

Next-Generation Security Platform and Architecture

PAN-OS® 11.0

Course Overview

Day 1

Platform and Architecture
Initial-Configure
Basic-Interface-Configure
Security-and-NAT-Policies

Lab Installation

Lab Set Management Interface
Lab Connect firewall and Client
Lab Access Internet

Day 2

Site to Site VPN
Backup and Restore Configure
Report Management
High available
Add Panorama on firewall

Lab VPN Site to Site

LAB Captive portal
Lab QOS Shape BW
Lab Block traffic by application
Lab Block URL by web filter

1.

Platforms and Architecture

Hardware Platforms for SMB



PA-220

- 500Mbps FW throughput
- 150Mbps threat prevention
- 64K sessions (max.)
- 8 - 1G – copper
- 15 security zones (max.)
- 2500 policy rules (max.)*



PA-820

- 940Mbps FW throughput
- 610Mbps threat prevention
- 128K sessions
- 4 - 1G - copper
8 - 1G - fiber SFP
- 30 security zones
- 5,000 policy rules*

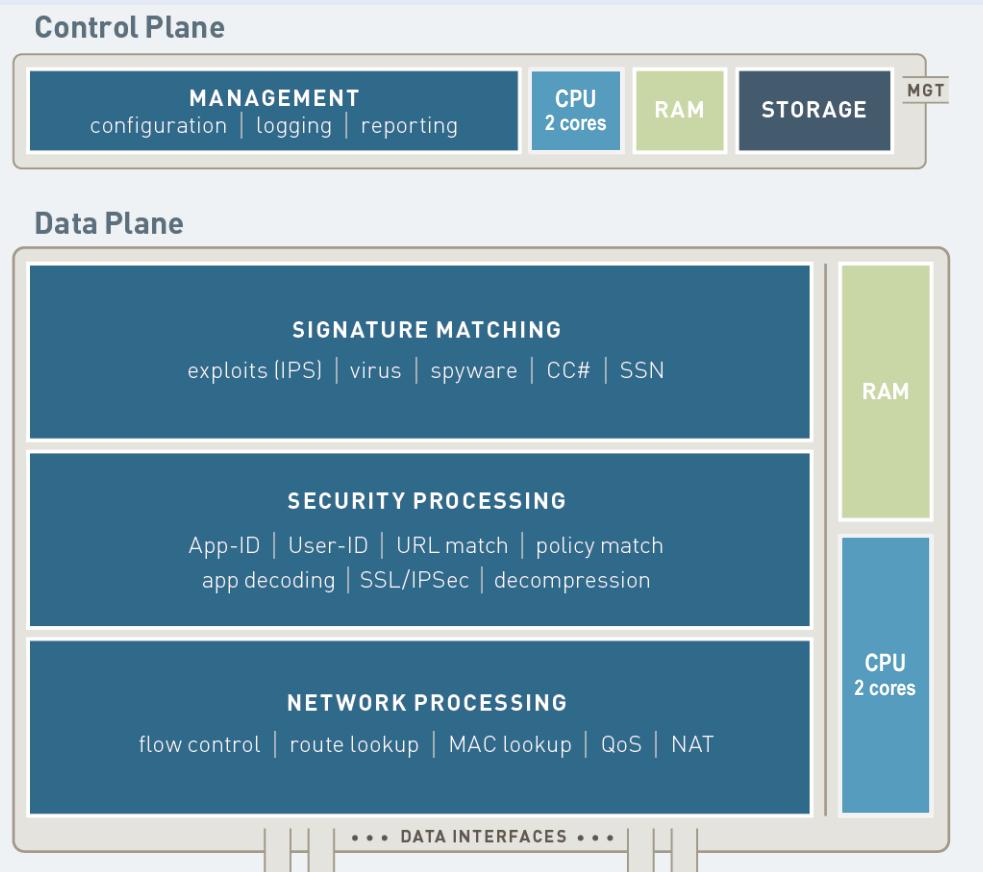


PA-850

- 1.9Gbps FW throughput
- 780Mbps threat prevention
- 192K sessions
- 4 - 1G - copper
4 - 1G - fiber SFP
4 – 1/10G - fiber SFP/+
- 40 security zones
- 5,000 policy rules*

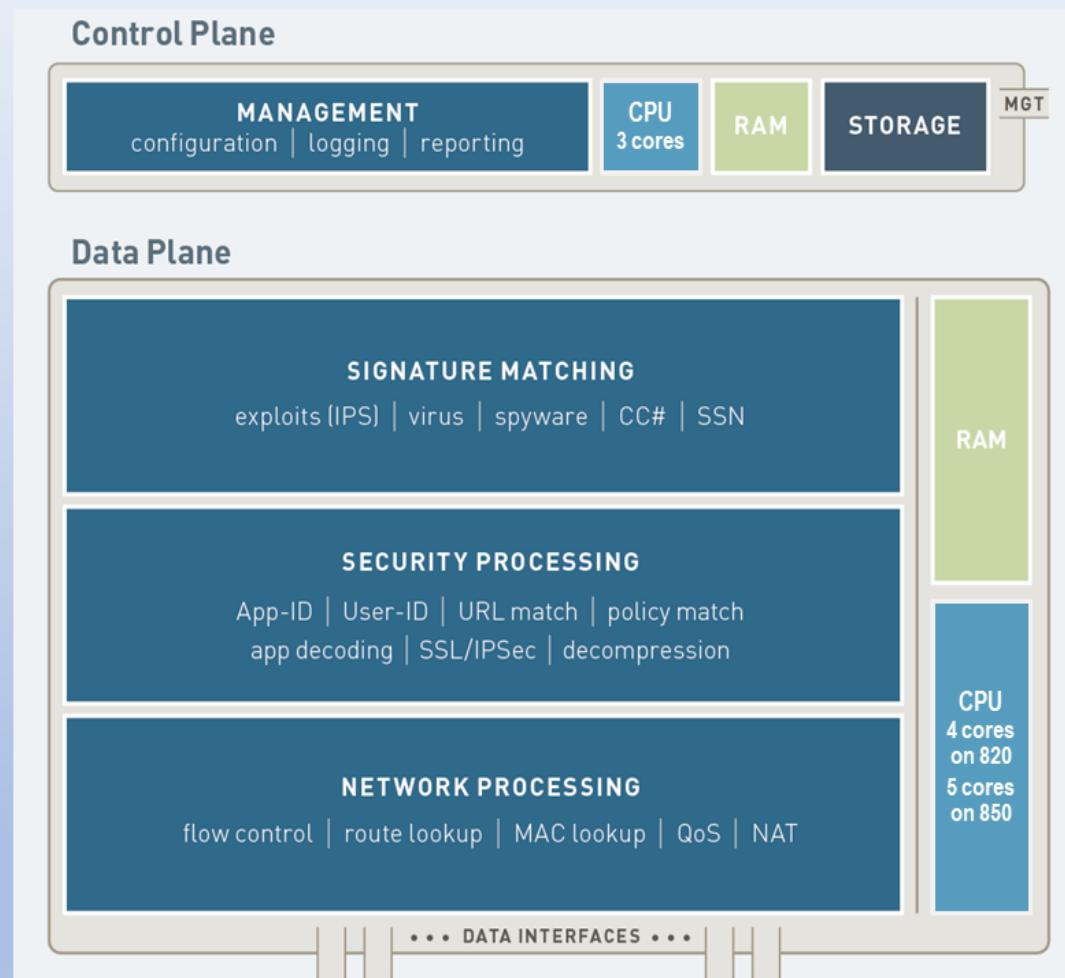
*Maximum capacity of the routing forwarding table per IP version. IPv4 + IPv6 = 2x number of rules.

PA-220 Series Architecture



- 500Mbps firewall throughput
- 150Mbps threat prevention throughput
- 100Mbps IPsec VPN throughput
- 64,000 max. sessions
- 4,200 sessions per second
- 1,000 IPsec VPN tunnels
- 250 GlobalProtect client users
- 2,500 max. number of policies
- 15 security zones

PA-800 Series Architecture (820/850)



- 0.9/1.9Gbps firewall throughput
- 610/780Mbps threat prevention throughput
- 400/500Mbps IPsec VPN throughput
- 130/197K max. sessions
- 8.3/9.5K sessions per second
- 2,000 IPsec VPN tunnels
- 1,000 GlobalProtect users
- 5,000 max. number of policies
- 30/40 security zones

Hardware Platforms for Medium-Size to Large Entities

PA-3000 Series



PA-3020

- 2Gbps FW throughput
- 1Gbps threat prevention
- 250,000 sessions (max.)
- 12 -1G - copper
4 - 1G - SFP
- 40 security zones
- 2,500 policy rules (max.)*



PA-3050

- 4Gbps FW throughput
- 2Gbps threat prevention
- 500,000 sessions (max.)
- 12 -1G - copper
8 - 1G - SFP
- 40 security zones
- 10K policy rules*



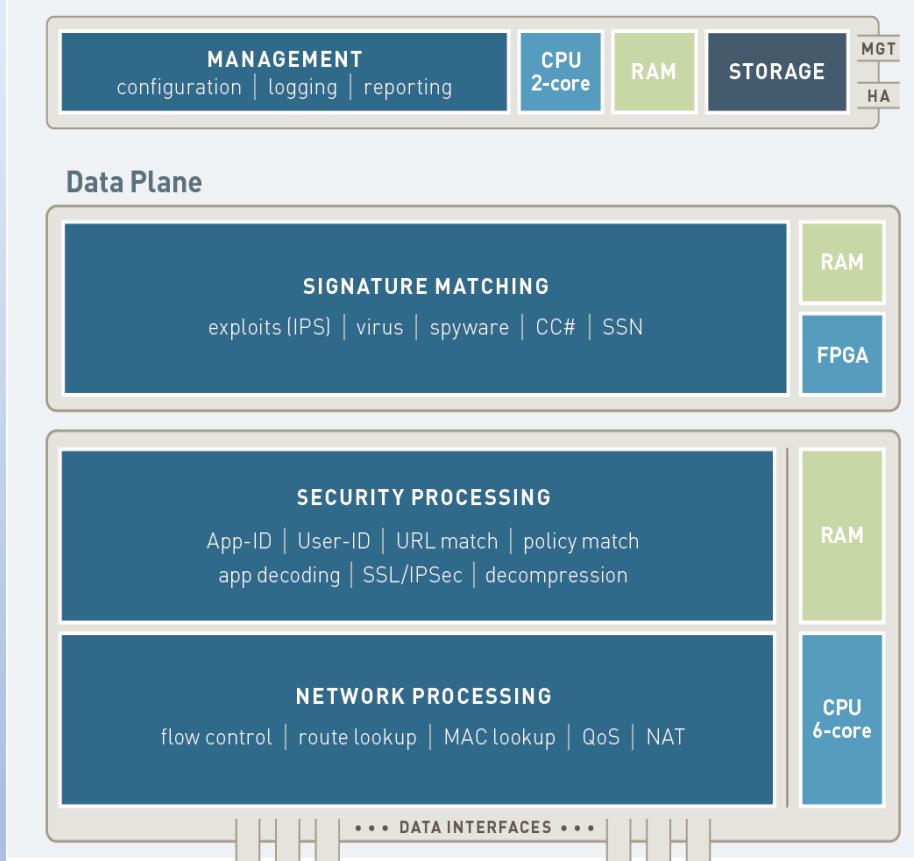
PA-3060

- 4Gbps FW throughput
- 2Gbps threat prevention
- 500,000 sessions (max.)
- 8 -1G - copper
8 - 1G - SFP
2 - 1/10G - SFP/+
- 40 security zones
- 10K policy rules*

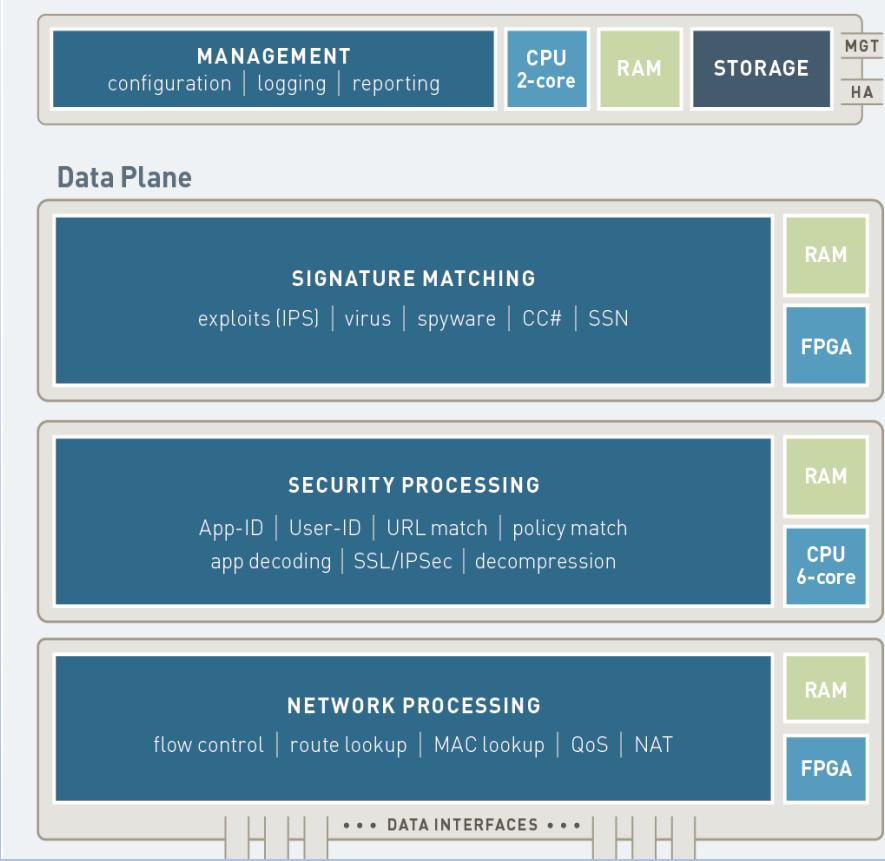
*Maximum capacity of the routing forwarding table per IP version. IPv4 + IPv6 = 2x number of rules.

PA-3000 Series Architecture

PA-3020



PA-3050/3060



VM-Series with Troubleshooting Notes



VM-50

- 50K sessions
- 2,500 rules*
- 15 security zones
- 2 cores



VM-100

- 250K sessions
- 5,000 rules*
- 20 security zones
- 2 cores



VM-300

- 800K sessions
- 10,000 rules*
- 40 security zones
- 2 or 4 cores



VM-500

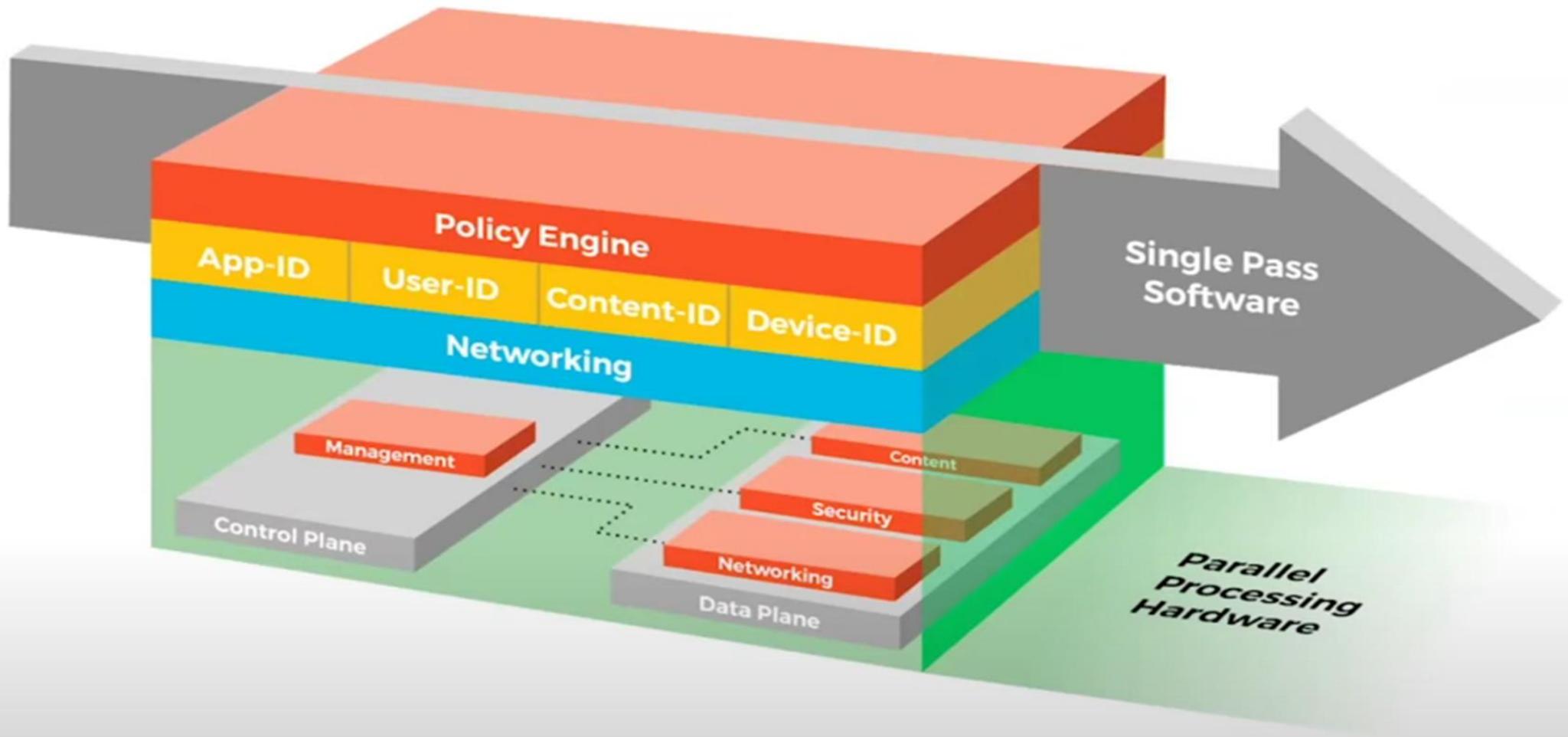
- 2M sessions
- 32,000 rules*
- 200 security zones
- 2, 4, or 8 cores



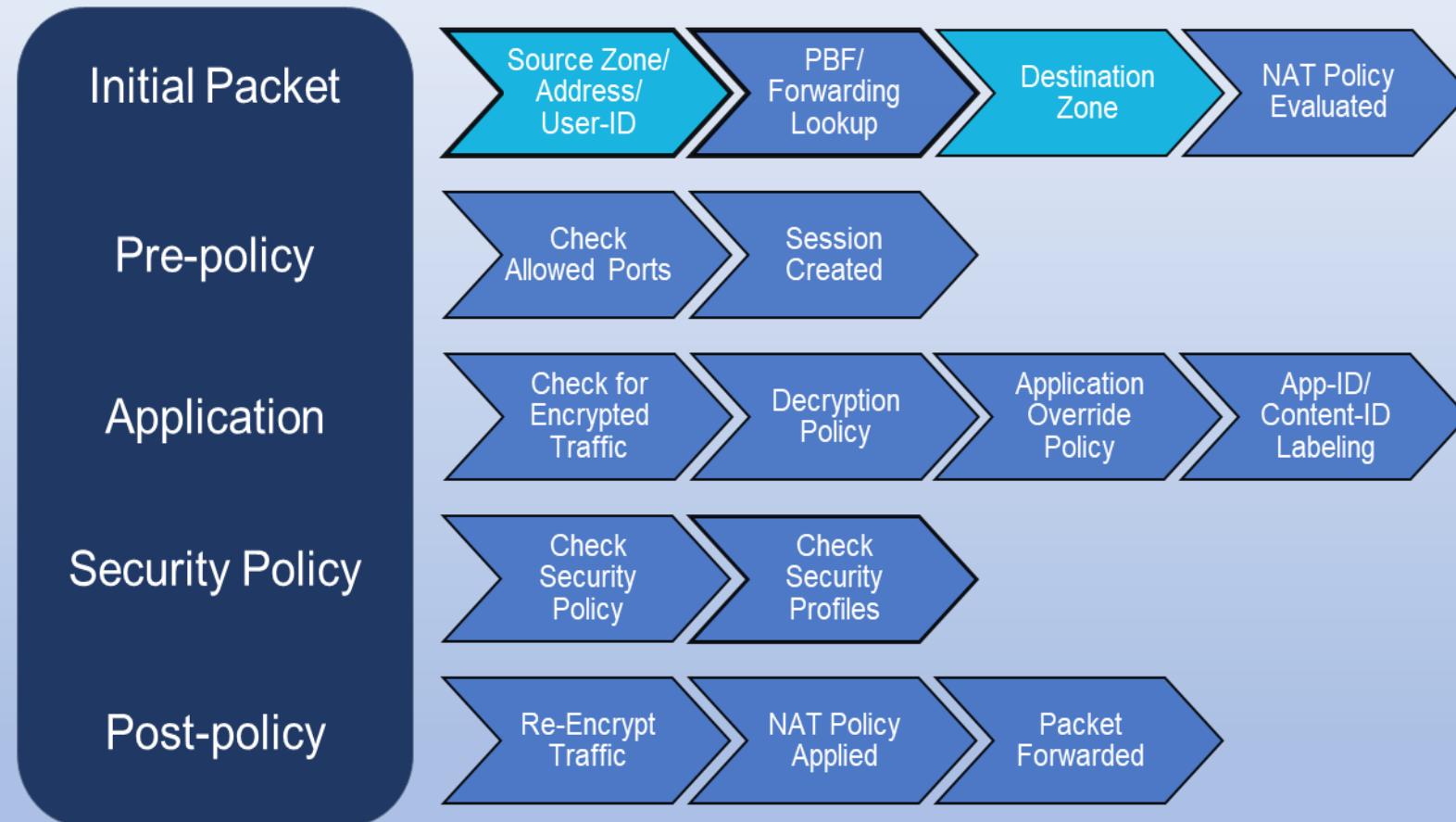
VM-700

- 10M sessions
- 100,000 rules*
- 200 security zones
- 2, 4, 8, or 16 cores

* Maximum capacity of the routing forwarding table.



Flow Logic of the Next-Generation Firewall



Initial Access to the System

Initial Access to the Firewall

Dedicated out-of-band network management

- Ethernet interface (MGT).

- Serial console connection.

IP addressing:

- MGT port has a factory default IP address of 192.168.1.1

- VM-Series MGT port is configured as a DHCP client.

Factory default single administrative account

- Username: admin

- Password: admin

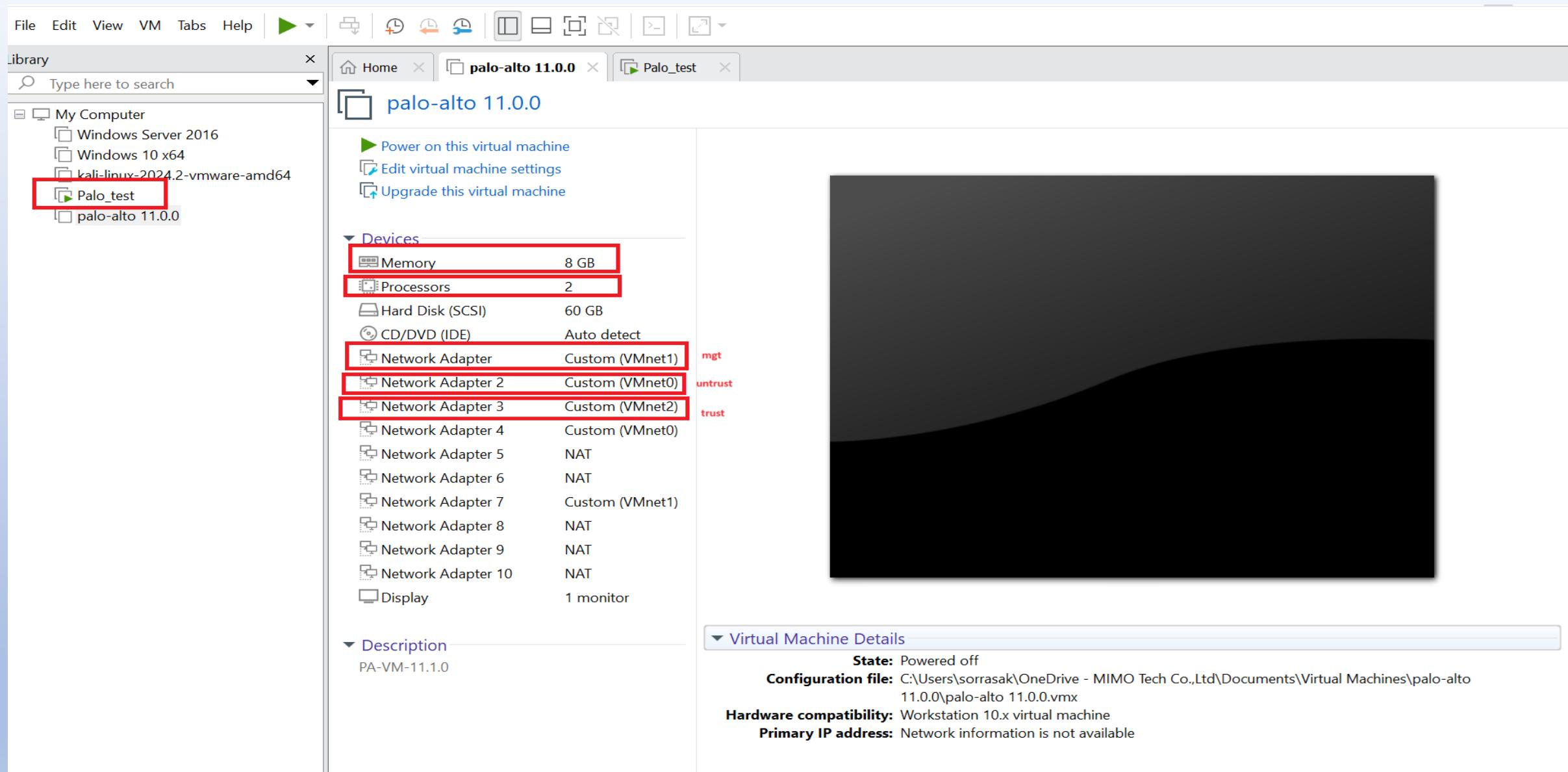
A warning message appears at login in the web interface and the CLI until the default password is changed.

Local admin password is encrypted using the firewall's master key.



Console
Port

MGT
Port



Library x Home x palo-alto 11.0.0 x Palo_test x

Type here to search

My Computer

- Windows Server 2016
- Windows 10 x64
- kali-linux-2024.2-vmware-amd64
- Palo_test
- palo-alto 11.0.0

Last login: Sat Jul 27 00:23:17 on tty1

Number of failed attempts since last successful login: 0

```
admin@PA-VM> configure
admin@PA-VM> [edit]
Entering configuration mode
[edit]
admin@PA-VM# set deviceconfig system t
+ timezone    timezone
> type        Static/DHCP ip-allocation
admin@PA-VM# [set deviceconfig system type static]
[edit]
admin@PA-VM# set deviceconfig system ip
+ ip-address      IP address for the management interface
+ ip-address-lookup-url  ip-address-lookup-url
+ ipv6-address   IPv6 address for the management interface
+ ipv6-default-gateway  IPv6 Default gateway
+ ipv6-enable    enable/disable ipv6 on management interface
> ipv6-gw-type   Static/Dynamic default ipv6 gateway assignment
> ipv6-type     Static/Dynamic ip-allocation
admin@PA-VM# set deviceconfig system ip-address 192.168.1.10 netmask 255.255.255.0 default-gateway 1
92.168.1.1 dns-setting
> dns-proxy-object  dns proxy object to use for resolving dns
> servers          Primary and secondary dns servers
<Enter>           Finish input
admin@PA-VM# set deviceconfig system ip-address 192.168.1.10 netmask 255.255.255.0 default-gateway 1
92.168.1.1 dns-setting servers primary 8.8.8.8
```

Administrative Access

This screenshot shows the Palo Alto Firewall's web-based administrative interface. The top navigation bar includes links for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. The main content area displays 'General Information' with details like Device Name (NewHedge), IP Address (202.208.1.254), and MAC Address (00:98:9C:5D:95:95). Below this are sections for Device Logs (listing various log entries) and System Logs (showing system activity such as updates and configuration changes).

Web Interface

This screenshot shows the 'Panorama' section of the Palo Alto Firewall's web interface. It lists various managed devices under the 'Managed Devices' category. Each device entry includes information such as its name, IP address, and connection status. The interface also includes tabs for Device Status, Virtual Systems, Host, Tags, Serial Number, IP Address, and Template.

Panorama

This screenshot shows the Palo Alto Firewall's SSH or Console CLI interface. The user is at the prompt 'student@Student-DS>'. A detailed command-line menu is displayed, listing various system and network-related commands such as show, config, authentication, and interface.

SSH/Console CLI

```
<response status="success" code="19">
  <result>
    <msg>
      <line>Commit job enqueued with jobid 17</line>
    </msg>
    <job>17</job>
  </result>
</response>
```

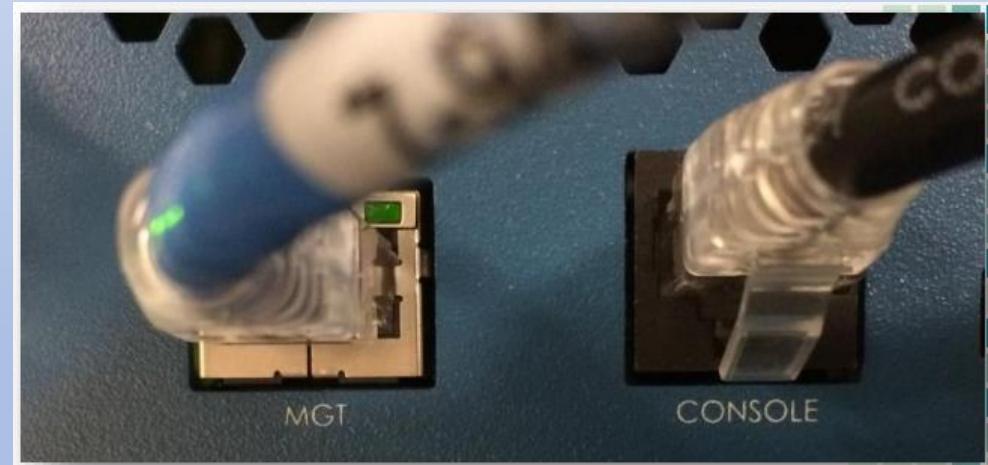
REST XML API

Configuring the MGT Interface – CLI

```
>configure
```

```
#set deviceconfig system ip-address 192.168.101.1 netmask  
255.255.255.0 default-gateway 192.168.101.254 dns-setting  
servers primary 172.16.20.230
```

```
# commit
```



Layout 3 Columns

Widgets

Last updated 15:51:53

5 mins

General Information



Device Name	PA-VM
MGT IP Address	192.168.1.200
MGT Netmask	255.255.255.0
MGT Default Gateway	192.168.1.1
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::20c:29ff:fe43:768f/64
MGT IPv6 Default Gateway	
MGT MAC Address	00:0c:29:43:76:8f
Model	PA-VM
Serial #	007051000255397
CPU ID	ESX:000FA500FFFFB8B17
UUID	564D93F0-553C-5199-3008-5F3F1743768F
VM Cores	2
VM Memory	7.78 GB
VM License	VM-100
VM Capacity Tier	6.5 GB
VM Mode	VMware ESXi
Software Version	11.1.2
GlobalProtect Agent	0.0.0
Application Version	8818-8612 (03/04/24)
Threat Version	8818-8612 (03/04/24)
Antivirus Version	4750-5268 (03/07/24)
Device Dictionary Version	118-481 (03/06/24)
WildFire Version	853801-857666 (03/07/24)
URI Filtering Version	20240308.20132

Logged In Admins



Admin	From	Client	Session Start	Idle For
admin	192.168.100.10	Web	03/07/2024 18:27:46	00:00:04s
_openconfig	127.0.0.1	Web	03/08/2024 00:03:20	00:48:36s

Data Logs



File Name	Name	Time
@ResourceName	Adobe Portable Document Format (PDF)	03/08 00:17:34
@ResourceName	Adobe Portable Document Format (PDF)	03/08 00:17:19
@ResourceName	Adobe Portable Document Format (PDF)	03/08 00:17:04
@ResourceName	Adobe Portable Document Format (PDF)	03/08 00:16:54
@ResourceName	Adobe Portable Document Format (PDF)	03/08 00:16:39
@ResourceName	Adobe Portable Document Format (PDF)	03/08 00:16:29
@ResourceName	Adobe Portable Document Format (PDF)	03/08 00:16:19
@ResourceName	Adobe Portable Document Format (PDF)	03/08 00:16:04
@ResourceName	Adobe Portable Document Format (PDF)	03/08 00:15:54
@ResourceName	Adobe Portable Document Format (PDF)	03/08 00:15:39

System Logs



Description	Time

Config Logs



Command	Path	Admin	Time
commit		admin	03/07 23:52:34
edit	vsys vsys1 rulebase decryption rules test	admin	03/07 23:51:56

Locks



No locks found

ACC Risk Factor (Last 60 minutes)

3.3



Configuring the MGT Interface - GUI

Device > Setup > Management > Management > Interface Settings

The screenshot shows the 'Management Interface Settings' dialog box overlaid on the main interface settings page. The dialog box contains fields for IP Type (Static), IP Address (192.168.100.1), Netmask (255.255.255.0), Default Gateway (192.168.100.254), Speed (auto-negotiate), and MTU (1500). It also lists 'PERMITTED IP ADDRESSES' and 'DESCRIPTION'. Under 'Administrative Management Services', 'HTTPS' and 'SSH' are checked. Under 'Network Services', 'Ping' is checked. At the bottom are 'OK' and 'Cancel' buttons.

Management Interface Settings

PERMITTED IP ADDRESSES	DESCRIPTION

Administrative Management Services

HTTP	HTTPS
<input type="checkbox"/>	<input checked="" type="checkbox"/>
Telnet	SSH
<input type="checkbox"/>	<input checked="" type="checkbox"/>

Network Services

HTTP OCSP	Ping
<input type="checkbox"/>	<input checked="" type="checkbox"/>
SNMP	User-ID
<input type="checkbox"/>	<input type="checkbox"/>
User-ID Syslog Listener-SSL	User-ID Syslog Listener-UDP
<input type="checkbox"/>	<input type="checkbox"/>

OK Cancel

Configure the Hostname and Domain

Device > Setup > Management > General Settings

The screenshot shows the Palo Alto VM interface with the 'DEVICE' tab selected in the top navigation bar. A modal dialog box titled 'General Settings' is open in the center. The 'Hostname' field contains 'Palo-Training' and the 'Domain' field contains 'test.com'. Under the 'SSL/TLS Service Profile' section, 'None' is selected. In the bottom right corner of the dialog, there are 'OK' and 'Cancel' buttons.

