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-Polices

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

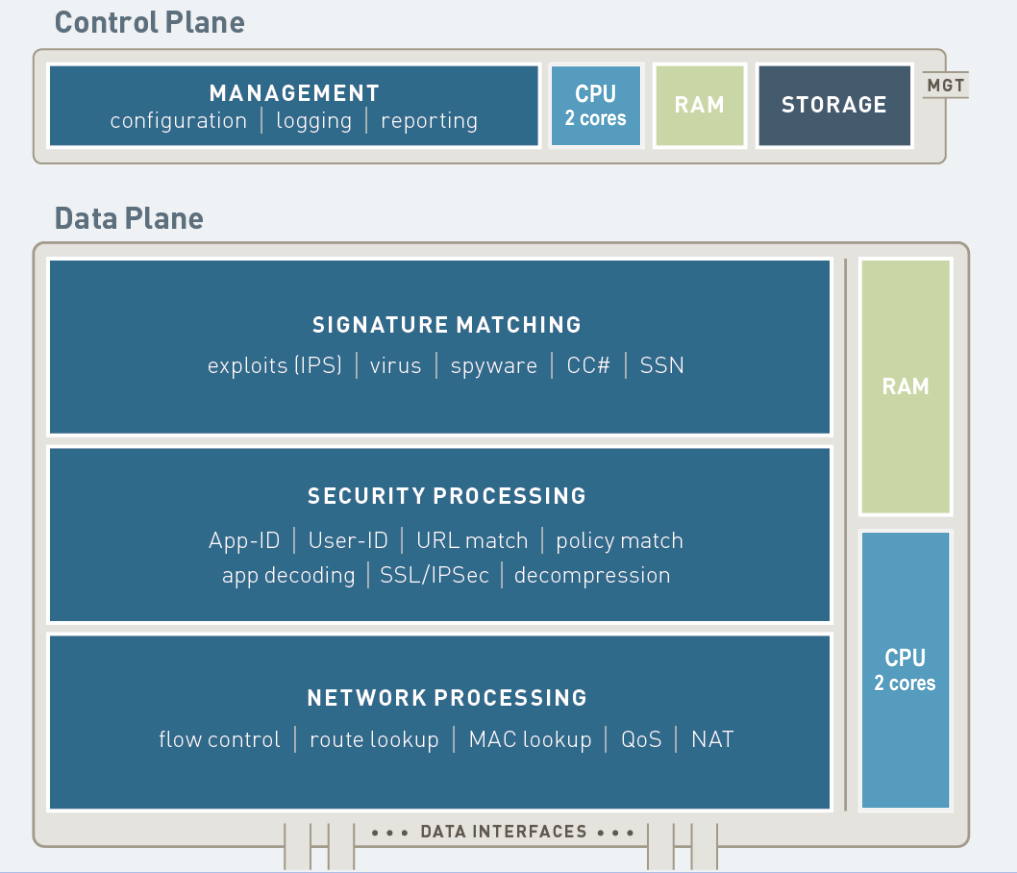
- 940Mbps FW throughput
- 610Mbps threat prevention
- 128K sessions
- 4 - 1G - copper
  8 - 1G - fiber SFP
- 30 security zones
- 5,000 policy rules*

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*

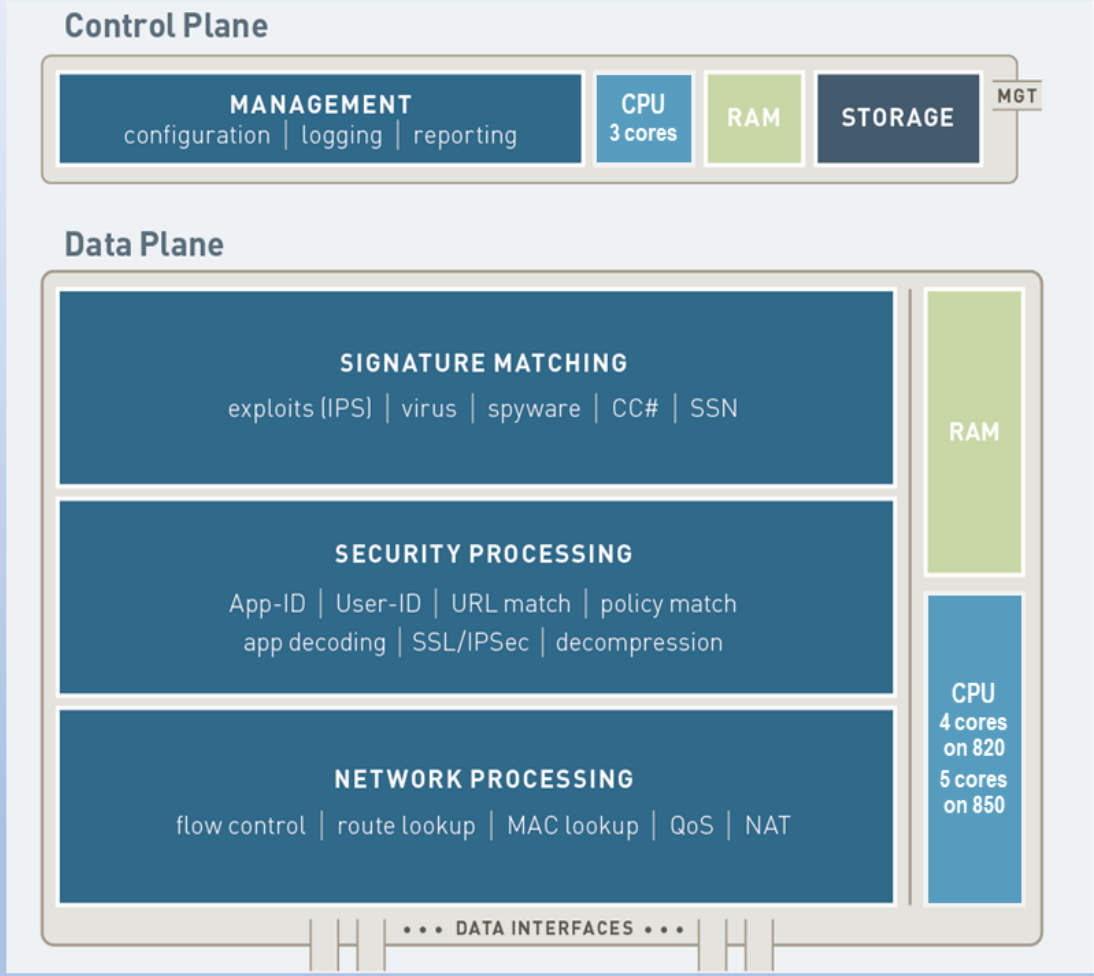
*Maximum capacity of the routing forwarding table per IP version. IPv4 + IPv6 = 2x number of rules.

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*

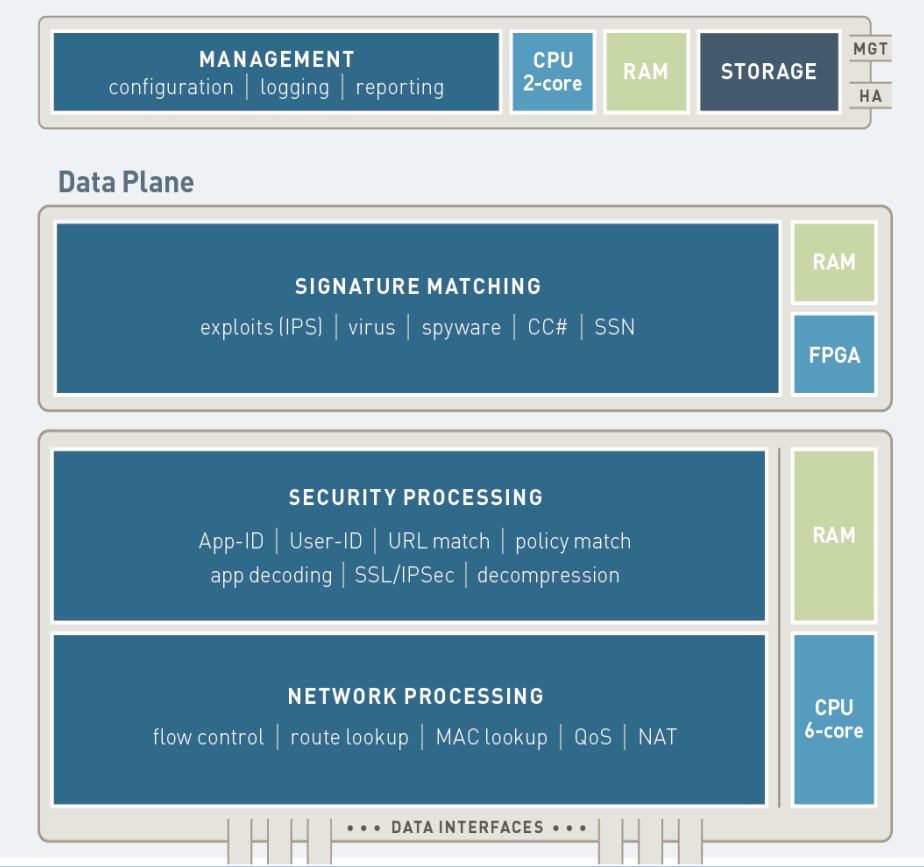
PA-3060

- 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*

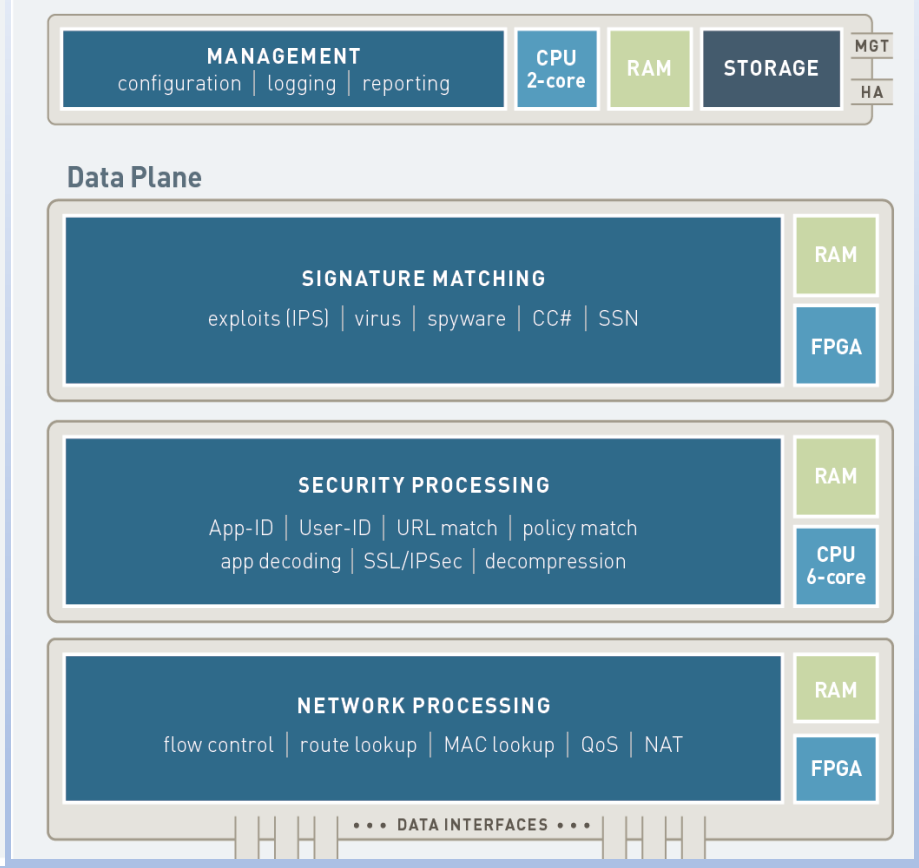
*Maximum capacity of the routing forwarding table per IP version. IPv4 + IPv6 = 2x number of rules.

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

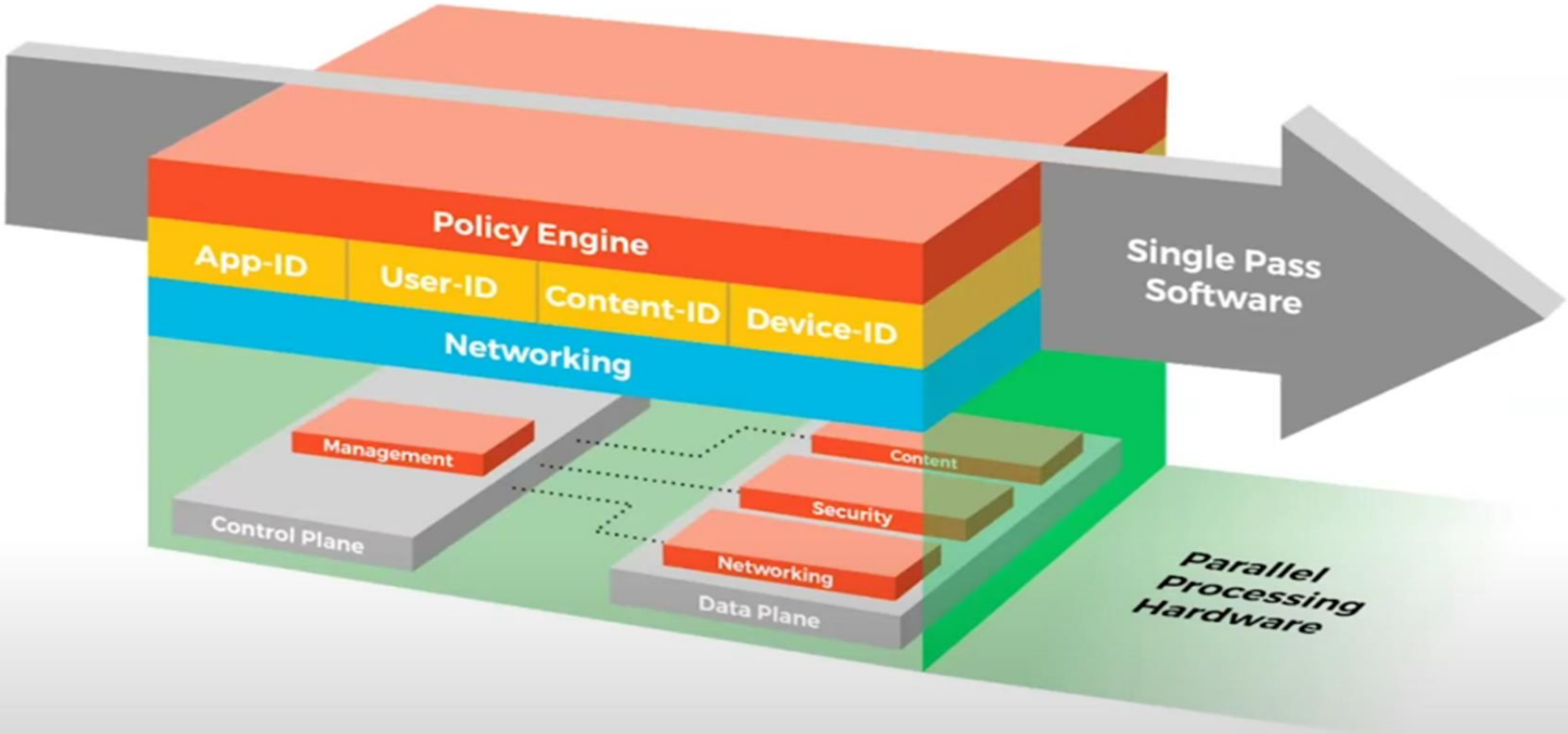
VM-500

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

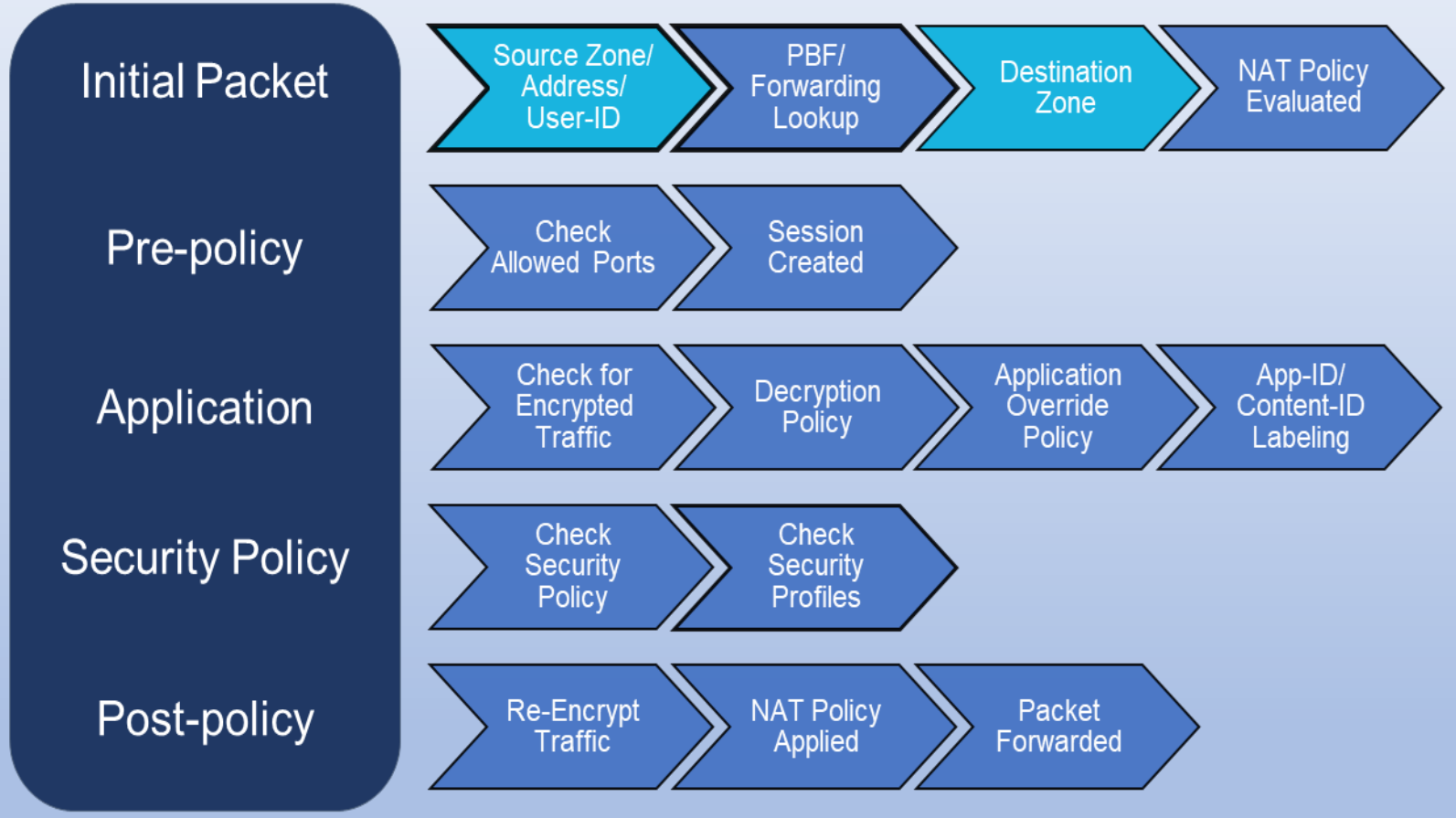
VM-700

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

* Maximum capacity of the routing forwarding table.


Policy Engine
App-ID
User-ID
Content-ID
Device-ID
Networking
Single Pass Software
Management
Control Plane
Content
Security
Networking
Data Plane
Parallel Processing Hardware

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:

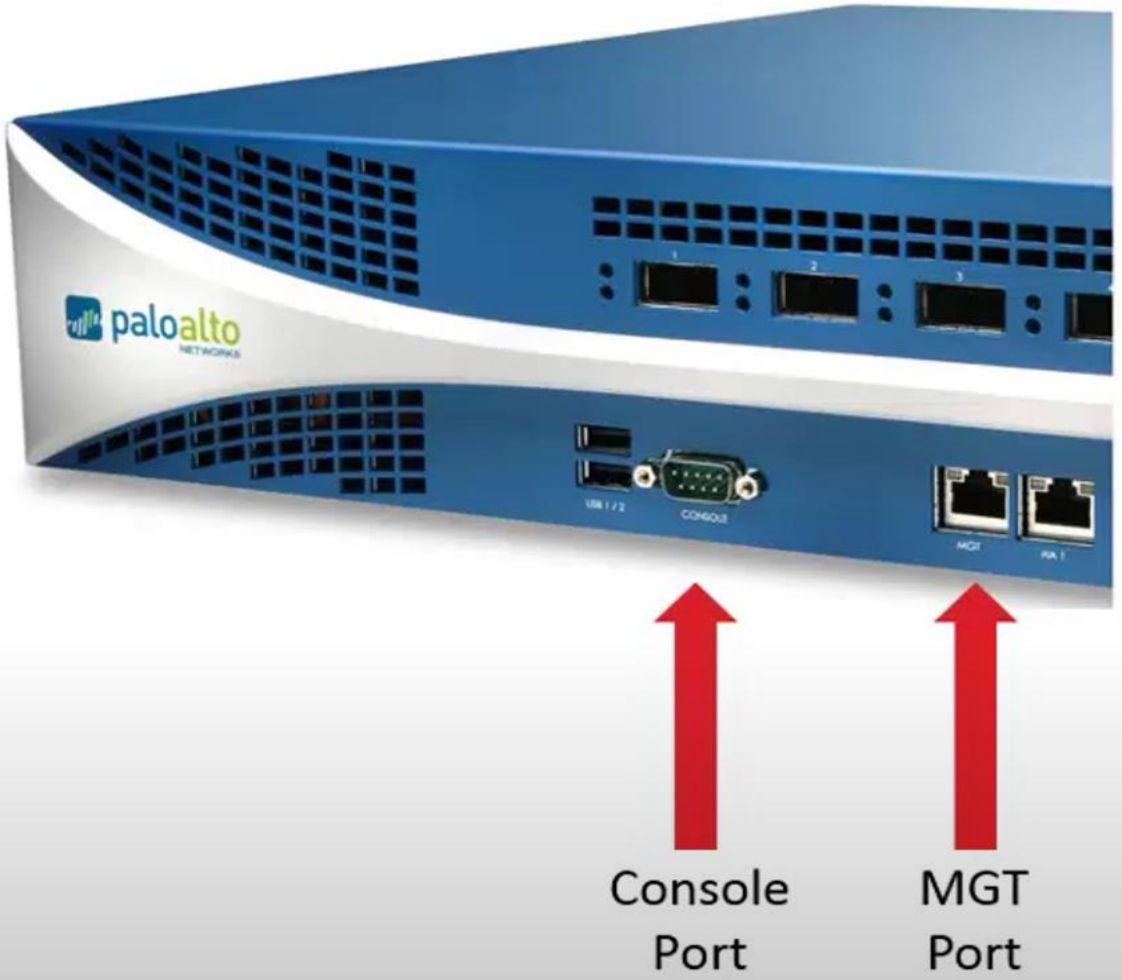
- MGT port has a factory default IP address of 192.168.1.1
- VM-Series MGT port is configured as a DHCP client.

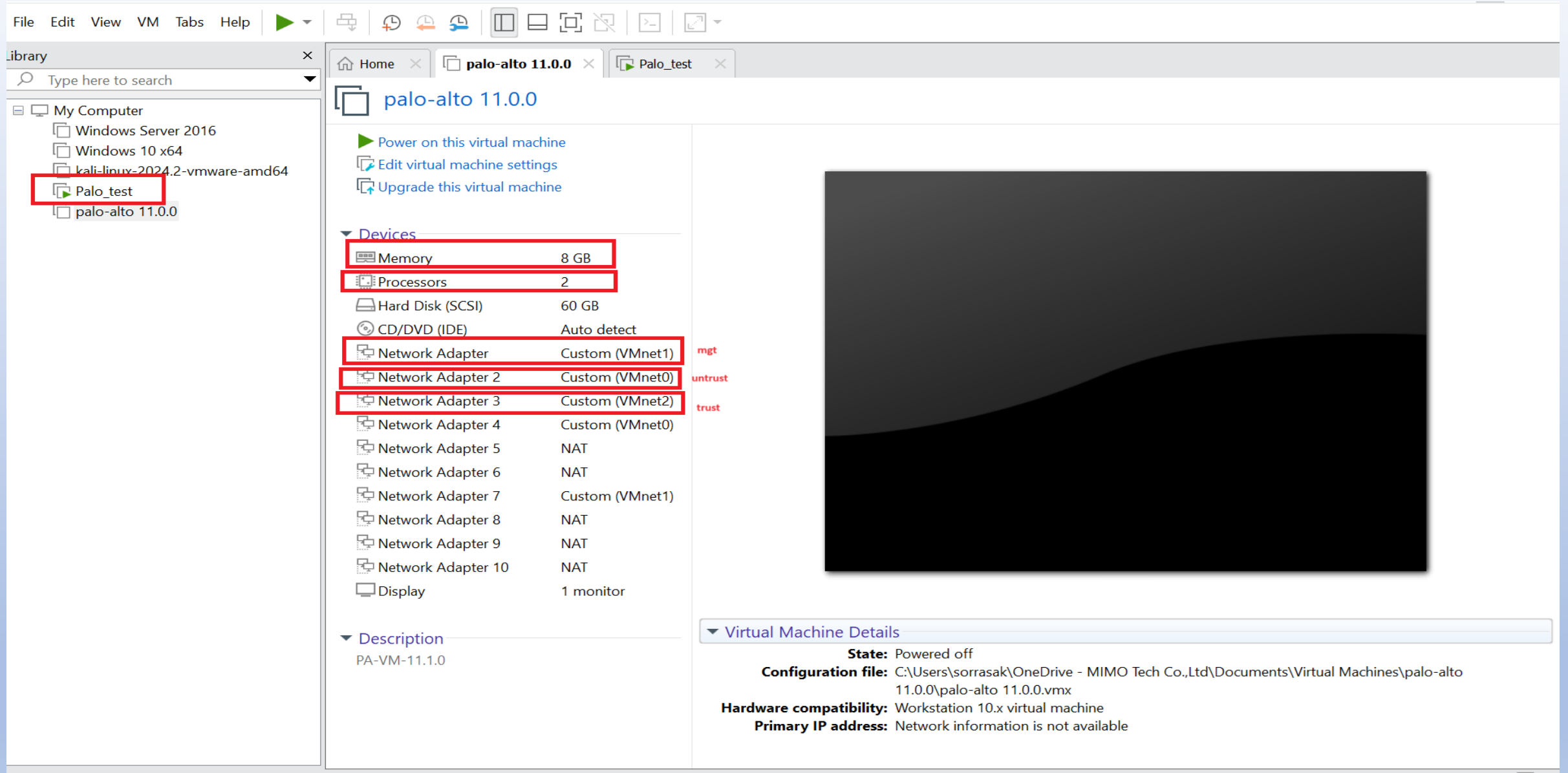
Factory default single administrative account

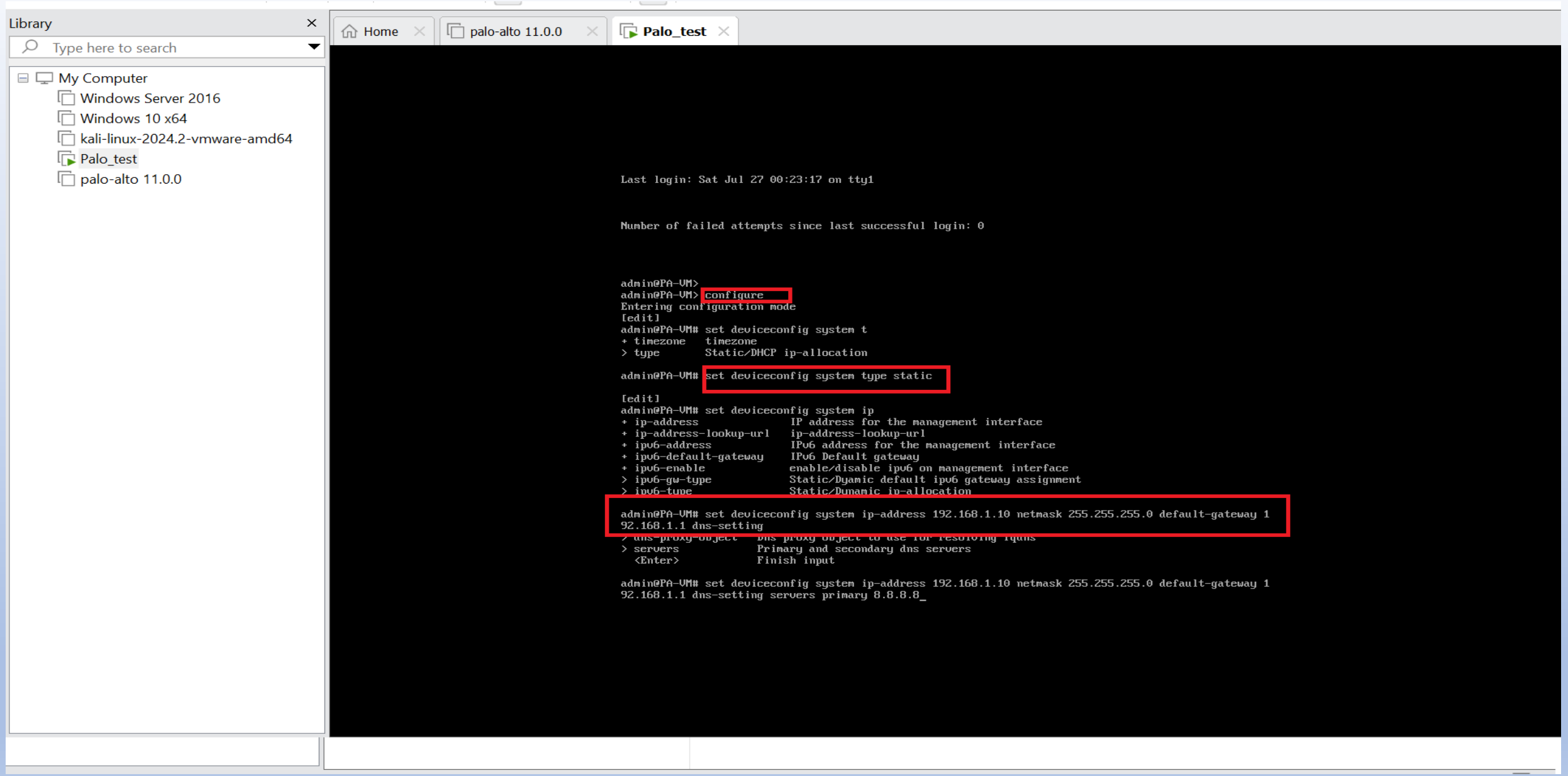
- Username: admin
- Password: admin

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

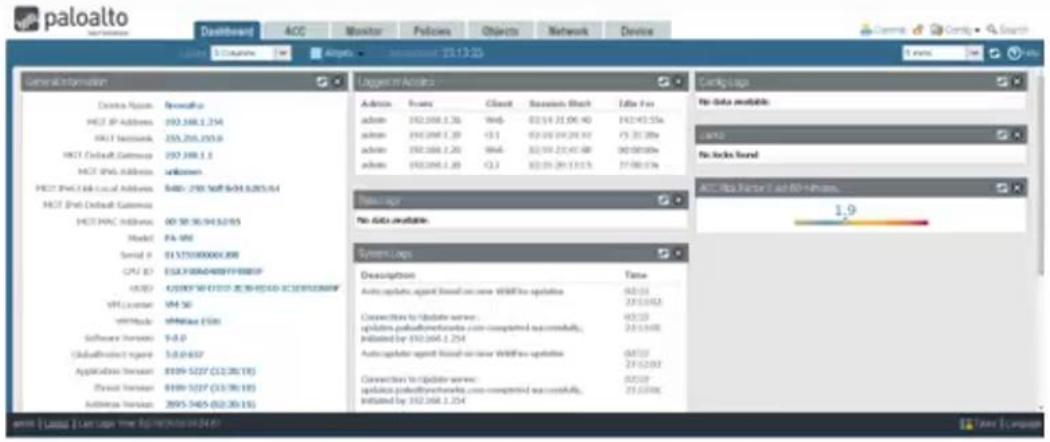
Local admin password is encrypted using the firewall's master key.




