

# Best Practices Workshop



Version 1.1

November 2022

# Agenda

- Standard Practices
- Best Practices Documentation
- Day 1 Configurations and Iron Skillets
- Security Lifecycle Report (SLR)
- Best Practices Assessment (BPA and BPA+)
- AIOps
- Getting the most from your firewall
- Zero Trust
- Expedition
- Resources

# Standard Practices

# Standard Practices

- Set a standard, document it, and stick to it:
  - Firewall naming conventions
  - Zone, object, and policy naming
  - Build subnets with growth in mind
  - Document your naming conventions
  - Backup your configurations
- Have a different account for every user who has access to devices.
  - Set the password to the admin account and lock it in a safe place never to be used again.
  - Configure 2FA/MFA
- Baseline your network and security. Do you know what normal looks like?

# Standard Practices

Always add descriptions:

## Security Policy Rule

**General**

Source

Destination

Application

Service/URL Category

Actions

Target

Usage

Name

Rule Type

Description

Tags

Group Rules By Tag

Audit Comment

[Audit Comment Archive](#)

# Standard Practices

- Get familiar with the CLI:
  - [Using the CLI Documentation](#)
  - [CLI Jumpstart](#)
  - [CLI Cheat Sheets](#)

IF YOU WANT TO...	USE...
<ul style="list-style-type: none"><li>• Show general system health information.</li></ul>	<pre>&gt; show system info</pre>
<ul style="list-style-type: none"><li>• Show percent usage of disk partitions. Include the optional <code>files</code> parameter to show information about inodes, which track file storage.</li></ul>	<pre>&gt; show system disk-space files</pre>
<ul style="list-style-type: none"><li>• Show the maximum log file size.</li></ul>	<pre>&gt; show system logdb-quota</pre>

# Standard Practices

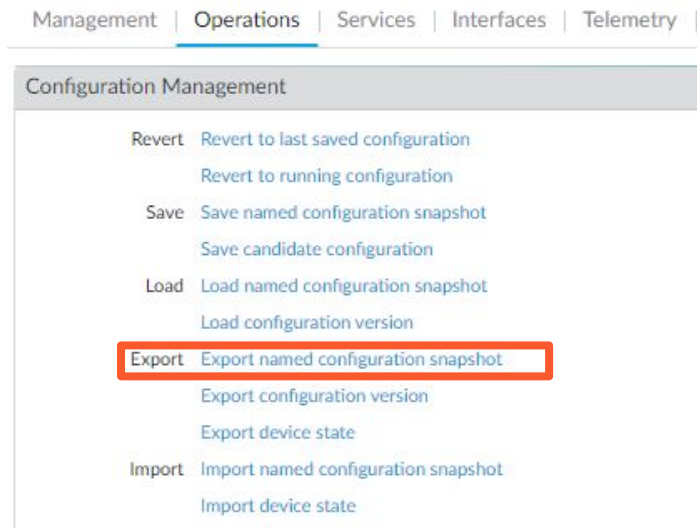
- Scripting your configuration
- Build a script for every new firewall you add to Panorama

```
***** Default Configuration *****
configure
set deviceconfig system ip-address 172.31.45.25 netmask 255.255.255.0 default-gateway 172.31.45.1 dns-setting servers primary 172.31.50.18
set deviceconfig system panorama local-panorama panorama-server 172.31.45.10
commit
request content upgrade check
request content upgrade info
request content upgrade download <content version>
request system software check
request system software info
request system software download version 10.1.0
request system software download version 10.1.6
request system software install version 10.1.6
commit
request restart system
exit
```

# Standard Practices

- Configurations are in XML format
- [XML Basics](#)

- Configuration Backups





# Standard Practices

- EoL Resources:
  - <https://docs.paloaltonetworks.com/resources/eol#sort=relevancy&layout=card&numberOfResults=25>
  - 8.1, 9.0, and 10.0 are EoL
- Upgrading Software
  - Determine the upgrade path from your current version:
    - <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-upgrade/upgrade-pan-os/upgrade-the-firewall-pan-os/determine-the-upgrade-path>
  - Determine the preferred releases software:
    - <https://live.paloaltonetworks.com/t5/customer-resources/support-pan-os-software-release-guidance/ta-p/258304>
- Example upgrade path for a firewall running 9.1.13 to 10.1.6-h6
  - Verify Dynamic Updates are up to date
  - Download and install 9.1.14-h4
  - Download 10.0
  - Download and install 10.0.11-h1
  - Upgrade Dynamic Updates
  - Download 10.1
  - Download and install 10.1.6-h6
  - Upgrade Dynamic Updates

# Best Practices Documentation

# Best Practices Documentation

- <https://docs.paloaltonetworks.com/best-practices>

## Best Practices

At Palo Alto Networks, it's our mission to develop products and services that help you, our customer, detect and prevent successful cyberattacks. We've developed our best practice documentation to help you do just that. Whether you're looking for the best way to secure administrative access to your next-gen firewalls and Panorama, create best practice security policy to safely enable application access at the internet gateway and the data center, or learn the best way roll out a decryption policy to prevent threats from sneaking into your network, you will find the guidance you need here in our best practice documentation. And, our best practice library keeps growing and evolving to keep up with the ever-changing threat landscape, so be sure to check back often!

### Spotlight

#### Transition to Best Practices

Documents, checklists, videos, webinars, best practice assessment tools, and more help you learn about and apply security best practices.

Transition Now

#### Best Practices for Managing Firewalls with Panorama

Use the Panorama Best Practices to help manage and



#### Best Practices Assessment (BPA)

Run the BPA Now

#### Administrative Access Best Practices

Firewalls and Panorama's centralized management centers

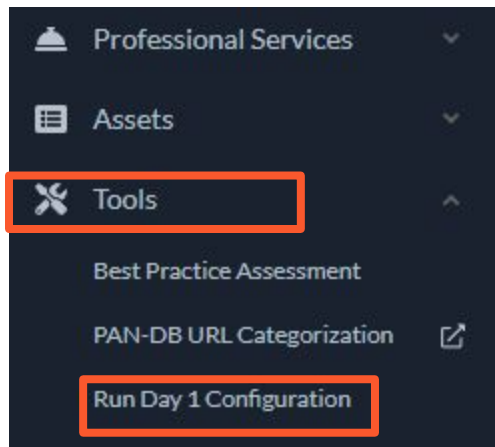
### GETTING STARTED

- 1 Run the BPA
- 2 Use Best Practices to Secure Administrative Access
- 3 Use Content Update Best Practices
- 4 Configure a Best Practice Internet Gateway

# Day 1 Configurations and Iron Skillets

# Day 1 Configuration

- Download a Day 1 Configuration for a registered device
- <https://support.paloaltonetworks.com/>



- *Note: A Day 1 Configuration will overwrite any configuration on the device!*

# Day 1 Configuration

- Day 1 Configurations can be for Panorama or NGFW
- All devices must be registered in the system and have the appropriate licenses registered

## Run Day 1 Configuration

Please enter the Serial Number of the device, or cloud based firewall, for which you would like to create a Day 1 Configuration

**Note:** Placing a Day 1 Configuration on your firewall will replace any other configurations currently in place

Serial number:



Confirm Serial Number

# Day 1 Configuration

**Current Account** Palo Alto Networks **Post answers**

## RUN DAY 1 CONFIGURATION

**Setup**

- Serial Number: JW4306003
- Device Type: PAN-OS
- Enter the PAN-OS version you specified during device registration → PAN-OS Version: Choose one PAN-OS Version...
- Enter a Host Name → Hostname: sample

**Management**

- Management Type: ☒ Static ☐ DHCP Client
- Enter IP information matching your deployment → IPv4: 192.168.55.10
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.55.2
- Primary DNS: 8.8.8.8
- Secondary DNS: 8.8.4.4

**Logging**

- Enter logging server information → SMTP Server IP: 192.0.2.1
- From: username@domain.com
- To: username@domain.com
- Logging Server IP: 192.0.2.2

[Generate Config File](#)

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

## Configuration Management

- Revert** [Revert to last saved configuration](#)  
[Revert to running configuration](#)
- Save** [Save named configuration snapshot](#)  
[Save candidate configuration](#)
- Load** [Load named configuration snapshot](#)  
[Load configuration version](#)
- Export** [Export named configuration snapshot](#)  
[Export configuration version](#)  
[Export device state](#)
- Import** [Import named configuration snapshot](#)  
[Import device state](#)

# Iron Skillets

- What is an Iron Skillet?
  - 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.
- [Iron Skillet Documentation](#)
- [Iron Skillet Github](#)

panos_v10.1 ▾ iron-skillet / templates / panos /	
BoraMutluoglu Removed QoS snippet	
..	
baseline	10.1 first update
full	Removed QoS snippet
set_commands	Full config Bug Fixes
snippets	Full config Bug Fixes