General Settings

Hostname: Palo-Training
Domain: test.com

Accept DHCP server provided Hostname
 Accept DHCP server provided Domain

Login Banner:

Force Admins to Acknowledge Login Banner

SSL/TLS Service Profile: None

Time Zone: Asia/Bangkok
Locale: en
Date: 2023/09/10
Time: 02:04:27
Latitude:
Longitude:

Automatically Acquire Commit Lock
 Certificate Expiration Check
 Use Hypervisor Assigned MAC Addresses
 GTP Security
 SCTP Security
 Advanced Routing
 Tunnel Acceleration

OK Cancel

Configure DNS and NTP Servers

Device > Setup > Services

The screenshot shows the Palo Alto VM interface with the following details:

- Header:** PA-VM, DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE, Commit, Undo, Redo, Search.
- Left Sidebar (Setup):**
 - High Availability
 - Config Audit
 - Password Profiles
 - Administrators
 - Admin Roles
 - Authentication Profile
 - Authentication Sequence
 - User Identification
 - Data Redistribution
 - Device Quarantine
 - VM Information Sources
 - Troubleshooting
 - Certificate Management
 - Certificates
 - Certificate Profile
 - OCSP Responder
 - SSL/TLS Service Profile
 - SCEP
 - SSL Decryption Exclusive
 - SSH Service Profile
 - Response Pages
 - Log Settings
 - Server Profiles
 - SNMP Trap
 - Syslog
 - Email
 - HTTP
- Top Navigation:** Management, Operations, Services (selected), Interfaces, Telemetry, Content-ID, WildFire, Session, HSM, DLP.
- Services Section:**
 - Update Server: updates.paloaltonetworks.com
 - Verify Update Server Identity:
 - DNS Servers
 - Primary DNS Server: 8.8.8.8
 - Secondary DNS Server: 8.8.4.4
 - Minimum FQDN Refresh Time (sec): 30
 - FQDN Stale Entry Timeout (min): 1440
 - Proxy Server
 - Primary NTP Server Address
 - Secondary NTP Server Address
- Services Features:** Service Route Configuration
- Bottom Bar:** admin | Logout | Last Login Time: 09/02/2023 00:15:46 | Session Expire Time: 10/10/2023 02:02:27, Tasks, Language, paloalto networks logo.

Service Route Configuration

Device > Setup > Services

The screenshot shows the 'Service Route Configuration' dialog box overlaid on the main 'Management | Operations' interface of the Palo Alto VM. The dialog box is titled 'Service Route Configuration' and contains a table of service routes. The table has columns for SERVICE, SOURCE INTERFACE, and SOURCE ADDRESS. All services listed have 'ethernet1/1' as the source interface and '49.0.116.142/28' as the source address. There are tabs for IPv4, IPv6, and Destination, with IPv4 selected. At the bottom of the dialog box are 'OK' and 'Cancel' buttons.

SERVICE	SOURCE INTERFACE	SOURCE ADDRESS
AutoFocus	ethernet1/1	49.0.116.142/28
CRL Status	ethernet1/1	49.0.116.142/28
Data Services	ethernet1/1	49.0.116.142/28
DDNS	ethernet1/1	49.0.116.142/28
Panorama pushed updates	ethernet1/1	49.0.116.142/28
DNS	ethernet1/1	49.0.116.142/28
External Dynamic Lists	ethernet1/1	49.0.116.142/28
Email	ethernet1/1	49.0.116.142/28
HSM	ethernet1/1	49.0.116.142/28
HTTP	ethernet1/1	49.0.116.142/28
IoT	ethernet1/1	49.0.116.142/28
Kerberos	ethernet1/1	49.0.116.142/28
LDAP	ethernet1/1	49.0.116.142/28

Service Route Configuration

Device > Setup > Services

The screenshot shows the Palo Alto Network Management interface with the following details:

- Header:** PA-VM, DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE, Commit, Lock, Print, Search.
- Left Sidebar (Setup):** High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, Data Redistribution, Device Quarantine, VM Information Sources, Troubleshooting, Certificate Management, Certificates, Certificate Profile, OCSP Responder, SSL/TLS Service Profile, SCEP, SSL Decryption Exclusive, SSH Service Profile, Response Pages, Log Settings, Server Profiles, SNMP Trap, Syslog, Email, HTTP.
- Central View:** Management | Operations, Services, Verify Update, Primary, Secondary, Minimum FQDN Refresh, FQDN Stale Entry T, Primary NTP Se, Secondary NTP Se, Services Features, Service Route Configuration.
- Modal Dialog:** Service Route Configuration (IPv4 tab selected).
 - Use Management Interface for all Customize
 - IPv4 | IPv6 | Destination
 - Table: SERVICE, SOURCE INTERFACE, SOURCE ADDRESS
 - IoT, ethernet1/1, 49.0.116.142/28
 - Kerberos, ethernet1/1, 49.0.116.142/28
 - LDAP, ethernet1/1, 49.0.116.142/28
 - SCEP, ethernet1/1, 49.0.116.142/28
 - SNMP Trap, ethernet1/1, 49.0.116.142/28
 - Service Route Source
 - Service: paloalto-networks-services
 - Source Interface: ethernet1/1
 - Source Address: 49.0.116.142/28
 - Buttons: OK, Cancel
- Bottom Navigation:** admin | Logout | Last Login Time: 09/02/2023 00:15:46 | Session Expire Time: 10/10/2023 02:02:27, Tasks, Language, paloalto.

Licensing and Software Updates

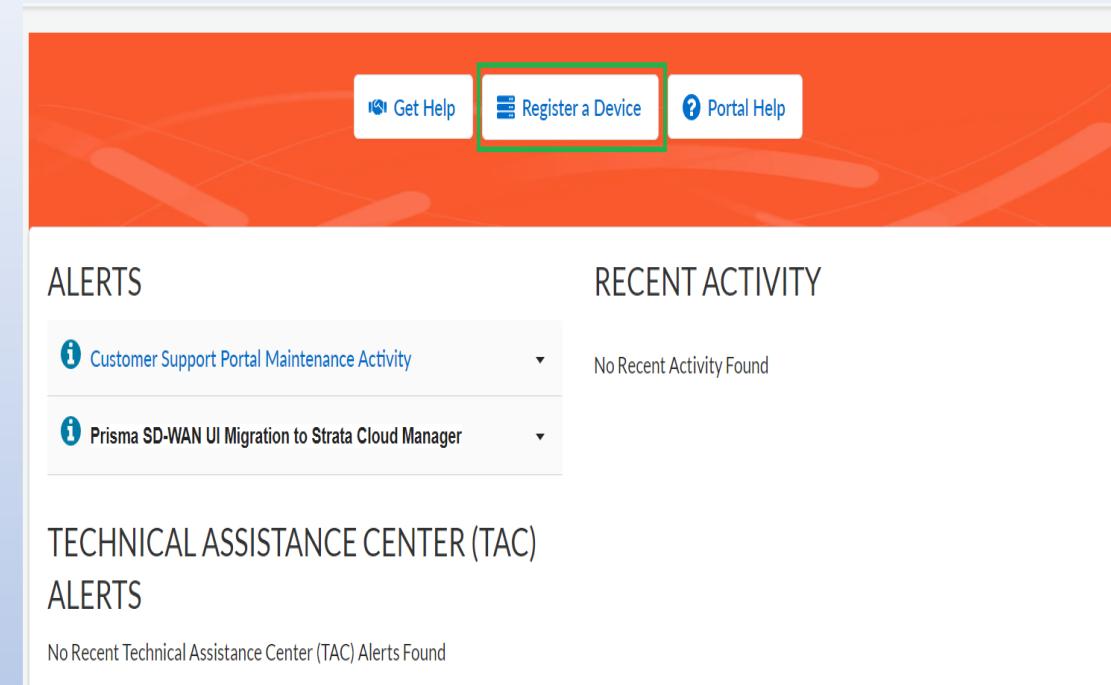
Activating PAN Firewall Services

Register With Palo Alto Networks

- Obtain the Serial Number from the WebUi Dashboard
- Login to <https://support.paloaltonetworks.com>
- If you haven't already, register for a Support account with your serial number enter the assigned serial number and click Register Device

Manage Content Updates

- Updates include the latest application and threat signatures and URL filtering database



Activating PAN VM-Series Firewalls

Register With Palo Alto Networks

- set of authorization codes will be emailed
- Login to <https://support.paloaltonetworks.com>
- If you haven't already, register for a Support account with your capacity auth-code and purchase or sales order number
- Click the Product >Device> VM-Series Auth-Codes
- Authentication Code link to manage your VM-Series firewall licenses and download the software

Activate Licenses

- Select Device >Licenses and select the Activate feature using authentication code link



CUSTOMER SUPPORT PORTAL

- Devices
- Enterprise Agreements
- IONs
- Line Cards/Optics/FRUs
- Manage Shipments
- Search Current Account
- Search Multiple Accounts
- Site Licenses
- Software NGFW Credits
- Software NGFW Devices
- Spares
- Training Credits
- VM-Series Auth-Codes**
- XSOAR
- ZTP Service
- Tools

sorrasak Khunrach

VM-Series Auth-Codes

Auth Code	Quantity of VM Provisioned	Part Description	Expiration Date	ASC	Actions
V6685071	2/10	Palo Alto Networks VM-100 Evaluation	8/17/2023		<button>Register VM</button>
V9577706	1/10	Palo Alto Networks VM-100 Evaluation	7/16/2023		<button>Register VM</button>
V2755489	1/10	Palo Alto Networks VM-100 Evaluation	7/13/2023		<button>Register VM</button>
V1543894	1/10	Palo Alto Networks VM-300 Evaluation	6/22/2023		<button>Register VM</button>
V1604997	3/10	Palo Alto Networks VM-300 Evaluation	5/19/2023		<button>Register VM</button>

[API Key Management](#)[Asset History](#)[Bulk Registration](#)[Bulk Registration History](#)[Cloud Services](#)[CN-Series Licensing](#)[Device Certificates](#)[Devices](#)[Enterprise Agreements](#)[IONs](#)[Line Cards/Optics/FRUs](#)[Manage Shipments](#)[Search Current Account](#)[Search Multiple Accounts](#)[Site Licenses](#)[Software NGFW Credits](#) sorrasak Khunrach

Account Selector

Default

Feedback

Find answers



99+



Credit Pool ID: 2219145951
Expiration Date: 09-07-2026

SUPPORT

Premium

DEPLOYMENT PROFILES

1

CREDIT USAGE

- Allocated 30.27
 - Consumed 30.27
- Available 0.73
- Total Credits 31

[Transfer Credits](#)[Details](#)[Create Deployment Profile](#)

Credit Pool ID: 7702811194
Expiration Date: 06-27-2026

SUPPORT

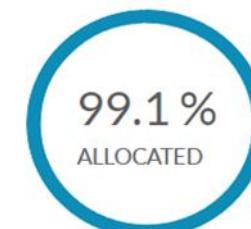
Premium

DEPLOYMENT PROFILES

1

CREDIT USAGE

- Allocated 12.88
 - Consumed 12.88
- Available 0.12
- Total Credits 13

[Transfer Credits](#)[Details](#)[Create Deployment Profile](#)

BLS FW



SSP Select Service Partners NGFW Credits

1 SELECT VM-SERIES OR CN-SERIES

VM-Series

CN-Series

2 NUMBER OF FIREWALLS

1

3 NUMBER OF vCPUs PER FIREWALL

2 vCPUs (Formerly VM-100) with Standard Subscriptions

2

4 ENVIRONMENT

ESXi

5 CUSTOMIZE SUBSCRIPTIONS

Subscription Customization

 Advanced Threat Prevention Advanced URL Filtering Data Loss Protection SD-WAN

CREDIT SUMMARY

Firewall(s)	7.00
Subscriptions * (20% = 1.54 Credits Saved)	6.16
Panorama	0.00
Support	1.97

PERFORMANCE ON ESXI

APP-ID Up to 4 Gbps per Firewall

Threat Prevention Up to 1.5 Gbps per Firewall

● Verified based on HTTP Transaction Size of 64K. Actual performance may vary depending on your server configuration, firewall configuration and hypervisor settings

15.13

CREDITS



GET CREDITS

Licensing

Device > Licenses

Device > Support

Licensing

GlobalProtect Portal

- Date Issued: September 09, 2023
- Date Expires: October 09, 2023
- Description: GlobalProtect Portal License

Premium

- Date Issued: September 09, 2023
- Date Expires: October 09, 2023
- Description: 24 x 7 phone support; advanced replacement hardware service

Threat Prevention

- Date Issued: September 09, 2023
- Date Expires: October 09, 2023
- Description: Threat Prevention

License Management

- [Retrieve license keys from license server](#)
- [Activate feature using authorization code](#)
- [Manually upload license key](#)
- [Deactivate VM](#)
- [Upgrade VM capacity](#)

GlobalProtect Gateway

- Date Issued: September 09, 2023
- Date Expires: October 09, 2023
- Description: GlobalProtect Gateway License

PAN-DB URL Filtering

- Date Issued: September 09, 2023
- Date Expires: October 09, 2023
- Description: Palo Alto Networks URL Filtering License

SD WAN

- Date Issued: September 09, 2023
- Date Expires: October 09, 2023
- Description: License to enable SD WAN feature

WildFire License

- Date Issued: September 09, 2023
- Date Expires: October 09, 2023
- Description: WildFire signature feed, integrated WildFire logs, WildFire API

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Commit ▾ 🔍 ⌂ ?

admin | Logout | Last Login Time: 09/10/2023 02:02:27 | Session Expire Time: 10/10/2023 03:37:30

Tasks | Language

Dynamic Updates

Device > Dynamic Updates

The screenshot shows the Palo Alto VM (PA-VM) interface for managing dynamic updates. The left sidebar is expanded to show the 'Dynamic Updates' section, which is highlighted with a red box. At the bottom of the sidebar, there is a red box around the 'Check Now' button. The main table lists 14 items of dynamic updates, each with columns for Version, File Name, Features, Type, Size, SHA256, Release Date, Download Status, Currently Installed, Action, and Documentation.

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLO...	CURRENTLY INSTALLED	ACTION	DOCUMENTA...
8688-7937	panupv2-all-apps-8688-7937	Apps	Full	60 MB	ebf971ea...	2023/03/20 13:57:21 PDT			Download	Release Notes
8690-7941	panupv2-all-apps-8690-7941	Apps	Full	61 MB	1045a6c...	2023/03/22 16:02:55 PDT			Download	Release Notes
8691-7946	panupv2-all-apps-8691-7946	Apps	Full	61 MB	efcdc491...	2023/03/27 14:05:16 PDT			Download Review Policies Review Apps	Release Notes
8692-7955	panupv2-all-apps-8692-7955	Apps	Full	61 MB	b4ad129...	2023/03/29 13:19:52 PDT			Download	Release Notes
8693-7959	panupv2-all-apps-8693-7959	Apps	Full	61 MB	57836ea...	2023/03/31 10:10:23 PDT			Download	Release Notes
8694-7964	panupv2-all-apps-8694-7964	Apps	Full	61 MB	d1b0f9d9...	2023/04/03 14:38:32 PDT			Download Review Policies Review Apps	Release Notes
8695-7968	panupv2-all-apps-8695-7968	Apps	Full	61 MB	9437569f...	2023/04/05 15:33:17 PDT			Download	Release Notes
8696-7977	panupv2-all-apps-8696-7977	Apps	Full	61 MB	ec5046d...	2023/04/11 13:08:36 PDT	✓		Install Review Policies Review Apps	Release Notes
8697-7981	panupv2-all-apps-8697-7981	Apps	Full	61 MB	bab6ae59...	2023/04/13 19:18:59 PDT			Download	Release Notes
8698-7988	panupv2-all-apps-8698-7988	Apps	Full	61 MB	d6579eb...	2023/04/17 19:02:07 PDT			Download	Release Notes
8699-7991	panupv2-all-apps-8699-7991	Apps	Full	61 MB	4ad3a0bf...	2023/04/18 20:12:54 PDT	✓		Install Review Policies Review Apps	Release Notes

Check Now **Upload** **Install From File**

PAN-OS Software Updates

Device > Software

The screenshot shows the Palo Alto Network Management UI for PAN-OS Software Updates. The top navigation bar includes tabs for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE, with the DEVICE tab selected. The left sidebar provides navigation through various profiles and databases, with the Software category highlighted by a red box. The main content area displays a table of software versions, each with details such as Version, Size, Release Date, Availability, Current Installation status (with a checked checkbox for 11.0.2), Actions (Validate, Export, Install, Reinstall), and Release Notes. The table lists 259 items.

VERSION	SIZE	RELEASE DATE	AVAILABLE	CURRENTLY INSTALLED	ACTION	RELEASE NOTES
11.0.2	497 MB	2023/06/28 12:13:04	Downloaded	<input checked="" type="checkbox"/>	Validate Export Install Reinstall	Release Notes
11.0.2-h1	497 MB	2023/08/16 14:25:42			Validate Download	Release Notes
11.0.1-h2	493 MB	2023/05/30 13:11:06			Validate Download	Release Notes
11.0.1	492 MB	2023/03/29 15:05:25			Validate Download	Release Notes
11.0.0	1037 MB	2022/11/17 08:45:28	Downloaded		Validate Export Install	Release Notes
10.2.5	575 MB	2023/08/17 12:41:56			Validate Download	Release Notes
10.2.4-h3	551 MB	2023/07/05 09:58:19			Validate Download	Release Notes
10.2.4-h2	502 MB	2023/05/16 12:19:44			Validate Download	Release Notes
10.2.4	582 MB	2023/03/30 09:25:44			Validate Download	Release Notes
10.2.4-h4	553 MB	2023/07/27 11:01:55			Validate Download	Release Notes
10.2.3-h4	566 MB	2023/02/13 14:51:11			Validate Download	Release Notes
10.2.3	545 MB	2022/09/29 11:26:49			Validate Download	Release Notes
10.2.3-h2	565 MB	2022/12/13 10:27:27			Validate Download	Release Notes
10.2.2	529 MB	2022/04/07 10:21:50			Validate Download	Release Notes

Check Now Upload

Global Protect Client

CLI Tools

Commands and options must be typed completely

- Tab key and Space bar will auto-complete
- Most output can be piped through a match or except filter to limit results

Online help: ? or Tab key

- Online help will provide a list of available options
 - If no output is given, the preceding option is invalid
 - Standard help messages include:
 - | Pipe command output through match or except filter
- <Enter> Command can be executed without further options

Command Line

```
admin@PA-VM> show
> admins
> advanced-routing
> api-key-expiration-ts
 ould be invalid
> applications
  groups
> arp
> auth
> authentication
> bad-custom-signature
> chassis-ready
> cli
> clock
> cloud-appid
> cloud-auth-service-alerts
e profiles
> cloud-auth-service-metadata
or a region
> cloud-auth-service-profiles
f a tenant for a region
> cloud-auth-service-regions
egions
> cloud-auth-service-tenants
r a region
> cloud-management-status
> cloud-userid
> cluster-flow
> cluster-membership
le
> commit-locks
--more--
```

```
Show active administrators
Show Advanced Routing runtime state
Shows the time before which any API keys wo
uld be invalid
Show applications for application filter or
Show ARP information
auth state variables
Show authentication related information
Show bad performance custom signatures
Show whether dataplane has a running policy
Show CLI properties
Show system date and time
Show cloud appid information
Get alerts from cloud authentication servic
Get cloud authentication service metadata f
Get cloud authentication service profiles o
Get cloud authentication service deployed r
Get cloud authentication service tenants fo
Show cloud management connection status
Show cloud userid information
Show flow information
information of membership global member tab
Show list of commit locks
```

```
admin@PA-VM> traceroute source 49.0.116.142 host 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
1 49.0.116.130 (49.0.116.130) 10.518 ms 10.531 ms 10.528 ms
2 49-231-33-6.sbn-idc.com (49.231.33.6) 10.522 ms 10.518 ms 10.523 ms
3 49-231-33-5.sbn-idc.com (49.231.33.5) 10.517 ms 10.513 ms 10.510 ms
4 49.231.47.132 (49.231.47.132) 10.504 ms 10.484 ms 10.480 ms
5 * * *
6 103-3-64-242.ais-idc.com (103.3.64.242) 32.317 ms 31.683 ms 31.555 ms
7 216.239.41.111 (216.239.41.111) 31.539 ms 31.496 ms 31.485 ms
8 209.85.245.51 (209.85.245.51) 29.426 ms 29.440 ms 29.394 ms
9 dns.google (8.8.8.8) 29.381 ms 29.378 ms 29.370 ms
admin@PA-VM>
```

```
admin@PA-VM> ping source 49.0.116.142 host 8.8.8.8
PING 8.8.8.8 (8.8.8.8) from 49.0.116.142 : 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=57 time=29.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=57 time=28.10 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3ms
rtt min/avg/max/mdev = 28.988/29.271/29.554/0.283 ms
admin@PA-VM>
```

```
admin@PA-VM> show interface all
total configured hardware interfaces: 6
name id speed/duplex/state mac address
----- -----
ethernet1/1 16 10000/full/up 00:50:56:b4:7f:bc
ethernet1/2 17 10000/full/up 00:50:56:b4:e4:a3
ethernet1/3 18 10000/full/up 00:50:56:b4:65:2f
ethernet1/4 19 10000/full/up 00:50:56:b4:84:7f
ethernet1/5 20 10000/full/up 00:50:56:b4:d2:e1
tunnel 4 [n/a] [n/a]/up 7c:89:c3:7d:10:04

aggregation groups: 0

total configured logical interfaces: 7
name id vsys zone forwarding tag address
----- -----
ethernet1/1 16 1 Untrust vr:default 0 49.0.116.142/28
ethernet1/2 17 1 Trust vr:default 0 10.252.112.54/29
ethernet1/3 18 1 SGL vr:default 0 10.250.250.1/24
ethernet1/4 19 1 Untrust vr:default 0 192.168.1.1/24
ethernet1/5 20 1 WLC_Minor vr:default 0 10.200.200.2/30
tunnel N/A
tunnel.100 256 1 SSL vr:default 0 N/A
admin@PA-VM>
```

show Command

The show command will display information about the current candidate configuration

 49.0.116.142 - PuTTY

```
admin@PA-VM> show
> admins                                Show active administrators
> advanced-routing                      Show Advanced Routing runtime state
> api-key-expiration-ts                Shows the time before which any API keys would be invalid
> applications                          Show applications for application filter or groups
> arp                                    Show ARP information
> auth                                   auth state variables
> authentication                         Show authentication related information
> bad-custom-signature                  Show bad performance custom signatures
> chassis-ready                         Show whether dataplane has a running policy
> cli                                    Show CLI properties
> clock                                  Show system date and time
> cloud-appid                           Show cloud appid information
> cloud-auth-service-alerts             Get alerts from cloud authentication service profiles
> cloud-auth-service-metadata          Get cloud authentication service metadata for a region
> cloud-auth-service-profiles          Get cloud authentication service profiles of a tenant for a region
> cloud-auth-service-regions          Get cloud authentication service deployed regions
> cloud-auth-service-tenants          Get cloud authentication service tenants for a region
> cloud-management-status            Show cloud management connection status
> cloud-userid                           Show cloud userid information
> cluster-flow                           Show flow information
> cluster-membership                    information of membership global member table
> commit-locks                           Show list of commit locks
> config                                 Show configuration
> config-locks                          Show list of config locks
> counter                               Show system counter information
> ctd-agent                             Show ctd-agent related information
```

ping Command

ping source <IP address> host <IP address>

```
admin@PA-VM> ping
+ bypass-routing      Bypass routing tables and send directly to a host on an attached network
+ count               Number of requests to send (1..2000000000 packets)
+ do-not-fragment    Don't fragment echo request packets (IPv4)
+ inet6              Force to IPv6 destination
+ interval            Delay between requests (seconds)
+ no-resolve          Don't attempt to print addresses symbolically
+ pattern             Hexadecimal fill pattern
+ size                Size of request packets (0..65468 bytes)
+ source              Source address of echo request
+ tos                 IP type-of-service value (0..255)
+ ttl                IP time-to-live value (IPv6 hop-limit value) (0..255 hops)
+ verbose             Display detailed output
* host                Hostname or IP address of remote host
```

```
admin@PA-VM> ping [REDACTED]
```

```
admin@PA-VM> ping source 49.0.116.142 host 8.8.8.8
PING 8.8.8.8 (8.8.8.8) from 49.0.116.142 : 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=57 time=30.0 ms
^C
--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 30.005/30.005/30.005/0.000 ms
admin@PA-VM> [REDACTED]
```

Reset to Factory Configuration

```
firewall-a login: admin  
Password:  
Last login: Tue Jun 30 21:23:36 on tty1
```

```
Number of failed attempts since last successful login: 0
```

```
admin@firewall-a> request system private-data-reset  
Executing this command will remove all logs and configuration will revert back to factory defaults. The system will restart and then reset the data. Are you sure you want to continue? (y/n) (y or n) _
```

If you know the admin account password you can reset a firewall to its factory default settings from CLI with command **request system private-data-reset**.

- Erases all logs, resets all settings, including IP addressing, which causes loss of connectivity

If you do not know the admin account password, you must first place the firewall in maintenance mode.

As the firewall is booting up, type the command **maint** into the CLI through the console port.

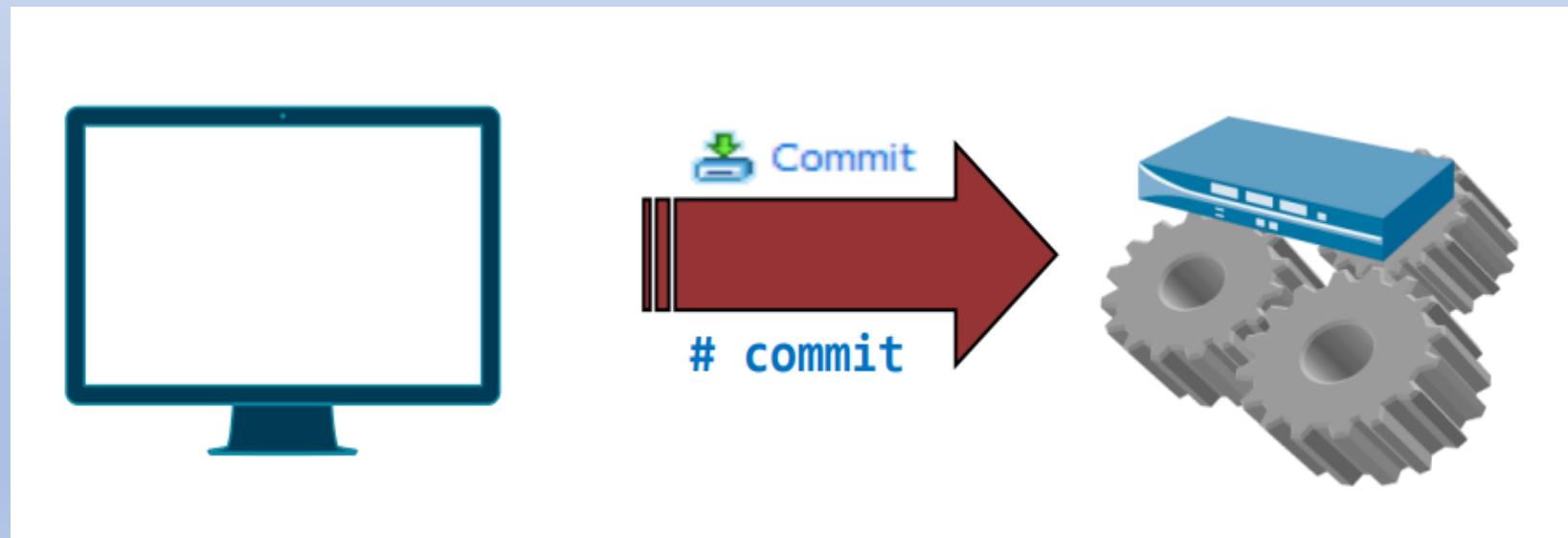
After some time, you can choose the option: Reset to Factory Default

Configuration Management

Config Types

Candidate Config

- What is shown in the UI becomes Running Config upon successful Commit
- Running Config
- Active on the firewall



Configuration Management

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Commit | 🔍 | ⚙️ | ?

Setup

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

 - Certificates
 - Certificate Profile
 - OCSP Responder
 - SSL/TLS Service Profile
 - SCEP
 - SSL Decryption Exclusive
 - SSH Service Profile

- Response Pages
- Log Settings
- Server Profiles

 - SNMP Trap
 - Syslog
 - Email
 - HTTP

Management | Operations | Services | Interfaces | Telemetry | Content-ID | WildFire | Session | HSM | DLP

Operations

Configuration Management

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

Device Operations

- Reboot Device
- Shutdown Device

Miscellaneous

- Custom Logos
- SNMP Setup

admin | Logout | Last Login Time: 09/02/2023 00:15:46 | Session Expire Time: 10/10/2023 02:02:27

Tasks | Language

paloaltonetworks

Config Auditing

- Any two configuration files can be compared
- The differences between the two compared files are displayed
- Device > Config Audit

The screenshot shows the 'PA-VM' interface with the 'DEVICE' tab selected. On the left, a sidebar lists various configuration categories like Setup, High Availability, and Certificates. The 'Config Audit' section is highlighted.

The main area displays a 'Candidate Configuration' table comparing two configurations. The table has two columns for code snippets, each with line numbers and a '...' button. A header row indicates the configuration was committed on 2023/03/17 at 04:28:23 by Admin.

Candidate Configuration		54 Committed On 2023/03/17 04:28:23 By Admin
...
120 mfa-enable no;	120 mfa-enable no;	
121 }	121 }	
122 method {	122 method {	
123 local-database;	123 local-database;	
124 }	124 }	
125 allow-list all;	125 allow-list all;	
126 }	126 }	
127 }	127 }	
128 local-user-database {	128 local-user-database {	
129 user {	129 user {	
130 sorrasak {	130 KK {	
131 phash \$1\$aaawtgewe\$qZbjMeOVn.B4b7vj9JA01;	131 phash \$1\$ujcnfenv\$cLFN3gXT5ql39wapRql9R1;	
132 }	132 }	
133 chanon {	133 sorrasak {	
134 phash \$1\$xejtrqgh\$.jwQBB7yJqmgynpK3RDp.0;	134 phash \$1\$aaawtgewe\$qZbjMeOVn.B4b7vj9JA01;	
135 }	135 }	
136 naparat {	136 chanon {	
137 phash \$1\$okmgkvht\$0meLss2bLrDAbEC6AGDPE1;	137 phash \$1\$xejtrqgh\$.jwQBB7yJqmgynpK3RDp.0;	
138 }	138 }	
139 mongcolc {	139 naparat {	
140 phash \$1\$qibuwthr\$kmrRwA/d0l3tP3XU.5f1G0;	140 phash \$1\$lfujhqqq\$z6J8P685JUBAAe8PhgdRD.;	
141 }	141 }	
142 awn {	142 mongcolc {	
143 phash \$1\$pxtiojys\$1eKV RTPn32.ozvfDeM891/;	143 phash \$1\$bxsnpypycc\$KT.5WZe7RMaCxJUgGe3k./;	

At the bottom, there are navigation buttons for 'Local Candidate config', a date/time selector ('54 Committed On 2023/03/17 04:28:23 by at'), 'Context 10', and a 'Go' button. The footer includes links for 'Tasks', 'Language', and the 'paloaltonetworks' logo.

User Management

Administrator Roles

A role defines the type of access an administrator has to the system

- Dynamic Roles: Built-in roles such as Superuser and Device Administrator
- Admin Role Profiles: Custom-made roles

The screenshot shows the configuration of an administrator role and the creation of an admin role profile.

Administrator Configuration:

- Name: [Redacted]
- Authentication Profile: None
- Use only client certificate authentication (Web UI):
- Password: [Redacted]
- Confirm Password: [Redacted]
- Password Requirements:
 - Minimum Password Length (Count) 8
- Use Public Key Authentication (SSH):
- Administrator Type: Dynamic Role Based
- Superuser: [Redacted]
- Password Profile: None

Admin Role Profile Creation:

The "Admin Role Profile" dialog is open, showing two tabs: Web UI and XML API. Both tabs have a "Selected" section and a "Available" section with checkboxes.

Web UI Tab:

- Selected:** Dashboard, ACC, Monitor, Logs, Traffic, Threat, URL Filtering, WildFire Submissions, Data Filtering, HIP Match, GlobalProtect, IP-Tag, User-ID, Decryption, Tunnel Inspection.
- Available:** Report, Log, Configuration, Operational Requests, Commit, User-ID Agent, IoT Agent, Export, Import.

XML API Tab:

- Selected:** Report, Log, Configuration, Operational Requests, Commit, User-ID Agent, IoT Agent, Export, Import.
- Available:** Report, Log, Configuration, Operational Requests, Commit, User-ID Agent, IoT Agent, Export, Import.

