

# Basic Firewall Configuration

---

Version 1.0



# Agenda

- Platform
- Ways to Manage
- Configuration Management
- Initial Configuration
- Interfaces
- Zones
- DHCP
- NAT
- Objects
- Licenses and Profiles
- Security Policies
- Routing
- Policy Based Forwarding
- USER-ID
- Troubleshooting
- Resources

# Platform

# Palo Alto Networks Portfolio

<b>Strata PA-Series</b>
<b>ML-Powered Next-Generation Firewall</b>
App-ID   User-ID   Content-ID   Device-ID
<b>VM-Series</b>
<b>Virtual Next-Generation Firewall</b>
App-ID   User-ID   Content-ID   Device-ID
<b>CN-Series</b>
<b>Containerized Next-Generation Firewall</b>
App-ID   User-ID   Content-ID   Device-ID
<b>Panorama</b>
<b>Firewall Management</b>

<b>Prisma Access</b>
<b>Secure Access Service Edge</b>
FWaaS   Secure Web Gateway   ZTNA   Next-Gen CASB
<b>Prisma SD-WAN</b>
<b>Next-Generation SD-WAN</b>
SD-WAN
<b>Prisma Cloud</b>
<b>Cloud Native Application Protection Platform</b>
Cloud Security Posture Management   Cloud Workload Protection   Cloud Network Security   Cloud Infrastructure Entitlement Management   Cloud Code Security

<b>Cortex XDR</b>
<b>Extended Detection and Response</b>
Endpoint Threat Prevention   Endpoint Detection & Response   Behavioral Analytics   Managed Detection & Response
<b>Cortex XSOAR</b>
<b>Extended Security Orchestration, Automation and Response</b>
Security Orchestration, Automation & Response   Threat Intelligence Management
<b>Cortex Xpanse</b>
<b>Attack Surface Management</b>
Internet-Connected Asset Discovery & Mitigation

Cloud-Delivered Security Services									
<b>DNS Security</b> ● ●	<b>ADV Threat Prevention</b> ● ● ●	<b>ADV URL Filtering</b> ● ●	<b>WildFire</b> ● ● ●	<b>IoT Security</b> ● ● ●	<b>GlobalProtect</b> ● ●	<b>SD-WAN</b> ● ●	<b>DLP</b> ● ●	<b>SaaS Security</b> ● ●	<b>Data Lake</b> ● ● ●
DNS Attack Prevention	Exploit, Malware, C2 Prevention	Malicious Site & Phishing Prevention	Malware Prevention	Enterprise IoT Security	Mobile User Security	Secure Branch Connectivity	Data Protection & Compliance	In-line & API SaaS Application Security	Cloud Logging Service

Unit 42 Security Consulting Services				
<b>Incident Response</b>	<b>Digital Forensics</b>	<b>Proactive Services</b>	<b>Exec &amp; BoD Advisory</b>	<b>Cybersecurity Services</b>
Ransomware   BEC   Cloud   APT   PCI	Forensics   Insider Threat   Expert Witness	Ransomware   BEC   Cyber Risk Breach Assessments	vCISO   Program Design Strategy Review   M&A	Data Breach Response   Cyber Risk & Resilience Management   Incident Response Services

# Platform Components



## Panorama Management

### Security Subscriptions



APP-ID



Content-ID



Device-ID

**PAN-OS**



User-ID



Cloud Identity



Decryption

**Hardware  
PA-Series**

**Software  
VM-Series / CN-Series**

**Cloud Service  
Prisma Access**

# Hardware: PA-Series

## World's First Machine Learning-Powered Next Generation Firewall

### PA-400 Series



#### PA-460

4.4 Gbps App-ID



#### PA-450

2.9 Gbps App-ID



#### PA-445

2.2 Gbps App-ID



#### PA-440

2.2 Gbps App-ID



#### PA-415

1.2 Gbps App-ID



#### PA-410

1.1 Gbps App-ID

### PA-1400 Series



#### PA-1420

9.5 Gbps App-ID



#### PA-1410

6.8 Gbps App-ID

### PA-3400 Series



#### PA-3440

24 Gbps App-ID



#### PA-3430

20.5 Gbps App-ID



#### PA-3420

16.9 Gbps App-ID



#### PA-3410

11 Gbps App-ID

### PA-5400 Series



#### PA-5440

72 Gbps App-ID



#### PA-5430

61 Gbps App-ID



#### PA-5420

56 Gbps App-ID



#### PA-5410

43.5 Gbps App-ID

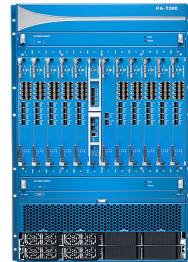
### PA-5450



#### PA-5450

Up to 200 Gbps App-ID

### PA-7000 Series



#### PA-7080

635 Gbps App-ID



#### PA-7050

384 Gbps App-ID

Small Branches

Network Perimeter

Large Data Centers

# Platform

## Firewall Types

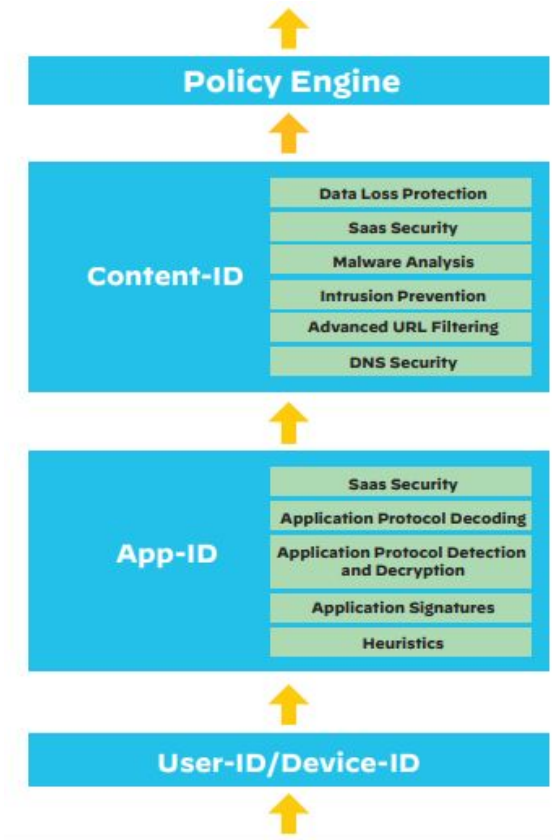
- Physical
  - Subscriptions (CDSS)/Bundles
    - Core Security Bundle
      - Advanced Threat Prevention
      - Advanced Wildfire
      - Advanced URL
      - DNS Security
      - SD-WAN
    - Globalprotect
  - Support
- Software (NGFW Credits)
  - On Premise
  - Cloud

# Platform

Firewalls: Packet Flow

Single Pass Parallel Processing

Packet Flow Processing





# Ways to Manage

# Ways to Manage

- Console
- CLI
- Web GUI
- API
- Panorama
- Strata Cloud Manager



Management

Console

# Ways to Manage

CLI:

```
admin@PA440-WAN> show interface management
|           Pipe through a command
<Enter>    Finish input

admin@PA440-WAN> show interface management

-----
Name: Management Interface
Link status:
  Runtime link speed/duplex/state: 1000/full/up
  Configured link speed/duplex/state: auto/auto/auto
MAC address:
  Port MAC address 8c:36:7a:02:c6:46

Ip address: 192.168.18.13
Netmask: 255.255.255.0
Default gateway: 192.168.18.1
Ipv6 address: unknown
Ipv6 link local address: fe80::8e36:7aff:fe02:c646/64
Ipv6 default gateway:
-----
```

# Ways to Manage

## Rest-API:

- You can view the full list of resources in the REST API Reference on the firewall at [https://<IP\\_address>/restapi-doc](https://<IP_address>/restapi-doc).

### List Ethernet Interfaces

Get Ethernet Interfaces.

#### QUERY PARAMETERS

name	string The name of the entry
location	string Value: "panorama-pushed"
output-format	string Default: "json" Enum: "json" "xml" Specify the output format to be JSON or XML. This is equivalent to setting the <code>Accept</code> header to <code>application/json</code> or <code>application/xml</code> . If you include both <code>output-format</code> and <code>Accept</code> header, the value of <code>output-format</code> will override the header.

GET /restapi/v10.2/Network/EthernetInterfaces

Response samples

200 400 401 403 404 default

Content type  
application/json

Copy Expand all Collapse all

```
{
  "@status": "success",
  "@code": "19",
  "result": {
    "@count": "1",
    + "entry": [ - ]
  }
}
```

# Configuration Management

# Configuration Management

- Candidate Configuration - Configuration before a commit
- Running Configuration - Configuration after a commit

### Commit ?

Doing a commit will overwrite the running configuration with the commit scope..

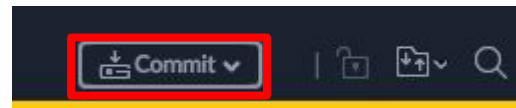
Commit All Changes  Commit Changes Made By: (1) admin

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
▶ policy-and-objects	Policy and Objects			
▶ device-and-network	Device and Network Configuration			

[Preview Changes](#) [Change Summary](#) [Validate Commit](#)

Note: This shows all the changes in login admin's accessible domain.

Description



# Configuration Management

- Commit All Changes
- Commit Changes Made by current user




Commit

Doing a commit will overwrite the running configuration with the commit scope.

Commit All Changes  Commit Changes Made By: (1) admin

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
▼ policy-and-objects	Policy and Objects			
outside		tag		admin
inside		tag		admin
Allowed URLs		Others		admin
default-1		Others		admin
dmz		tag		admin
Custom-URL-Profile		Others		admin
▶ device-and-network	Device and Network Configuration			

# Configuration Management

 Preview Changes  Change Summary  Validate Commit

Note: This shows all the changes in login admin's accessible domain.

Description

Recommended

## Device Config Audit (WAN-VM)

Wed Jan 24 14:27:33 CST 2024

Legend: Added Modified Deleted

Local Device Changes	
Running Configuration	Candidate Configuration
260 dampening-profile {	260 dampening-profile {
261 default {	261 default {
262 cutoff 1.25;	262 cutoff 1.25;
263 reuse 0.5;	263 reuse 0.5;
264 max-hold-time 900;	264 max-hold-time 900;
265 decay-half-life-reachable 300;	265 decay-half-life-reachable 300;
266 decay-half-life-unreachable 900;	266 decay-half-life-unreachable 900;
267 enable yes;	267 enable yes;
268 }	268 }
269 }	269 }
&nbsp;	270 routing-options {
&nbsp;	271 graceful-restart {
&nbsp;	272 enable yes;
&nbsp;	273 }
&nbsp;	274 }
&nbsp;	275 }
&nbsp;	276 rip {
&nbsp;	277 enable no;
&nbsp;	278 }
&nbsp;	279 ospf {
&nbsp;	280 enable no;

## Preview Changes

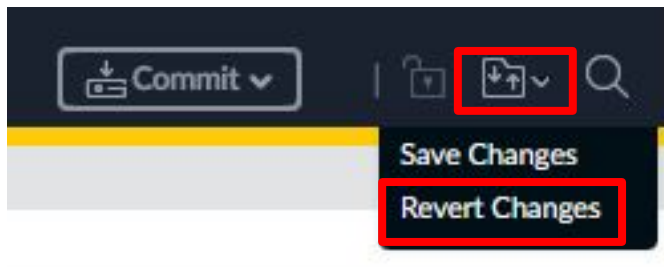
Lines of Context



# Configuration Management

Revert candidate configuration changes:

- Remove changes made to the candidate configuration
- This is done before you commit changes



# Configuration Management

Backing up a configuration:

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE**

Setup

High Availability  
Config Audit  
Password Profiles  
Administrators  
Admin Roles  
Authentication Profile  
Authentication Sequence  
User Identification  
IoT  
Data Redistribution  
Device Quarantine  
VM Information Sources  
Troubleshooting  
Certificate Management  
Certificates

Management **Operations** Services | Interfaces | Telemetry | Content-ID | WildFire | Session

Configuration Management

- Revert Revert to last saved configuration  
Revert to running configuration
- Save **Save named configuration snapshot** Save a configuration by name  
Save candidate configuration
- Load Load named configuration snapshot  
Load configuration version
- Export **Export named configuration snapshot** Export the running or named configuration  
Export configuration version  
Export device state
- Import Import named configuration snapshot  
Import device state

# Configuration Management

Restore a configuration:

The screenshot shows the PA-VM Configuration Management interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE'. The left sidebar contains 'Setup' and various configuration categories. The main content area is titled 'Configuration Management' and lists several actions: Revert, Save, Load, Export, and Import. The 'Load' action is highlighted with a red box, and the 'Import' action is highlighted with a cyan box. A red box also highlights the 'Operations' tab in the top navigation bar.

Action	Description
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

Load a configuration into the current candidate configuration

Imports a named configuration (change name if running-config.xml)

# Configuration Management

XML vs Set view:

- Exported configurations are in XML format
- [XML Basics](#)
  
- Set commands are used to configure a firewall via CLI or Console

View the configuration as a set command or XML format in the CLI or Console:

- "set" format: > set cli config-output-format set
- "xml" format: > set cli config-output-format xml

# Configuration Management

## XML Format (default)

```
admin@PA440-WAN# show
deviceconfig {
  system {
    hostname PA440-WAN;
    timezone US/Central;
    login-banner "You have accessed a protected system. Log off immediately if you are not an authorized user.";
    ntp-servers {
      primary-ntp-server {
        ntp-server-address 0.pool.ntp.org;
      }
      secondary-ntp-server {
        ntp-server-address 1.pool.ntp.org;
      }
    }
    snmp-setting {
      access-setting {
        version {
          v3;
        }
      }
    }
    update-schedule {
      threats {
        recurring {
          every-30-mins {
            at 2;
            action download-and-install;
          }
        }
      }
    }
  }
}
```

# Configuration Management

Set command format:

```
admin@PA440-WAN# show
set deviceconfig system hostname PA440-WAN
set deviceconfig system timezone US/Central
set deviceconfig system login-banner "You have accessed a protected system. Log off immediately if you are not an authorized user."
set deviceconfig system ntp-servers primary-ntp-server ntp-server-address 0.pool.ntp.org
set deviceconfig system ntp-servers secondary-ntp-server ntp-server-address 1.pool.ntp.org
set deviceconfig system snmp-setting access-setting version v3
set deviceconfig system update-schedule threats recurring every-30-mins at 2
set deviceconfig system update-schedule threats recurring every-30-mins action download-and-install
set deviceconfig system update-schedule threats recurring threshold 48
```

# Initial Configuration

# Initial Configuration

## Management Interface Configuration:

- Default IP Address 192.168.1.1/24

## Static IP Address

- Set new IP Address and Netmask
- Set Default-Gateway
- Set DNS Servers

## DHCP IP Address

- Receive all information from a DHCP Server



# Initial Configuration

CLI Configuration for Static IP Address on Management Interface:

```
configure
set deviceconfig system type static
set deviceconfig system ip-address <IP_Address> netmask <Net_Mask>
set deviceconfig system default-gateway <Gateway>
set deviceconfig system dns-setting servers primary <dns-server>
set deviceconfig system dns-setting servers secondary <dns-server>
commit
exit
```

# Initial Configuration

GUI Configuration for Management Interface:

The screenshot displays the Palo Alto Networks PA-VM GUI. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE'. The 'DEVICE' tab is selected. On the left sidebar, the 'Setup' menu is expanded, showing options like 'High Availability', 'Config Audit', 'Password Profiles', and 'Administrators'. The main content area shows a breadcrumb trail: 'Management | Operations | Services | Interfaces | Telemetry | Content-ID | WildFire | Session | HSM | ACE | DLP'. The 'Interfaces' tab is active, displaying a table with the following data:

INTERFACE NAME	ENABLED	SPEED
Management	<input checked="" type="checkbox"/>	auto-negotiate

# Initial Configuration

## Management Interface Settings

IP Type  Static  DHCP Client

IP Address 192.168.18.31

Netmask 255.255.255.0

Default Gateway 192.168.18.1

IPv6 Address/Prefix Length

Default IPv6 Gateway

Speed auto-negotiate

MTU 1500

### Administrative Management Services

HTTP

Telnet

HTTPS

SSH

### Network Services

HTTP OCSP

SNMP

User-ID Syslog Listener-SSL

Ping

User-ID

User-ID Syslog Listener-UDP

# Initial Configuration

The screenshot displays the Palo Alto VM configuration interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE'. The 'DEVICE' tab is selected. On the left sidebar, the 'Setup' menu is expanded, and the 'Services' sub-tab is selected. The main content area shows the 'Services' configuration page, which includes a settings gear icon in the top right corner. The configuration details are as follows:

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

# Initial Configuration

## Services

### Services

### NTP

Update Server



Verify Update Server Identity

### DNS Settings

DNS



Servers



DNS Proxy Object

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

## Services



### Services

### NTP

#### Primary NTP Server

NTP Server Address

0.pool.ntp.org

Authentication Type

None



#### Secondary NTP Server

NTP Server Address

1.pool.ntp.org

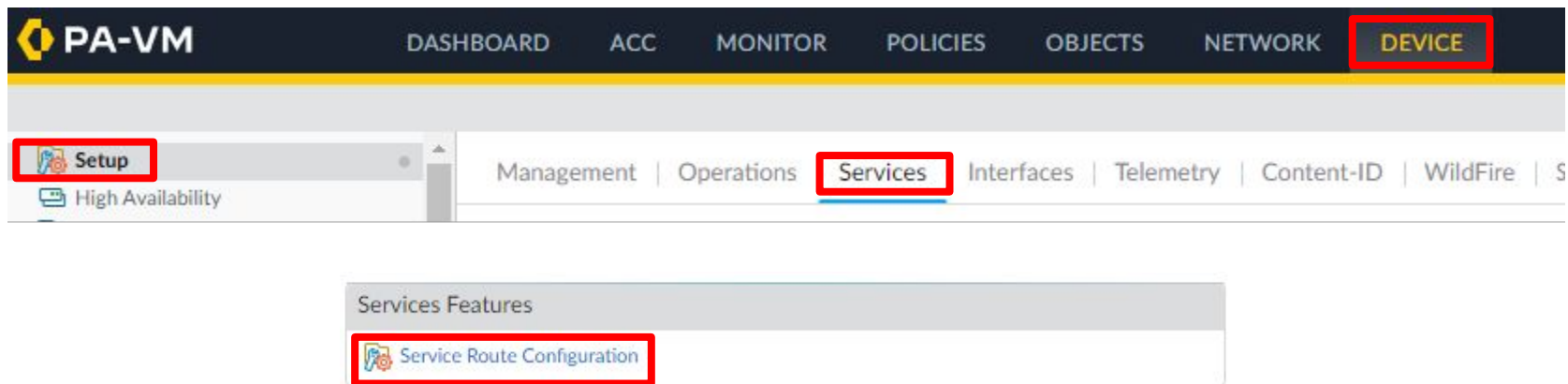
Authentication Type

None



# Initial Configuration

Service Routes:



# Initial Configuration

### Service Route Configuration ?

Use Management Interface for all  Customize

IPv4 | IPv6 | Destination

<input type="checkbox"/>	SERVICE	SOURCE INTERFACE	SOURCE ADDRESS
<input type="checkbox"/>	AutoFocus	Use default	Use default
<input type="checkbox"/>	CRL Status	Use default	Use default
<input type="checkbox"/>	Data Services	Use default	Use default
<input type="checkbox"/>	DDNS	Use default	Use default
<input type="checkbox"/>	Panorama pushed updates	Use default	Use default
<input type="checkbox"/>	DNS	Use default	Use default
<input type="checkbox"/>	External Dynamic Lists	Use default	Use default
<input type="checkbox"/>	Email	Use default	Use default
<input type="checkbox"/>	HSM	Use default	Use default
<input type="checkbox"/>	HTTP	Use default	Use default
<input type="checkbox"/>	IoT	Use default	Use default
<input type="checkbox"/>	Kerberos	Use default	Use default

Set Selected Service Routes

### Service Route Source ?

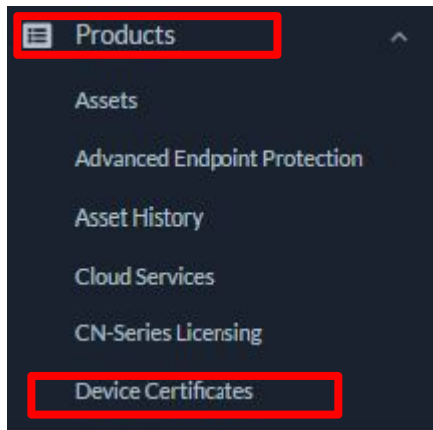
Service

Source Interface

Source Address

# Initial Configuration

Device Certificate:



## One Time Password

Choose the "One-Time Password" option if:

1. You are manually managing the Firewalls (Hardware/VM-Series).
2. You are using the Panorama to manage the Firewalls (Hardware/VM-Series).
3. You have Panorama (Hardware/VM-Series).