File Edit View VM Tabs Help
Library
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
Home
palo-alto 11.0.0
Palo_test
palo-alto 11.0.0
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices
Memory 8 GB
Processors 2
Hard Disk (SCSI) 60 GB
CD/DVD (IDE) Auto detect
Network Adapter Custom (VMnet1)
Network Adapter 2 Custom (VMnet0)
Network Adapter 3 Custom (VMnet2)
Network Adapter 4 Custom (VMnet0)
Network Adapter 5 NAT
Network Adapter 6 NAT
Network Adapter 7 Custom (VMnet1)
Network Adapter 8 NAT
Network Adapter 9 NAT
Network Adapter 10 NAT
Display 1 monitor
mgt
untrust
trust
Description
PA-VM-11.1.0
Virtual Machine Details
State: Powered off
Configuration file: C:\Users\sorrasak\OneDrive - MIMO Tech Co.,Ltd\Documents\Virtual Machines\palo-alto 11.0.0\palo-alto 11.0.0.vmx
Hardware compatibility: Workstation 10.x virtual machine
Primary IP address: Network information is not available

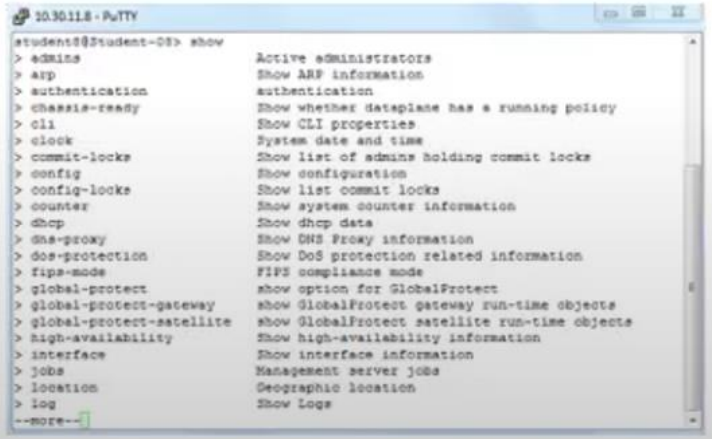

Library
Type here to search
My Computer
Windows Server 2016
Windows 10 x64
kali-linux-2024.2-vmware-amd64
Palo_test
palo-alto 11.0.0
Home
palo-alto 11.0.0
Palo_test
Last login: Sat Jul 27 00:23:17 on tty1
Number of failed attempts since last successful login: 0
admin@PA-VM>
admin@PA-VM> configure
Entering 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/Dyamic 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
> 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



Web Interface

Panorama



SSH/Console CLI

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

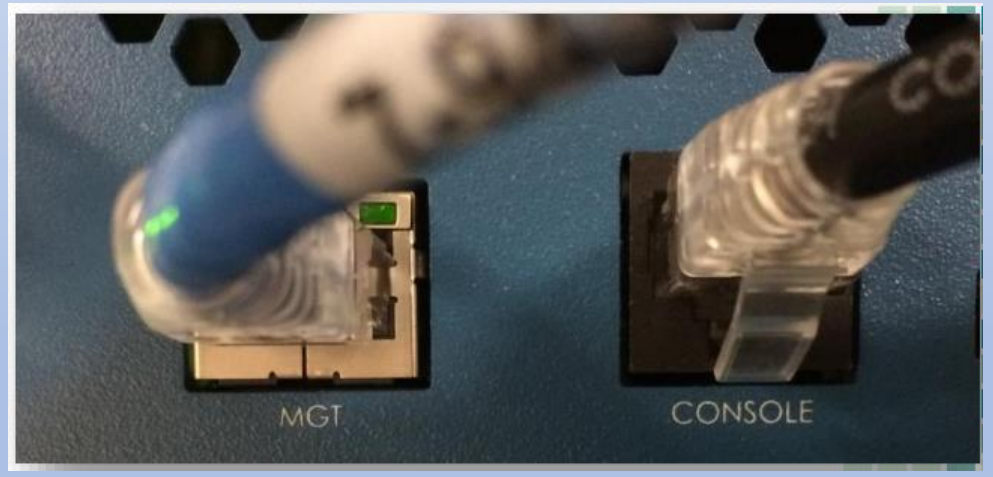
REST XML API

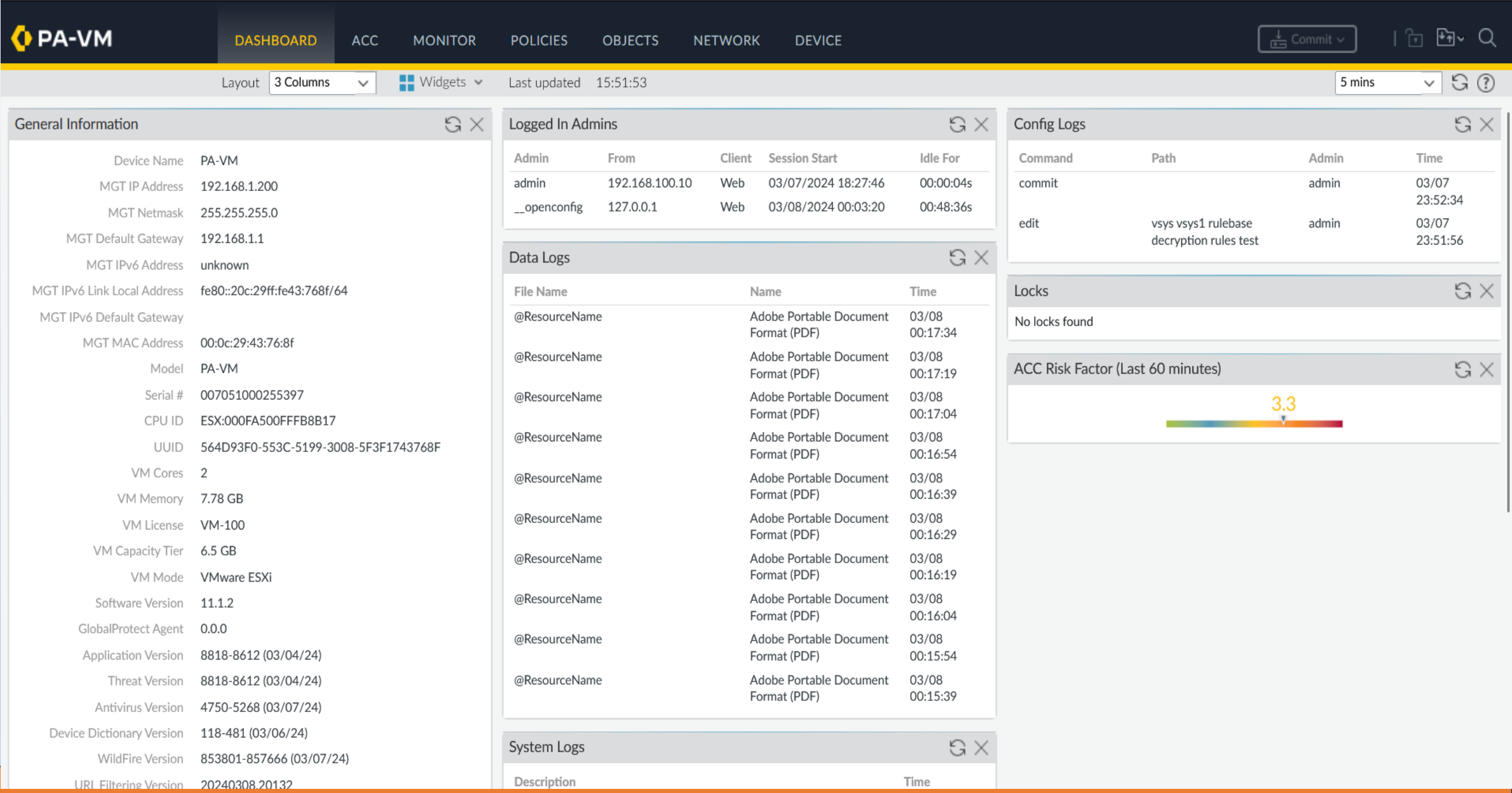
Configuring the MGT Interface – CLI

>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

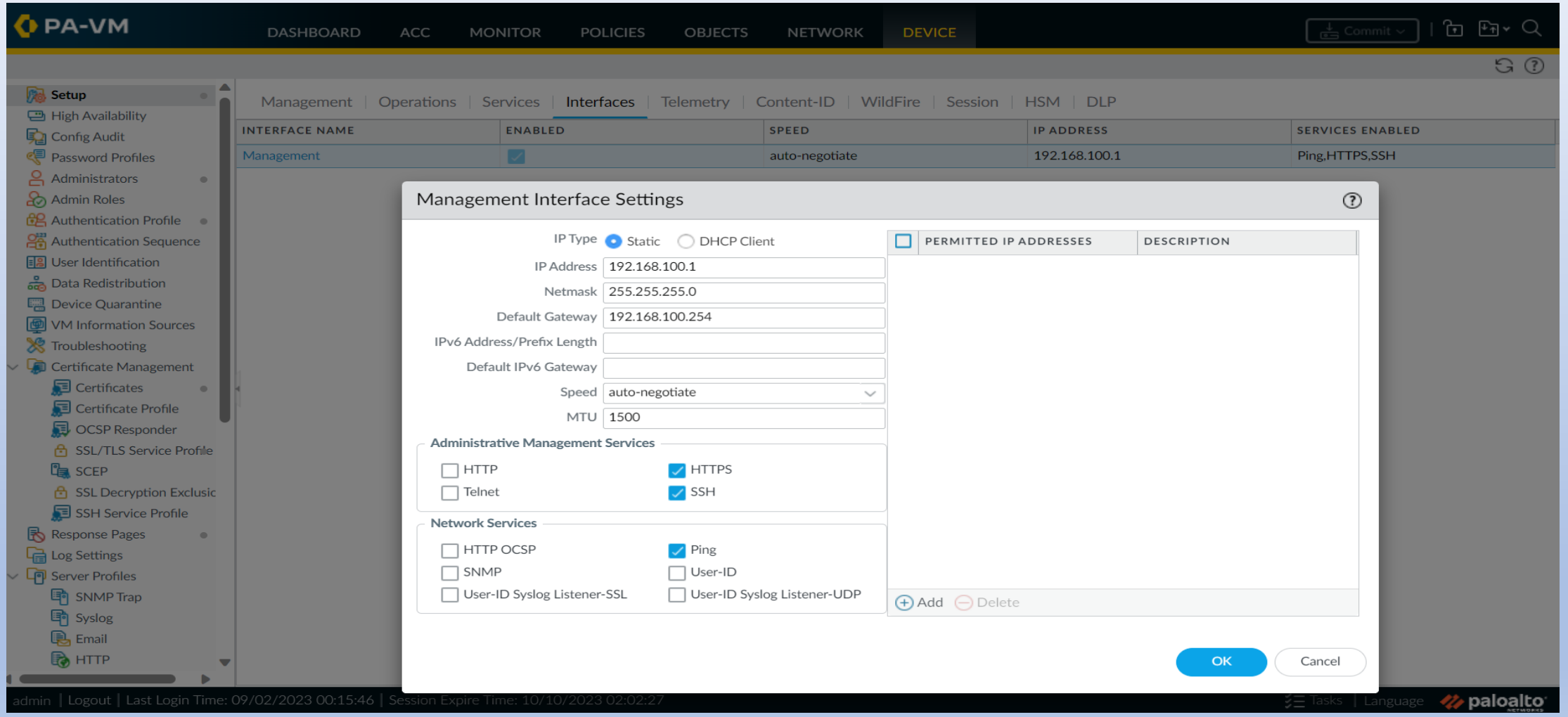
commit




PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
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:000FA500FFFB8B17
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)
URL 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

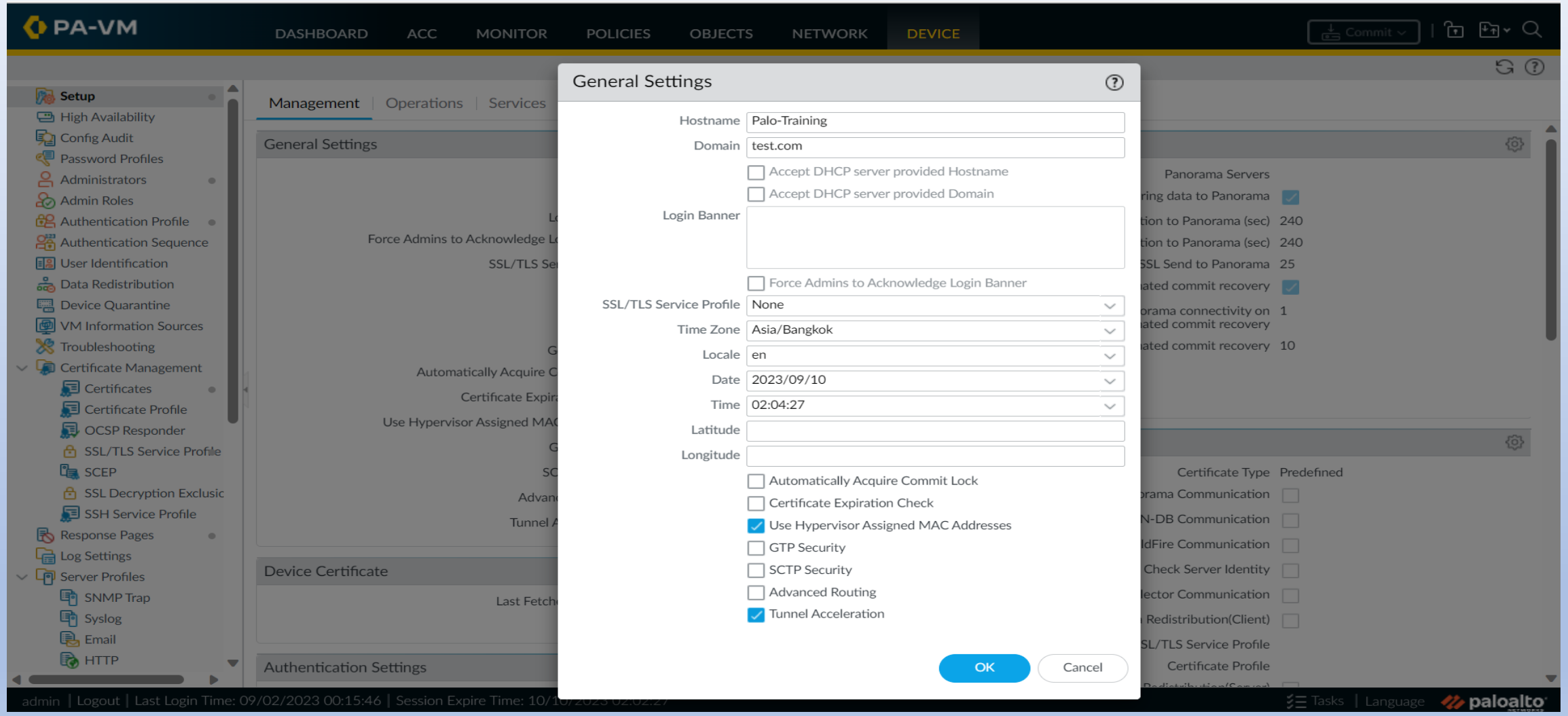
Configuring the MGT Interface - GUI

Device > Setup > Management > Management >Interface Settings



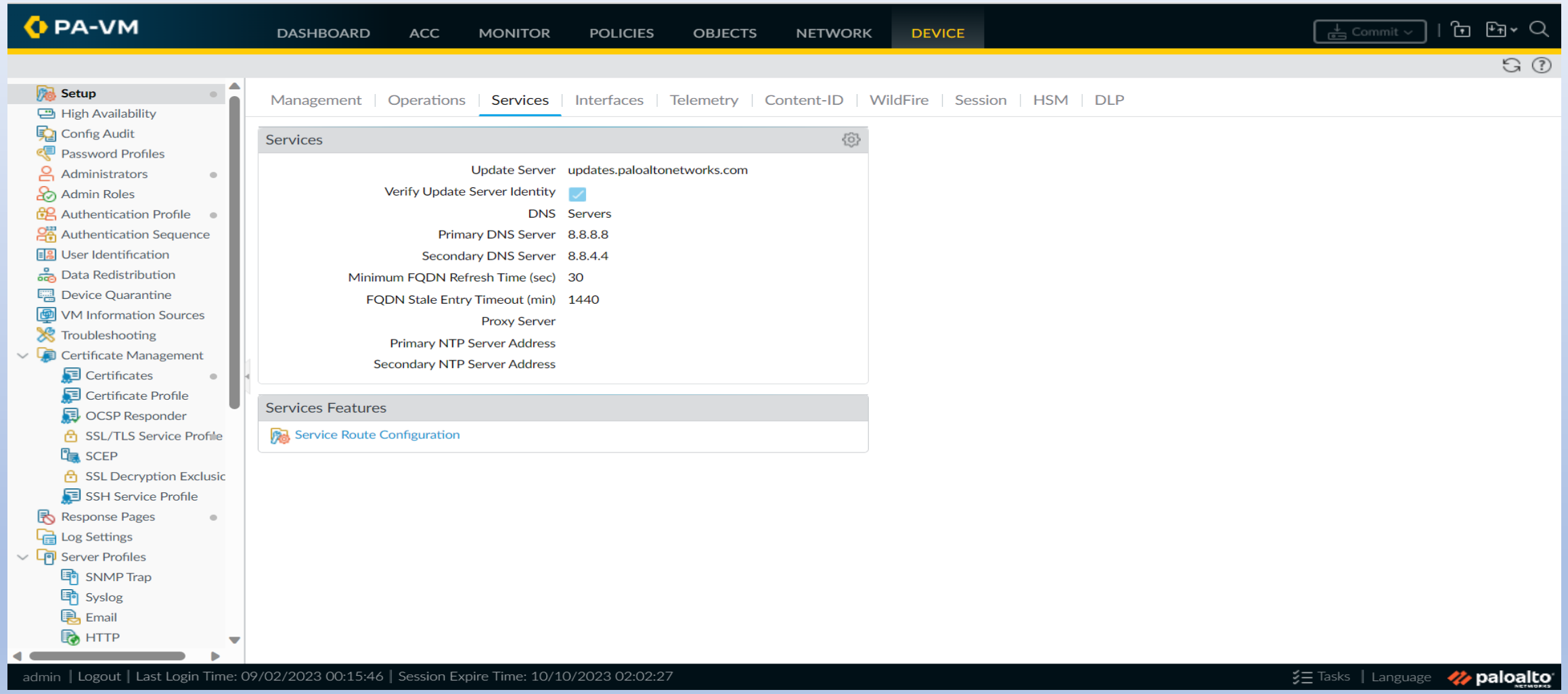
Configure the Hostname and Domain

Device > Setup > Management > General Settings



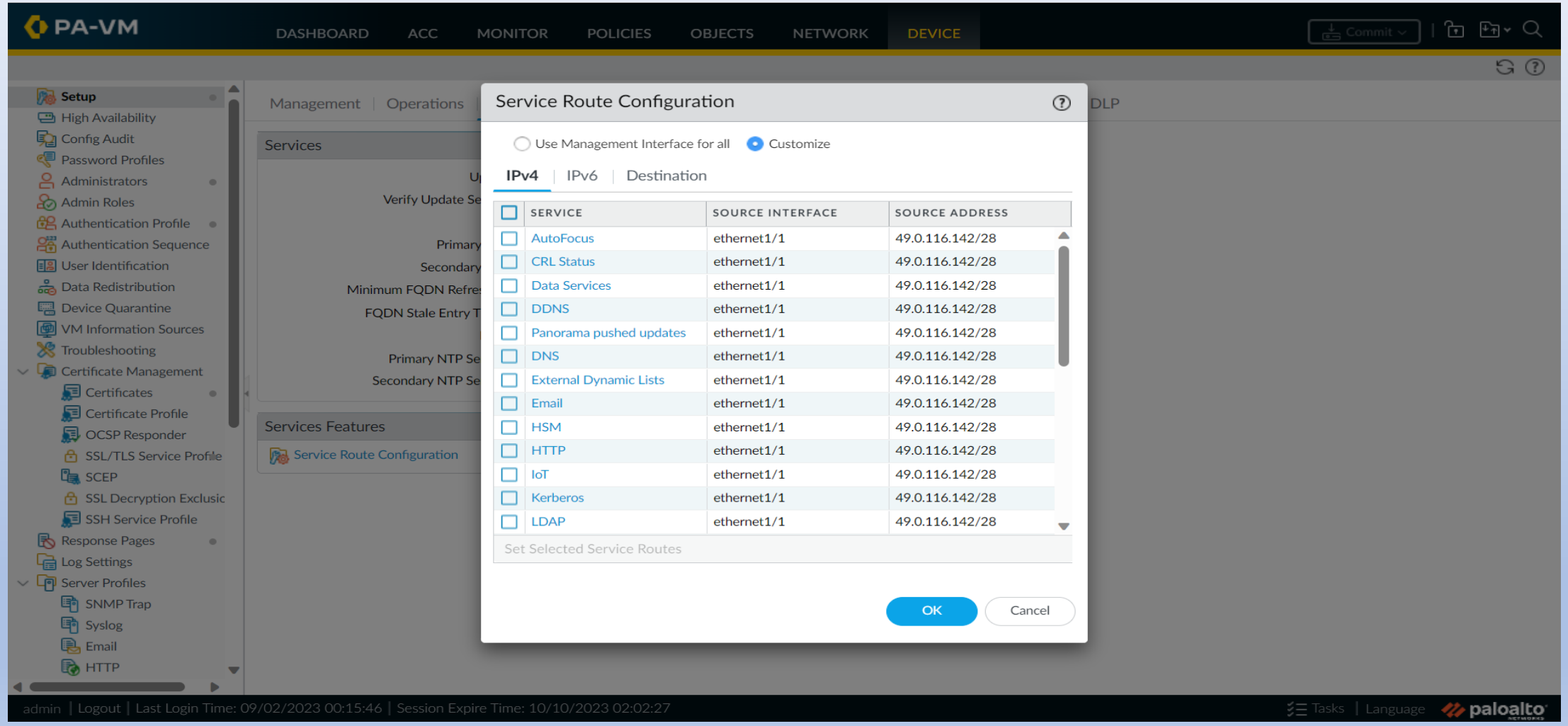
Configure DNS and NTP Servers

Device > Setup > Services



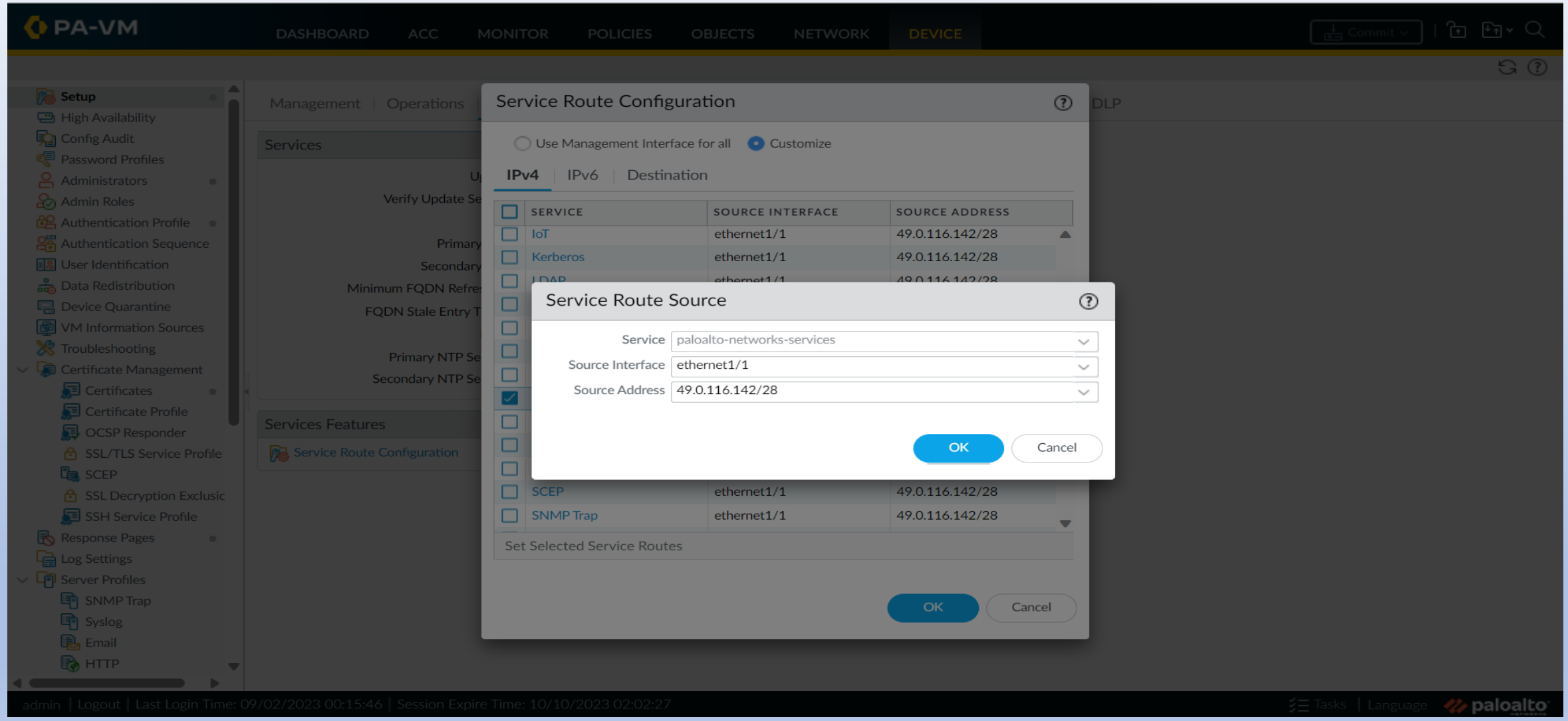
Service Route Configuration

Device >Setup >Services



Service Route Configuration

Device > Setup >Services



Licensing and Software Updates

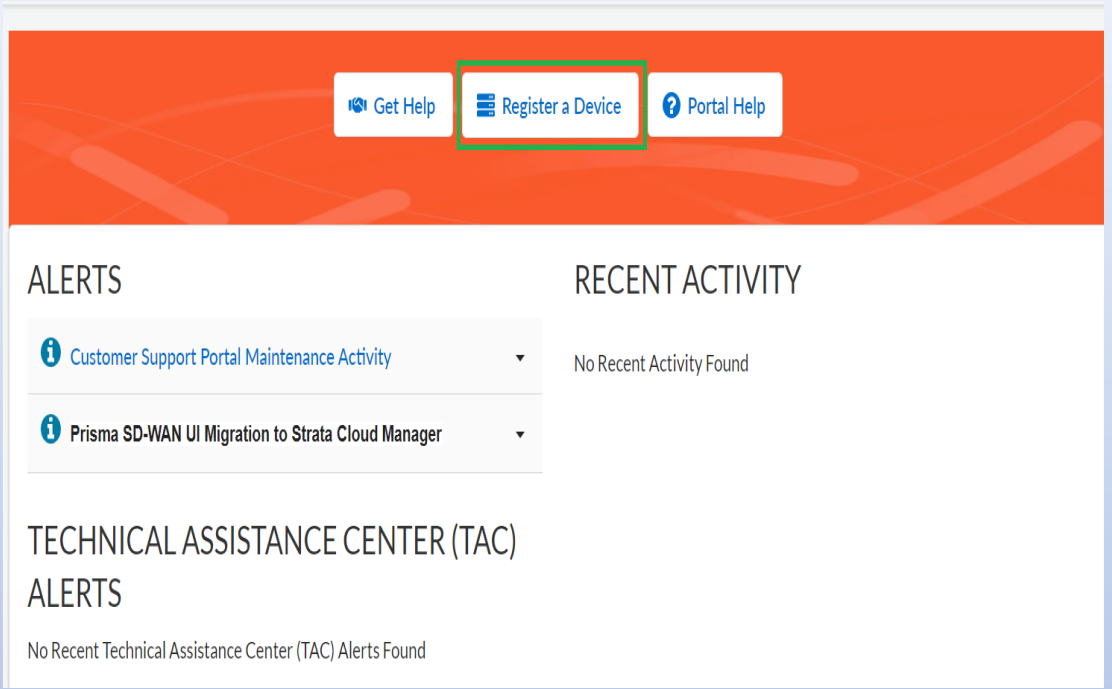
Activating PAN Firewall Services

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



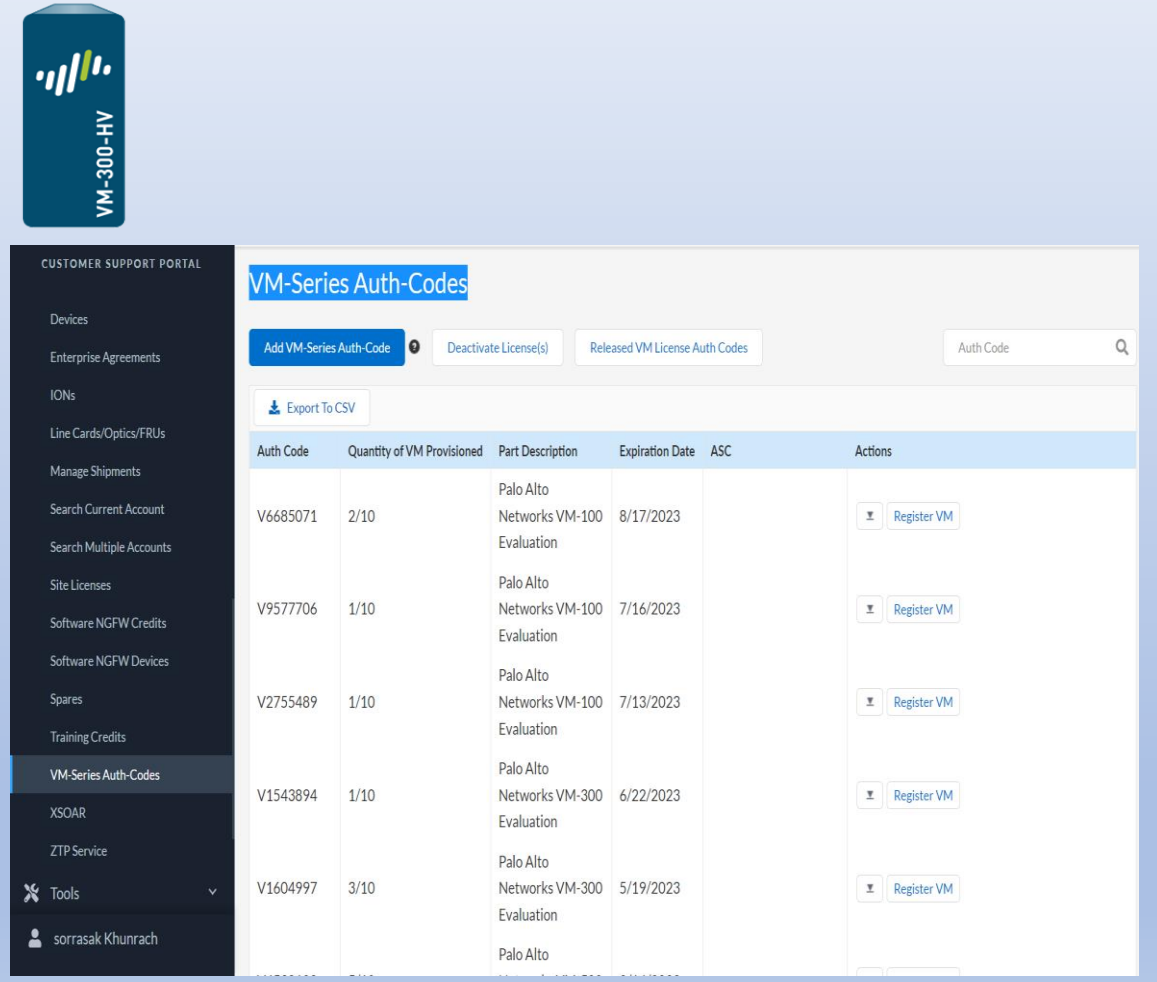
Activating PAN VM-Series Firewalls

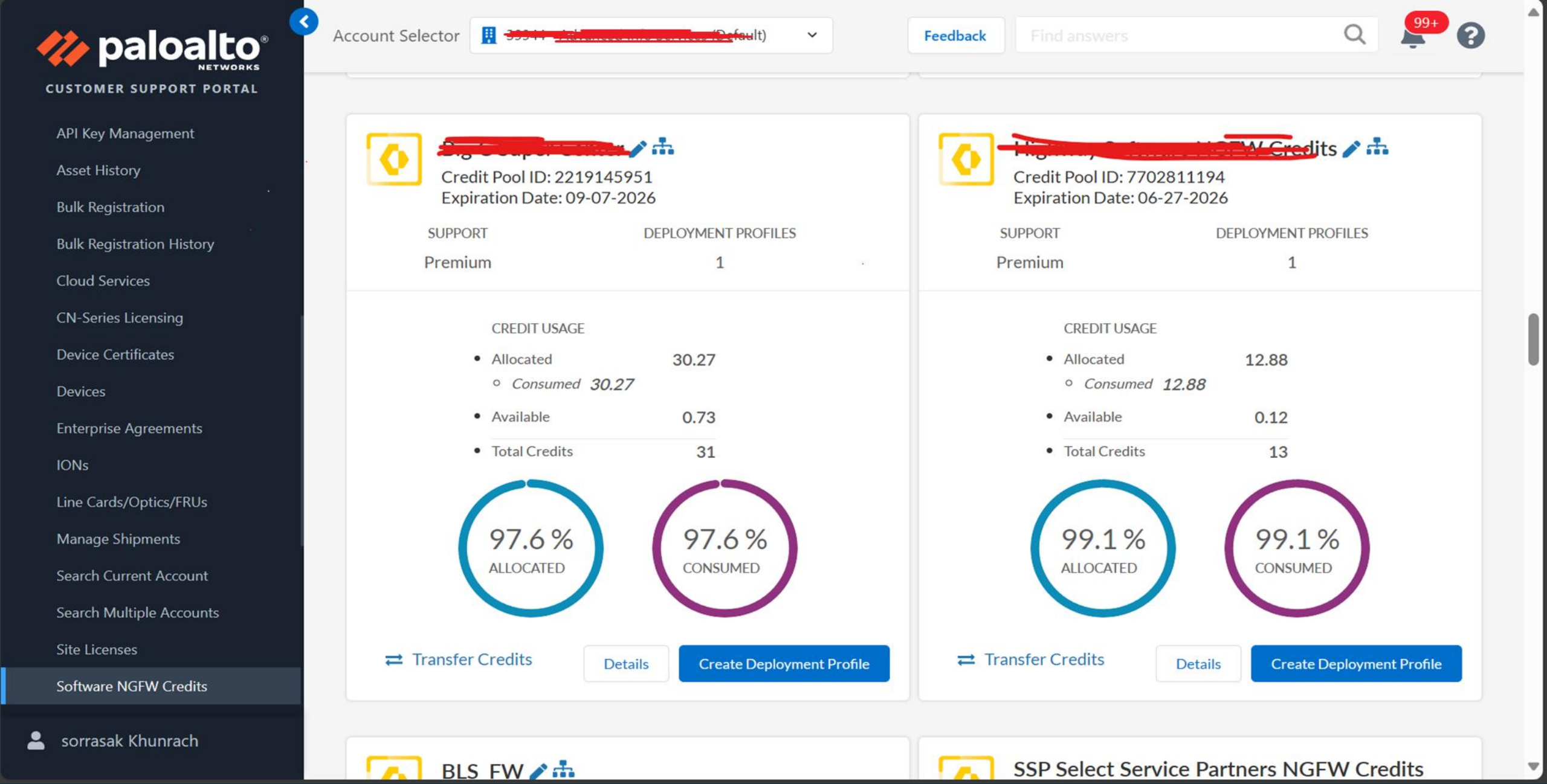
Register With Palo Alto Networks

- 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





Palo Alto Firewall By Sorrasak

https://www.paloaltonetworks.com/resources/tools/ngfw-credits-estimator

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
- [ ] Data Loss Protection
- [x] Advanced URL Filtering
- [ ] 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 Firev
Threat Prevention	Up to 1.5 Gbps per Firev