Legend: Enable Read Only Disable

Creating Administrator Accounts

Device > Administrators

Administrator

Name	<input type="text"/>
Authentication Profile	<input type="text"/> None
<input type="checkbox"/> Use only client certificate authentication (Web)	
Password	<input type="text"/>
Confirm Password	<input type="text"/>
Password Requirements	
• Minimum Password Length (Count) 8	
<input type="checkbox"/> Use Public Key Authentication (SSH)	
Administrator Type	<input checked="" type="radio"/> Dynamic <input type="radio"/> Role Based
Superuser	
Password Profile	<input type="text"/> None

OK Cancel

Authentication Profile

Name	<input type="text"/>
Authentication	
Factors	<input type="text"/>
Advanced	
Type	<input type="text"/> None
User Domain	<input type="text"/> None
Username Modifier	<input type="text"/> Cloud Authentication Service
Single Sign On	<input type="text"/> Local Database
Kerberos Realm	
RADIUS	
LDAP	
TACACS+	
SAML	
Kerberos	

Administrator

Name	<input type="text"/>
Authentication Profile	<input type="text"/> None
<input type="checkbox"/> Use only client certificate authentication (Web)	
Password	<input type="text"/>
Confirm Password	<input type="text"/>
Password Requirements	
• Minimum Password Length (Count) 8	
<input type="checkbox"/> Use Public Key Authentication (SSH)	
Administrator Type	<input checked="" type="radio"/> Dynamic <input type="radio"/> Role Based
Superuser	
Profile	<input type="text"/> Superuser
Superuser (read-only)	
Device administrator	
Device administrator (read-only)	

Administrator

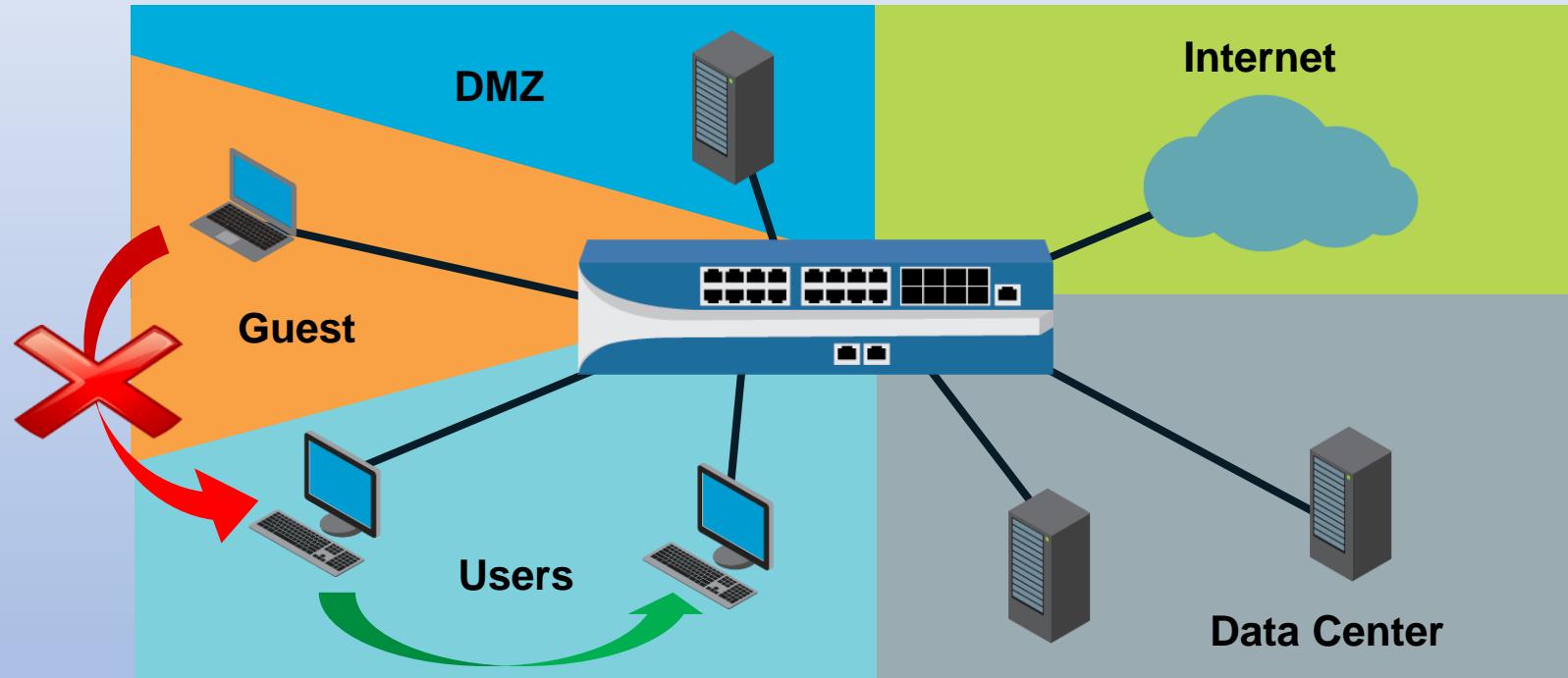
Name	<input type="text"/>
Authentication Profile	<input type="text"/> None
<input type="checkbox"/> Use only client certificate authentication (Web)	
Password	<input type="text"/>
Confirm Password	<input type="text"/>
Password Requirements	
• Minimum Password Length (Count) 8	
<input type="checkbox"/> Use Public Key Authentication (SSH)	
Administrator Type	<input type="radio"/> Dynamic <input checked="" type="radio"/> Role Based
Profile	<input type="text"/> auditadmin
cryptoadmin	
securityadmin	
New Admin Role Profile	

3. Basic Interface Config

Security Zones

Security Zones and Security Policy Rules

- Traffic within a zone is *allowed* by default.
- Traffic between zones is *denied* by default.



Interface Types and Zone Types

- Different zone types support only specific interfaces types:

Tap Zone

Tap interfaces

Layer 2 Zone

Layer 2 interfaces

Layer 3 Zone

- Layer 3 interfaces
- VLAN interfaces
- Loopback interfaces
- Tunnel interfaces

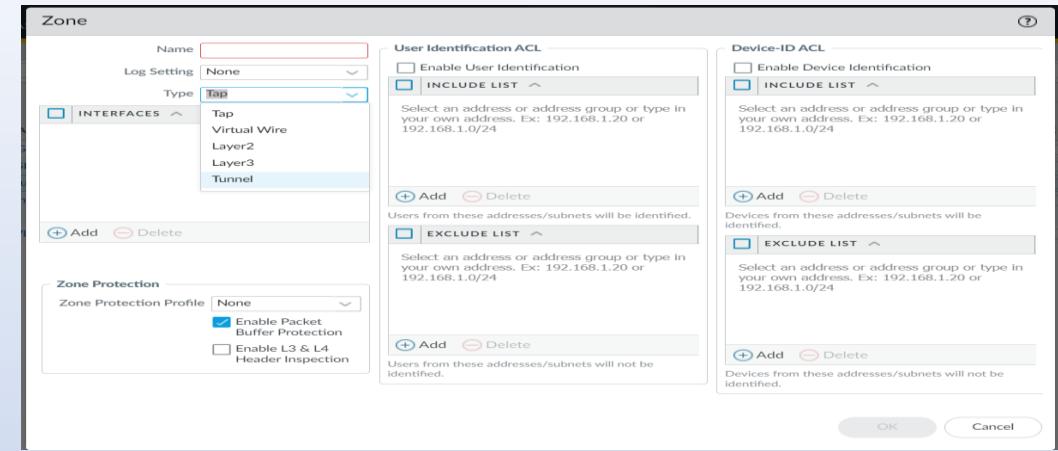
Tunnel Zone

No interfaces assigned

Virtual Wire Zone

Virtual Wire interfaces

- MGT and HA interfaces are not assigned to a zone



Security Zone Interfaces

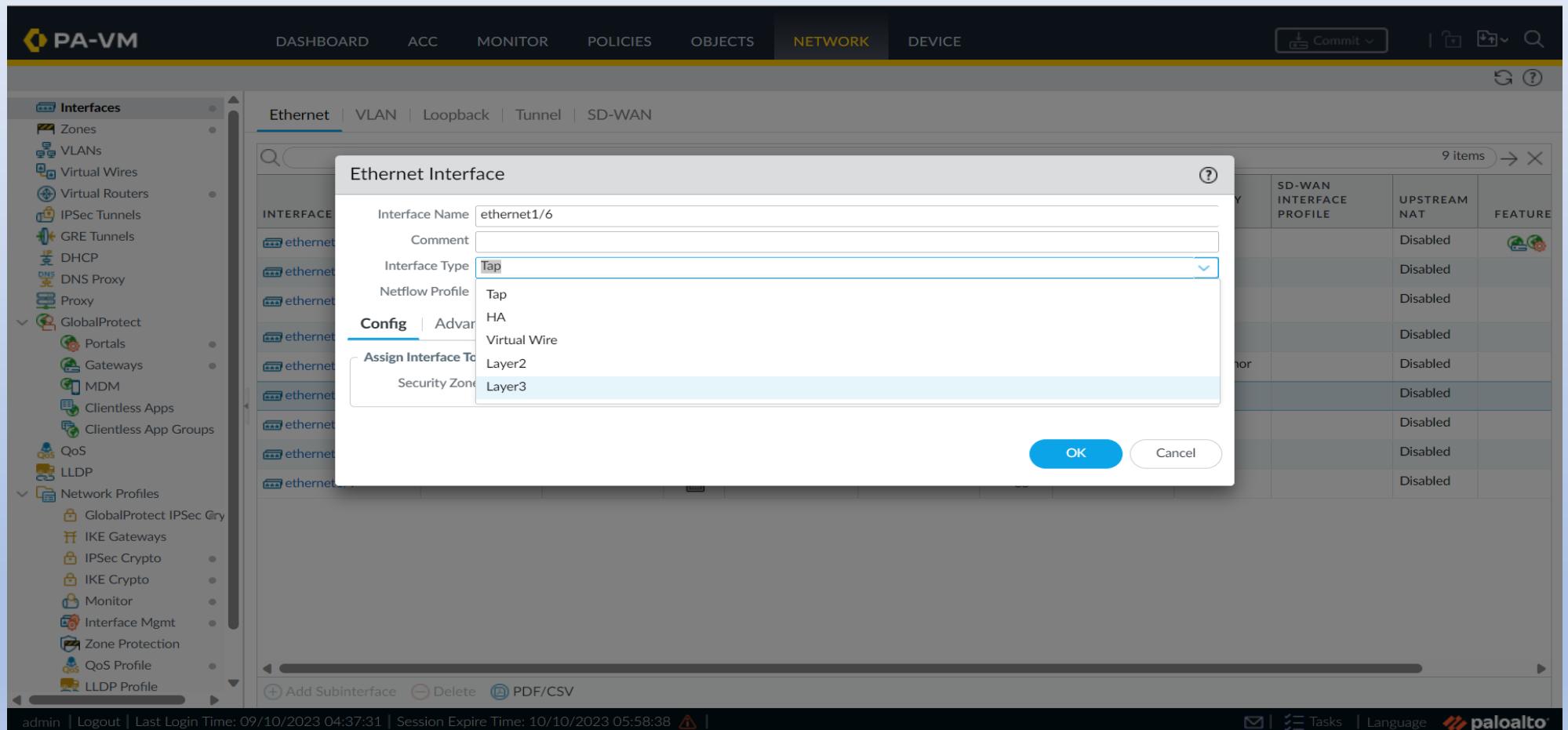
- An Interface is configured to one zone only
- A Security Zone can have multiple Interfaces

Interface	Zone	Address
E 1/10	Internet	161.23.4.254
E 1/11	DMZ	172.16.1.254
E 1/12	--	--
E 1/12.10	Users	192.168.10.254
E 1/12.20	Users	192.168.20.254
E 1/12.30	VoIP	192.168.30.254
Tunnel.4	Remote-LAN	10.5.1.254

Interface Types

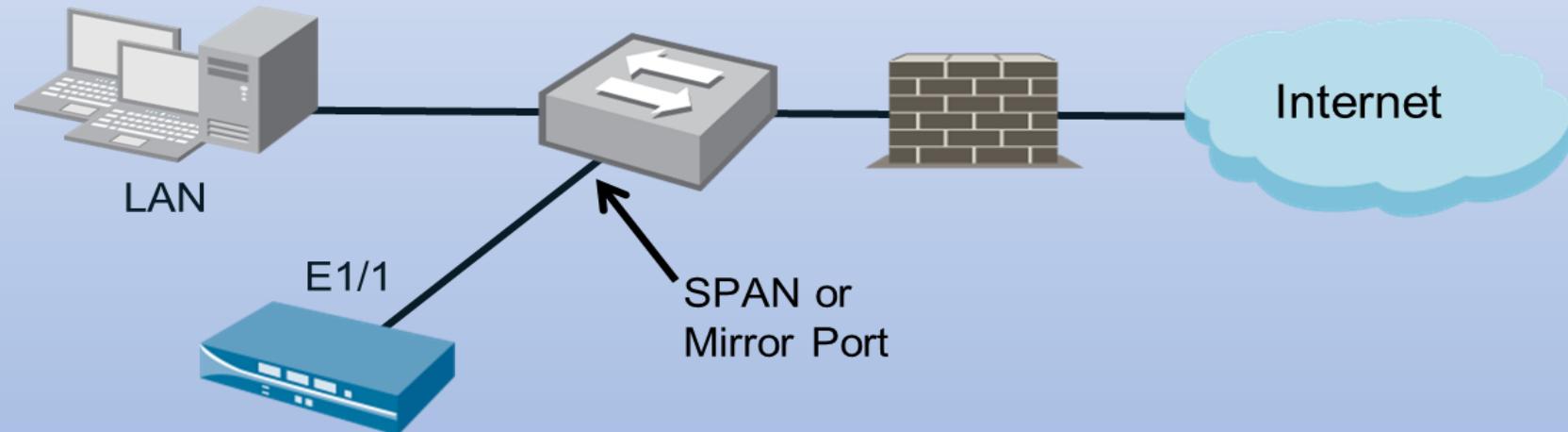
Interface Types

- Ethernet Tap, HA, Virtual Wire, Layer 2, Layer 3
- Aggregate
- VLAN
- Loopback
- Tunnel



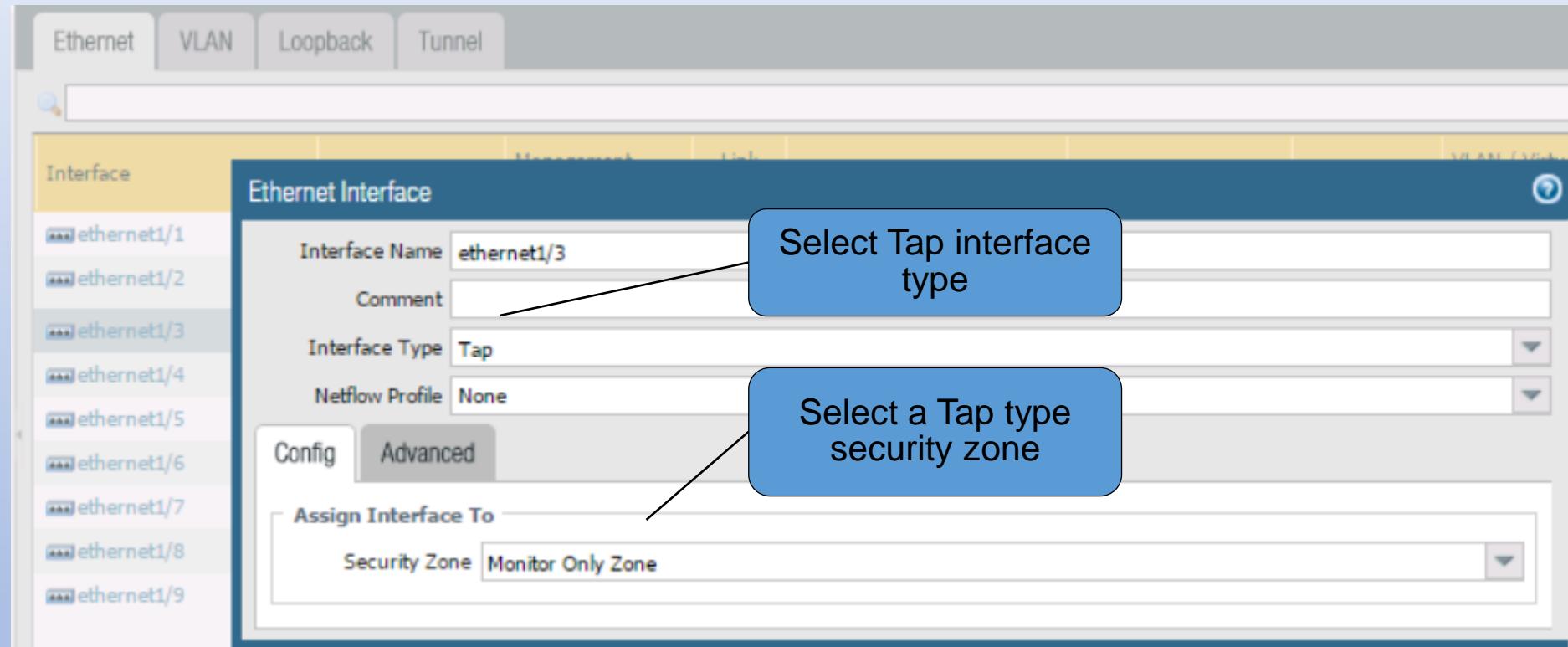
Ethernet Tap Interface

- Tap mode deployment allows the capability to passively monitor traffic flows across a network by way of a switch SPAN or mirror port
- Firewall cannot perform traffic shaping or blocking
- Must be assigned to a security zone for ACC and Reporting capabilities



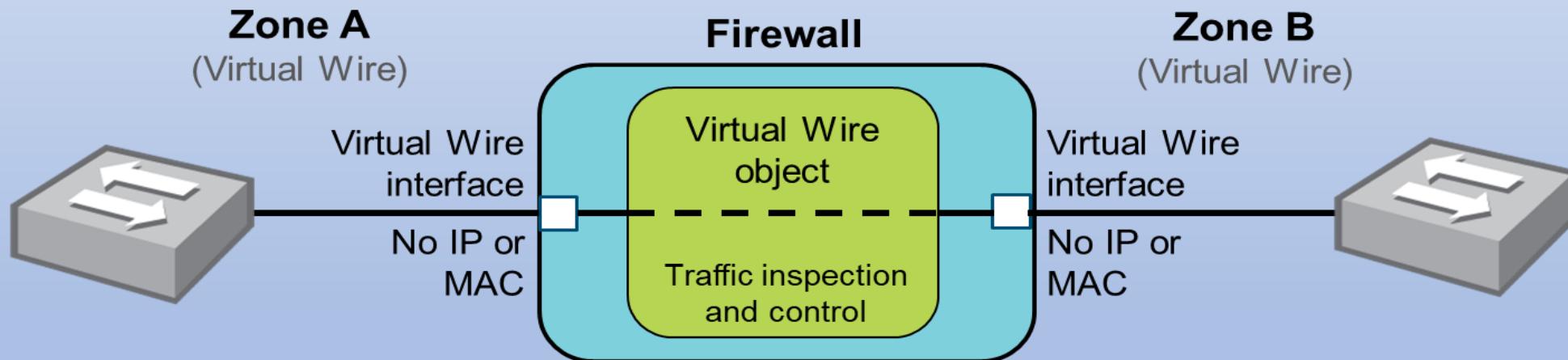
Configuring a Tap Interface

Network > Interfaces > Ethernet > <select_interface>



Virtual Wire Interface

- Binds two firewall interfaces together through Virtual Wire object
- Typically used when no switching or routing is needed
- No configuration changes for adjacent network devices



Configuring a Virtual Wire Object

Network > Virtual Wires > Add

- Virtual Wire object connects to Virtual Wire interfaces.
- A virtual wire can accept traffic based on 802.1Q VLAN tags:
 - 0 = untagged traffic

Virtual Wire

Name vwire-object-1

Interface1 ethernet1/4

Interface2 ethernet1/5

Tag Allowed [0 - 4094]
Enter either integers (e.g. 10) or ranges (100-200) separated by commas. Integer values can be between 0 and 4094

Multicast Firewalling

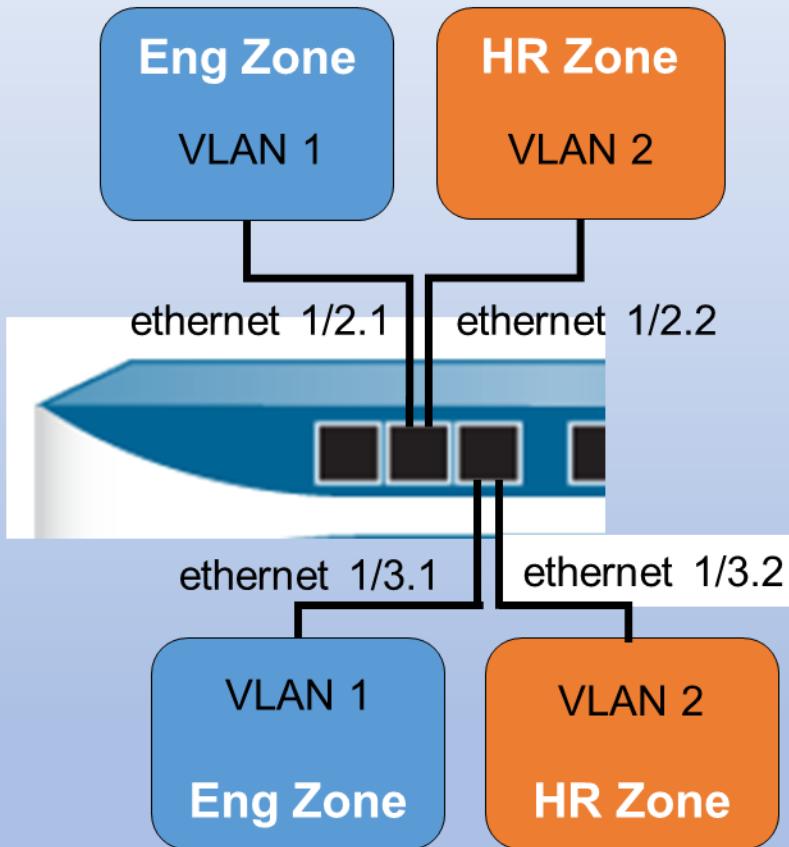
Link State Pass Through

Multicast traffic is forwarded

Link state is forwarded

Ethernet Layer 2 Interfaces

Layer 2 Subinterfaces



Assign subinterfaces to zones

VLAN traffic isolated by subinterfaces:

- Need route between VLANs

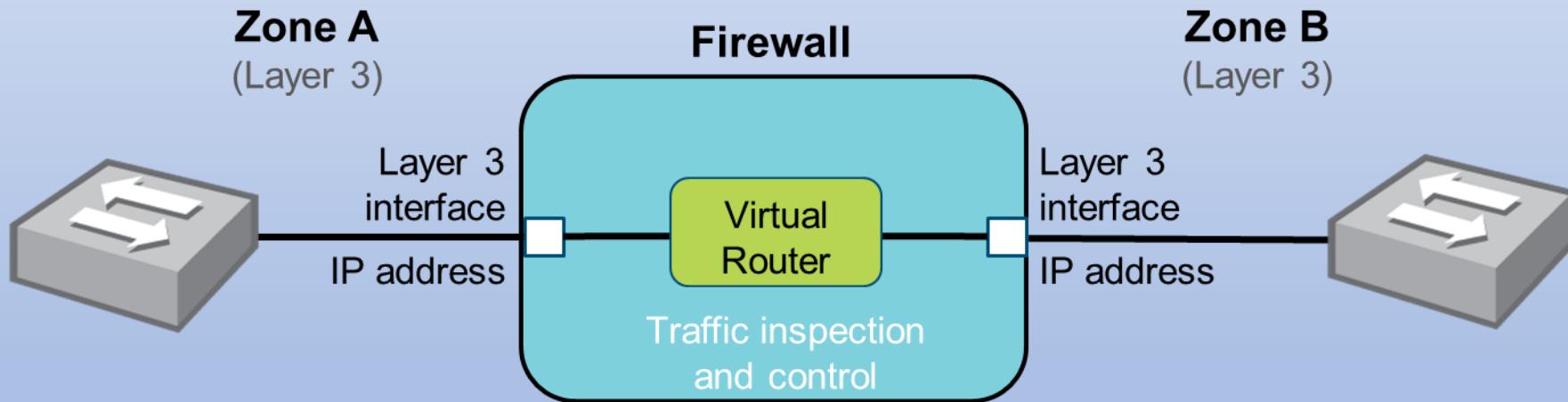
- Security policy blocks interzone traffic by default

Useful configuration for multi-tenant networks

Layer 3 Interfaces

Layer 3 Interfaces

- Enables routing between multiple interfaces:
 - Requires a virtual router
- Requires network configuration to accommodate new IP addresses



Configuring a Layer 3 Interface – Config

Network > Interfaces > Ethernet > <select_interface>

Ethernet Interface

Interface Name	ethernet1/1		
Comment			
Interface Type	Layer3		
Netflow Profile	None		
Config	IPv4	IPv6	Advanced
Assign Interface To			
Virtual Router	Student-VR		
Security Zone	Untrust-L3		

Select Layer3

Select a virtual router

Select a Layer 3 type security zone

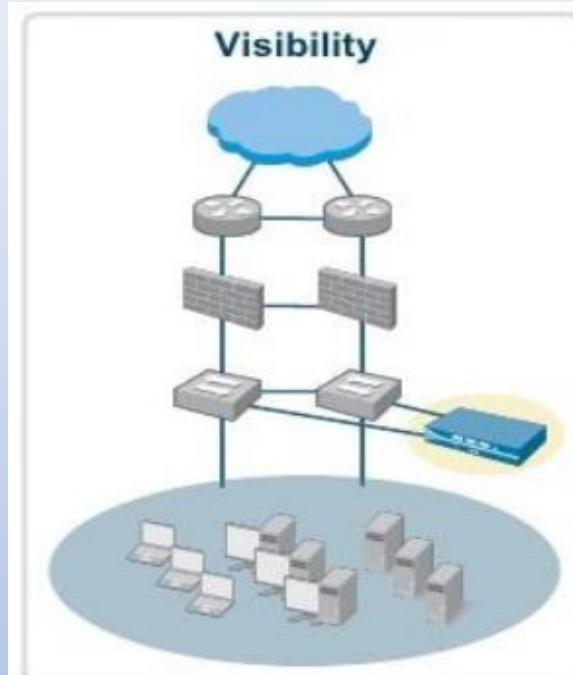
The screenshot shows the configuration interface for an Ethernet interface named 'ethernet1/1'. The 'Interface Type' is set to 'Layer3'. In the 'Assign Interface To' section, the 'Virtual Router' is set to 'Student-VR' and the 'Security Zone' is set to 'Untrust-L3'. Three callout boxes with arrows point to these fields: one to 'Select Layer3' points to the 'Interface Type' field, another to 'Select a virtual router' points to the 'Virtual Router' field, and a third to 'Select a Layer 3 type security zone' points to the 'Security Zone' field.

Configuring a Layer 3 Interface – IPv4

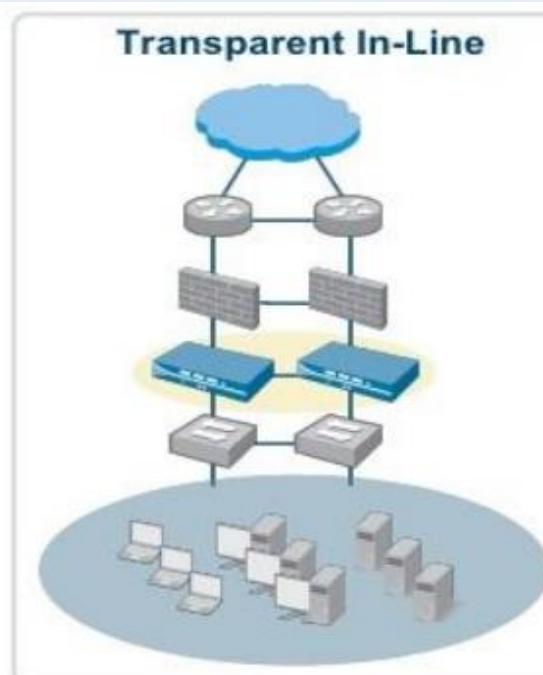
Network > Interfaces > Ethernet > <select_interface>

The screenshot shows the 'Ethernet Interface' configuration page. At the top, there are fields for 'Interface Name' (set to 'ethernet1/1'), 'Comment', 'Interface Type' (set to 'Layer3'), and 'Netflow Profile' (set to 'None'). Below these are tabs for 'Config', 'IPv4', 'IPv6', and 'Advanced'. The 'IPv4' tab is selected, showing a table with one row: 'IP' (checkbox checked) and '172.16.1.7/24'. At the bottom of the table is a toolbar with 'Add', 'Delete', 'Move Up', and 'Move Down' buttons, and a note 'IP address/netmask, Ex. 192.168.2.254/24'. A large callout box points to the 'Type' radio buttons ('Static', 'PPPoE', 'DHCP Client') in the main configuration area, with the text 'Select to specify a static or DHCP assigned IP address'. Another callout box points to the 'IP' column in the table, with the text 'Enter the static IP address(es) with CIDR notation'.

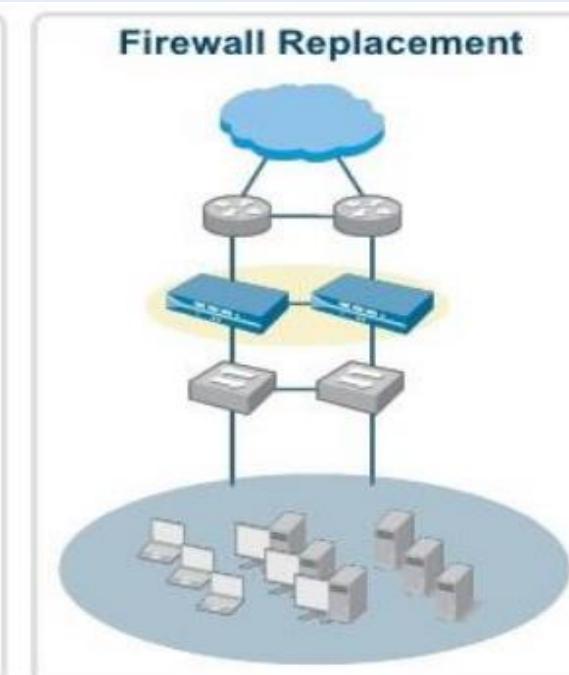
Deployment Options For Ethernet Interfaces



- Application, user and content visibility without inline deployment



- IPS with app visibility & control
- Consolidation of IPS & URL filtering

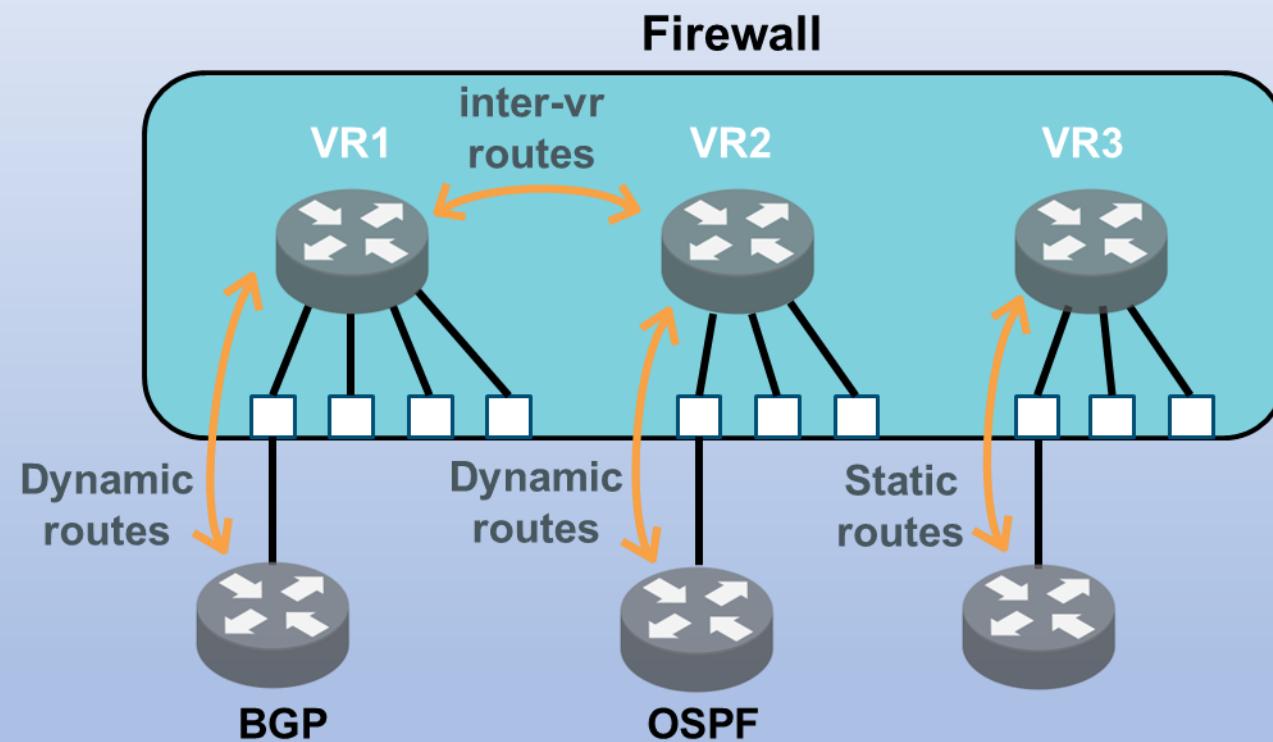


- Firewall replacement with app visibility & control
- Firewall + IPS
- Firewall + IPS + URL filtering

Virtual Routers

Virtual Routers

- Support one or more static routes
- Support dynamic routing:
 - RIPv2
 - OSPFv2
 - OSPFv3
 - BGPv4
- Support multicast routing
 - PIM-SM
 - PIM-SSM



Virtual Router General Settings

Network > Virtual Routers

Virtual Router - Student-VR

Router Settings Name: Student-VR

General ECMP

Interfaces ▾

- ethernet1/1.211
- ethernet1/2
- tunnel.1
- vlan.1
- ethernet1/1
- ethernet1/1.211
- ethernet1/2
- loopback
- tunnel
- tunnel.1
- vlan
- vlan.1

Add Delete

Administrative Distances

Static	10
Static IPv6	10
OSPF Int	30
OSPF Ext	110
OSPFv3 Int	30
OSPFv3 Ext	110
IBGP	200
EBGP	20
RIP	120

Interfaces that the virtual router can use to forward traffic

	Value
Static	10
Static IPv6	10
OSPF Int	30
OSPF Ext	110
OSPFv3 Int	30
OSPFv3 Ext	110
IBGP	200
EBGP	20
RIP	120

Adding a Static Default Route

Network > Virtual Routers > Static Routes > Add

Virtual Router - Static Route - IPv4

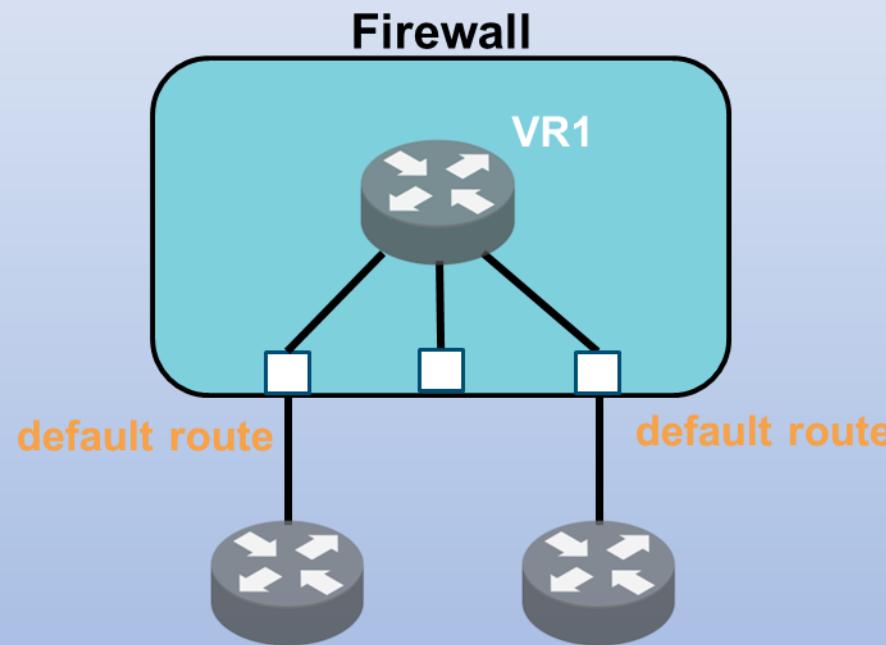
Name	default-route
Destination	0.0.0.0/0
Interface	ethernet1/1
Next Hop	IP Address
	203.0.113.1
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

Path Monitoring

IP Address
Next VR
Discard
None

Unicast
Multicast
Both
No Install

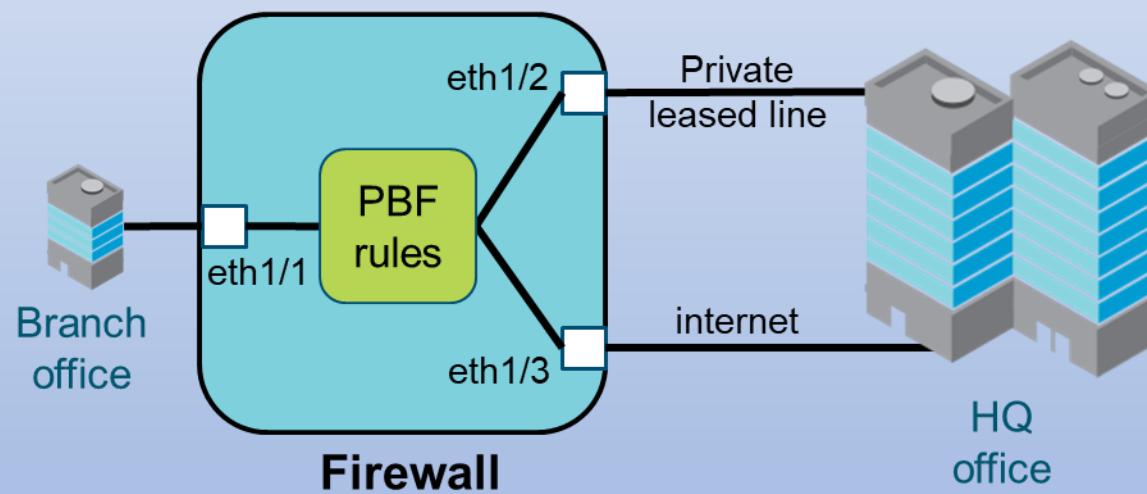
Multiple Static Default Routes



- Can configure multiple default routes
- Route with lowest metric is used
- Path monitoring determines if routes are usable
- Firewall switches default route during path failure

Policy-Based Forwarding

- Specifies different egress interface from that specified in route table
- Possible use for performance or security reasons



Specify egress interface for:

- Bandwidth sensitive applications
- Unencrypted applications

Specify egress interface for:

- Non-bandwidth sensitive applications
- Encrypted applications

PBF Rules

- PBF rules use match criteria to match traffic.
- PBF path monitoring enables the firewall to verify network path connectivity.