# Iron Skillets

2641 lines (2641 sloc) | 102 KB

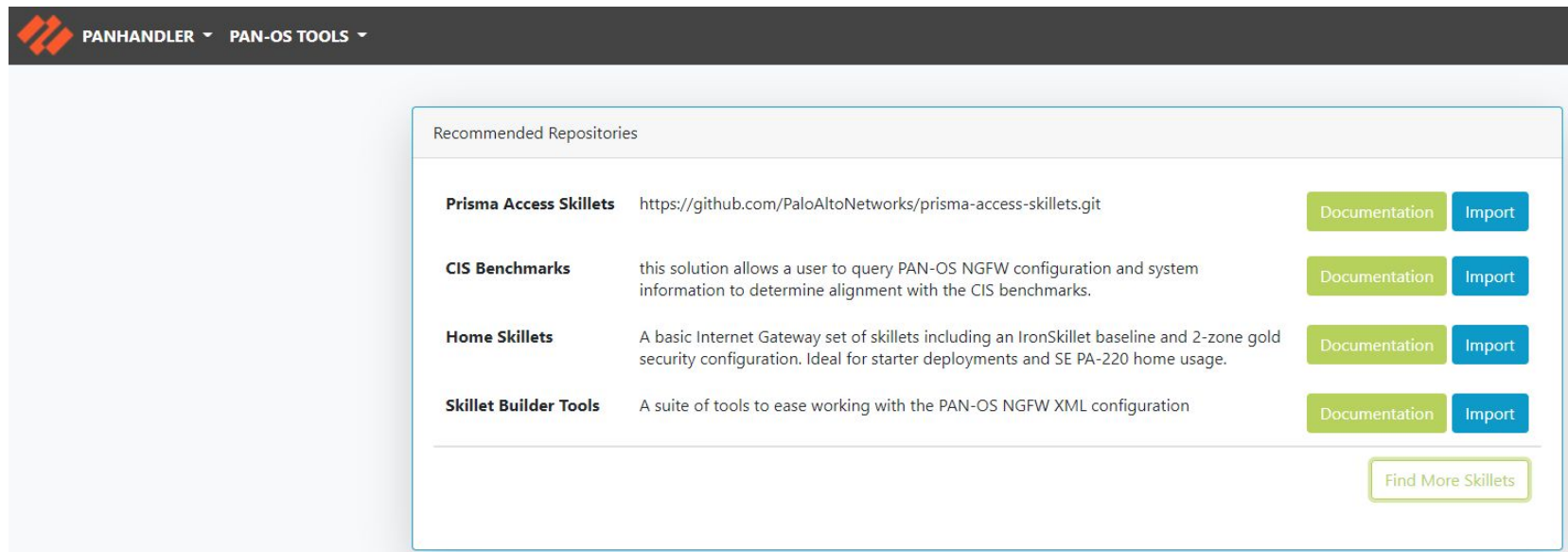
```
1 <config version="10.1.0" urldb="paloaltonetworks">
2   <mgt-config>
3     <users>
4       <entry name="{{ADMINISTRATOR_USERNAME}}">
5         <phash>{{ADMINISTRATOR_PASSWORD | md5_hash}}</phash>
6         <permissions>
7           <role-based>
8             <superuser>yes</superuser>
9           </role-based>
10          </permissions>
11        </entry>
12      </users>
13      <password-complexity>
14        <enabled>yes</enabled>
15        <minimum-length>12</minimum-length>
16        <minimum-uppercase-letters>1</minimum-uppercase-letters>
17        <minimum-lowercase-letters>1</minimum-lowercase-letters>
18        <minimum-numeric-letters>1</minimum-numeric-letters>
19        <minimum-special-characters>1</minimum-special-characters>
20        <block-username-inclusion>yes</block-username-inclusion>
21        <password-history-count>24</password-history-count>
22        <new-password-differs-by-characters>3</new-password-differs-by-characters>
23      </password-complexity>
24    </mgt-config>
```

824 lines (799 sloc) | 71.1 KB

```
1 # set command configuration for panos v10.1
2 # commands are expected to be loaded in order
3 # this template uses jinja format
4 # either 'search and replace' or the scripts in the tools dir can be used to create a loadable configuration
5
6 # management interface configuration may be skipped if already online
7 set deviceconfig system hostname {{ FW_NAME }}
8 set deviceconfig system ip-address {{ MGMT_IP }}
9 set deviceconfig system netmask {{ MGMT_MASK }}
10 set deviceconfig system default-gateway {{ MGMT_DG }}
11 set deviceconfig system dns-setting servers primary {{ DNS_1 }}
12 set deviceconfig system dns-setting servers secondary {{ DNS_2 }}
13
14 # alternate configuration for a management interface using DHCP
15 set deviceconfig system type dhcp-client send-hostname yes
16 set deviceconfig system type dhcp-client send-client-id no
17 set deviceconfig system type dhcp-client accept-dhcp-hostname no
18 set deviceconfig system type dhcp-client accept-dhcp-domain no
```

# Panhandler

- Panhandler is an open-source application that allows you to import and playback any skillet using a web interface.
- [Panhandler Documentation](#)
- [Panhandler Quickstart](#)



The screenshot displays the Panhandler web interface. At the top, a dark navigation bar contains the Panhandler logo and two dropdown menus labeled 'PANHANDLER' and 'PAN-OS TOOLS'. The main content area is titled 'Recommended Repositories' and lists four categories of skillet resources, each with a description and buttons for 'Documentation' and 'Import'.

Recommended Repositories			
<b>Prisma Access Skillets</b>	<a href="https://github.com/PaloAltoNetworks/prisma-access-skillets.git">https://github.com/PaloAltoNetworks/prisma-access-skillets.git</a>	<a href="#">Documentation</a>	<a href="#">Import</a>
<b>CIS Benchmarks</b>	this solution allows a user to query PAN-OS NGFW configuration and system information to determine alignment with the CIS benchmarks.	<a href="#">Documentation</a>	<a href="#">Import</a>
<b>Home Skillets</b>	A basic Internet Gateway set of skillets including an IronSkillet baseline and 2-zone gold security configuration. Ideal for starter deployments and SE PA-220 home usage.	<a href="#">Documentation</a>	<a href="#">Import</a>
<b>Skillet Builder Tools</b>	A suite of tools to ease working with the PAN-OS NGFW XML configuration	<a href="#">Documentation</a>	<a href="#">Import</a>

[Find More Skillets](#)

# Panhandler

Local Panorama paloalto

Environments

Create Environment

View Context

Clear Cache

View SSH Public Key

Logout

## Local Panorama

PaloAltoNetworks Panorama

Load

Configure

Clone

Delete

## LA-FW01

EVE-NG Firewall on LA network.

Load

Configure

Clone

Delete

## Local PAN-OS

PaloAltoNetworks PAN-OS VM50

Load

Configure

Clone

Delete

## DC-FW01

EVE-NG Firewall on the DC network.

Load

Configure

Clone

Delete

# Panhandler

## Skillet Collections

Filter Related Collections

Deploy	<b>Configure</b>	Assess	Respond	Demonstrate
--------	------------------	--------	---------	-------------

Search

Best Practice

4 Skillets in the Best Practice Collection

Go

IPSEC

2 Skillets in the IPSEC Collection



Go

IronSkillet

11 Skillets in the IronSkillet Collection

Go


# Panhandler

Render Template  

## Customize Template: v10.0 Iron-Skillet Full XML Configuration for NGFW

Firewall hostname:

firewall management IP type:

select if the management interface will use DHCP or static configuration

primary NTP server:


secondary NTP server:

admin username:

admin password:

primary dns server:

# Panhandler


 PANHANDLER ▾ PAN-OS TOOLS ▾

DC-FW01 paloalto ▾

Continue

Print

Save



## Iron Skillet full validation


PAN-OS 10.0


Hostname: West-FW01

Generated: 2022-07-26 13:25:43






### Validation Statistics

Total Checks  
52

  
Checks Passed  
3

  
Checks Failed  
49

### Iron Skillet validation results

Validation Check	Result
threat content updates recurring every 30 minutes	
AV content updates recurring every hour	
WF content updates recurring real-time or every 1 minute	
SNMPv3 instead of older versions	
DNS primary and secondary servers configured	

# Security Lifecycle Review

# Security Lifecycle Assessment (SLR)

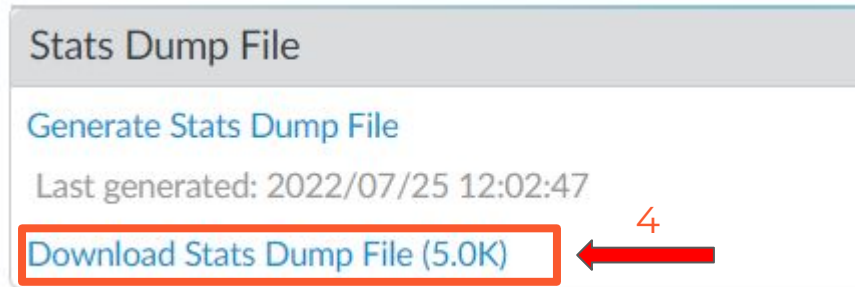
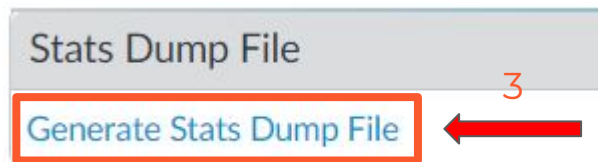
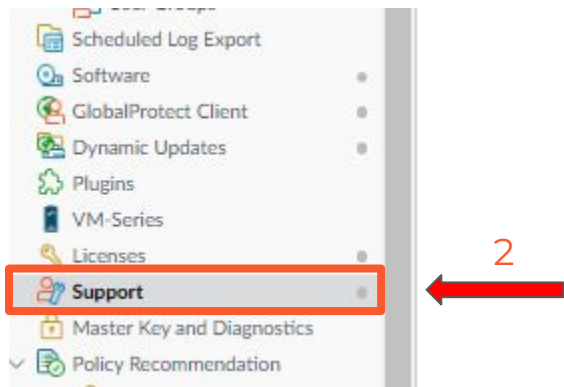
*An assessment of network vulnerabilities, threats and risks*

Visibility into traffic, URL activity, content, threats, IoT devices, applications