[View OTP History](#)

[Generate OTP](#)



# Initial Configuration

Device Number

Generate OTP for a Next-Gen Firewall (PanOS)

Generate OTP for a Panorama

Generate OTP for Panorama managed devices

Generate OTP for WF-500 devices

Cancel **Next**

## Generate OTP for a Next-Gen Firewall (PanOS)

OTP provides users the password to input into the PAN-OS device.

This is a required step to enable secured use of the PAN-OS device for some functions.

The password is valid for a limited time.

If the time expires before you use this password, please generate a new password.

\* PAN-OS Device:

Cancel Back **Generate OTP**



# Initial Configuration

Import the OTP: CLI

You can also install the device certificate from the **firewall CLI** using the command:

```
admin>request certificate fetch otp <otp_value>
```

The screenshot displays the Palo Alto Networks PA-VM management interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE', with 'DEVICE' highlighted. Below this, a secondary navigation bar shows 'Setup' (highlighted), 'Management' (highlighted), 'Operations', 'Services', 'Interfaces', 'Telemetry', 'Content-ID', 'WildFire', and 'Ses'. The main content area is titled 'Device Certificate' and displays the message 'Last Fetched Message Device certificate not found'. A 'Get certificate' button is visible at the bottom of the message area.

# Initial Configuration

Device Certificate Validation:

The screenshot shows the top navigation bar of the Palo Alto VM interface. The 'DEVICE' tab is highlighted in red. Below it, the 'Setup' and 'Management' sub-menus are also highlighted in red. The 'Management' sub-menu is expanded, showing options like Operations, Services, Interfaces, Telemetry, Content-ID, WildFire, and Ses.

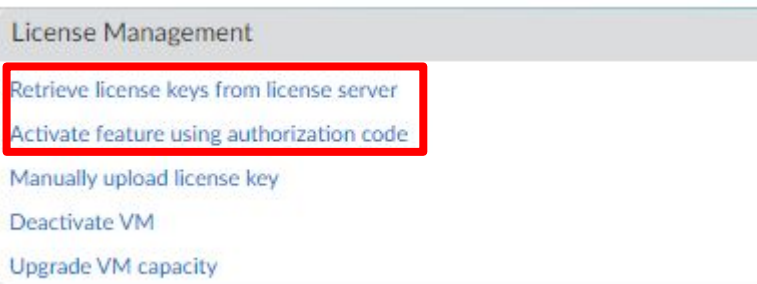
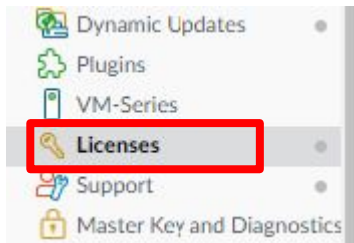
The screenshot shows the 'Device Certificate' page. The 'Current Device Certificate Status' is highlighted in red and shows 'Valid'. Below this, there are several fields with their values:

Current Device Certificate Status	Valid
Not Valid Before	2023/12/08 04:03:49 CST
Not Valid After	2024/03/07 04:03:48 CST
Last Fetched Message	Successfully fetched Device Certificate
Last Fetched Status	success
Last Fetched Timestamp	2023/12/08 04:13:49 CST

At the bottom of the page, there is a 'Get certificate' button.

# Initial Configuration

License the firewall: Device -> Licenses

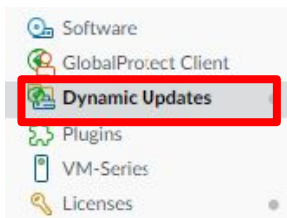


Premium	
Date Issued	March 20, 2023
Date Expires	November 14, 2024
Description	24 x 7 phone support; advanced replacement hardware service

WildFire License	
Date Issued	March 20, 2023
Date Expires	November 14, 2024
Description	WildFire signature feed, integrated WildFire logs, WildFire API

# Initial Configuration

## Dynamic Updates: Device -> Dynamic Updates



VERSION ^	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED	ACTION
∨ Applications and Threats	Last checked: 2024/01/16 17:04:06 CST Schedule: Every Wednesday at 01:02 (Download only)								
8791-8464	panupv2-all-contents-8791-8464	Apps, Threats	Full	76 MB	e398e1db9b8729...	2023/12/18 15:25:59 CST			Download
8792-8469	panupv2-all-contents-8792-8469	Apps, Threats	Full	76 MB	d1469dd23f5408...	2023/12/19 16:38:55 CST			Download
8793-8478	panupv2-all-contents-8793-8478	Apps, Threats	Full	76 MB	bb01505fbcaa9e...	2023/12/27 14:33:32 CST			Download
8795-8489	panupv2-all-contents-8795-8489	Apps, Threats	Full	76 MB	717744f8cd8feaa...	2024/01/08 12:26:00 CST			Download
8796-8491	panupv2-all-contents-8796-8491	Apps, Threats	Full	76 MB	917f47a2bda325...	2024/01/09 10:50:27 CST			Download
8797-8498	panupv2-all-contents-8797-8498	Apps, Threats	Full	77 MB	b996d57bf5d3c1...	2024/01/12 14:58:30 CST			Download
∨ GlobalProtect Clientless VPN	Last checked: 2024/01/16 17:04:12 CST Schedule: None								
98-260	panup-all-gp-98-260	GlobalProtectClientlessV...	Full	77 KB	52ef80beb11d00...	2023/05/22 17:41:22 CDT			Download
∨ Device Dictionary	Last checked: 2024/01/16 17:04:08 CST								
107-458	panup-all-deviceid-107-458	IoT	Full	204 KB	ef96b8a528944f7...	2023/12/22 17:14:26 CST			
108-460	panup-all-deviceid-108-460	IoT	Full	204 KB	9f2fe8468061f71...	2023/12/29 13:37:56 CST			
109-462	panup-all-deviceid-109-462	IoT	Full	204 KB	91819e632a9396...	2024/01/04 16:31:12 CST			
110-464	panup-all-deviceid-110-464	IoT	Full	205 KB	301b6a5e18080c...	2024/01/11 10:28:40 CST			
∨ WildFire	Last checked: 2024/01/16 17:04:11 CST Schedule: None								
839107-842935	panupv3-all-wildfire-839107-842935	PAN OS 10.0 And Later	Full	8 MB	885442387929f7...	2024/01/16 17:02:14 CST			Download

# Initial Configuration

Dynamic Updates: Device -> Dynamic Updates

- | DOWNLOADED | CURRENTLY INSTALLED | ACTION  |
|------------|---------------------|---|
|            |                     | Download  |
|            |                     | Download  |
|            |                     | Download  |
|            |                     | Download  |
|            |                     | Download  |
| ✓          |                     | Install<br>Review Policies<br>Review Apps<br>Export |
- |   |   |  |
|---|---|--|
| ✓ | ✓ | Review Policies<br>Review Apps<br>Export |
|---|---|--|
- |           |        |                   |
|-----------|--------|-------------------|
| Check Now | Upload | Install From File |
|-----------|--------|-------------------|

VERSION ^	FILE NAME	
∨ Antivirus		Last checked: 2024/01/16 17:14:04 CST Schedule: None
4695-5213	panup-all-antivirus-4695-5213	
4696-5214	panup-all-antivirus-4696-5214	
4697-5215	panup-all-antivirus-4697-5215	
4698-5216	panup-all-antivirus-4698-5216	
4699-5217	panup-all-antivirus-4699-5217	
∨ Applications and Threats		Last checked: 2024/01/16 17:13:59 CST Sched
8791-8464	panupv2-all-contents-8791-8464	
8792-8469	panupv2-all-contents-8792-8469	
8793-8478	panupv2-all-contents-8793-8478	
8795-8489	panupv2-all-contents-8795-8489	
8796-8491	panupv2-all-contents-8796-8491	
8797-8498	panupv2-all-contents-8797-8498	

# Interfaces



# Interfaces

## Interface Types:

- Tap
- Virtual Wire
- Layer 2
- Layer 3
- Aggregate Ethernet
- HA
- Decrypt Mirror

# Interfaces

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Interfaces Ethernet VLAN | Loopback | Tunnel | SD-WAN

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE
ethernet1/1				none	none	Untagged	none	none
ethernet1/2				none	none	Untagged	none	none
ethernet1/3				none	none	Untagged	none	none
ethernet1/4				none	none	Untagged	none	none
ethernet1/5				none	none	Untagged	none	none
ethernet1/6				none	none	Untagged	none	none

# Interfaces

Tap Interface:

Ethernet Interface

Interface Name

Comment

**Interface Type**

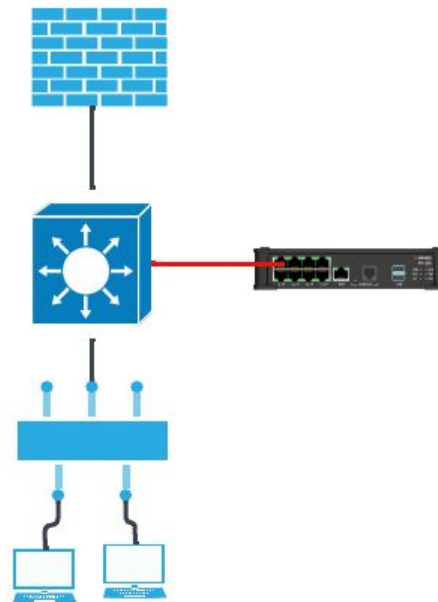
Netflow Profile

**Config** | Advanced

Assign Interface To

**Security Zone**

Add a Zone for the interface



# Interfaces

vWire Interface:

Ethernet Interface ?

Interface Name ethernet1/8

Comment

Interface Type Virtual Wire

Netflow Profile None

**Config** | Advanced

Assign Interface To

Virtual Wire None

Security Zone None

New Virtual Wire

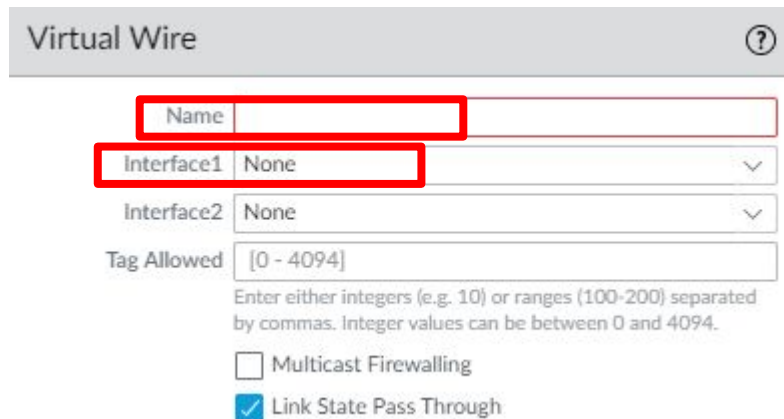
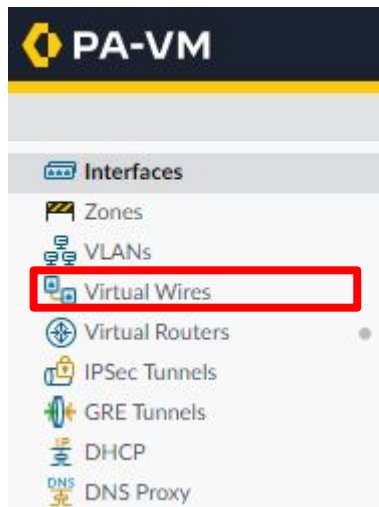
OK Cancel

Add a Zone for the interface



# Interfaces

vWire Interface:



# Interfaces

## Layer 2 Interface: Create VLAN



VLAN ?

Name

VLAN Interface

Static MAC Configuration

INTERFACES ^		MAC ADDRESS	INTERFACE
+ Add - Delete		+ Add - Delete	

# Interfaces

Layer 2 Interface:

The screenshot shows the PA-VM web interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK' (highlighted with a red box), and 'DEVICE'. On the left sidebar, 'Interfaces' is highlighted with a red box, with sub-items 'Zones', 'VLANs', and 'Virtual Wires'. The main content area shows 'Ethernet' (highlighted with a red box) as the selected interface type, with 'VLAN', 'Loopback', 'Tunnel', and 'SD-WAN' as options. Below this is a search bar and a table with several empty columns.

# Interfaces

Layer 2 Interface: Single VLAN

Ethernet Interface ?

Interface Name

Comment

Interface Type


Netflow Profile

**Config** | Advanced

Assign Interface To

VLAN

Security Zone

- None
- VLAN10
- New  VLAN



# Interfaces

Layer 2 Interface: Multiple VLANs

Select the Interface and at the bottom of the page select:

 + Add Subinterface

Layer2 Subinterface ?

Interface Name ethernet1/5 10

Comment





Tag 10

Netflow Profile None

Assign Interface To

VLAN VLAN10

Security Zone None

 ethernet1/5	▼	Layer2		none	none	Untagged	none
 ethernet1/5.10		Layer2		none	none	10	VLAN10

# Interfaces

Layer 2 Interface: VLAN Interface

The screenshot displays the Palo Alto Networks PA-VM web interface. The top navigation bar includes the PA-VM logo and menu items: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, and NETWORK. The NETWORK menu item is highlighted with a red box. On the left sidebar, the Interfaces menu item is also highlighted with a red box. Below the sidebar, the main content area shows navigation options: Ethernet, VLAN (highlighted with a red box), Loopback, Tunnel, and SD-WAN. A search bar is visible below these options.

# Interfaces

## Layer 2 Interface: VLAN Interface

VLAN Interface ?

Interface Name  .

Comment

Netflow Profile  ▾

**Config** | IPv4 | IPv6 | Advanced

Assign Interface To

VLAN  ▾

Virtual Router  ▾

Security Zone  ▾

# Interfaces

## Layer 2 Interface: VLAN Interface

VLAN Interface ?

Interface Name  .

Comment

Netflow Profile  ▼

Config **IPv4** | IPv6 | Advanced

Type  Static  DHCP Client

<input type="checkbox"/>	IP
<input checked="" type="checkbox"/>	10.0.1.1/24 <span>▼</span>
<input type="text" value="New Address"/>	
<input checked="" type="checkbox"/>	<input type="text"/>

Add  Delete

IP address/netmask. Ex. 192.168.2.254/24

# Interfaces

Layer 3 Interface:

Ethernet Interface ?

Interface Name

Comment

Interface Type **Layer3**

Netflow Profile

**Config** | IPv4 | IPv6 | SD-WAN | Advanced

Assign Interface To

Virtual Router	None
Security Zone	None

OK Cancel

Add a Zone and VR for the interface

# Interfaces

Layer 3 Interface:

Ethernet Interface ?

Interface Name

Comment

Interface Type

Netflow Profile

Config **IPv4** | IPv6 | SD-WAN | Advanced

Enable SD-WAN

Type  Static  PPPoE  DHCP Client

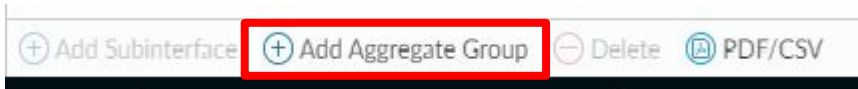
<input type="checkbox"/>	IP
<input checked="" type="checkbox"/>	10.0.1.1/24
	<input type="button" value="New Address"/>
<input checked="" type="button" value="+ Add"/>	<input type="button" value="- Delete"/> <input type="button" value="↑ Move Up"/> <input type="button" value="↓ Move Down"/>

# Interfaces

Port Aggregation:

Needs to be Physical hardware.

Select the interfaces you want to aggregate.



# Interfaces

Port Aggregation:

Aggregate Ethernet Interface ?

Interface Name

Comment

Interface Type

Netflow Profile

**Config** | IPv4 | IPv6 | LACP | SD-WAN | Advanced

Assign Interface To

Virtual Router

Security Zone

Add a Zone and VR  
for the interface



# Interfaces

Port Aggregation:

Config | IPv4 | IPv6 | **LACP** | SD-WAN | Advanced

Enable LACP

Mode  Passive  Active

Transmission Rate  Fast  Slow

Fast Failover

System Priority

Maximum Interfaces

# Interfaces

Port Aggregation:

### Ethernet Interface ?

Interface Name

Comment

Interface Type

Aggregate Group

#### Advanced

Link Settings

Link Speed  Link Duplex  Link State

LACP Port Priority

# Interfaces

Interface Management Profiles:



# Interfaces

## Interface Management Profiles:

Interface Management Profile ?