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

15.13

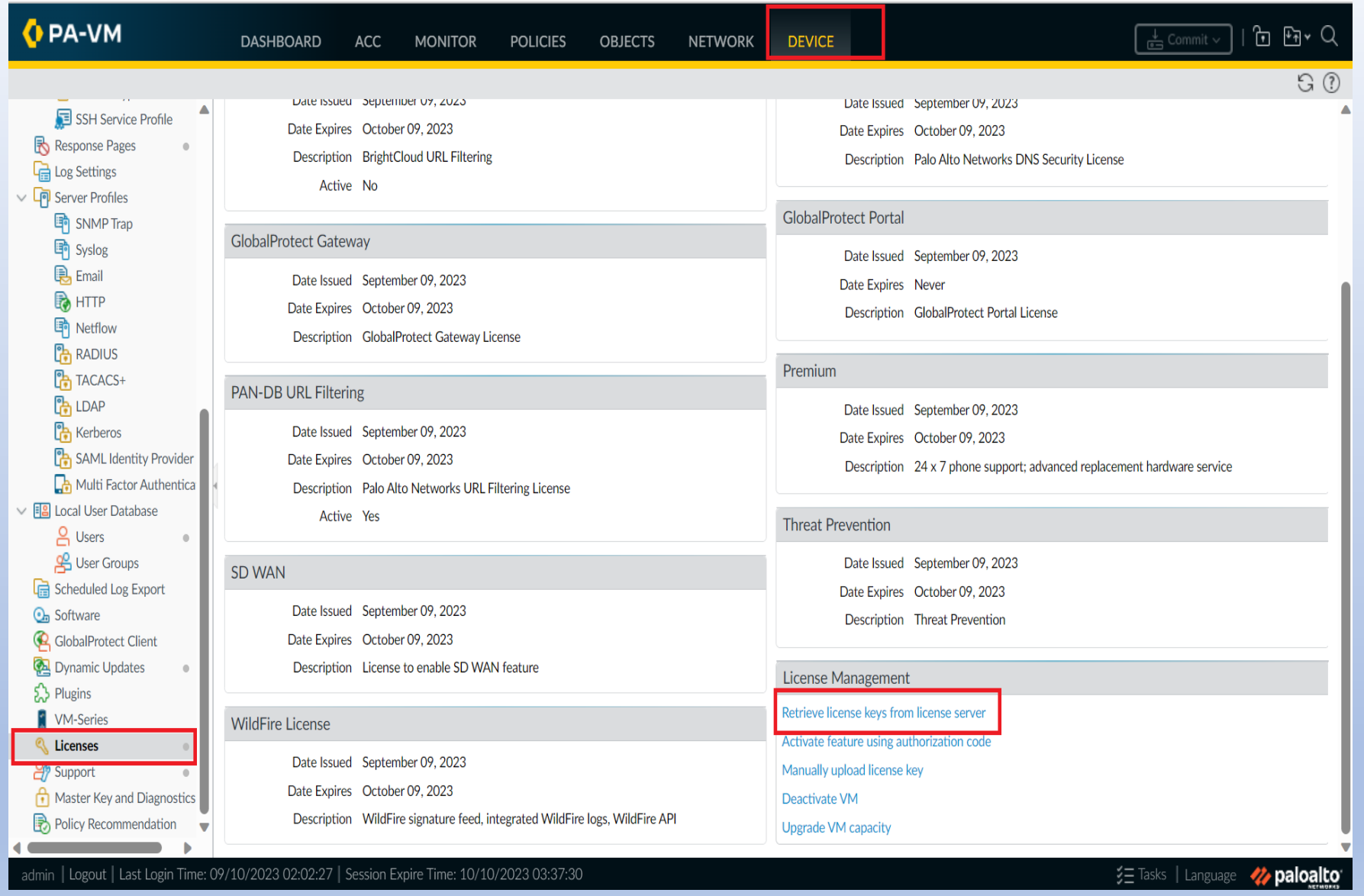
CREDITS

GET CREDITS

Licensing

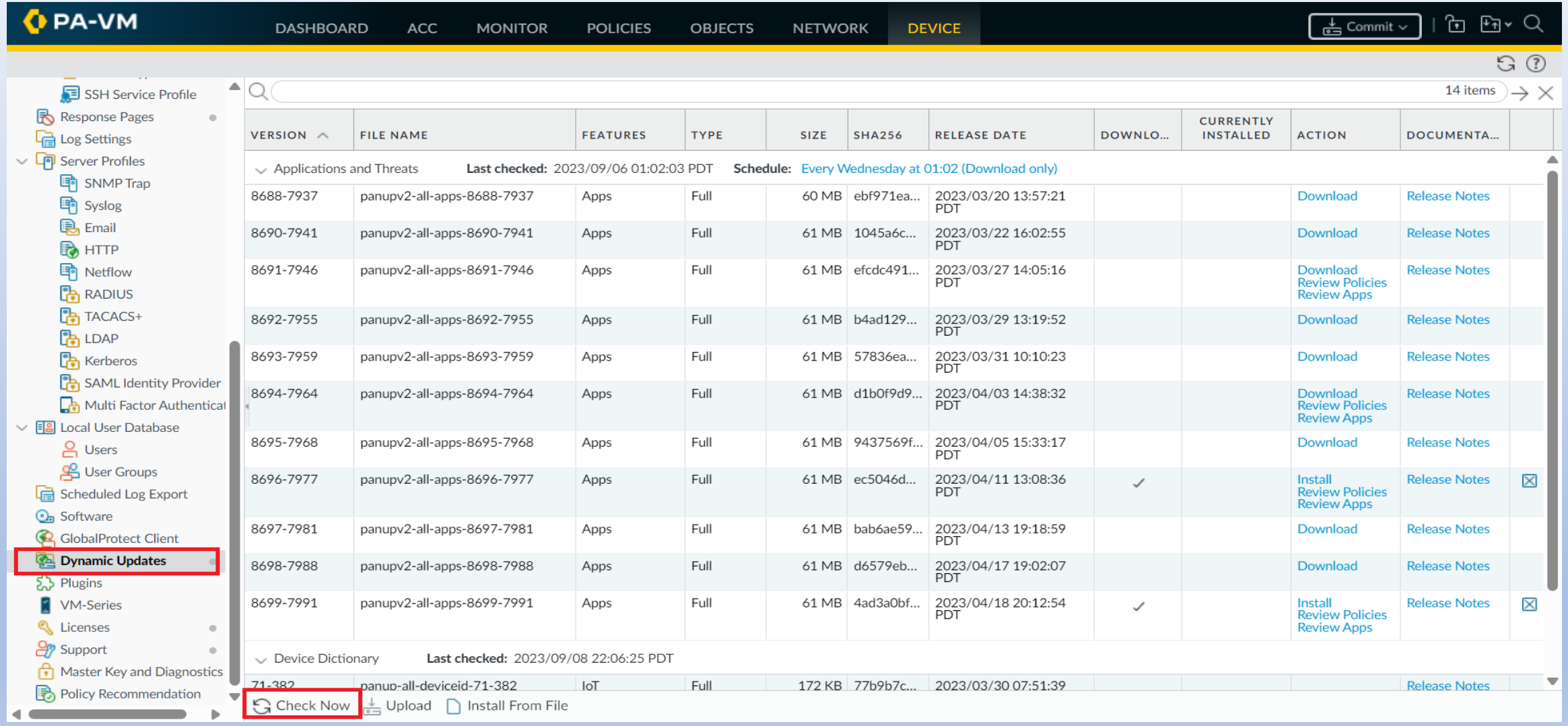
Device > Licenses

Device > Support



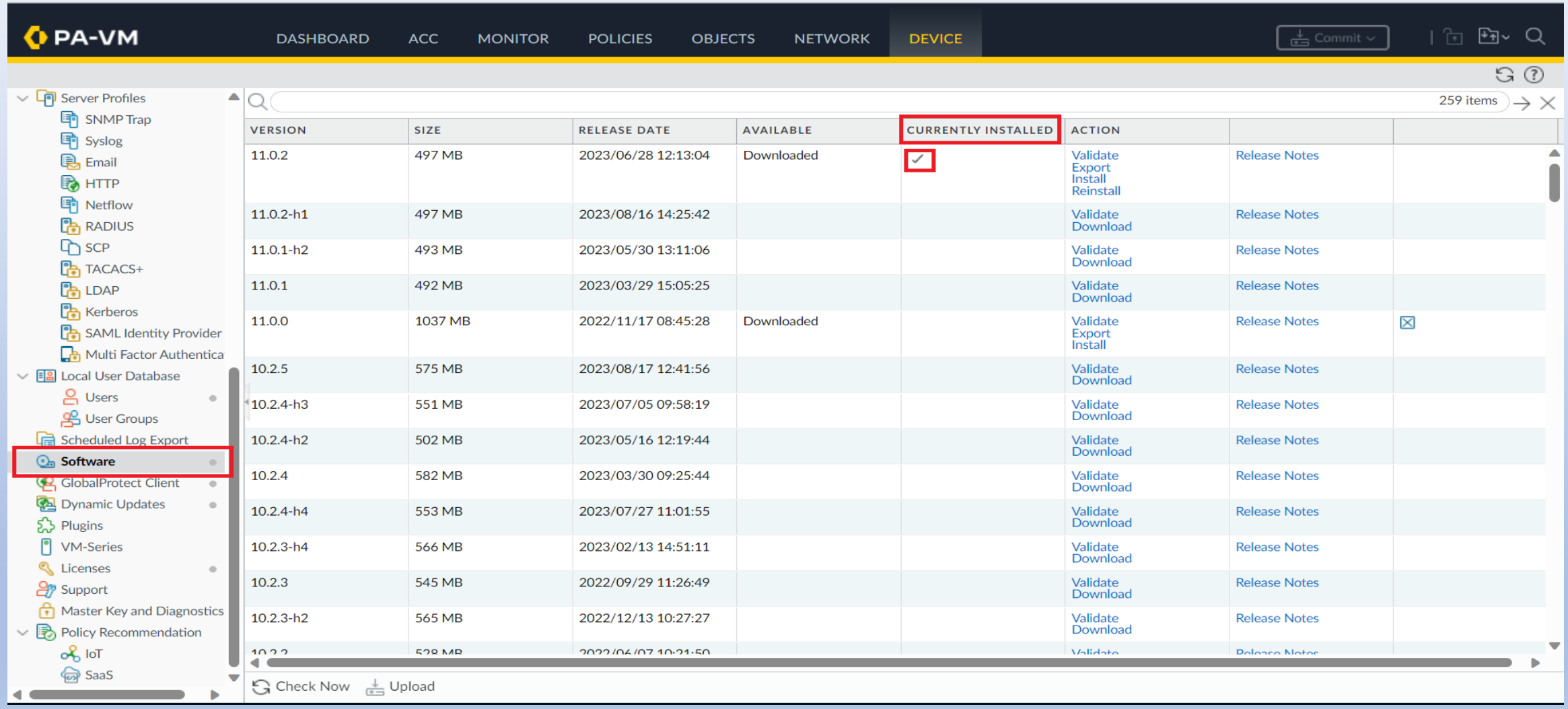
Dynamic Updates

Device > Dynamic Updates

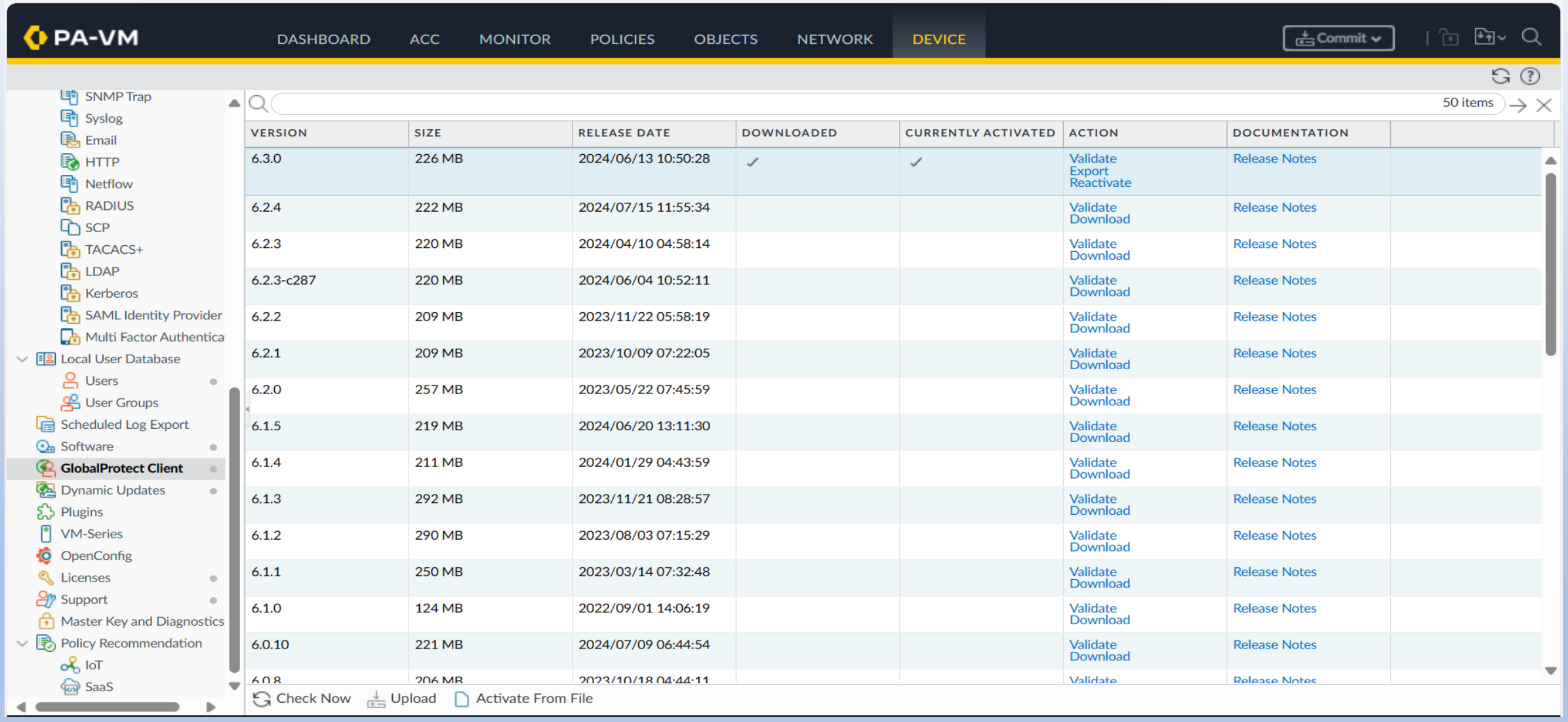


PAN-OS Software Updates

Device > Software



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                          Show active administrators
> advanced-routing                Show Advanced Routing runtime state
> api-key-expiration-ts           Shows the time before which any API keys wo
uld 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 servic
e profiles
> cloud-auth-service-metadata     Get cloud authentication service metadata f
or a region
> cloud-auth-service-profiles     Get cloud authentication service profiles o
f a tenant for a region
> cloud-auth-service-regions      Get cloud authentication service deployed r
egions
> cloud-auth-service-tenants      Get cloud authentication service tenants fo
r 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 tab
le
> commit-locks                    Show list of commit locks
--more--
```

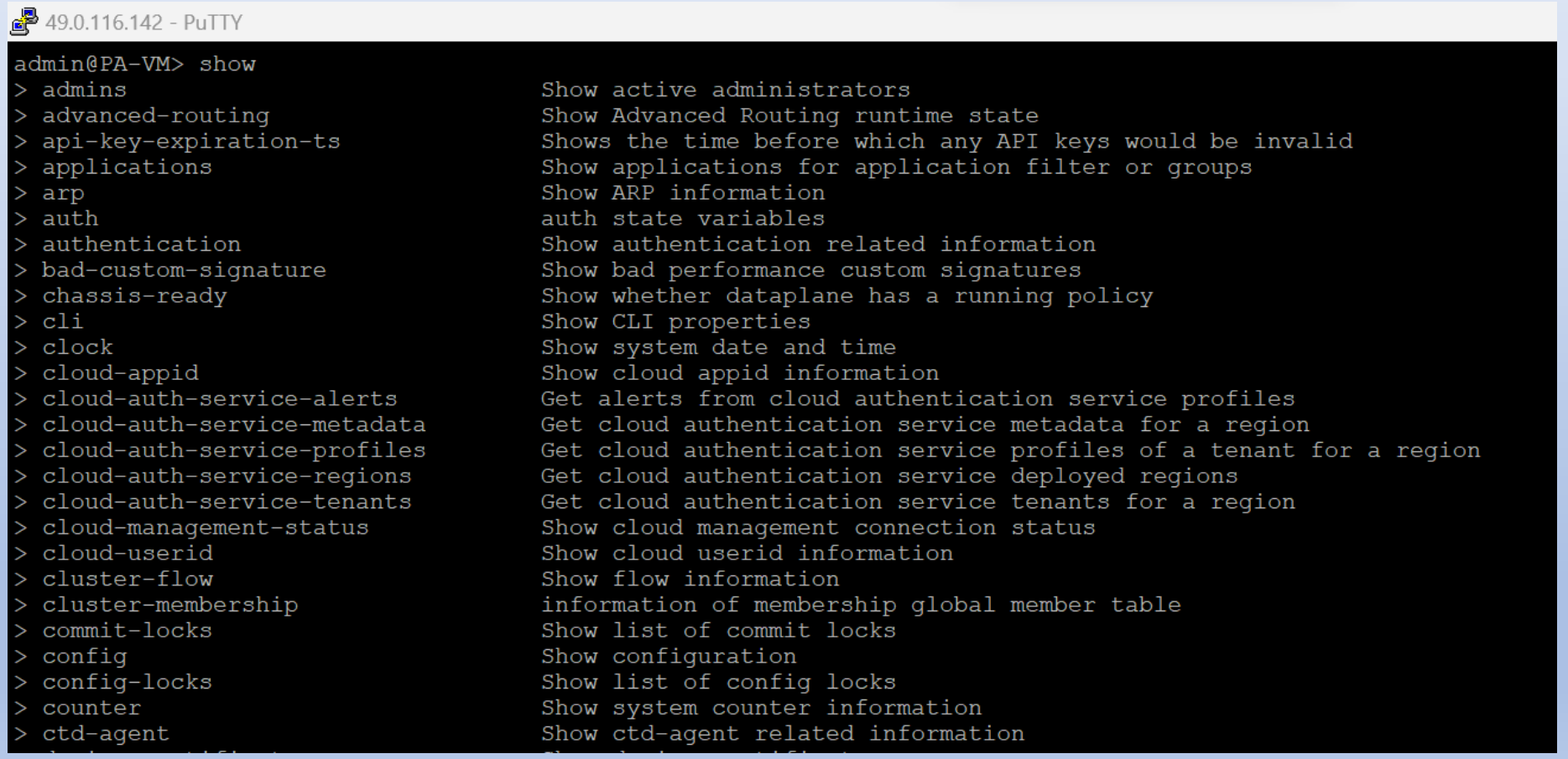
```
admin@PA-VM> ping source 49.0.116.142 host 8.8.8.8
PING 8.8.8.8 (8.8.8.8) from 49.0.116.142 : 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=57 time=29.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=57 time=28.10 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0%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

```
admin@PA-VM> 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> 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:b4:84:77
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              4     1                    N/A                     0      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



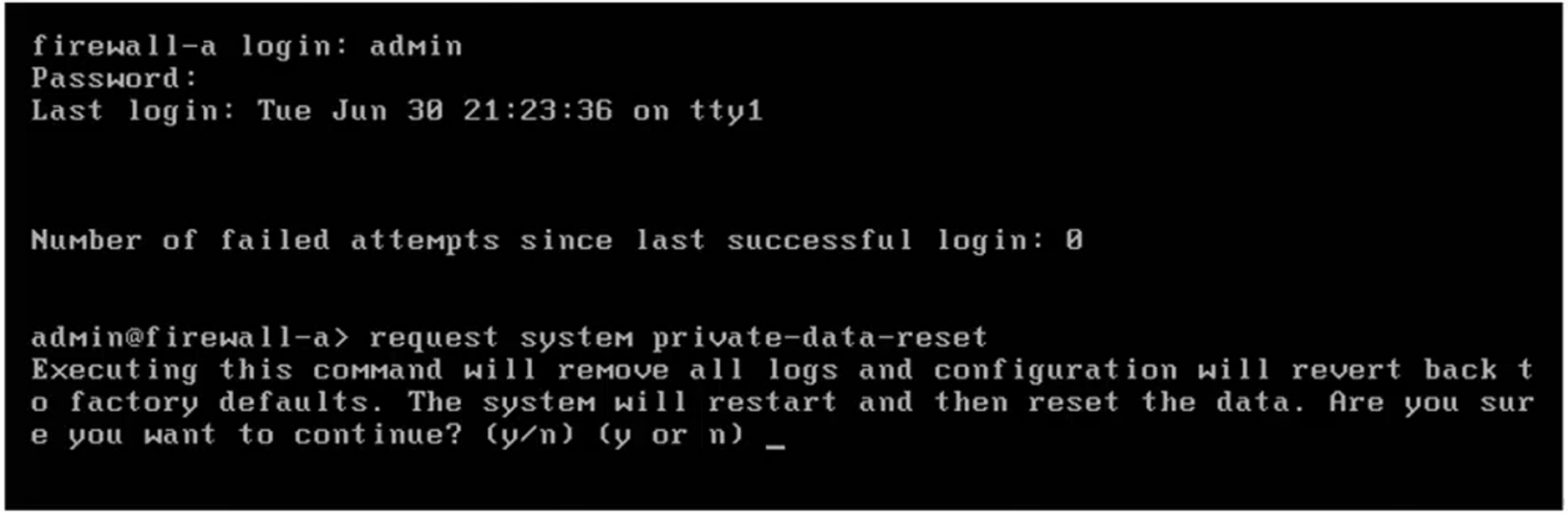
ping Command

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
```

```
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>
```

Reset to Factory Configuration



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.

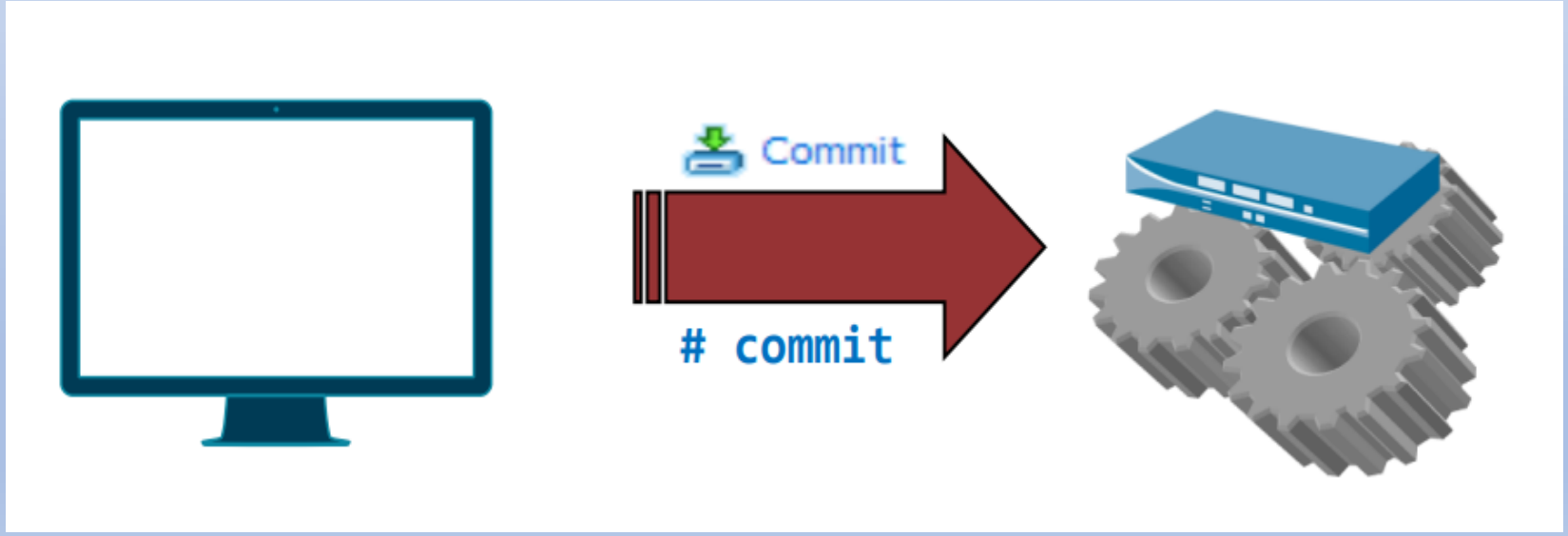
After some time, you can choose the option: Reset to Factory Default

Configuration Management

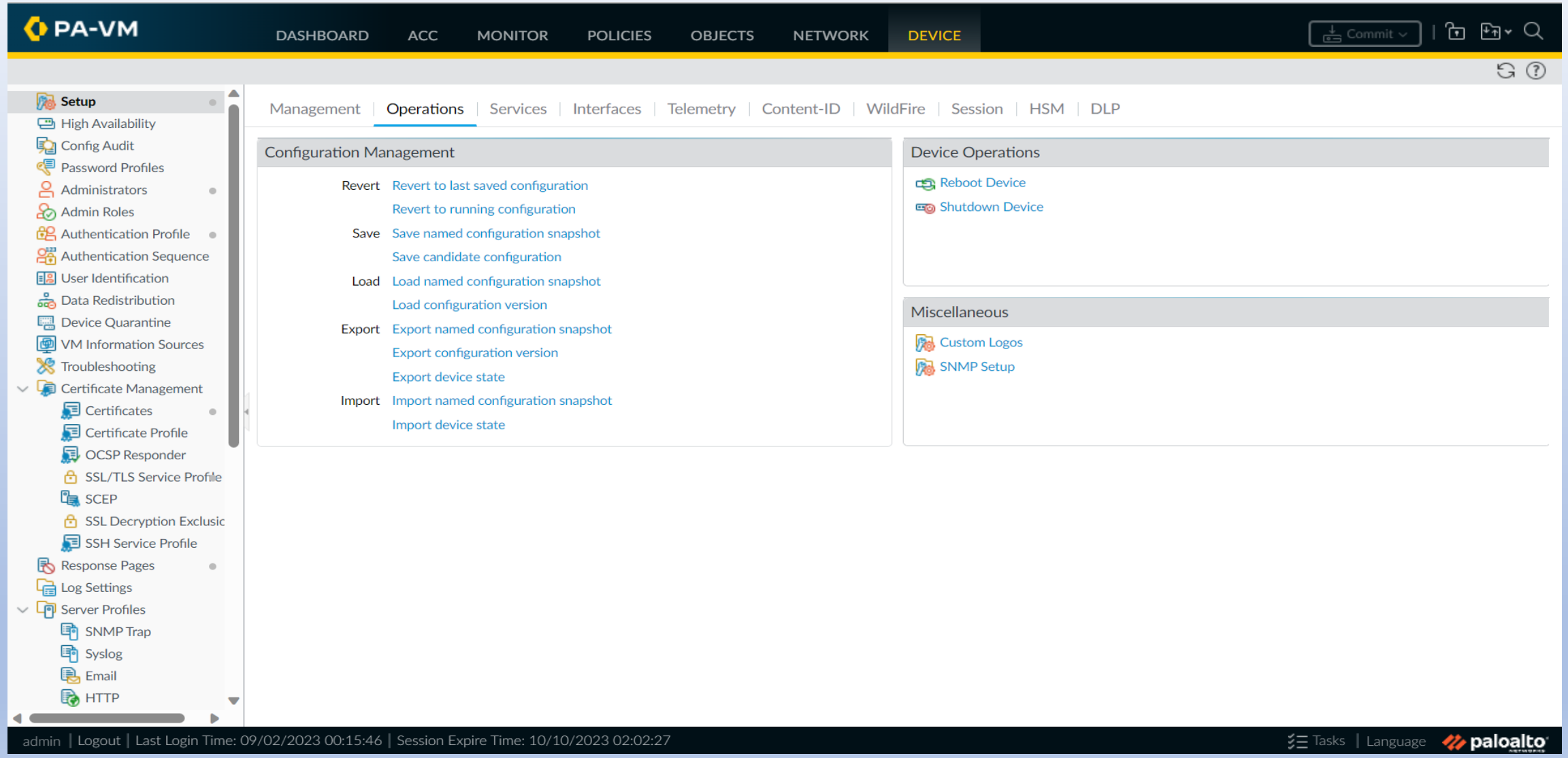
Config Types

Candidate Config

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

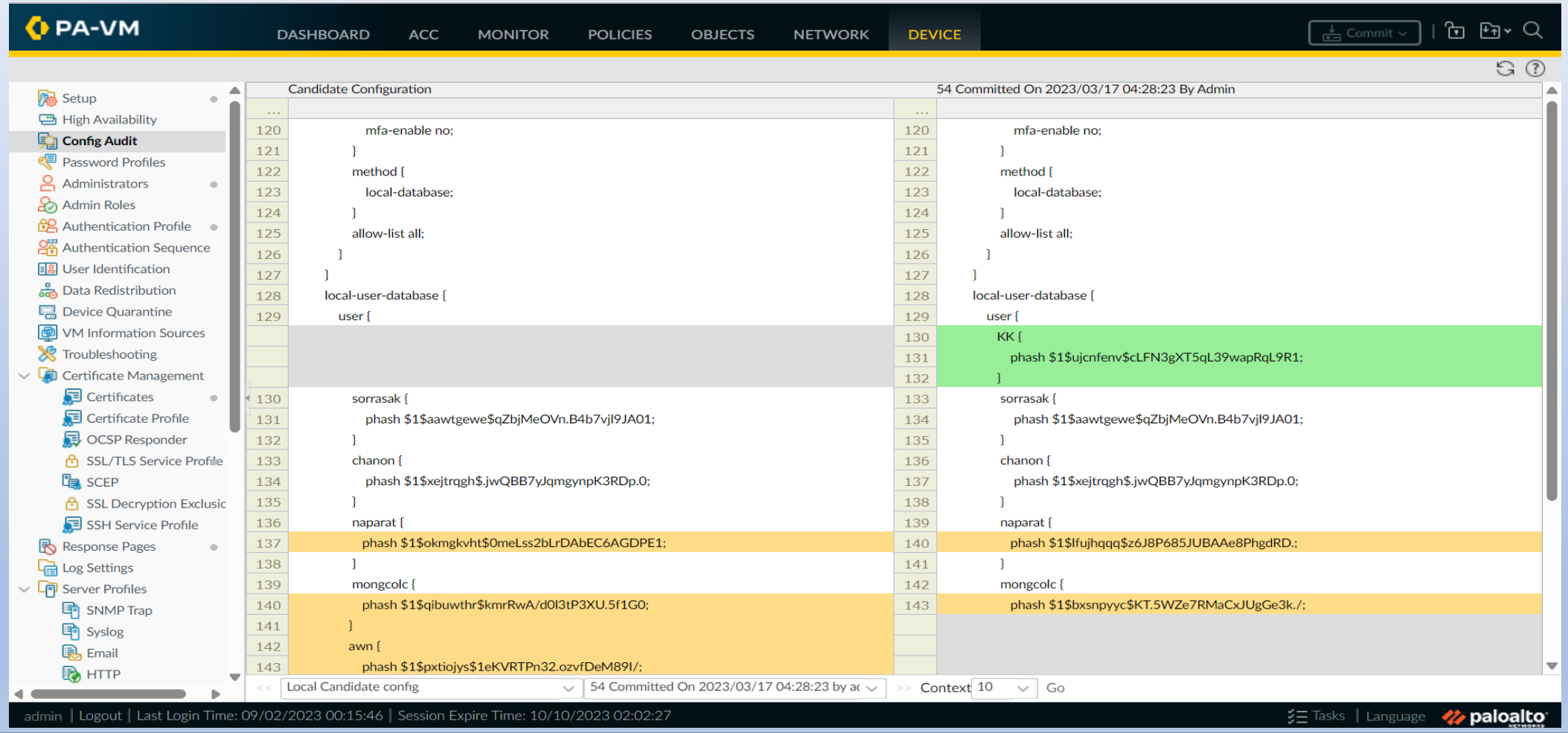


Configuration Management



Config Auditing

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

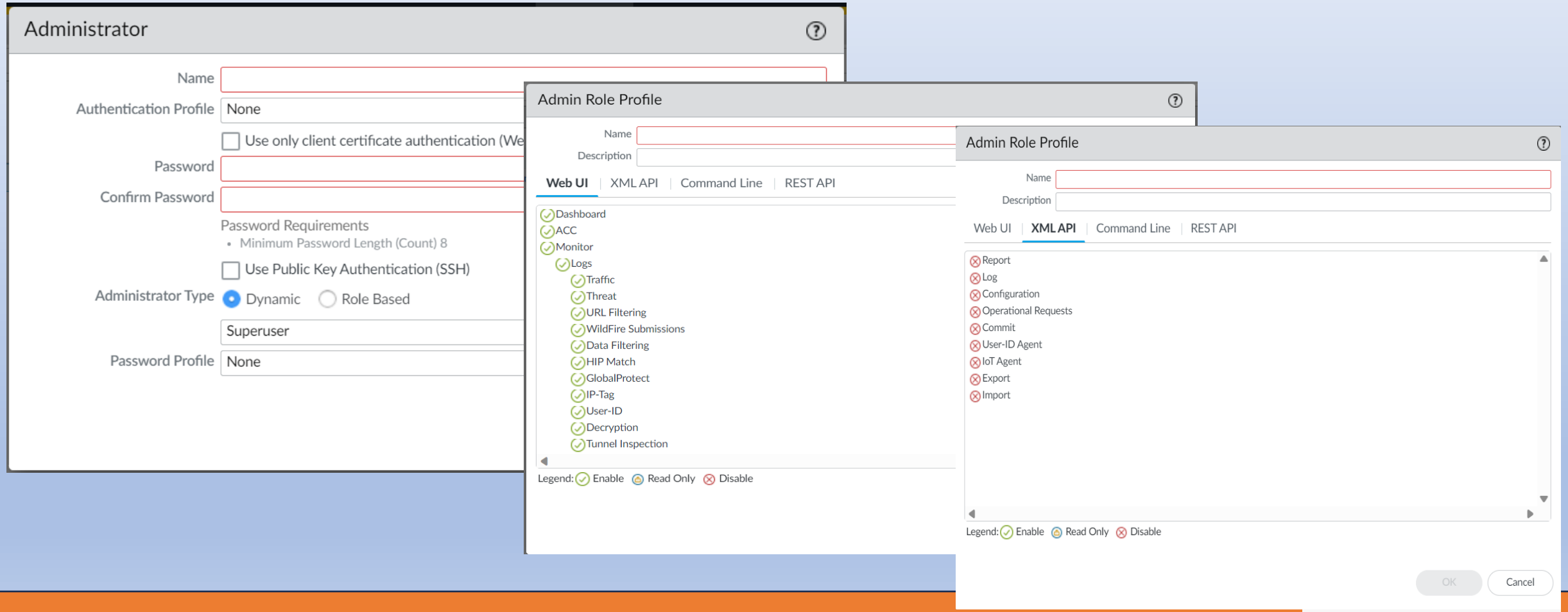


User Management

Administrator Roles

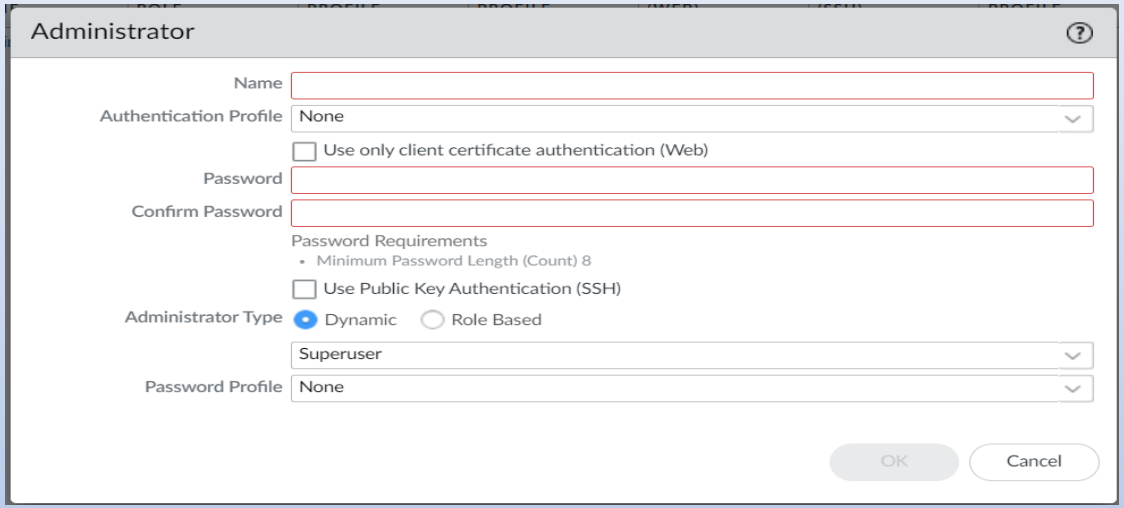
A role defines the type of access an administrator has to the system