	Name	Tags	Source			Destination		Application	Service	Action	Forwarding			Profile
			Zone/Interface	Address	User	Address	Address				Egress I/F	Next Hop	Enforce Symmetric Return	
1	Mail OnlyTraffic	none	Trust-L3	any	any	Mail Servers	any	SMTP	forward		ethernet1/6	201.34.17.6	false	default

DHCP Server

- When an interface is configured as a DHCP server, it will assign addresses to DHCP clients.
- If an interface on the firewall is a client of an external DHCP server, the DHCP Server can forward information to its own clients

DHCP Server (Left Screenshot - Lease Tab)

Interface: ethernet1/2
Mode: auto

Lease | Options

Ping IP when allocating new IP:
Lease: Unlimited Timeout

IP POOLS

192.168.1.10-192.168.1.100

RESERVED ADDRESS

192.168.1.20 xx:xx:xx:xx:xx:xx (O)

Add **Delete**

DHCP Server (Right Screenshot - Options Tab)

Interface: ethernet1/2
Mode: auto

Lease | Options

Inheritance Source: None

Gateway: 192.168.1.254
Subnet Mask: 255.255.255.0
Primary DNS: 8.8.8.8
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

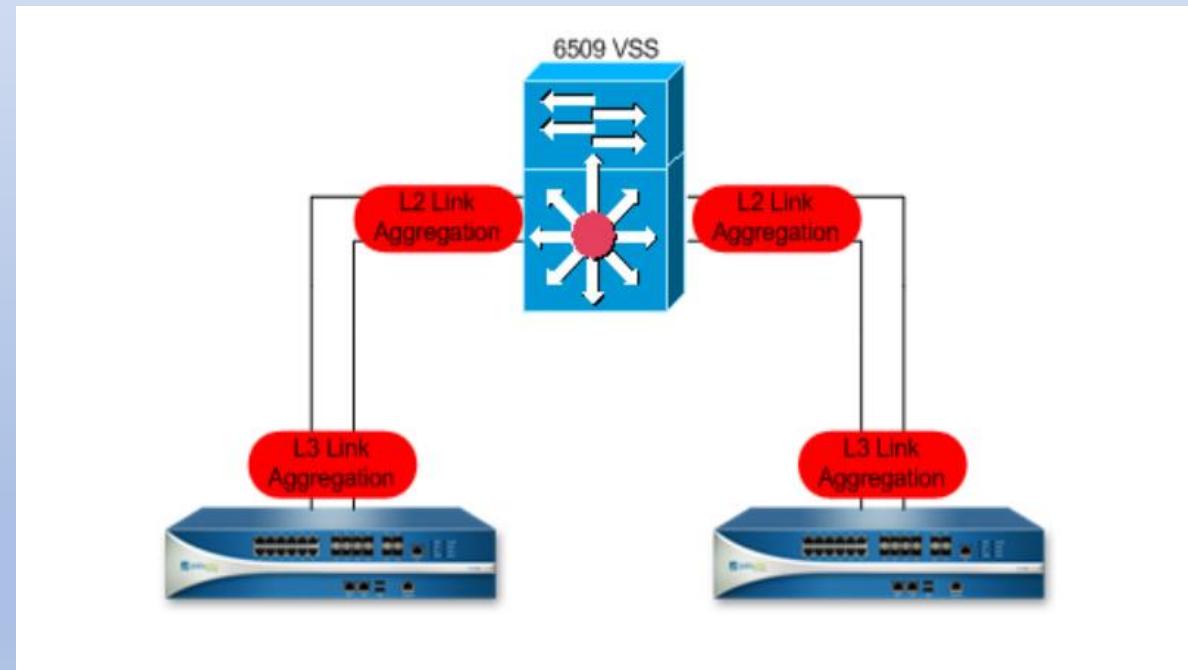
Custom DHCP options

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

Add **Delete** **↑ Move Up** **↓ Move Down**

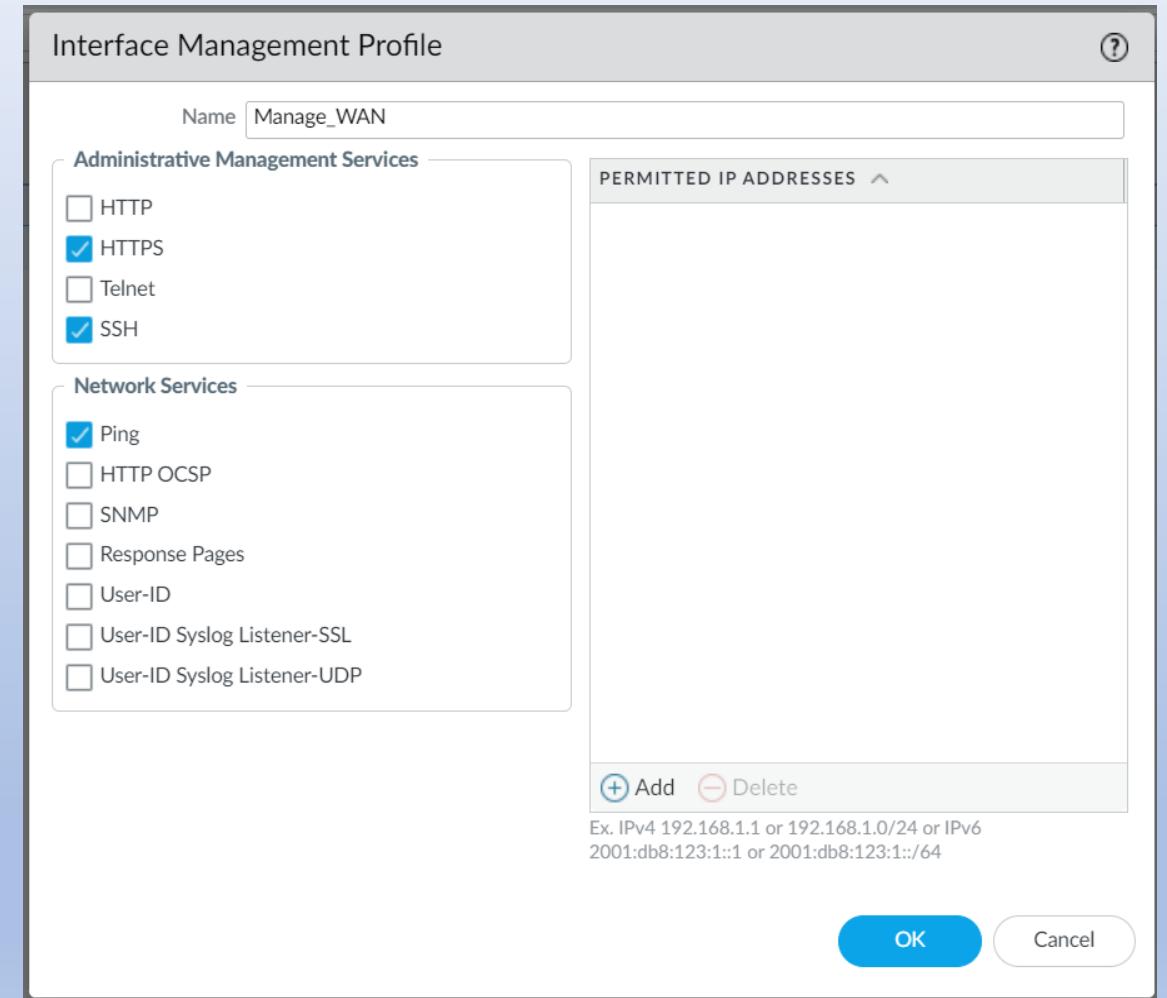
Aggregate Interfaces

- An aggregate interface group combines up to 8 Ethernet interfaces using link aggregation
- Increased throughput and link redundancy
- The aggregate interface is a logical interface that can be configured as if it were a regular interface
- LACP is supported



Interface Management Profile

- Defines which management functions are allowed on a traffic interface
- Management Profiles are applied to Layer 3 Interfaces

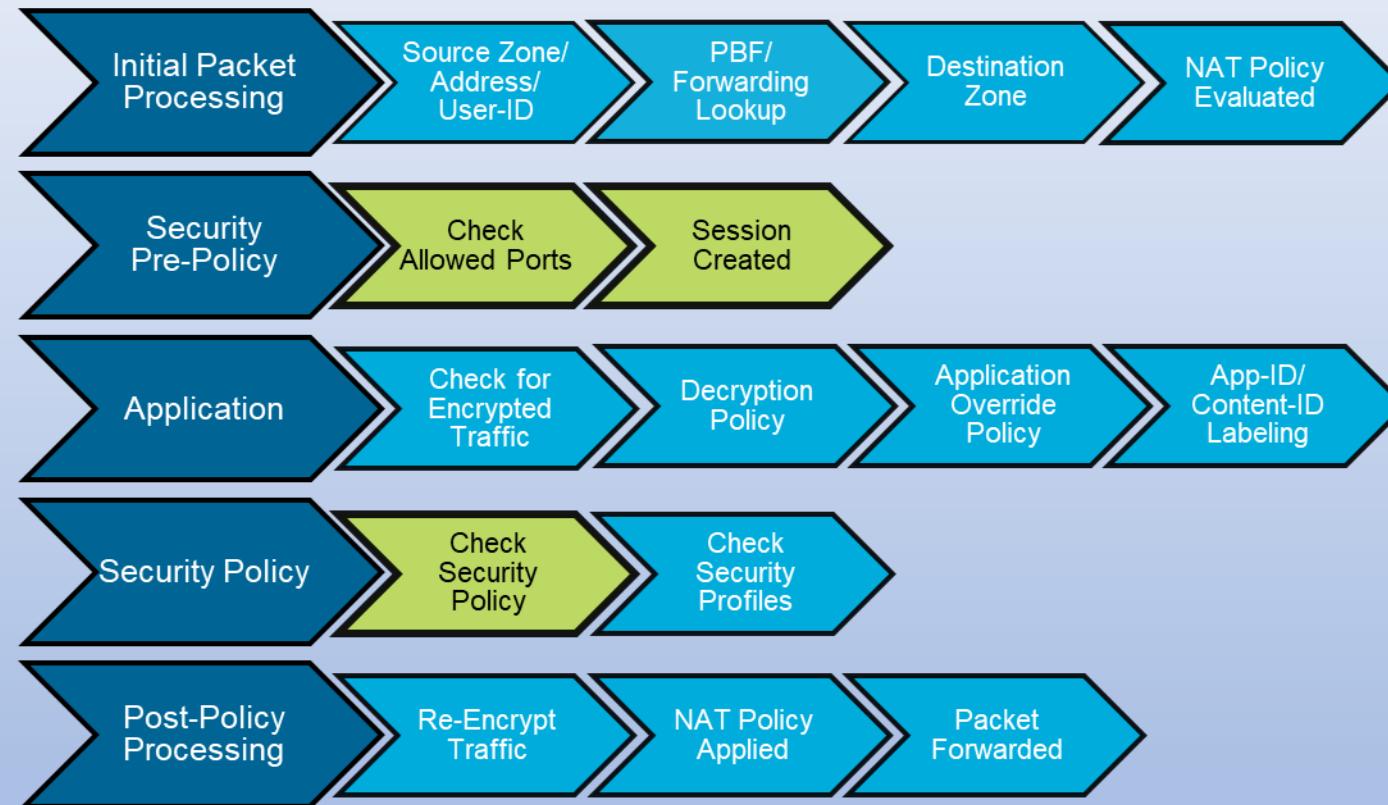


4.

Security Policy and NAT Policies

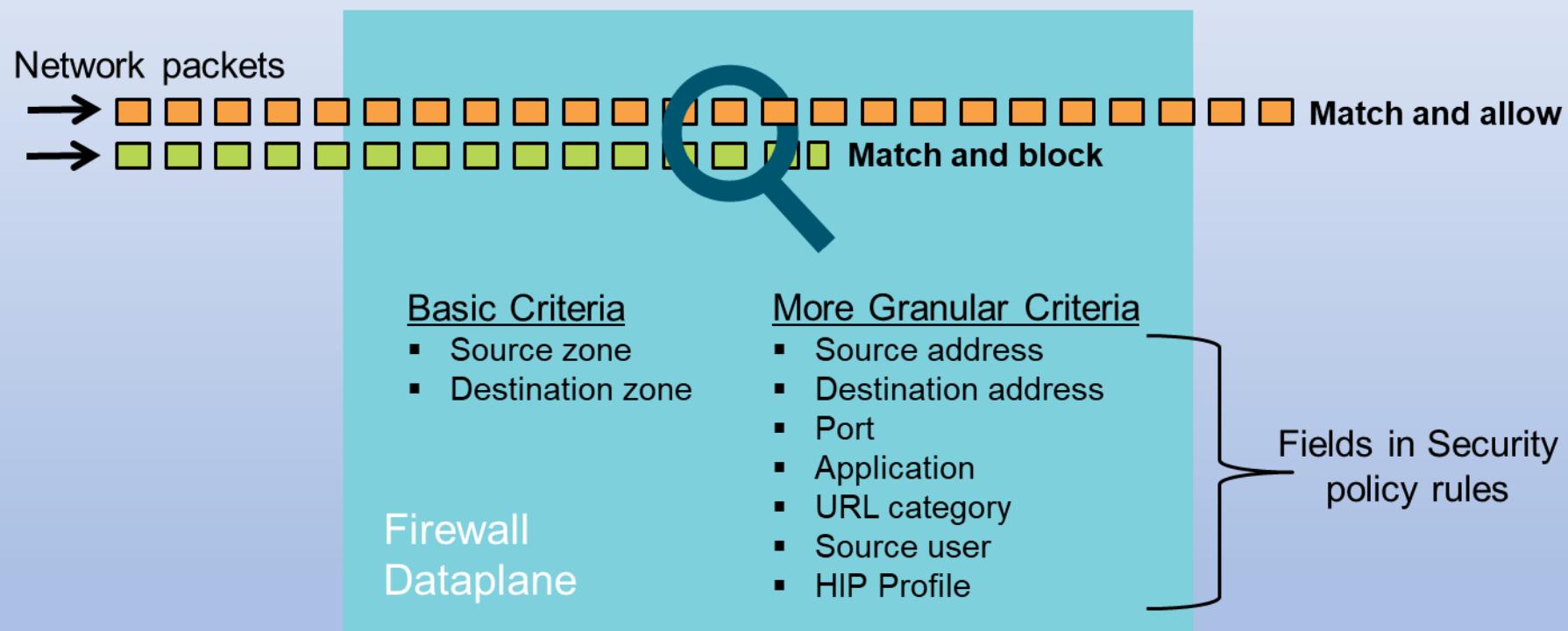
Security Policy Configuration

Flow Logic of the Next-Generation Firewall



Controlling Network Traffic

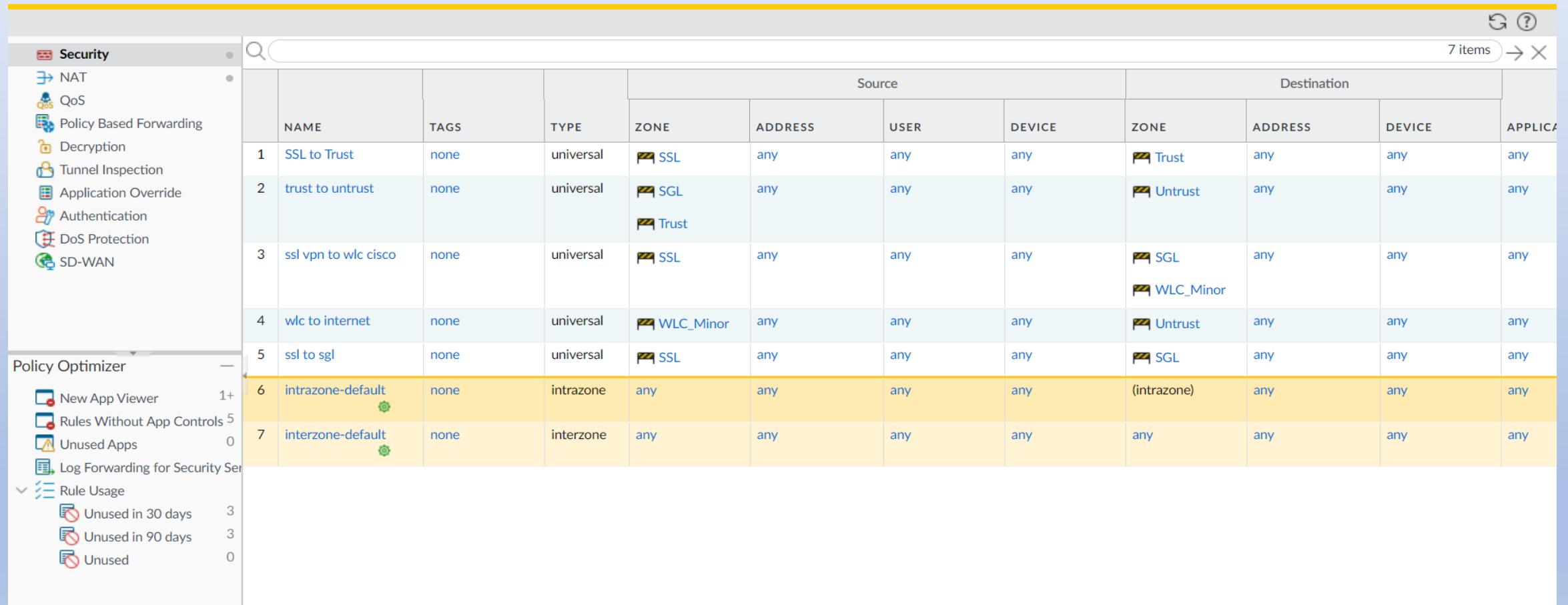
Multiple match criteria available to control network traffic



Security Policy

Policy list is evaluated from the top down

- The first rule that matches the traffic is used
- No further rules are evaluated after the match



The screenshot shows the Palo Alto Firewall's Security Policy configuration. The left sidebar includes links for NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN. Below that is the Policy Optimizer section with New App Viewer (1+), Rules Without App Controls (5), Unused Apps (0), and Log Forwarding for Security Services. The Rule Usage section shows 3 rules unused in 30 days, 3 rules unused in 90 days, and 0 unused rules.

The main table displays 7 security policies:

ID	NAME	TAGS	TYPE	Source				Destination			APPLICATION
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	
1	SSL to Trust	none	universal	SSL	any	any	any	Trust	any	any	any
2	trust to untrust	none	universal	SGL Trust	any	any	any	Untrust	any	any	any
3	ssl vpn to wlc cisco	none	universal	SSL	any	any	any	SGL WLC_Minor	any	any	any
4	wlc to internet	none	universal	WLC_Minor	any	any	any	Untrust	any	any	any
5	ssl to sgl	none	universal	SSL	any	any	any	SGL	any	any	any
6	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any
7	interzone-default	none	interzone	any	any	any	any	any	any	any	any

Security Zone Rules – Three Types

Intrazone – Traffic within the same zone

- Allowed by default

Interzone – Traffic traversing from one zone to another

- Denied by default

Universal (default) – Traffic applying to both zones (Intrazone and Interzone)

- Behaves as normal – checks the rule and applies the action

Security Policy Rule

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

Name:

Rule Type:

Description:
intrazone
interzone

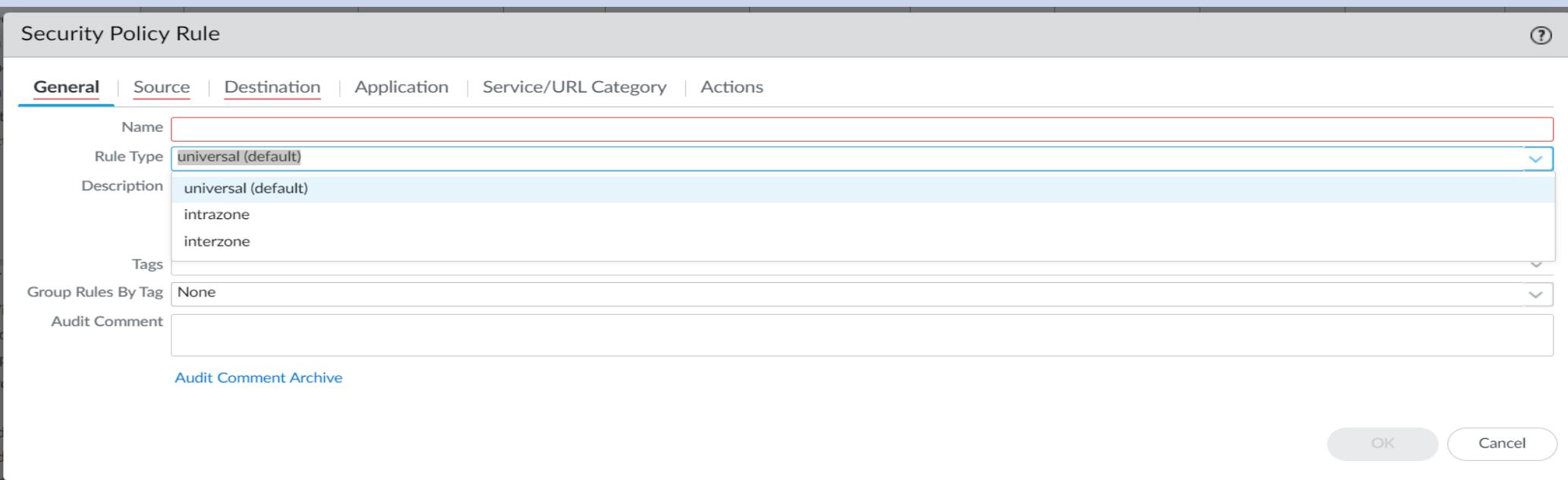
Tags:

Group Rules By Tag:

Audit Comment:

Audit Comment Archive:

OK Cancel



Security Zones Within a Policy

Security Policies are configured by Zone – Not by Interface!

	NAME	TAGS	TYPE	Source				Destination			APPLICA
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	
1	SSL to Trust	none	universal	SSL	any	any	any	Trust	any	any	any
2	trust to untrust	none	universal	SGL Trust	any	any	any	Untrust	any	any	any
3	ssl vpn to wlc cisco	none	universal	SSL	any	any	any	SGL WLC_Minor	any	any	any
4	wlc to internet	none	universal	WLC_Minor	any	any	any	Untrust	any	any	any
5	ssl to sgl	none	universal	SSL	any	any	any	SGL	any	any	any
6	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any
7	interzone-default	none	interzone	any	any	any	any	any	any	any	any

Address Objects

Created to reference frequently used IP addresses or ranges

Available types:

- IP Netmask
- IP Range
- FQDN

The screenshot shows the Palo Alto Networks UI interface. The top navigation bar includes tabs for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS (which is highlighted with a red box), NETWORK, and DEVICE. A 'Commit' button is located in the top right corner. On the left, a sidebar lists various object types: Addresses (selected and highlighted with a red box), Address Groups, Regions, Dynamic User Groups, Applications, Application Groups, Application Filters, Services, Service Groups, Tags, Devices, GlobalProtect (with HIP Objects and HIP Profiles), External Dynamic Lists, Custom Objects (with Data Patterns, Spyware, Vulnerability, and URL Category), and Security Profiles (with Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, and WildFire Analysis). Below the sidebar is a search bar and a table with columns: NAME, LOCATION, TYPE, ADDRESS, and TAGS. At the bottom of the sidebar is a '+ Add' button. A modal window titled 'Address' is open in the center. It contains fields for Name (IP_192.168.1.100_32, highlighted with a red box), Description, Type (IP Netmask, highlighted with a red box), and Address (192.168.1.100/32, highlighted with a red box). A note below the address field says: '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)'. The modal has 'OK' and 'Cancel' buttons at the bottom.

Apply to Policy

Apply group in policy same as any other address group and commit

- Can drill down and click more to see registered IPs

The screenshot shows the Palo Alto Networks Firewall interface. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies (selected), Objects, Network, and Device. On the right, there are Commit and Save buttons. The main area displays a table of security policies. One row, labeled '6 Dyn-Address-Group1', has its 'Address' column value 'dyn-group1' highlighted with a red box. A context menu is open over this cell, with the 'Inspect' option selected. A modal window titled 'Address Group' provides details about the selected group:

Name	Type	Match
dyn-group1	Dynamic	(test2 and 'test1') or 'tag1'

The bottom left corner shows a list of address groups with their names and addresses:

Name	Address
test1	10.30.0.0/23
support.palo...	support.paloaltonet...
tac.paloalto...	tac.paloaltonetwor...
Trust_Lan	192.168.210.0/24

URL Category

- For HTTP/HTTPS traffic only
- Can include custom URL categories
- Requires a license for non-custom URL categories
- URL lookups are cached for faster retrieval

Security Policy Rule

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

application-default ▾

SERVICE ▾

Any

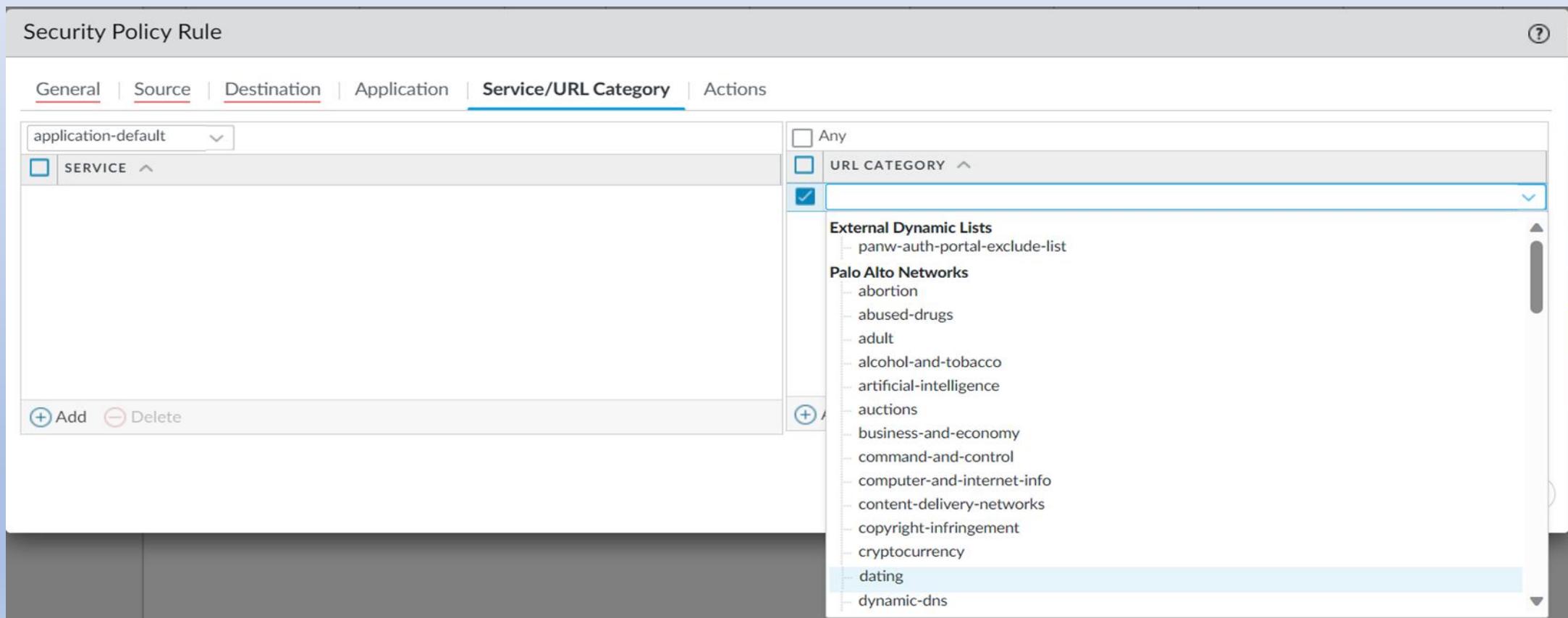
URL CATEGORY ▾

External Dynamic Lists
panw-auth-portal-exclude-list

Palo Alto Networks

- abortion
- abused-drugs
- adult
- alcohol-and-tobacco
- artificial-intelligence
- auctions
- business-and-economy
- command-and-control
- computer-and-internet-info
- content-delivery-networks
- copyright-infringement
- cryptocurrency
- dating
- dynamic-dns

+ Add - Delete



Security Zone Rule – Enable Logging

Two pre-defined default rules and both are “Read Only”.

- Intrazone-Default
- Interzone-Default

“Override” to configure additional settings

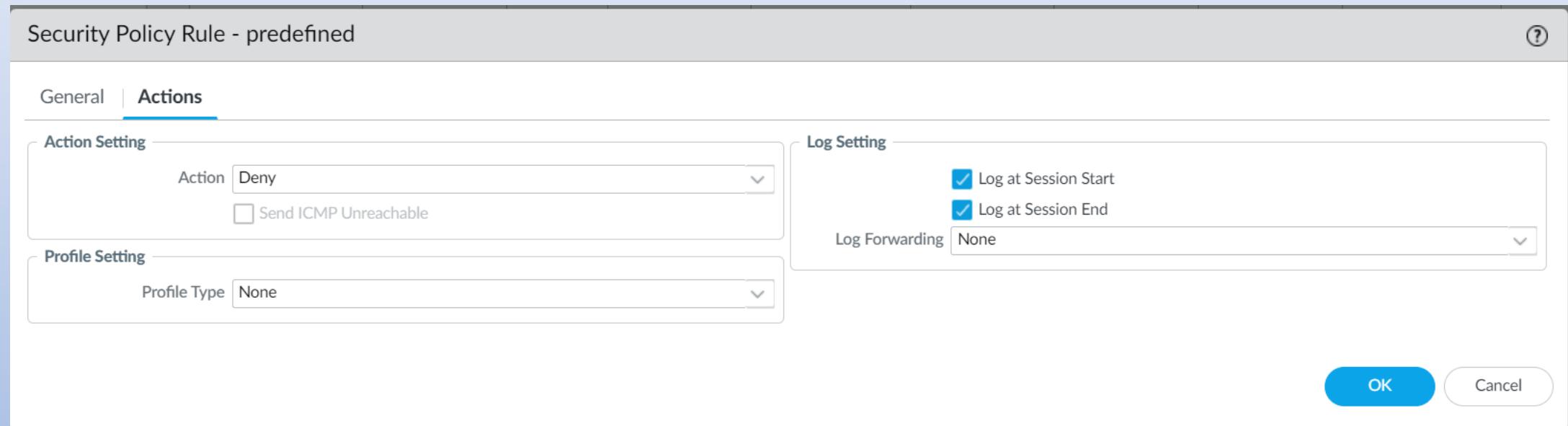
	NAME	TAGS	TYPE	Source				Destination			APPLICA
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	
1	SSL to Trust	none	universal	SSL	any	any	any	Trust	any	any	any
2	trust to untrust	none	universal	SGL Trust	any	any	any	Untrust	any	any	any
3	ssl vpn to wlc cisco	none	universal	SSL	any	any	any	SGL WLC_Minor	any	any	any
4	wlc to internet	none	universal	WLC_Minor	any	any	any	Untrust	any	any	any
5	ssl to sgl	none	universal	SSL	any	any	any	SGL	any	any	any
6	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any
7	interzone-default	none	interzone	any	any	any	any	any	any	any	any

Security Zone Rule – Enable Logging

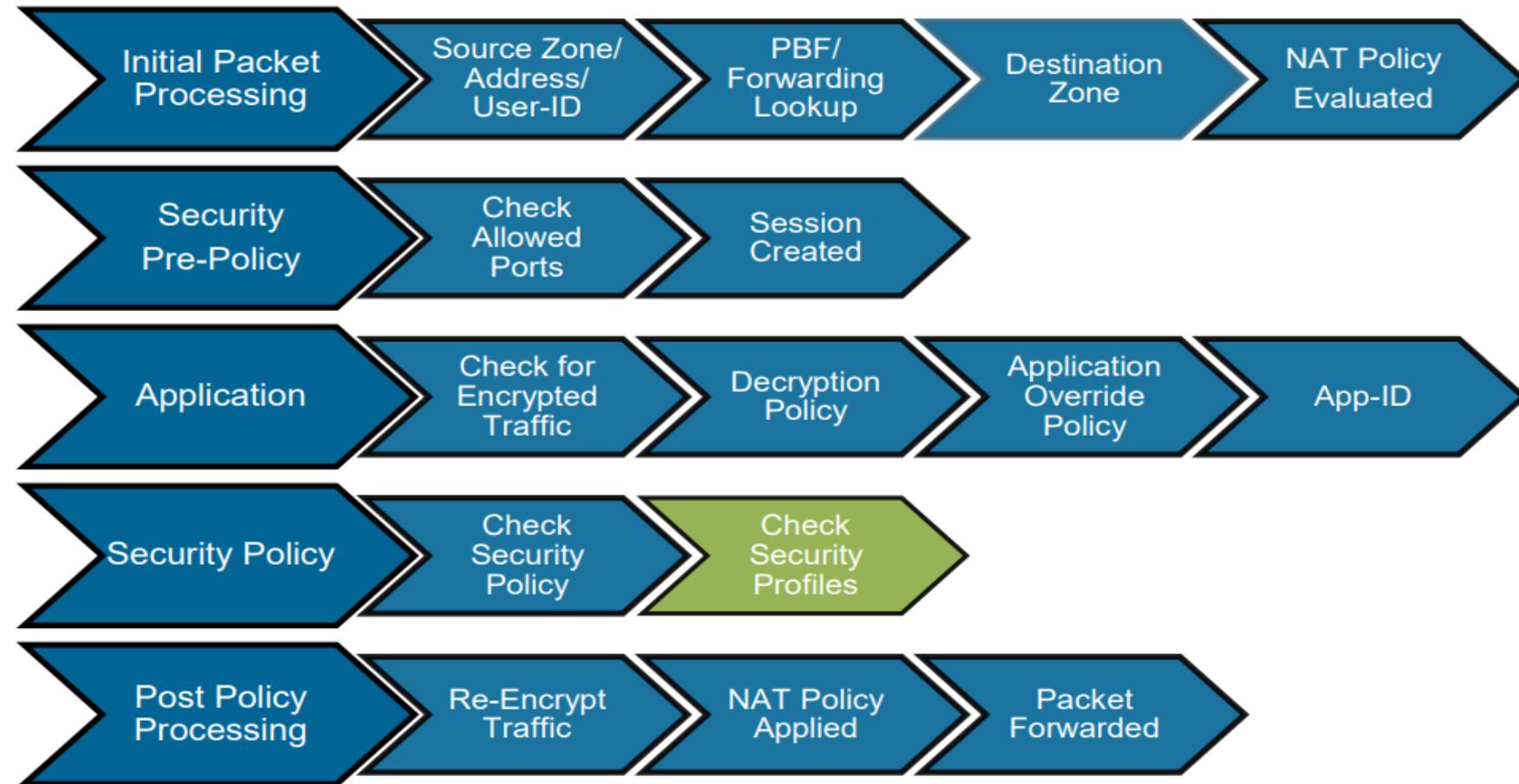
Two pre-defined default rules and both are “Read Only”.

