13.69.5 Audit

Navigate to Policies > Security.

For each exposed host, verify that a Security Policy exists with:

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

13.69.6 Remediation

Remediation:

Navigate to Policies > Security.

For each exposed host, set a Security Policy exists with:

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

13.69.7 Default Value

Not Configured

13.69.8 References

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

13.70 7.3 Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists

13.70.1 Scored/Not Scored

(Scored)

13.70.2 Profile Applicability

Level 1

13.70.3 Description

Create a pair of security rules at the top of the security policies ruleset to block traffic to and from IP addresses known to be malicious. Note: This recommendation (as written) requires a Palo Alto "Active Threat License". Third Party and Open Source Threat Intelligence Feeds can also be used for this purpose.

13.70.4 Rationale

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

13.70.5 Audit

Navigate to Policies > Security

Verify a Security Policy exists similar to:

- General tab: Name set to Deny to Malicious IP
- Source tab: Source Zone set to Any,
- Destination tab: Destination Zone set to Any,
- Destination Address set to Palo Alto Networks - Known malicious IP addresses
- Application tab: Application set to Any
- Service/URL Category tab: Service set to Any
- Actions tab: Action set to Block, Profile Type set to None
- Verify a Security Policy exists with:
 - General tab: Name set to Deny from Malicious IP
 - Source tab: Source Zone set to Any, Source Address set to Palo Alto Networks - Known malicious IP addresses
 - Destination tab: Destination Zone set to Any
 - Application tab: Application set to Any
 - Service/URL Category tab: Service set to Any
 - Actions tab: Action set to Block, Profile Type set to None

Note: This recommendation requires a Palo Alto “Active Threat License”

13.70.6 Remediation

Navigate to Policies > Security

Create a Security Policy similar to:

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

Create a Security Policy similar to with:

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

This recommendation requires a Palo Alto “Active Threat License”

13.70.7 Impact

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

13.70.8 Default Value

Not Configured

13.70.9 References

1. “PAN-OS 9.0 Admin Guide: Built-in External Dynamic Lists”: <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/built-in-edls.html#>
2. “PAN-OS 9.0 Admin Guide: Create Rules Based on Trusted Threat Intelligence Sources”: <https://docs.paloaltonetworks.com/best-practices/9-0/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/define-the-initial-internet-gateway-security-policy/step-1-create-rules-based-on-trusted-threat-intelligence-sources.html#>

13.71 8.1 Ensure 'SSL Forward Proxy Policy' for traffic destined to the Internet is configured

13.71.1 Scored/Not Scored

(Scored)

13.71.2 Profile Applicability

Level 1

13.71.3 Description

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

13.71.4 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.

13.71.5 Audit

Navigate to Policies > Decryption.

Verify SSL Forward Proxy is set for all traffic destined to the Internet.

Verify each Decryption Policy Rule:

Source tab:

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

Destination tab:

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

Service/URL Category tab:

- Verify that all URL Category entries are included except financial-services, government and health-and-medicine (this list may vary depending on your organization and its policies).

Options tab:

- Verify that the Type is set to SSL Forward Proxy

13.71.6 Remediation

Navigate to Policies > Decryption. Create a Policy for all traffic destined to the Internet.

This Policy should include:

Source tab:

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

Destination tab:

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

Service/URL Category tab:

- all URL Category entries should be included except financial-services, government and
- health-and-medicine (this list may vary depending on your organization and its policies).

Options tab:

- Type set to SSL Forward Proxy

13.71.7 Impact

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

13.71.8 Default Value

Not Configured

13.71.9 References

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

13.72 8.2 Ensure 'SSL Inbound Inspection' is required for all untrusted traffic destined for servers using SSL or TLS

13.72.1 Scored/Not Scored

(Scored)

13.72.2 Profile Applicability

Level 1

13.72.3 Description

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

13.72.4 Rationale

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

13.72.5 Audit

Navigate to Policies > Decryption.

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

Navigate to Policies > Decryption.

For each service published to the internet (or other untrusted zones), verify the following settings:

General tab: Name set to a descriptive name

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

Destination tab: Destination Zone should be set to the appropriate zone, or Any. Destination Address set to the target host address Options tab: Type set to SSL Inbound Inspection

13.72.6 Remediation

Navigate to Policies > Decryption.

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

Navigate to Policies > Decryption.