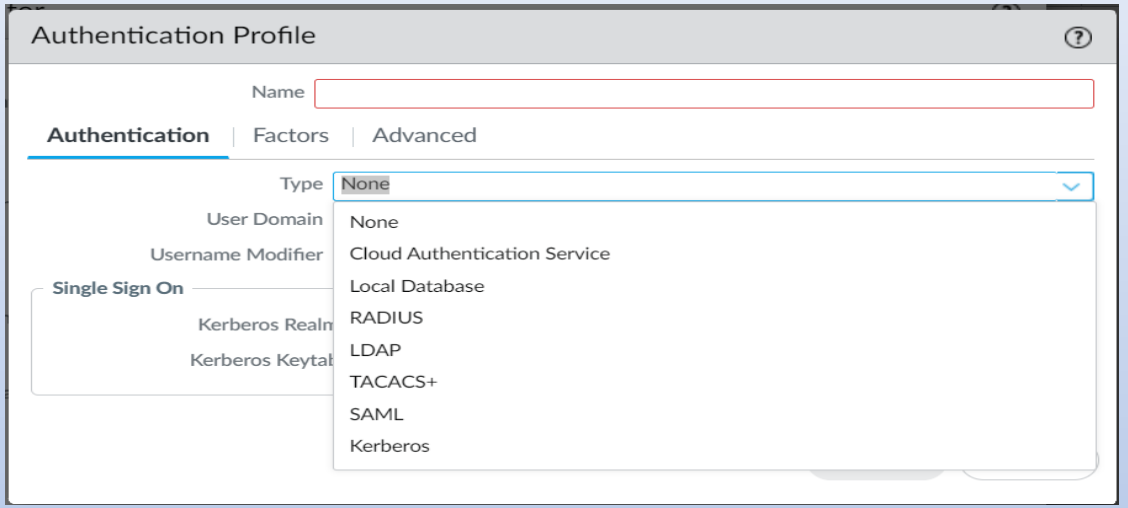
- Dynamic Roles: Built-in roles such as Superuser and Device Administrator
- Admin Role Profiles: Custom-made roles

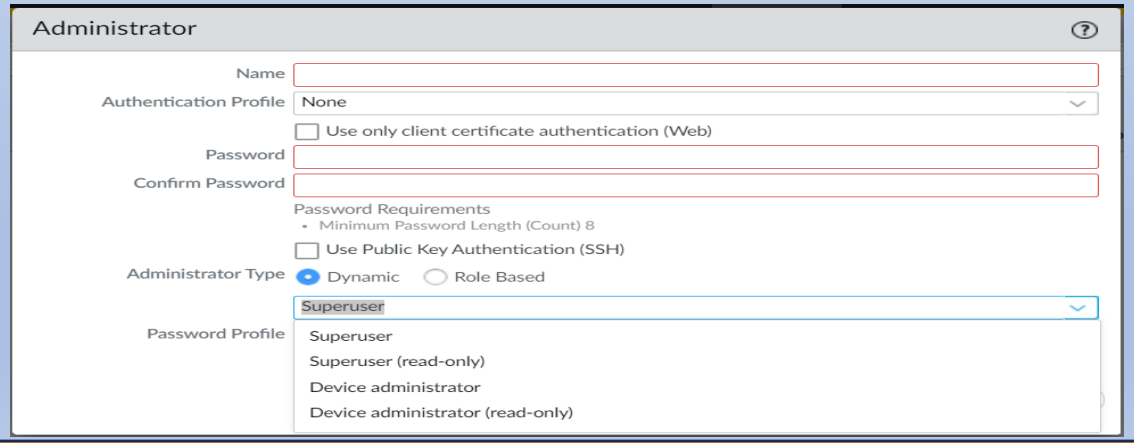


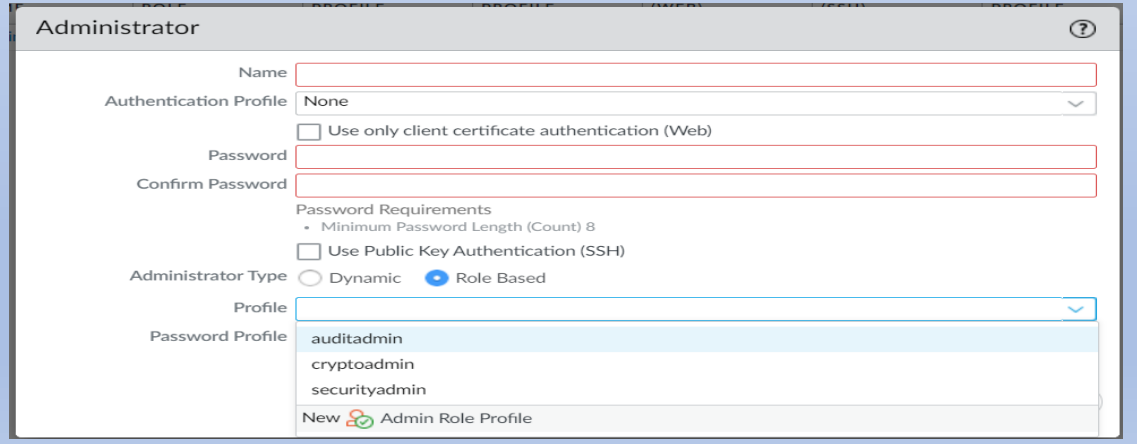
Creating Administrator Accounts

Device > Administrators







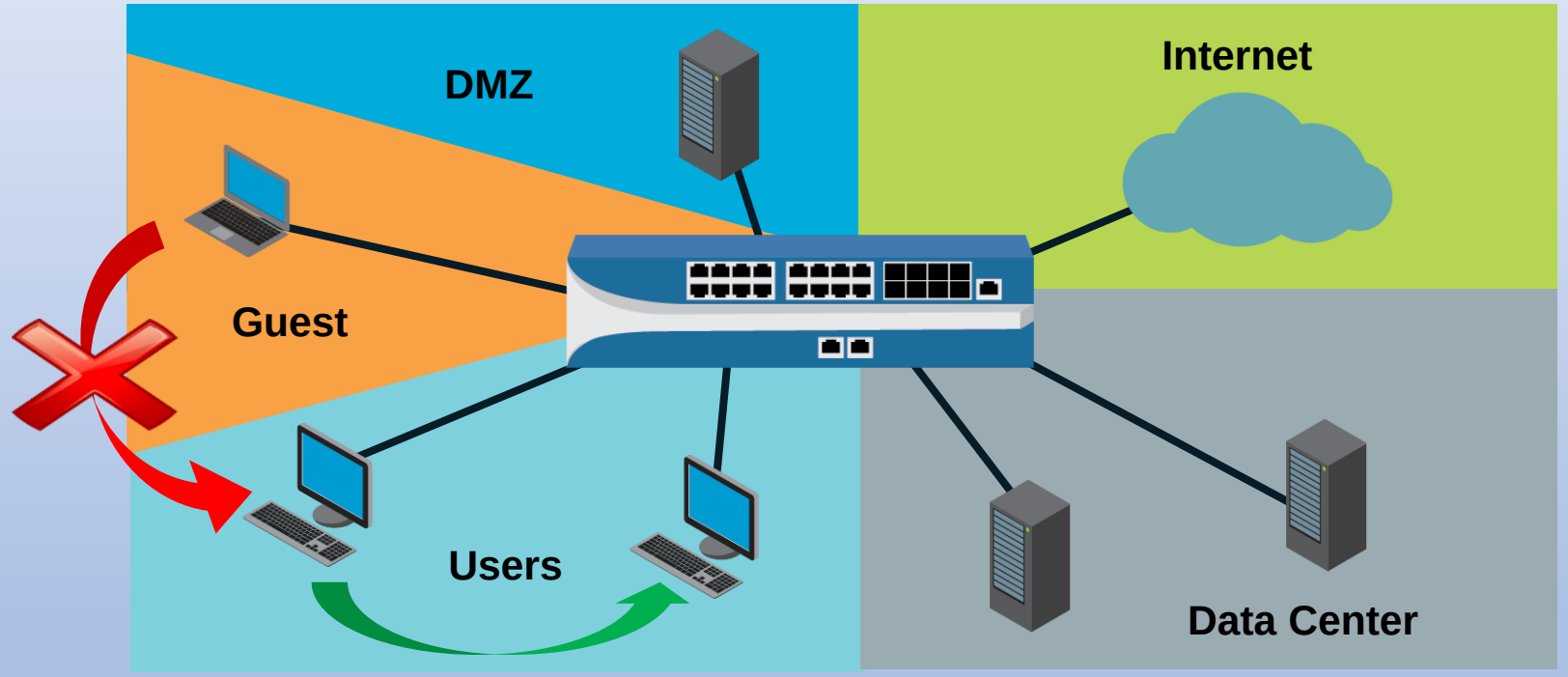


3.
Basic Interface Config

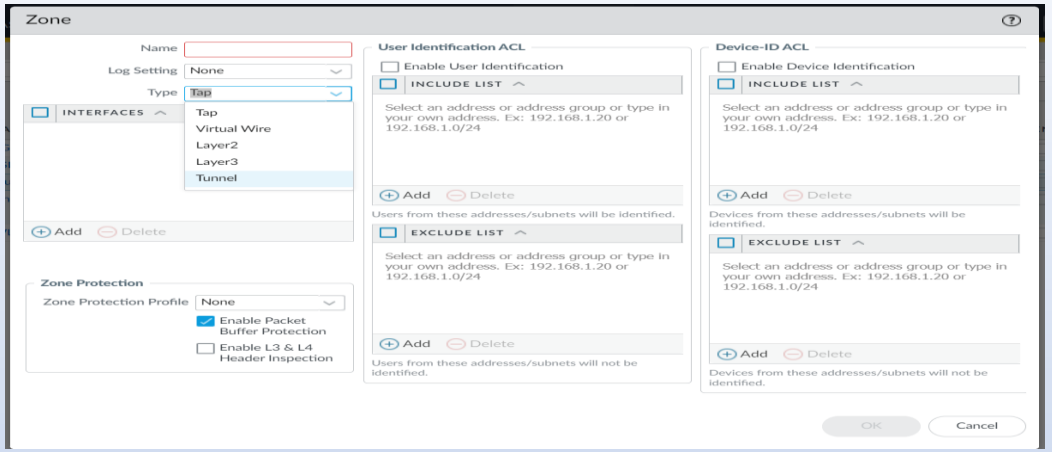
Security Zones

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

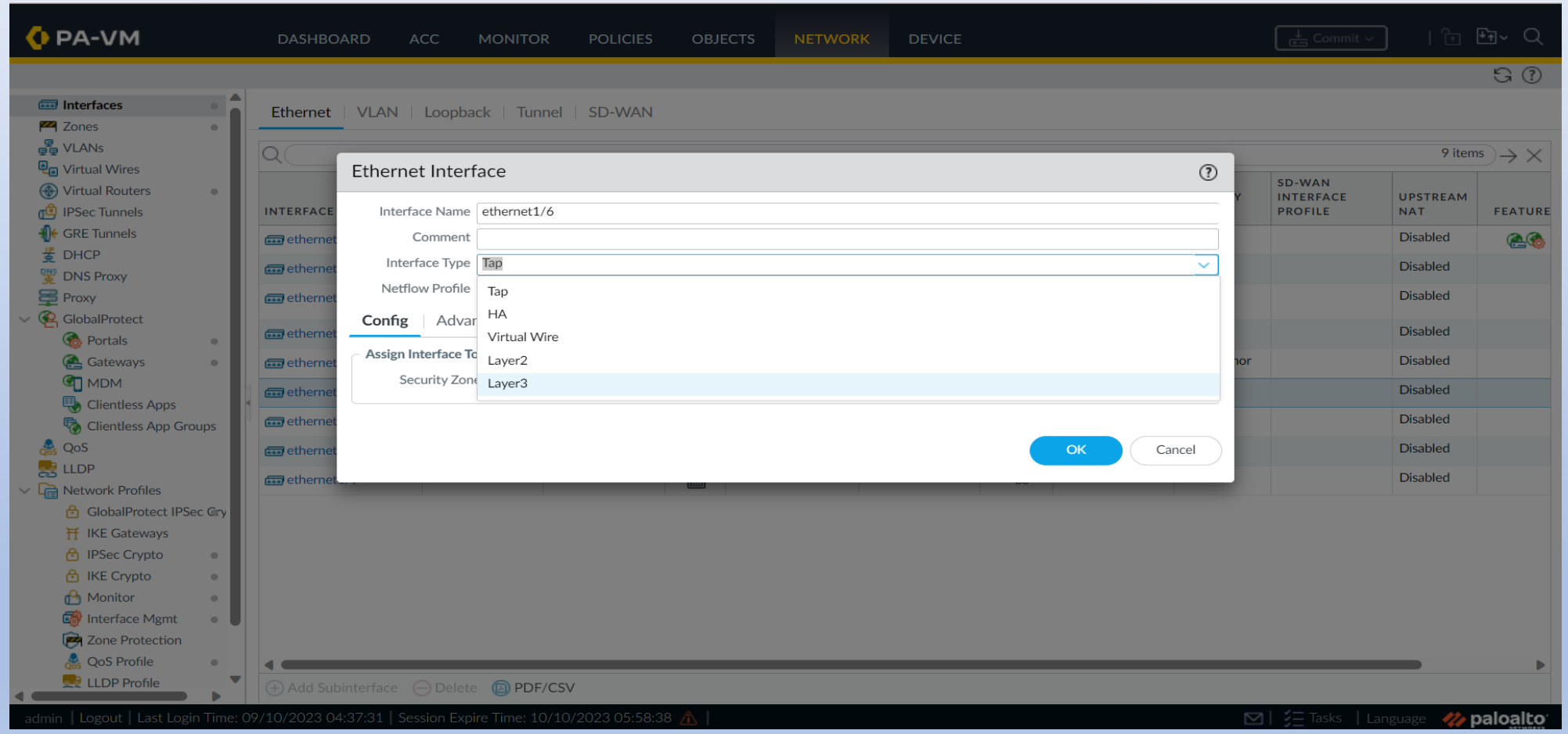
- An Interface is configured to one zone only
- A Security Zone can have multiple Interfaces

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

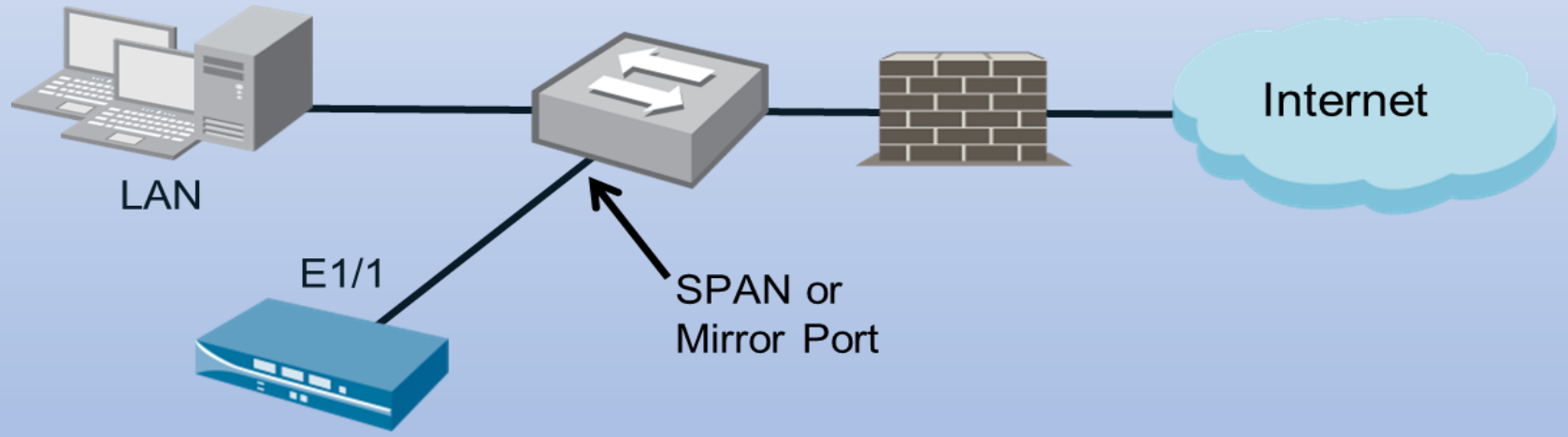
Interface Types

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



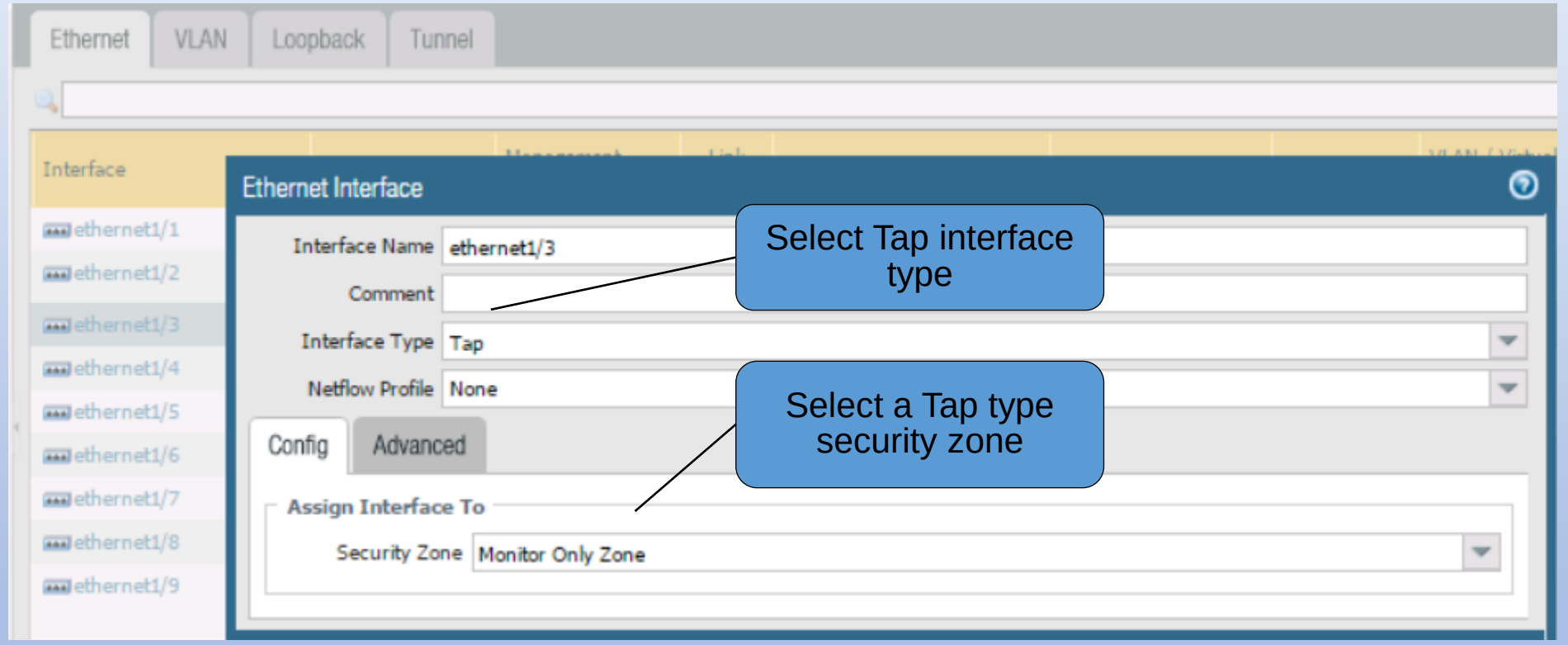
Ethernet Tap Interface

- 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



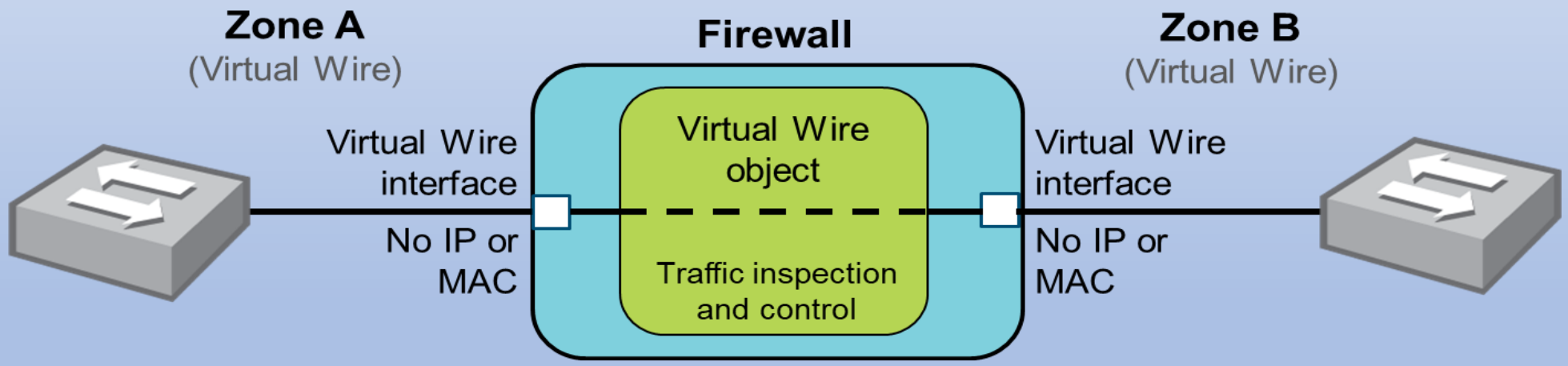
Configuring a Tap Interface

Network > Interfaces > Ethernet > <select_interface>



Virtual Wire Interface

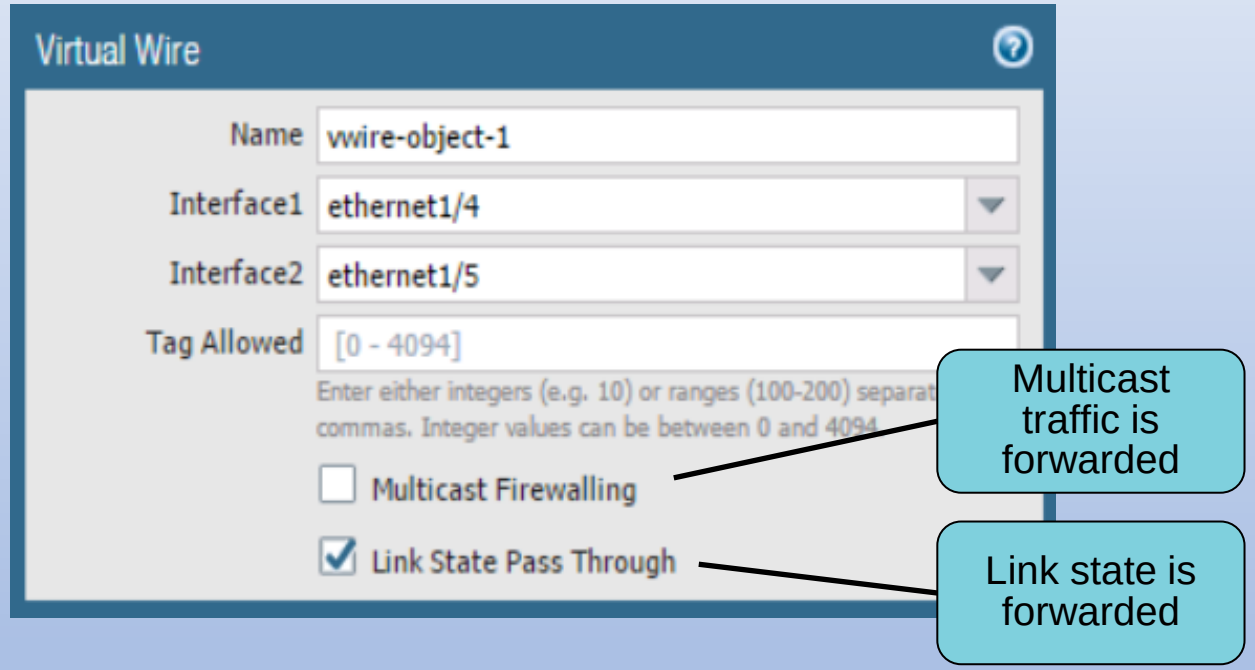
- Binds two firewall interfaces together through Virtual Wire object
- Typically used when no switching or routing is needed
- No configuration changes for adjacent network devices



Configuring a Virtual Wire Object

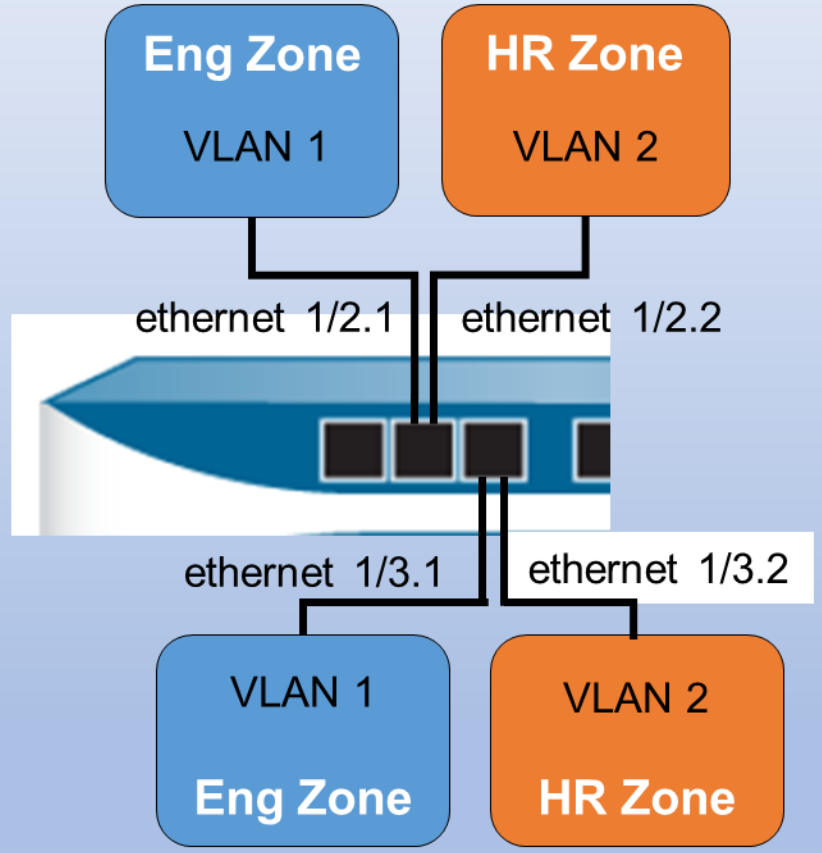
- Virtual Wire object connects to Virtual Wire interfaces.
- A virtual wire can accept traffic based on 802.1Q VLAN tags:
  - 0 = untagged traffic

Network > Virtual Wires > Add



Ethernet Layer 2 Interfaces

Layer 2 Subinterfaces

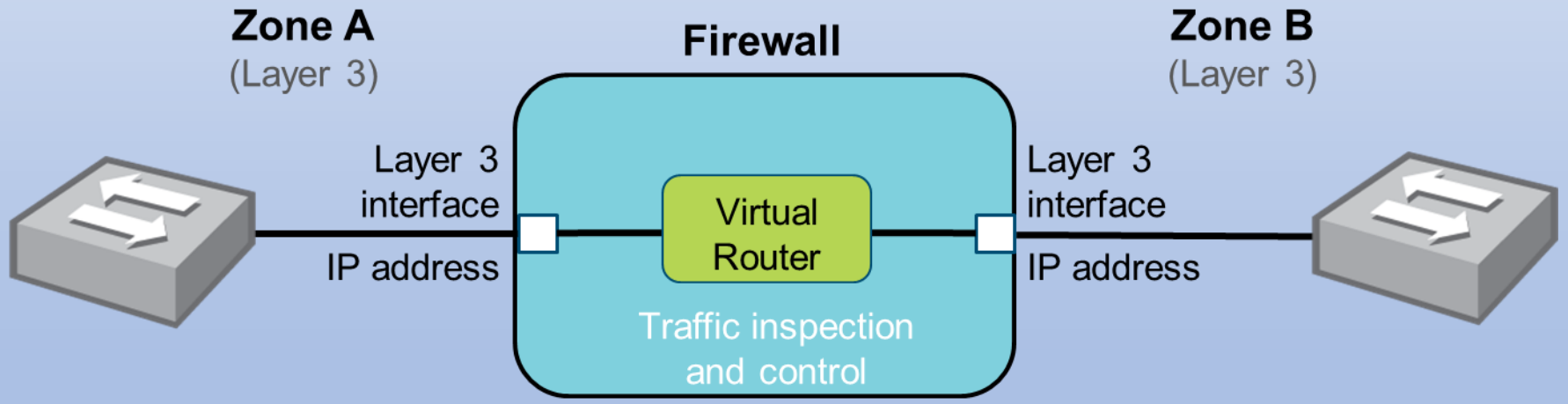


- Assign subinterfaces to zones
- VLAN traffic isolated by subinterfaces:
  - Need route between VLANs
  - Security policy blocks interzone traffic by default
- Useful configuration for multi-tenant networks

Layer 3 Interfaces

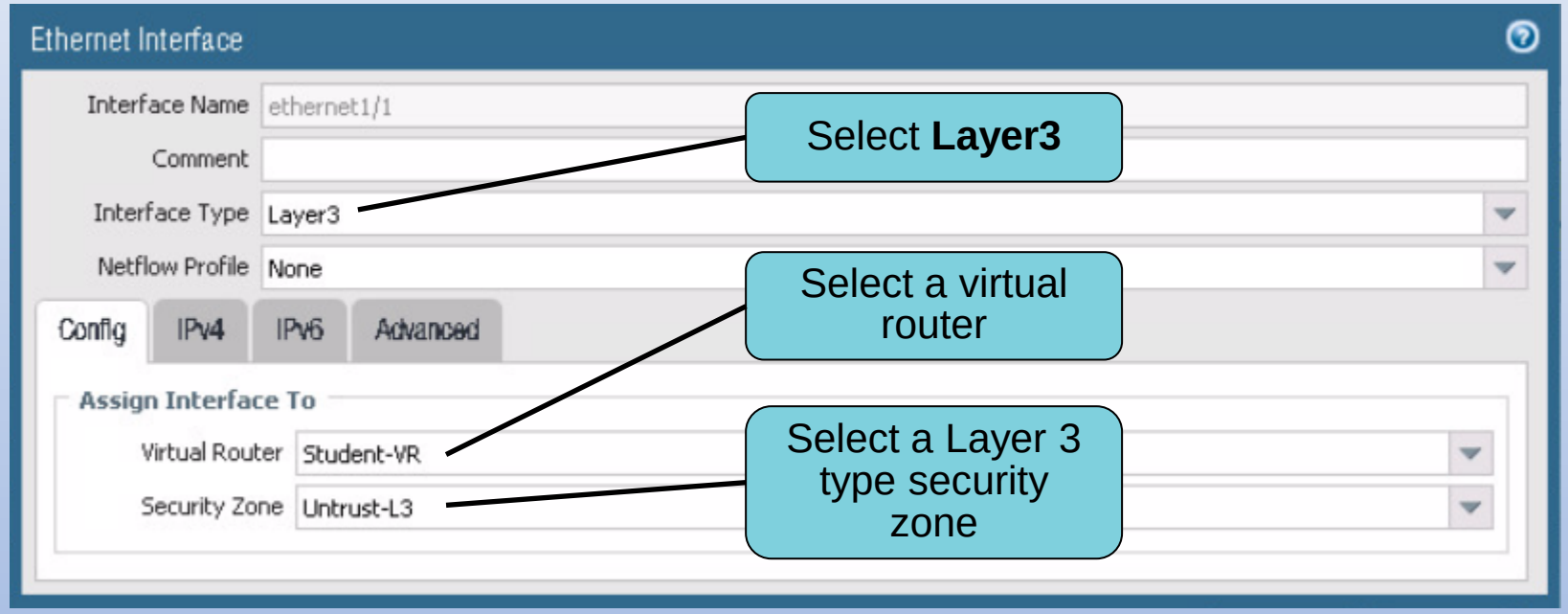
Layer 3 Interfaces

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



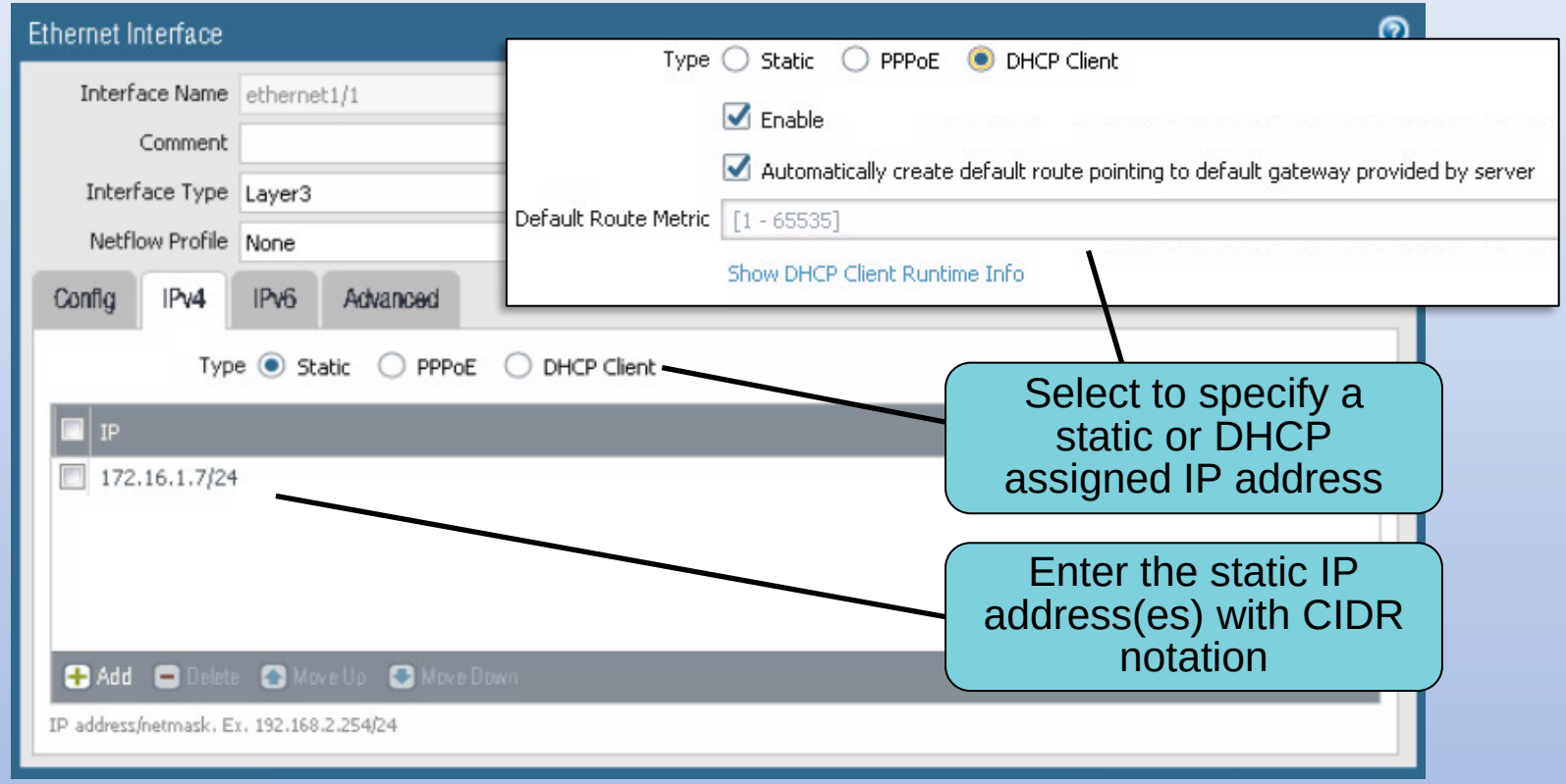
Configuring a Layer 3 Interface – Config