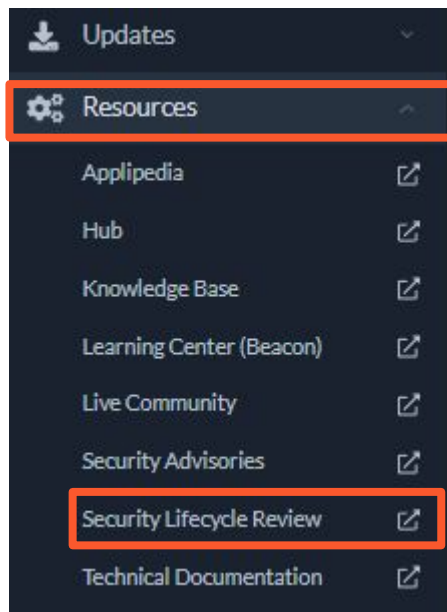


# SLR

- Get the information for the SLR



# SLR



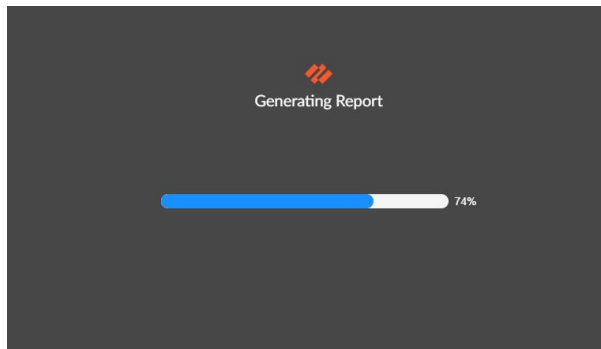
The 'Generate New Report' form is shown with the 'Account Information' tab selected. The progress bar indicates the first step is complete. The form contains the following fields:

- Account Name\*: PAN SE - [dellis@paloaltonetworks.com]
- Industry\*: High Technology
- Country\*: United States
- Geographic Region\*: North America, Latin America, Canada
- Deployment Location\*: Perimeter/Internet Gateway
- Prepared By\*: David Ellis
- Language\*: English

A 'Next' button is located at the bottom right of the form.

The 'Generate New Report' form is shown with the 'Upload' tab selected. The progress bar indicates the second step is in progress. The form includes a 'Single File' button (selected) and a 'Multiple Files' button. Below these is a dashed box containing a file upload icon and the text: 'Drag & drop or browse to upload a stats dump file', 'Total file size cannot exceed 50 MB', and 'Stats Dump File (\*.tar.gz, \*.gz)'. At the bottom right, there are 'Back' and 'Upload' buttons.

# SLR



## SECURITY LIFECYCLE REVIEW

- Report Customization
  - ☒ Executive Summary
  - ☒ Applications at a Glance
  - ☒ Applications that Introduce Risk
  - ☒ Advanced URL Filtering Analysis
- SLR Help Resources
  - Download PDF**
  - Report an Issue

### EXECUTIVE SUMMARY FOR PAN SE - [dellis@paloaltonetworks.com]

The Security Lifecycle Review summarizes the business and security risks facing **PAN SE - [dellis@paloaltonetworks.com]**. The data was gathered by Palo Alto Networks during the report time period. The report provides actionable intelligence around the application content, and threats traversing the network, including recommendations that can be employed to reduce the organization's overall risk.

*Confidential Information - Do Not Redistribute*

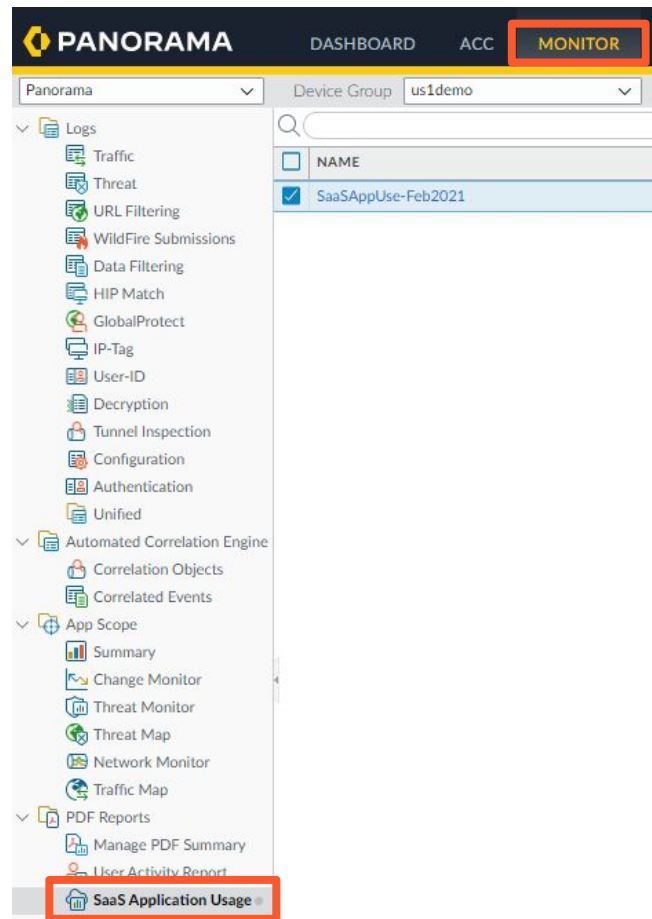
**KEY FINDINGS**

**13**  
APPLICATIONS IN USE

**3**  
HIGH RISK APPLICATIONS

# SLR and SaaS App Report

- [SLR PDF Report](#)
- [SaaS Application Usage Report](#)



# Best Practices Assessment

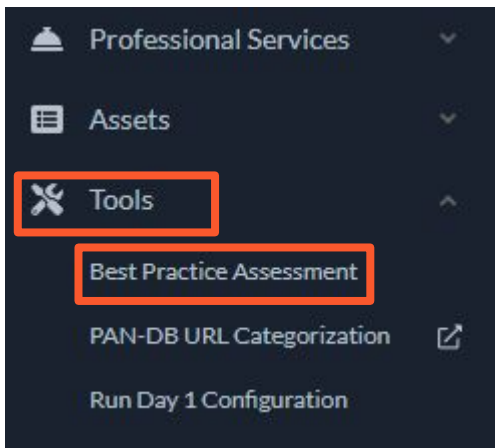
# BPA and BPA+

- Get the information for the BPA or BPA+

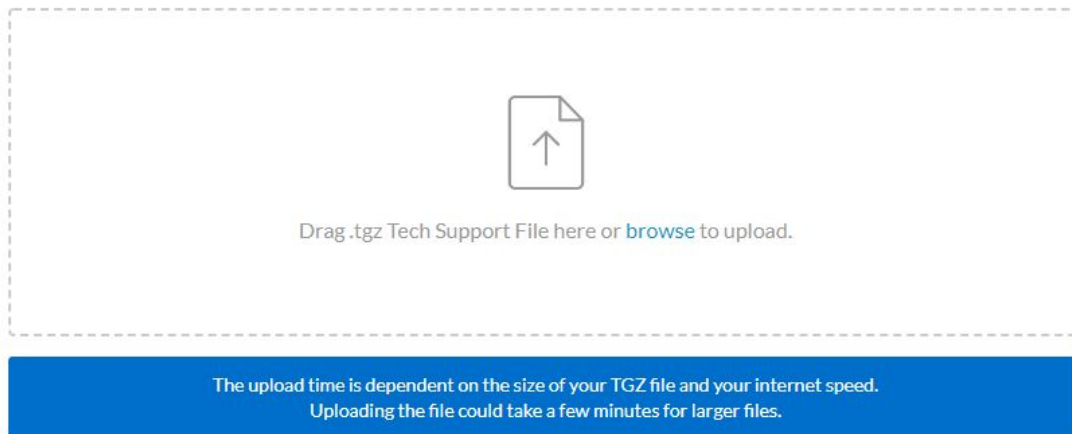
The screenshot illustrates the process of generating a Tech Support File in the Palo Alto Networks PA-VM interface. The interface has a dark blue header with the PA-VM logo and navigation tabs: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. A red arrow labeled '1' points to the 'DEVICE' tab. Below the header, a left sidebar contains a list of options: Scheduled Log Export, Software, GlobalProtect Client, Dynamic Updates, Plugins, VM-Series, Licenses, Support, Master Key and Diagnostics, and Policy Recommendation. A red arrow labeled '2' points to the 'Support' option. The main content area on the right shows two sections. The top section, titled 'Tech Support File', contains a button 'Generate Tech Support File' highlighted with a red box and a red arrow labeled '3'. The bottom section, also titled 'Tech Support File', shows the text 'Last generated: 2022/07/21 13:14:44' and a button 'Download Tech Support File (52.3M)' highlighted with a red box and a red arrow labeled '4'.

# BPA

- Upload your Tech Support File to the CSP
- <https://support.paloaltonetworks.com/>
- \*\* Partners get Cyberforce XP for running BPAs for customers\*\*



Run a Best Practice Assessment (BPA) to measure what, where, and how you are applying capabilities across your Palo Alto Networks NGFW or Panorama, and how your configurations compare to best practices.



# BPA

## Architecture Classification

Area of Architecture Mapping: Please map each zone listed below to the Area of Architecture: Perimeter, Internal Core, Mobility, or Datacenter. If you are not ready to map each zone to Area of Architecture, the default values will be set to Undefined and you can just click the 'Skip this step' button at the bottom of the page.

Note: If there aren't any zones listed below that is because none of the zones have been applied to a Security Policy.

<input type="checkbox"/>	ZONE	DEVICE GROUP	CLASSIFICATION
<input type="checkbox"/>	outside	vsys1	Internet
<input type="checkbox"/>	inside	vsys1	Internal Core
<input type="checkbox"/>	tunnel_zone	vsys1	Remote Office/MPLS
<input type="checkbox"/>	ra-vpn	vsys1	Remote Users/VPN

### ARCHITECTURE CLASSIFICATION

Please drag your selection from here to the correct Zone and Device classification

- ▼ Enterprise
  - ▼ Perimeter
    - Internet
    - DMZ
    - 3rd Party/Vendor
  - ▼ Internal Core
    - Users
    - IT Infrastructure
    - Out-of-Band Management
    - Remote Office/MPLS
  - ▼ Mobility
    - Remote Users/VPN
    - Guest
    - BYOD
  - ▼ Datacenter
    - Web-tier
    - App-tier
    - DB-tier
    - PCI

[< Back](#)[Skip this step](#)[Next >](#)



# BPA

CLASSIFY

If you need to review or edit your Architecture Classifications, please go BACK now.