For each service published to the internet (or other untrusted zones), create a Policy and set the following options:

General tab: Name set to a descriptive name

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

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

Options tab: Type set to SSL Inbound Inspection

13.72.7 Impact

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

13.72.8 Default Value

Not Configured

13.72.9 References

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

13.73 8.3 Ensure that the Certificate used for Decryption is Trusted

13.73.1 Scored/Not Scored

(Not Scored)

13.73.2 Profile Applicability

Level 1 Level 2

13.73.3 Description

The CA Certificate used for in-line HTTP Man in the Middle should be trusted by target users. For SSL Forward Proxy configurations, there are classes of users that need to be considered. 1: Users that are members of the organization, users of machines under control of the organization. For these people and machines, ensure that the CA Certificate is in one of the Trusted CA certificate stores. This is easily done in Active Directory, using Group Policies for instance. 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 the hosting organization. In this last case, visitors will see a certificate warning, but the issuing CA will be the organization that they are visiting.

13.73.4 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.

13.73.5 Audit

Verify the CA Certificate(s):

Navigate to Device > Certificate Management > Certificates

Verify that appropriate internal certificates are imported, and that all certificates in the list are valid. In particular, verify the Subject, Issuer, CA, Expires, Algorithm and Usage fields. Alternatively, if an internal CA is implemented on the firewall, verify that target clients have the root certificate for this CA imported into their list of trusted certificate authorities.

Verify the Certificate Profile needed for the SSL Forward Proxy:

Navigate to Device > Certificate Management > Certificate Profile.

Verify that an appropriate profile is created.

13.73.6 Remediation

Set the CA Certificate(s): Navigate to Device > Certificate Management > Certificates.

Import the appropriate CA Certificates from any internal Certificate Authorities.

Alternatively, generate a self-signed certificate for an internal CA on the firewall, and then import the root certificate for that CA into the trusted CA list of target clients. In an Active Directory environment this can be facilitated using a Group Policy.

Set the Certificate Profile needed for the SSL Forward Proxy:

Navigate to Device > Certificate Management > Certificate Profile.

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

13.73.7 Default Value

Decryption is not enabled by default.

13.73.8 References

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

NEW PAN-OS VERSION UPDATES

14.1 11.0 new features

14.1.1 Security profiles

- URL Filtering: Added “ransomware” and “encrypted-dns” categories with recommended enforcement settings
- Vulnerability Protection: Enabled Cloud Inline Analysis
- Vulnerability Protection: Enabled and Configured “SQL Injection” and “Command Injection” categories with recommended settings

14.2 10.2 new features

14.2.1 Security profiles

- URL Filtering: Enable Cloud and Local Inline Categorizations
- URL Filtering: Enable HTTP Header Logging options, User-Agent, Referer, X-Forwarded-For
- Antivirus: Enable MsOffice and Shell analysis settings
- External Dynamic Lists: Added Bulletproof and Tor Exit IP address EDLs
- Zone Protection Profile: Added Alert Only ZPP

14.2.2 Device configuration

- Disabled reporting of benign files

14.3 10.1 new features

14.3.1 Security profiles

- Anti-spyware profile: New DNS Security Service malicious categories set to sinkhole
- URL Filtering: Set new real-time url category to alert

14.3.2 Device configuration

- packet buffer protection: set to allow (default)

14.4 10.0 new features

14.4.1 Security profiles

- Antivirus profile: Wildfire ML dynamic classification to block all malicious file types
 - set all decoders to reset-both
 - set all file types to enabled
- Anti-spyware profile: DNS Security Service malicious categories set to sinkhole
- URL Filtering: realtime page analysis; block all engines types under Dynamic Classification

14.4.2 Device configuration

- dynamic updates: set Wildfire schedule to 'realtime'

14.4.3 Decryption profile

- set protocol max version to TLSv1.3

14.4.4 Log Setting

- GlobalProtect log forwarding

9.0 Update Items

This includes changes from the 8.1 IronSkillet configurations

14.5 Syntax changes

- move packet cap xml element in spyware profile
- remove url 'block' stand-alone entry
- custom url categories
 - add 'type' value to allow config to commit
- sinkhole IPv4 address uses FQDN instead of IP value

14.6 9.0 new features

14.6.1 Security profiles

- new url categories (risk, new domain)
 - set new categories to alert
 - over time move to custom dual category blocks (eg. parked + high)
- new pan cloud dns option in spyware profile
 - action = sinkhole with single packet capture
- AV profile and http2
 - set http2 decoder same as http for each profile