Network > Interfaces > Ethernet > <select_interface>

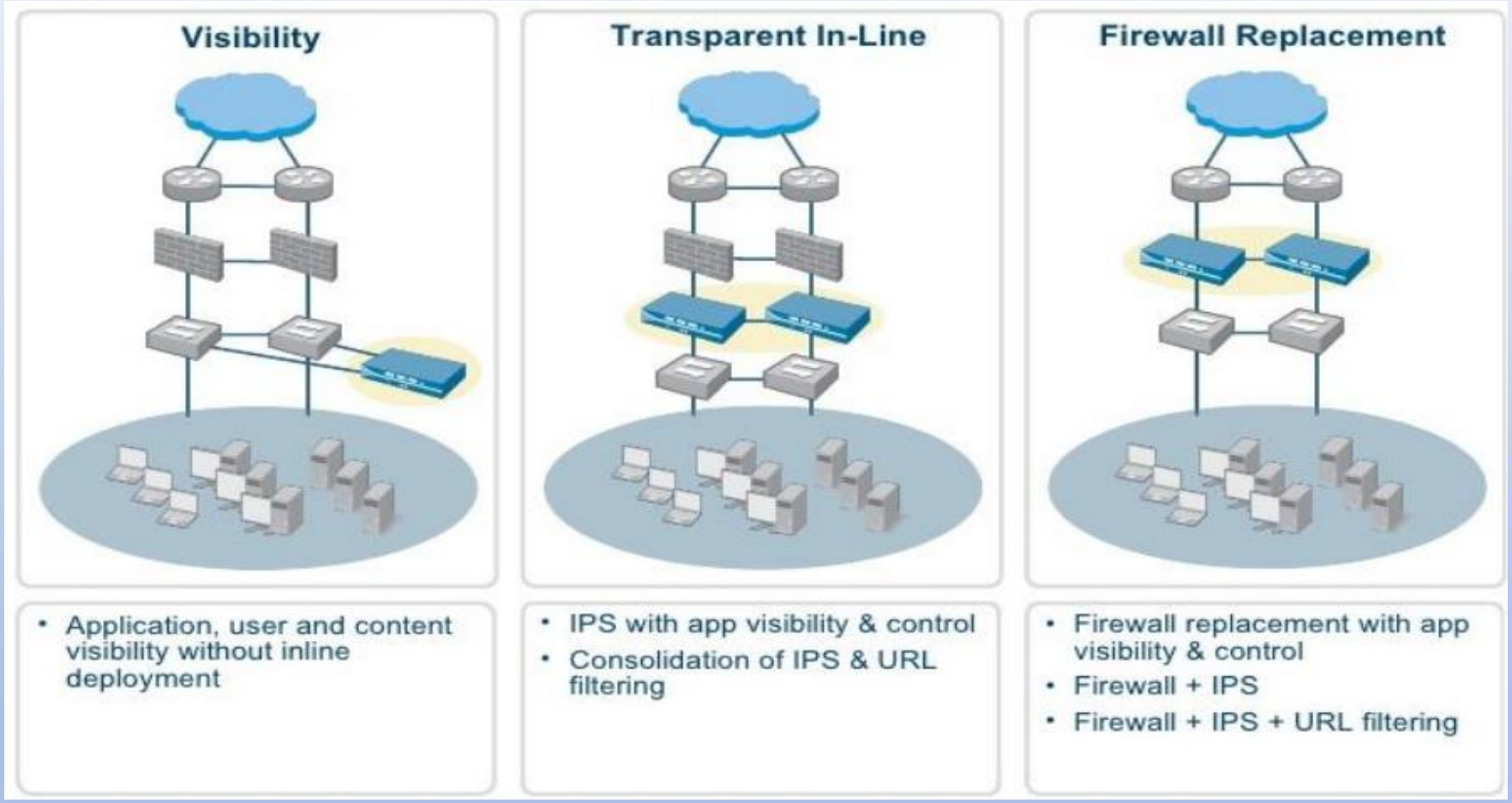


Configuring a Layer 3 Interface – IPv4

Network > Interfaces > Ethernet > <select_interface>



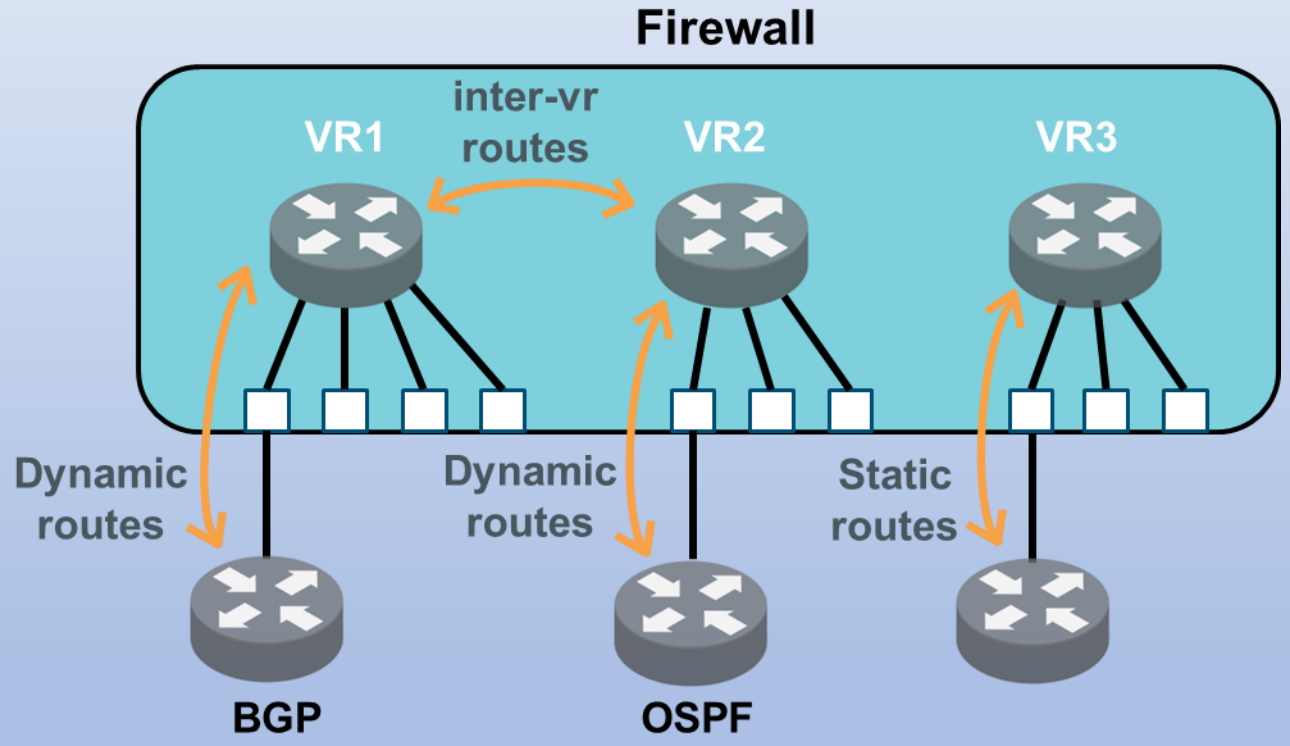
Deployment Options For Ethernet Interfaces



Virtual Routers

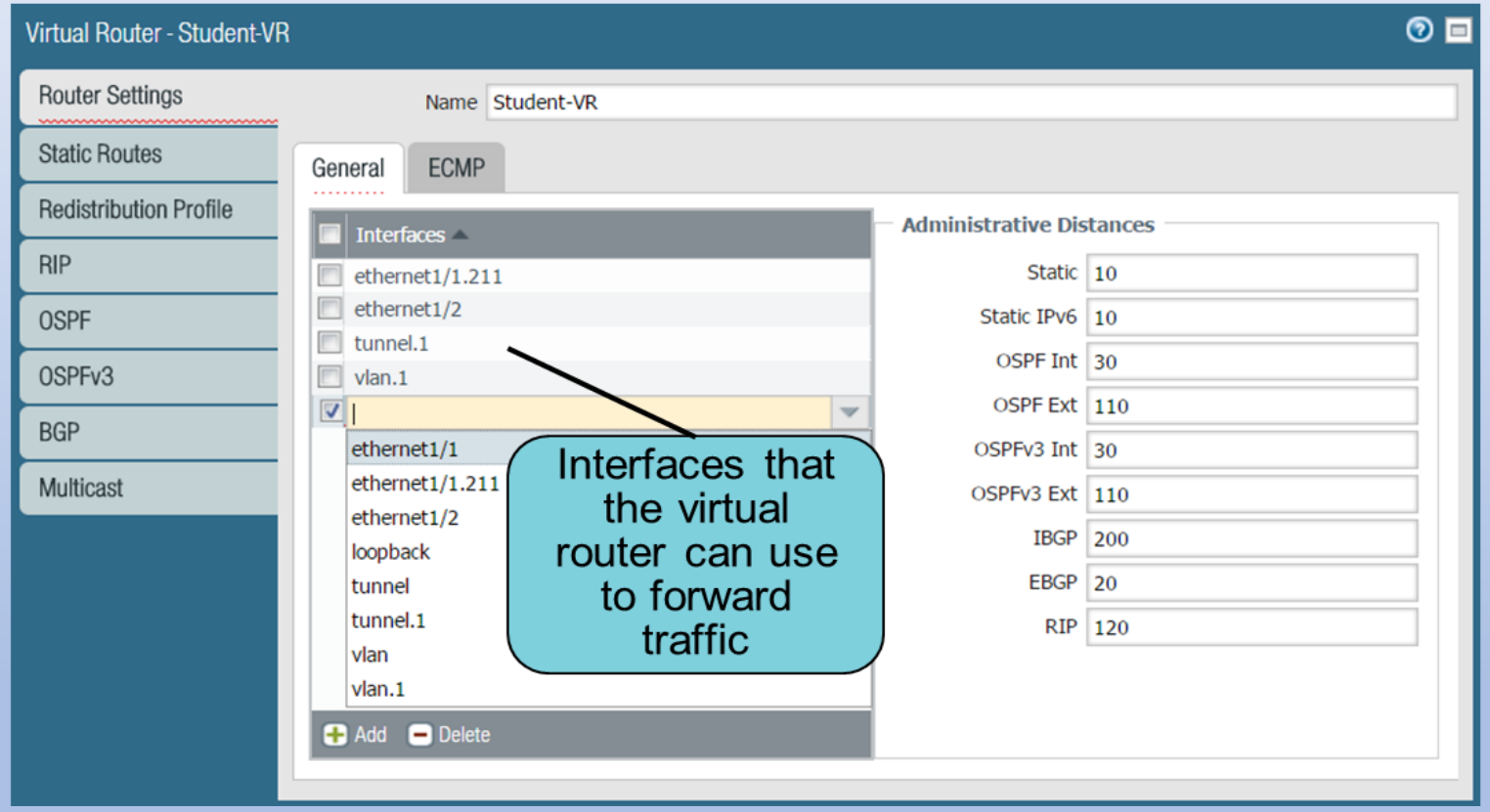
Virtual Routers

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



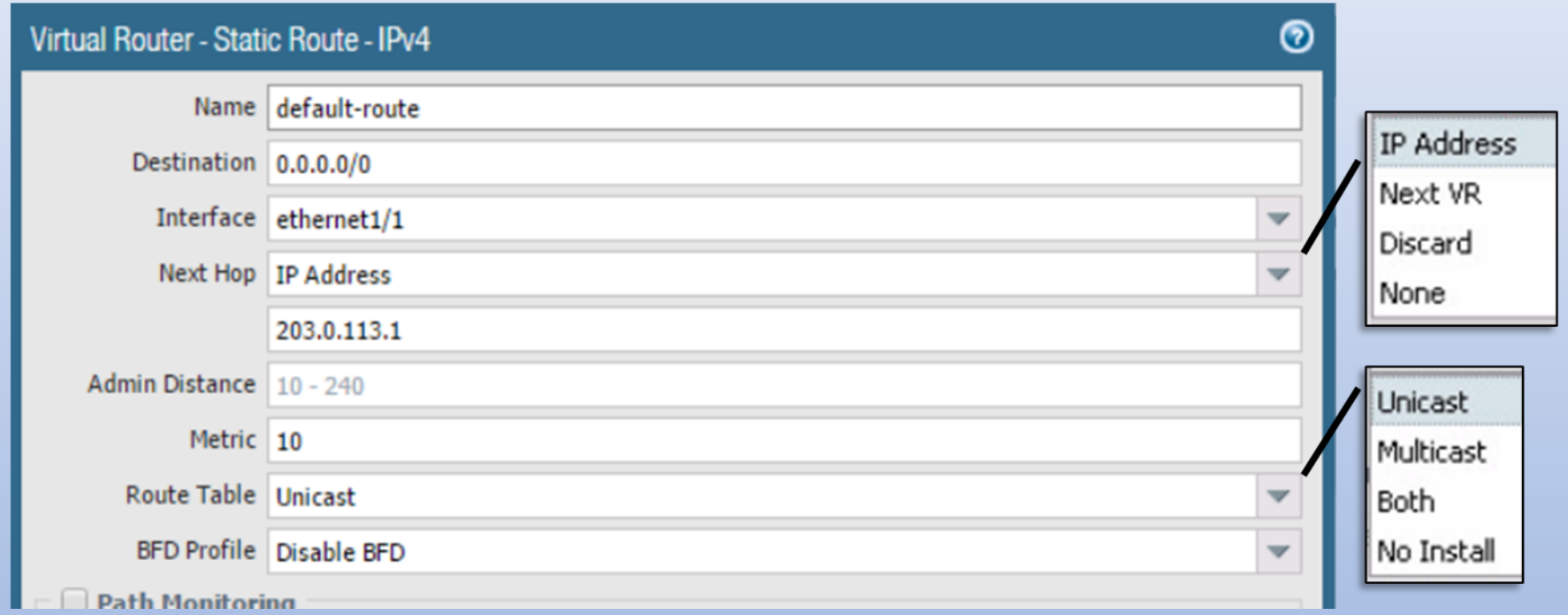
Virtual Router General Settings

Network > Virtual Routers

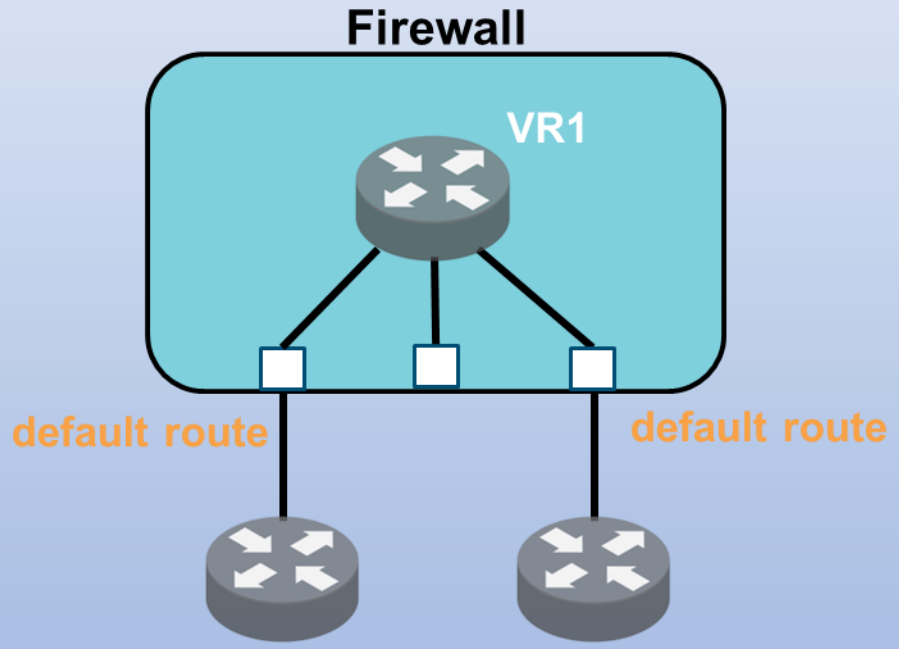


Adding a Static Default Route

Network > Virtual Routers > Static Routes > Add



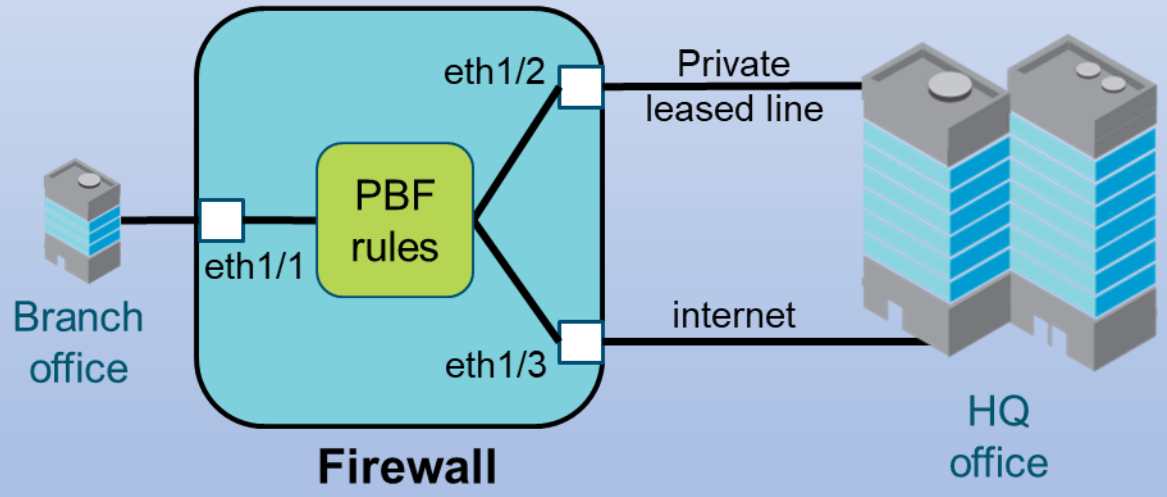
Multiple Static Default Routes



- 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

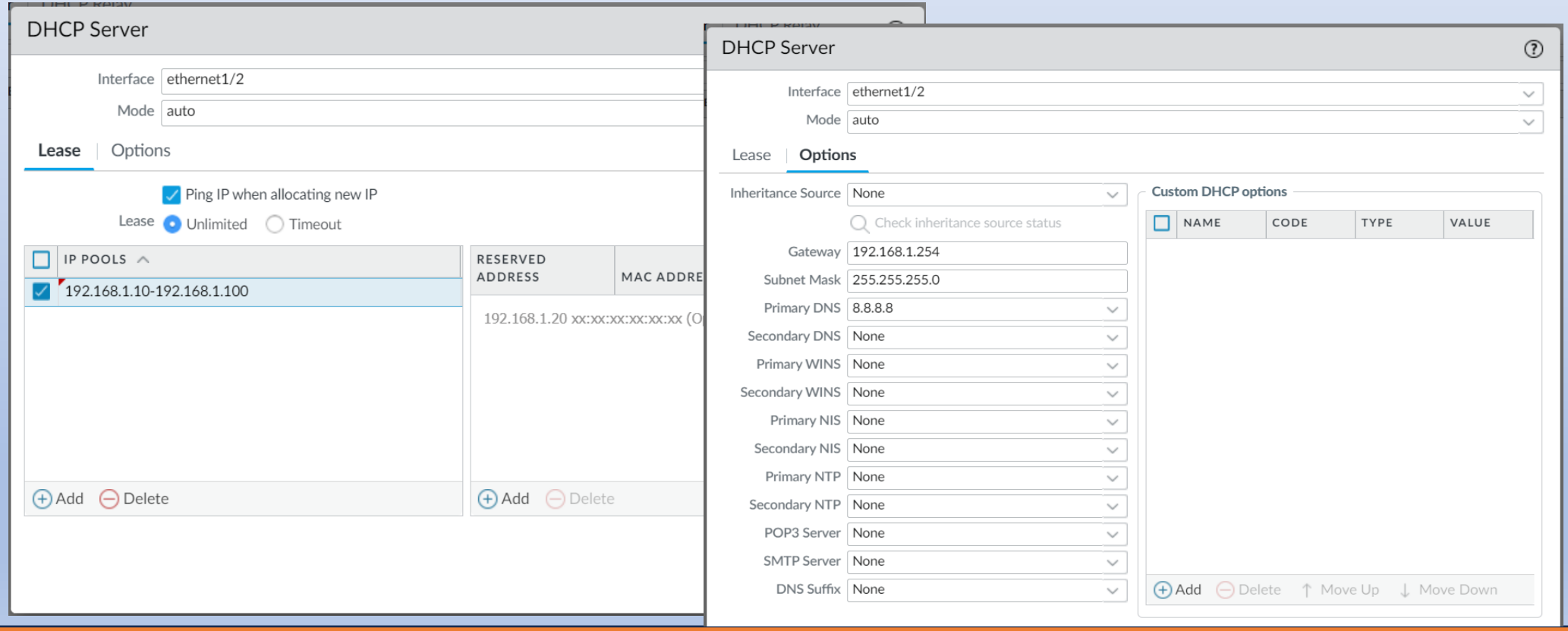
PBF Rules

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

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

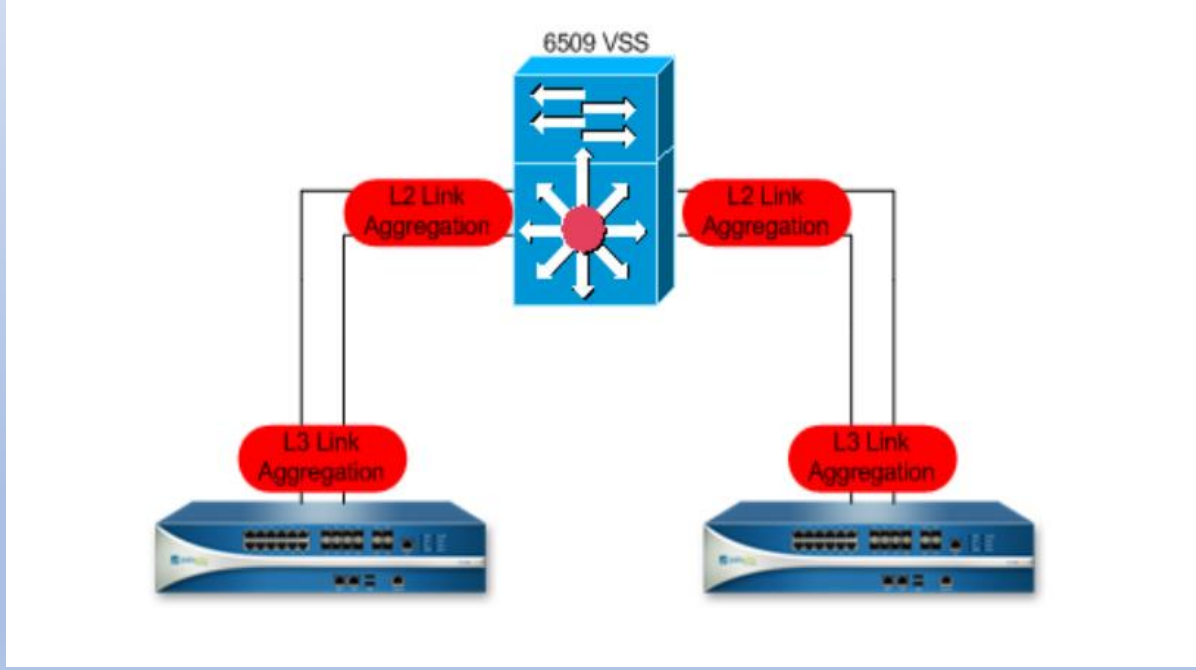
DHCP Server

- 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



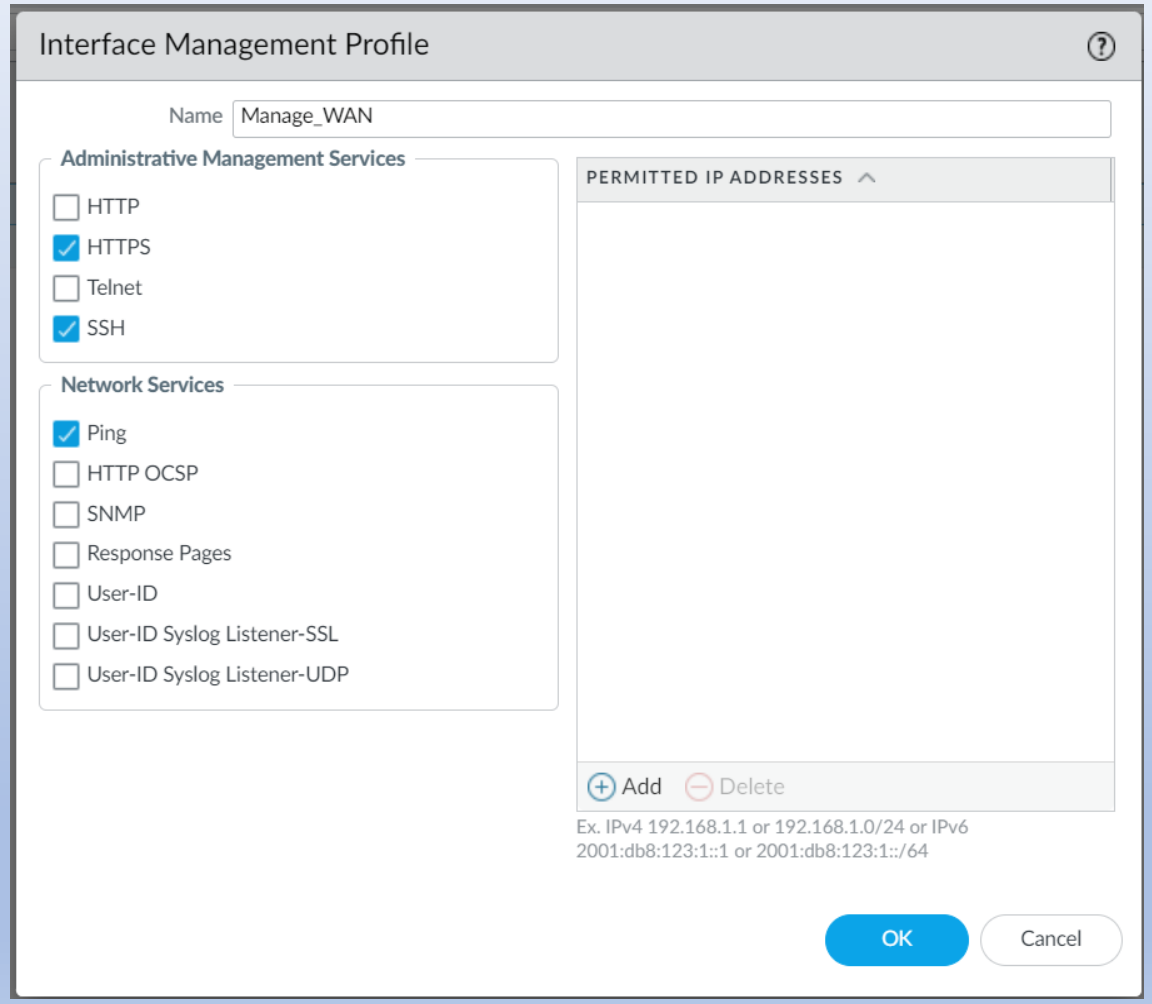
Aggregate Interfaces

- 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

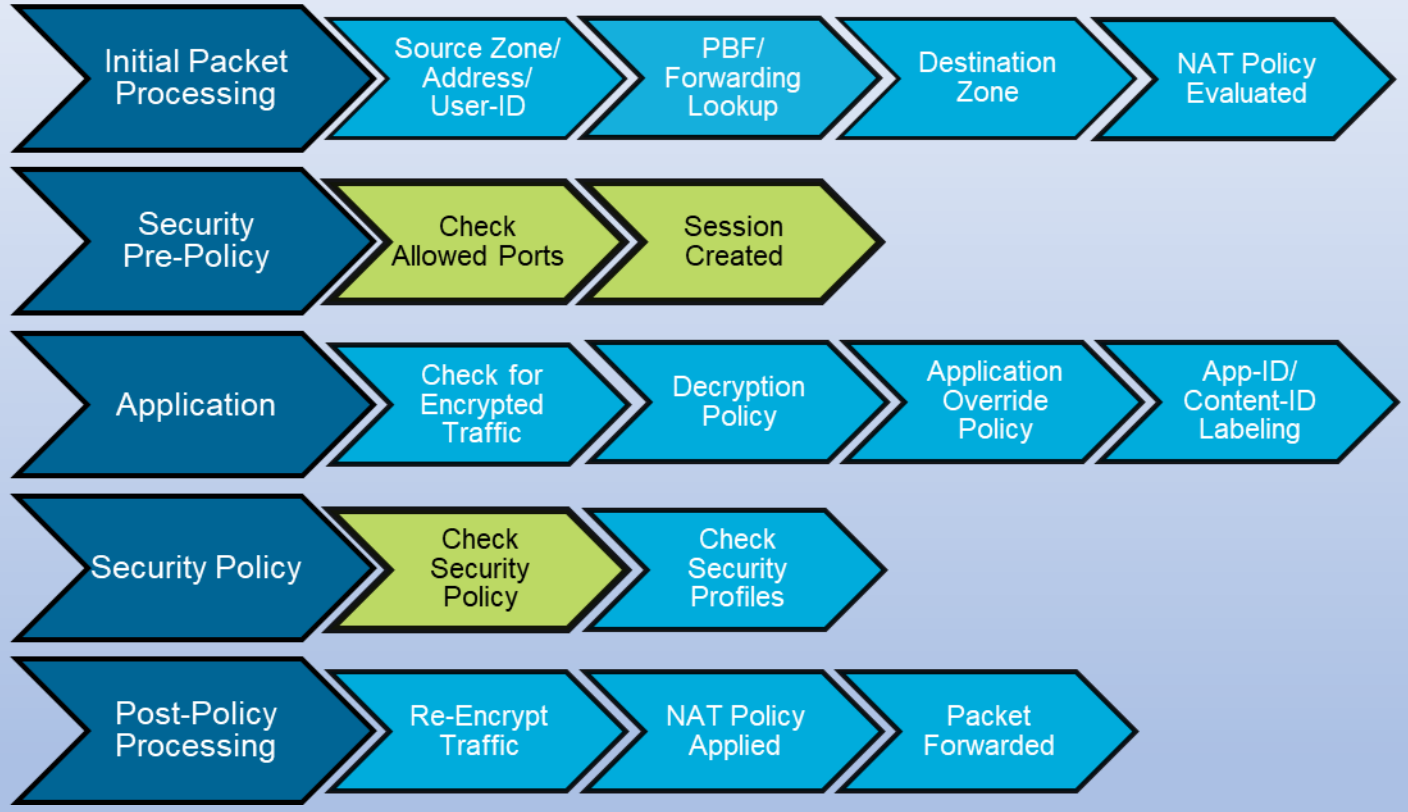
- Defines which management functions are allowed on a traffic interface
- Management Profiles are applied to Layer 3 Interfaces



4.
Security Policy and NAT Policies

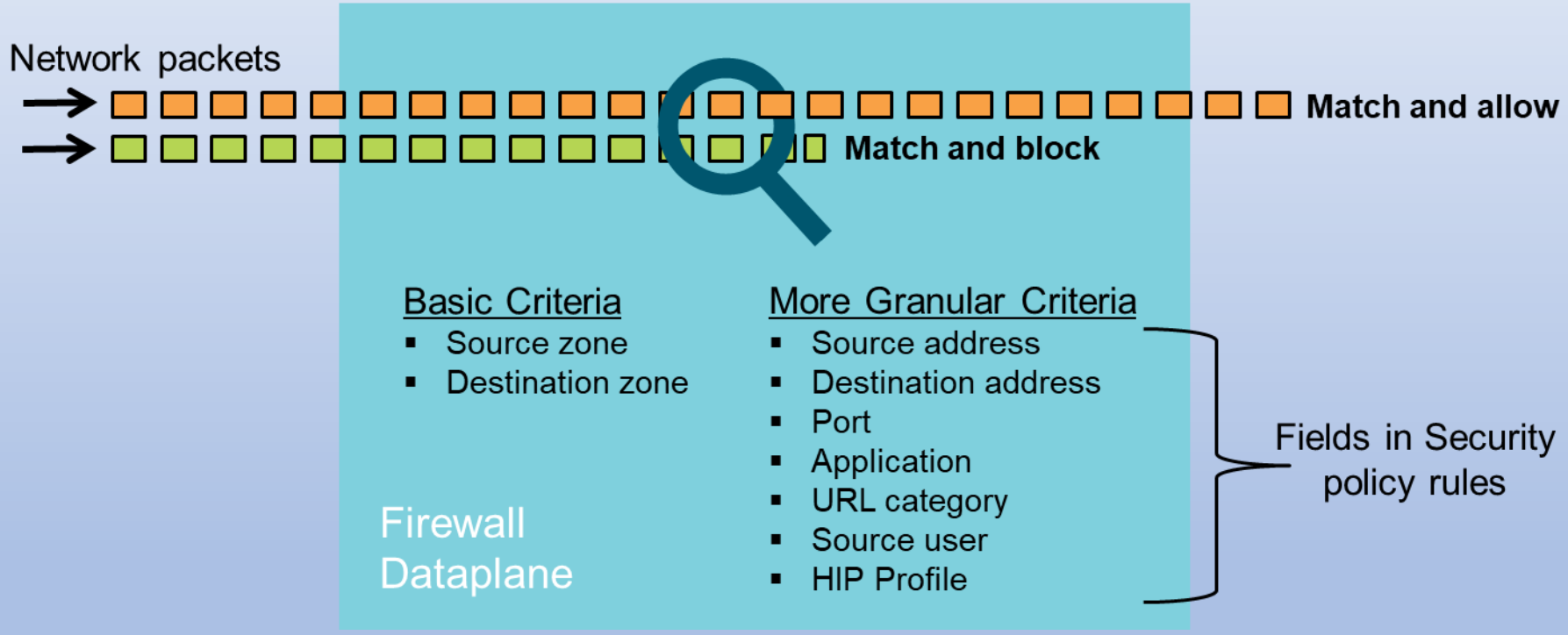
Security Policy Configuration

Flow Logic of the Next-Generation Firewall



Controlling Network Traffic

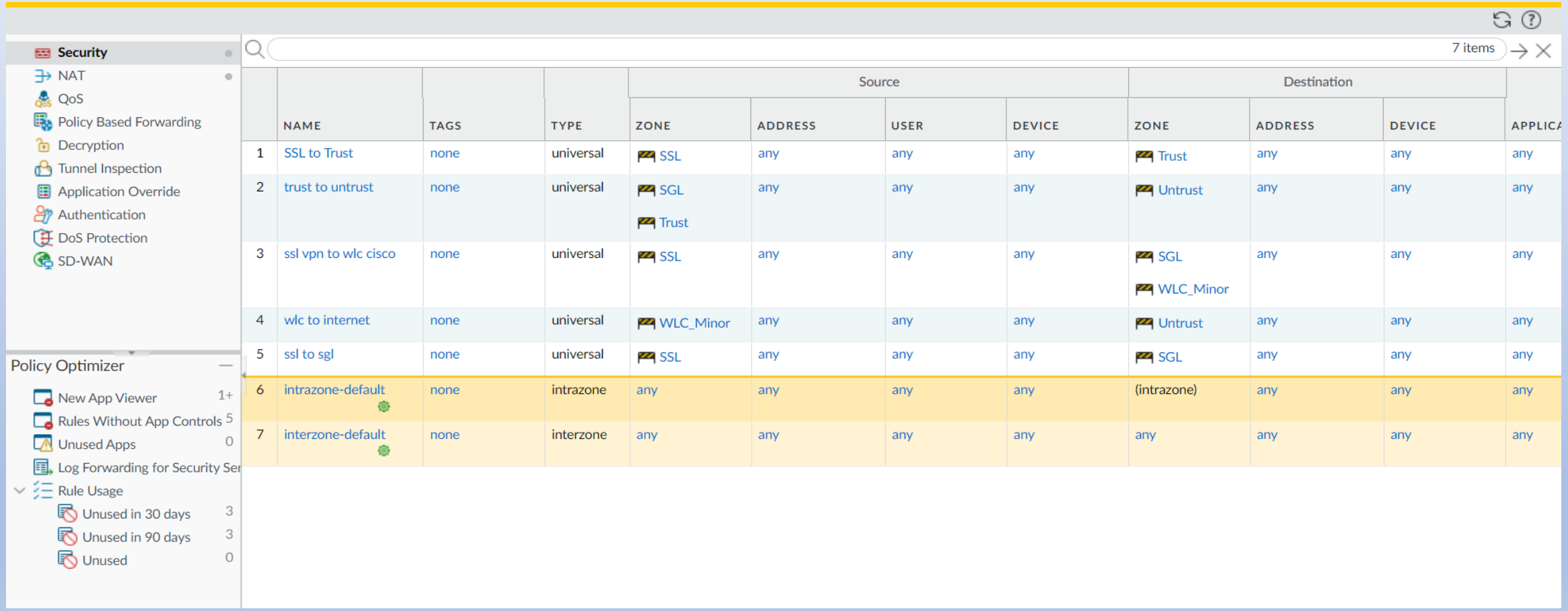
Multiple match criteria available to control network traffic



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



				Source				Destination			
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICA
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

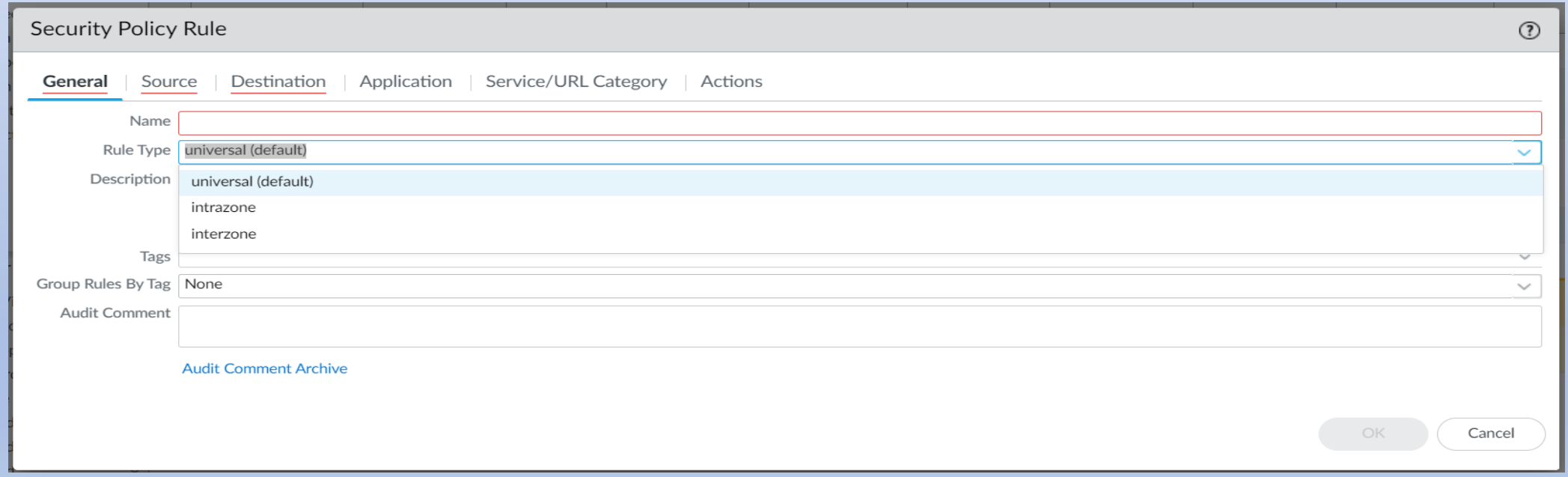
- Allowed by default

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 Zones Within a Policy

Security Policies are configured by Zone – Not by Interface!