Otherwise, you are now ready to generate your Best Practice Assessment Report.

Click on "Generate & Download Report" button to view your summary and download the detailed report.

Your current industry is selected by default. To compare your BPA results against a particular industry, please make a selection from the drop down below.

*\*Default industry is based on the Dun & Bradstreet database.*

High Technology



Generate & Download Report

## Best Practice Assessment (BPA) Summary

Device: East-FW01 - 007954000286198

Prepared by Ellis - 2022-07-21 13:27 (UTC-05:00)

[View History](#)

[Download Summary](#)

[Best Practice Summary](#)

[Security Profile Adoption](#)

[Application & User Control Adoption](#)

[Logging & Zone Protection Adoption](#)

[Decryption Summary](#)

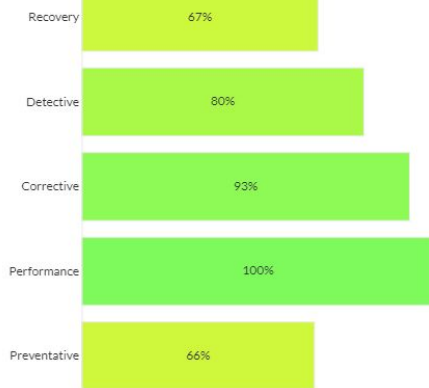
[Recommended Readings](#)

### Capability & Control Category

Class Summary

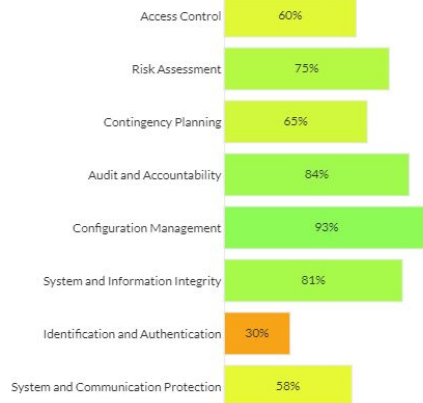
CIS Critical Security Controls

### Capability Summary






Security controls are safeguards or countermeasures put into place to reduce overall risk.  
Additional information available at <https://www.microsoftpressstore.com/articles/article.aspx?p=2201319>.

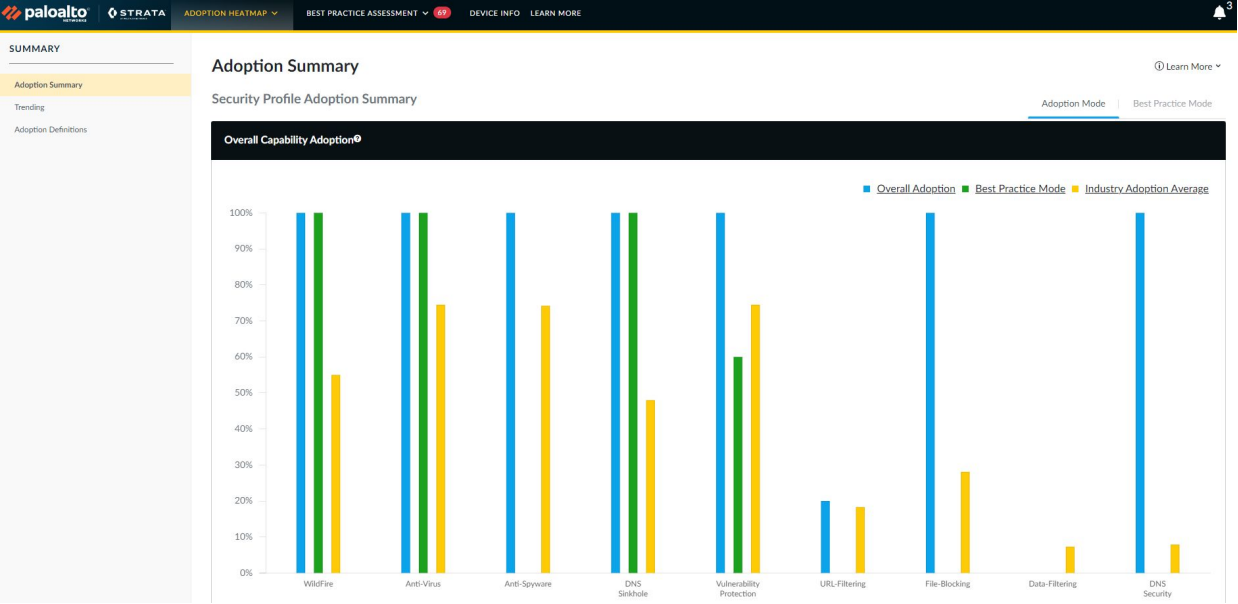
### Control Category Summary



Security controls and assessment procedures for federal information systems and organizations.  
Additional information available at <https://nvd.nist.gov/800-53/Rev4>.

# BPA

Name	Type
 Best Practice Assessment - Strata - East-F...	Chrome HTML Document
 Best Practice Checks - Strata - East-FW01...	XLSX File
 BPA Executive Summary - Strata - East-F...	Adobe Acrobat Document



## BPA - Open File

- [BPA HTML Report](#)
- [BPA Executive Summary PDF Report](#)

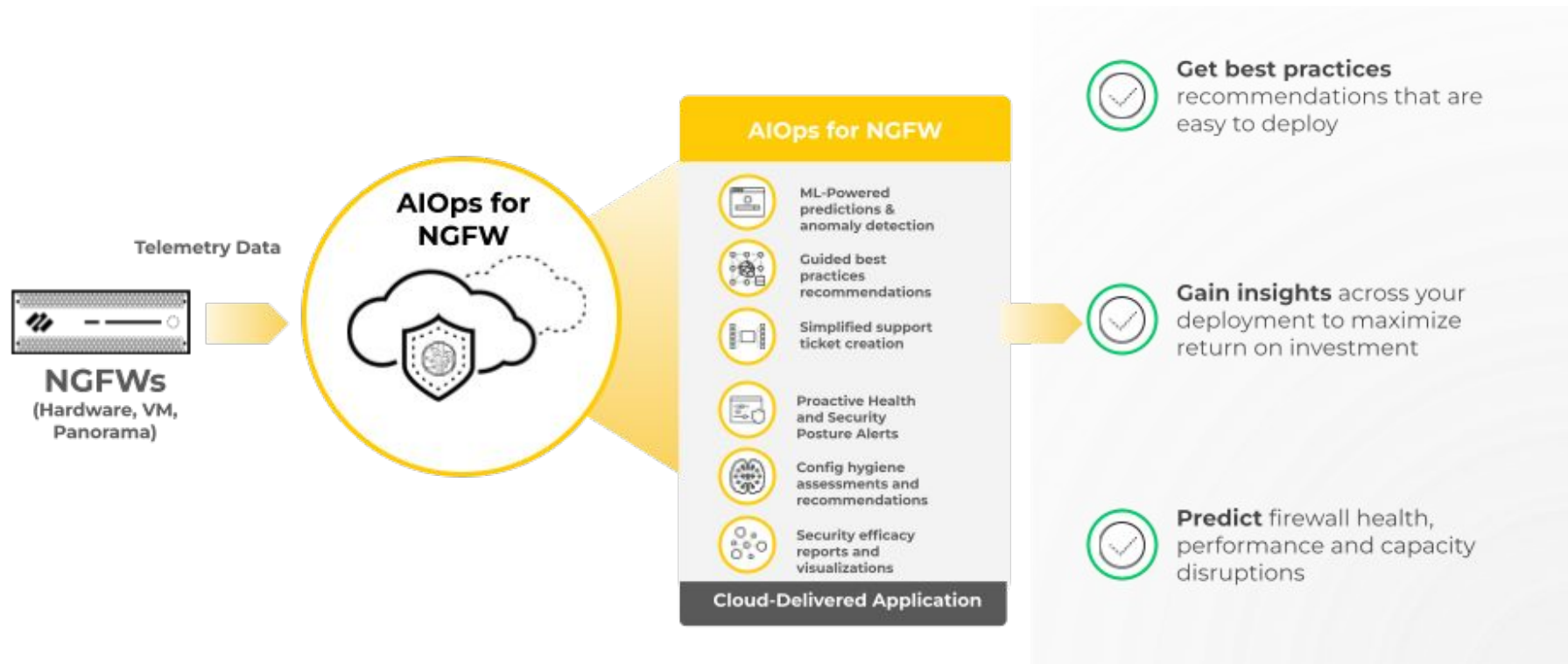
# AIOps

# AIOps

- AIOps for NGFW gives you an overview of the health and security posture of your next-generation firewall deployment to help you identify areas of improvement and close security gaps.
- Requires PAN-OS 10.0 or higher
- Requires Cortex Data Lake (CDL) or Telemetry
- Free or Premium Version
- DNS Security Dashboard

FEATURE SET	FREE	PREMIUM
<b>Strengthen Security Posture</b>	Yes	Yes
• Device configuration best practices assessment	Yes	Yes
• Recommendations for closing security gaps	Yes	Yes
• CLI commands for remediation	Yes	Yes
<b>Proactively Resolve Firewall Disruptions</b>	Partial	Yes
• Hardware alerts	Yes	Yes
• Software and licensing alerts	Yes	Yes
• Config limit alerts	Yes	Yes
• Stale threat content alerts	Yes	Yes
• Resource limit alerts	Partial (Critical system resources, such as Dataplane and Management Plane CPU/Memory)	Yes
<b>Troubleshoot with Logs</b>	Yes	Yes
• View, query and export logs	Yes	Yes

# AIOps



# AIOps

- Setup CDL or Telemetry on NGFW and/or Panorama
- Send information to CDL or Telemetry
- \*\*\*\*\* Allow 24 hours between these steps \*\*\*\*\*
- Activate your AIOps subscription in [The Hub](#)

The screenshot displays the 'The Hub' interface, a central dashboard for Palo Alto Networks applications. At the top, a blue header bar contains the 'HUB' logo, a link to 'Have an auth code?', and an 'Activate App' button. Below this, four app icons are shown: AIOps for NGFW, Cloud Identity Engine, Cortex Data Lake, and Explore. The main content area, titled 'Explore Apps from Palo Alto Networks', features a grid of eight app cards. Each card includes an icon, the app name, a brief description, and 'Activate' and 'Learn More' buttons. The apps shown are: AIOps for NGFW (Device telemetry, log visualization and reporting), Cloud Identity Engine (The industry's first cloud native identity and authentication service), Cortex Data Lake (Enable AI-based innovations for cybersecurity), Cortex XSOAR (Cortex™ XSOAR unifies security orchestration and automation), Cortex XSOAR Marketplace (Discover, try, and buy content packs), Enterprise DLP (Protect sensitive data and enable compliance), Explore (Dive into your logs to gain critical insights), and IoT Security (AI-powered IoT discovery and security).