14.6.2 Device settings

- API key lifetime
 - Initially set to a high value with configuration variable
 - Default in minutes -> 525,600 is 1 year

14.7 9.1 new features

14.7.1 Security profiles

- new url categories (grayware, cryptocurrency)
 - set grayware to block
 - set cryptocurrency to alert

Note: these are shown with their initial 9.1 release but also supported in prior PAN-OS releases

8.1 Update Items

This includes changes from the 8.0 IronSkillet configurations

14.8 Syntax changes

- `allow-http-range` in device settings

14.9 8.1 new features

- WF file sizes
 - new file type script, set to max 2000 file size [available in later releases]

RELEASE AND UPDATE HISTORY

Includes:

- template releases
- tools updates
- documentation revisions

15.1 11.0 Template Release History

Template content updates are high level. Details can be found in the template guides.

15.1.1 0.0.1

Released December 27th, 2022

- Update Vulnerability Protection Profiles to include Inline Cloud Analysis for Advanced Threat Prevention
- Added and configured “SQL Injection” and “Command Injection” to Vulnerability Protection Profiles
- Added new Advanced URL categories “ransomware” and “encrypted-dns”
- Fixed Panorama duplicate template stack “sample_stack” entry error

15.2 10.2 Template Release History

Template content updates are high level. Details can be found in the template guides.

15.2.1 0.0.2

Released February 15th, 2023

- Updated AS profiles to enable cloud inline analysis
- Set all cloud inline analysis engine models with the respective best-practice actions for each AS profile

15.2.2 0.0.1

Released March 30th, 2022

- Update AV profiles to include inline ML MsOffice and Shell analysis support settings
- Enabled cloud-delivered Advanced Threat Protection for URL Filtering profiles
- Added Tor Exit and Bulletproof IP addresses External Dynamic Lists
- Disabled Wildfire reporting of benign files
- Added an Alert Only Zone Protection profile
- Removed all Exception Profiles

15.3 10.1 Template Release History

Template content updates are high level. Details can be found in the template guides.

15.3.1 0.0.2

Released June 30th, 2021

- Update Alert-Only-AV profile to have ELF file detection and prevention set to Alert-Only
- Update all other AV profiles to have ELF file detection and prevention set to Enable

15.3.2 0.0.1

Released June 10th, 2021

- URL filtering profiles: Updating real-time-detection category in the following URL Filtering profiles, Outbound-URL, Alert-Only-URL and Exception-URL
- URL filtering profiles: set real-time-detection to alert
- Anti-Spyware profiles: Updating the following DNS policies, Phishing Domains, Grayware Domains and proxy Avoidance and Anonymizers within the following anti-spyware profiles Outbound-AS, Inbound-AS and Internal-AS
- Anti-Spyware profiles: set DNS policies to sinkhole/single-packet
- Anti-Spyware profiles: Updating all DNS policies within Alert-Only-AS anti-spyware profile to allow/single-packet except for Parked Domains
- Anti-Spyware profiles: set DNS policies to allow/single-packet
- Allow packet buffer protection
- Allow forwarding of decrypted content

15.4 10.0 Template Release History

Template content updates are high level. Details can be found in the template guides.

15.4.1 0.0.3

Released June 30th, 2021

- Update Alert-Only-AV profile to have ELF file detection and prevention set to Alert-Only
- Update all other AV profiles to have ELF file detection and prevention set to Enable

15.4.2 0.0.2

Released June 17th, 2021

- URL filtering profiles: Updating real-time-detection category in the following URL Filtering profiles, Outbound-URL, Alert-Only-URL and Exception-URL
- Added playlists directory and IronSkillet Components Submodules
- Update IronSkillet Submodules repo with real-time-detection category

15.4.3 0.0.1

Released July 21, 2020

- set Wildfire dynamic updates to realtime
- Antivirus profile: reset-both for dynamic classification, all file types enabled
- Anti-spyware profile: set DNS malicious categories to sinkhole
- set max version of TLSv1.3 in the decryption profile
- URL filtering profile: use ML analysis and set to dynamic classification to block
- URL filtering profile: move 'hacking' category to alert since not malicious
- remove sinkhole address block policy and associated address object
- remove http partial response so now allowed
- remove XFF global configuration; now profile or policy specific
- remove 'no decrypt' decryption policy that checks for expired/invalid certs; too strict
- update WF malicious reports using 'neq benign' instead of equal to malicious categories
- remove telemetry configuration; new opt-in cert-based model in 10.0
- add email profile protocol 'SMTP' required in configuration; TLS config is optional
- add GlobalProtect log forwarding in log settings
- update validation skillets based on above modifications
- update metadata file for XML snippet skillets w/ option to skip IP address/admin user/DNS configuration elements
- add helper commands for scripting-mode on for CLI copy-paste model