- Intrazone-Default
- Interzone-Default

“Override” to configure additional settings



Flow Logic of the Next-Generation Firewall



Security Profiles

Policies are processed in two steps: Check to see if traffic matches the Security Policy

- Action is set to Deny, the packet is dropped
- Action is set to Allow, go to step 2

Name	Type	Zone	Source		Zone	Destination		Application	Service	Action	Profile
RestrictYouTube	universal	Trust-L3	any	any	Untrust-L3	any		youtube	application-default	✓	
Disable-FB	universal	Trust-L3	any	any	Untrust-L3	any		facebook-base	application-default	✗	none
General Access	universal	Trust-L3	any	any	Untrust-L3	any	any	any	any	✓	

Step 1:
Security Policy

Step 2:
Security Profile

Security Profile Types

Policy>Security Profile

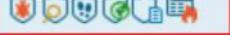
Security

NAT
QoS
Policy Based Forwarding
Decryption
Tunnel Inspection
Application Override
Authentication
DoS Protection
SD-WAN

inor

Policy Optimizer

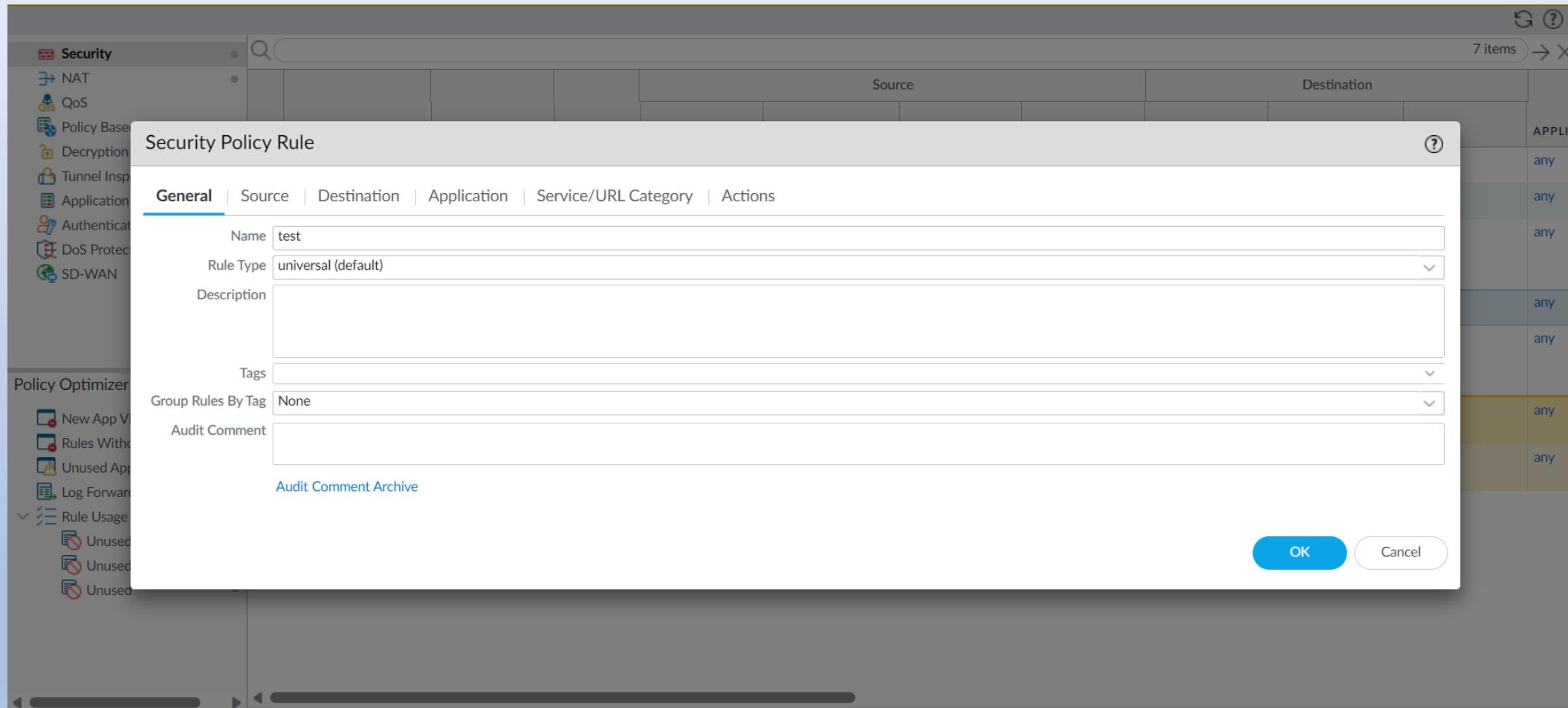
- New App Viewer 1+
- Rules Without App Controls 5
- Unused Apps 0

Destination								
	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	HIT COUNT
	any	any	any	application-d...	Allow	none		583768
	any	any	any	any	Allow	none		629672
	any	any	any	application-d...	Allow	none		10024
	any	any	any	application-d...	Allow	none		13843
	any	any	any	application-d...	Allow			13508
	any	any	any	any	Allow	none	none	9146643
	any	any	any	any	Deny	none	none	33379



Security Policy Administration

Creating Security Policy Rules – General Tab



Re-Ordering Rules

Moving the Rules to re-order them automatically re-numbers them

The screenshot illustrates the process of re-ordering firewall rules. It shows two identical policy lists side-by-side, separated by a large yellow curved arrow pointing from left to right.

Top Policy List (Initial Order):

	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service
1	wtamTrust-VPN		trust	any	any	any	p2 untrust	any	any	any
2	tag1-policy	test1	trust	Trust_Lan	any	any	p2 untrust	support.paloalt...	any	application-d...
3	tag1-tag2-policy	test1	trust	Trust_Lan	any	any	p2 untrust	tac.paloaltonet...	any	application-d...
4	TEST									
5	block-incoming									
6	allow-any									

Bottom Policy List (Reordered):

	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service
1	wtamTrust-VPN		trust	any	any	any	p2 untrust	any	any	any
2	tag1-policy	test1	trust	Trust_Lan	any	any	p2 untrust	support.paloalt...	any	application-d...
3	TEST		trust	any	any	any	p2 untrust	any	any	any
4	tag1-tag2-policy	test1	trust	Trust_Lan	any	any	p2 untrust	tac.paloaltonet...	any	application-d...
5	block-incoming	test1	p2 untrust	any	any	any	p2 trust	any	any	any
6	allow-any		any	any	any	any	any	any	any	any

Moving Rules Another Way

Moving the Rules to re-order them automatically re-numbers them

The screenshot shows the Palo Alto Firewall's configuration interface. On the left, there's a sidebar with various policy categories like Security, NAT, QoS, etc. Below that is a 'Policy Optimizer' section with metrics for New App Viewer, Rules Without App Controls, Unused Apps, and Log Forwarding for Security Services. At the bottom, there's a 'Rule Usage' section with filters for Unused in 30 days, Unused in 90 days, and Unused.

The main area displays a table of 7 security rules. Rule 4 ('ssl to sgl') is currently selected. A modal dialog titled 'Move - ssl to sgl' is open over the table, containing a dropdown menu labeled 'Select a Rule' with the following options:

- 1 wlc to internet
- 2 SSL to Trust
- 3 trust to untrust
- 5 ssl vpn to wlc cisco

The rule '3 trust to untrust' is highlighted with a blue background in the dropdown menu. The table rows are numbered 1 through 7, corresponding to the rules listed in the dropdown.

NAME	TAGS	TYPE	Source				Destination				APPLIC
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
1 wlc to internet	none	universal	WLC_Minor	any	any	any	Untrust	any	any	any	
2 SSL to Trust	none	universal	SSL	any	any	any	Trust	any	any	any	
3 trust to untrust	none	universal	SGL	any	any	any	Untrust	any	any	any	
4 ssl to sgl	none						SGL	any	any	any	
5 ssl vpn to wlc cisco	none						SGL	any	any	any	
6 intrazone-default	none						(intrazone)	any	any	any	
7 interzone-default	none	interzone	any	any	any	any	any	any	any	any	

Displaying Policy Columns

Columns can be selected, deselected, and resized Adjust columns to minimize screen sprawls

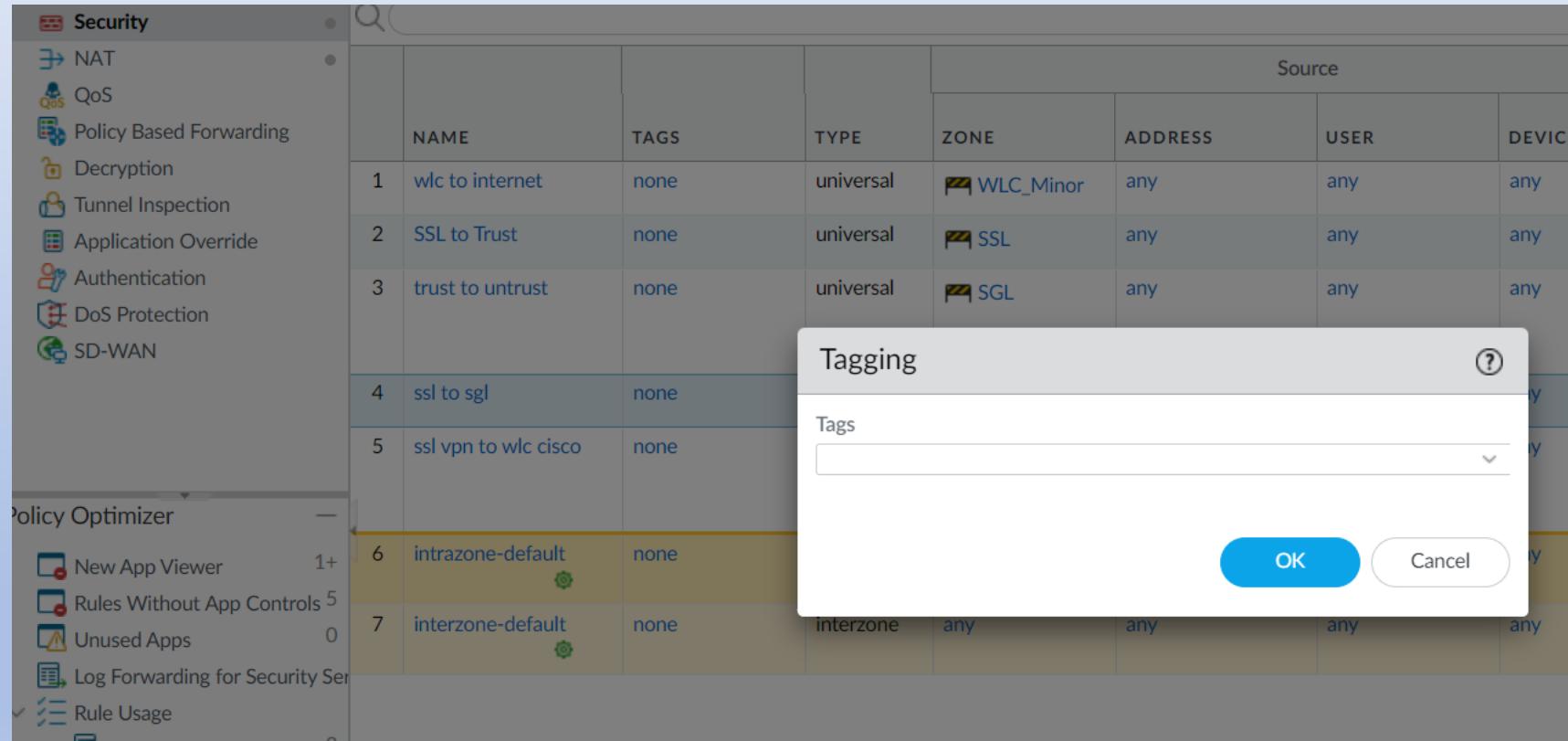
The screenshot shows the Palo Alto Firewall's policy list interface. On the left, there is a navigation sidebar with various security-related options like NAT, QoS, Policy Based Forwarding, etc. Below that is a 'Policy Optimizer' section with links for New App Viewer, Rules Without App Controls, Unused Apps, Log Forwarding for Security Services, and Rule Usage (Unused in 30 days, Unused in 90 days, Unused). The main area displays a table of policies:

	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	Source	Destination
1	wlc to internet	none	universal	WLC_Minor	any			
2	SSL to Trust	none	universal	SSL	any			
3	trust to untrust	none	universal	SGL	any	any		
4	ssl to sgl	none	universal	SSL	any	any		
5	ssl vpn to wlc cisco	none	universal	SSL	any	any		
6	intrazone-default	none	intrazone	any	any	any		
7	interzone-default	none	interzone	any	any	any		

A context menu is open over the 6th row (intrazone-default), showing options to 'Columns' and 'Adjust Columns'. To the right of the table is a large list of available columns, many of which are checked (e.g., Name, Tags, Type, Source Zone, etc.). At the bottom of the interface, there are buttons for Add, Delete, Clone, Override, Revert, Enable, Disable, Move, PDF/CSV, and Hit Counter. The URL is https://49.0.116.142:4443/?# and the session expire time is 10/10/2023 05:58:38.

Security Policy Admin Tags

- You can now tag objects and add color to the tag in order to visually distinguish tagged objects.
- Tags can be added to the following objects: Address Objects, Address Groups, Zones, Service Groups, and Policy Rules



Creating Color Coded Tags

Apply to:

- Address Groups
- Address Objects
- Zones
- Services
- Service Groups

Tag

Name	Corp
Color	Red
Comments	

OK Cancel

Address

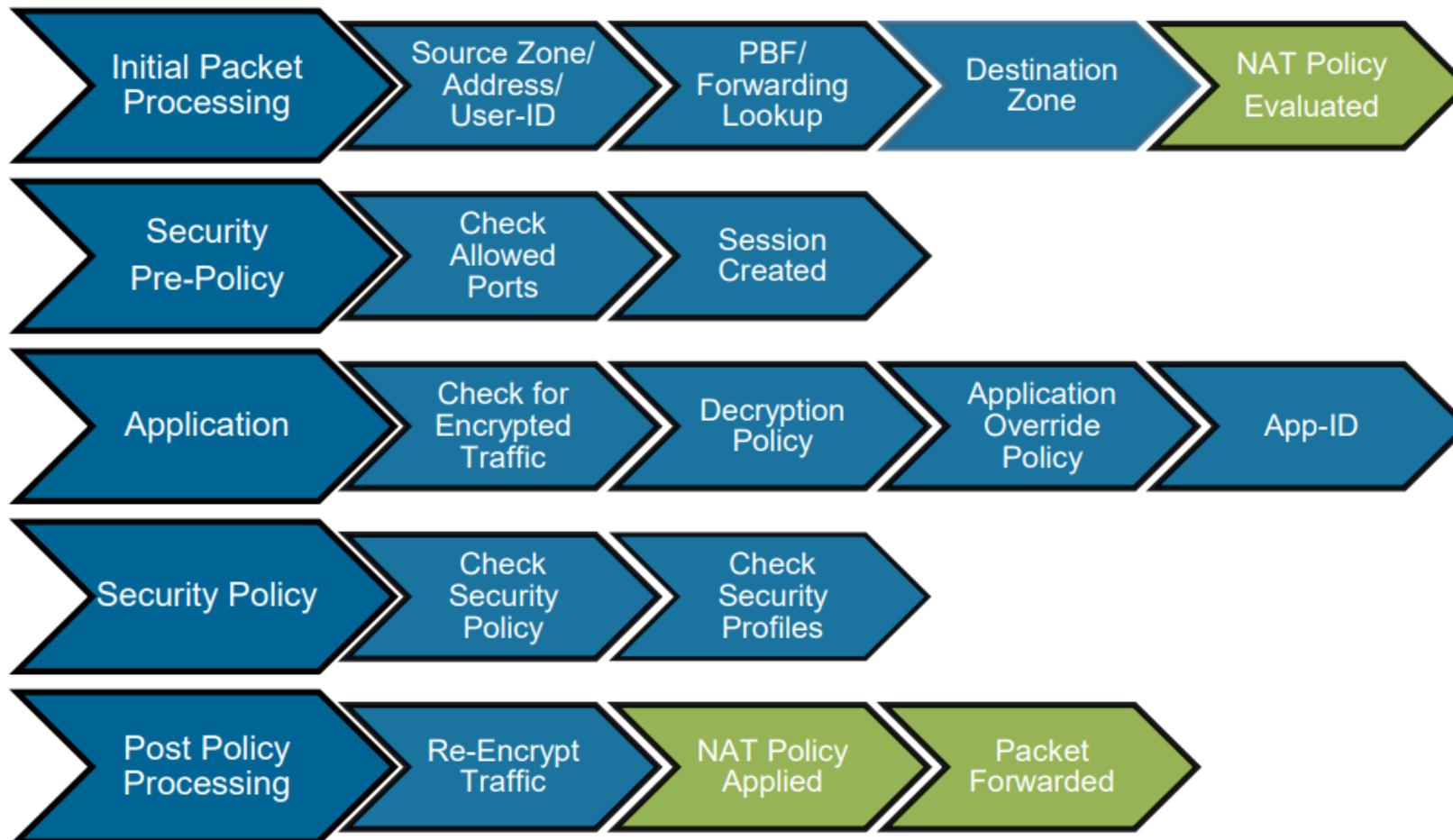
Name	DMZ_LAN		
Description			
Type	IP Netmask	10.10.0.1/32	Resolve
Tags	Corp		

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)

OK Cancel

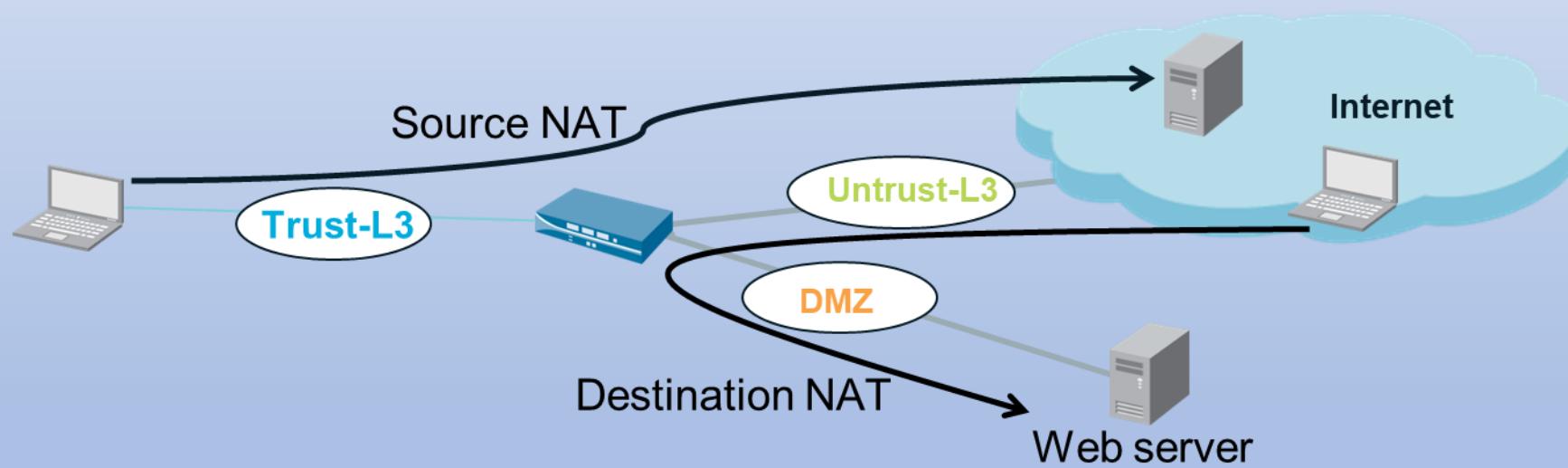
Network Address Translation (NAT)

Flow Logic of the Next-Generation Firewall



NAT Types

- Source NAT is commonly used for private (internal) users to access the public internet (outbound traffic).
- Destination NAT often is used to provide external (public) access to servers on the private network (inbound traffic).



Source NAT Types

Static IP

1-to-1 fixed translations

- Change the source IP address while leaving the source port unchanged

Dynamic IP

- 1-to-1 translations of a source IP address only (no port number)
- Private source address translates to the next available address in the range

Dynamic IP/Port (DIPP)

- Multiple clients use the same public IP addresses with different source port numbers
- Assigned address can be set to Interface address or Translated address

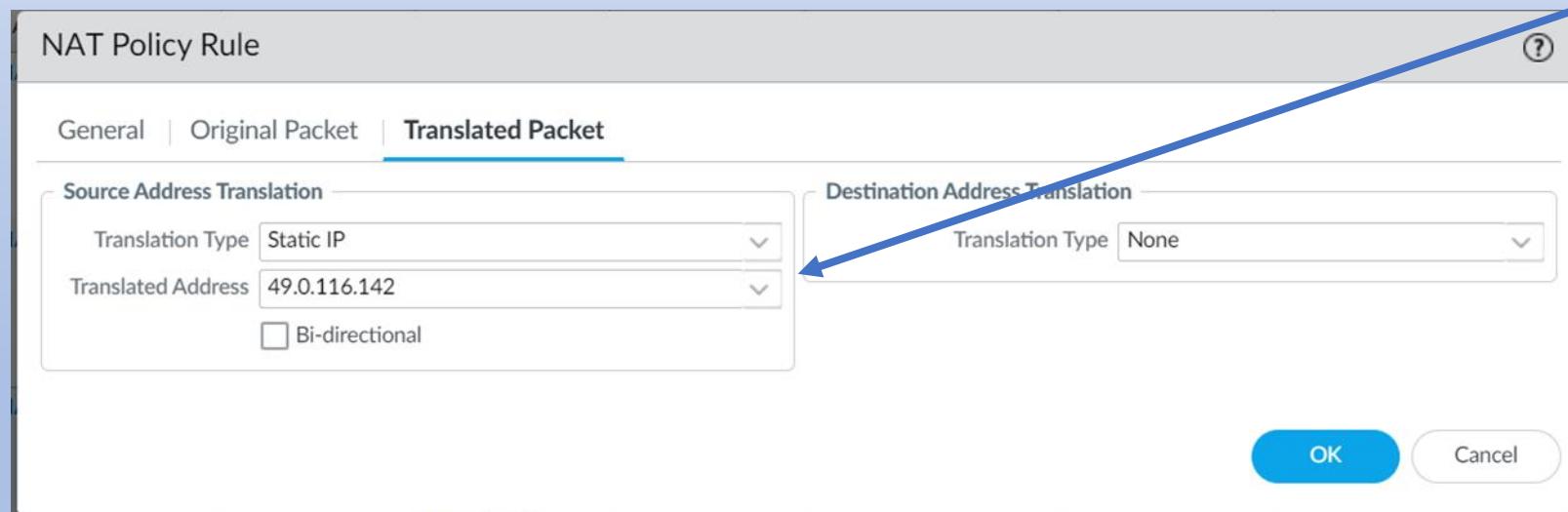
Source NAT Types

Static IP

1-to-1 fixed translations

Change the source IP address while leaving the source port unchanged

3	NAT to internet	none	Trust	Untrust	any	192.168.1.10/...	any	any	static-ip 49.0.116.142 bi-directional: no
---	-----------------	------	-------	---------	-----	------------------	-----	-----	---

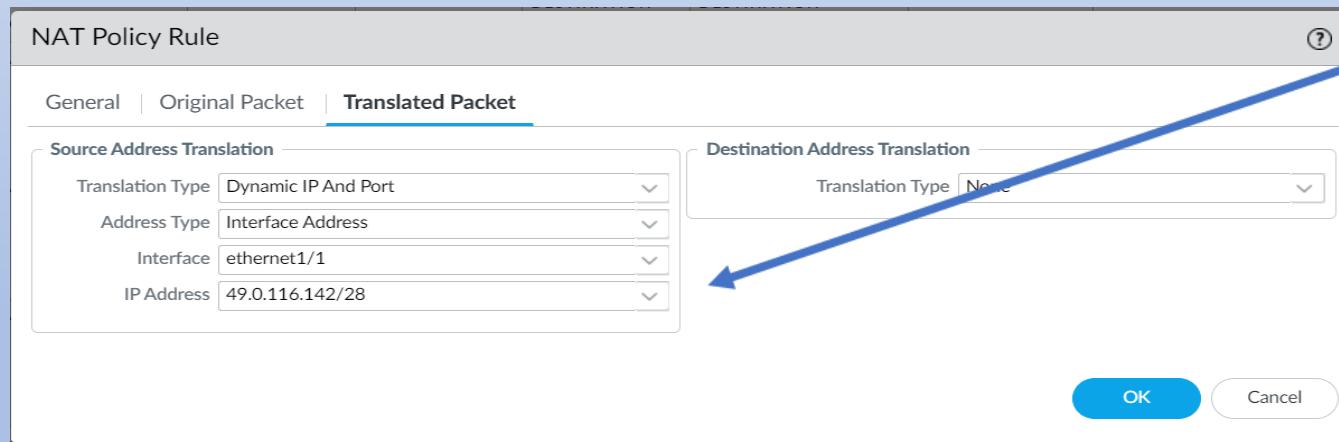


Source NAT Types

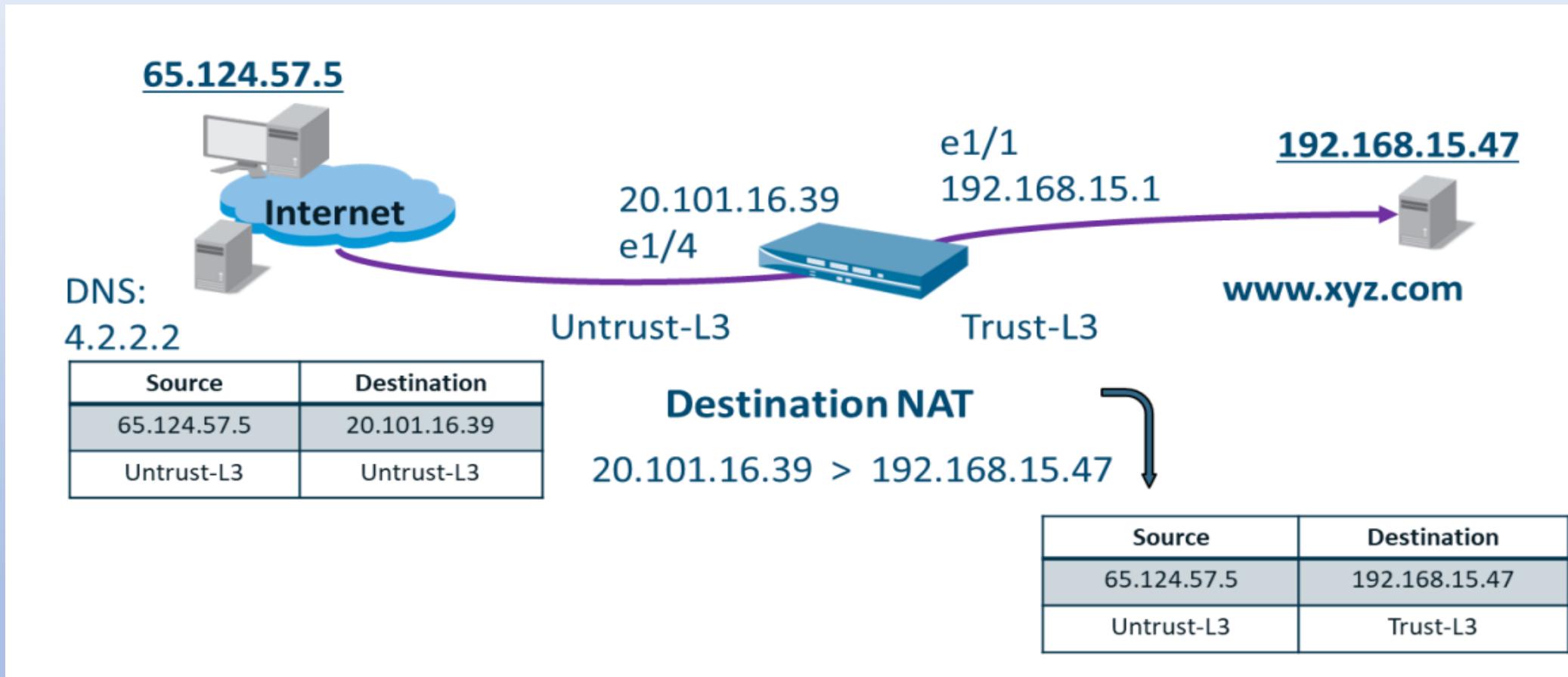
Dynamic IP/Port

- Multiple clients use the same public IP addresses
- Assigned address can be set to Interface address

3	NAT to internet	none	Trust	Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1 49.0.116.142/28
---	-----------------	------	-------	---------	-----	-----	-----	-----	---



Destination NAT Example

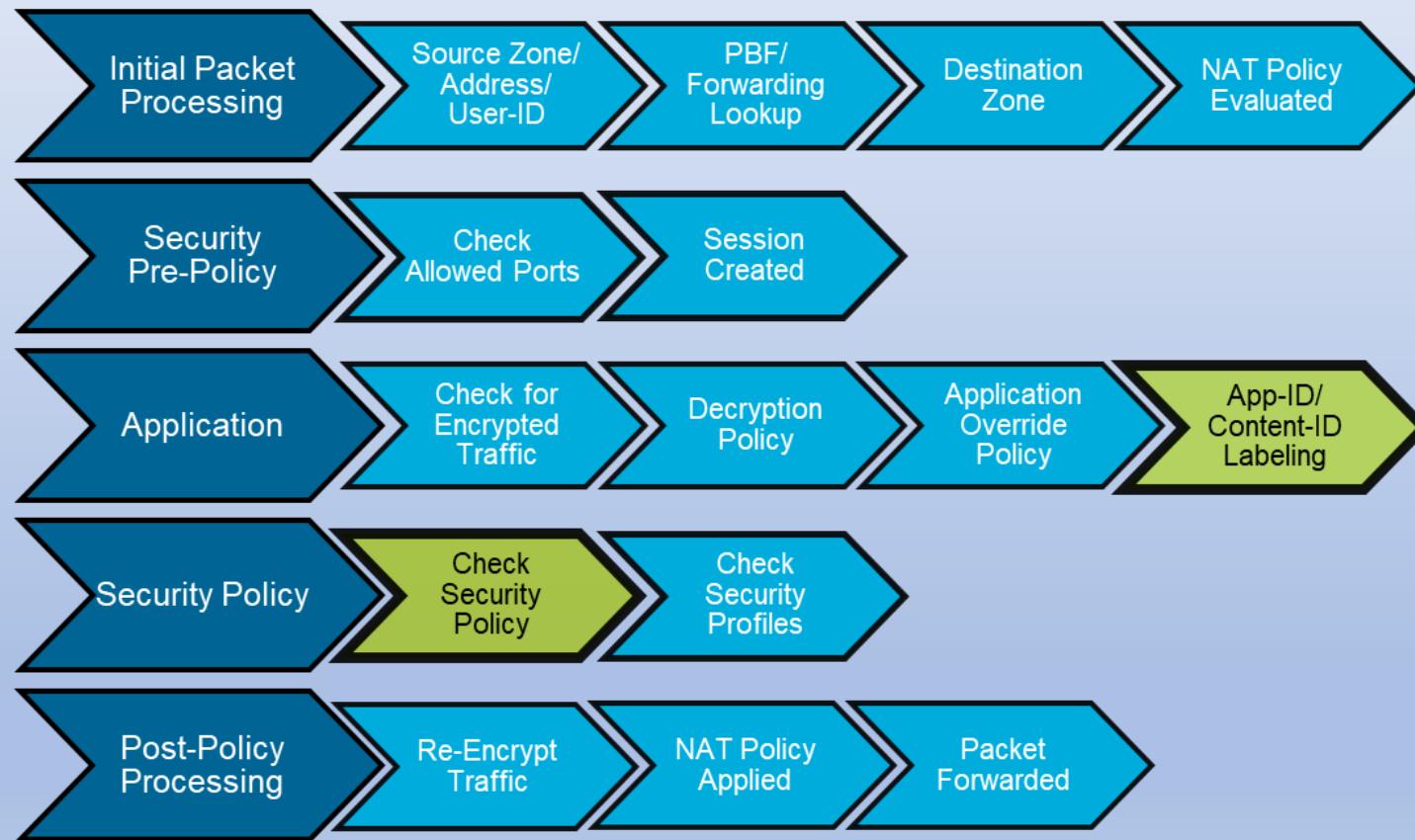


Destination NAT Example Policies

Policies > NAT										
Original Packet										
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	DST NAT	none	Untrust-L3	Untrust-L3	any	any	20.101.16.39	any	none	address: 192.168.15.47
Translated Packet										
Policies > Security										
Source										
	Name	Tags	Type	Zone	Address	Zone	Address	Application	Service	Action
1	Int Server Access	none	universal	Untrust-L3	any	Trust-L3	20.101.16.39	web-browsing	service-http	<input checked="" type="checkbox"/>
Post-NAT Destination										
Source		Pre-NAT Destination				Post-NAT Destination				
65.124.57.5		20.101.16.39				192.168.15.47				
Untrust-L3		Untrust-L3				Trust-L3				

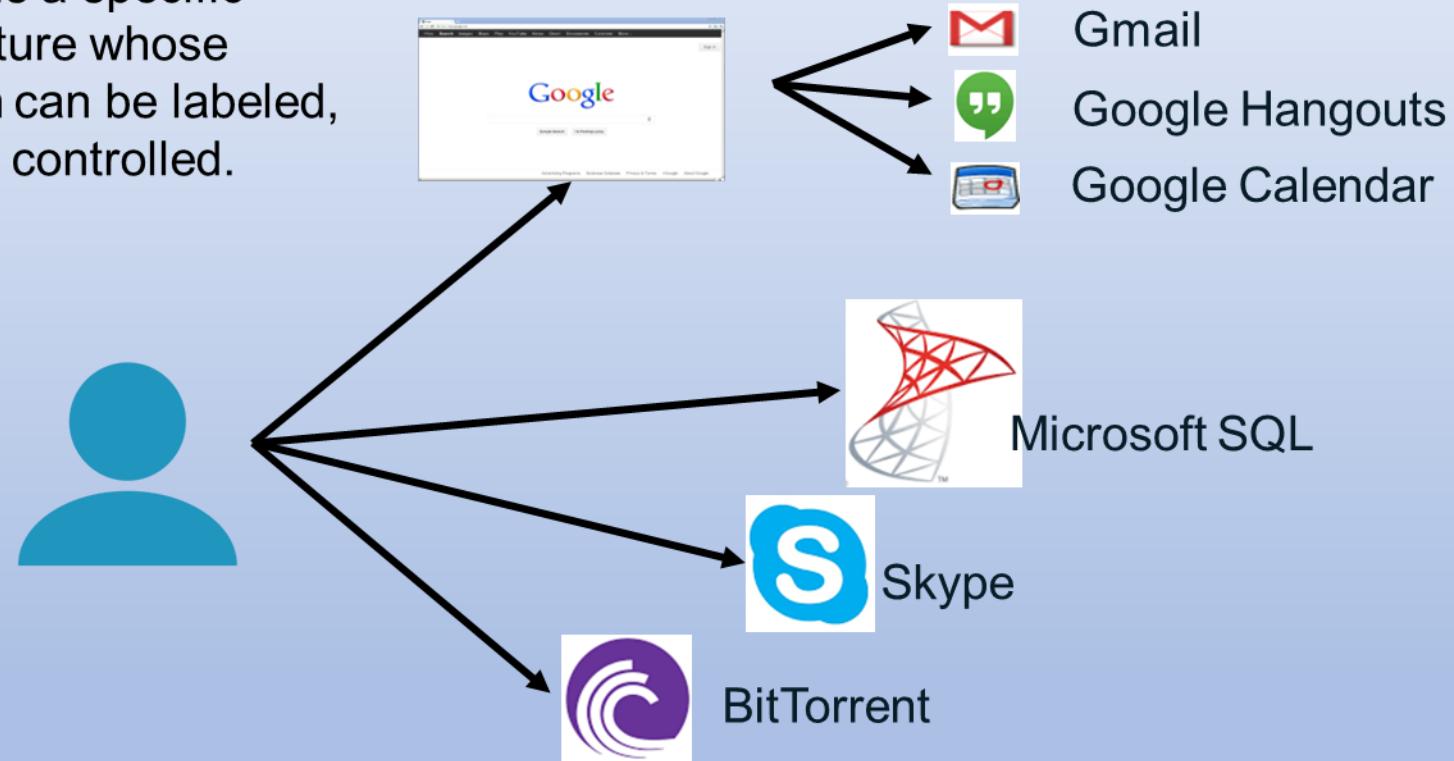
App-ID

Flow Logic of the Next-Generation Firewall



What Is an Application?