HUB | Have an auth code? [Activate App](#)

AIOps for NGFW Cloud Identity Engine Cortex Data Lake Explore

Explore More Apps

### Explore Apps from Palo Alto Networks

**AIOps for NGFW**  
Device telemetry, log visualization and reporting  
[Activate](#) [Learn More >](#)

**Cloud Identity Engine**  
The industry's first cloud native identity and authentication service providing a single source of identity for all your users.  
[Activate](#) [Learn More >](#)

**Cortex Data Lake**  
Enable AI-based innovations for cybersecurity.  
[Activate](#) [Learn More >](#)

**Cortex XSOAR**  
Cortex™ XSOAR unifies security orchestration and automation, case management, real-time collaboration and threat intel management to serv...  
[Activate](#) [Learn More >](#)

**Cortex XSOAR Marketplace**  
Discover, try, and buy content packs from an ecosystem of trusted contributors to automate any security process.  
[Learn More >](#)

**Enterprise DLP**  
Protect sensitive data and enable compliance and data privacy across the organization  
[Learn More >](#)

**Explore**  
Dive into your logs to gain critical insights from Cortex Data Lake by viewing, searching, and exporting data.  
[Learn More >](#)

**IoT Security**  
AI-powered IoT discovery and security that is easy to deploy and operationalize.  
[Learn More >](#)



# AIOps



# Getting the most from your firewall

# Getting the most from your firewall

- File Blocking
- Cloud Delivered Security Services (CDSS)
- Credential Theft Prevention
- Zone Protection Policies
- Geo Blocking Rules
- Built-in External Dynamic Lists

# File Blocking

- **basic file blocking**—Attach this profile to the Security policy rules that allow traffic to and from less sensitive applications to block files that are commonly included in malware attack campaigns or that have no real use case for upload/download. This profile blocks upload and download of PE files ( .scr, .cpl, .dll, .ocx, .pif, .exe) , Java files (.class, .jar), Help files (.chm, .hlp) and other potentially malicious file types, including .vbe, .hta, .wsf, .torrent, .7z, .rar, .bat. Additionally, it prompts users to acknowledge when they attempt to download encrypted-rar or encrypted-zip files. This rule alerts on all other file types to give you complete visibility into all file types coming in and out of your network.
- **strict file blocking**—Use this stricter profile on the Security policy rules that allow access to your most sensitive applications. This profile blocks the same file types as the other profile, and additionally blocks flash, .tar, multi-level encoding, .cab, .msi, encrypted-rar, and encrypted-zip files.

# File Blocking

- Objects -> Security Profiles -> File Blocking

File Blocking Profile (Read Only) ?

Namebasic file blocking

Description

☐ Shared

☐ Disable override

3 items → ×

<input type="checkbox"/>	NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION	
<input type="checkbox"/>	Block high risk file types	any	7z bat chm class cpl dll exe hlp	both	block	▲ ▼

+ Add

- Delete

RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
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	any	both	alert

# CDSS

- Advanced Threat Prevention (ATP)
  - Wildfire (WF)
  - Advanced URL Filtering (AURL)
  - DNS Security (DNS)
  - Globalprotect (GP)
  - SaaS Security Inline
  - Data Loss Prevention (DLP)
  - Internet of Things (IoT)
- 
- [CDSS Documentation](#)

# Credential Phishing Prevention

Phishing sites are sites that attackers disguise as legitimate websites with the intent to steal user information, especially the credentials that provide access to your network. When a phishing email enters a network, it takes just a single user to click the link and enter credentials to set a breach into motion. You can detect and prevent in-progress phishing attacks, thereby preventing credential theft, by controlling sites to which users can submit corporate credentials based on the site's URL category. This allows you to block users from submitting credentials to untrusted sites while allowing credential submissions to corporate and sanctioned sites.

Credential phishing prevention works by scanning username and password submissions to websites and comparing those submissions against valid corporate credentials. You can choose what websites you want to either allow or block corporate credential submissions to based on the URL category of the website. When the firewall detects a user attempting to submit credentials to a site in a category you have restricted, it either displays a block response page that prevents the user from submitting credentials or presents a continue page that warns users against submitting credentials to sites in certain URL categories but still allows them to continue with the submission. You can customize these block pages to educate users against reusing corporate credentials, even on legitimate, non-phishing sites.

# Credential Phishing Prevention

- Enable User-ID
- Enable Best Practices AURL Filtering profile (**AURL License Required**)
- Add a decryption policy (optional but recommended)
- Configure AURL filtering profile for Credential Protection
- Apply profile to a policy
- [Credential Phishing Prevention Doc](#)
- Objects -> Security Policy -> URL Filtering

**URL Filtering Profile (Read Only)**

Name: Outbound-URL

Description:

Categories | URL Filtering Settings | **User Credential Detection**

**User Credential Detection**

☒ Use IP User Mapping

**URL Filtering Profile (Read Only)**

Name: Outbound-URL

Description:

Categories | URL Filtering Settings | User Credential Detection | HTTP Header Insertion | Inline ML

77 items

CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
<input type="checkbox"/> Custom-No-Decrypt *	none	none
Pre-defined Categories		
<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
<input type="checkbox"/> auctions	alert	block



# Credential Phishing Prevention

- Using AI/ML to stop phishing attacks

URL Filtering Profile (Read Only) ?

NameOutbound-URL

Description

Categories | URL Filtering Settings | User Credential Detection | HTTP Header Insertion **Inline ML**

Available Models

Q

2 items → ×

MODEL	DESCRIPTION	ACTION
Javascript Exploit Detection	Machine Learning engine to dynamically detect Javascript based exploitation attacks	block
Phishing Detection	Machine Learning engine to dynamically identify credential phishing pages for panos versions after 10.2.0	block

Exceptions

☐ CUSTOM URL CATEGORY/EDL ^

+ Add

- Delete

# Zone Protection Policies

Segmenting the network into functional and organizational zones reduces the network's attack surface—the portion of the network exposed to potential attackers. Zone protection defends network zones against flood attacks, reconnaissance attempts, packet-based attacks, and attacks that use non-IP protocols. Tailor a Zone Protection profile to protect each zone (you can apply the same profile to similar zones). Denial-of-service (DoS) protection defends specific critical systems against flood attacks, especially devices that user access from the internet such as web servers and database servers, and protects resources from session floods. Tailor DoS Protection profiles and policy rules to protect each set of critical devices.

# Zone Protection Policies

- [Configuring Zone Protection Policies Documentation](#)
- Network -> Network Profiles -> Zone Protection

Zone Protection Profile - lab\_stack (Read Only) ?

Name

Recommended\_Zone\_Protection

Description

Flood Protection

Reconnaissance Protection

Packet Based Attack Protection

Protocol Protection

Ethernet SGT Protection

☒ SYN

Action

Random Early Drop

Alarm Rate (connections/sec)

10000

Activate (connections/sec)

10000

Maximum (connections/sec)

40000

☒ UDP

Alarm Rate (connections/sec)

10000

Activate (connections/sec)

10000

Maximum (connections/sec)

40000

☒ ICMP

Alarm Rate (connections/sec)

10000

Activate (connections/sec)

10000

Maximum (connections/sec)

40000

☒ ICMPv6

Alarm Rate (connections/sec)

10000

Activate (connections/sec)

10000

Maximum (connections/sec)

40000

☒ Other IP

Alarm Rate (connections/sec)

10000

Activate (connections/sec)

10000


Maximum (connections/sec)

40000

OK

Cancel

51 | © 2022 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

 paloalto  
NETWORKS

# Geo Blocking Rules

## What are Geolocation and Geoblocking?













Geolocation is the estimation of the real-world geographic location of an object. In our specific use case, I am referring to the physical location of your PC, laptop, mobile device, or from the servers you are trying to reach.

Geoblocking is when you start restricting or allowing access to content based on the geolocation.

The next-generation firewall supports creation of policy rules that apply to specified countries or regions. The region is available as an option when specifying source and destination for security policies, decryption policies, and DoS policies. You can choose from a standard list of countries or use the region settings described in this section to define custom regions to include as options for security policy rules.