- converted customer URL-filtering profile lingo from White-List/Black-List to Allow/Block
- fixed Panorama set commands: include type “URL-List”
- fix internal spyware XML snippets with medium severity as default

15.5 9.1 Template Release History

Template content updates are high level. Details can be found in the template guides.

15.5.1 0.0.3

Released September 16, 2020

- URL filtering profile: move ‘hacking’ category to alert since not malicious
- remove sinkhole address block policy and associated address object
- remove http partial response so now allowed
- remove ‘no decrypt’ decryption policy that checks for expired/invalid certs; too strict
- update WF malicious reports using ‘neq benign’ instead of equal to malicious categories
- update validation skilletts based on above modifications
- update metadata file for XML snippet skilletts w/ option to skip IP address/admin user/DNS configuration elements
- converted customer URL-filtering profile lingo from White-List/Black-List to Allow/Block

15.5.2 0.0.2

Released April 28, 2020

- Update WF file size limits to match the BPA
- validation updates including grayware check and WF file size limits
- metadata file updates: variable clean up with toggle_hint and help_text
- Panorama not shared skillet file reference error

15.5.3 0.0.1

Released January 22, 2020

- first release based on v9.0
- no release specific additions

15.6 9.0 Template Release History

Template content updates are high level. Details can be found in the template guides.

15.6.1 0.0.6

Released September 16, 2020

- URL filtering profile: move 'hacking' category to alert since not malicious
- remove sinkhole address block policy and associated address object
- remove http partial response so now allowed
- remove 'no decrypt' decryption policy that checks for expired/invalid certs; too strict
- update WF malicious reports using 'neq benign' instead of equal to malicious categories
- update validation skillets based on above modifications
- update metadata file for XML snippet skillets w/ option to skip IP address/admin user/DNS configuration elements
- converted customer URL-filtering profile lingo from White-List/Black-List to Allow/Block

15.6.2 0.0.5

Released April 28, 2020

- Update WF file size limits to match the BPA
- validation updates including grayware check and WF file size limits
- metadata file updates: variable clean up with toggle_hint and help_text
- Panorama not shared skillet file reference error

15.6.3 0.0.4

Released January 22, 2020

- added grayware and cryptocurrency url categories
- added missing User tag log settings
- inclusion of validation skillets

15.6.4 0.0.3

Released c September, 2019

- minor updates

15.6.5 0.0.2

Released July 30, 2019

- Added password complexity and admin lockout elements
- Dynamic updates for GlobalProtect
- Opt-out default for the Palo Alto Networks EDL associated security rules
- Removed the IPv4 and IPv6 Bogon EDLs and associated security rules
- Updated the IPv4 sinkhole to use FQDN instead of an IP address
- Clean up for the baseline configuration to remove IPSEC, IKE, QoS defaults
- Clean up for URL Block and Allow category usage in profiles

15.6.6 0.0.1

Released March 15, 2019

- migrated initial template from 8.1
- inclusion of new features per the 9.0 new features documentation

15.7 8.x Template Release History

Template content updates are high level. Details can be found in the template guides.

15.7.1 1.0.6

Released July 30, 2019

- Added password complexity and admin lockout elements
- Dynamic updates for GlobalProtect
- Opt-out default for the Palo Alto Networks EDL associated security rules
- Removed the IPv4 and IPv6 Bogon EDLs and associated security rules
- Updated the IPv4 sinkhole to use FQDN instead of an IP address
- Clean up for the baseline configuration to remove IPSEC, IKE, QoS defaults
- Clean up for URL Block and Allow category usage in profiles

15.7.2 1.0.5

Released March 18, 2019

Template Content

- added max lines for log csv output

15.7.3 1.0.4

Released January 8, 2019

Template Content

- updated virus profiles from ‘default’ to ‘reset-both’ so explicit blocking
- added set commands template as text file and Excel spreadsheet
- loadable default configurations include full xml and set commands
- update to the template stack snippet including <config> tree elements
- removed GTP logging elements since not supported on all hardware platforms