An *application* is a specific program or feature whose communication can be labeled, monitored, and controlled.



What Is App-ID?

- Multiple techniques to label traffic by application rather than just port

Port-based security rule

	Name	Type	Source			Destination					
			Zone	Address	User	Zone	Address	Application	Service		Action
1	FTP	universal	████ inside	any	any	████ outside	any	any	FTP	service-ftp	Allow

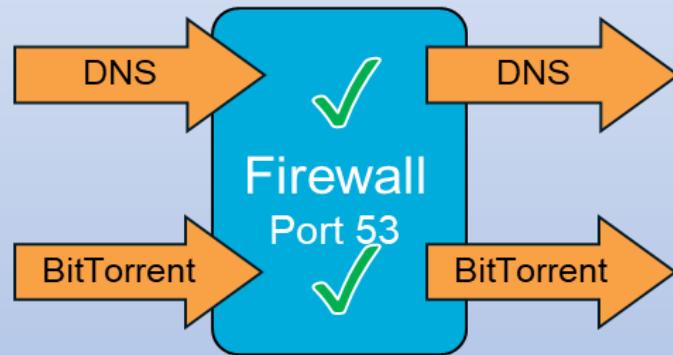
Application-based security rule

	Name	Type	Source			Destination					
			Zone	Address	User	Zone	Address	Application	Service		Action
1	FTP	universal	████ inside	any	any	████ outside	any	FTP	FTP	application-default	Allow

Port-Based Versus Next-Generation Firewalls

Traditional Firewalls

Firewall Rule: ALLOW Port 53



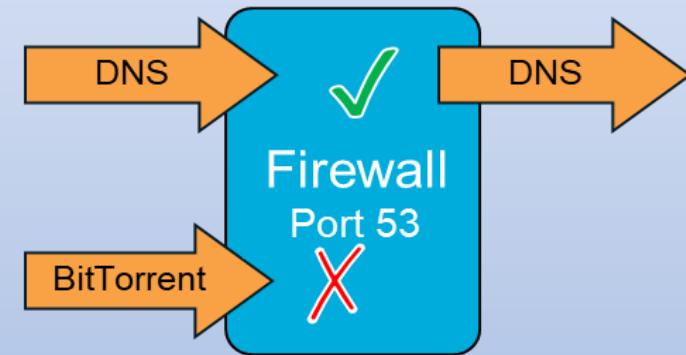
Packet on port 53: Allow

Packet on port 53: Allow

Visibility: Port 53 allowed

Palo Alto Networks Firewalls with App-ID

Firewall Rule: ALLOW DNS



DNS = DNS: Allow

BitTorrent ≠ DNS: Deny

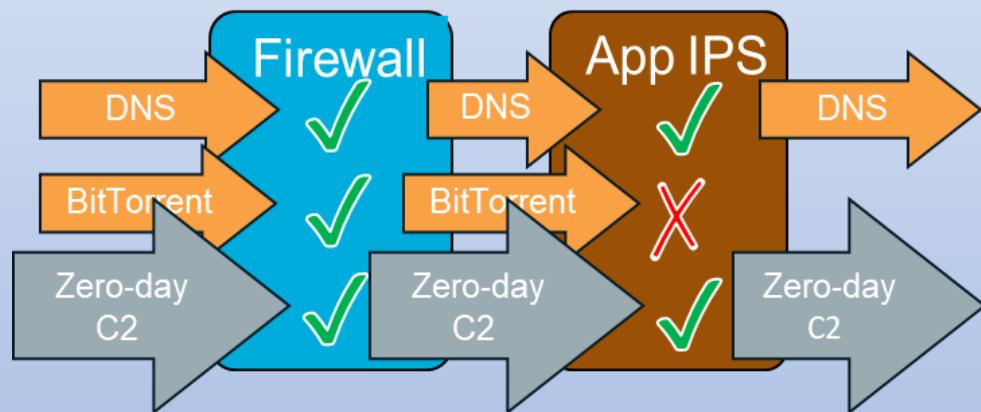
Visibility: BitTorrent detected and blocked

Zero-Day Malware – IPS Versus App-ID

Legacy Firewalls

Firewall Rule: ALLOW Port 53

Application IPS Rule: Block BitTorrent



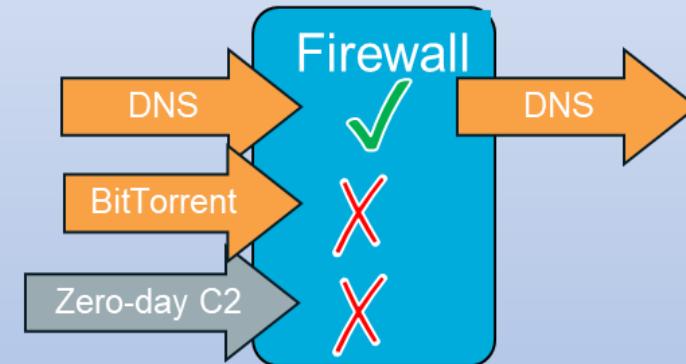
Packet on port 53: Allow

C2 ≠ BitTorrent: Allow

Visibility: Packet on port 53 allowed

Palo Alto Networks Firewall with App-ID

Firewall Rule: ALLOW DNS



DNS = DNS: Allow

C2 ≠ DNS: Deny

Visibility: Unknown traffic detected and blocked

Decryption Ruleset Example

- Decrypt everything except sensitive, legally protected traffic
- Create exception rules for specific zones, destination IP, source users, and URL categories
- Attach Decryption Profiles for more granular control

Policies > Decryption

	Name	Source			Destination						Type	Decryption Profile
	Name	Zone	Address	User	Zone	Address	URL Category	Service	Action			
1	Dest IP Addr Bypass	Trust-L3	any	any	UnTrust-L3	203.0.113.38	any	any	no-decrypt	ssl-forward-proxy	Lenient Profile	
2	Source User Exception	Trust-L3	any	User123	UnTrust-L3	any	any	any	no-decrypt	ssl-forward-proxy	Lenient Profile	
3	URL Exception Bypass	Trust-L3	any	any	UnTrust-L3	any	Decrypt Bypass	any	no-decrypt	ssl-forward-proxy	Lenient Profile	
4	Sensitive Category Bypass	Trust-L3	any	any	UnTrust-L3	any	financial-services government health-and-medicine military shopping	any	no-decrypt	ssl-forward-proxy	Lenient Profile	
Use multiple match criteria (not just URL categories) to refine decrypt rules												
5	Decrypt All Traffic	Trust-L3	any	any	UnTrust-L3	any	any	service-https	decrypt	ssl-forward-proxy	Tight SSL Control	

Using App-ID in a Security Policy

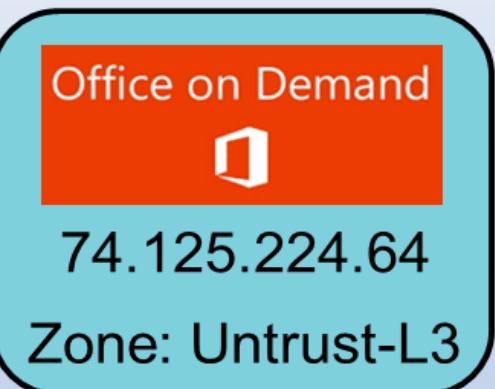
Dependent Applications



<http://translate.google.com>
 Destination Port: TCP 80

1. HTTP GET = web-browsing

2. Request specifically Office on Demand



	Name	Type	Source			Destination						URL Category	Action
			Zone	Address	User	Zone	Address	Application	Service				
1	Required Apps	universal	Trust-L3			Untrust-L3		ssl web-browsing ms-office365-base office-on-demand sharepoint-online				office-on-demand dependent on ms-office365-base and sharepoint-online	allow
2	Office 365	universal	Trust-L3	any	any	Untrust-L3	any						allow

Application shift



Applications and Security Policy Rules

Policies > Security

	Name	Type	Source			Destination		Application	Service	Action
			Zone	Address	User	Zone	Address			
1	Social Networking	universal	private	any	any	public	any	social-networking	application-default	Allow
2	Office Programs	universal	private	any	any	public	any	office-programs	application-default	Allow
3	FTP	universal	private	192...	any	public	any	ftp	application-default	Allow

Application
filter

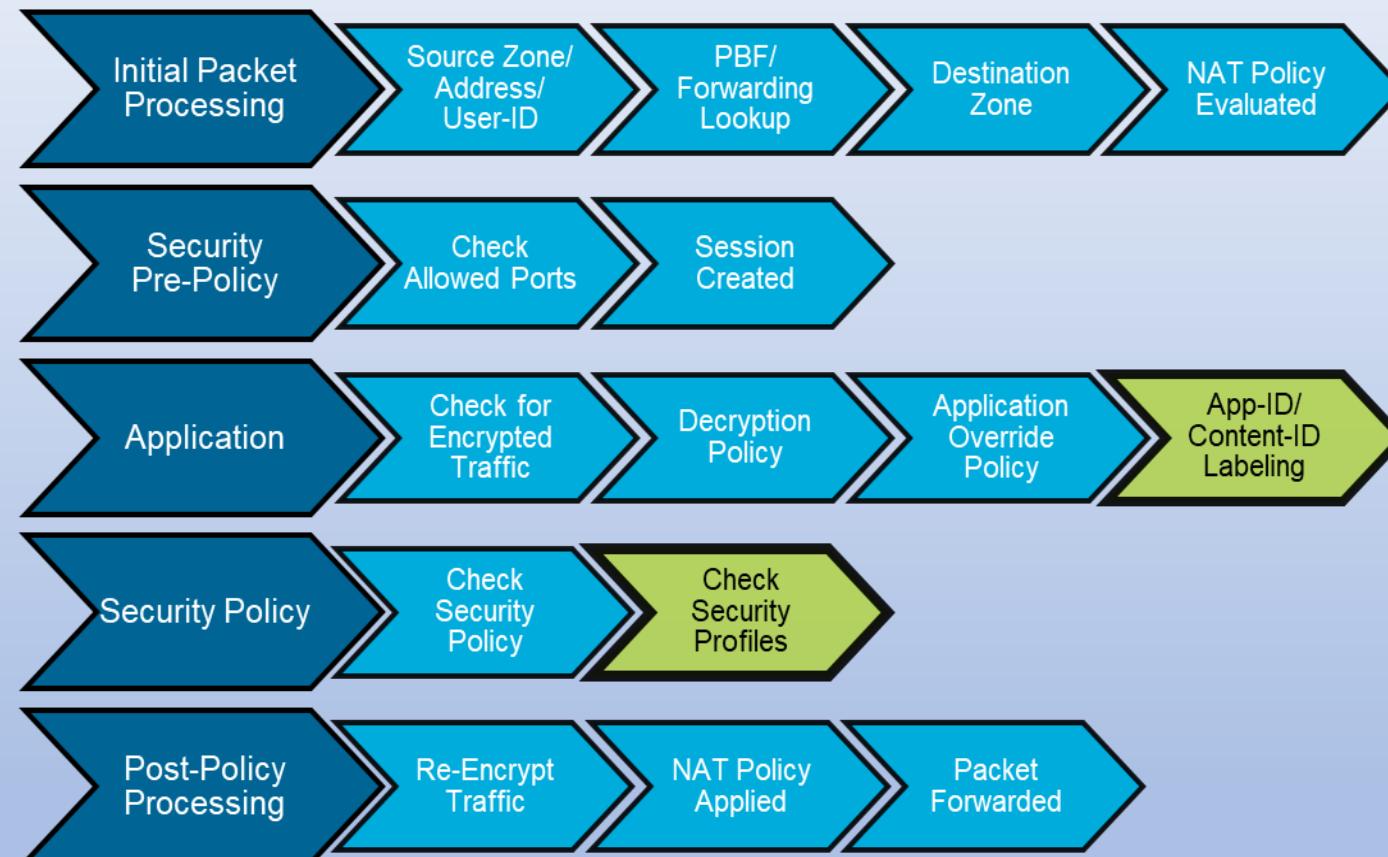
Application
group

Application

Content-ID

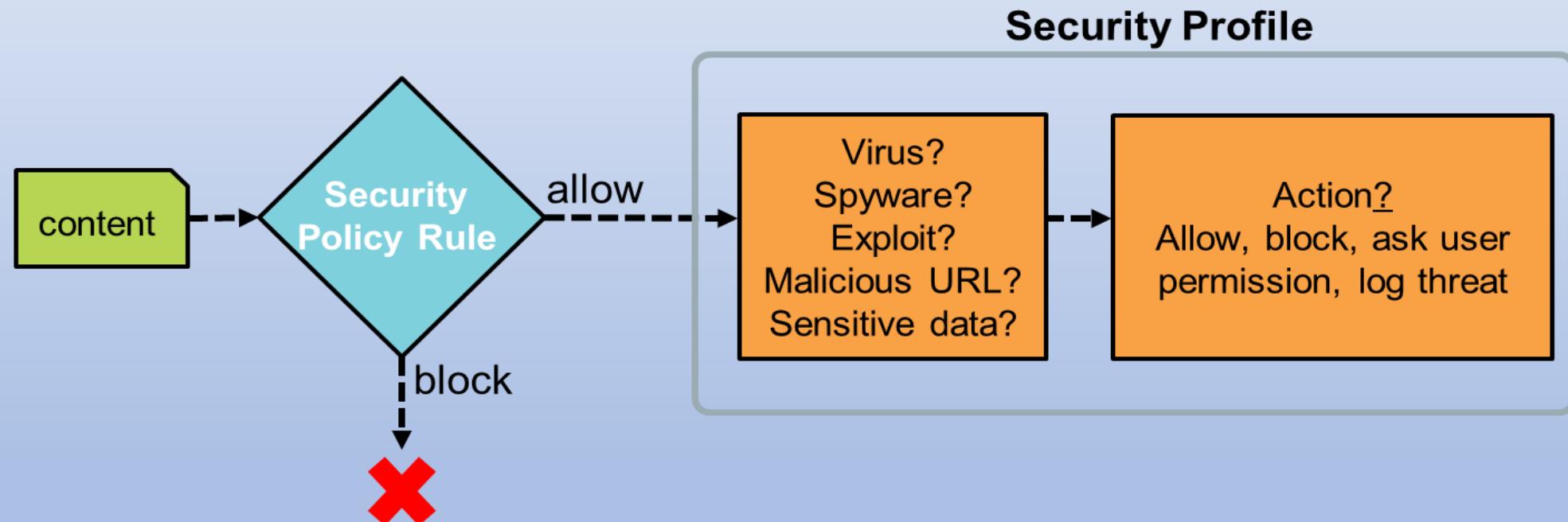
- Content-ID overview
- Vulnerability Protection Security Profiles
- Antivirus Security Profiles
- Anti-Spyware Security Profiles
- File Blocking Profiles
- Attaching Security Profiles to Security policy rules
- Telemetry and threat intelligence

Flow Logic



Security Policy with Security Profiles

- Security Profiles implement additional security checks on allowed traffic.



Security Profile Types

Policies > Security

	Name	Type	Source			Destination				Action	Profile
			Zone	Address	User	Zone	Address	Application	Service		
1	Limited Remote Access	universal	Trust-L3	192.168.1.3/24	any	Untrust-L3	any	dns ftp office-on-de...	application-default	Allow	
2	Unexpected Traffic	universal	Untrust-L3	any	any	Trust-L3	any	any	application-default	Allow	



Antivirus



Anti-Spyware



Vulnerability Protection



URL Filtering



File Blocking



Data Filtering



WildFire Analysis



Security Profile Group

Threat Log

- Vulnerability Protection, Antivirus, and Anti-spyware Profiles log events to the Threat log.

Monitor > Logs > Threat

	Receive Time	Type	ID	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	Severity
	11/08 09:18:49	vulnera...	42000	PDF-Exploit	Untrust-L3	Trust-L3	98.139.135.129	192.168.7.50	53920	web-browsing	reset-both	high
	11/08 09:18:25	vulnera...	42000	PDF-Exploit	Untrust-L3	Trust-L3	98.139.135.129	192.168.7.50	53919	web-browsing	reset-both	high
	11/08 09:17:50	vulnera...	42000	PDF-Exploit	Untrust-L3	Trust-L3	98.139.135.129	192.168.7.50	53912	web-browsing	reset-both	high
	11/08 07:10:14	virus	100000	Eicar Test File	Untrust-L3	Trust-L3	213.211.198.62	192.168.7.50	52797	web-browsing	reset-server	medium
	11/08 07:06:15	virus	100000	Eicar Test File	Untrust-L3	Trust-L3	213.211.198.62	192.168.7.50	52749	web-browsing	alert	medium

Click a column header to change number of displayed columns

Includes packet capture

Open Threat Details window

Vulnerability Protection Security Profiles

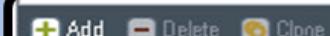
Default Vulnerability Protection Security Profiles

Objects > Security Profiles > Vulnerability Protection

Name	Location	Count	Rule Name	Threat Name	Host Type	Severity	Action	Packet Capture
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...					
default	Predefined	Rules: 6	simple-client-critical	any	client	critical	default	disable

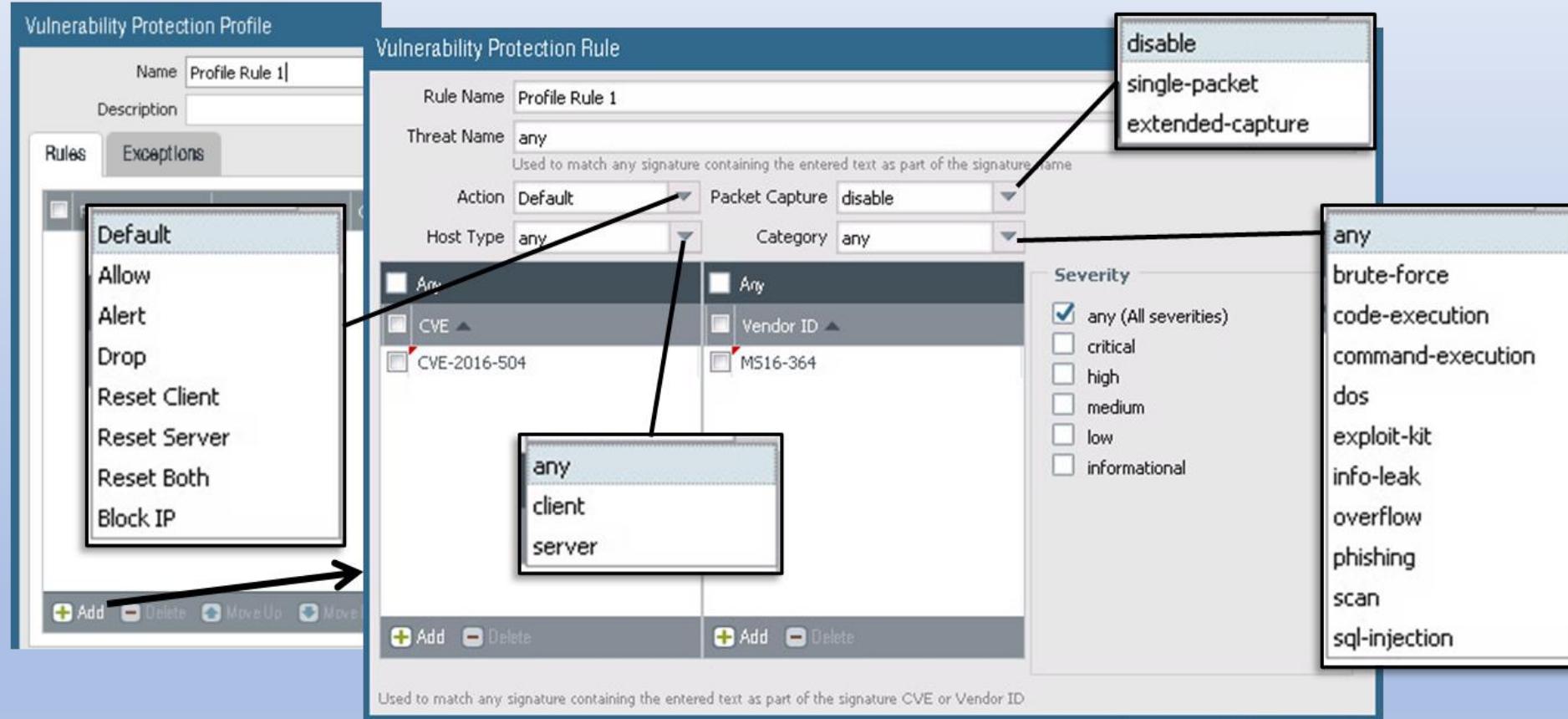
- To create customized profile actions:
 - Clone** the default read-only profile and edit clone, or
 - Add** a brand new profile

Rules specify actions on detected events



Vulnerability Protection Profile Rules

Objects > Security Profiles > Vulnerability Protection > Add > Rules



Vulnerability Exceptions

Objects > Security Profiles > Vulnerability Protection > Add

Screenshot of the Palo Alto Networks UI for adding a Vulnerability Protection Profile. The interface shows a list of threats with columns for ID, Threat Name, IP Address Exemptions, Rule, CVE, Host, Category, Severity, Action, and Packet Capture.

Annotations:

- A callout points to the "IP Address Exemptions" column with the text: "Override the action configured in the rules".
- A callout points to the "Packet Capture" column with the text: "Click to modify packet capture setting".
- A callout points to the bottom-left of the table with the text: "Click to view or add IP addresses".
- A callout points to the "Show all signatures" checkbox at the bottom-left of the table with a black border around it.

Enable	ID	Threat Name	IP Address Exemptions	Rule	CVE	Host	Category	Severity	Action	Packet Capture
<input type="checkbox"/>	35931	HP Data Protector OmniNet Opcode Buffer Overflow Vulnerability	3		CVE-2011-1865	server	overflow	high	default (alert)	disable
<input type="checkbox"/>	35933	HP Data Protector OmniNet Opcode 27 Buffer Overflow Vulnerability			CVE-2011-1865	server	overflow	high	default (alert)	disable
<input type="checkbox"/>	34168	HP OpenView Data Protector Application Recovery Manager Buffer Overflow Vulnerability				server	overflow	high	default (reset-server)	disable
<input type="checkbox"/>	39371	HP Data Protector Client EXEC_CMD Command Execution Vulnerability			CVE-2011-0923	server	code-execution	high	default (alert)	disable

Antivirus Security Profiles

Default Antivirus Security Profile

Objects > Security Profiles > Antivirus



The screenshot shows the 'Antivirus' security profile configuration. The 'Decoders' section is highlighted with a black border. The 'Action' column lists actions like 'default (reset-both)', 'default (alert)', and 'default (allow)'. The 'WildFire Action' column lists actions like 'allow' and 'reset-both'. A callout box points to the 'default' profile in the list, labeled 'Out-of-the-box profile'. Another callout box points to the 'Decoders' section, explaining the 'Action' and 'WildFire Action' columns.

Name	Location	Packet Capture	Decoders			Application Exceptions			Threat Exceptions
			Name	Action	WildFire Action	Name	Action		
default	Predefined		http	default (reset-both)	allow				0
			smtp	default (alert)	allow				
			imap	default (alert)	allow				
			pop3	default (alert)	allow				
			ftp	default (reset-both)	allow				
			smb	default (reset-both)	allow				

Action to take based on antivirus signatures delivered in content updates

WildFire Action to take based on signatures delivered by WildFire

- To create customized profile actions:
 - Clone** the default read-only profile and edit clone, or
 - Add** a brand new profile

Creating a New Antivirus Profile

Objects > Security Profiles > Antivirus > Add

Available actions

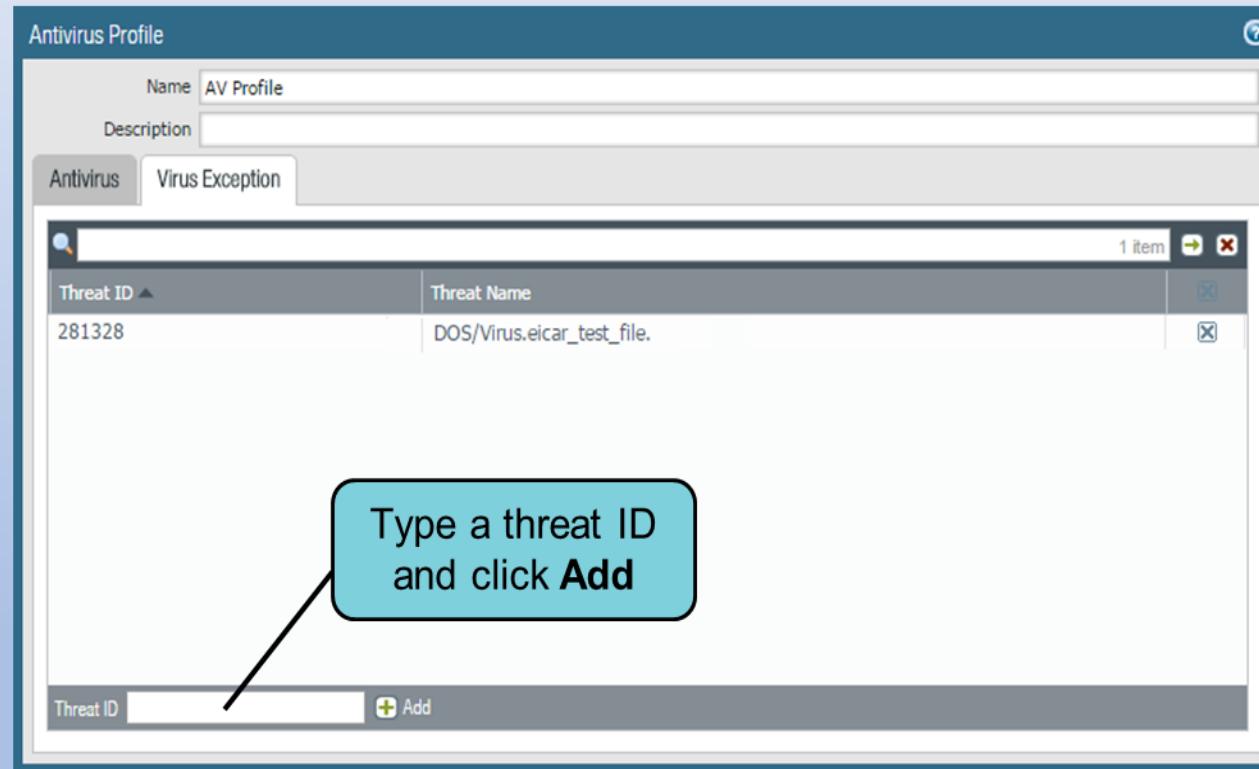


The screenshot shows the 'Antivirus Profile' configuration screen. The 'Name' field is set to 'AV Profile'. The 'Decoders' section lists various protocols (ftp, http, imap, pop3, smb, smtp) with their corresponding 'Action' and 'WildFire Action' set to 'default (reset-both)'. A callout box with the text 'Click to modify to something other than “default” action' points to the 'Action' column of the decoder table. To the right, there's a 'Application Exception' section which is currently empty, with a callout box stating 'Add applications to exempt from the profile'.

Decoder	Action	WildFire Action
ftp	default (reset-both)	default (reset-both)
http	default (reset-both)	default (reset-both)
imap	default (alert)	default (alert)
pop3	default (alert)	default (alert)
smb	default (reset-both)	default (reset-both)
smtp	default (alert)	default (alert)

Creating a New Antivirus Profile (Cont.)