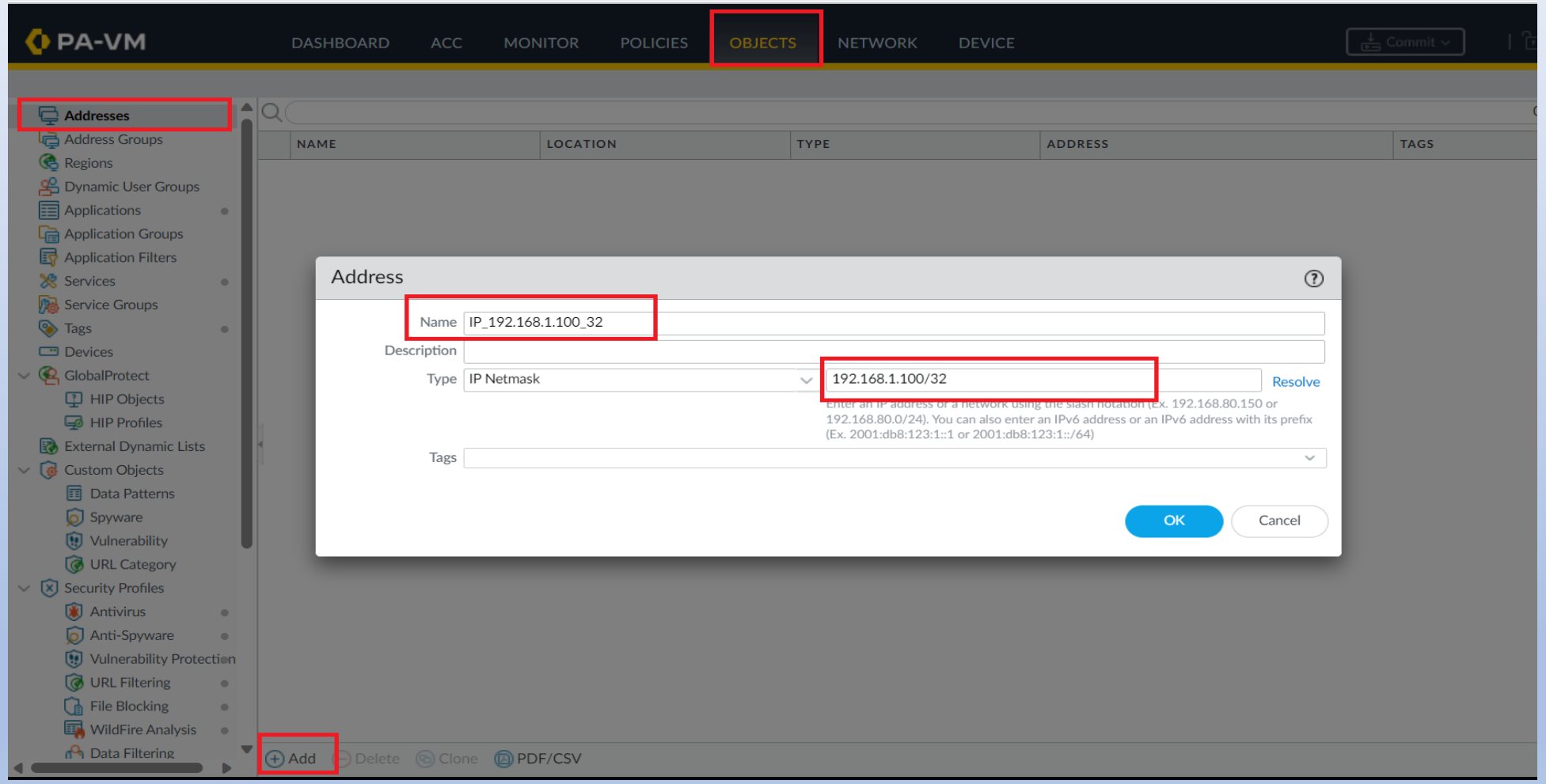
				Source				Destination			
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICA
1	SSL to Trust	none	universal	SSL	any	any	any	Trust	any	any	any
2	trust to untrust	none	universal	SGL Trust	any	any	any	Untrust	any	any	any
3	ssl vpn to wlc cisco	none	universal	SSL	any	any	any	SGL WLC_Minor	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:

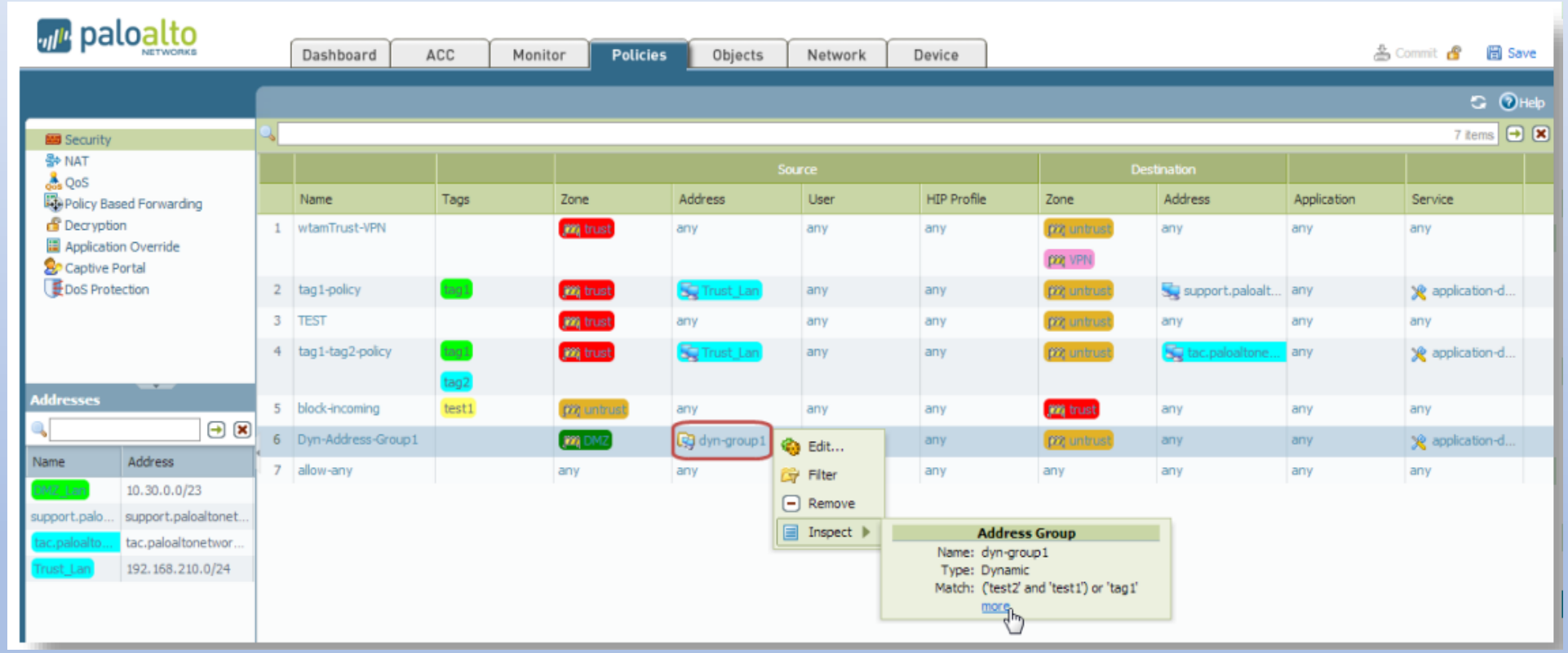
- IP Netmask
- IP Range
- FQDN



Apply to Policy

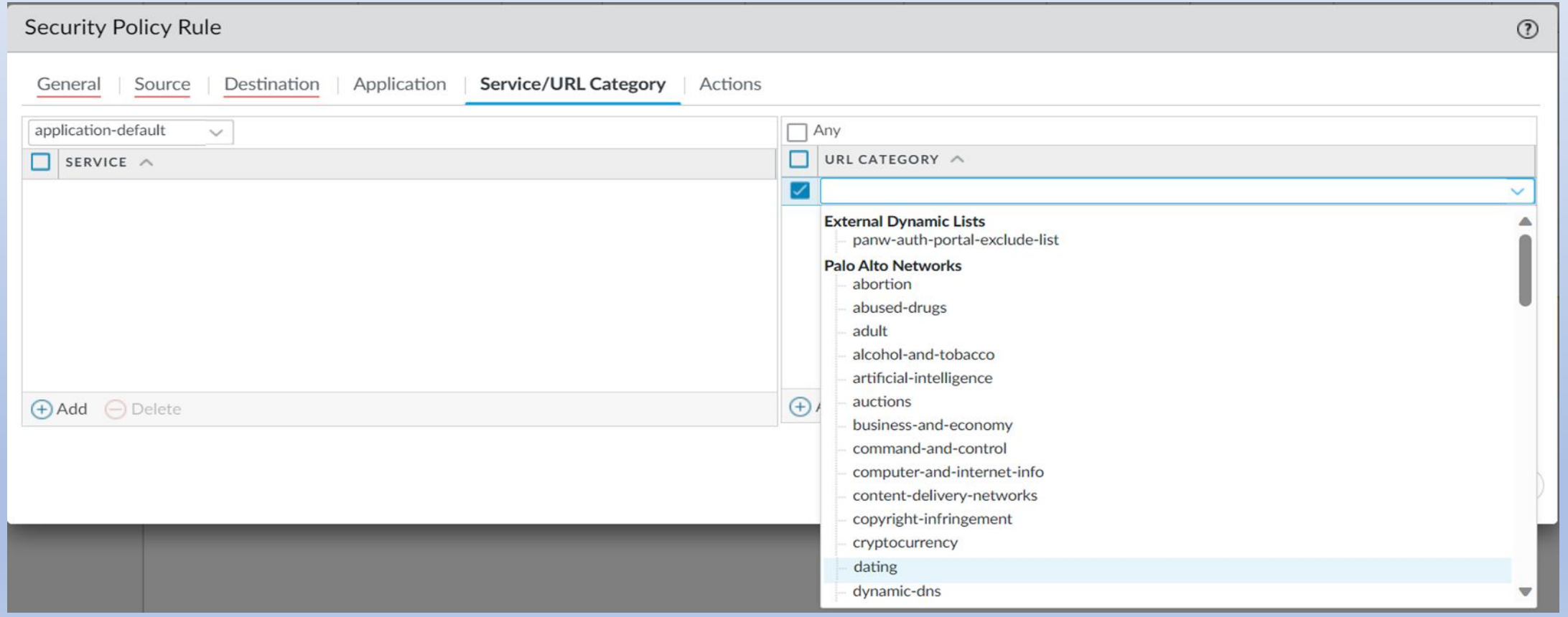
Apply group in policy same as any other address group and commit

- Can drill down and click more to see registered IPs



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 Zone Rule – Enable Logging

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

- Intrazone-Default
- Interzone-Default

“Override” to configure additional settings

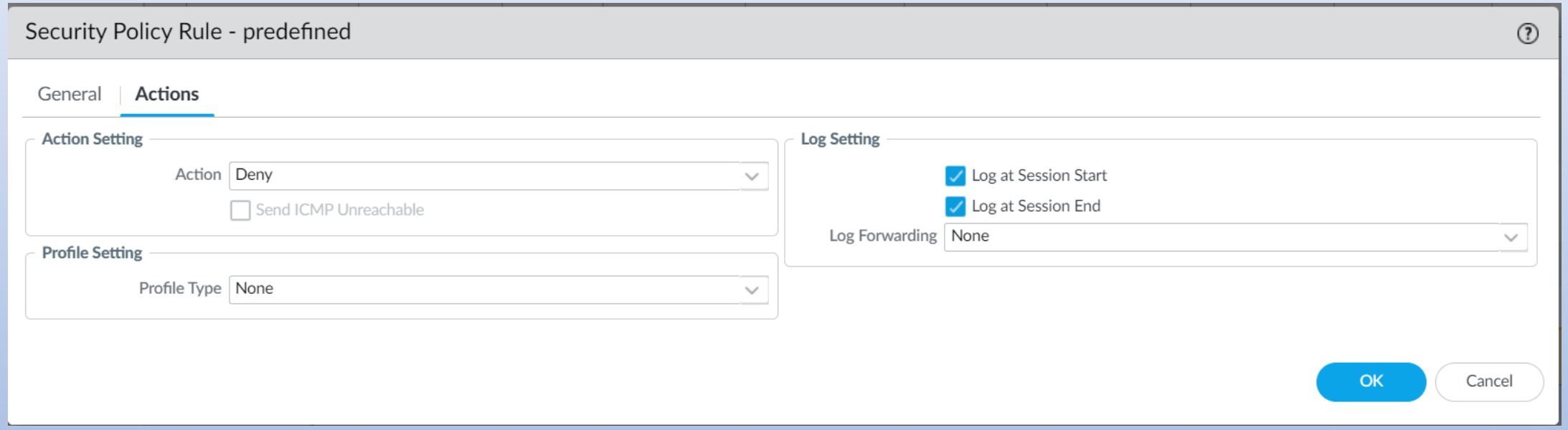
				Source				Destination			
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICA
1	SSL to Trust	none	universal	SSL	any	any	any	Trust	any	any	any
2	trust to untrust	none	universal	SGL Trust	any	any	any	Untrust	any	any	any
3	ssl vpn to wlc cisco	none	universal	SSL	any	any	any	SGL WLC_Minor	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

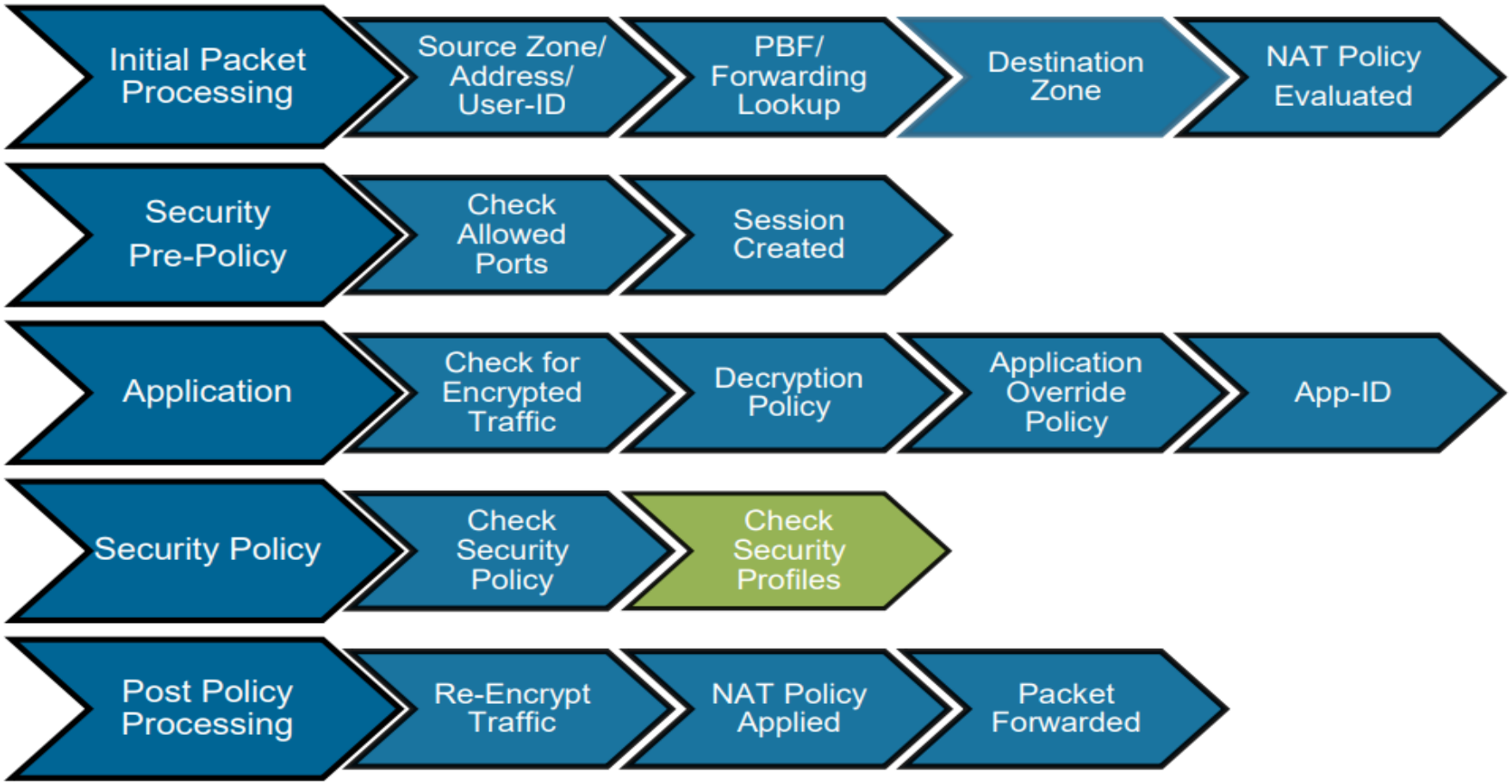
Two pre-defined default rules and both are “Read Only”.

- Intrazone-Default
- Interzone-Default

“Override” to configure additional settings



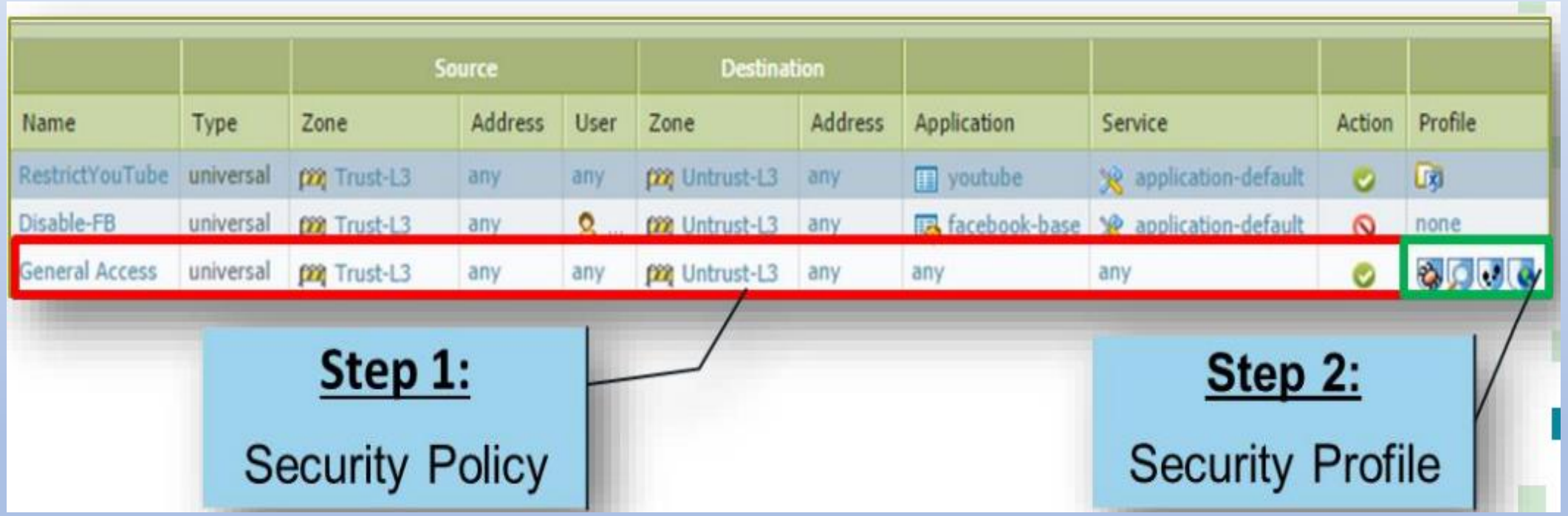
Flow Logic of the Next-Generation Firewall



Security Profiles

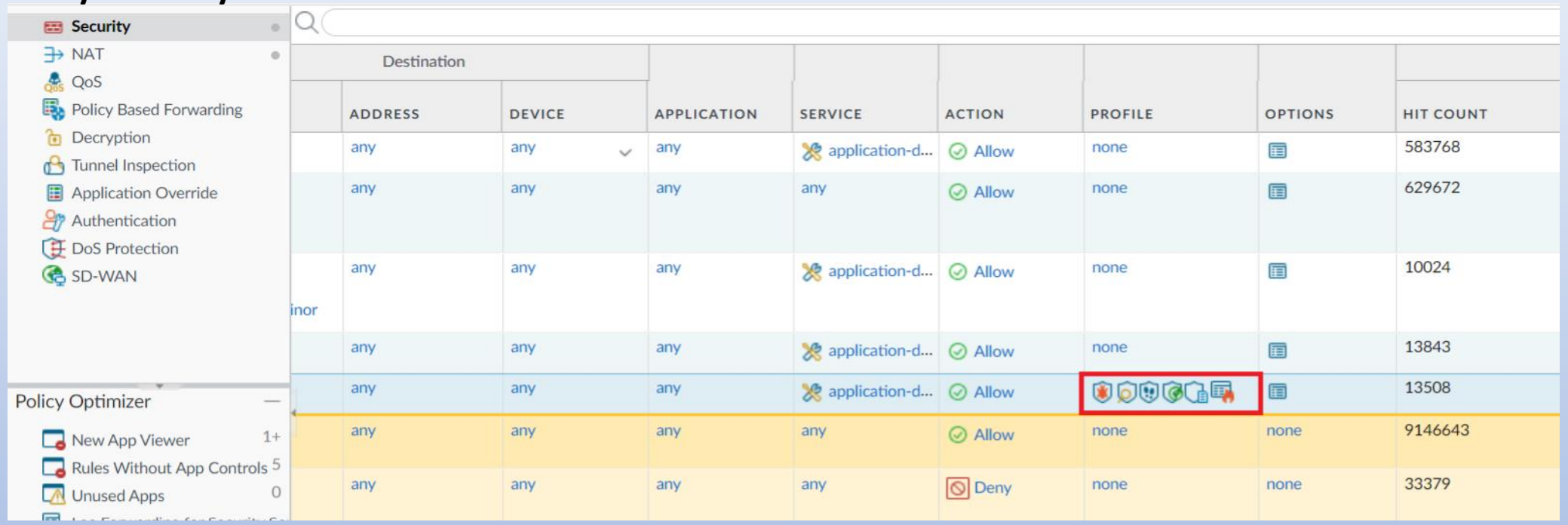
Policies are processed in two steps: Check to see if traffic matches the Security Policy