# Geo Blocking Rules

- [Geoblocking Documentation](#)
- [Verify PAN-OS IP Region Mapping](#)

3	Known-Bad-Countries-Inbound	lab_dg	none	universal	any	 CN  IR  KP  RU	any	any	any	any	any	any	any	 application-...	 Deny
4	Known-Bad-Countries-Outbound	lab_dg	none	universal	any	any	any	any	any	 CN  IR  KP  RU	any	any	any	 application-...	 Deny

## Geo Blocking Rules

- Block all except rule option

Security Policy Rule

General


**Source**

Destination

Application

Service/URL Category

Actions

<input type="checkbox"/> Any	<input type="checkbox"/> Any
<input checked="" type="checkbox"/> SOURCE_ZONE ^	<input checked="" type="checkbox"/> SOURCE_ADDRESS ^
	<input checked="" type="checkbox"/>  US
<div><div>+ Add</div><div>- Delete</div></div>	<div><div>+ Add</div><div>- Delete</div></div>
	<input checked="" type="checkbox"/> Negate

# Built-in External Dynamic Lists

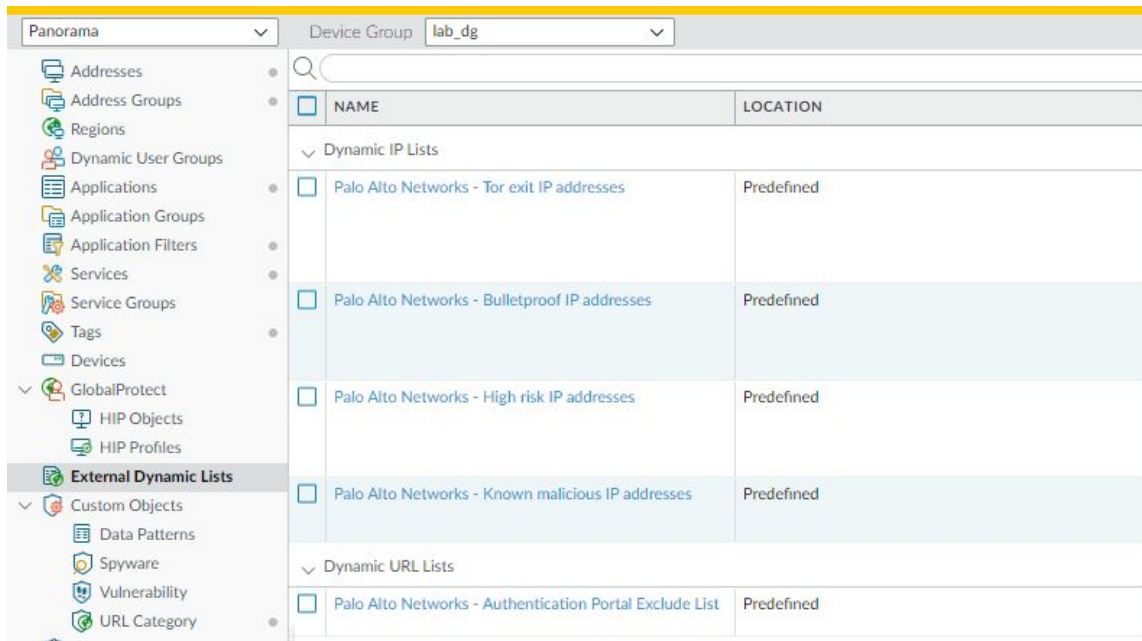
With an **active Threat Prevention license**, Palo Alto Networks provides built-in IP address EDLs that you can use to protect against malicious hosts.

- Palo Alto Networks Bulletproof IP Addresses—Contains IP addresses provided by bulletproof hosting providers. Because bulletproof hosting providers place few, if any, restrictions on content, attackers frequently use these services to host and distribute malicious, illegal, and unethical material.
- Palo Alto Networks High-Risk IP Addresses—Contains malicious IP addresses from threat advisories issued by trusted third-party organizations. Palo Alto Networks compiles the list of threat advisories, but does not have direct evidence of the maliciousness of the IP addresses.
- Palo Alto Networks Known Malicious IP Addresses—Contains IP addresses that are verified malicious based on WildFire analysis, Unit 42 research, and data gathered from telemetry (Share Threat Intelligence with Palo Alto Networks). Attackers use these IP addresses almost exclusively to distribute malware, initiate command-and-control activity, and launch attacks.
- Palo Alto Networks Tor Exit IP Addresses—Contains 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 can serve a legitimate purpose, however, is disproportionately associated with malicious activity, especially in enterprise environments.

The firewall receives updates for these feeds in content updates, allowing the firewall to automatically enforce policy based on the latest threat intelligence from Palo Alto Networks. You cannot modify the contents of the built-in lists. Use them as-is (see Enforce Policy on an External Dynamic List), or create a custom external dynamic list that uses one of the lists as a source (see Configure the Firewall to Access an External Dynamic List) and exclude entries from the list as needed.

# Built-in External Dynamic Lists

- [Built-in EDL Documentation](#)
- Objects -> External Dynamic Lists















The screenshot shows the Palo Alto Networks management console interface. At the top, there are dropdown menus for 'Panorama' and 'Device Group' (set to 'lab\_dg'). Below these is a search bar and a table of External Dynamic Lists (EDLs).

NAME	LOCATION
Dynamic IP Lists	
<input type="checkbox"/> Palo Alto Networks - Tor exit IP addresses	Predefined
<input type="checkbox"/> Palo Alto Networks - Bulletproof IP addresses	Predefined
<input type="checkbox"/> Palo Alto Networks - High risk IP addresses	Predefined
<input type="checkbox"/> Palo Alto Networks - Known malicious IP addresses	Predefined
Dynamic URL Lists	
<input type="checkbox"/> Palo Alto Networks - Authentication Portal Exclude List	Predefined



# Built-in External Dynamic Lists

- Create policies for inbound and outbound traffic
- Build under Policies

	NAME	LOCATION	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION
					ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
1	Known-Bad-EDL-Inbound	lab_dg	none	universal	any	 Palo Alto Netw...  Palo Alto Netw...  Palo Alto Netw...  Palo Alto Netw...	any	any	any	any	any	any	 application-...	 Deny
2	Known-Bad-EDL-Outbound	lab_dg	none	universal	any	any	any	any	any	 Palo Alto Netw...  Palo Alto Netw...  Palo Alto Netw...  Palo Alto Netw...	any	any	 application-...	 Deny

# Zero Trust

# Zero Trust

- What is Zero Trust
- Zero Trust Best Practices
- Methodology - [Web Link](#)
- APP-ID
- Content-ID
- User-ID
- Decryption

# What is Zero Trust?

- Zero Trust is a business-driven, strategic approach to securing your most critical data, applications, assets, and services (DAAS) as well as your users based on what is important to your particular business, in a protect surface. Zero Trust strategy is infrastructure-neutral, so you can apply it to all physical and virtual locations—network, public cloud, private cloud, and endpoint. The concept behind Zero Trust is simple: trust is a vulnerability. Trust nothing in the digital environment—packets, identities, devices, or services—and verify everything. There is no such thing as default trust.
- Implementing the strategy is not something you do once and cookie-cutter copy from network to network because each environment and protect surface is different. As businesses change over time, the goals and DAAS elements also change. Strategy is business-specific and security strategy is specific to protecting what's important to your particular business.
- The goal of Zero Trust strategy is to eliminate trust from the network. Eliminating trust helps prevent successful data breaches, simplifies operations through automation and a reduced rulebase, and simplifies regulatory compliance and audits because Zero Trust environments are designed for compliance and easy auditing.

# Zero Trust Best Practices

The following best practices prepare for and help you transition your network to a Zero Trust architecture:

- Define your desired business outcomes before architecting your Zero Trust environment. The Zero Trust model supports and enables secure business functions.
- Design from the inside-out instead of from the outside-in to protect what's most valuable to your business first. Your most valuable assets are more likely to be in your data center than at your perimeter.
- Use an integrated, centrally managed platform that reduces the total cost of ownership, rather than a collection of point products that don't work well together. Palo Alto Networks shares information among platform elements and enables centralized management and simplified operation using Panorama, GlobalProtect, and Prisma Access to provide consistent policy, prevention, and protection across all locations.
- Use Palo Alto Networks Next-Generation Firewalls as segmentation gateways to consolidate security technologies on one platform and to apply consistent security policy in all locations natively at Layer 7 using App-ID, User-ID, and Content-ID. A segmentation gateway segments and controls the network based on applications, users, and data, and should provide granular access control and secure all traffic as it crosses microperimeters and gains access to a protect surface.
- Segment your network based on what's valuable to your business to prevent unauthorized lateral movement.
- Apply the principle of least-privilege access to your protect surfaces. Determine who needs access to what resources, how they need access, and when they need access. Allow only the exact level of access required for each user and device, assert identity (including proper authorization), and then map Layer 7 policy to identity.
- Decrypt, inspect, and log every packet through Layer 7 that regulations, compliance, and your business practices allow you to inspect. You must inspect and log Layer 7 traffic. Remember, every attacker knows how to bypass security controls at Layer 3 and Layer 4.
- Create a strategy for **tagging workloads to group objects** and **registering tags dynamically** to help automate security policy.
- Develop processes to operate, maintain, and continually update prevention controls as you develop your strategy and design the network. Document processes, educate and train personnel, set baselines, and measure progress against the baselines.
- Transition to a Zero Trust environment gradually, one segment at a time, beginning with one or more non-critical segments from which you learn and gain experience. Zero Trust segments coexist with legacy segments, so you can use a safe, iterative approach instead of a risky rip-and-replace approach.