Name

**Administrative Management Services**

- HTTP
- HTTPS
- Telnet
- SSH

**Network Services**

- Ping
- HTTP OCSP
- SNMP
- Response Pages
- User-ID
- User-ID Syslog Listener-SSL
- User-ID Syslog Listener-UDP

**PERMITTED IP ADDRESSES**

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6  
2001:db8:123:1::1 or 2001:db8:123:1::/64

# Interfaces

## Interface Management Profile: Apply to the Interface

### Ethernet Interface ?

Interface Name

Comment

Interface Type

Netflow Profile

Config | IPv4 | IPv6 | SD-WAN | **Advanced**

#### Link Settings

Link Speed

Link Duplex

Link State

**Other Info** | ARP Entries | ND Entries | NDP Proxy | LLDP | DDNS | Cluster

Management Profile

MTU

Adjust TCP MSS

IPv4 MSS Adjustment | 40

# Zones

# Zones

Security zones are a logical way to group physical and virtual interfaces on the firewall to control and log the traffic that traverses specific interfaces on your network. An interface on the firewall must be assigned to a security zone before the interface can process traffic. A zone can have multiple interfaces of the same type assigned to it (such as tap, layer 2, or layer 3 interfaces), but an interface can belong to only one zone.

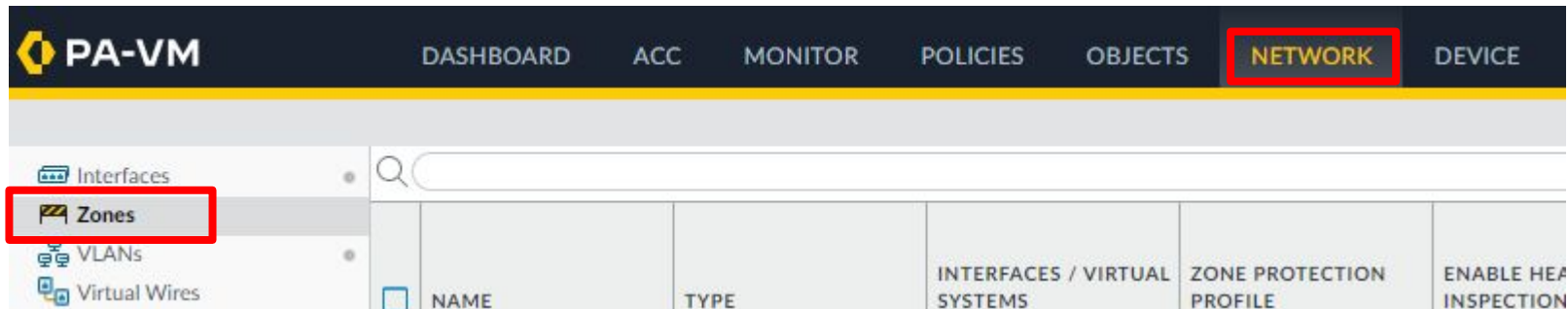
Policy rules on the firewall use security zones to identify where the traffic comes from and where it is going. Traffic can flow freely within a zone but traffic cannot flow between different zones until you define a Security policy rule that allows it. To allow or deny inter-zone traffic, Security policy rules must reference a source zone and destination zone (not interfaces) and the zones must be of the same type; that is, a Security policy rule can allow or deny traffic from one Layer 2 zone only to another Layer 2 zone.

Intrazone - Same Zone

Interzone - Different Zone

# Zones

Zones need to match the interfaces they are protecting. (i.e. L3 Zone -> L3 Interface)



The screenshot shows the Palo Alto VM Network configuration interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK' (highlighted with a red box), and 'DEVICE'. The left sidebar contains 'Interfaces', 'Zones' (highlighted with a red box), 'VLANs', and 'Virtual Wires'. The main content area displays a table with columns for 'NAME', 'TYPE', 'INTERFACES / VIRTUAL SYSTEMS', 'ZONE PROTECTION PROFILE', and 'ENABLE HEA INSPECTION'. A search bar is located above the table.

	NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	ENABLE HEA INSPECTION



# Zones

## Zone ?

Name

Log Setting None ▾

Type Layer3 ▾

INTERFACES ▾

Zone Protection

Zone Protection Profile None ▾

- Enable Packet Buffer Protection
- Enable L3 & L4 Header Inspection

### User Identification ACL

Enable User Identification

INCLUDE LIST ▾

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

EXCLUDE LIST ▾

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will be identified.

Users from these addresses/subnets will not be identified.

### Device-ID ACL

Enable Device Identification

INCLUDE LIST ▾

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

EXCLUDE LIST ▾

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Devices from these addresses/subnets will be identified.

Devices from these addresses/subnets will not be identified.

# DHCP

# DHCP

DHCP Server - Firewall is the source for IP Addressing

DHCP Relay - Firewall relays request to a server on a different subnet

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS **NETWORK** DEVICE

Interfaces  
Zones  
VI ANs  
Virtual Wires  
Virtual Routers  
IPSec Tunnels  
GRE Tunnels  
**DHCP**  
DNS Proxy

DHCP Server | DHCP Relay

SEARCH

<input type="checkbox"/>	INTERFACE	MODE	PROE
--------------------------	-----------	------	------

# DHCP

DHCP Server

+ Add - Delete PDF/CSV

## DHCP Server ?

Interface

Mode

**Lease**

Options

Ping IP when allocating new IP

Lease  Unlimited  Timeout

<input type="checkbox"/> IP POOLS <span>^</span>	RESERVED ADDRESS	MAC ADDRESS	DESCRIPTION
192.168.1.20, 192.168.1.0/24 or 192.168.1.10-192.168.1.20	192.168.1.20	xx:xx:xx:xx:xx:xx	(Optional MAC Address)
<span>+ Add</span> <span>- Delete</span>	<span>+ Add</span> <span>- Delete</span>		

# DHCP

## DHCP Server: Options

DHCP Server ?

Interface

Mode **auto**

Lease **Options**

Inheritance Source **None**

Custom DHCP options

<input type="checkbox"/>	NAME	CODE	TYPE	VALUE
--------------------------	------	------	------	-------

Gateway

Subnet Mask

Primary DNS **None**

Secondary DNS **None**

Primary WINS **None**

Secondary WINS **None**

Primary NIS **None**

Secondary NIS **None**

Primary NTP **None**

Secondary NTP **None**

POP3 Server **None**

SMTP Server **None**

DNS Suffix **None**

# DHCP

DHCP Relay:

DHCP Relay



Interface

IPv4

DHCP SERVER IP ADDRESS

IPv6

DHCP SERVER IPV6 ADDRESS

INTERFACE

Specify outgoing interface when using an IPv6 multicast address for your DHCPv6 server

# NAT

# NAT

Types of Network Address Translation (NAT) Policies:

Source NAT:

- Static IP - 1-to-1 translation to a defined address
- Dynamic IP - 1-to-1 translation to an address from a pool. Pool should match needs.
- Dynamic IP and Port (DIPP) - 1-to-1 translation to an address from a pool or interface. Pool does not match needs and multiple devices share the same IP and require a different port. Also called Port Address Translation (PAT)

Destination NAT:

- Static IP - 1-to-1 translation to a defined address
- Dynamic IP (with Session Disruption) - 1-to-1 translation to a dynamic IP on the destination device via FQDN.



# NAT

NAT Policies:

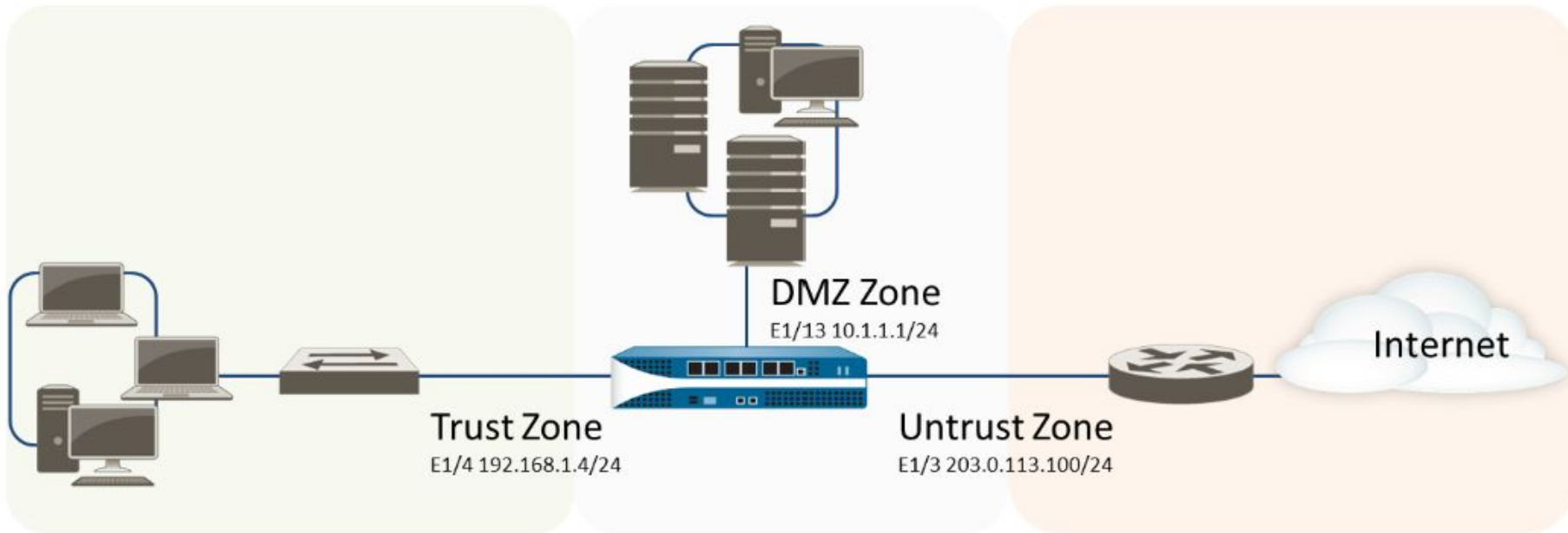
The screenshot shows the Palo Alto Networks PA-VM interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES' (highlighted with a red box), 'OBJECTS', 'NETWORK', and 'DEVICE'. On the left sidebar, 'Security' is expanded, and 'NAT' is selected (highlighted with a red box). Below the sidebar is a search bar and a table of NAT policies. The table has columns for 'NAME', 'TAGS', 'SOURCE ZONE', 'DESTINATION ZONE', 'DESTINATION INTERFACE', and 'SOURCE'. The 'DESTINATION ZONE', 'DESTINATION INTERFACE', and 'SOURCE' columns are grouped under the heading 'Original Packet'. At the bottom, a toolbar contains buttons for '+ Add' (highlighted with a red box), '- Delete', 'Clone', 'Enable', 'Disable', and 'Move'.

NAME	TAGS	Original Packet			
		SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE

Toolbar: + Add, - Delete, Clone, Enable, Disable, Move

# NAT

Source NAT:



# NAT

Source NAT Example:

NAT Policy Rule ?

**General** | Original Packet | Translated Packet

Name	Source NAT 1-1
Description	
Tags	
Group Rules By Tag	None
NAT Type	ipv4
Audit Comment	

[Audit Comment Archive](#)

# NAT

Source NAT Example:

NAT Policy Rule ?

General **Original Packet** Translated Packet

<input type="checkbox"/> Any	Destination Zone	<input checked="" type="checkbox"/> Any	<input checked="" type="checkbox"/> Any
<input type="checkbox"/> SOURCE ZONE ^	Outside	<input type="checkbox"/> SOURCE ADDRESS ^	<input type="checkbox"/> DESTINATION ADDRESS ^
<input checked="" type="checkbox"/> Inside			
	Destination Interface		
	ethernet1/5		
	Service		
	any		
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>		<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>

# NAT

Source NAT Example:

NAT Policy Rule

General | Original Packet | **Translated Packet**

Source Address Translation

Translation Type: **Static IP**

Translated Address: **1.2.3.4**

Bi-directional

Static translation can be to a single address or a subnet of addresses. The subnet will translate to a 1-1 relationship. (i.e. 10.0.0.50 -> 100.0.0.50)

NAT Policy Rule

General | Original Packet | **Translated Packet**

Source Address Translation

Translation Type: **Dynamic IP**

TRANSLATED ADDRESS ^

+ Add - Delete

Advanced (Dynamic IP/Port Fallback)

**None**

Translated Address

Interface Address

None

# NAT

## Source NAT Example:

### NAT Policy Rule

General | Original Packet

**Translated Packet**

#### Source Address Translation

Translation Type **Dynamic IP And Port**

Address Type **Translated Address**

TRANSLATED ADDRESS ^

**+ Add** - Delete

### NAT Policy Rule

General | Original Packet

**Translated Packet**

#### Source Address Translation

Translation Type **Dynamic IP And Port**

Address Type **Interface Address**

Interface **ethernet1/5**

IP Address **1.2.3.1/24**

# NAT

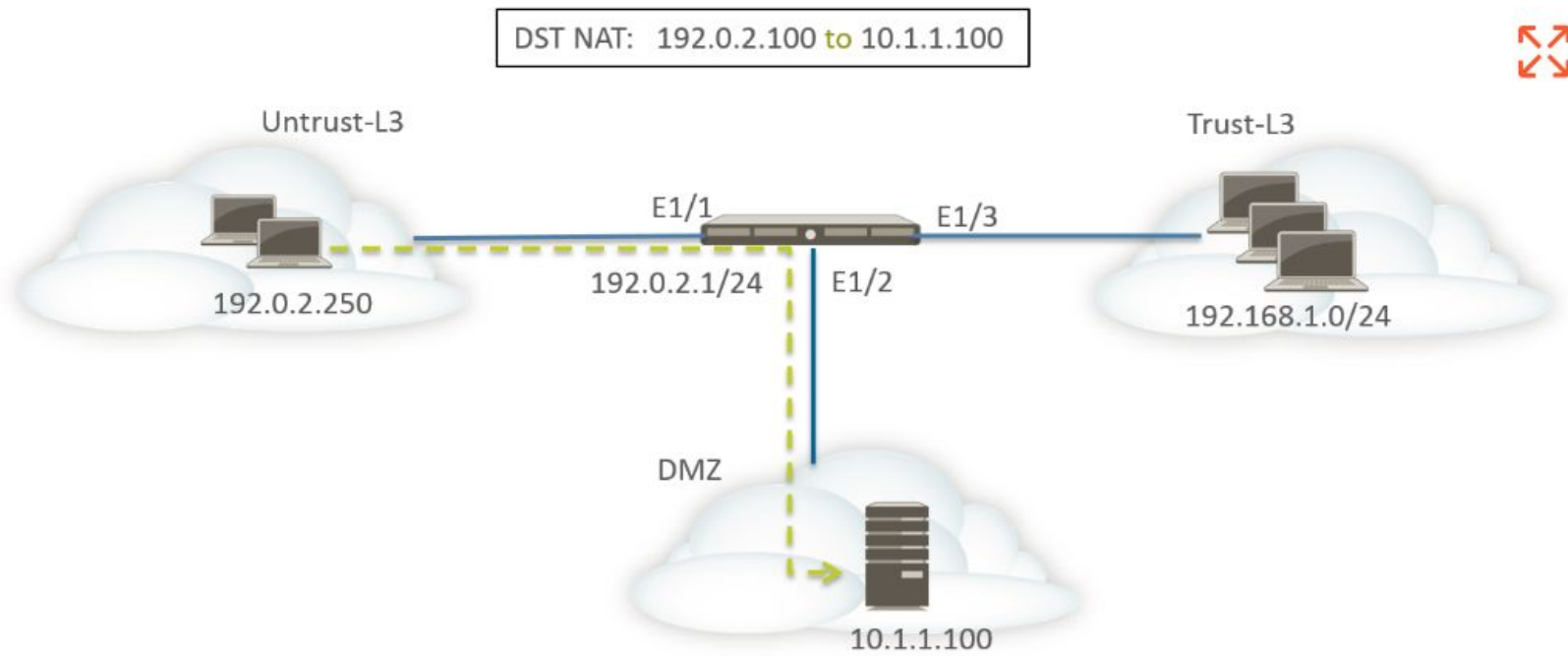
## Multiple ISP NAT:

- If you have multiple ISPs, you need multiple NAT policies.

	NAME	TAGS	Original Packet						Translated Packet	
			SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	ISP-1-NAT-Hub	none	inside	outside	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1 10.4.0.2/30	none
2	ISP-2-NAT-Hub	none	inside	outside	ethernet1/2	any	any	any	dynamic-ip-and-port ethernet1/2 10.4.1.2/30	none

# NAT

Destination NAT:





# NAT

Destination NAT Example:

## NAT Policy Rule



**General**

Original Packet | Translated Packet

Name Destination NAT

Description

Tags

Group Rules By Tag

None

NAT Type

ipv4

Audit Comment

[Audit Comment Archive](#)

# NAT

## Destination NAT Example:

NAT Policy Rule ?

General **Original Packet** Translated Packet

<input type="checkbox"/> Any	Destination Zone	<input checked="" type="checkbox"/> Any	<input type="checkbox"/> Any
<input type="checkbox"/> SOURCE ZONE ^	Outside	<input type="checkbox"/> SOURCE ADDRESS ^	<input type="checkbox"/> DESTINATION ADDRESS ^
<input checked="" type="checkbox"/> Outside			<input checked="" type="checkbox"/> 192.0.2.20/24
	Destination Interface		
	any (any interface)		
	Service		
	any		
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>		<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>

# NAT

Destination NAT Example:

NAT Policy Rule ?

General | Original Packet | **Translated Packet**

---

**Source Address Translation**

Translation Type: None

**Destination Address Translation**

Translation Type: Static IP

Translated Address: 10.1.1.100/24

Translated Port: [1 - 65535]

Enable DNS Rewrite

Direction: reverse

# Objects

# Objects



- Addresses**
- Address Groups
- Regions
- Dynamic User Groups
- Applications**
- Application Groups
- Application Filters
- Services
- Service Groups
- Tags
- Devices

## **External Dynamic Lists**

- Security Profile Groups
- Log Forwarding**
- Authentication
- Decryption
  - Decryption Profile

# Objects

Addresses:

Address ?