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



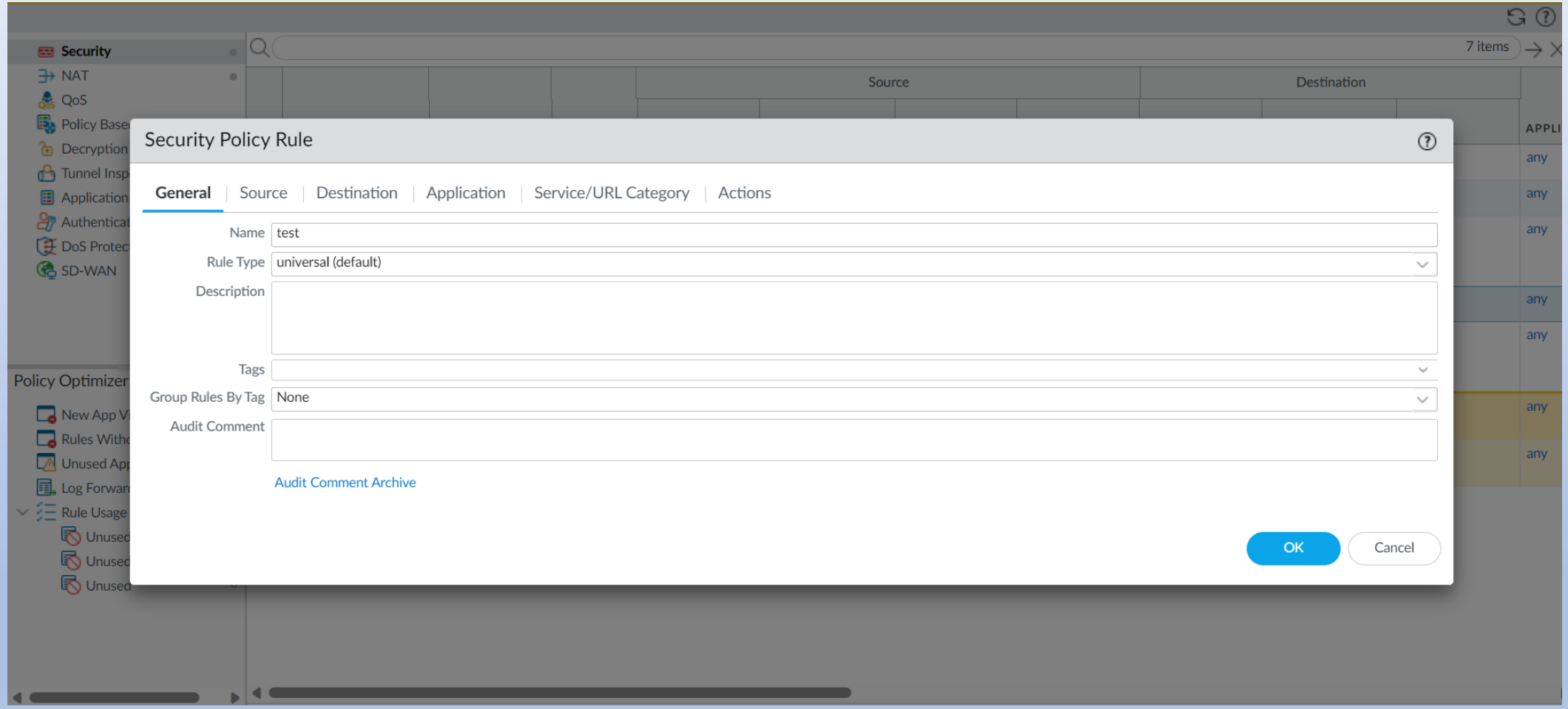
Security Profile Types

Policy>Security Profile



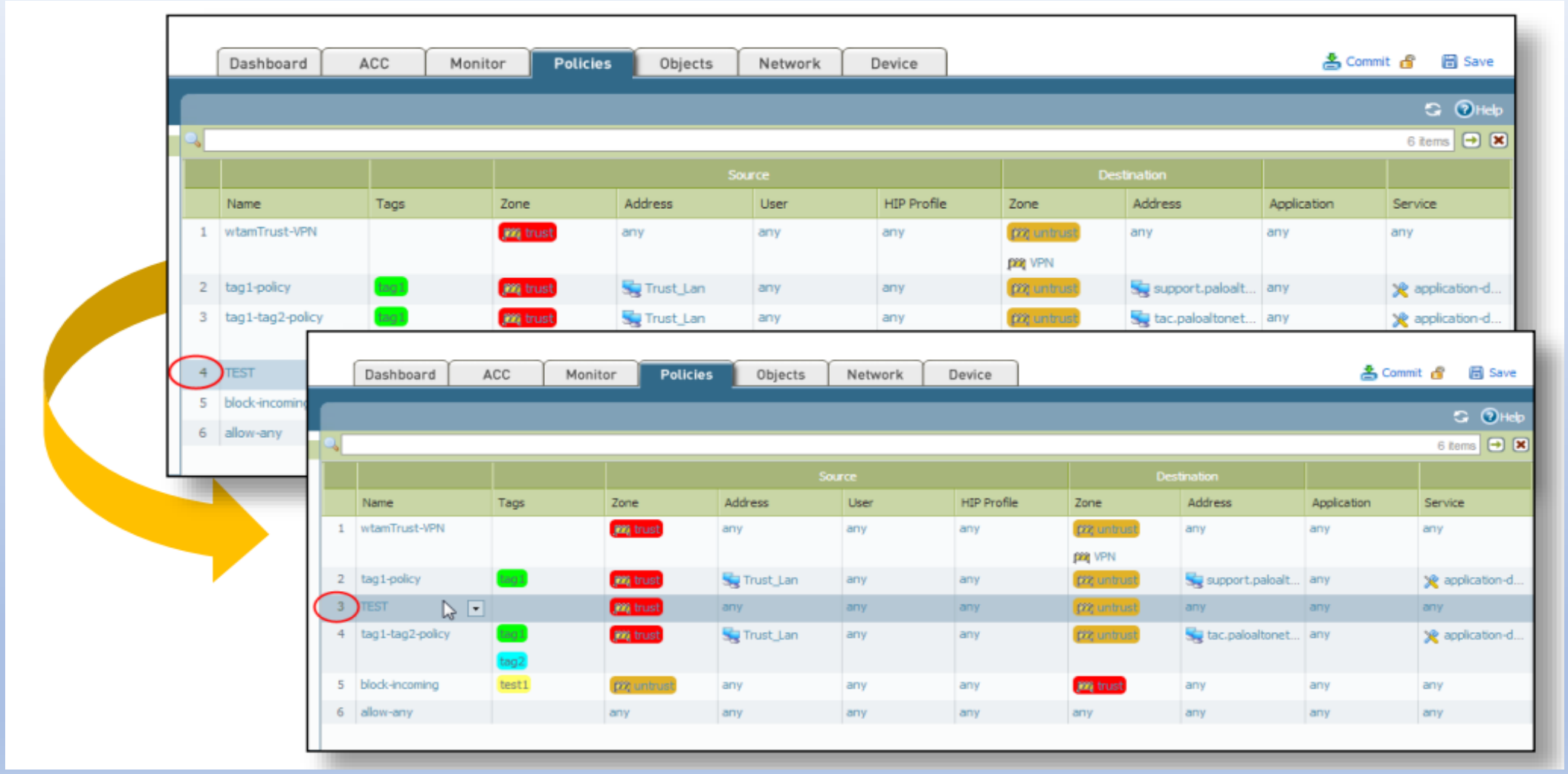
Security Policy Administration

Creating Security Policy Rules – General Tab



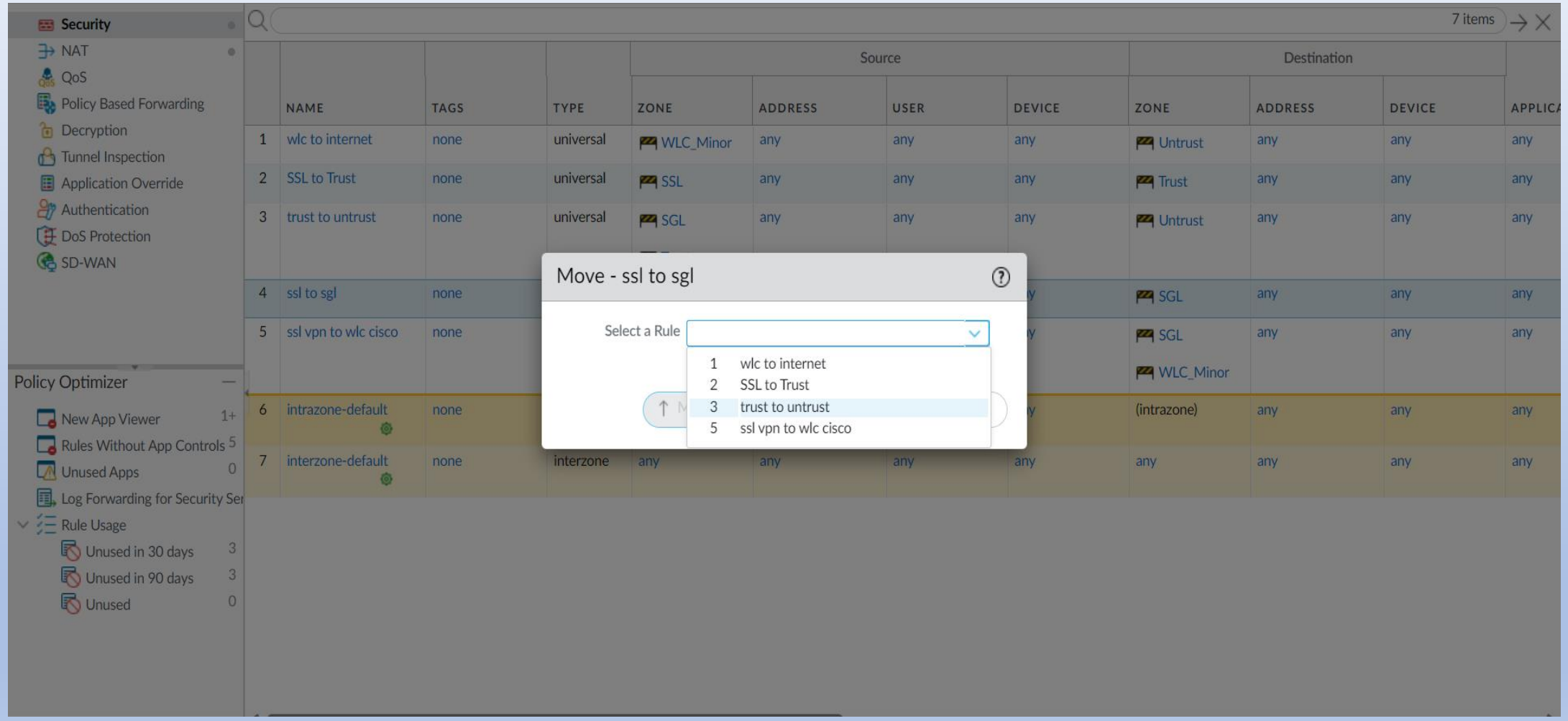
Re-Ordering Rules

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



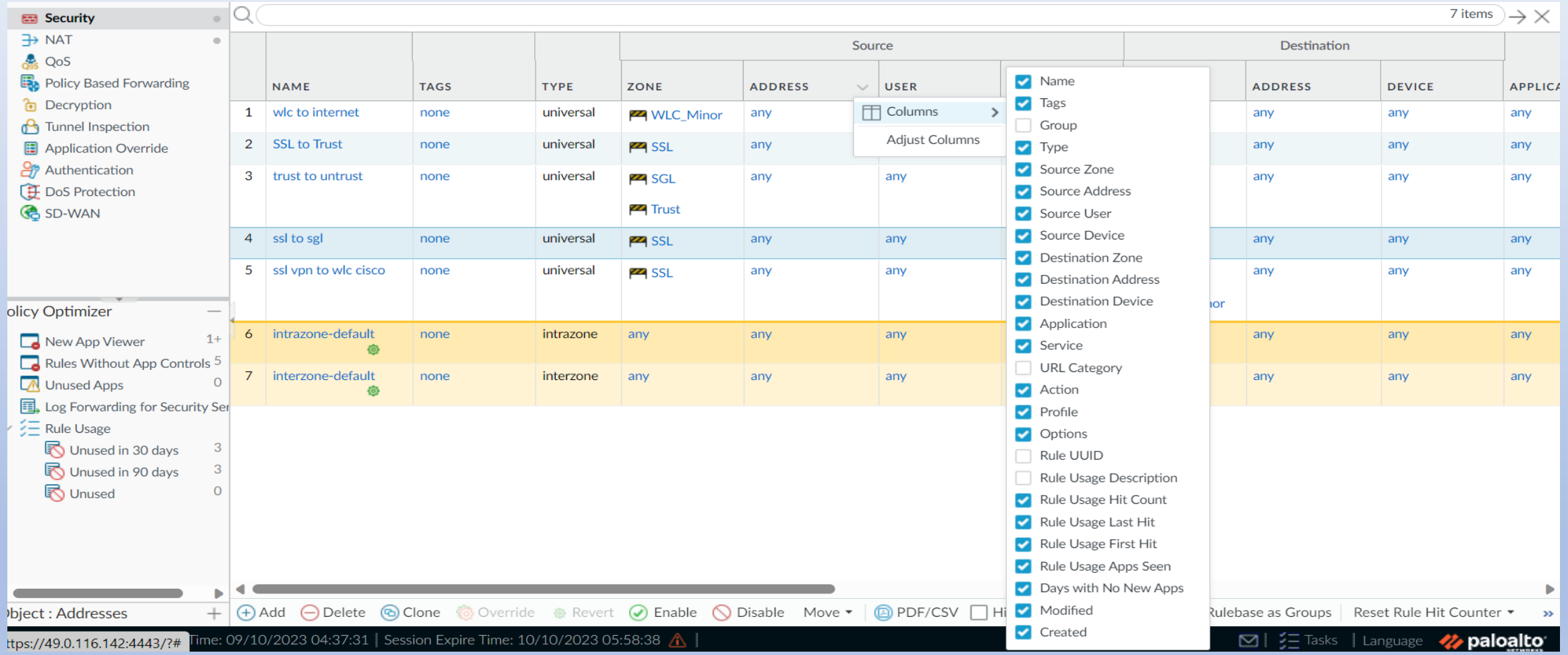
Moving Rules Another Way

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



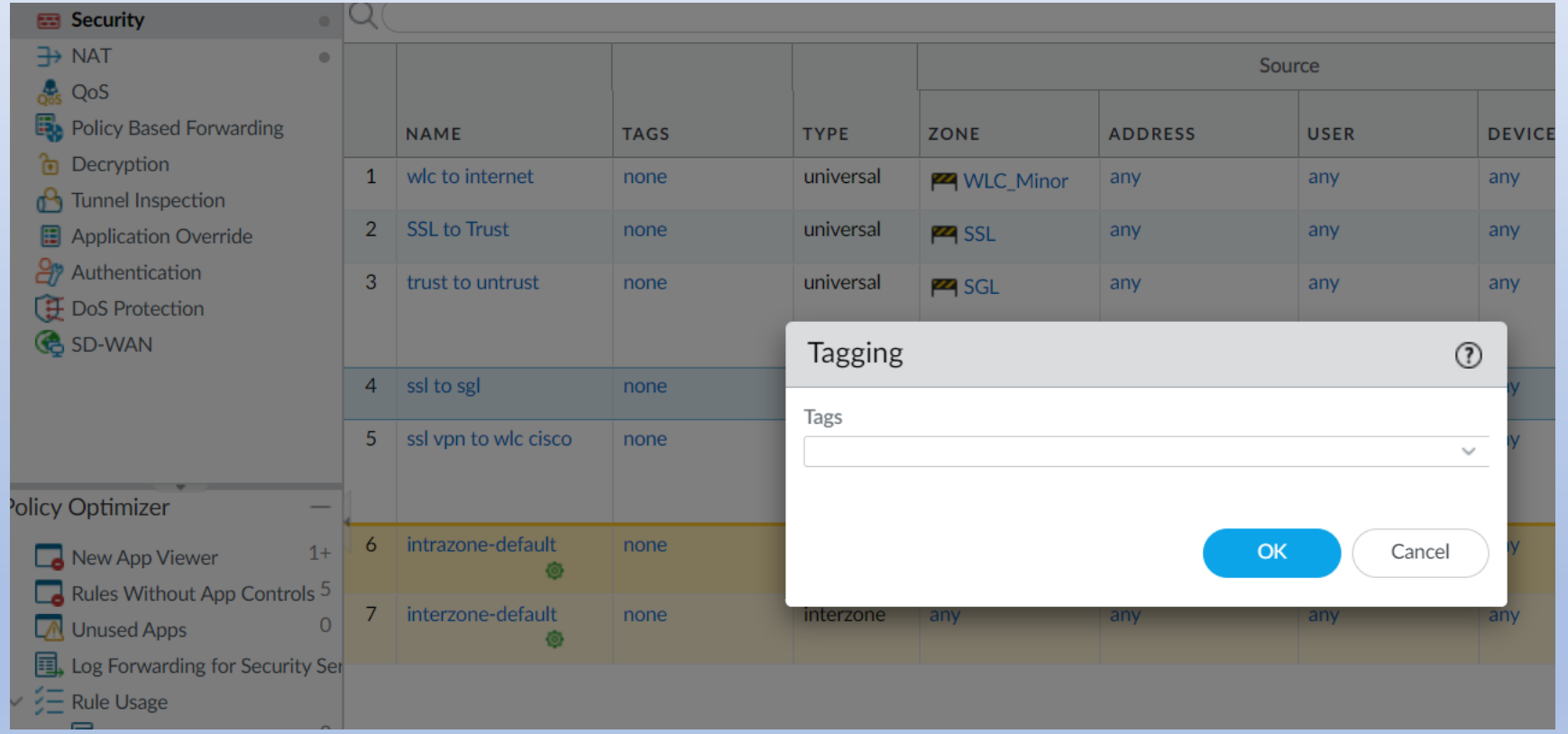
Displaying Policy Columns

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



Security Policy Admin Tags

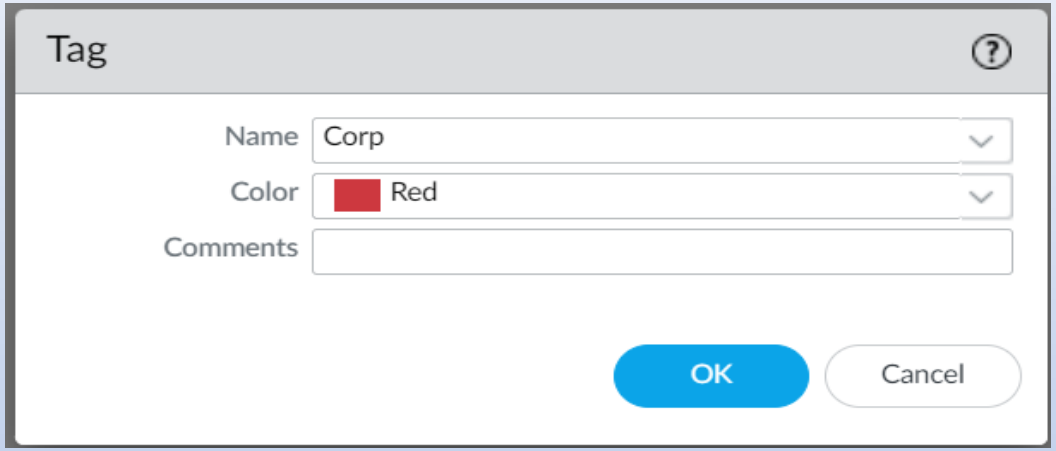
- You can now tag objects and add color to the tag in order to visually distinguish tagged objects.
- Tags can be added to the following objects: Address Objects, Address Groups, Zones, Service Groups, and Policy Rules



Creating Color Coded Tags

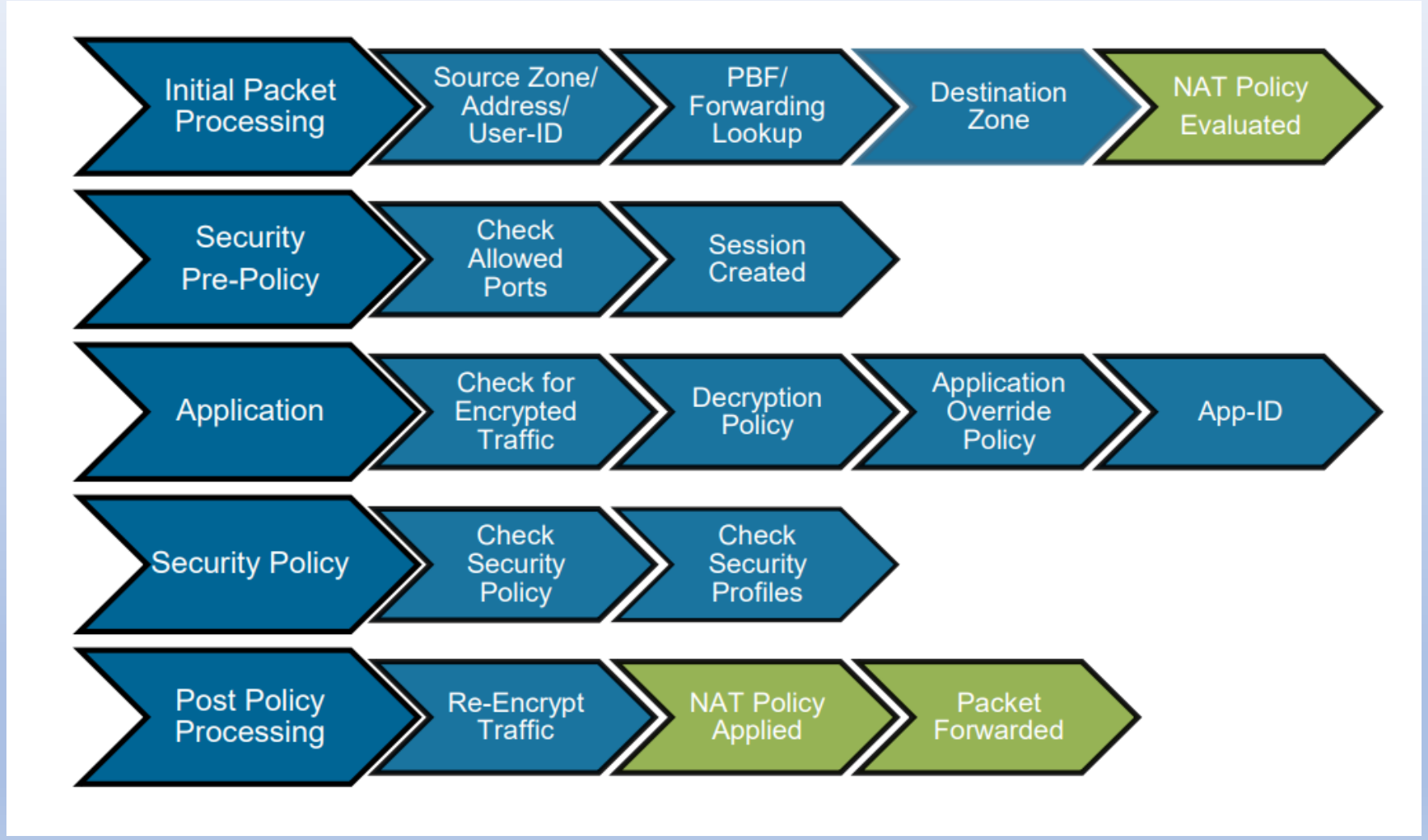
Apply to:

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



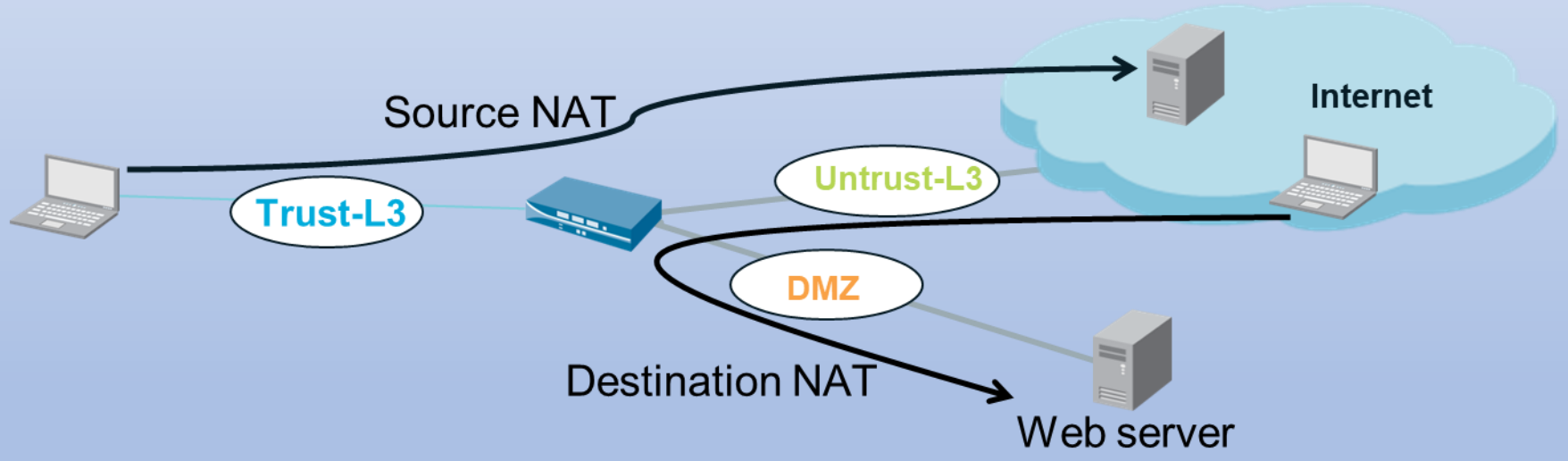
Network Address Translation (NAT)

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

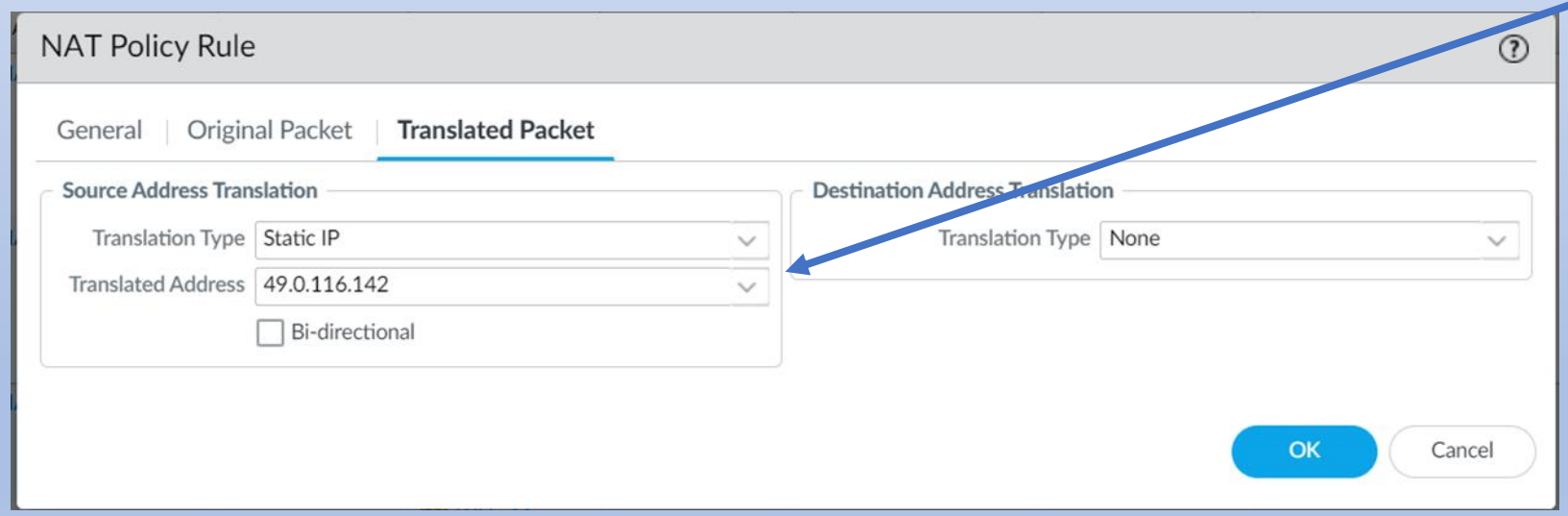
Source NAT Types

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

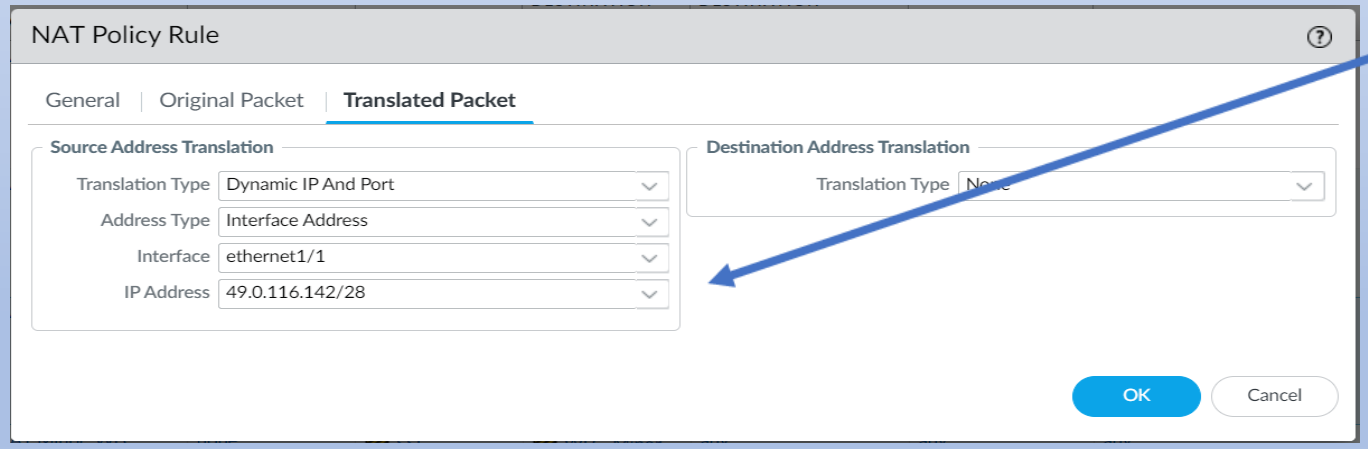


Source NAT Types

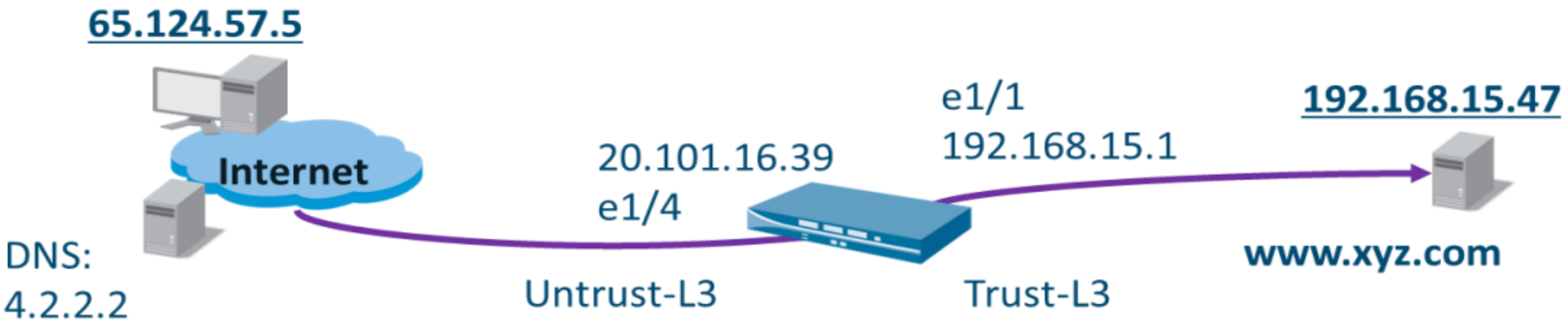
Dynamic IP/Port

- 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



Source	Destination
65.124.57.5	20.101.16.39
Untrust-L3	Untrust-L3

Destination NAT

20.101.16.39 > 192.168.15.47

Source	Destination
65.124.57.5	192.168.15.47
Untrust-L3	Trust-L3

Destination NAT Example Policies

Pre-NAT

Pre-NAT

Post-NAT

Policies > NAT

			Original Packet						Translated 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

Pre-NAT

Post-NAT

Pre-NAT

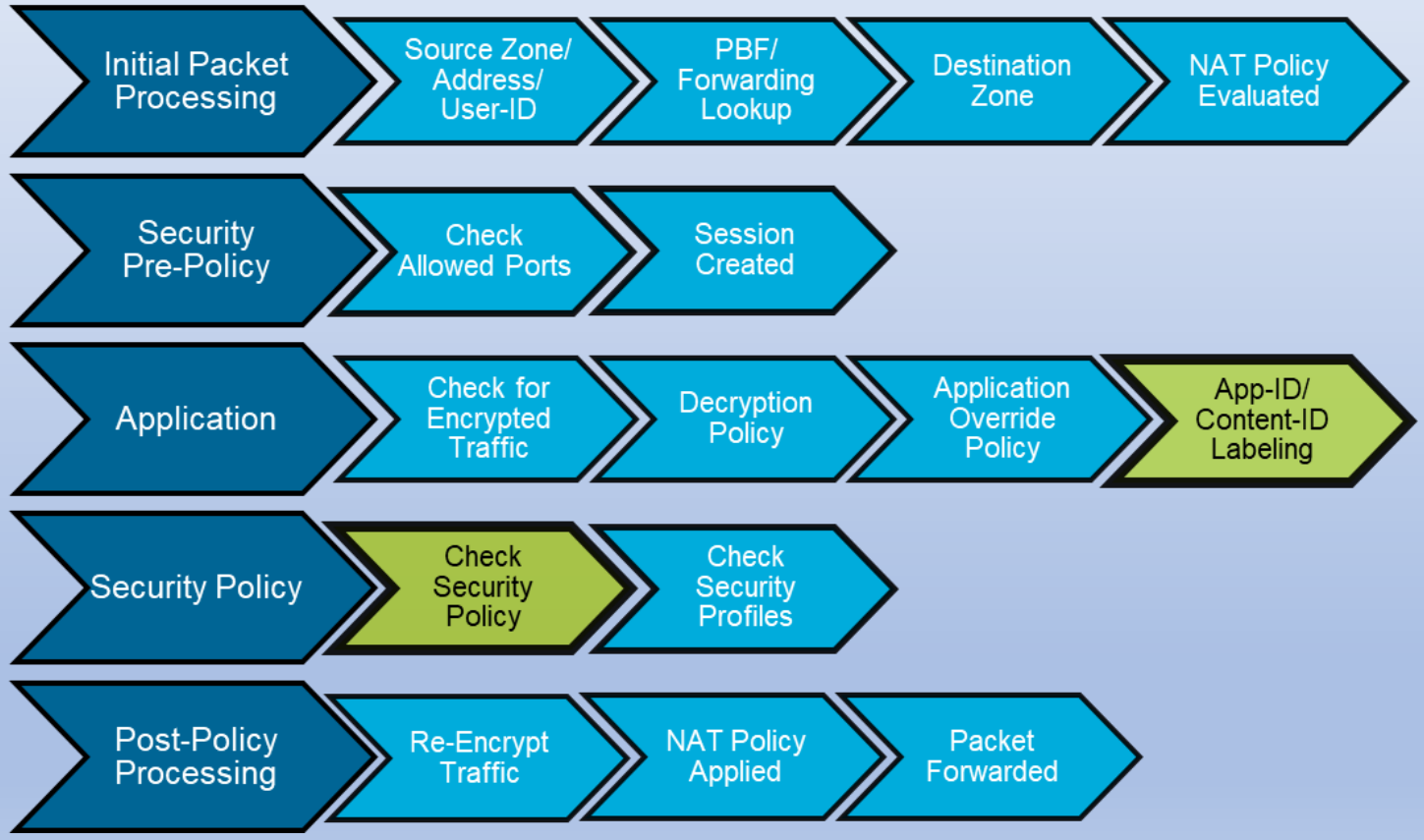
Policies > Security

				Source		Destination				
	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	

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

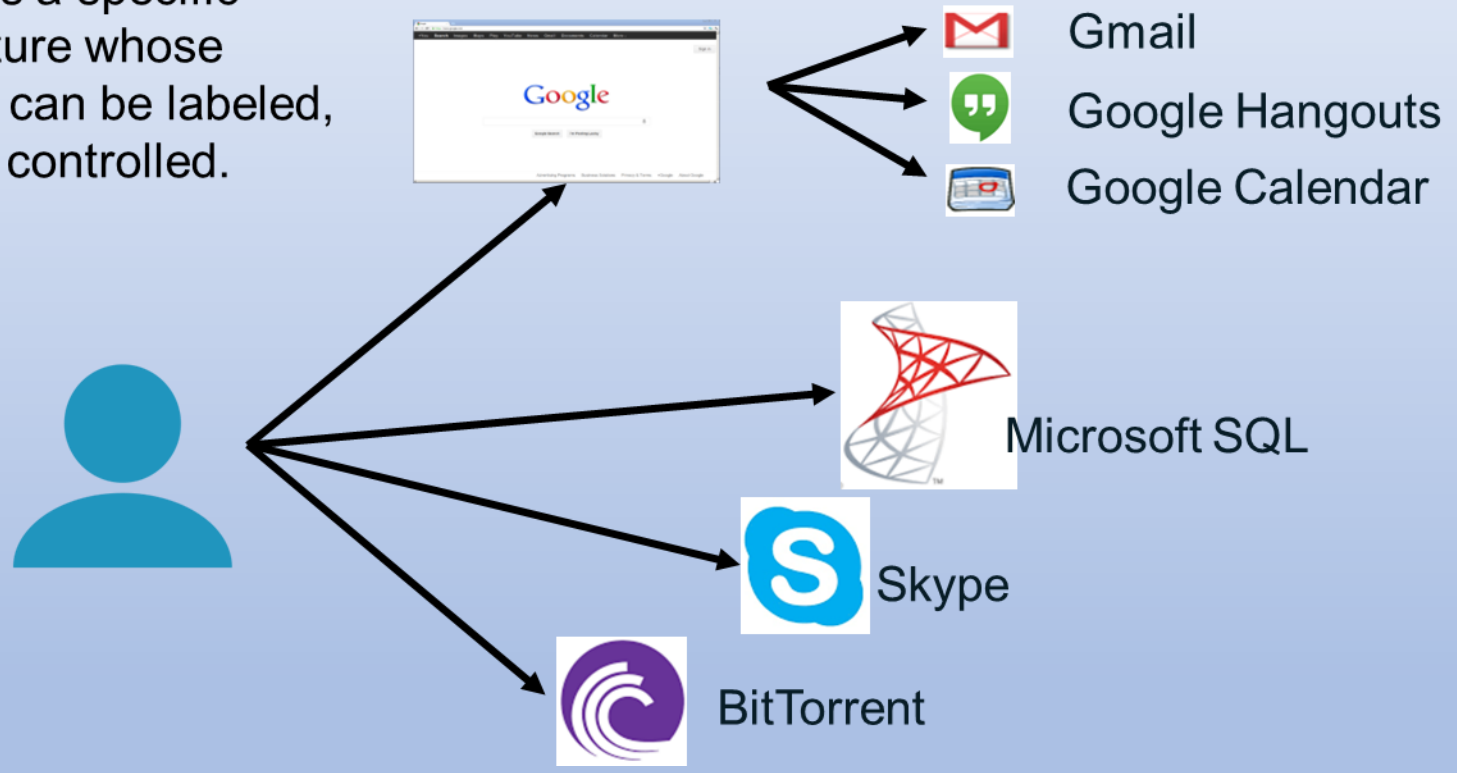
App-ID

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

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

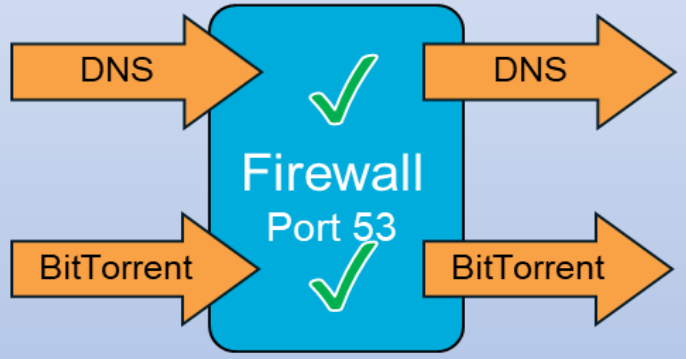
Application-based security rule

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

Port-Based Versus Next-Generation Firewalls

Traditional Firewalls

Firewall Rule: ALLOW Port 53



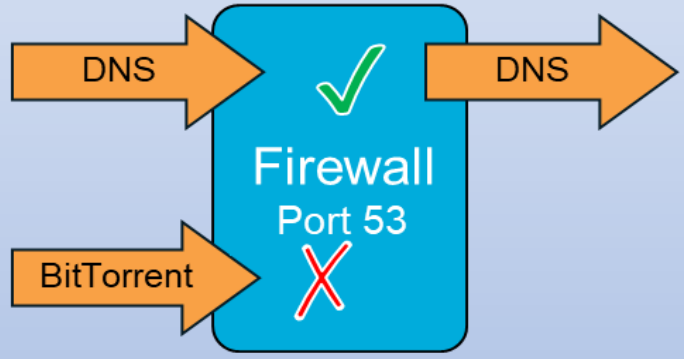
Packet on port 53: Allow

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

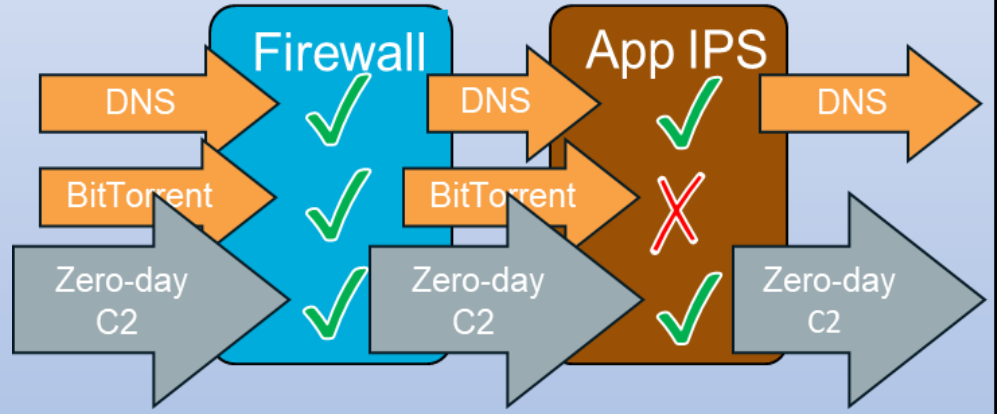
Visibility: BitTorrent detected and blocked