Objects > Security Profiles > Antivirus > Add



- To reduce false positives use Threat ID to create an exemption
- Threat IDs recorded in Threat log

Anti-Spyware Security Profiles

Default Anti-Spyware Security Profiles

Objects > Security Profiles > Anti-Spyware

Name	Location	Count	Rule Name	Threat Name	Severity	Action	Packet Capture	DNS Packet Capture
default	Predefined	Rules: 4	simple-critical	any	critical	default	disable	disable
			simple-high	any	high	default	disable	
			simple-medium	any	medium	default	disable	
			simple-low	any	low	default	disable	
strict	Predefined	Rules: 5	simple-critical	any	critical	reset-both	disable	disable
			simple-high	any	high	reset-both		
			simple-medium	any	medium	reset-both		
			simple-informational	any	informational	default		
			simple-low	any	low	default		

Out-of-the-box profiles

Rules specify actions on detected spyware

Add **Delete** **Clone**

- To create customized profile actions:
 - Clone** a default read-only profile and edit clone, or
 - Add** a brand new profile

Configuring Anti-Spyware Profile Rules

Objects > Security Profiles > Anti-Spyware > Add > Rules

Anti-Spyware Profile

Name: Strict-AntiS

Description:

Rules Exceptions DNS

Anti-Spyware Rule

Rule Name: New Rule

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

Category: backdoor

Action: Default

Packet Capture: disable

Severity

- any (All severities)
- critical
- high
- medium
- low
- informational

Actions:

- disable
- single-packet
- extended-capture

Threat Names:

- adware
- any
- autogen
- backdoor
- botnet
- browser-hijack
- data-theft
- dns
- dns-wildfire
- keylogger
- net-worm
- p2p-communication
- spyware

Anti-Spyware Exceptions

Objects > Security Profiles > Anti-Spyware > Add

Anti-Spyware Profile

Name: Strict-AntiSpyware

Description:

Rules Exceptions DNS Signatures

Can override the action configured in the rules

Click to override rule's packet capture setting

Click to view or add IP addresses

Show all signatures

Enable	ID	Threat Name	IP Address Exemptions	Rule	Category	Severity	Action	Packet Capture
<input type="checkbox"/>	10585	CIA_1_22 Get password		simple-high	data-theft	high	default (alert)	disable
<input type="checkbox"/>	10313	Ezula_Toptext Popup		simple-low	adware	low	default (alert)	enable
<input type="checkbox"/>	10328	FeRAT_1		simple-high	adware	high	default (alert)	enable
<input type="checkbox"/>	10373	Wintective_Keylogger		simple-high	keylogger	high	default (alert)	enable
<input type="checkbox"/>	10046	Scar User-Agent Traffic		simple-medium	spyware	medium	default (alert)	enable
<input type="checkbox"/>	10522	SearchBossToolbar				low	default (alert)	enable
<input type="checkbox"/>	10223	FunBuddyIcons View Fub Buddy icons				low	default (alert)	enable
<input type="checkbox"/>	10286	Virtumonde info post				low	default (alert)	enable
<input type="checkbox"/>	10333	OpnT_Trojan_1_1 connection				high	default (alert)	enable

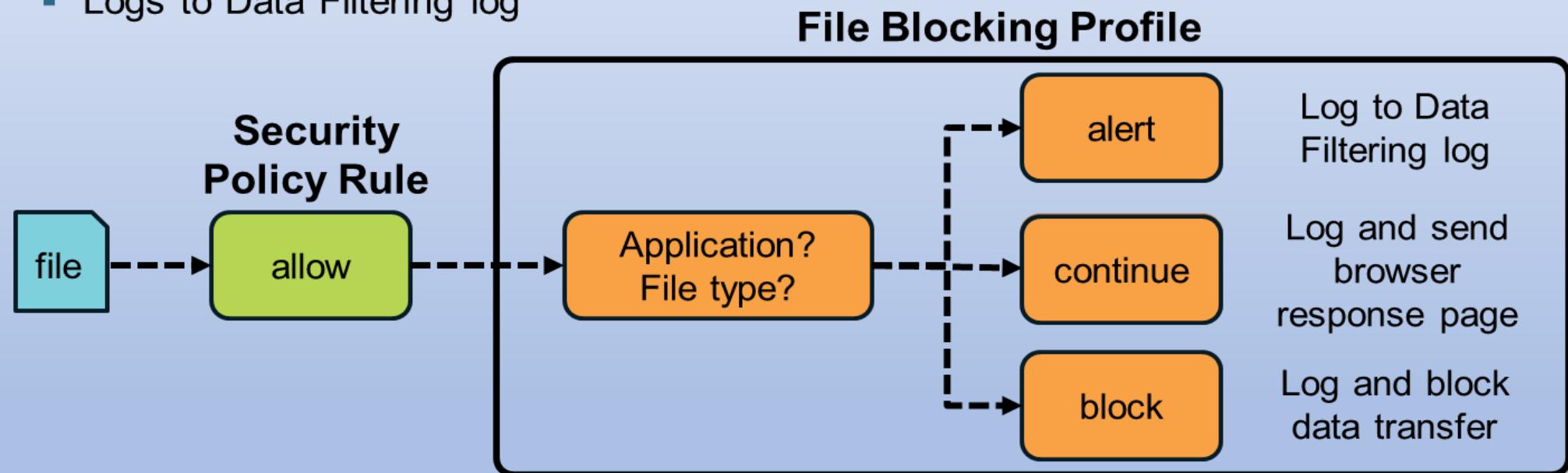
4118 items

1 of 138 | Page | Displaying 1 - 30 / 4118 threats

File Blocking Profiles

File Blocking Overview

- Prevent introduction of malicious data
- Prevent exfiltration of sensitive data
- Logs to Data Filtering log



Data Filtering Log

- Data Filtering log records name and file type of blocked files
- Source is the system that sent the file.
- Destination is the system that received the file.

Monitor > Logs > Data Filtering

	Receive Time	File Name	Name	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
	08/12 21:24:00	44.0.2403.155_44.0.2403.130_chrome_updater.exe	Microsoft PE File	Untrust-L3	Trust-L3	74.125.170.11	192.168.14.50	61813	web-browsing	deny	General Internet
	08/12 21:23:25	44.0.2403.155_44.0.2403.130_chrome_updater.exe	Microsoft PE File	Untrust-L3	Trust-L3	74.125.170.11	192.168.14.50	61811	web-browsing	deny	General Internet
	08/12 21:22:19	44.0.2403.155_44.0.2403.130_chrome_updater.exe	Microsoft PE File	Untrust-L3	Trust-L3	74.125.170.11	192.168.14.50	61810	web-browsing	deny	General Internet
	08/12 21:21:13	44.0.2403.155_44.0.2403.130_chrome_updater.exe	Microsoft PE File	Untrust-L3	Trust-L3	74.125.170.11	192.168.14.50	61807	web-browsing	deny	General Internet
	08/12 21:20:07	44.0.2403.155_44.0.2403.130_chrome_updater.exe	Microsoft PE File	Untrust-L3	Trust-L3	74.125.170.11	192.168.14.50	61803	web-browsing	deny	General Internet
	08/12 21:19:00	44.0.2403.155_44.0.2403.130_chrome_updater.exe	Microsoft PE File	Untrust-L3	Trust-L3	74.125.170.11	192.168.14.50	61802	web-browsing	deny	General Internet

Creating a New File Blocking Profile

Objects > Security Profiles > File Blocking > Add

File Blocking Profile

Name: file-blocking

Description:

Name	Applications	File Types	Direction	Action
A	web-browsing	any	both	alert
B	any	any	both	continue

Add one or more rules to control file transfer

upload
download
both

alert
block
continue

Add Delete

Continue Response Page

- A "continue" action requires user permission to complete file transfer.
- Only functional with web-browsing application

File Download Blocked

Access to the file you were trying to download has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

File name: Support_services_ds1.pdf

Please click **Continue** to download/upload the file.

Attaching Security Profiles to Security Policy Rules

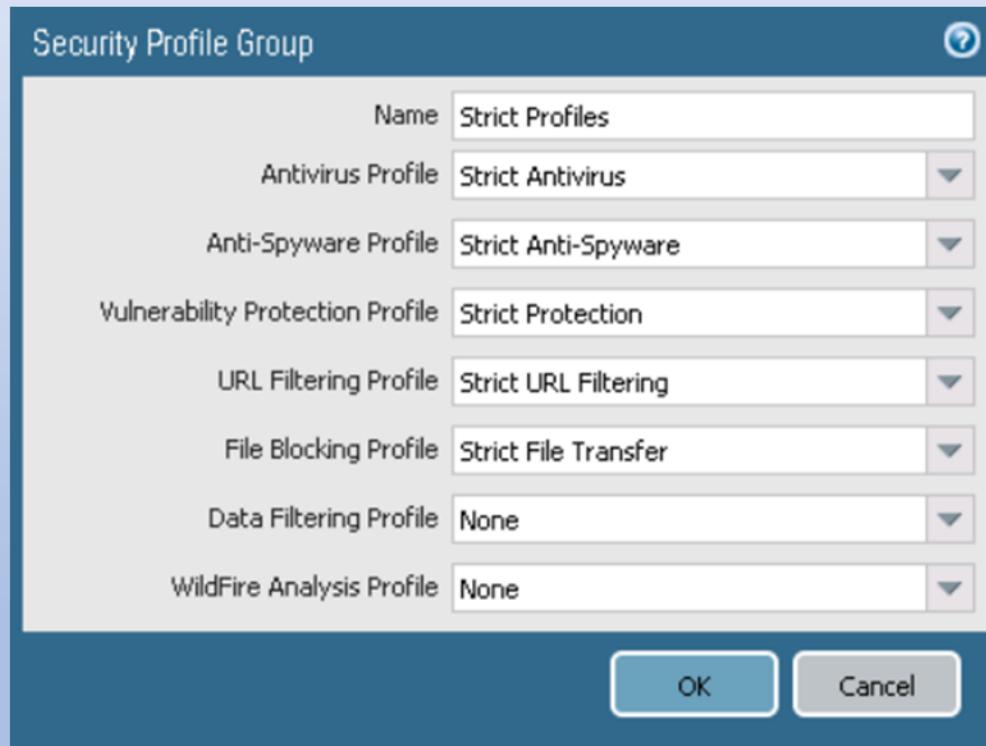
Security Profile Groups

Objects > Security Profile Groups > Add

Security Profile Group

Name	Strict Profiles
Antivirus Profile	Strict Antivirus
Anti-Spyware Profile	Strict Anti-Spyware
Vulnerability Protection Profile	Strict Protection
URL Filtering Profile	Strict URL Filtering
File Blocking Profile	Strict File Transfer
Data Filtering Profile	None
WildFire Analysis Profile	None

OK Cancel



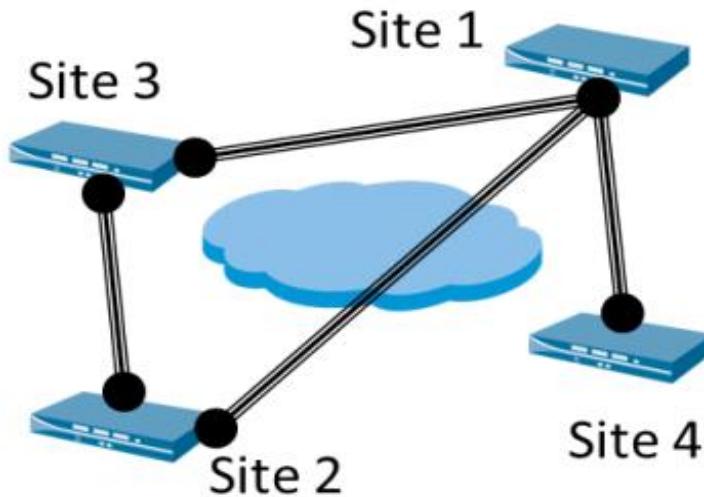
- Add Security Profiles that are commonly used together
- Simplifies Security policy rule administration

5.

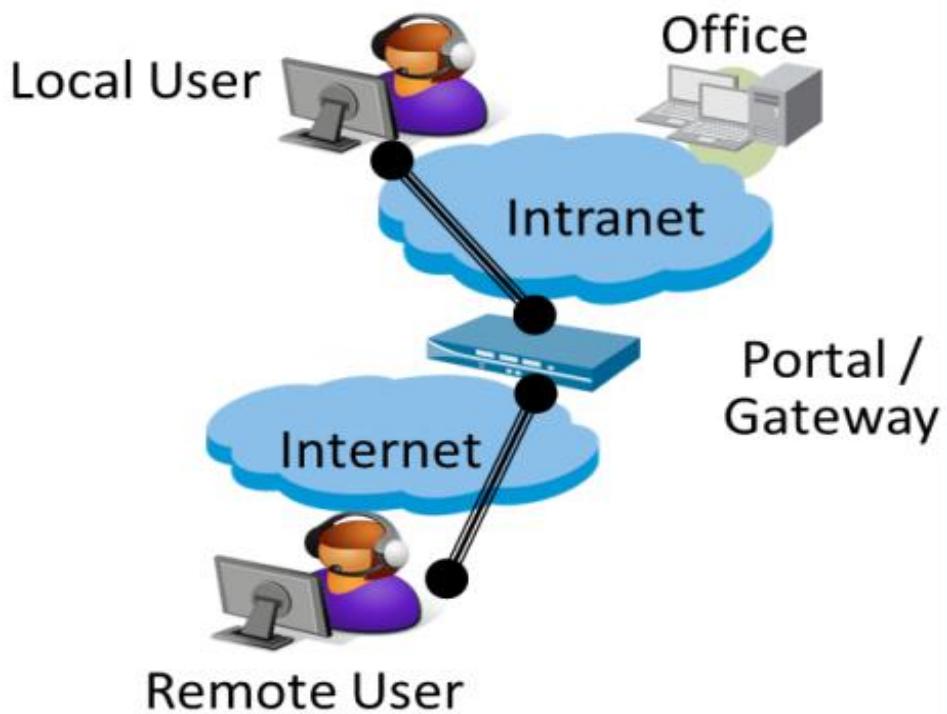
Site-to-Site VPNs

Site-to-Site and Client VPNs

IPsec VPN for site-to-site
and site-to-multi site



GlobalProtect SSL-VPN
for user-to-gateway



Site-to-Site Overview

PAN-OS implements route based IPsec VPNs

- Traffic is tunneled based on the destination of traffic
- Policy-based systems match the traffic on source and destination addresses, as well as service (port) The tunnel is represented by a logical tunnel interface
- Tunnel interface is placed into a Zone The Routing table chooses the tunnel settings

Phase 1 – Internet Key Exchange (IKE)

IKE Phase 1 identifies the end points of the VPN
IKE Phase 1 uses Peer IDs to identify the devices

- For devices with known addresses, the Peer ID is usually the IP address
- A Peer ID can also be a domain name or other string

Three Settings (Modes): Aggressive, Main, Auto



Phase 2 - IPsec

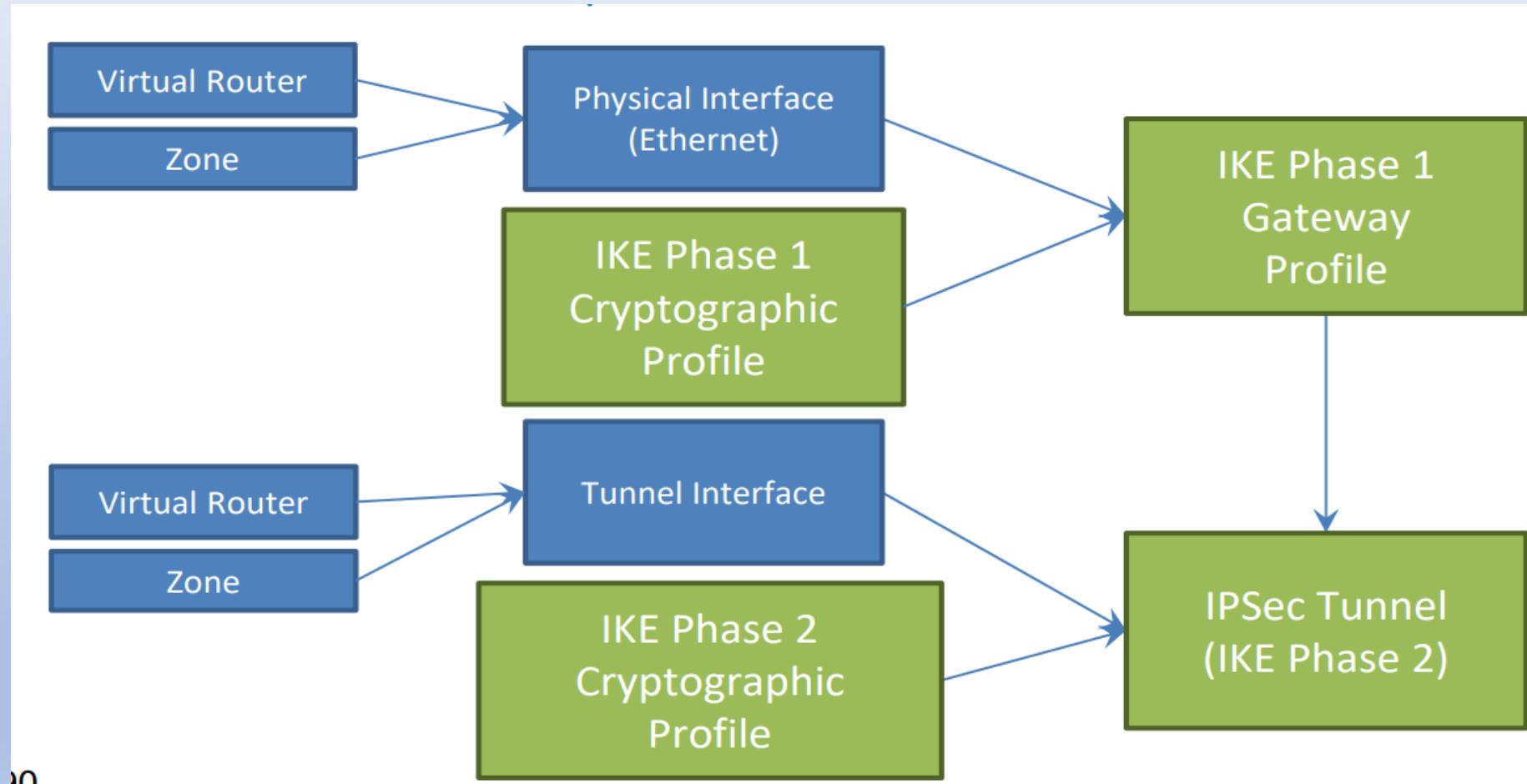
IKE Phase 2 defines connected private networks and creates the Tunnel

Each side of the Tunnel will have a Proxy ID to ID traffic

- Support for multiple Proxy IDs Networks are identified by Proxy ID and can be either:
 - Masked Network (e.g., 10.2.0.0/24)
 - Any network (0.0.0.0/0)
 - Perfect Forward Secrecy uses a second DH key exchange



VPN Tunnel Component Interaction



Reporting

Dashboard

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE Commit Widgets Last updated 20:22:47

Layout 3 Columns ▾ 5 mins ▾

General Information

Device Name	PA-VM
MGT IP Address	192.168.100.1
MGT Netmask	255.255.255.0
MGT Default Gateway	192.168.100.254
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::250:56ff:feb4:ead6/64
MGT IPv6 Default Gateway	
MGT MAC Address	00:50:56:b4:ea:d6
Model	PA-VM
Serial #	007051000246043
CPU ID	ESX:50060500FFFFB8B1F
UUID	42340F05-0EFO-CA6E-C559-ECAF3B123EA0
VM Cores	2
VM Memory	7126152
VM License	VM-100
VM Capacity Tier	6.5 GB
VM Mode	VMware ESXi
Software Version	11.0.2
GlobalProtect Agent	0.0.0
Application Version	8752-8277 (09/08/23)
Threat Version	8752-8277 (09/08/23)
Device Dictionary Version	62-361 (11/11/22)
URL Filtering Version	20230909.20200

Logged In Admins

Admin	From	Client	Session Start	Idle For
admin	49.228.231.238	Web	09/10/2023 05:58:38	00:00:01s

Data Logs
No data available.

System Logs

Description	Time
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 49.0.116.142	09/10 11:14:47
PAN-DB was upgraded to version 20230909.20200.	09/10 11:11:13
PAN-DB was upgraded to version 20230909.20199.	09/10 11:06:12
PAN-DB was upgraded to version 20230909.20198.	09/10 11:01:12
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 49.0.116.142	09/10 10:59:49
PAN-DB was upgraded to version 20230909.20196.	09/10 10:56:11
PAN-DB was upgraded to version 20230909.20195.	09/10 10:51:10
PAN-DB was upgraded to version 20230909.20194.	09/10 10:46:09
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 49.0.116.142	09/10 10:44:26

Top High Risk Applications

Application	SSL
ssl	ssl

Application Command Center (ACC)

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE |

Network Activity Threat Activity Blocked Activity Tunnel Activity GlobalProtect Activity SSL Activity Auto Refresh

Time 09/10 10:15:00-09/10 11:14:59

Global Filters

Application View Risk Sanctioned State Show system events

Application Usage

bytes sessions threats content URLs users

Home

Application Categories

- networking
- encrypted-tunnel
- ssl

APPLICATION	RISK	BYTES	SESSIONS	THREATS	CONTENT	URLS	USERS
ssl	4	6.2M	45	0	0	0	2
ntp-base	2	43.2k	66	0	0	0	3
dns-base	3	3.7k	20	0	0	0	2

User Activity

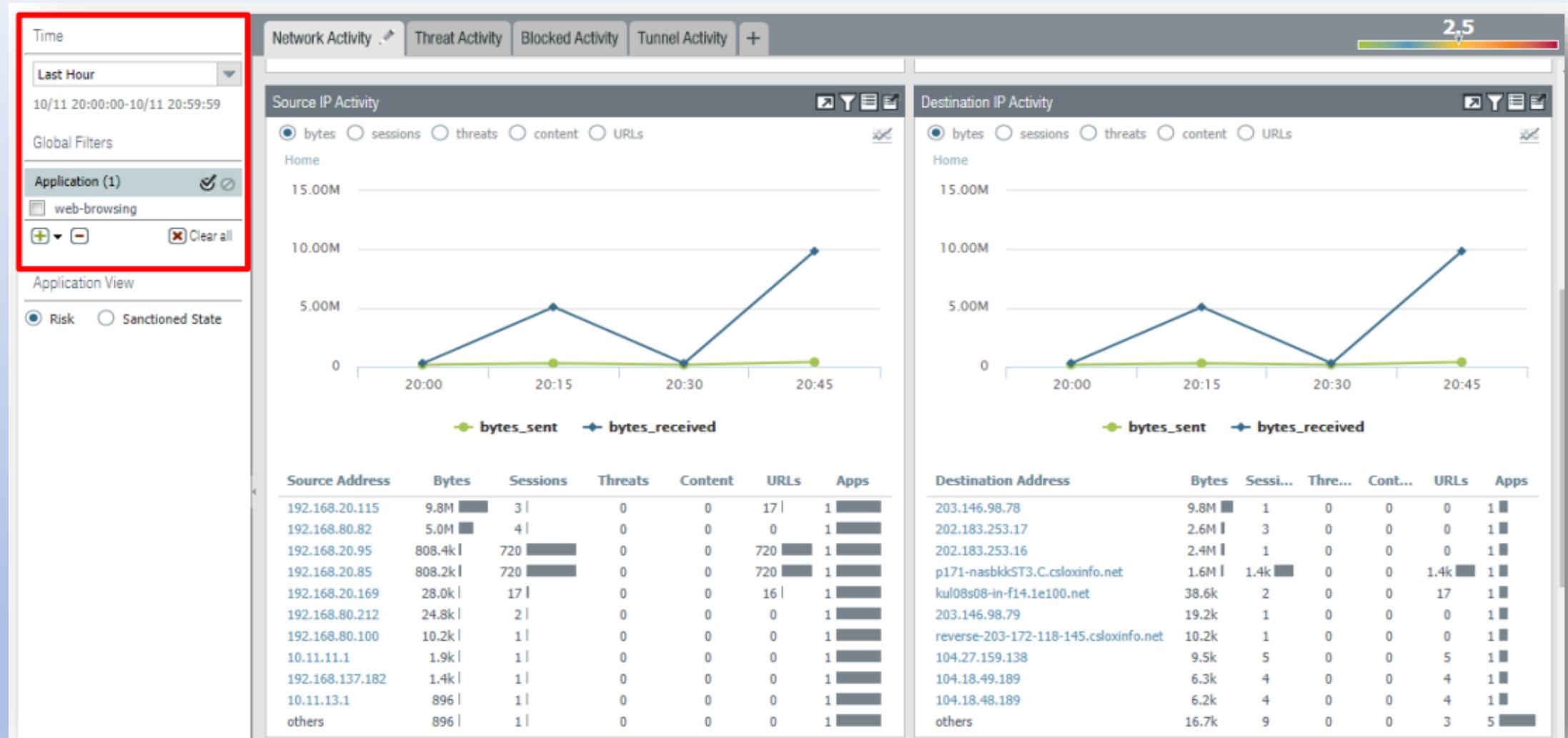
bytes sessions threats content URLs apps

Home

bytes_sent (green line with circles) and bytes_received (blue line with diamonds)

SOURCE	USER	DESTINATION	BYTES	SESSIONS	THREATS	CONTENT	URLS	APPS
None	None	None	6.3M	131	0	0	0	3

Drilling Down



Session Browser

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE Commit □ □ □ ?

HIP Match GlobalProtect IP-Tag User-ID Decryption Tunnel Inspection Configuration System Alarms Authentication Unified Packet Capture App Scope Summary Change Monitor Threat Monitor Threat Map Network Monitor Traffic Map Session Browser Botnet PDF Reports Manage PDF Summary User Activity Report SaaS Application Usage Report Groups Email Scheduler Manage Custom Reports Reports PDF/CSV

Filters → × +

	START TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATI...	FROM PORT	TO PORT	PROTOC...	APPLICATI...	RULE	INGRESS I/F	EGRESS I/F	BYTES	VIRTUAL SYSTEM	CLE...
[+]	09/10 11:20:38	Untrust	Untrust	49.228.231....	49.0.116.142	56536	4443	6	ssl	intrazon... default	ethernet1/1	ethernet1/1	42320	vsys1	<input checked="" type="checkbox"/>
[+]	09/10 11:22:39	Untrust	Untrust	49.228.231....	49.0.116.142	45202	4443	6	ssl	intrazon... default	ethernet1/1	ethernet1/1	35103	vsys1	<input checked="" type="checkbox"/>
[+]	09/10 11:04:09	Untrust	Untrust	49.0.116.142	35.190.82.33	56675	443	6	paloalto-updates	intrazon... default	ethernet1/1	ethernet1/1	20054	vsys1	<input checked="" type="checkbox"/>
[+]	09/10 11:20:38	Untrust	Untrust	49.228.231....	49.0.116.142	56533	4443	6	ssl	intrazon... default	ethernet1/1	ethernet1/1	162533	vsys1	<input checked="" type="checkbox"/>
[+]	09/10 11:22:39	Untrust	Untrust	49.228.231....	49.0.116.142	27533	4443	6	ssl	intrazon... default	ethernet1/1	ethernet1/1	1290	vsys1	<input checked="" type="checkbox"/>
[+]	09/10 11:21:54	Untrust	Untrust	162.216.15...	49.0.116.142	52338	30103	6	undecided	intrazon... default	ethernet1/1	ethernet1/1	60	vsys1	<input checked="" type="checkbox"/>
[+]	09/10 11:22:37	Untrust	Untrust	49.228.231....	49.0.116.142	56555	4443	6	ssl	intrazon... default	ethernet1/1	ethernet1/1	1290	vsys1	<input checked="" type="checkbox"/>
[+]	09/10 11:21:26	Untrust	Untrust	175.178.10...	49.0.116.142	57990	6379	6	undecided	intrazon... default	ethernet1/1	ethernet1/1	74	vsys1	<input checked="" type="checkbox"/>
[+]	09/10 11:20:38	Untrust	Untrust	49.228.231....	49.0.116.142	56537	4443	6	ssl	intrazon... default	ethernet1/1	ethernet1/1	55990	vsys1	<input checked="" type="checkbox"/>
[+]	09/10 11:22:28	Trust	Untrust	10.252.112....	8.8.8.8	45134	53	17	dns-base	trust to untrust	ethernet1/2	ethernet1/1	190	vsys1	<input checked="" type="checkbox"/>
[+]	09/10 11:21:39	Untrust	Untrust	192.241.20...	49.0.116.142	39424	1830	6	undecided	intrazon... default	ethernet1/1	ethernet1/1	60	vsys1	<input checked="" type="checkbox"/>
[+]	09/10 11:22:39	Untrust	Untrust	49.228.231....	49.0.116.142	56565	4443	6	ssl	intrazon... default	ethernet1/1	ethernet1/1	7175	vsys1	<input checked="" type="checkbox"/>
[+]	09/10 11:21:55	Untrust	Untrust	113.200.98....	49.0.116.142	45917	8088	6	undecided	intrazon... default	ethernet1/1	ethernet1/1	60	vsys1	<input checked="" type="checkbox"/>
[+]	09/10 11:21:16	Untrust	Untrust	49.0.116.142	34.111.40.29	42645	443	6	pan-db-cloud	intrazon... default	ethernet1/1	ethernet1/1	86932	vsys1	<input checked="" type="checkbox"/>
[+]	09/10 11:22:39	Untrust	Untrust	49.228.231...	49.0.116.142	56562	1112	4	ssl	intrazon...	ethernet1/1	ethernet1/1	74660	vsys1	<input checked="" type="checkbox"/>

Page 1 of 1 Displaying 1 - 48 of 48

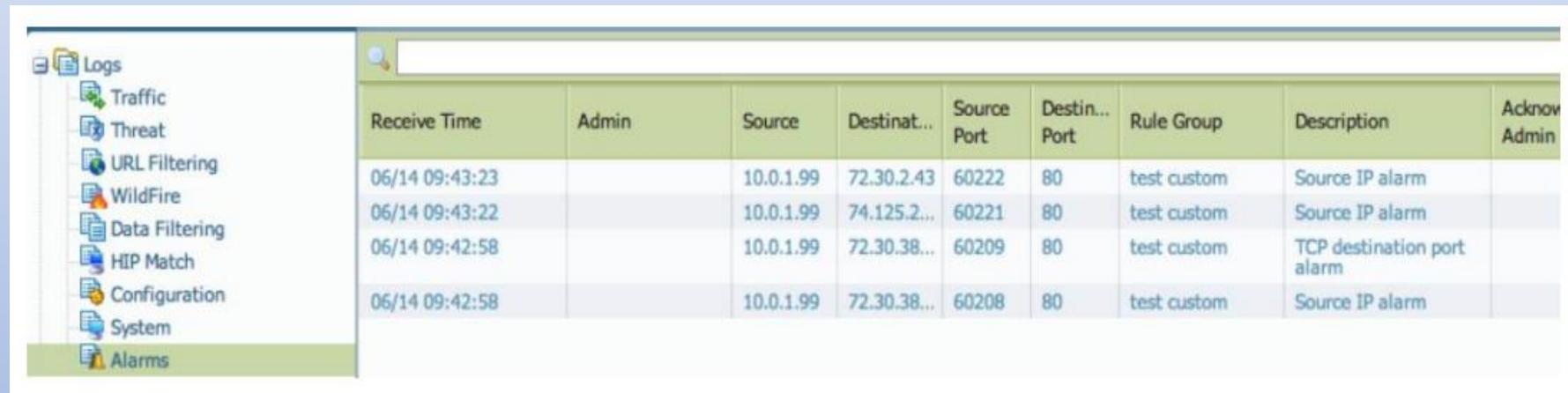
Logging

Log Types

- Traffic Logs
 - Traffic allowed or denied by Security Policies
- Threat Log
 - Threats blocked by Security Profiles
- URL Filtering
- WildFire Submissions
- Data Filtering
 - Sensitive data filtered from going out and file blocking
- HIP Match
- Configuration
- System
- Alarms

Alarms

- Logs specific events
 - For example: Log DB growing too large,
Encryption/Decryption errors, too many denies for a specific IP address
- Alarm generation be enabled is Device > Log Settings > Alarms

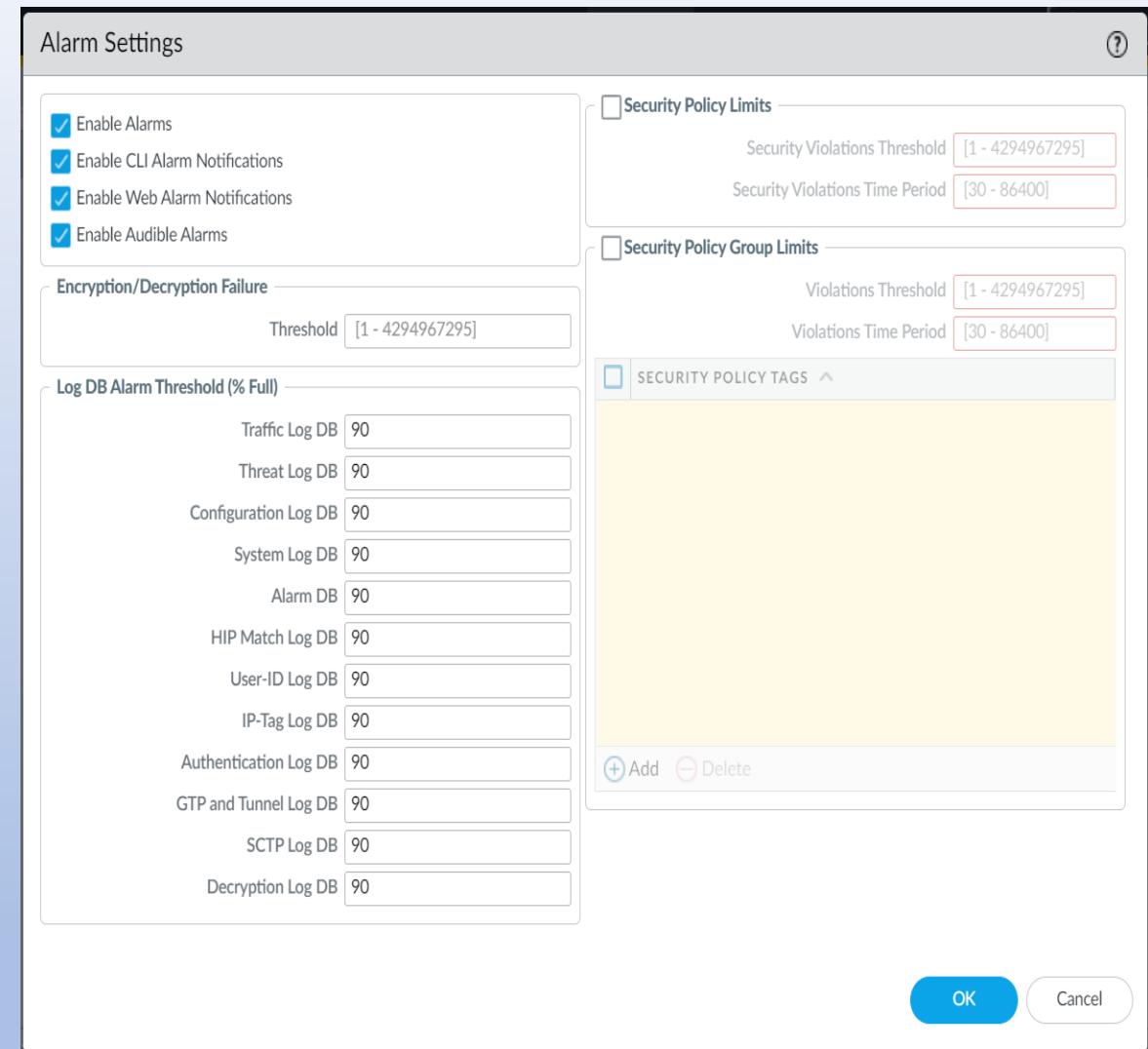


The screenshot shows the 'Logs' section of the Palo Alto Firewall configuration interface. The 'Alarms' category is selected, highlighted with a green background. The main area displays a table of alarm logs.