# Zero Trust Methodology

- Zero Trust 5 Step Methodology
  - Define your Protect Surface
    - Data
    - Application
    - Assets
    - Services
  - Map the Protect Surface Transaction flows
  - Architect a Zero Trust Network
  - Create Zero Trust Policies
    - Kipling Method
      - Who
      - What
      - When
      - Where
      - Why
      - How
  - Monitor and Maintain the Network

# Zero Trust Methodology

The Kipling Method enables you to create security policy that defends each protect surface appropriately because it leads you to understand who should have access, how they should have access, when they should have access, and the protections to apply. You develop policy rules by developing business statements based on the Kipling Method. For example:

	WHO	WHAT	WHEN	WHERE	WHY	HOW
<b>Method</b>	User-ID	App-ID	Time limits	System object	Classification	Content-ID
<b>On-Premise</b>	Epic_Users	Epic	Any	Epic_Srvr	Toxic (data has high value)	Decrypt, inspect (security profiles), log traffic
<b>Cloud</b>	Sales	Salesforce	Working hours	USA	Toxic (data has high value)	Decrypt, inspect (security profiles), log traffic

## Zero Trust - APP-ID

- App-ID, a patented traffic classification system only available in Palo Alto Networks firewalls, determines what an application is irrespective of port, protocol, encryption (SSH or SSL) or any other evasive tactic used by the application. It applies multiple classification mechanisms—application signatures, application protocol decoding, and heuristics—to your network traffic stream to accurately identify applications.
- New and modified App-IDs are delivered to the firewall as part of Applications and Threats Content Updates.
- 4k+ Applications with NGFW and 16k+ applications with SaaS license



# Zero Trust - APP-ID

- View Applications
  - Panorama or NGFW - Objects -> Applications
  - [Applipedia](#)

Device Grouplab\_dg

Search

All

Clear Filters

CATEGORY ^		SUBCATEGORY ^		RISK ^		TAGS ^	
1247	business-systems	54	audio-streaming	1623	1	15	DLP App Exclusion
447	collaboration	24	auth-service	978	2	26	eLearning
355	general-internet	5	content-management	568	3	87	Enterprise VoIP
323	media	41	database	365	4	32	Entertainment Video
495	networking	2	design	143	5	18	G Suite
808	saas	89	email				
2	unknown	72	encrypted-tunnel				
		45 app.com					

	NAME	LOCATION	CATEGORY	SUBCATEGORY	RISK	TAGS
<input type="checkbox"/>	100bao		general-internet	file-sharing	5	
<input type="checkbox"/>	iec-60870-5-104					
<input type="checkbox"/>	104apci-supervisory		business-systems	ics-protocols	2	
<input type="checkbox"/>	104apci-unnumbered		business-systems	ics-protocols	2	
<input type="checkbox"/>	104apci-unnumbered-startdt-act		business-systems	ics-protocols	1	
<input type="checkbox"/>	104apci-unnumbered-startdt-con		business-systems	ics-protocols	1	
<input type="checkbox"/>	104apci-unnumbered-stopdt-act		business-systems	ics-protocols	1	
<input type="checkbox"/>	104apci-unnumbered-stopdt-con		business-systems	ics-protocols	1	
<input type="checkbox"/>	104apci-unnumbered-test-act		business-systems	ics-protocols	1	

# Zero Trust - APP-ID

- Building Policies by Application
  - Create an application filter - Objects -> Application Filters -> ADD
  - Build a policy with the application filter

Application Filter

NAME  ☐ Shared ☐ Disable override ☐ Apply to New App-IDs only  Clear Filters 18 matching as

CATEGORY ^	SUBCATEGORY ^	RISK ^	TAGS ^	CHARACTERISTIC ^
1 general-internet	5 email	9 2	0	1 Evasive
17 saas	1 file-sharing	5 3	App-ID Cloud Engine	2 Excessive Bandwidth
	2 internet-utility	3 4	1 DLP App Exclusion	4 HIPAA
	10 office-programs	1 5	0 eLearning	13 No Certifications
			0 Enterprise VoIP	17 SaaS
			0	4 SOC II
			0	13 Transfers Files

NAME	LOCATION	CATEGORY	SUBCATEGORY	RISK	TAGS	STANDARD PORTS	EXCLUDE
gmail (5 out of 8 s					Sanctioned		<input type="checkbox"/>
gmail-base		saas	email	4	G Suite Web App	443,465,587,80,993,5	<input type="checkbox"/>
gmail-downlo		saas	email	2	G Suite Web App	443.tcp	<input type="checkbox"/>
gmail-enterpr		saas	email	4	G Suite Web App	443,80.tcp	<input type="checkbox"/>

Page 1 of 1

Displaying 1 - 21 of 21

Show Technology Column

OK

Cancel

Security Policy Rule

General | Source | Destination | **Application** | Service/URL Category | Actions

☐ Any

☐ APPLICATIONS ^

☒ Google

Application Filter

Google Apps

New

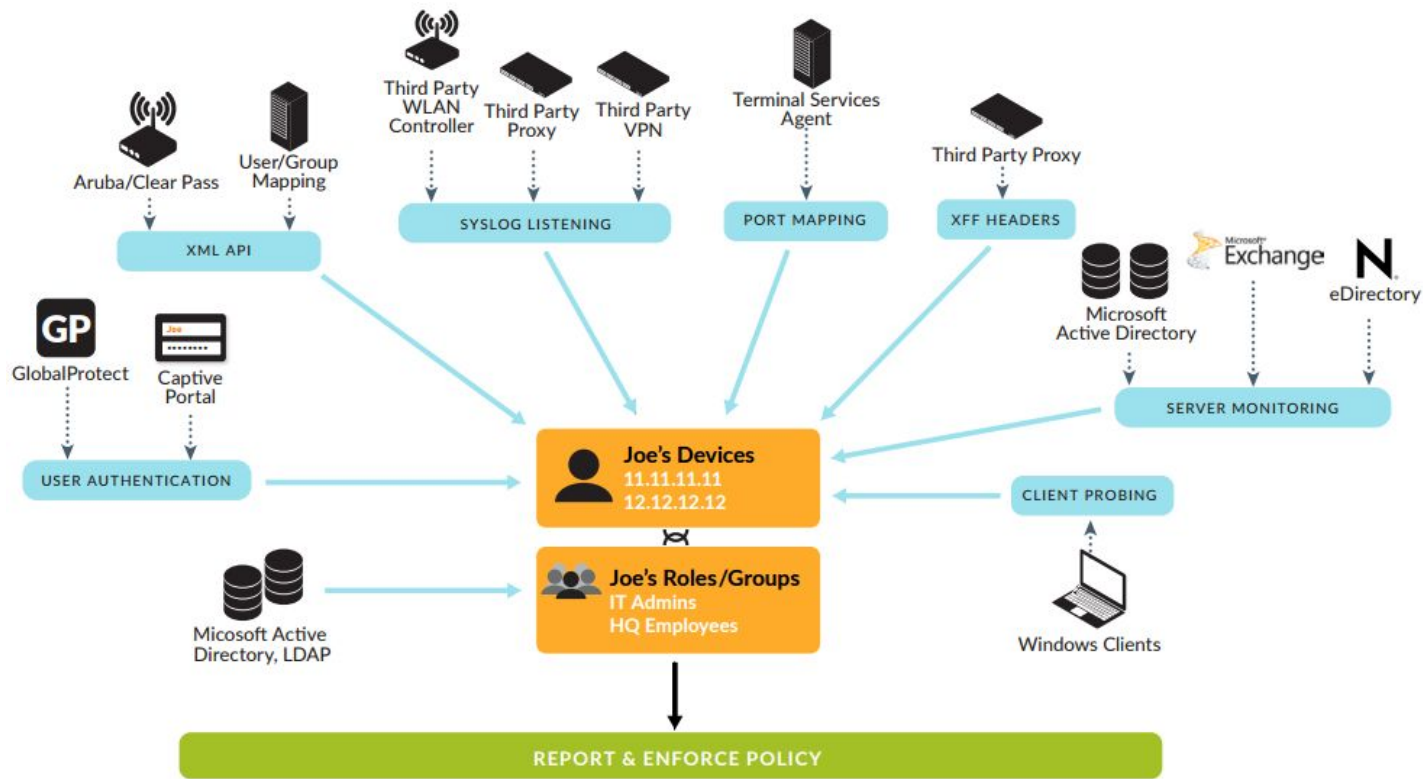
## Zero Trust - Content-ID

- Content-ID combines a real-time threat prevention engine with a comprehensive URL database and elements of application identification to limit unauthorized data and file transfers and detect and block a wide range of exploits, malware, dangerous web surfing as well as targeted and unknown threats. The application visibility and control delivered by App-ID, combined with the content inspection enabled by Content-ID means that IT departments can regain control over application traffic and related content.
- Threat Prevention and Advanced Threat Prevention
- Advanced URL Filtering

# Zero Trust - User-ID

- User-ID™ enables you to identify all users on your network using a variety of techniques to ensure that you can identify users in all locations using a variety of access methods and operating systems, including Microsoft Windows, Apple iOS, Mac OS, Android, and Linux®/UNIX. Knowing who your users are instead of just their IP addresses enables:
  - Visibility—Improved visibility into application usage based on users gives you a more relevant picture of network activity. The power of User-ID becomes evident when you notice a strange or unfamiliar application on your network.
  - Policy control—Tying user information to Security policy rules improves safe enablement of applications traversing the network and ensures that only those users who have a business need for an application have access.
  - Logging, reporting, forensics—If a security incident occurs, forensics analysis and reporting based on user information rather than just IP addresses provides a more complete picture of the incident.
- To enforce user- and group-based policies, the firewall must be able to map the IP addresses in the packets it receives to usernames. User-ID provides many mechanisms to collect this User Mapping information.

# Zero Trust - User-ID



# Zero Trust - User-ID







- User to Group Mapping
  - Add an LDAP Server Profile - Device -> Server Profile -> LDAP
  - Configure Group Mapping - Device -> User Identification -> Group Mapping Settings

- User to IP Mapping

The way you do this depends on where your users are located and what types of systems they are using, and what systems on your network are collecting login and logout events for your users. You must configure one or more User-ID agents to enable **User Mapping**:

- Configure User Mapping Using the Windows User-ID Agent.
- Configure User Mapping Using the PAN-OS Integrated User-ID Agent.
- Configure User-ID to Monitor Syslog Senders for User Mapping.
- Configure User Mapping for Terminal Server Users.
- Send User Mappings to User-ID Using the XML API.
- Insert Username in HTTP Headers.