Name

Description

Type   [Resolve](#)

Enter an IP address or a network using the slash notation (Ex. 192.168.80.150 or 192.168.80.0/24). You can also enter an IPv6 address or an IPv6 address with its prefix (Ex. 2001:db8:123:1::1 or 2001:db8:123:1::/64)

Tags

Type

- IP Netmask
- IP Range
- IP Wildcard Mask
- FQDN

Tags

# Objects

## Address Groups: Static

Address Group ? ☰

Name Servers

Description

Type Static

Addresses

<input type="checkbox"/>	ADDRESS ^
<input type="checkbox"/>	ADServer-Internal
<input checked="" type="checkbox"/>	WebServer-Internal

🔍 Browse ⊕ Add ⊖ Delete

Tags

# Objects

Address Groups: Dynamic

DAG needs to be used in a Policy to populate.

The screenshot displays the Palo Alto Networks configuration interface. On the left, a list of address objects is shown with columns for NAME, TYPE, and DETAILS. The 'Servers' object is highlighted with a red box. On the right, the 'Address Group' configuration window is open, showing the 'Servers-Dyn' group. The 'Name', 'Type', and 'Match' fields are highlighted with red boxes. A green arrow points from the 'Servers' object in the list to the 'Add Match Criteria' button in the configuration window. The 'Tags' field at the bottom of the configuration window also shows 'Servers' with a red box.

NAME	TYPE	DETAILS
Inside	static	+
Outside	static	+
<b>Servers</b>	static	+
DMZ	static	+

Address Group configuration:

- Name: Servers-Dyn
- Type: Dynamic
- Match: 'Servers'
- Tags: Servers



# Objects

Addresses and Address Groups Use:

Security Policy Rule

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

Any

SOURCE ZONE ^

Inside

Any

SOURCE ADDRESS ^

[Dropdown]

Address

- ADServer-Internal
- WebServer-Internal

Address Group

- Servers

any

SOURCE USER ^

# Objects

Tags:

Tag ?

Name **DMZ**

Color any (any zone)

Comments DMZ  
Inside  
Outside

Zones Automatically populate to create tags

Tag ?

Name Servers

Color Blue

Comments

Ability to create custom tags

# Objects

Services:

Service ?

Name

Description

Protocol  TCP  UDP

Destination Port

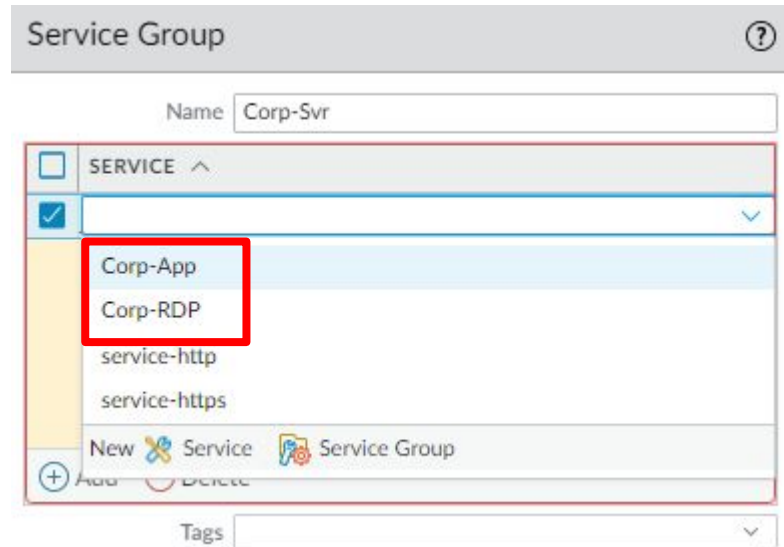
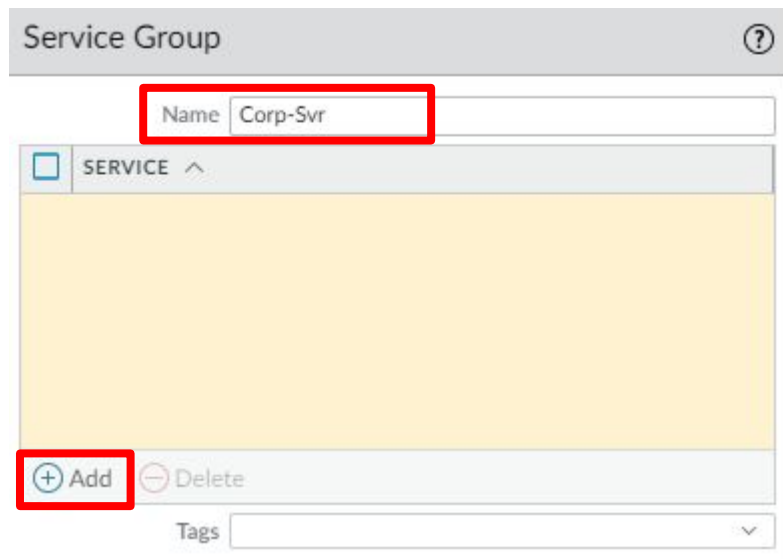
Source Port   
Port can be a single port #, range (1-65535), or comma separated (80, 8080, 443)

Session Timeout  Inherit from application  Override

Tags

# Objects

Service Groups:



# Objects

Service and Service Group Usage:

Security Policy Rule

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

select

SERVICE ^

[Service]

Service

- service-http
- service-https

New Service Service Group

+ Add - Delete

# Objects

Applications:

CATEGORY ^		SUBCATEGORY ^		RISK ^		TAGS ^	
2 business-systems	9 file-sharing	4	1	1	Downloading		
1 collaboration	1 office-programs	5	2	1	Editing		
1 general-internet	1 storage-backup	3	3	1	Posting		
9 saas	2 web-posting	1	4	1	Sharing		
				2	Uploading		

	NAME	CATEGORY	SUBCATEGORY	RISK	TAGS
<input type="checkbox"/>	aerofs	saas	file-sharing	3	Web App
<input type="checkbox"/>	draw.io (1 out of 2 shown)				
<input type="checkbox"/>	draw.io-cloud	business-systems	office-programs	2	Web App
<input type="checkbox"/>	dropbox				
<input type="checkbox"/>	dropbox-base	saas	file-sharing	4	Web App
<input type="checkbox"/>	dropbox-downloading	saas	file-sharing	2	Download... Web App
<input type="checkbox"/>	dropbox-editing	saas	file-sharing	1	Editing Web App
<input type="checkbox"/>	dropbox-lansync-discovery	saas	file-sharing	1	Web App

# Objects

## Applications:

### Application ?

<b>Name:</b> dropbox-base	<b>Description:</b> Dropbox is a file hosting service that offers cloud storage, file synchronization, personal cloud, and client software.
<b>Standard Ports:</b> tcp/80,443,17500, udp/17500	
<b>Depends on:</b> google-base	
<b>Implicitly Uses:</b> ssl, web-browsing	
<b>Deny Action:</b> drop-reset	

**Additional Information:** Wikipedia Website Google Yahoo!

<b>Characteristics</b>	<b>Options</b>
<b>Evasive:</b> yes	<b>TCP Timeout (seconds):</b> 3600 <a href="#">Customize...</a>
<b>Tunnels Other Applications:</b> no	<b>UDP Timeout (seconds):</b> 30 <a href="#">Customize...</a>
<b>Excessive Bandwidth Use:</b> no	<b>Prone to Misuse:</b> no
<b>Used by Malware:</b> no	<b>TCP Half Closed (seconds):</b> 120 <a href="#">Customize...</a>
<b>Widely Used:</b> yes	<b>TCP Time Wait (seconds):</b> 15 <a href="#">Customize...</a>
<b>Capable of File Transfer:</b> yes	<b>SaaS:</b> yes
<b>Has Known Vulnerabilities:</b> yes	<b>App-ID Enabled:</b> yes

<b>Classification</b>	<b>SaaS Characteristics</b>
<b>Category:</b> saas	<b>Certifications:</b> HIPAA, PCI, SOC I, SOC II, SSAE16
<b>Subcategory:</b> file-sharing	<b>Data Breaches:</b> no
<b>Risk:</b> 4 <a href="#">Customize...</a>	<b>IP Based Restrictions:</b> no
	<b>Poor Financial Viability:</b> no
	<b>Poor Terms Of Service:</b> no

**Tags**

[Web App](#) [Edit](#)

# Objects

## Applications: Custom

Application ?

**Configuration**

Advanced

Signatures

### General

Name

Description

### Properties

Category

Subcategory

Technology

Parent App

Risk

### Characteristics

- |   |  |   |
|---|--|---|
| <input type="checkbox"/> Capable of File Transfer   | <input type="checkbox"/> Has Known Vulnerabilities | <input type="checkbox"/> Pervasive                                |
| <input type="checkbox"/> Excessive Bandwidth Use    | <input type="checkbox"/> Used by Malware           | <input type="checkbox"/> Prone to Misuse                          |
| <input type="checkbox"/> Tunnels Other Applications | <input type="checkbox"/> Evasive                   | <input type="checkbox"/> Continue scanning for other Applications |



# Objects

Application: Custom

Application ?

Configuration

**Advanced**

Signatures

## Defaults

Port  IP Protocol  ICMP Type  ICMP6 Type  None

### PORT

Enter each port in the form of [tcp|udp]/[dynamic|0-65535] Example: tcp/dynamic or udp/32

## Timeouts

Timeout

TCP Timeout

UDP Timeout

TCP Half Closed

TCP Time Wait

## Scanning (activated via Security Profiles)

File Types

Viruses

Data Patterns

# Objects

Application: Custom

The screenshot shows the configuration interface for a custom application signature. The left sidebar has tabs for Configuration, Advanced, and Signatures, with the Signatures tab highlighted. Below the tabs is a search bar and a table with columns for SIGNATURE NAME and COMMENT. At the bottom of the sidebar, there are buttons for + Add and - Delete, with the + Add button highlighted. A green arrow points from the + Add button to the main configuration area. The main area is titled 'Signature' and contains fields for Signature Name and Comment. Below these fields are radio buttons for Scope (Transaction selected, Session unselected) and a checked checkbox for Ordered Condition Match. A table with columns AND CONDITION, COND..., OPERATOR, CONTEXT, and PATTERN is shown below. At the bottom of the main area, there are buttons for + Add Or Condition, + Add And Condition, - Delete, ↑ Move Up, and ↓ Move Down.

Application

Configuration | Advanced | **Signatures**

Signature

Signature Name

Comment

Scope  Transaction  Session

Ordered Condition Match

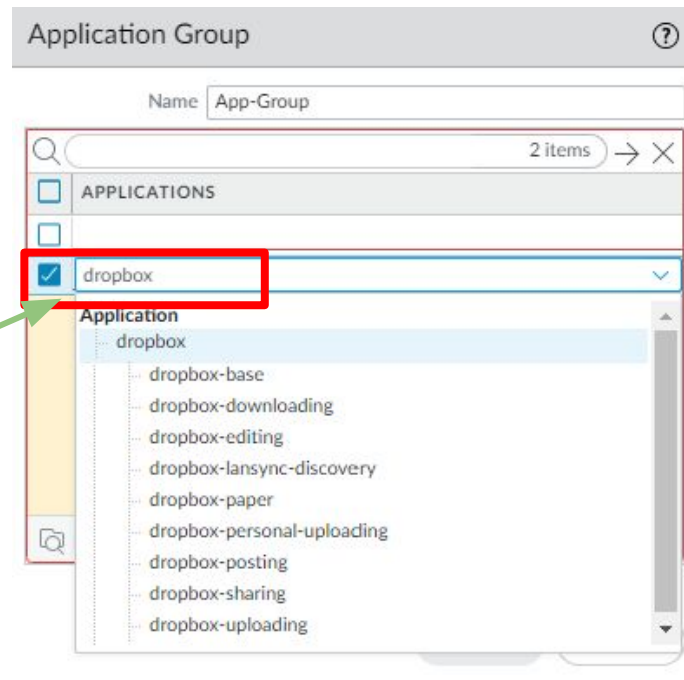
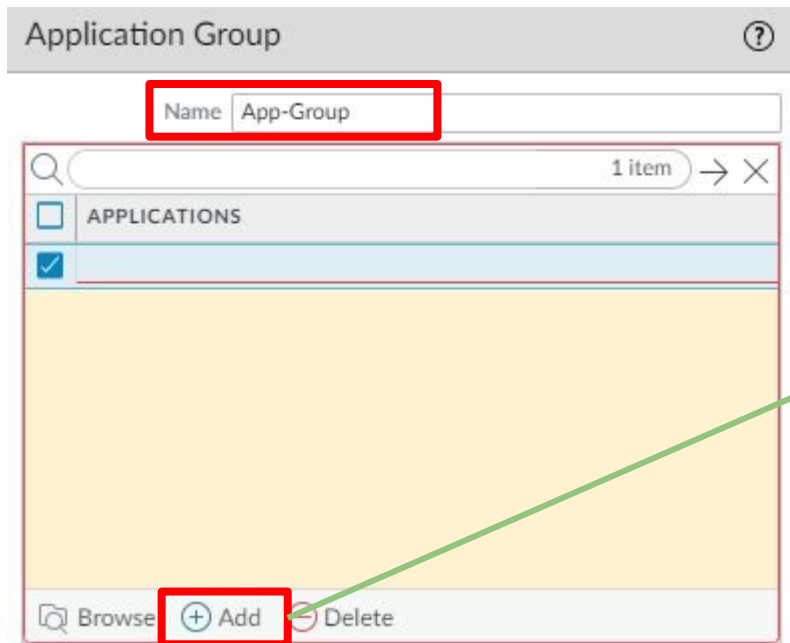
<input type="checkbox"/>	AND CONDITION	COND...	OPERATOR	CONTEXT	PATTERN
--------------------------	---------------	---------	----------	---------	---------

+ Add - Delete

+ Add Or Condition + Add And Condition - Delete ↑ Move Up ↓ Move Down

# Objects

## Application Groups: Static



# Objects:

## Application Filters: Dynamic

Application Filter ?

NAME   Apply to New App-IDs only  Clear Filters 4380 matching applications

CATEGORY ^	SUBCATEGORY ^	RISK ^	TAGS ^	CHARACTERISTIC ^
1841 business-systems	26 artificial-intelligence	2253 1	0	36 Data Breaches
456 collaboration	55 audio-streaming	1034 2	App-ID Cloud Engine	646 Evasive
359 general-internet	25 auth-service	580 3	3 Deleting	672 Excessive Bandwidth
339 media	1 collaboration-productivity	370 4	14 DLP App Exclusion	53 FEDRAMP
510 networking	5 content-managemen	143 5	81 Downloading	3 FINRA
873 saas	3 customer-service			117 HIPAA
2 unknown				87 IP Based Restrictions

NAME	CATEGORY	SUBCATEGORY	RISK	TAGS	STANDARD PORTS	EXCLUDE
100bao	general-intern	file-sharing	5		11300,3468,6346,tcp	<input checked="" type="checkbox"/>
iec-60870-5-104						<input checked="" type="checkbox"/>
104apci-supervisory	business-syste	ics-protocols	2		2404,tcp	<input checked="" type="checkbox"/>
104apci-unnumbered	business-syste	ics-protocols	2		2404,tcp	<input checked="" type="checkbox"/>
104apci-unnumbered	business-syste	ics-protocols	1		2404,tcp	<input checked="" type="checkbox"/>
104apci-unnumbered	business-syste	ics-protocols	1		2404,tcp	<input checked="" type="checkbox"/>

Page 1 of 118 ▶▶▶ Displaying 1 - 84 of 4711

Select what will be used to filter for applications (Category, Subcategory, Risk Level, Tag, Characteristic)

# Objects:

## External Dynamic Lists: Predefined

<input type="checkbox"/>	NAME	LOCATION	DESCRIPTION	SOURCE
∨ Dynamic IP Lists				
<input type="checkbox"/>	Palo Alto Networks - Tor exit IP addresses	Predefined	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.	panw-torexit-ip-list
<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.	panw-bulletproof-ip-list
<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.	panw-highrisk-ip-list
<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.	panw-known-ip-list
∨ Dynamic URL Lists				
<input type="checkbox"/>	Palo Alto Networks - Authentication Portal Exclude List	Predefined	Domains and URLs to exclude from Authentication Policy. This list is managed by Palo Alto Networks.	Palo Alto Networks - Authentication Portal Exclude List

# Objects:

External Dynamic List: Custom

External Dynamic Lists ?

Name Custom-EDL

**Create List** List Entries And Exceptions

Type IP List

Description

Source

Server Authentication

Certificate Profile

Check for updates

- Predefined IP List
- Predefined URL List
- IP List
- Domain List
- URL List
- Subscriber Identity List
- Equipment Identity List

# Objects:

## External Dynamic List: Custom

External Dynamic Lists ?

Name Custom-EDL

**Create List** List Entries And Exceptions

Type IP List

Description

Source http://10.8.6.4/

Server Authentication

Certificate Profile None

Check for updates Every five minutes

# Objects

Custom EDL:

Lists must be applied to a policy to retrieve information from server.

The screenshot shows the 'External Dynamic Lists' configuration page. The 'Name' field is set to 'CINS Army Feed'. The 'Create List' dropdown is set to 'List Entries And Exceptions', which is highlighted with a red box. Below this, there are two panels: 'List Entries' and 'Manual Exceptions'. The 'List Entries' panel shows a search bar with '15000 items' and a list of IP addresses, with the list area highlighted by a cyan border. The 'Manual Exceptions' panel shows a search bar with '0 items' and a single entry 'LIST ENTRIES' with a checkbox. An arrow points from the 'List Entries' panel to the 'Manual Exceptions' panel.

External Dynamic Lists ?