Receive Time	Admin	Source	Destinat...	Source Port	Destin... Port	Rule Group	Description	Acknow Admin
06/14 09:43:23		10.0.1.99	72.30.2.43	60222	80	test custom	Source IP alarm	
06/14 09:43:22		10.0.1.99	74.125.2...	60221	80	test custom	Source IP alarm	
06/14 09:42:58		10.0.1.99	72.30.38...	60209	80	test custom	TCP destination port alarm	
06/14 09:42:58		10.0.1.99	72.30.38...	60208	80	test custom	Source IP alarm	

Enabling Alarm Settings

- Enable Alarms
- CLI Alarm Notification
- Web Alarm Notification
 - Will make alarms pop up in Web interface
- Audible Alarms
 - Will play sound until the alarms are acknowledged



Viewing and Filtering Logs

Constructing a Log Filter

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE Commit Manual

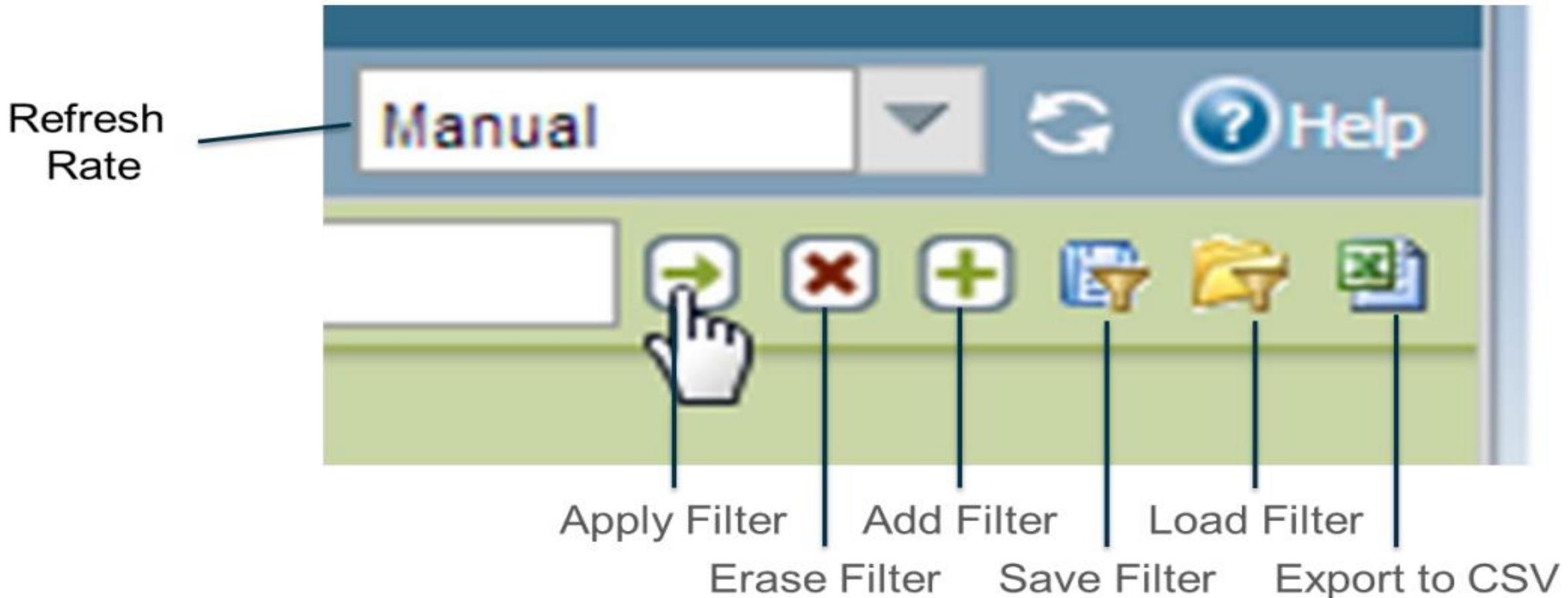
Logs

- Traffic
- Threat
- URL Filtering
- WildFire Submissions
- Data Filtering
- HIP Match
- GlobalProtect
- IP-Tag
- User-ID
- Decryption
- Tunnel Inspection
- Configuration
- System
- Alarms
- Authentication
- Unified
- Packet Capture
- App Scope
- Summary
- Change Monitor
- Threat Monitor
- Threat Map
- Network Monitor
- Traffic Map
- Session Browser
- Botnet

(addr.src in '10.250.250.3')

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION
[Search]	09/10 11:36:21	end	SGL	Untrust	10.250.250.3			208.91.112.61			123	ntp-ba
[Search]	09/10 11:36:21	end	SGL	Untrust	10.250.250.3			208.91.112.63			123	ntp-ba
[Search]	09/10 11:34:16	end	SGL	Untrust	10.250.250.3			208.91.112.61			123	ntp-ba
[Search]	09/10 11:34:16	end	SGL	Untrust	10.250.250.3			208.91.112.63			123	ntp-ba
[Search]	09/10 11:32:11	end	SGL	Untrust	10.250.250.3			208.91.112.61			123	ntp-ba
[Search]	09/10 11:32:11	end	SGL	Untrust	10.250.250.3			208.91.112.63			123	ntp-ba
[Search]	09/10 11:30:06	end	SGL	Untrust	10.250.250.3			208.91.112.61			123	ntp-ba
[Search]	09/10 11:30:06	end	SGL	Untrust	10.250.250.3			208.91.112.63			123	ntp-ba
[Search]	09/10 11:28:01	end	SGL	Untrust	10.250.250.3			208.91.112.61			123	ntp-ba
[Search]	09/10 11:28:01	end	SGL	Untrust	10.250.250.3			208.91.112.63			123	ntp-ba
[Search]	09/10 11:25:56	end	SGL	Untrust	10.250.250.3			208.91.112.61			123	ntp-ba
[Search]	09/10 11:25:56	end	SGL	Untrust	10.250.250.3			208.91.112.63			123	ntp-ba
[Search]	09/10 11:23:51	end	SGL	Untrust	10.250.250.3			208.91.112.61			123	ntp-ba
[Search]	09/10 11:23:51	end	SGL	Untrust	10.250.250.3			208.91.112.63			123	ntp-ba
[Search]	09/10 11:21:46	end	SGL	Untrust	10.250.250.3			208.91.112.61			123	ntp-ba
[Search]	09/10 11:21:46	end	SGL	Untrust	10.250.250.3			208.91.112.63			123	ntp-ba
[Search]	09/10 11:19:41	end	SGL	Untrust	10.250.250.3			208.91.112.61			123	ntp-ba

Filter Buttons



Reports

Reports

- Predefined Reports
 - Over 40 reports including Applications, Traffic, Threat, and URL Filtering
- Custom Reports
 - With Query Builder
- User or Group Activity Reports
 - Including URL categories and browse time calculations
- Botnet Reports
 - Behavior-based mechanisms to identify potential infected hosts
- PDF Summary Reports
 - Aggregate reports
- Report Groups
 - Compile reports into a single emailed PDF

Custom Reports

Custom Report

Report Setting

Load Template → Run Now

Name: untitled

Description:

Database: Application Statistics

Scheduled

Time Frame: Last 24 Hrs

Sort By: Bytes

Group By: App Category

Available Columns

- App Category
- Device SN
- Hour
- Packets
- Quarter Hour

Selected Columns

- App Container
- App Technology
- Day
- App Sub Category
- Application Name

Top Up Down Bottom

Query Builder

Please type (or) add a filter using the filter builder

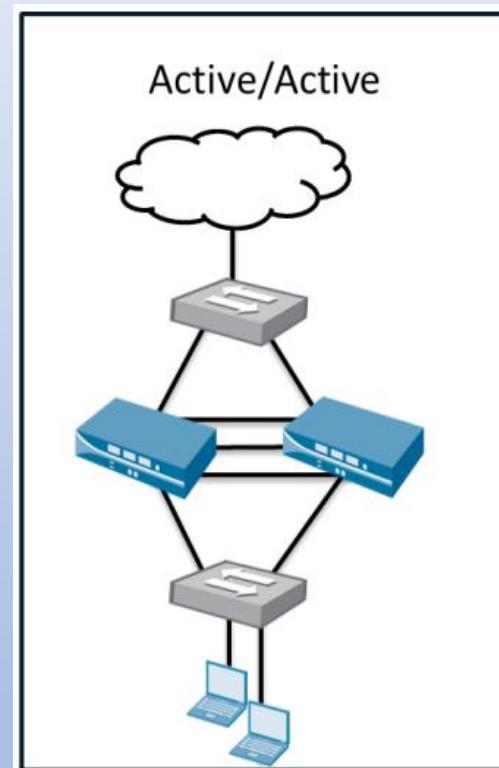
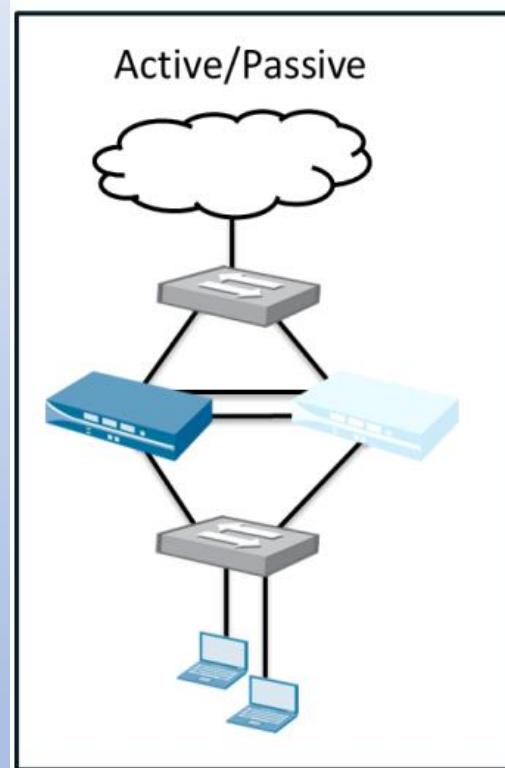
Filter Builder

If using Headers Inserted field, then Report will contain truncated header values

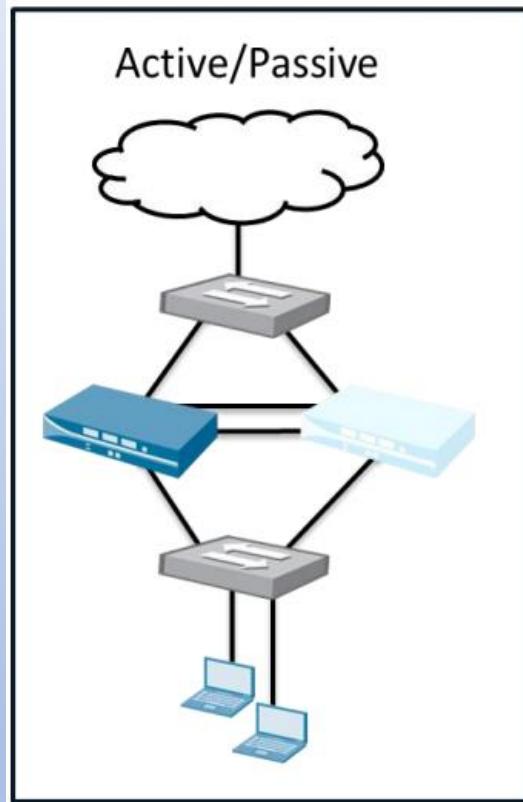
OK Cancel

High Availability (HA) Overview

High Availability (HA)



Active/Passive Overview

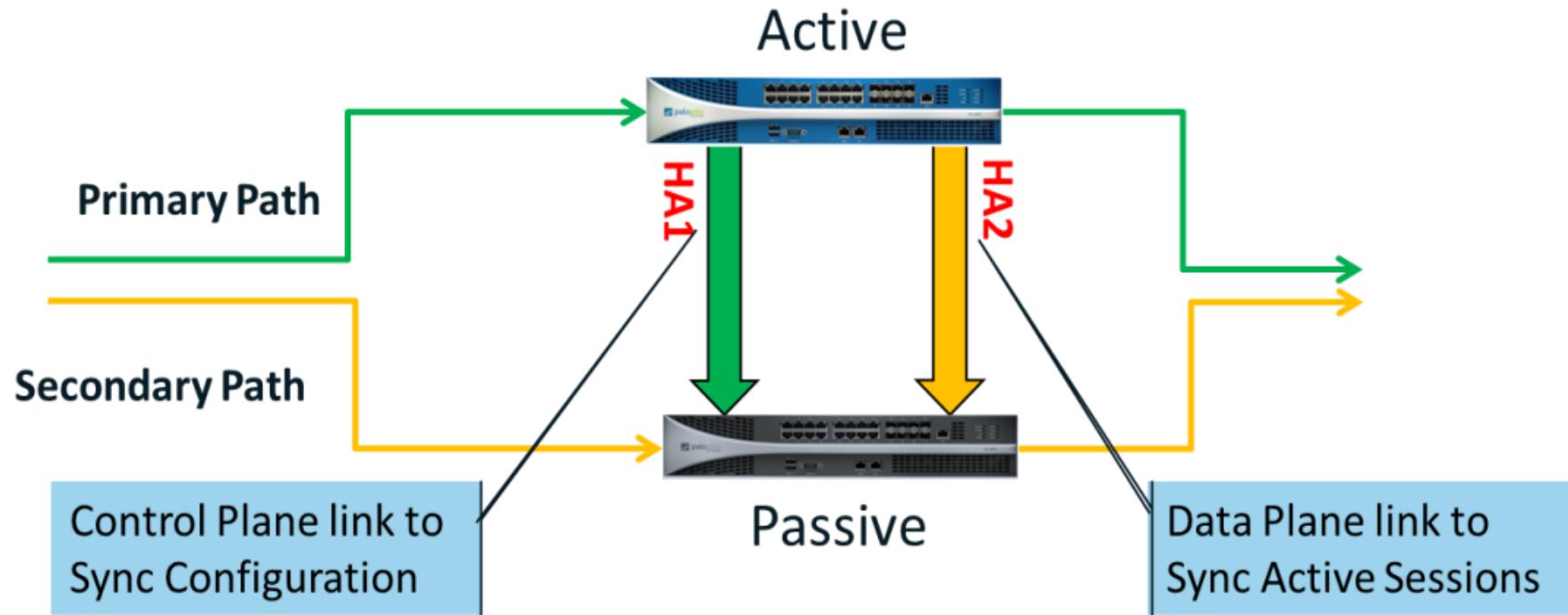


Supported Modes:

- Layer 2, Layer 3, Virtual Wire Synchronization of:
- Stateful connections
- Certificates
- Response Pages
- Configuration Not Synchronized:
- State-less connections, HA configuration

Active/Passive HA Links

HA is configured between exactly two firewalls



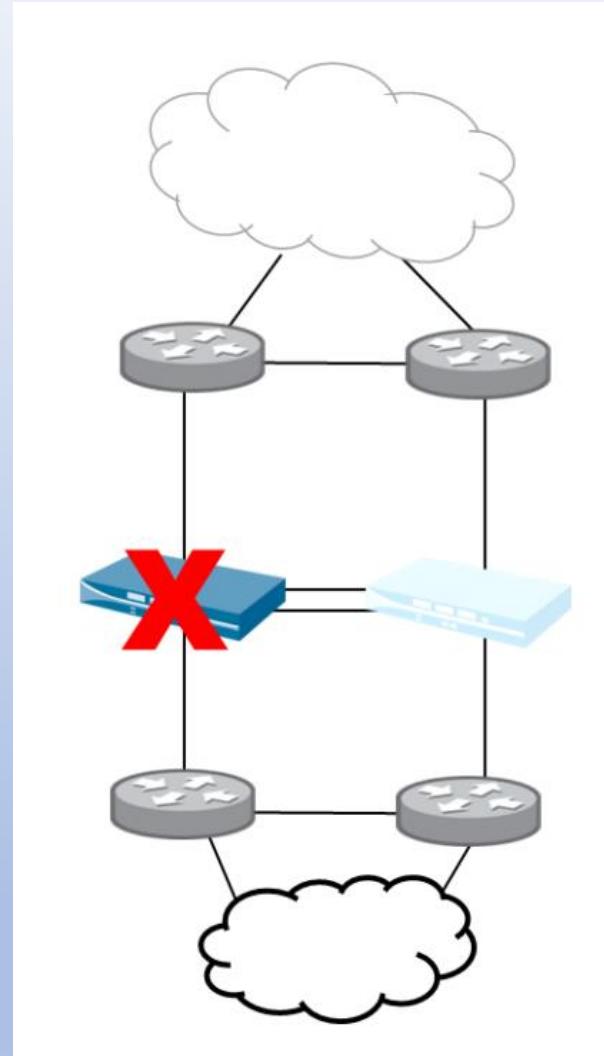
Device States

High Availability	
Mode	Active-Passive
Local	● passive
Peer (10.30.11.76)	● active
Running Config	● not synchronized Sync to peer 
App Version	● Match
Threat Version	● Match
Antivirus Version	● Match
PAN-OS Version	● Match
GlobalProtect Version	● Match
HA1	● up
Heart Beat Backup	● up

- Initial
- Active
- Passive
- Suspend
- Non-Functional
- Unknown

Device States

- Heartbeat Polling
- Path Monitoring
- Link Monitoring

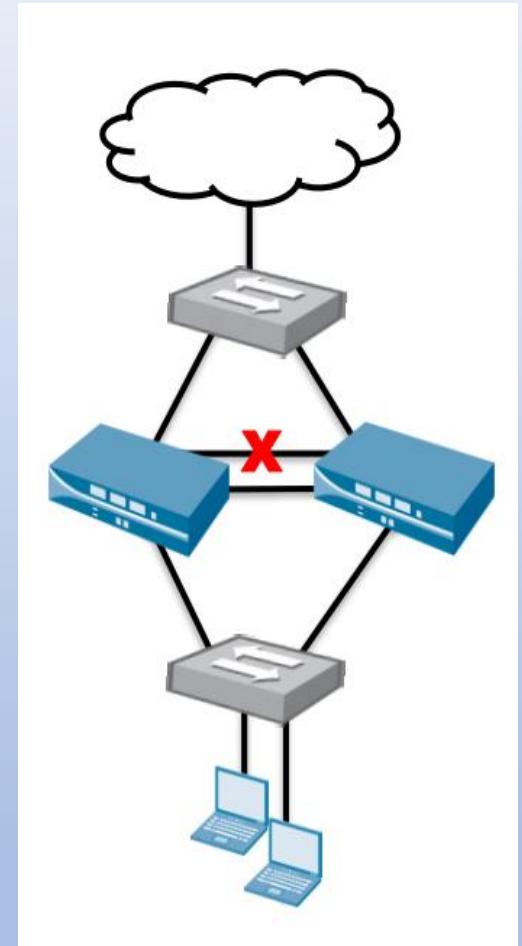


Split Brain

“Split Brain”: When both firewalls attempt to enter the Active state.

If the Passive device loses connection to the Active device, it cannot distinguish between a down peer device and a communication problem.

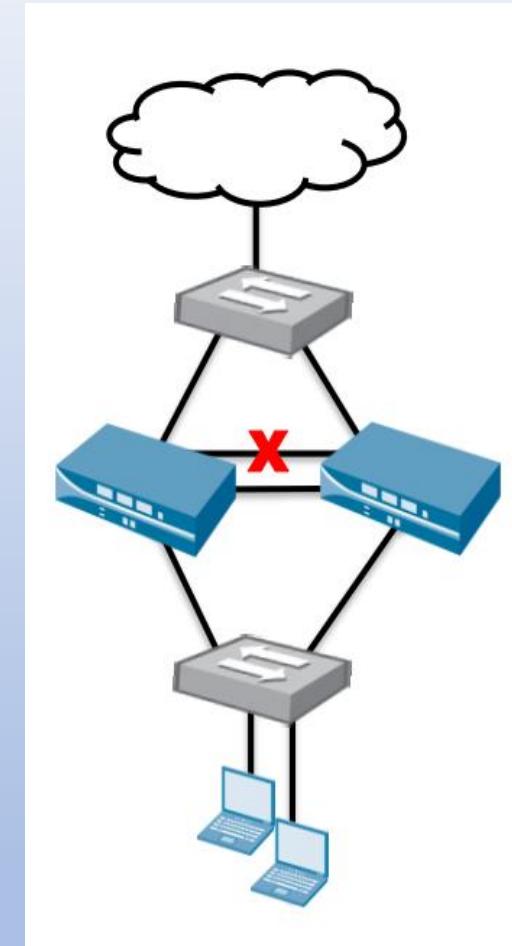
If the Active device loses connection to the Passive device, path and link monitoring will not be honored as the Active device doesn't know that the peer will take over.



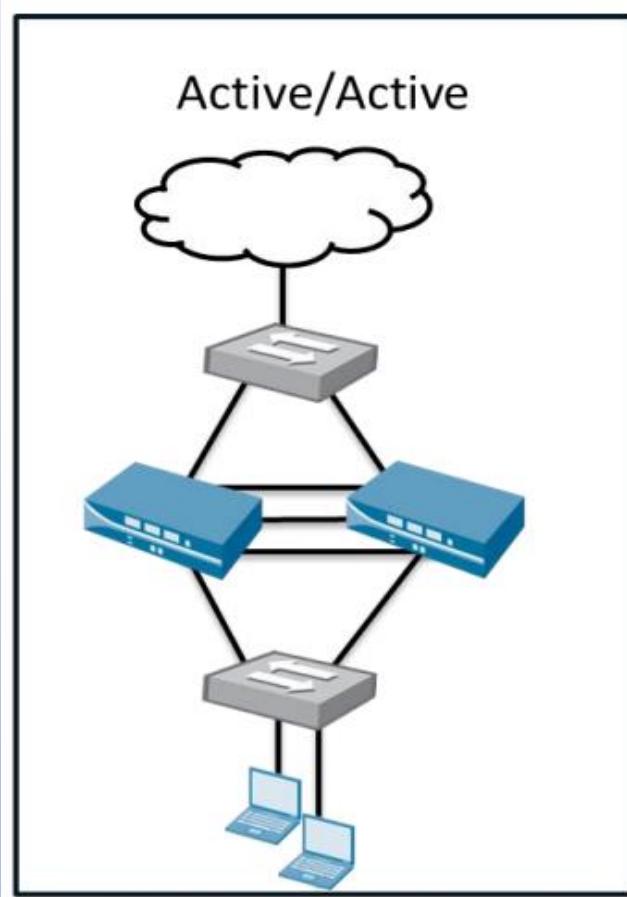
Split Brain Solutions

Enable Heartbeat Backup Use the Management (MGT) interface as a non-dedicated reduced functionality secondary HA control link

The Management Interface IP address is sent to the HA peer over the HA1 interface when both devices are running



Active/Active Introduction



Devices back each other up, taking over primary ownership

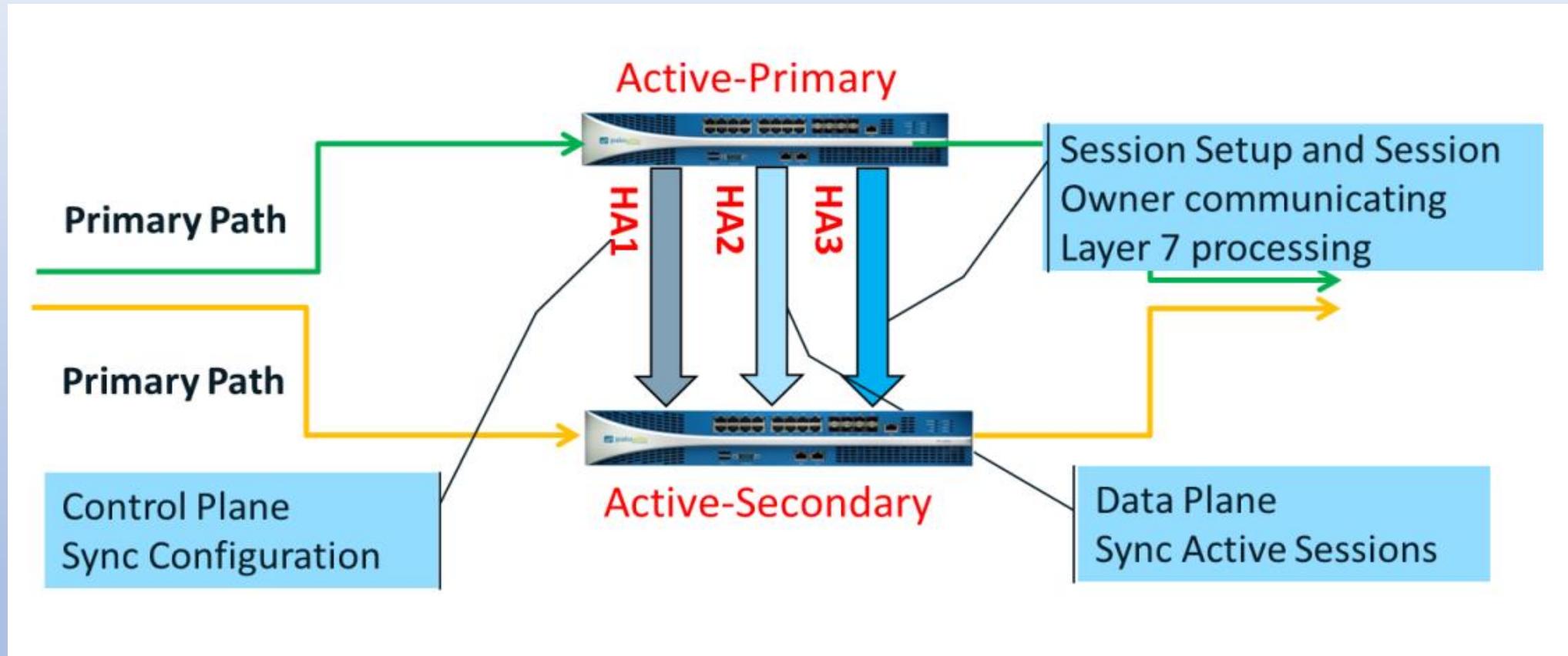
Both devices in the cluster are:

- Actively processing and passing traffic
- Load-sharing the traffic

No increase in session capacity

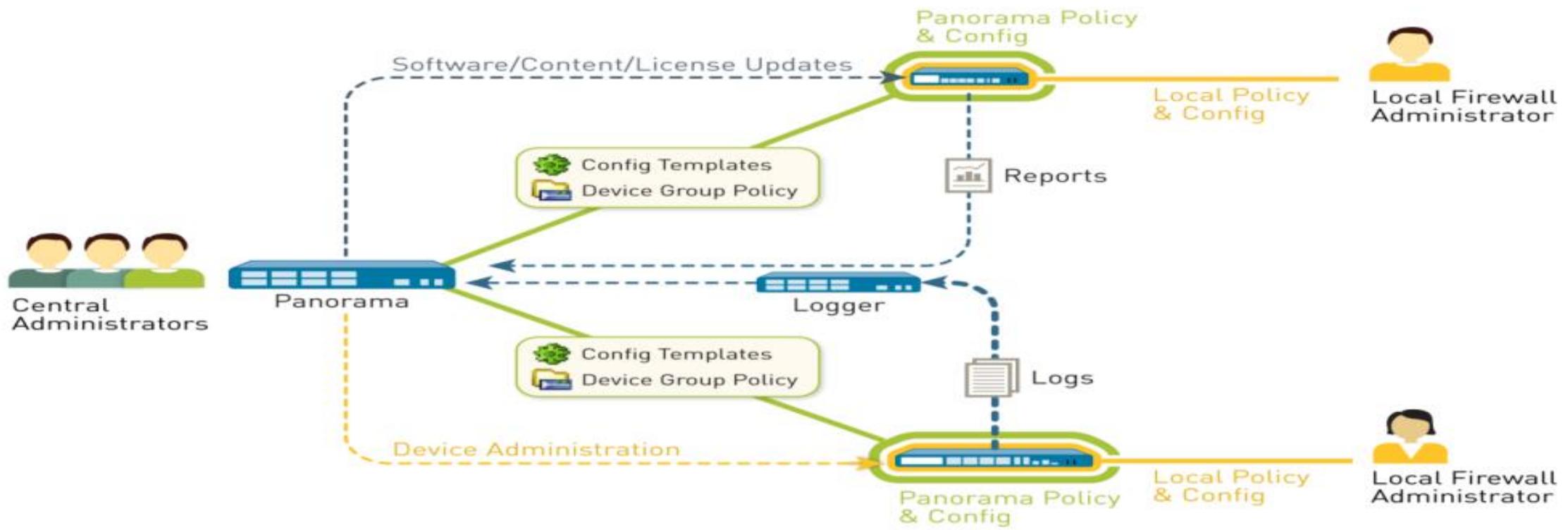
Not designed to increase throughput

Active/Active Links



Panorama

Panorama Benefits



- Centralized configuration and deployment
- Aggregated logging with central oversight for analysis and reporting
- Distributed administration

Panorama Platforms



Installed on VMware, Amazon AWS or KVM

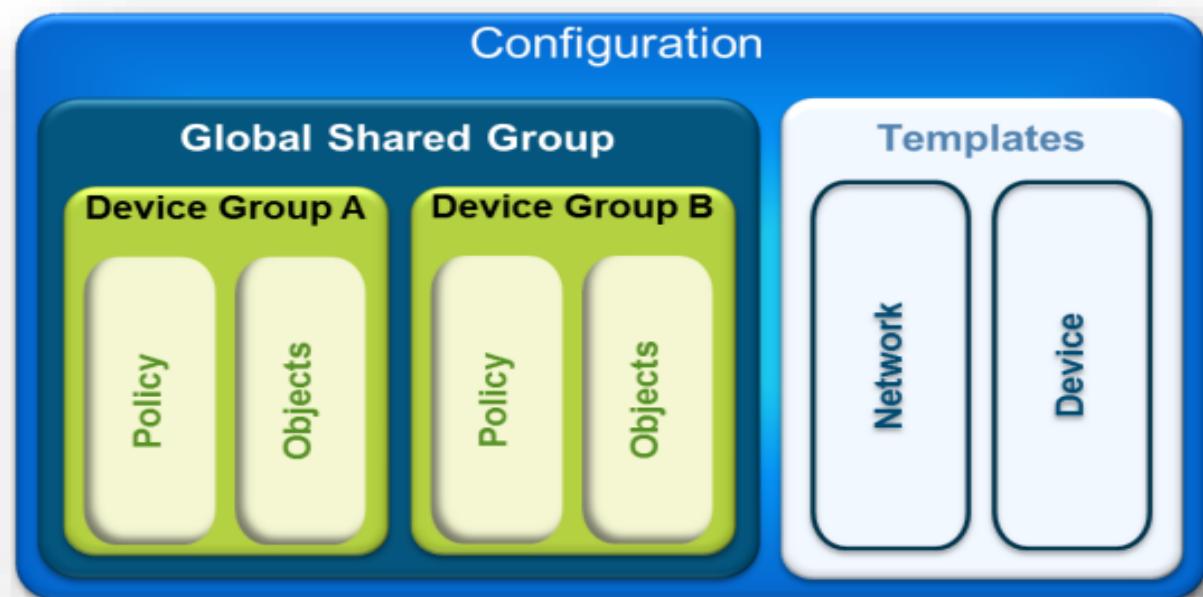
- Allows for a tailored hardware and operating system
- Supports fewer than 10 firewalls and log-rates less than 10,000 logs/second



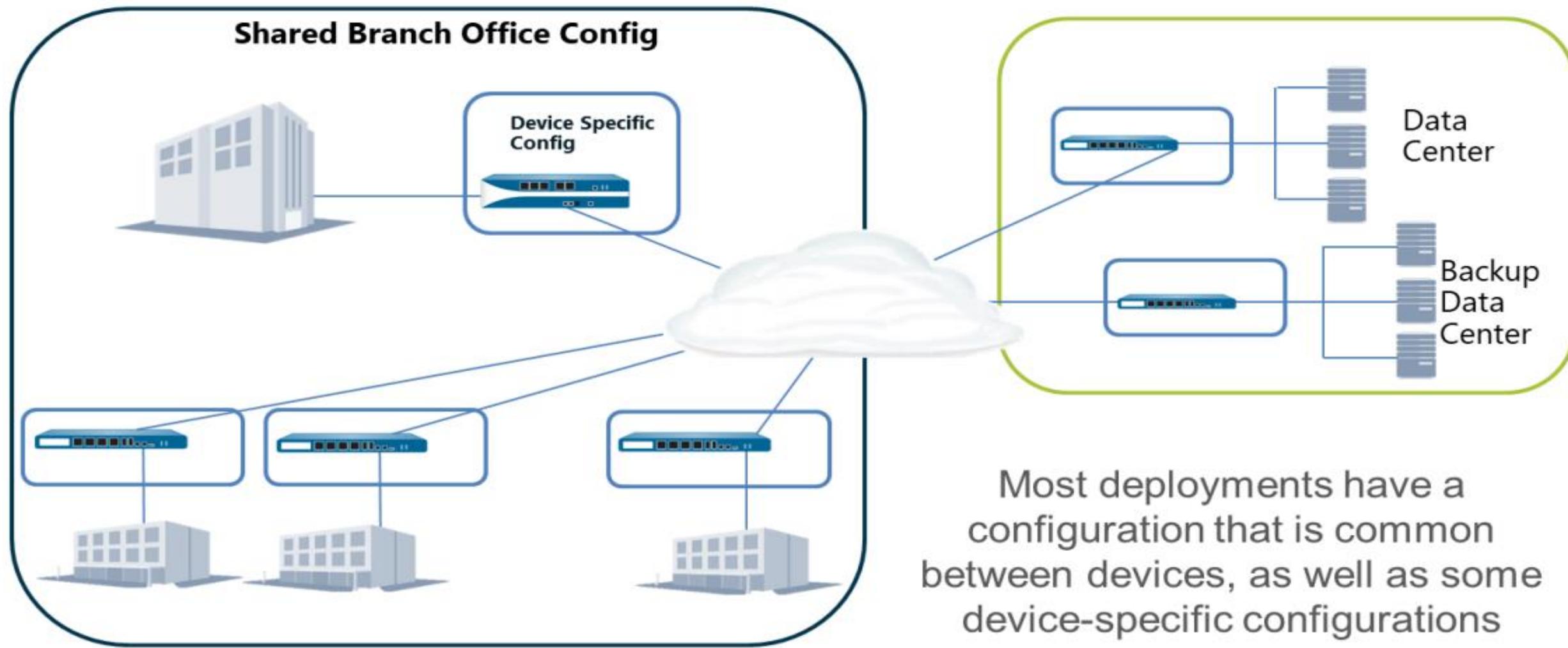
- Supports up to 100 firewalls and 10,000 logs/sec
- Can be put into distributed log architecture with dedicated Log Collectors
 - Up to 1000 firewalls
 - > 10,000 logs/sec (Max)
(Max 50,000 logs/sec per collector)

Centralized Configuration and Deployment

- Device Groups
 - Group together firewalls that require similar configurations
 - Manage Shared Policies and Shared Objects
- Templates
 - Define Network and Device base configurations
 - Push the base config to firewalls



Device Groups Example: Functional/Boundary



Device Group Policies

Policies can be created on Panorama and then pushed to Device Groups

- Panorama rules cannot be edited on firewall once pushed
- Policies are specified as either Pre-rules or Post-Rules

Name	Source			Destination			Service	Action
	Zone	Address	User	Zone	Address	Application		
Shared-Corp-Policy-1	Trust-L3	any	any	Untrust-L3	any	facebook	application-default	
DG01-Box-Deny	Trust-L3	any	any	Untrust-L3	any	boxnet	any	
Allow-WebBrowsing	Trust-L3	any	any	Untrust-L3	any	web-browsing	any	
Known_Good	any	any	any	any	any	Known-Good	any	
Known-Bad	Trust-L3	any	any	Untrust-L3	any	Known-Bad	any	
Corp-Cleanup-Policy	Trust-L3	any	any	Untrust-L3	any	any	any	