# Zero Trust - User-ID

		RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP
		07/26 15:35:35	end	inside	outside	172.16.32.101	netadminlab\sue	
		07/26 15:35:35	end	inside	outside	172.16.32.101	netadminlab\sue	
		07/26 15:35:35	end	inside	outside	172.16.32.101	netadminlab\sue	
		07/26 15:35:35	end	inside	outside	172.16.32.101	netadminlab\sue	
		07/26 15:35:35	end	inside	outside	172.16.32.101	netadminlab\sue	
		07/26 15:35:35	end	tunnel_z...	inside	172.16.34.1	netadminlab\svc_paloalto	
		07/26 15:35:30	end	inside	outside	172.16.32.25		
		07/26 15:35:30	end	inside	outside	172.16.32.101		



# Zero Trust - Decryption

The Secure Sockets Layer (SSL) and Secure Shell (SSH) encryption protocols secure traffic between two entities, such as a web server and a client. SSL and SSH encapsulate traffic, encrypting data so that it is meaningless to entities other than the client and server with the certificates to affirm trust between the devices and the keys to decode the data. Decrypt SSL and SSH traffic to:

- Prevent malware concealed as encrypted traffic from being introduced into your network. For example, an attacker compromises a website that uses SSL encryption. Employees visit that website and unknowingly download an exploit or malware. The malware then uses the infected employee endpoint to move laterally through the network and compromise other systems.
- Prevent sensitive information from moving outside the network.
- Ensure the appropriate applications are running on a secure network.
- Selectively decrypt traffic; for example, create a Decryption policy and profile to exclude traffic for financial or healthcare sites from decryption.

Palo Alto Networks firewall decryption is policy-based, and can decrypt, inspect, and control inbound and outbound SSL and SSH connections. A Decryption policy enables you to specify traffic to decrypt by destination, source, service, or URL category, and to block, restrict, or forward the specified traffic according to the security settings in the associated Decryption profile. A Decryption profile controls SSL protocols, certificate verification, and failure checks to prevent traffic that uses weak algorithms or unsupported modes from accessing the network. The firewall uses certificates and keys to decrypt traffic to plaintext, and then enforces App-ID and security settings on the plaintext traffic, including Decryption, Antivirus, Vulnerability, Anti-Spyware, URL Filtering, WildFire, and File-Blocking profiles. After decrypting and inspecting traffic, the firewall re-encrypts the plaintext traffic as it exits the firewall to ensure privacy and security.

The firewall provides three types of Decryption policy rules: **SSL Forward Proxy** to control outbound SSL traffic, **SSL Inbound Inspection** to control inbound SSL traffic, and **SSH Proxy** to control tunneled SSH traffic. You can attach a Decryption profile to a policy rule to apply granular access settings to traffic, such as checks for server certificates, unsupported modes, and failures.

SSL decryption (both forward proxy and inbound inspection) requires certificates to establish the firewall as a trusted third party, and to establish trust between a client and a server to secure an SSL/TLS connection. You can also use certificates when excluding servers from SSL decryption for technical reasons (the site breaks decryption for reasons such as certificate pinning, unsupported ciphers, or mutual authentication). SSH decryption does not require certificates.



# Zero Trust - Decryption

- Set Goals
  - What traffic can and cannot be decrypted
- Work with Stakeholders
- Develop a Plan
  - PKI deployment
    - Windows CA
- Take a Baseline
  - Firewall sizing
  - CPU Utilization
- Plan a Staged Deployment
  - Few Users
  - Few users in different areas of the business
  - Larger subsets of users
  - Decrypt it ALL!!!

# Zero Trust - Decryption

- Configure Certificates
- Configure Decryption Profiles
  - SSL Inbound Inspection
  - SSL Forward Proxy
  - SSH Proxy
  - No-Decryption Profile
- Configure Decrypt and Non-Decrypt Policies
- SSL Decryption Exclusion List
  - Predefined list from Palo Alto
- Block Google Quick UDP Internet Connections Protocol (QUIC)
- Forward decrypted SSL traffic to Wildfire

# Certificates

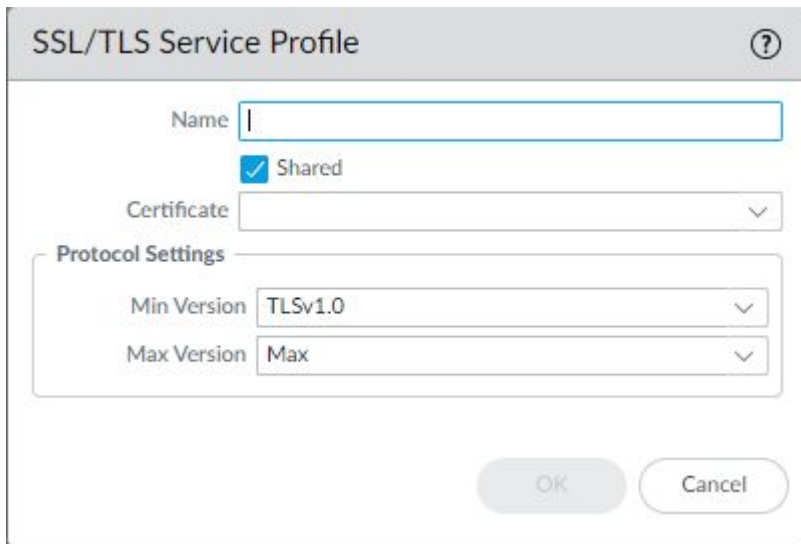
- Example:
  - Deploy a Microsoft Windows Server Enterprise Certificate Authority (CA and Web)
  - Generate a Certificate Request - Device -> Certificate Management -> Certificates



- Get a certificate from the Windows CA Web Portal
- Deploy Certificates to all AD managed users and computers via GPO
- Works for decryption and Global Protect

# Certificates - Continued

- Configure an SSL/TLS Service Profile
  - Device -> Certificate Management -> SSL/TLS Service Profile



The screenshot shows a configuration window titled "SSL/TLS Service Profile" with a help icon (question mark) in the top right corner. The window contains the following fields and options:

- Name:** A text input field with a vertical cursor.
- Shared:** A checkbox that is checked, with the label "Shared" to its right.
- Certificate:** A dropdown menu with a downward arrow.
- Protocol Settings:** A section containing two dropdown menus:
  - Min Version:** Set to "TLSv1.0".
  - Max Version:** Set to "Max".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

# Decryption Profile

- Create a Decryption Profile
  - Objects -> Decryption -> Decryption Profile

Decryption Profile

Name

Recommended\_Decryption\_Profile

☒ Shared

Decryption Mirroring

Interface

None

☐ Forwarded Only

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

☐ Append certificate's CN value to SAN extension

Details

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.

OK

Cancel

# Decryption Policy

- Create a Decryption Policy
  - Policies -> Decryption

Decryption Policy Rule

General

Source

Destination

Service/URL Category

Options

Target

Action

Decrypt

Type

SSL Forward Proxy

Decryption Profile

Recommended\_Decryption\_Profile

Log Settings

☐ Log Successful SSL Handshake

☒ Log Unsuccessful SSL Handshake

Log Forwarding

default

Packet Broker Profile

None

To decrypt and forward TLS traffic on PAN-OS (Seattle version or later), use Network packet Broker Policy. Decryption Broker configurations work only on PAN-OS 10.0 and earlier.

OK

Cancel

# Block Google QUIC

Service

Name

quic\_udp\_ports

Description

Protocol

☐ TCP

☒ UDP

Destination Port

80, 443

Source Port

Port can be a single port #, range (1-65535), or comma separated (80, 8080, 443)

Session Timeout

☒ Inherit from application

☐ Override

Tags

OK

Cancel

PA-220

DASHBOARD

ACC

MONITOR

POLICIES

OBJECTS

NETWORK

DEVICE

Commit

Security

NAT

QoS

Policy Based Forwarding

Decryption

Tunnel Inspection

Application Override

Authentication

DoS Protection

SD-WAN

NAME

TAGS

TYPE

ZONE

ADDRESS

USER

DEVICE

ZONE

ADDRESS

DEVICE

APPLICATION

SERVICE

ACTION

1

Block QUIC UDP

none

universal

I3-vlan-trust

Sinkhole

any

any

any

any

I3-untrust

any

any

any

quic\_udp\_ports

Deny

2

Block QUIC

none

universal

I3-vlan-trust

Sinkhole

any

any

any

any

I3-untrust

any

any

quic

application-default

Deny

# Expedition



# Expedition

## EXPEDITION



Expedition is the fourth evolution of the Palo Alto Networks Migration Tool. The purpose of this tool is to help reduce the time and efforts of migrating a configuration from a supported vendor to Palo Alto Networks.

By using Expedition, everyone can convert a configuration from Checkpoint, Cisco, or any other vendor to a PAN-OS and give you more time to improve the results. Expedition 3 added some functionalities to allow our customers to enforce security policies based on App-ID and User-ID as well. [READ MORE](#)

**NOTE:** Expedition is supported by the community as best effort. The Palo Alto Networks TAC does not provide support, so please post your questions in the [Expedition discussions](#) area.

- [Expedition Live Page](#)

# Expedition



# Resources

# Resources

- [Palo Alto Technical Documentation](#)
- [Compatibility Matrix](#)
- [Applipedia](#)
- [Optics Datasheet](#)
- [PA Series Hardware Architectures](#)
- [Cyberpedia](#)

**Questions?**

**Thank You!**