Name: CINS Army Feed

Create List: **List Entries And Exceptions**

List Entries: 15000 items → X

	LIST ENTRIES
<input type="checkbox"/>	1.10.184.106
<input type="checkbox"/>	1.117.145.83
<input type="checkbox"/>	1.117.204.147
<input type="checkbox"/>	1.117.219.226
<input type="checkbox"/>	1.117.236.166
<input type="checkbox"/>	1.117.91.115
<input type="checkbox"/>	1.119.194.226
<input type="checkbox"/>	1.119.194.226

Manual Exceptions: 0 items → X

<input type="checkbox"/>	LIST ENTRIES
--------------------------	--------------

+ Add - Delete



# Objects:

## Log Forwarding:

<input type="checkbox"/>	NAME	LOCATION	DESCRIPTION	LOG TYPE	FILTER	PANORAMA	SNMP	EMAIL	SYSLOG	HTTP
<input type="checkbox"/>	IoT Security Default Profile	Predefined		traffic	All Logs	<input checked="" type="checkbox"/>				
				threat	All Logs	<input checked="" type="checkbox"/>				
				wildfire	All Logs	<input checked="" type="checkbox"/>				
				url	All Logs	<input checked="" type="checkbox"/>				
				data	All Logs	<input checked="" type="checkbox"/>				
				tunnel	All Logs	<input checked="" type="checkbox"/>				
				auth	All Logs	<input checked="" type="checkbox"/>				
				decryption	All Logs	<input checked="" type="checkbox"/>				

### Log Forwarding Profile ?

Name

Description

0 items → ×

<input type="checkbox"/>	NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS
<input checked="" type="checkbox"/>					

# Objects:

## Log Forwarding:

Log Forwarding Profile Match List

Name:

Description:

Log Type: traffic

Filter: All Logs

Forward Method

- SNMP
- EMAIL
- SYSLOG**
- HTTP
- Panorama

Built-in Actions

- Quarantine
- | NAME | TYPE |
|------|------|
|------|------|

Log Type

- traffic
- auth
- data
- decryption
- threat
- traffic
- tunnel
- url
- wildfire

Create a filter to select specific logs

# Licenses and Profiles

# Licenses

## Subscription Licenses and CDSS

- Advanced Threat Prevention
  - Advanced URL Filtering
  - Advanced Wildfire
  - DNS Security - Requires ATP
  - SD-WAN - Requires Panorama
  - GlobalProtect Gateway
  - Internet of Things (IoT) Security
  - Enterprise Data Loss Prevention (DLP)
  - SaaS Security Inline
  - Support
  - Virtual Systems (vSys)
  - Strata Cloud Manager / AIOps Premium
  - Strata Logging Manager (Formally Cortex Data Lake or CDL)
- Part of the Core Security Bundle (CoreSec)

# Licenses

What happens when subscriptions expire: [Docs Link](#)

Palo Alto Networks **subscriptions** provide the firewall with added functionality and/or access to a Palo Alto Networks cloud-delivered service. When a license is within 30 days of expiration, a warning message displays in the system log daily until the subscription is renewed or expires. Upon license expiration, some subscriptions continue to function in a limited capacity, and others stop operating completely. Here you can find out what happens when each subscription expires.



The precise moment of license expiry is at the beginning of the following day at 12:00 AM (GMT). For example, if your license is scheduled to end on 1/20 you will have functionality for the remainder of that day. At the start of the new day on 1/21 at 12:00 AM (GMT), the license will expire. All license-related functions operate on Greenwich Mean Time (GMT), regardless of the configured time zone on the firewall.

## DNS Security

### **You can still:**

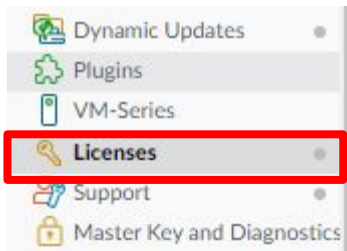
- Use local DNS signatures if you have an active Threat Prevention license.

### **You can no longer:**

- Get new DNS signatures.

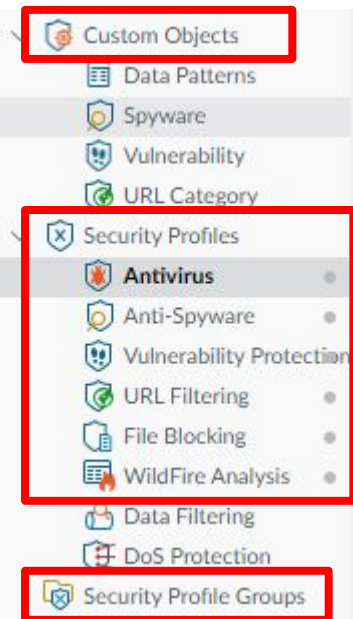
# Licenses

Licenses:



<b>Advanced URL Filtering</b>
Date Issued March 20, 2023
<b>Date Expires November 14, 2024</b>
Description Palo Alto Networks Advanced URL License
<b>DNS Security</b>
Date Issued March 20, 2023
Date Expires November 14, 2024
Description Palo Alto Networks DNS Security License

# Profiles



# Profiles

Security Profiles:

- Predefined rules cannot be modified or deleted.
- Rules can be cloned as a starting point for a new custom profile.
- Create a custom profile from scratch.



<input type="checkbox"/>	NAME	LOCATION
<input type="checkbox"/>	default	Predefined
<input type="checkbox"/>	strict	Predefined



# Profiles

AntiVirus (ATP): Antivirus profiles protect against viruses, worms, and trojans as well as spyware downloads.

<input type="checkbox"/>	NAME	LOCATION	PACKET CAPTURE	HOLD MODE	Decoders			
					PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION
<input type="checkbox"/>	default	Predefined	<input type="checkbox"/>	<input type="checkbox"/>	http	default (reset-both)	default (reset-both)	default (reset-both)
					http2	default (reset-both)	default (reset-both)	default (reset-both)
					smtp	default (alert)	default (alert)	default (alert)
					imap	default (alert)	default (alert)	default (alert)
					pop3	default (alert)	default (alert)	default (alert)
					ftp	default (reset-both)	default (reset-both)	default (reset-both)
					smb	default (reset-both)	default (reset-both)	default (reset-both)

# Profiles

## AntiVirus (ATP):

Antivirus Profile ?

Name Custom-AV-Profile

Description

**Action** | Signature Exceptions | WildFire Inline ML

Enable Packet Capture  Hold for WildFire Real Time Signature Look Up

Decoders

PROTOCOL ^	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION
ftp	default (reset-both)	default (reset-both)	default (reset-both)
http	default (reset-both)	default (reset-both)	default (reset-both)
http2	default (reset-both)	default (reset-both)	default (reset-both)
imap	default (alert)	default (alert)	default (alert)
pop3	default (alert)	default (alert)	default (alert)
smb	default (reset-both)	default (reset-both)	default (reset-both)

Application Exceptions

0 items → ×

APPLICATION	ACTION
-------------	--------

+ Add - Delete

default (reset-both)

allow

alert

drop

reset-client

reset-server

reset-both

# Profiles

AntiSpyware (ATP): Anti-Spyware profiles blocks spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers, allowing you to detect malicious traffic leaving the network from infected clients.

<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

# Profiles

AntiSpyware (ATP): Custom

## Anti-Spyware Profile



Name Custom-AS-Profile

Description

Signature Policies

Signature Exceptions

DNS Policies

DNS Exceptions

Inline Cloud Analysis



POLICY NAME

SEVERITY

ACTION

PACKET CAPTURE



Add



Delete



Move Up



Move Down



Clone



Find Matching Signatures

# Profiles

AntiSpyware (ATP): Custom

Anti-Spyware Policy ?

Policy Name

Threat Name   
Used to match any signature containing the entered text as part of the signature name

Category

Action

Packet Capture

Severity

- any (All severity levels)
- critical
- high
- medium
- low
- informational

Default

Allow

Alert

Drop

Reset Client

Reset Server

Reset Both

Block IP

# Profiles

## DNS Security: (ATP and DNS)

Anti-Spyware Profile

Name Custom-AS-Profile

Description

Signature Policies | Signature Exceptions | **DNS Policies** | DNS Exceptions | Inline Cloud Analysis

### DNS Policies

SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
Palo Alto Networks Content			
default-paloalto-dns		sinkhole	disable
DNS Security			
Ad Tracking Domains	default (informational)	default (allow)	disable
Command and Control Domains	default (high)	default (block)	disable
Dynamic DNS Hosted Domains	default (informational)	default (allow)	disable
Grayware Domains	default (low)	default (block)	disable
Malware Domains	default (medium)	default (block)	disable
Parked Domains	default (informational)	default (allow)	disable
Phishing Domains	default (low)	default (block)	disable

### DNS Sinkhole Settings

Sinkhole IPv4 Palo Alto Networks Sinkhole IP (sinkhole.paloaltonetworks.com)

Sinkhole IPv6 IPv6 Loopback IP (::1)

### Block DNS Record Types

SVCB

HTTPS

ANY

default

allow

block

sinkhole

# Profiles

Vulnerability Protection (ATP): Vulnerability Protection profiles stop attempts to exploit system flaws or gain unauthorized access to systems. While Anti-Spyware profiles help identify infected hosts as traffic leaves the network, Vulnerability Protection profiles protect against threats entering the network.

<input type="checkbox"/>	NAME	LOCATION	COUNT	RULE NAME	THREAT NAME	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	strict	Predefined	Rules: 10	simple-client-critical	any	client	critical	reset-both	disable
				simple-client-high	any	client	high	reset-both	disable
				simple-client-medium	any	client	medium	reset-both	disable
				simple-client-informational	any	client	informational	default	disable
				simple-client-low	any	client	low	default	disable
				simple-server-critical	any	server	critical	reset-both	disable
				simple-server-high	any	server	high	reset-both	disable
				more...					
<input type="checkbox"/>	default	Predefined	Rules: 6	simple-client-critical	any	client	critical	default	disable

# Profiles

Vulnerability Protection (ATP): Custom

### Vulnerability Protection Profile ?

Name **Custom-TP-Profile**

Description

**Rules** | Exceptions | Inline Cloud Analysis

<input type="checkbox"/>	RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
--------------------------	-----------	-------------	-----	-----------	----------	--------	----------------

**+** Add Delete Move Up Move Down Clone Find Matching Signatures



# Profiles

Advanced URL Filtering: URL Filtering profiles enable you to monitor and control how users access the web over HTTP and HTTPS. URL Filtering profiles enable you to monitor and control how users access the web over HTTP and HTTPS.

<input type="checkbox"/>	NAME	LOCATION	SITE ACCESS	USER CREDENTIAL SUBMISSION
<input type="checkbox"/>	default	Predefined	Allow Categories (59) Alert Categories (6) Continue Categories (0) Block Categories (12) Override Categories (0)	Allow Categories (77) Alert Categories (0) Continue Categories (0) Block Categories (0)

# Profiles

## URL Filtering: Custom

### URL Filtering Profile

Name Custom-URL-Profile

Description

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

<input type="checkbox"/>	CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
∨	Pre-defined Categories		
<input type="checkbox"/>	abortion	allow	allow
<input type="checkbox"/>	abused-drugs	allow	allow
<input type="checkbox"/>	adult	allow	allow
<input type="checkbox"/>	alcohol-and-tobacco	allow	allow
<input type="checkbox"/>	artificial-intelligence	allow	allow
<input type="checkbox"/>	auctions	allow	allow

alert  
allow  
block  
continue  
override

alert  
allow  
block  
continue

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

[Check URL Category](#)

# Profiles

## URL Filtering: Credential Theft Prevention - USER-ID Required

URL Filtering Profile ?

Name

Description

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

User Credential Detection

▼

- Disabled
- Use IP User Mapping
- Use Domain Credential Filter
- Use Group Mapping

# Profiles

Advanced WildFire: Use a WildFire analysis profile to enable forwarding of unknown files or email links for WildFire analysis.

WildFire Analysis Profile (Read Only) ?

Name

Description

1 item → ×

<input type="checkbox"/>	NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
<input type="checkbox"/>	default	any	any	both	public-cloud

# Profiles

## File Blocking 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.

<input type="checkbox"/>	NAME	LOCATION	RULE NAME	APPLICATIONS	FILE TYPES
<input type="checkbox"/>	basic file blocking	Predefined	Block high risk file types Continue prompt encrypted files Log all other file types	any any any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf encrypted-rar, encrypted-zip any

- 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.

<input type="checkbox"/>	strict file blocking	Predefined	Block all risky file types Block encrypted files Log all other file types	any any 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 encrypted-rar, encrypted-zip any
--------------------------	----------------------	------------	---	-------------------	---

# Profiles

Security Profile Groups:

Security Profile Group ?

Name	Outbound-Profile-Group
Antivirus Profile	default
Anti-Spyware Profile	strict
Vulnerability Protection Profile	strict
URL Filtering Profile	default
File Blocking Profile	basic file blocking
Data Filtering Profile	None
WildFire Analysis Profile	default

WildFire Analysis Profile

default

None

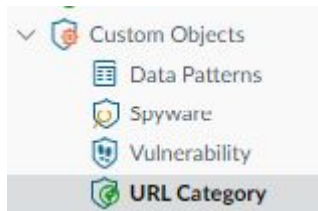
default

New WildFire Analysis

# Profiles

## Custom Objects:

- Data Patterns - Defines patterns used in Data Filtering profile
- Spyware - Create custom signatures to use in a AS profile
- Vulnerability - Create custom signatures to use in a VP profile
- URL Category - Create custom URL categories to use in a URL Filtering profile



# Profiles

## Custom Objects: URL Category

Custom URL Category ?

Name Allowed URLs

Description

Type URL List

Matches any of the following URLs, domains or host names

1 item → ×

<input type="checkbox"/>	SITES
<input checked="" type="checkbox"/>	www.facebook.com

+ Add | - Delete | Import | Export



# Profiles

Custom Object: URL Category (Automatically added to a custom profile)

**URL Filtering Profile** ?

Name: Custom-URL-Profile

Description:

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

78 items → ×

<input type="checkbox"/>	CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
∨	Custom URL Categories		
<input type="checkbox"/>	Allowed URLs *	none	none
∨	Pre-defined Categories		
<input type="checkbox"/>	abortion	allow	allow
<input type="checkbox"/>	abused-drugs	block	block

# Security Policies

# Security Policies

Security Policies:

- Only intrazone traffic is allowed by default.
- All other traffic is denied.

The screenshot shows the Palo Alto VM Security Policies configuration page. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE'. The 'POLICIES' tab is highlighted. The left sidebar shows the 'Security' menu item highlighted. The main content area displays a table of security policies.

	NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
1	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow
2	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny

	NAME	ACTION
1	intrazone-default	Allow
2	interzone-default	Deny

# Security Policies

Parts of a rule:

- Required
  - Name
  - Rule Type
  - Source Zone
  - Destination Zone
  - Application
  - Action
- Optional
  - Tag
  - Description
  - Source Address
  - Destination Address
  - URL / URL Category
  - Service
  - Security Profile
  - Options

# Security Policies

## Security Policy Actions:

ACTION	DESCRIPTION
<b>Allow</b> (default)	Allows the traffic.
<b>Deny</b>	Blocks traffic and enforces the default <b>Deny Action</b> defined for the application that is being denied.
<b>Drop</b>	<p>Silently drops the traffic; for an application, it overrides the default deny action. A TCP reset isn't sent to the host/application.</p> <p>For Layer 3 interfaces, to optionally send an ICMP unreachable response to the client, set Action: <b>Drop</b> and enable the <b>Send ICMP Unreachable</b> check box. When enabled, the ICMP code is sent for communication with the destination is administratively prohibited—ICMPv4: Type 3, Code 13; ICMPv6: Type 1, Code 1.</p>
<b>Reset client</b>	Sends a TCP reset to the client-side device.
<b>Reset server</b>	Sends a TCP reset to the server-side device.
<b>Reset both</b>	Sends a TCP reset to both the client-side and server-side devices.


# Security Policies

Create a new policy:

Security Policy Rule

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

Name

Rule Type  

Description

Tags

Group Rules By Tag

Audit Comment

Audit Comment Archive

universal (default)  
intrazone  
interzone

# Security Policies

Create a new policy:

Security Policy Rule

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

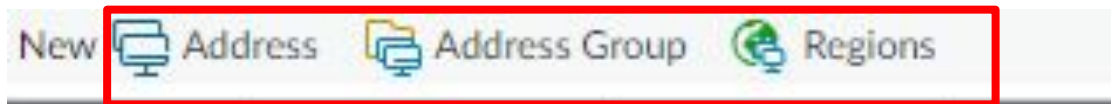
<input type="checkbox"/> Any	<input type="checkbox"/> Any	any	any
<input type="checkbox"/> SOURCE ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^	<input type="checkbox"/> SOURCE USER ^	<input type="checkbox"/> SOURCE DEVICE ^
<input type="checkbox"/> lan_zone	<input type="checkbox"/> All-LAN		
<input type="checkbox"/> + Add - Delete	<input type="checkbox"/> + Add - Delete	<input type="checkbox"/> + Add - Delete	<input type="checkbox"/> + Add - Delete

Negate All but above

# Security Policies

Address Options:

- Address
- Address Group
- External Dynamic List
- Region
  - Predefined - China (CN)
  - Custom





# Security Policies

Create a new policy:

Security Policy Rule

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

DESTINATION ZONE ^	DESTINATION ADDRESS ^	DESTINATION DEVICE ^
<input type="checkbox"/> select <input type="checkbox"/> wan_zone	<input checked="" type="checkbox"/> Any <input type="checkbox"/>	<input type="checkbox"/> any

Add  Delete       Add  Delete       Add  Delete

Negate

# Security Policies

Create a new policy:

Security Policy Rule

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

<input type="checkbox"/> Any		
<input type="checkbox"/> APPLICATIONS ^		<input type="checkbox"/> DEPENDS ON ^
<input type="checkbox"/> paloalto-logging-service		<p>If the added application has a dependency, it will show here</p>
<input type="checkbox"/> paloalto-shared-services		
<input type="checkbox"/> ssl		

# Security Policies

Create a new policy:

Security Policy Rule

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

application-default  
any  
select

select

SERVICE ^

CDL-Ports

Any

URL CATEGORY ^

Add  Delete

Add  Delete

# Security Policies

Create a new policy:

## Security Policy Rule

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

### Action Setting

Action **Allow**

Send ICMP Unreachable

### Profile Setting

Profile Type **Group**

Group Profile **Outbound**

### Log Setting

Log at Session Start

Log at Session End

Log Forwarding **default**

### Other Settings

Schedule **None**

QoS Marking **None**

Disable Server Response Inspection

# Security Policies

Create a new policy: Profile Settings

Profile Setting

Profile Type **None**

- Profiles
- Group
- None**

Profile Setting

**Profile Type** Group

Group Profile Outbound

Profile Setting

**Profile Type** Profiles

Antivirus default

Vulnerability Protection default

Anti-Spyware default

URL Filtering Custom-URL-Profile

File Blocking strict file blocking

Data Filtering None

WildFire Analysis default

# Security Policies

## Policies: Using Tags

Security Policy Rule

**General** | Source | Destination | Application

Name: LAN-to-WAN-Traffic

Rule Type: universal (default)

Description: Allow traffic from LAN to WAN zone.