15.7.4 1.0.3

Released Oct 3, 2018

Template Content

- added a default security profile group based on the Outbound group

Documentation

- fixed errors in the tools installation instructions

15.7.5 1.0.2

Released August 30, 2018

Template Content

- modified device_system type=dhcp configuration elements to fix dhcp-client commit error

15.7.6 1.0.1

Released: August 7, 2018

Template Content

- Device settings updates to increase security hardening
 - Prevent TCP and UDP buffer overflow and multi-part HTTP download evasions
 - Enable high DP load logging
 - Prevent App-ID buffer overflow evasion
 - set bypass-exceed-queue to ‘no’
 - Prevent TCP and MPTCP evasions
- Include default login banner
- Correct url-filtering Alert-All profile to include command-and-control
- Set default interzone action to a drop instead of deny
- include firewall management interface options for dhcp-client, standard or cloud models
- include Panorama options for standard or cloud deployments

- using a tag attribute for the template version numbering

Documentation

- moved docs to readthedocs.io
- move to release-specific documentation

Template Archive

- moved to release branch per software release in github

15.7.7 1.0.0

Released: May 10, 2018

- first release on github
- xml snippets and full config
- static pdf documentation

15.8 Tools Release Updates

15.8.1 July 14th 2021

- Added a Bash script the user can run that automatically updates the Submodules folder

15.8.2 May 28th 2021

- Major tooling revamp with all python scripts being obsoleted by the new SLI tool
- Replaced everything in the tooling directory with a README file on using SLI
- Sli has built in functions that do what the previous python scripts did in a more efficient fashion
- Added a Bash script the user can run that replaces the build_all.py script

15.8.3 Jul 21, 2020

- update set command and spreadsheet scripts to only use variables contained in config section
- modify set command expect test script to use start-stop row values

15.8.4 Jan 22, 2020

- updated the build_full_config.py with the ability to merge snippets using same xpath

15.8.5 Jul 30, 2019

- added build_all.py to create all full configs and spreadsheets
- test_set_commands.py and test_full_config.py to load and test configuration changes

15.8.6 Jan 8, 2019

- moved config variables from a python dictionary to a yaml format
- updated existing tools to support the yaml variables file
- added a utility to create the Excel spreadsheet from the set conf file
- removed the creation of default snippets output to loadable configs
- renamed the output from 'my configs' to 'loadable configs' for clarity

15.8.7 Oct 3, 2018

- modified variable model to support python 3.5 instead of 3.6 and later

15.8.8 August 7, 2018

- added the build_full_config utility to create a full template from the config snippets
- added the build_my_config utility
 - provide simple variable substitutions using the my_variable inputs
 - store output into the my_config folder with unique naming

15.8.9 May 3, 2019

- fixed tools issue so will load the panw edl based security rules

15.9 Documentation Revisions

Documentation revisions outside of template-tooling updates. These are documented by date, not version.

15.9.1 Jul 22, 2020

- update viz guide with 10.0 mods and UI
- update template text where required based on 10.0 mods

15.9.2 April 29, 2020

- update WF file size limit image in visual guide
- create sidebar menu sections
- add content for skillet players

15.9.3 January 22, 2020

- addition of visual guide for panos
- validation skillet section added
- add 9.1 related content links

15.9.4 July 30, 2019

- Move docs to their own doc branch and merge as a single doc set
- Add in associated template changes and new xml links (mgt user config and password complexity)
- Add a release variance doc to show deltas for new releases
- Addition of requirements and caveats to use IronSkillet
- Pointers to PanHandler and SkilletCLI as new tools to load configurations

15.9.5 March 18, 2019

- added instructions to remove security profiles for reduced capacity VM-50
- updated with inclusion of max csv lines for log output

15.9.6 Jan 8, 2019

- simplified repo main README for non-python users
- added documentation for the SET command spreadsheet
- added next-level directory README files for added context
- general edits for using tools based on tools changes
- added description for Panorama template variations in Panorama template docs

15.9.7 Nov 2, 2018

- added instructions for editing the full configuration template variables in the GUI
- added instructions for editing the full configuration template variables using the console

15.9.8 Oct 3, 2018

- fixed errors in the tools installation instructions

15.9.9 August 7, 2018

- moved docs to readthedocs.io
- move to release-specific documentation

15.9.10 May 10, 2018

- first release on github
- static pdf documentation