Tags: **Outbound** ✕

5	Block-Google-QUIC	<b>Outbound</b>	universal	any	any
6	Block WAN to WAN ...	none	universal	wan_zone	any
7	Rule for Exam	none	universal	lan_zone	10.0.40.103
8	Allow Traffic to CDL	<b>Outbound</b>	universal	lan_zone	Data
9	Email_Rule	<b>Outbound</b>	universal	lan_zone	All-LAN
10	LAN-to-WAN-Traffic	<b>Outbound</b>	universal	lan_zone	All-LAN
11	Internal_Traffic	<b>Internal</b>	universal	lan_zone	All-LAN

# Security Policies

## Policies: Grouping

Security Policy Rule

**General** | Source | Destination | Application

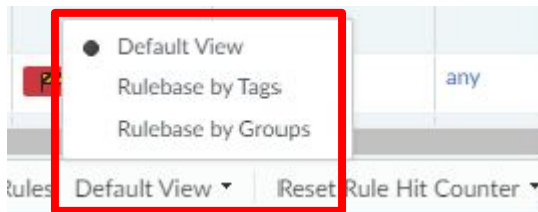
Name: LAN-to-WAN-Traffic

Rule Type: universal (default)

Description: Allow traffic from LAN to WAN zone.

Tags: **Outbound** ✕

Group Rules By Tag: **Outbound**



Policy Optimizer +

Tag Browser -

7 items → ✕

TAG(RULE COUNT)	RULE NUMBER
Inbound (1)	1
Outbound (1)	2
Inbound (1)	3
Outbound (2)	4-5
none (2)	6-7
Outbound (3)	8-10
Internal (1)	11

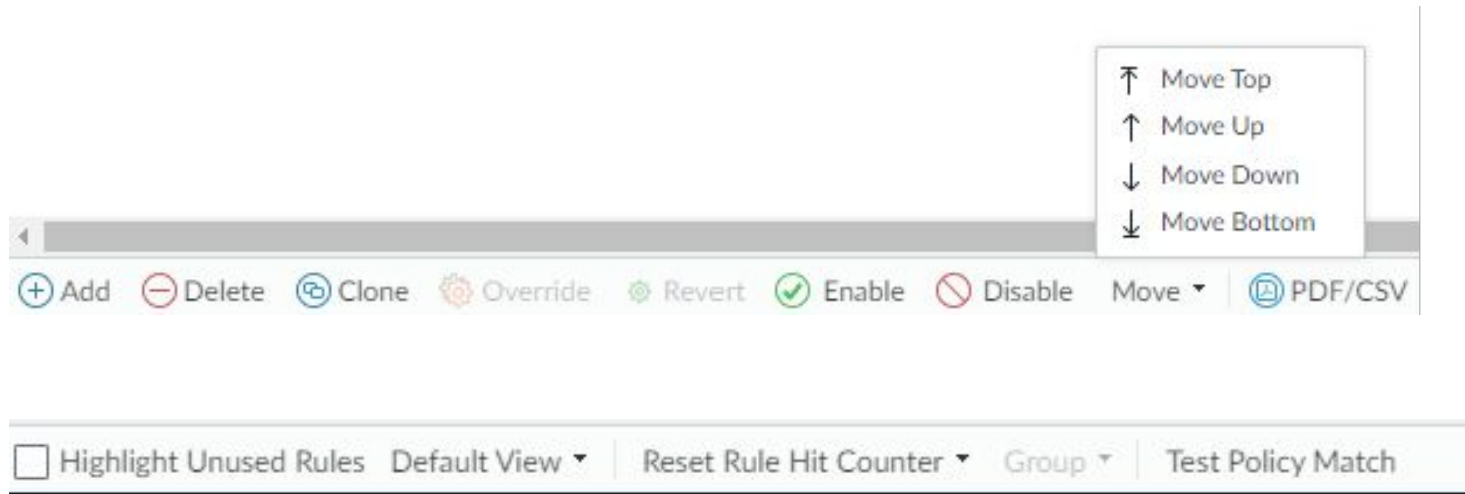
Filter by first tag in rule

Rule Order  Alphabetical

Object: Tags +

# Security Policies

Policy Options:



The screenshot displays the Palo Alto Networks Security Policies management interface. A context menu is open over the 'Move' button, showing the following options:

- Move Top
- Move Up
- Move Down
- Move Bottom

The main toolbar includes the following buttons: Add, Delete, Clone, Override, Revert, Enable, Disable, Move, and PDF/CSV. Below the toolbar, there are additional controls: a checkbox for 'Highlight Unused Rules', a 'Default View' dropdown, a 'Reset Rule Hit Counter' dropdown, a 'Group' dropdown, and a 'Test Policy Match' button.



# Security Policies

## Recommended Block Rules:

	NAME	TAGS	TYPE	Source				Destination	
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
1	Geo-Block-Inbound	Inbound	universal	any	CN IR KP RU	any	any	any	any
2	Geo-Block-Outbound	Outbound	universal	any	any	any	any	CN IR KP RU	
3	Known-Bad-EDL-Inb...	Inbound	universal	any	Palo Alto Networks - Bulletproo... Palo Alto Networks - High risk L... Palo Alto Networks - Known ma... Palo Alto Networks - Tor exit IP ...	any	any	any	any
4	Known-Bad-EDL-Ou...	Outbound	universal	any	any	any	any	Palo Alto Networks - Bulletproof IP a... Palo Alto Networks - High risk IP ad... Palo Alto Networks - Known malicio... Palo Alto Networks - Tor exit IP addr...	

# Security Policies

Recommended Block Rules:

5 | Block-Google-QUIC | Outbound | universal | any | any | any | any | any | any | any | quic | application-...

## Security Policy Rule

General | Source | Destination | Application

Any

APPLICATIONS ^

quic

# Security Policies

## Rule Usage:

Rule Usage				DAYS WITH NO NEW APPS	MODIFIED	CREATED
HIT COUNT	LAST HIT	FIRST HIT	APPS SEEN			
0	-	-	-	-	2024-01-04 09:40:36	2024-01-04 09:40:36
113247	2024-02-29 16:26:05	2024-01-05 16:18:21	-	-	2024-01-04 09:40:36	2024-01-04 09:40:36
485033	2024-02-29 16:30:53	2024-01-05 18:43:23	-	-	2024-01-05 18:39:30	2024-01-05 18:39:30
949	2024-01-12 17:26:44	2024-01-12 13:52:04	14	48	2024-01-12 17:33:16	2024-01-12 13:51:57
68955	2024-02-29 16:23:03	2024-01-05 17:21:39	3	55	2024-01-05 19:21:39	2024-01-05 17:15:37
19262	2024-02-29 16:18:16	2024-01-05 16:21:03	1	55	2024-01-05 19:21:39	2024-01-04 09:40:36
22519660	2024-02-29 16:31:00	2024-01-05 16:18:30	147	1	2024-01-05 19:21:39	2024-01-04 09:40:36
4019852	2024-02-29 16:31:01	2024-01-05 16:18:29	15	7	2024-01-05 19:21:39	2024-01-04 09:40:36

# Security Policies

Applications Seen:

Applications & Usage - LAN-to-WAN-Traffic

Timeframe: Anytime

Apps on Rule: Apps Seen 147

Any

APPLICATIONS ^

<input type="checkbox"/>	APPLICATIONS	SUBCATEGO...	RISK	FIRST SEEN	LAST SEEN	TRAFFIC (30 DAYS)
<input checked="" type="checkbox"/>	ssl	encrypted-tunnel	4	2024-01-05	2024-02-29	604.3G
<input type="checkbox"/>	paloalto-updates	software-update	2	2024-01-05	2024-02-29	347.7G
<input type="checkbox"/>	hulu-base	photo-video	2	2024-01-05	2024-02-28	288.2G
<input type="checkbox"/>	ipsec-esp-udp	encrypted-tunnel	2	2024-01-15	2024-02-29	29.6G
<input type="checkbox"/>	facebook-base	social-networking	4	2024-01-05	2024-02-29	18.4G
<input type="checkbox"/>	youtube-base	photo-video	4	2024-01-05	2024-02-29	15.4G
<input type="checkbox"/>	google-base	internet-utility	4	2024-01-05	2024-02-29	14.5G

Browse  Add  Delete  Create Cloned Rule  Add to This Rule  Add to Existing Rule  Match Usage

The last new app was discovered 1 days ago.

# Security Policies

Policy Optimizer:

Policy Optimizer

- New App Viewer 1+
- Rules Without App Controls 3
- Unused Apps 0
- Log Forwarding for Security Services
- Rule Usage
  - Unused in 30 days 4
  - Unused in 90 days 3
  - Unused 3

	NAME	SERVICE	APPLICATION	TRAFFIC (BYTES, 30 DAYS)	App Usage			
					APPS ALLOWED	APPS SEEN	DAYS WITH NO NEW APPS	COMPARE
10	LAN-to-WAN-Traffic	application-...	any	1.4T	any	147	1	Compare
11	Internal_Traffic	application-...	any	1.5G	any	15	7	Compare
7	Rule for Exam	any	any	0	any	14	48	Compare

# Security Policies

## Policy Optimizer:

Policy Optimizer

- New App Viewer 1+
- Rules Without App Controls 3
- Unused Apps 0
- Log Forwarding for Security Services
- Rule Usage
  - Unused in 30 days 4
  - Unused in 90 days 3
  - Unused 3

Timeframe All time

Usage Unused

Exclude rules reset during the last 90 days

	NAME	Rule Usage			RESET DATE	MODIFIED	CREATED
		HIT COUNT	LAST HIT	FIRST HIT			
4	Known-Bad-EDL-Outbound	0	-	-	-	2024-01-04 09:40:36	2024-01-04 09:40:36
12	intrazone-default	0	-	-	-	2024-01-01 10:14:24	2024-01-01 10:14:24
13	interzone-default	0	-	-	-	2024-01-01 10:14:24	2024-01-01 10:14:24

# Routing

# Routing

Disclaimer:

In this section we will cover the basic configuration of routing for a Palo Alto NGFW firewall. This is a basic configuration class and NOT A ROUTING CLASS! Prior knowledge of basic routing is expected and will be assumed during this section. Configuration of dynamic routing requires matching configurations on both ends of a peering and is outside the scope of this class.



# Routing

PA-VM      DASHBOARD   ACC   MONITOR   POLICIES   OBJECTS   **NETWORK**   DEVICE

Interfaces  
Zones  
VLANs  
Virtual Wires  
**Virtual Routers**  
IPSec Tunnels  
GRE Tunnels

SEARCH

<input type="checkbox"/>	NAME		INTERFACES	CONFIGURATION	RIP
<input type="checkbox"/>	default	▼	ethernet1/5 ethernet1/3 ethernet1/1	ECMP status: Disabled	

# Routing

Ways to route traffic:

- Static Routing
- Dynamic Routing
  - RIP
  - OSPF
  - OSPFv3
  - BGP
  - Redistribution
- Multicast Routing

Virtual Router - default\_vRouter

Router Settings

Name: default\_vRouter

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

General | ECMP

INTERFACES ^

ethernet1/1

ethernet1/1.400

ethernet1/1.410

ethernet1/1.420

ethernet1/2

# Routing

## Static Routes:

Virtual Router - default

Router Settings

**Static Routes**

IPv4 IPv6

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

NAME	DESTINA...	INTERF...
------	------------	-----------

**+** Add **-** Delete **⌂** Clone

Virtual Router - Static Route - IPv4

Name default-route

Destination 0.0.0.0/0

Interface None

Next Hop IP Address

20.1.2.3

Admin Distance 10 - 240

Metric 10

Route Table Unicast

BFD Profile Disable BFD

Path Monitoring

IP Address

Next VR

FQDN

Discard

None

# Routing

## Path Monitoring:

Virtual Router - Static Route - IPv4 ?

Name

Destination

Interface

Next Hop

Admin Distance

Metric

Route Table

BFD Profile

Path Monitoring

Failure Condition  Any  All

Preemptive Hold Time (min)

<input type="checkbox"/>	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT
--------------------------	------	--------	-----------	----------------	--------------------	------------

Path Monitoring Destination ?

Name

Enable

Source IP

Destination IP

Ping Interval(sec)

Ping Count

# Routing

RIP:

Virtual Router - default

Router Settings  Enable  Reject Default Route

Static Routes BFD None

Redistribution Profile

**RIP**

OSPF

OSPFv3

BGP

Multicast

Interfaces | Timers | Auth Profiles | Export Rules

<input type="checkbox"/>	INTERFACE	ENABLE	Default Route		AUTH PROFIL
			ADVERTISE	METRIC	
<input type="checkbox"/>					

Add  Delete

Interface ?

Interface ethernet1/1

Enable

Advertise Default Route

Auth Profile None

Mode normal

BFD Inherit Protocol's Global BFD Profile

# Routing

## OSPF:

Virtual Router - default

Router Settings  Enable  Reject Default Route

Static Routes Router ID IP Address

Redistribution Profile BFD None

RIP

**OSPF**

OSPFv3

BGP

Multicast

Areas | Auth Profiles | Export Rules | Advanced

<input type="checkbox"/>	AREA ID	TYPE	RANGE
--------------------------	---------	------	-------

Virtual Router - OSPF - Area

Area ID 0.0.0.0

Type Range Interface Virtual Link

Type Normal

# Routing

BGP:

Virtual Router - default

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

**BGP**

Multicast

Enable

Router ID IP Address

AS Number

BFD None

**General** | Advanced | Peer Group | Import | Export | Conditional Adv | Aggregate | Redis

Options

- Reject Default Route
- Install Route
- Aggregate MED

Default Local Preference 100

AS Format  2 Byte  4 Byte

Path Selection

- Always Compare MED
- Deterministic MED comparison

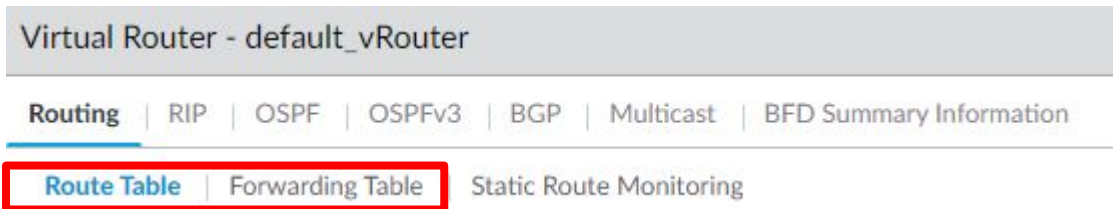
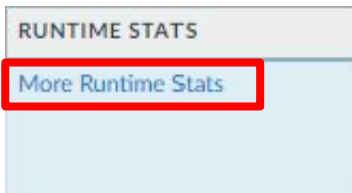
AUTH PROFILES

+ Add - Delete

# Routing

Routing databases:

- Route Table (RIB) - Where all routes are stored
- Forwarding Table (FIB) - Where the route used to forward traffic is stored





# Routing

Routing databases:

Virtual Router - default\_vRouter



Routing | RIP | OSPF | OSPFv3 | BGP | Multicast | BFD Summary Information

Route Table

Forwarding Table | Static Route Monitoring

Route Table  Unicast

Multicast

Display Address Family IPv4 and IPv6

23 items

DESTINATION	NEXT HOP	METRIC	WEIGHT	FLAGS	AGE	INTERFACE
0.0.0.0/0	0.0.0.0	5		A S		sdwan.901
0.0.0.0/0	10.4.0.1	10		S		ethernet1/1
0.0.0.0/0	10.4.1.1	20		S		ethernet1/2
1.1.1.1/32	0.0.0.0	0		A H		
3.3.3.3/32	0.0.0.0	10		A S		sdwan.904
4.4.4.4/32	0.0.0.0	10		A S		sdwan.905

# Routing

Routing databases:

Virtual Router - default\_vRouter



Routing | RIP | OSPF | OSPFv3 | BGP | Multicast | BFD Summary Information

Route Table | **Forwarding Table** | Static Route Monitoring

Display Address Family IPv4 and IPv6

20 items → X

DESTINATION	NEXT HOP	FLAGS	INTERFACE	MTU
0.0.0.0/0	0.0.0.0	u	sdwan.901	1500
1.1.1.1/32	0.0.0.0	uh	loopback.901	1500
3.3.3.3/32	0.0.0.0	u	sdwan.904	1500
4.4.4.4/32	0.0.0.0	u	sdwan.905	1500

# Routing

Routing databases: BGP

Virtual Router - default\_vRouter ? ☰

Routing | RIP | OSPF | OSPFv3 | **BGP** | Multicast | BFD Summary Information

Summary | **Peer** | Peer Group | Local RIB | RIB Out

🔍  2 items → ✕

NAME	GROUP	LOCAL IP	PEER IP	PEER AS	PASSWORD SET	STATUS	STATUS DURATION (SECS.)
Denver-FW_00795400...	branch_007954...	1.1.1.1:34075	3.3.3.3:179	65003	no	Established	178409
Asheville-FW_00795400...	branch_007954...	1.1.1.1:45493	4.4.4.4:179	65004	no	Established	177667

# Routing

Routing databases: BGP

Virtual Router - default\_vRouter



Routing | RIP | OSPF | OSPFv3 | **BGP** | Multicast | BFD Summary Information

Summary | Peer | Peer Group | **Local RIB** | RIB Out

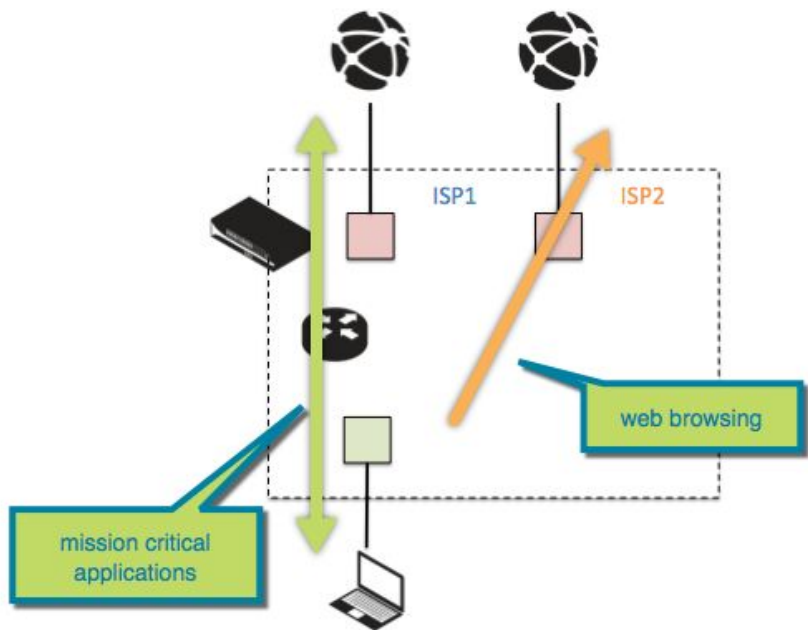
Q 3 items → X

PREFIX	FLAG	NEXT HOP	PEER	WEIGHT	LOCAL PREF.	AS PATH	ORIGIN	MED	FLAP COUNT
172.16.34.0/24	*	3.3.3.3	Denver-FW_0079...	0	100	65003	N/A	0	0
172.16.36.0/24	*	4.4.4.4	Asheville-FW_0079...	0	100	65004	N/A	0	0
172.16.32.0/24	*		Local	0	100		N/A	0	0

# Policy Based Forwarding

# Policy Based Forwarding

Policy Based Routing: [KB Link](#)



# Policy Based Forwarding

Policy Based Routing: [KB Link](#)

- Create Static Routes to each ISP and set the metric of the primary lower than the secondary
- Create a Policy Based Forwarding Policy
- Create Security Policy
- Create NAT Policies

# Policy Based Forwarding

Policy Based Routing: [KB Link](#)

The screenshot shows the PA-VM interface with the 'POLICIES' menu item highlighted in a red box. The left sidebar contains a list of categories, with 'Policy Based Forwarding' also highlighted in a red box. The main content area displays a table with columns for NAME, TAGS, ZONE/INTERFACE, ADDRESS, USER, and ADDRESS, under a 'Source' header. A search bar is visible above the table.

NAME	TAGS	Source			Destin
		ZONE/INTERFACE	ADDRESS	USER	ADDRESS



# Policy Based Forwarding

Policy Based Routing: [KB Link](#)

Policy Based Forwarding Rule	
<b>General</b>	<u>Source</u>   Destination/Application/Service   <u>Forwarding</u>
Name	ISP-PBF
Description	
Tags	
Group Rules By Tag	None
Audit Comment	
	<a href="#">Audit Comment Archive</a>

# Policy Based Forwarding

Policy Based Routing: [KB Link](#)

Policy Based Forwarding Rule

General **Source** Destination/Application/Service | Forwarding

Type  Zone  Any  any

<input type="checkbox"/> ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^	<input type="checkbox"/> SOURCE USER ^
<input checked="" type="checkbox"/> inside		

Negate

Zone dropdown menu:  
Zone  
Interface

# Policy Based Forwarding

Policy Based Routing: [KB Link](#)

## Policy Based Forwarding Rule



General | Source

**Destination/Application/Service**

Forwarding

<input checked="" type="checkbox"/> Any	<input checked="" type="checkbox"/> Any	any
<input type="checkbox"/> DESTINATION ADDRESS ^	<input type="checkbox"/> APPLICATIONS ^	<input type="checkbox"/> SERVICE ^
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>

Negate

# Policy Based Forwarding

Policy Based Routing: [KB Link](#)

## Policy Based Forwarding Rule

General | Source | Destination/Application/Service

**Forwarding**

Action Forward

Egress Interface ethernet1/1

Next Hop IP Address

1.2.3.4

Monitor

Profile


Disable this rule if nexthop/monitor ip is unreachable

IP Address

default

sdwan-default

Tunnel-1\_Monitor

New  Monitor Profile

IP Address to monitor

# USER-ID

# USER-ID

## USER-ID Concepts:

- Group Mapping - User to Group
- User Mapping - User to IP

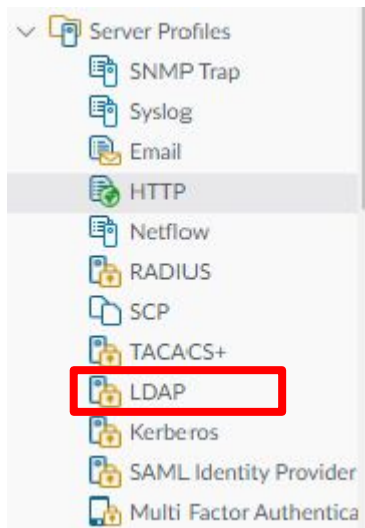
The screenshot shows the Palo Alto Networks management interface for a PA-440 device. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE' (highlighted with a red box). The left sidebar lists various configuration categories, with 'User Identification' highlighted by a red box. The main content area is titled 'Palo Alto Networks User-ID Agent Setup' and contains several configuration options:

- Domain's DNS Name
- Kerberos Server Profile
- Enable Security Log
- Server Log Monitor Frequency (sec) 2
- Enable Session
- Server Session Read Frequency (sec) 10
- Novell eDirectory Query Interval (sec) 30

At the top of the configuration area, there are four tabs: 'User Mapping' (highlighted with a red box), 'Connection Security', 'Terminal Server Agents', and 'Group Mapping Settings' (highlighted with a red box). The 'Trusted Source Address' tab is also visible.

# USER-ID

## Server Profile:



### LDAP Server Profile

Profile Name **Corp-LDAP-Profile**

Administrator Use Only

#### Server List

NAME	LDAP SERVER	PORT
Corp-DC	10.10.10.25	389

**+ Add** **- Delete**

Enter the IP address or FQDN of the LDAP server

#### Server Settings

Type: active-directory

Base DN: **dc=netadminlab,dc-us**

Bind DN: **svc\_paloalto@netadminlab.us**

Password: .....

Confirm Password: .....

Bind Timeout: 30

Search Timeout: 30

Retry Interval: 60

Require SSL/TLS secured connection

Verify Server Certificate for SSL sessions

Notice: Formatting

# USER-ID

## Group Mapping:

Group Mapping ?

Name **Corp-Group-Map**

**Server Profile** | User and Group Attributes | Group Include List | Custom Group

Server Profile **Lab-DC01** Update Interval [60 - 86400]

**Domain Setting**

User Domain

**Group Objects**

Search Filter

Object Class group

**User Objects**

Search Filter

Object Class person

Enabled

Fetch list of managed devices

Group Mapping

Name Corp-Group-Map

Server Profile **User and Group Attributes** G

**User Attributes**

NAME	DIRECTORY ATTRIBUTE
Primary Username	sAMAccountName
E-Mail	mail
Alternate Username 1	userPrincipalName
Alternate Username 2	
Alternate Username 3	

**Group Attributes**

NAME	DIRECTORY ATTRIBUTE
Group Name	name
Group Member	member
E-Mail	mail



# USER-ID

Group Mapping:

Group Mapping ?

Name

Server Profile | User and Group Attributes | **Group Include List** | Custom Group

Available Groups

→ ×

- > cn=keys
- > cn=managed service accounts
- > cn=program data
- > cn=system
- ✓ cn=users
  - cn=accounting
  - cn=allowed rodc password replication
  - cn=cert publishers
  - cn=cloneable domain controllers

⊕  
⊖

Included Groups

- netadminlab\accounting
- netadminlab\engineering

# USER-ID

## User Mapping: PAN-OS Integrated Agent ([Document](#))

User Mapping

Connection Security | Terminal Server Agents | Group Mapping Settings | Trusted Source Address | Auth

Palo Alto Networks User-ID Agent Setup

Domain's DNS Name

Kerberos Server Profile

Enable Security Log

Server Log Monitor Frequency (sec) 2

Enable Session

Server Session Read Frequency (sec) 10

Novell eDirectory Query Interval (sec) 30

Syslog Service Profile

Enable Probing

Probe Interval (min) 20

Enable User Identification Timeout

User Identification Timeout (min) 45

Allow matching usernames without domains

Server Monitoring

<input type="checkbox"/>	NAME	ENABLED	TYPE	NETWORK ADDRESS	STATUS
<input checked="" type="checkbox"/>	Corp-DC	Enabled	Microsoft Active Directory	10.10.10.25	

Add  Delete  Discover

### User Identification Monitored Server

Name Corp-DC

Description

Enabled  
Type Microsoft Active Directory

Transport Protocol WMI

Network Address 10.10.10.25

# USER-ID

## User Mapping: PAN-OS Integrated Agent

User Mapping | Connection Security | Terminal Server Agents | Group Mapping Settings | Trusted Source Address | Auth

Palo Alto Networks User-ID Agent Setup



- Domain's DNS Name
- Kerberos Server Profile
- Enable Security Log
- Server Log Monitor Frequency (sec) 2
- Enable Session
- Server Session Read Frequency (sec) 10
- Novell eDirectory Query Interval (sec) 30
- Syslog Service Profile
- Enable Probing
- Probe Interval (min) 20
- Enable User Identification Timeout
- User Identification Timeout (min) 45
- Allow matching usernames without domains

Server Monitoring

<input type="checkbox"/>	NAME	ENABLED	TYPE	NETWORK ADDRESS	STATUS
--------------------------	------	---------	------	-----------------	--------

[+ Add](#) [- Delete](#) [🔍 Discover](#)

# USER-ID

User Mapping: PAN-OS Integrated Agent

Palo Alto Networks User-ID Agent Setup - hub-stack

**Server Monitor Account**

Server Monitor

Client Probing

Cache

Syslog Filters

Ignore User List

Username netadminlab\svc\_paloalto

Domain's DNS Name 172.16.32.25

Password .....

Confirm Password .....

Kerberos Server Profile None

Notice: Formatting

# USER-ID

## User Mapping: Windows Agent ([Document](#))

- Install Windows Based User Agent ([Document](#))
  - Install on a domain server
- Configure Windows Based Agent ([Document](#))

## User Mapping: Terminal Server Users

- Map individual users coming from a TS environment
- Supported TS
  - Windows
  - Citrix

# Troubleshooting

# Troubleshooting

Configuration Vs Break fix issues: [Support Datasheet](#)

- Palo Alto Support is a break fix organization.
- Palo Alto Partners are used for configuration support.
  
- New configurations not working are not break fix issues. Putting in a ticket for these types of issues will not get you a resolution.
- Break fix is based on previously functioning configuration or device that has stopped working. This could be due to a software upgrade, content update, bug, device failure, etc.

# Troubleshooting

Management: License and Content/PANOS download issues

- Does the device have access to the internet?
- Is the device able to resolve DNS?
- Is the management interface the path to the internet?
- Did you activate the licenses or apply the authorization code?
- Do you own the license for the feature you are trying to use?
- Do you have support on the device?

Premium	
Date Issued	March 20, 2023
Date Expires	November 14, 2024
Description	24 x 7 phone support; advanced replacement hardware service

WildFire License	
Date Issued	March 20, 2023
Date Expires	November 14, 2024
Description	WildFire signature feed, integrated WildFire logs, WildFire API



# Troubleshooting

Troubleshooting tool:

Device -> Troubleshooting

- Policy Match Tests

- Security Policy Match
- QoS Policy Match
- Authentication Policy Match
- Decryption/SSL Policy Match
- NAT Policy Match
- Policy Based Forwarding Policy Match
- DoS Policy Match

- Connectivity Tests

- Routing
- Ping
- Trace Route
- Log Collector Connectivity
- External Dynamic List
- Test Cloud Logging Service Status
- Test Cloud GP Service Status
- Test Wildfire
- Threat Vault
- Update Server

# Troubleshooting

Ping:

The screenshot displays a network testing interface with two main panels: 'Test Configuration' and 'Test Result'. The 'Test Configuration' panel on the left includes a dropdown menu for 'Select Test' set to 'Ping', a 'Count' field with the value '5', and an 'Execute' button. The 'Test Result' panel in the center shows the command 'PING 8.8.8.8'. To the right, a 'Result Detail' panel provides a breakdown of the ping test results, including individual packet responses and summary statistics.

**Test Configuration**

Select Test: Ping

Bypass routing tables and send directly to a host on an attached network

Count: 5

Don't fragment echo request packets (IPv4)

Force to IPv6 destination

Interval: [1 - 2]

Source:

Don't attempt to print addresses symbolically

Pattern:

Size: [0 - 65468]

Tos: [1 - 255]

Ttl: [1 - 255]

Display detailed output

Host: 8.8.8.8

**Test Result**

PING 8.8.8.8

**Result Detail**

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=11.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=11.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=58 time=11.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=58 time=11.5 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=58 time=11.7 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 10ms
rtt min/avg/max/mdev = 11.286/11.527/11.790/0.218 ms
```

# Troubleshooting

## NAT Policy Match:

The screenshot displays the configuration and results of a NAT Policy Match test. The configuration is as follows:

Field	Value
Select Test	NAT Policy Match
From	None
To	None
Source	172.16.32.101
Destination	21.2.36.9
Source Port	[1 - 65535]
Destination Port	443
Protocol	TCP
To Interface	None
Ha Device ID	[0 - 1]

The test result is:

Test Name	Result
NAT Policy Match Result	Match

The result details are:

NAME	VALUE
Result	ISP-1-NAT-Hub

# Troubleshooting

## Routing Test:

The screenshot shows a web interface for configuring and running a routing test. The interface is divided into three main sections: Test Configuration, Test Result, and Result Detail.

**Test Configuration:**

- Select Test: Routing
- Radio buttons:  Fib Lookup,  Mfib Lookup
- Destination IP: 172.16.34.106
- Virtual Router: default\_vRouter
- ECMP section:
  - Source IP: [ ]
  - Source Port: [1 - 65535]
  - Destination IP: [ ]
  - Destination Port: [1 - 65535]
- Buttons: Execute, Reset

**Test Result:**

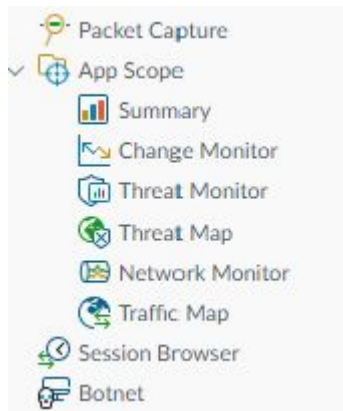
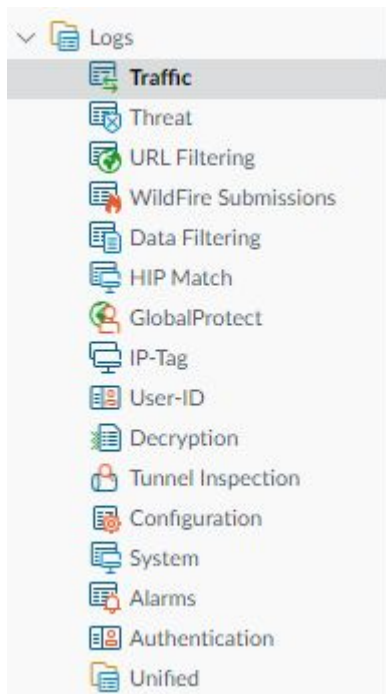
Routing Test Result

**Result Detail:**

NAME	VALUE
Data Plane	dp0
nh	ip
Interface	sdwan.904
Metric	6543






# Troubleshooting

Monitor:



# Troubleshooting

## Monitor: Traffic Logs

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	NAT SOURCE IP	NAT DEST IP	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE
	03/01 09:22:53	end	inside	outside	172.16.32.101	10.4.1.2	172.217.215.100	netadminlab\sue		172.217.215.100			443	ssl	allow	Allow-Files-MSUpdate
	03/01 09:22:53	end	inside	outside	172.16.32.101	10.4.0.2	172.217.215.100	netadminlab\sue		172.217.215.100			443	ssl	allow	Allow-Files-MSUpdate
	03/01 09:22:53	end	inside	outside	172.16.32.25	10.4.0.2	208.67.222.222			208.67.222.222			53	dns-base	allow	Inside-to-Outside-Traffic
	03/01 09:22:53	end	inside	outside	172.16.32.25	10.4.1.2	208.67.222.222			208.67.222.222			53	dns-base	allow	Inside-to-Outside-Traffic
	03/01 09:22:53	end	inside	outside	172.16.32.101	10.4.1.2	74.125.136.190	netadminlab\sue		74.125.136.190			443	youtube-base	allow	Inside-to-Outside-Traffic

### Detailed Log View

General	Source	Destination
Session ID 97955	Source User netadminlab\sue	Destination User
Action allow	Source 172.16.32.101	Destination 172.217.215.100
Action Source from-policy	Source DAG	Destination DAG
Host ID	Country 172.16.0.0-172.31.255.255	Country United States
Application ssl	Port 63541	Port 443
Rule Allow-Files-MSUpdate	Zone inside	Zone outside
Rule UUID acad8078-2f1b-425d-b92c-d89cedb437ed	Interface ethernet1/3	Interface sdwan.901
Session End Reason tcp-fin	NAT IP 10.4.1.2	NAT IP 172.217.215.100
	NAT Port 13375	NAT Port 443

PCAP	RECEIVE TIME	TYPE	APPLICAT...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG... LIST	VERDI...	URL	FILE NAME
	2024/03/01 09:22:53	end	ssl	allow	Allow-Files-MSUp...	acad80...	17...		any				

# Troubleshooting

Changing views for information gathering.

RECEIVE TIME	TYPE	
03/01 11:15:00		<input checked="" type="checkbox"/> NAT Dest IP
03/01 11:15:00		<input checked="" type="checkbox"/> Source User
03/01 11:15:00		<input checked="" type="checkbox"/> Source Dynamic Address Group
03/01 11:15:00		<input checked="" type="checkbox"/> Destination
03/01 11:15:00		<input checked="" type="checkbox"/> Destination Dynamic Address Group
03/01 11:15:05	deny	<input checked="" type="checkbox"/> Dynamic User Group
03/01 11:15:05	deny	<input checked="" type="checkbox"/> To Port
03/01 11:15:05	deny	<input checked="" type="checkbox"/> Application
03/01 11:15:00	deny	<input checked="" type="checkbox"/> Action
03/01 11:15:00	deny	<input checked="" type="checkbox"/> Rule
03/01 11:15:00	deny	<input checked="" type="checkbox"/> Session End Reason

A red box highlights the 'RECEIVE TIME' header and the 'Columns' menu option. The 'Columns' menu is open, showing a list of fields with checkboxes. The 'Session End Reason' option is highlighted in blue.

# Troubleshooting

Filtering Logs:

Manual [refresh] [help]

[add] [remove] [apply]

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	NAT SOURCE IP	NAT DEST IP	SOURCE USER
[info]	03/01 11:15:05	deny	zone-to-branch	inside	172.16.34.1			netadminlab\svc...
[info]	03/01 11:15:05	deny	zone-to-branch	inside	172.16.36.1			netadminlab\svc...
[info]	03/01 11:15:05	deny	zone-to-branch	inside	172.16.34.1			netadminlab\svc...

Click to add as a filter







# Troubleshooting

## Monitor: Traffic Log: NAT Translations

FROM ZONE	TO ZONE	SOURCE	NAT SOURCE IP	NAT SOURCE PORT	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION
lan_zone	wan_zone	192.168.18.100	173.235.189.251	0			134.238.183.164
lan_zone	wan_zone	10.0.41.102	173.235.189.251	6890			17.253.7.141
lan_zone	wan_zone	192.168.18.100	173.235.189.251	7598			170.114.52.2
lan_zone	wan_zone	192.168.18.100	173.235.189.251	14309			17.253.97.203
lan_zone	wan_zone	10.0.40.106	173.235.189.251	52330			71.18.43.229
lan_zone	lan_zone	192.168.18.100		0			192.168.18.1
lan_zone	wan_zone	10.0.40.109	173.235.189.251	28849			8.8.8.8
wan_zone	wan_zone	65.49.20.73		0			173.235.189.251






# Troubleshooting

## Monitor: Threat Logs

	RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION ADDRESS	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	SEVERITY
	12/20 15:14:54	spyware	Parked:gixel.network.me	inside	outside	172.16.32.25			208.67.222.222			53	dns-base	alert	informational
	04/28 13:38:30	flood	PBP Packet Drop	outside		10.6.0.2			0.0.0.0			0	not-applicable	drop	high
	04/27 10:43:23	flood	PBP Packet Drop	outside		10.4.0.2			10.5.1.2			27407	not-applicable	drop	high
	<a href="#">04/27 10:42:19</a>	flood	PBP Packet Drop	outside		10.4.1.2			10.5.0.2			17876	not-applicable	drop	high

# Troubleshooting

## Monitor: URL Logs

	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	APPLICATION	ACTION	HEADERS INSERTED	HTTP/2 CONNECTION SESSION ID
	03/01 09:32:49	computer-and-internet-info	computer-and-internet-info,low-risk	v10.vortex-win.d...	inside	outside	172.16.32.25			51.132.193.104			ssl	alert		0
	03/01 09:32:49	computer-and-internet-info	computer-and-internet-info,low-risk	v10.vortex-win.d...	inside	outside	172.16.32.25			51.132.193.104			ssl	alert		0
	03/01 09:32:49	computer-and-internet-info	computer-and-internet-info,low-risk	v10.vortex-win.d...	inside	outside	172.16.32.25			51.132.193.104			ssl	alert		0
	03/01 09:25:29	streaming-media	streaming-media,low-risk	www.youtube.c...	inside	outside	172.16.32.101	netadminlab\sue		142.250.105.91			youtube-base	alert		98632
	03/01 09:24:58	web-advertisements	web-advertisements,low-risk	match.adsrvr.org...	inside	outside	172.16.32.101	netadminlab\sue		3.33.220.150			web-browsing	alert		98716

# Troubleshooting

## Monitor: Configuration

RECEIVE TIME	ADMINISTRAT...	HOST	CLIENT	COMMA...	RESULT	CONFIGURATION PATH	FULL PATH	BEFORE CHANGE	AFTER CHANGE	SEQUENCE NUMBER
02/29 14:01:08	admin	192.168.18.100	Web	commit	Submitted					7333601583554363397
02/29 14:01:02	admin	192.168.18.100	Web	delete	Succeed...	vsys vsys1 external-list CINS Army Feed	/config/devices/... list/entry[@nam... Army Feed']			7333601583554363396
02/29 14:00:43	admin	192.168.18.100	Web	delete	Succeed...	vsys vsys1 rulebase security rules Test EDL	/config/devices/... EDL']	43decde9-12f9-412c-ab9f-32019a4f27a4		7333601583554363395
02/29 13:55:53	admin	192.168.18.100	Web	commit	Submitted					7333601583554363394
02/29 13:55:44	admin	192.168.18.100	Web	set	Succeed...	vsys vsys1 rulebase security rules Test EDL	/config/devices/... EDL']		Test EDL 43decde9-12f9-412c-ab9f-32019a4f27a4 { profile-setting	7333601583554363393
02/29 13:54:09	admin	192.168.18.100	Web	set	Succeed...	vsys vsys1 external-list CINS Army Feed	/config/devices/... list/entry[@nam... Army Feed']		external-list { CINS Army Feed { type { ip { recurring { five-m	7333601583554363392
01/05 16:57:23	Panorama-admin	0.0.0.0	Panorama	commit-all	Submitted					7320737447833239553

# Troubleshooting

## Monitor: Unified

	LOG TYPE	RECEIVE TIME	LOG SUBTYPE	SESSION ID	SOURCE ZONE	DESTINA... ZONE	SOURCE ADDRESS	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION ADDRESS	DEST... PORT	DESTINATION DYNAMIC ADDRESS GROUP	APPLICATION	ACTION	RULE	BYTES	THREAT ID/NAME	SEVERITY
	url	03/01 09:32:49	url	98950	inside	outside	172.16.32.25			51.132.193.104	443		ssl	alert	Allow-Files-MSUpdate			Informational
	decryption	03/01 09:32:44	0	98962	inside	outside	172.16.32.25			51.132.193.104	443		ssl	allow	Allow-Files-MSUpdate			
	decryption	03/01 09:32:44	0	98950	inside	outside	172.16.32.25			51.132.193.104	443		ssl	allow	Allow-Files-MSUpdate			
	decryption	03/01 09:32:44	0	98953	inside	outside	172.16.32.25			52.167.17.97	443		incomplete	allow	Allow-Files-MSUpdate			
	traffic	03/01 09:32:44	deny	98962	inside	outside	172.16.32.25			51.132.193.104	443		ssl	allow	Allow-Files-MSUpdate	304		
	traffic	03/01 09:32:44	deny	98950	inside	outside	172.16.32.25			51.132.193.104	443		ssl	allow	Allow-Files-MSUpdate	5.2k		

LOG TYPE
url
decryption
decryption
decryption
traffic
traffic

Multiple logs consolidated into one location

# Troubleshooting

## Device -> Packet Capture

Configure Filtering

**Manage Filters** (0/4 Filters Set)

Filtering  ON Pre-Parse Match  OFF

Configure Capturing

Packet Capture  OFF

Search: \_\_\_\_\_

<input type="checkbox"/>	STAGE	FILE
<input checked="" type="checkbox"/>	1	ethernet1/1

**+ Add** **- Delete** Set Selected Packet Capture Filter

**Packet Capture Filter**

<input type="checkbox"/>	ID	INGRESS INTERFACE	SOURCE	DESTINATION	SRC PORT	DEST PORT	PROTO
<input checked="" type="checkbox"/>	1	ethernet1/1					

**Packet Capture Stage** (?)

Stage:

File:   
File name should begin with a letter and can have letters, digits, '.', '+', '\_', and '^'.

Packet Count:

Byte Count:

**+ Add** **- Delete**

Settings

**Clear All Settings**

# Troubleshooting

## Monitor: Session Browser

	START TIME	FROM_ZONE	TO_ZONE	SOURCE	DESTINATION	FROM PORT	TO PORT	PROTOCOL	APPLICATION	RULE	INGRESS I/F	EGRESS I/F	BYTES
⊞	02/29 22:38:20	lan_zone	wan_zone	192.168.18.42	34.111.222.75	34904	443	6	paloalto-dlp-service	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	510634
⊞	03/01 11:12:00	lan_zone	wan_zone	10.0.40.109	8.8.8.8	44421	53	17	dns-base	LAN-to-WAN-Traffic	ethernet1/1400	ethernet1/2	188
⊞	03/01 11:11:51	lan_zone	wan_zone	192.168.18.33	8.8.8.8	44251	53	17	dns-base	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	303
⊞	02/29 11:16:39	lan_zone	wan_zone	192.168.18.100	52.159.127.243	49424	443	6	windows-push-notifications	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	76156
⊞	03/01 11:11:45	lan_zone	wan_zone	192.168.18.30	192.0.2.2	44906	514	17	syslog	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	1363
⊞	03/01 11:12:07	lan_zone	wan_zone	192.168.18.42	35.184.126.116	33298	443	6	paloalto-device-telemetry	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	31294
⊞	03/01 11:09:52	lan_zone	wan_zone	192.168.18.13	107.178.249.217	37787	443	6	paloalto-updates	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	17960
⊞	03/01 11:03:09	lan_zone	wan_zone	192.168.18.50	34.235.175.181	37572	443	6	ssl	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	66513
⊞	03/01 11:11:49	lan_zone	wan_zone	10.0.40.106	104.84.231.148	60052	443	6	tiktok-base	LAN-to-WAN-Traffic	ethernet1/1400	ethernet1/2	519372

# Troubleshooting

Command Line Interface: [Cheat Sheet](#)

- show system info
- show system resources
- show running resource-monitor
- request restart system
- show user group-mapping statistics
- show user group-mapping state all
- show user group list
- show user group name <group-name>
- show user ip-user-mapping all
- show routing route
- ping host <destination-ip-address>
- ping source <ip-address-on-dataplane> host <destination-ip-address>

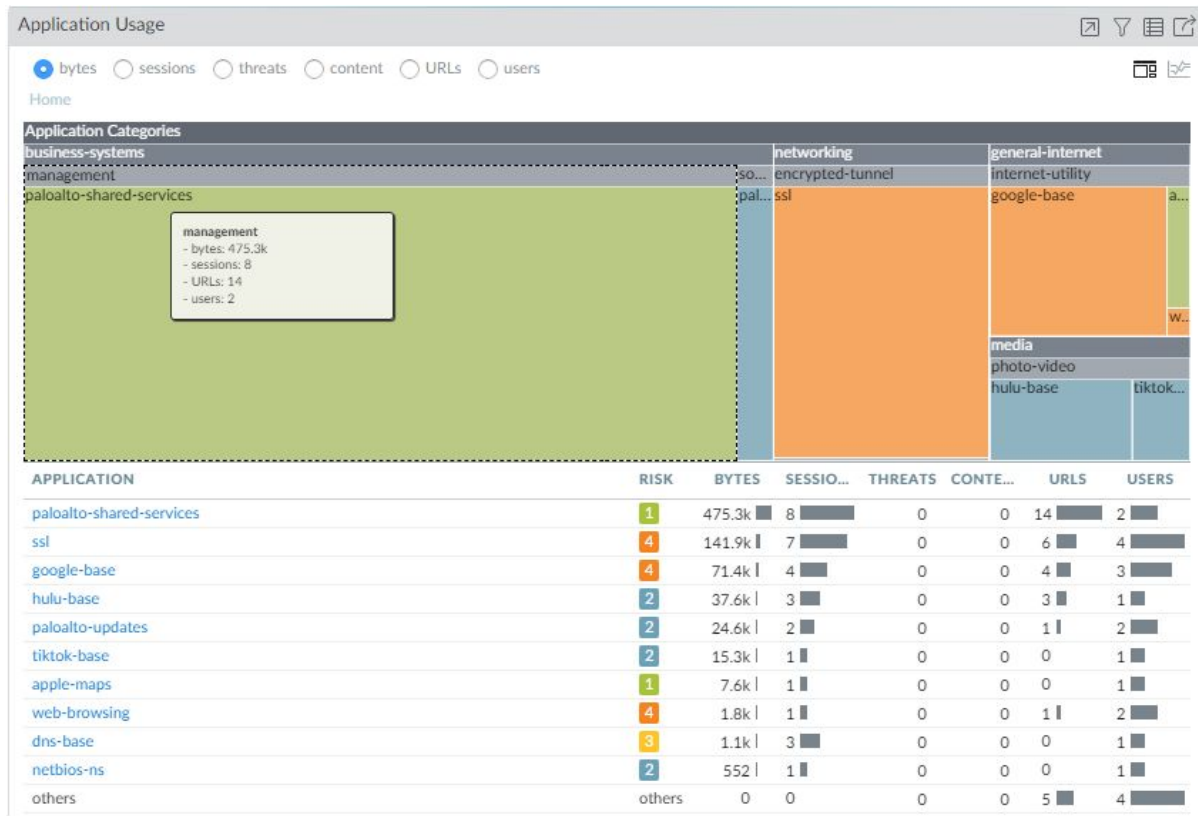


# Troubleshooting

Application Control Center (ACC):

The screenshot displays the Palo Alto Networks Application Control Center (ACC) interface. The top navigation bar includes tabs for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The ACC tab is highlighted. Below the navigation bar, there is an 'Export' button. The main content area shows a navigation bar with 'Network Activity' (selected), Threat Activity, Blocked Activity, Tunnel Activity, GlobalProtect Activity, and SSL Activity. A '+' button is visible to the right of this navigation bar. Below this, the 'Application Usage' section is visible, featuring radio buttons for 'bytes' (selected), 'sessions', 'threats', 'content', 'URLs', and 'users'. The 'Home' link is visible at the bottom left of the interface.

# Troubleshooting

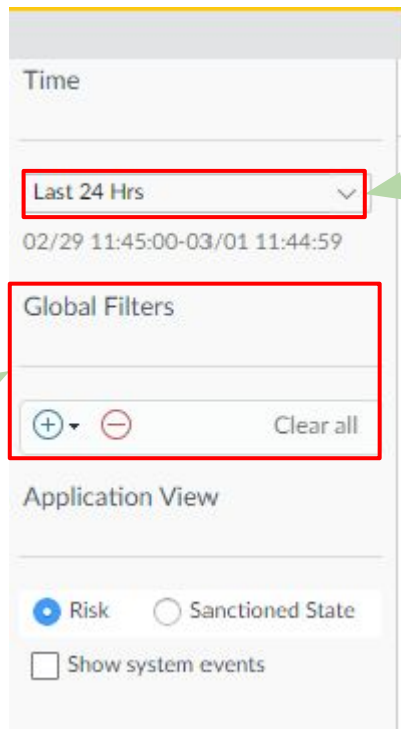


# Troubleshooting

ACC: Filtering



Global Filter



Time

Last 24 Hrs

02/29 11:45:00-03/01 11:44:59

Global Filters

+ - Clear all

Application View

Risk  Sanctioned State

Show system events

This screenshot shows the ACC interface. The 'Time' section has a dropdown menu set to 'Last 24 Hrs'. Below it is a date range '02/29 11:45:00-03/01 11:44:59'. The 'Global Filters' section has a red box around it, containing a plus icon, a minus icon, and a 'Clear all' button. Below that is the 'Application View' section with radio buttons for 'Risk' (selected) and 'Sanctioned State', and a checkbox for 'Show system events'.

Time Filter

APPLICATION

palalto-shared-services

ssl


google-base



Click to add  
to Global  
Filter

# Troubleshooting

Creating a new dashboard in the ACC:

Network Activity  | Threat Activity | Blocked Activity | Tunnel Activity | GlobalProtect Activity | SSL Activity 

**Add Custom Tab** 

Tab Name

WORKSPACE

- Content Activity
- Decryption Failure Reasons
- Destination IP Activity
- Destination Regions
- Destination Zones
- Device Profile Activity
- Egress Interfaces
- Explicit Proxy Authentication Activity
- Explicit Proxy Split based on Auth
- GlobalProtect Deployment Activity
- GlobalProtect Quarantine Activity
- HIP Information
- Hosts Generating Cloud Detected C2 traffic
- Hosts Resolving Malicious Domains
- Hosts Visiting Inline Categorized Malicious URLs

WORKSPACE

2 Column 

# Resources

# Resources

- [PANOS Administrator Guide](#)
- [CLI Cheat Sheet](#)
- [PANOS Recommended Releases](#)
- [Security Advisories](#)
- [Applipedia](#)
- [Hardware EoL List](#)
- [Software EoL List](#)
- [Compatibility Matrix](#)
- [AIOps for NGFW](#)
- [Quick Starts and Hardware Reference](#)
- [Product Selector \(Specifications\)](#)
- [PA Series Hardware Architectures](#)

# Resources

## Purchasing Lab Equipment:

- Palo Alto sells equipment and software designated for testing/lab purposes. This equipment is less expensive than normal equipment with the same functionality. It is not for production as it has a different level of support.
- All customers should have a lab or mock setup for testing purposes. New configurations and software updates should never be introduced into production.
- This is a perfect way to learn and train on platforms without disruptions to your production environment.

*Note: for Palo Alto Partners, this equipment is called NFR and not Lab.*

# Resources

## Cortex Data Lake (CDL)

Storing firewall logs in CDL provides AI/ML driven analytics to be used in AIOps vs only telemetry data to provide insights into your device health and security posture.

Storing firewall logs in CDL gives you an offsite repository of logs that can be accessed anywhere from the CDL App or Panorama.

Off site log storage allows multiple dispersed sites to log to a cloud instance instead of a single Panorama server at one location or multiple log collectors throughout the environment.



# Resources

AIOps:

- Install a device certificate.
- 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](#)

## Explore Apps from Palo Alto Networks



### AIOps for NGFW Free

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.

Launch

[Learn More](#)



### Cortex Data Lake

Enable AI-based innovations for cybersecurity.

Launch

[Learn More](#)

# Resources

## AIOps: Free Vs Premium (ver 3.0)

**Strengthen security posture**  
*Complete coverage in detecting security gaps*

- NEW** Implement security policies that comply with best practices at the time of configuration
- Detect and remediate policy anomalies that degrade security posture
- Maximize usage of underutilized security capabilities
- NEW** Track adoption lifecycle of the configured security features and services with added recommendations
- NEW** Gain deeper insights with best practice and security posture dashboards
- NEW** ATP Dashboard
- NEW** Compliance Summary Dashboard

**Proactively resolve firewall disruptions**  
*Detect and Prevent firewall health problems*

- Detect hardware and software system issues
- Predict operational outcomes using Advanced AI/ML
- Plan upgrades w/ guidance on software versions for your environment
- NEW** Capacity Analyzer
- NEW** Incident and alert experience
- NEW** Gain deeper insights with NGFW SD-WAN dashboard
- NEW** Customized support upon issue detection

**Simplify management at scale**  
*across Prisma Access, PA-Series, and VM series.*

- NEW** Consistent configuration management for uniform enforcement
- NEW** Flexible configuration sharing
- NEW** Auto VPN
- NEW** Scalable cloud-native architecture
- NEW** Consistent security infrastructure management across all enforcement points

**Security and health alert notifications**  
*Know when something needs attention*

- Alerts via email
- Alerts via integration with ServiceNow

**Engagement and support**  
*for all firewall and AIOps for NGFW queries*

- Web Support via Live Community
- Easy 1-click support ticket creation for system issues
- Easy 1-click support ticket creation for operational issues
- NEW** Automatic support ticket creation

**Legend:**

- Available in Free version
- Available in Premium (Paid version). Requires CDL for minimum 30 days.
- With corresponding security subscription

\* Refer full list [here](#)  
NEW = New features introduced in AIOps 3.0

# Questions?

**Thank You!**