Zero-Day Malware – IPS Versus App-ID

Legacy Firewalls

Firewall Rule: ALLOW Port 53

Application IPS Rule: Block BitTorrent



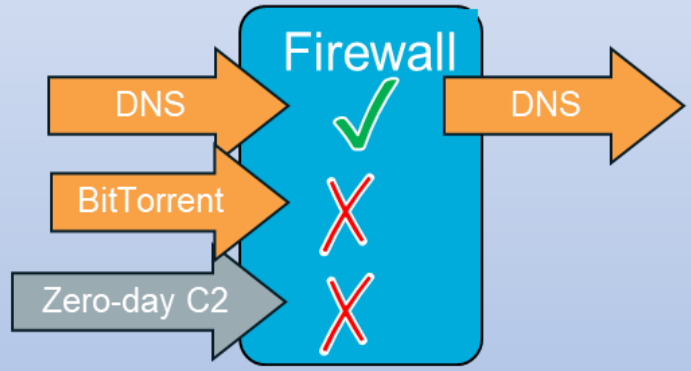
Packet on port 53: Allow

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

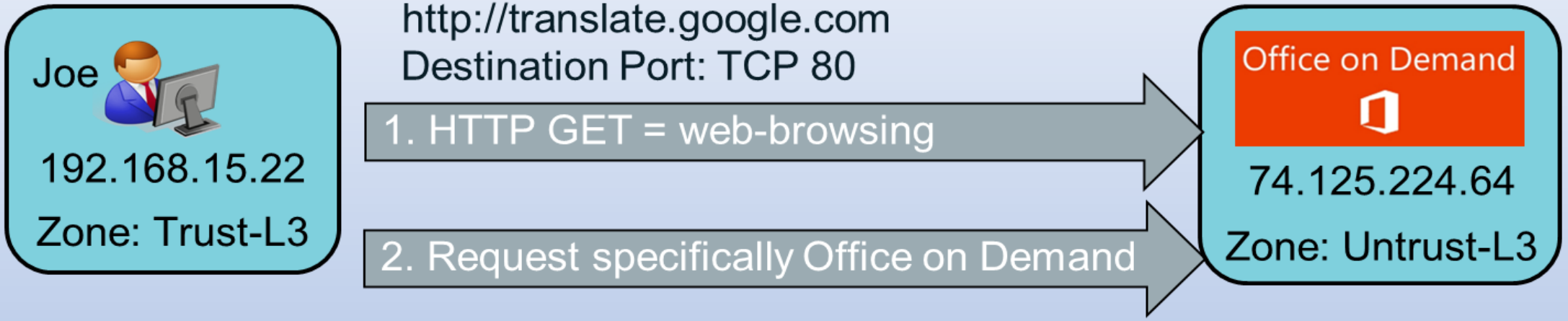
Policies > Decryption

		Source			Destination						
	Name	Zone	Address	User	Zone	Address	URL Category	Service	Action	Type	Decryption Profile
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
5	Decrypt All Traffic	Trust-L3	any	any	UnTrust-L3	any	any	service-https	decrypt	ssl-forward-proxy	Tight SSL Control

Use multiple match criteria (not just URL categories) to refine decrypt rules

Using App-ID in a Security Policy

Dependent Applications



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

Application shift

office-on-demand dependent on ms-office365-base and sharepoint-online

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

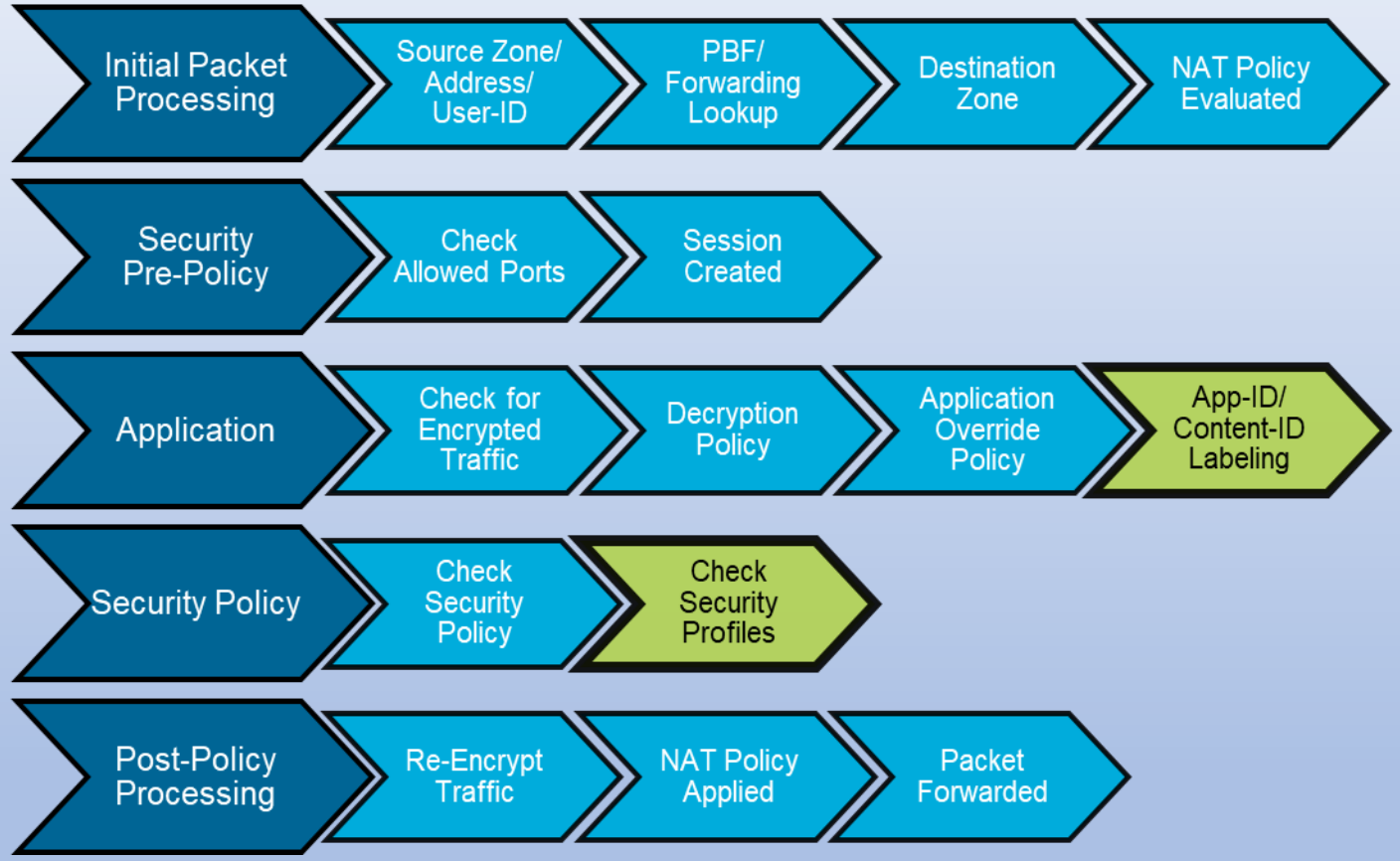
Application group

Application

Content-ID

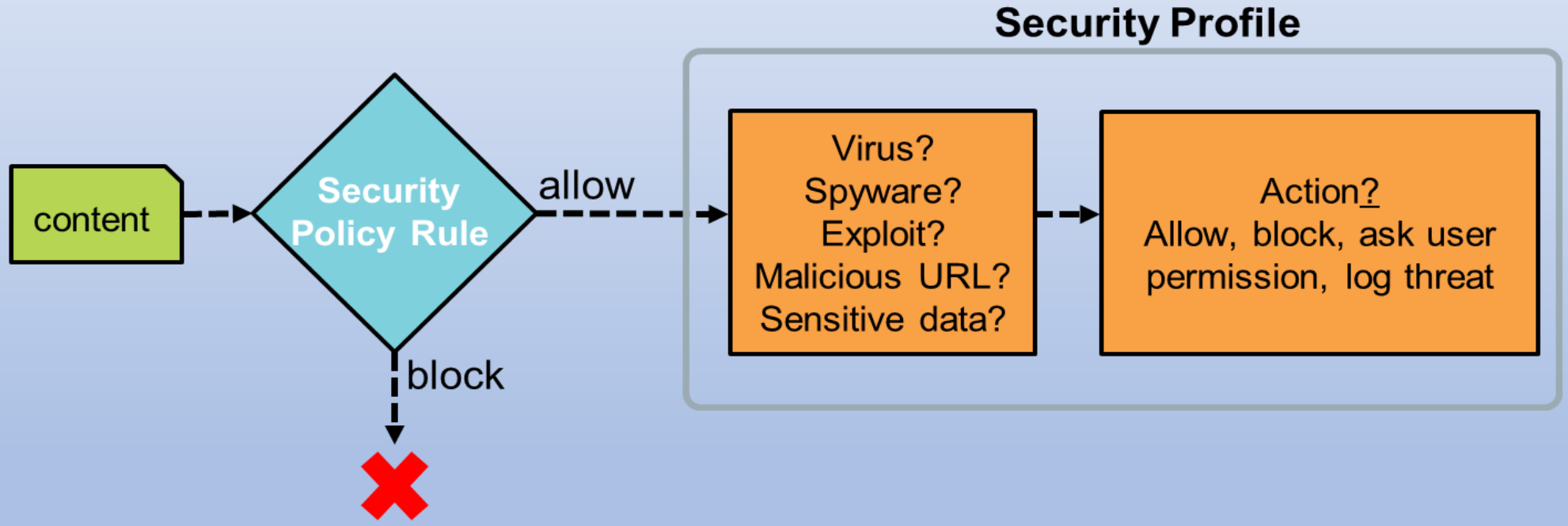
- Content-ID overview
- Vulnerability Protection Security Profiles
- Antivirus Security Profiles
- Anti-Spyware Security Profiles
- File Blocking Profiles
- Attaching Security Profiles to Security policy rules
- Telemetry and threat intelligence

Flow Logic


Initial Packet Processing
Source Zone/ Address/ User-ID
PBF/ Forwarding Lookup
Destination Zone
NAT Policy Evaluated
Security Pre-Policy
Check Allowed Ports
Session Created
Application
Check for Encrypted Traffic
Decryption Policy
Application Override Policy
App-ID/ Content-ID Labeling
Security Policy
Check Security Policy
Check Security Profiles
Post-Policy Processing
Re-Encrypt Traffic
NAT Policy Applied
Packet Forwarded

Security Policy with Security Profiles

- Security Profiles implement additional security checks on allowed traffic.



Security Profile Types

Policies > Security

	Name	Type	Source			Destination		Application	Service	Action	Profile
			Zone	Address	User	Zone	Address				
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	Uenexpected Traffic	universal	Untrust-L3	any	any	Trust-L3	any	any	application-default	Allow	

Antivirus

Anti-Spyware

Vulnerability Protection

URL Filtering

File Blocking

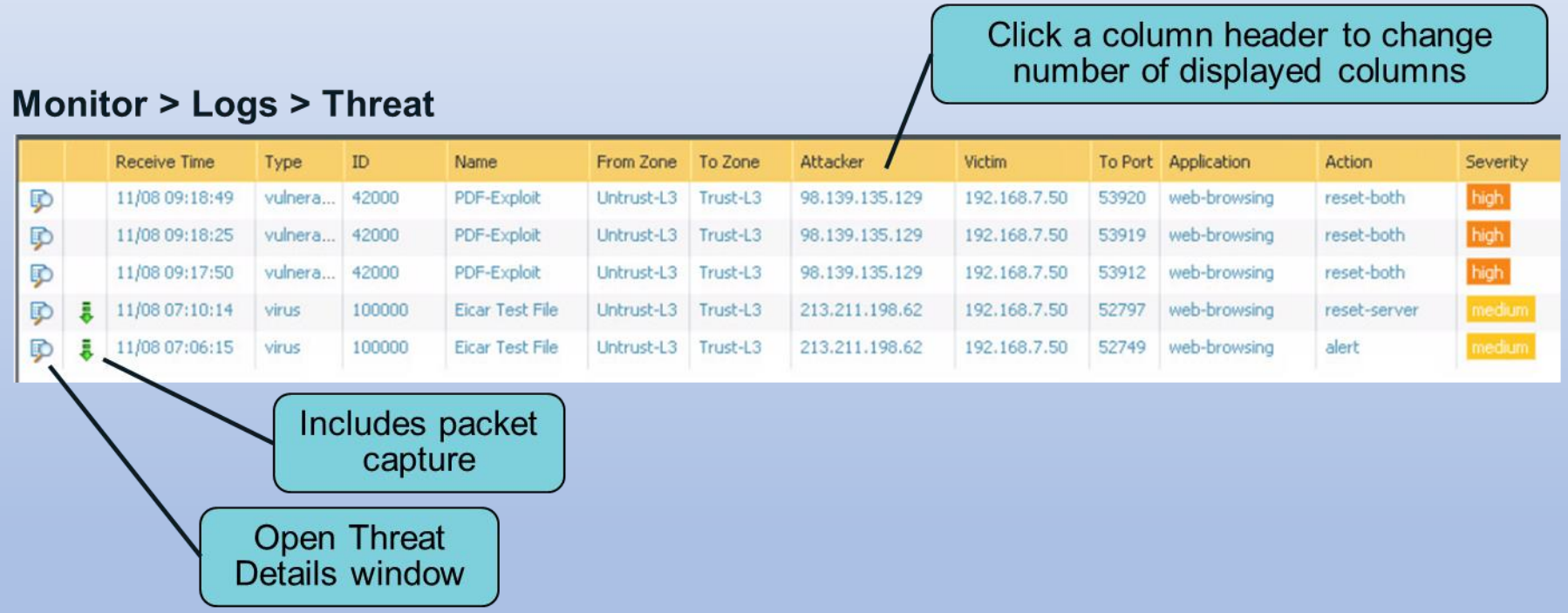
Data Filtering

WildFire Analysis

Security Profile Group

Threat Log

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



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
						high	default	disable
						medium	default	disable
						critical	default	disable
						high	default	disable
						medium	default	disable
			medium					

Add Delete Clone

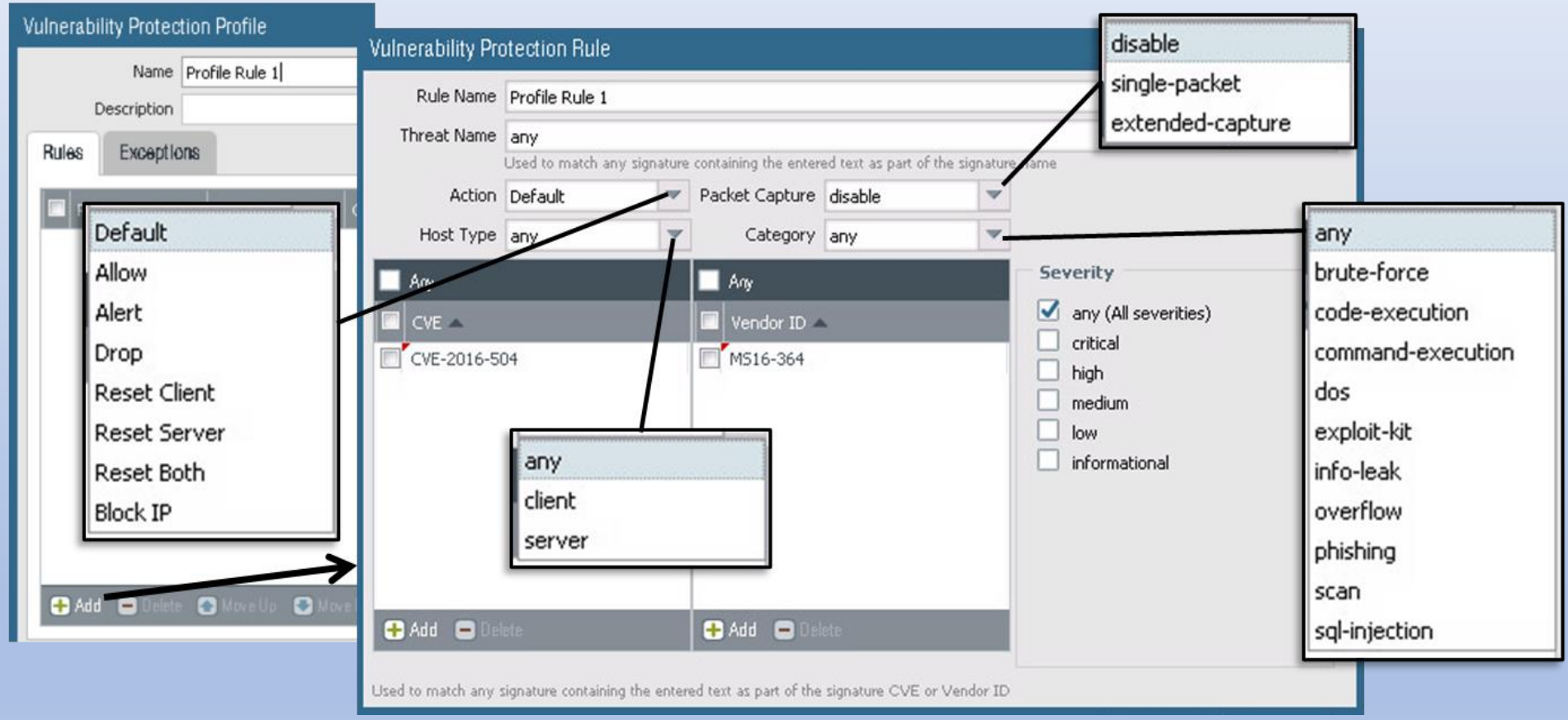
Default (read-only) profiles

Rules specify actions on detected events

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

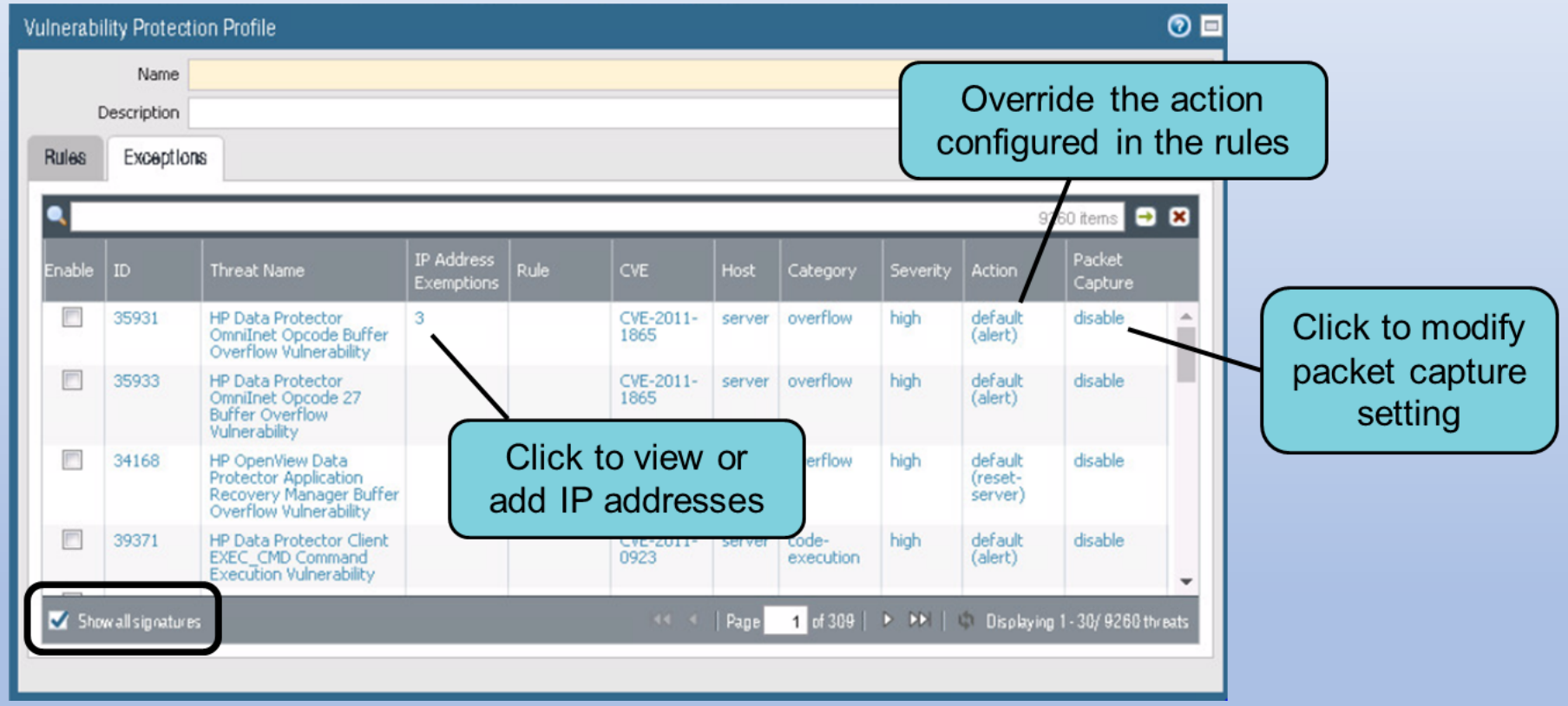
Vulnerability Protection Profile Rules

Objects > Security Profiles > Vulnerability Protection > Add > Rules



Vulnerability Exceptions

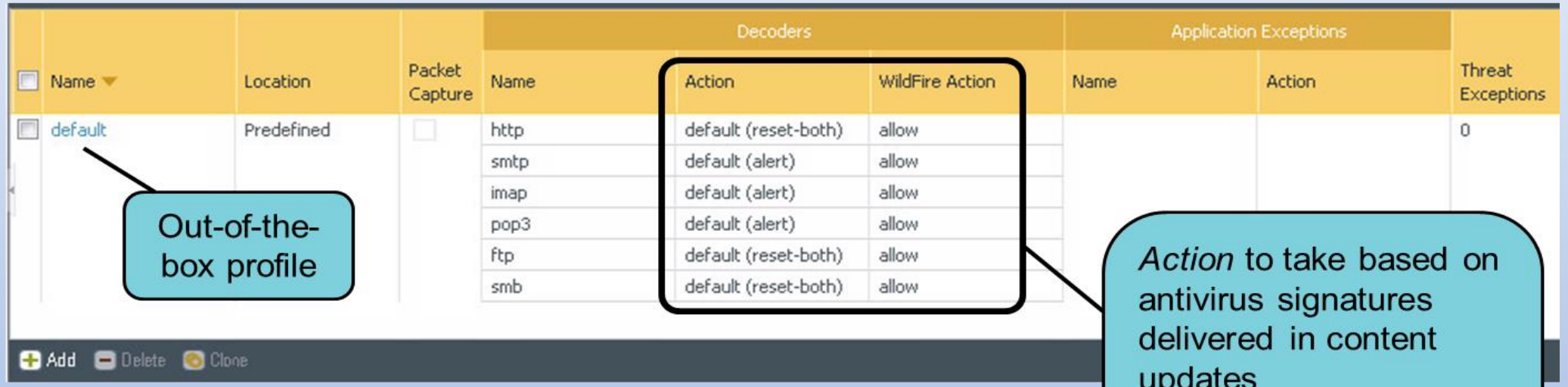
Objects > Security Profiles > Vulnerability Protection > Add



Antivirus Security Profiles

Default Antivirus Security Profile

Objects > Security Profiles > Antivirus

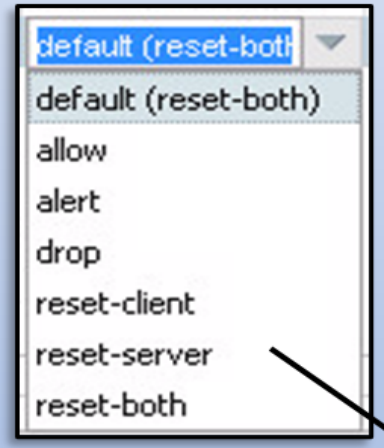


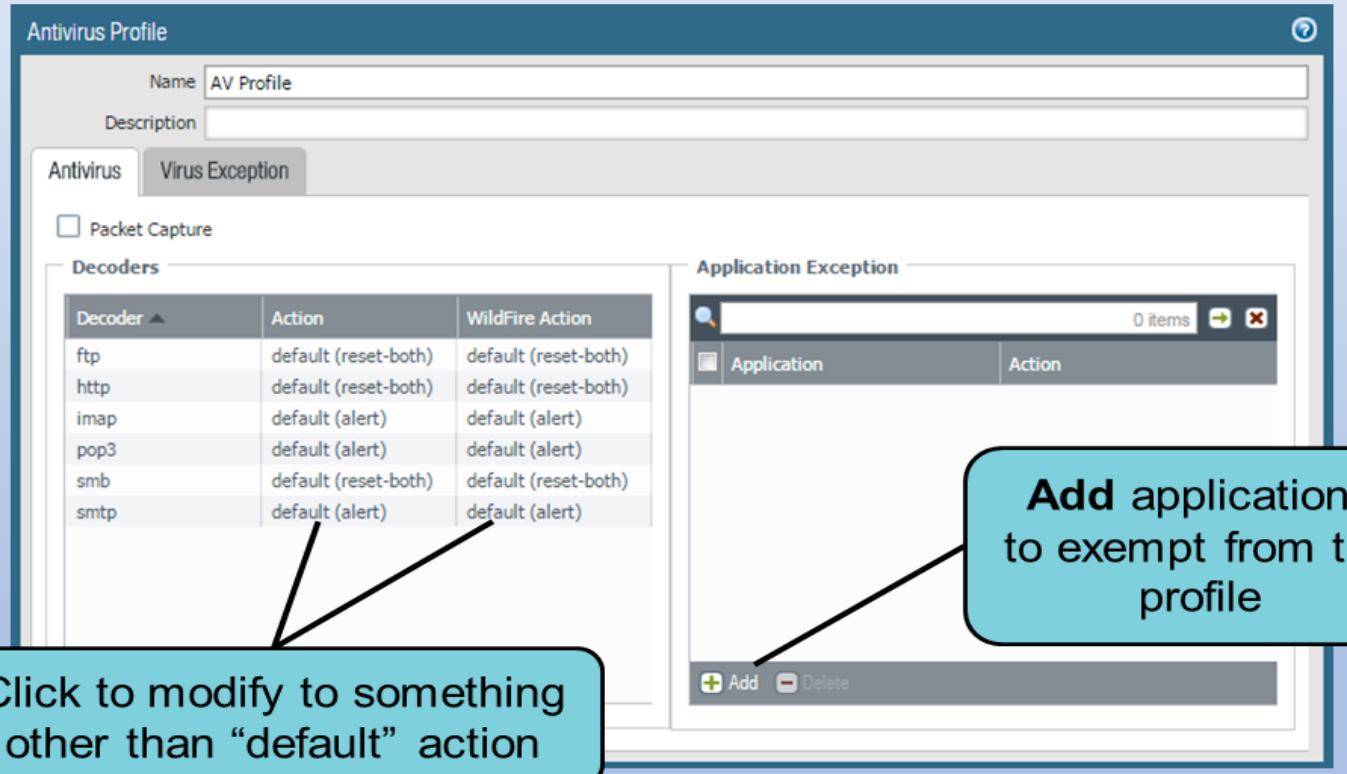
- To create customized profile actions:
  - **Clone** the default read-only profile and edit clone, or
  - **Add** a brand new profile

Creating a New Antivirus Profile

Objects > Security Profiles > Antivirus > Add

Available actions



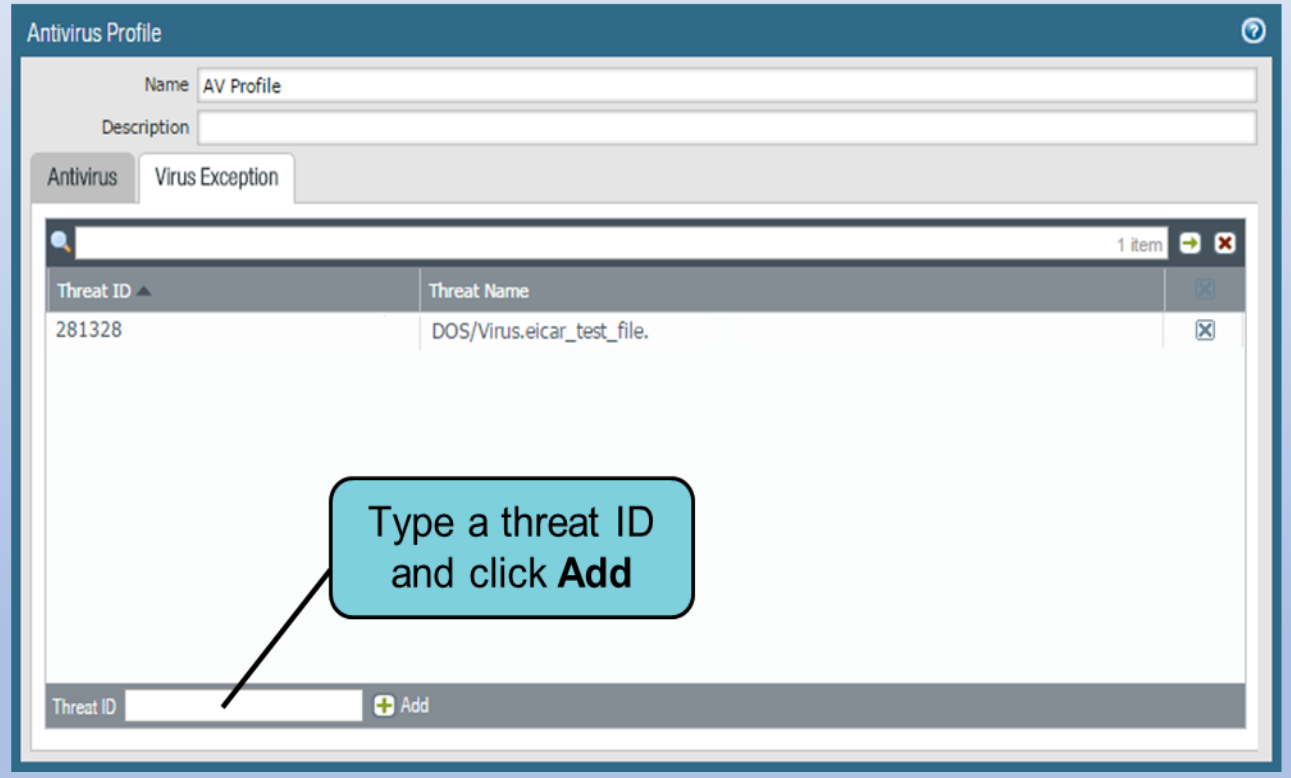


Click to modify to something other than “default” action

Add applications to exempt from the profile

Creating a New Antivirus Profile (Cont.)

Objects > Security Profiles > Antivirus > Add

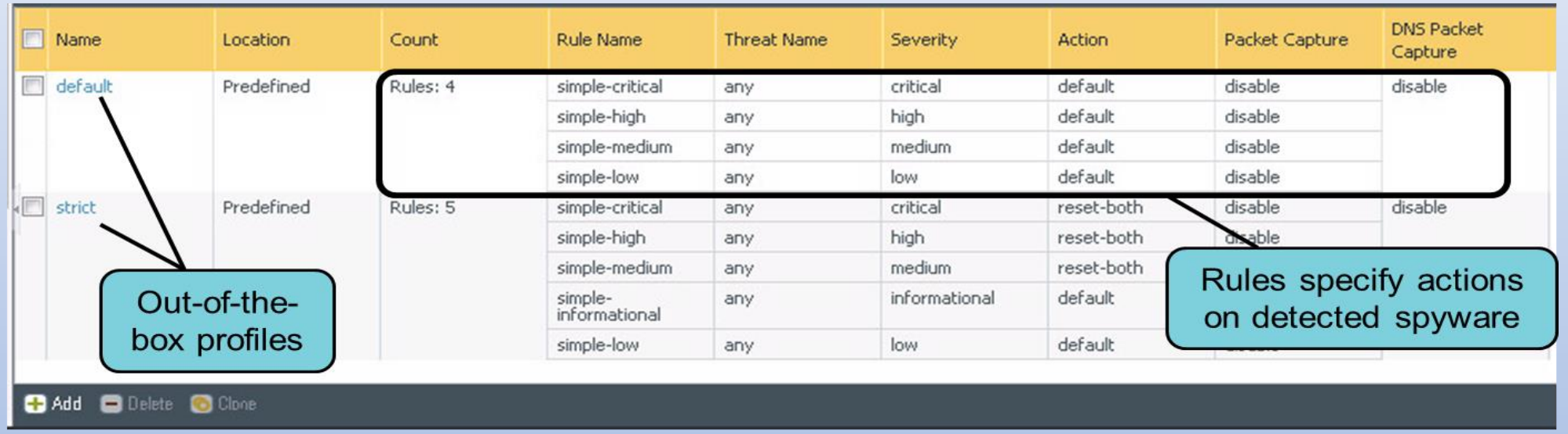


- To reduce false positives use Threat ID to create an exemption
- Threat IDs recorded in Threat log

Anti-Spyware Security Profiles

Default Anti-Spyware Security Profiles

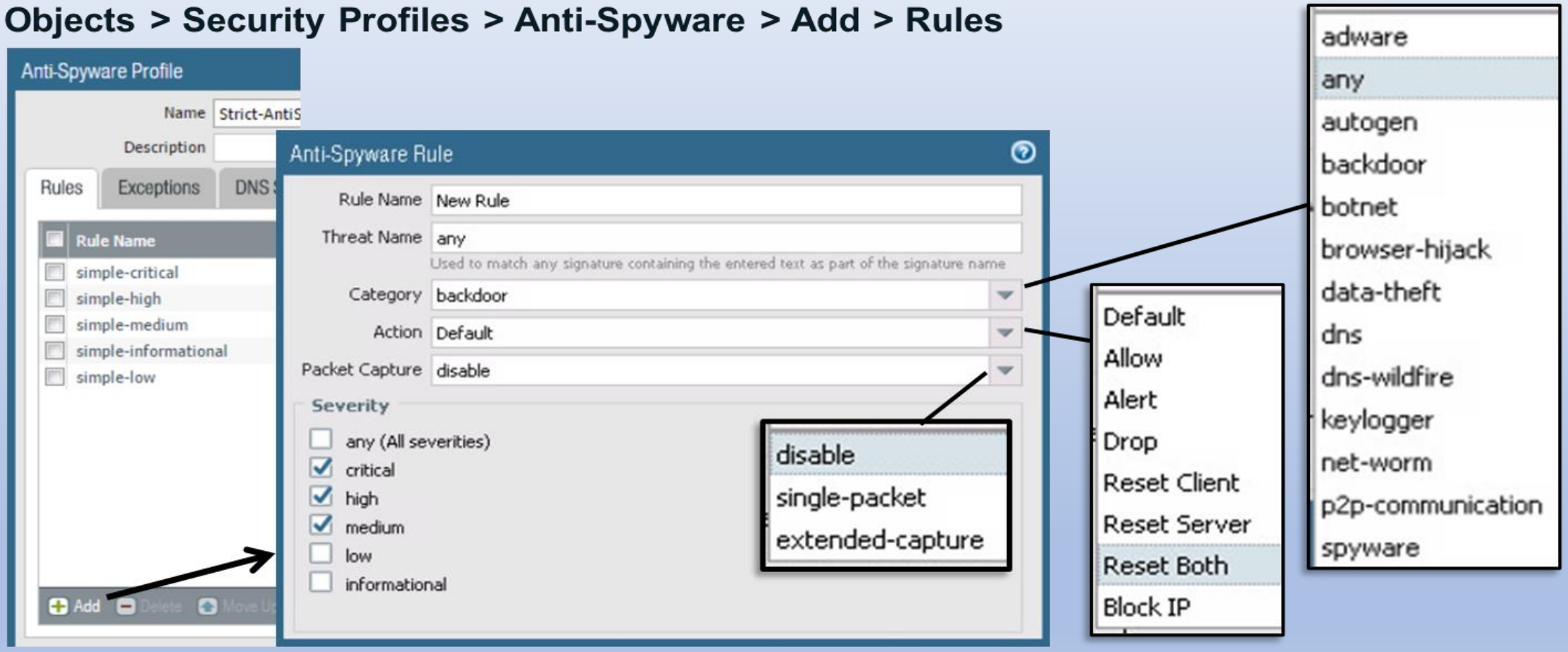
Objects > Security Profiles > Anti-Spyware



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

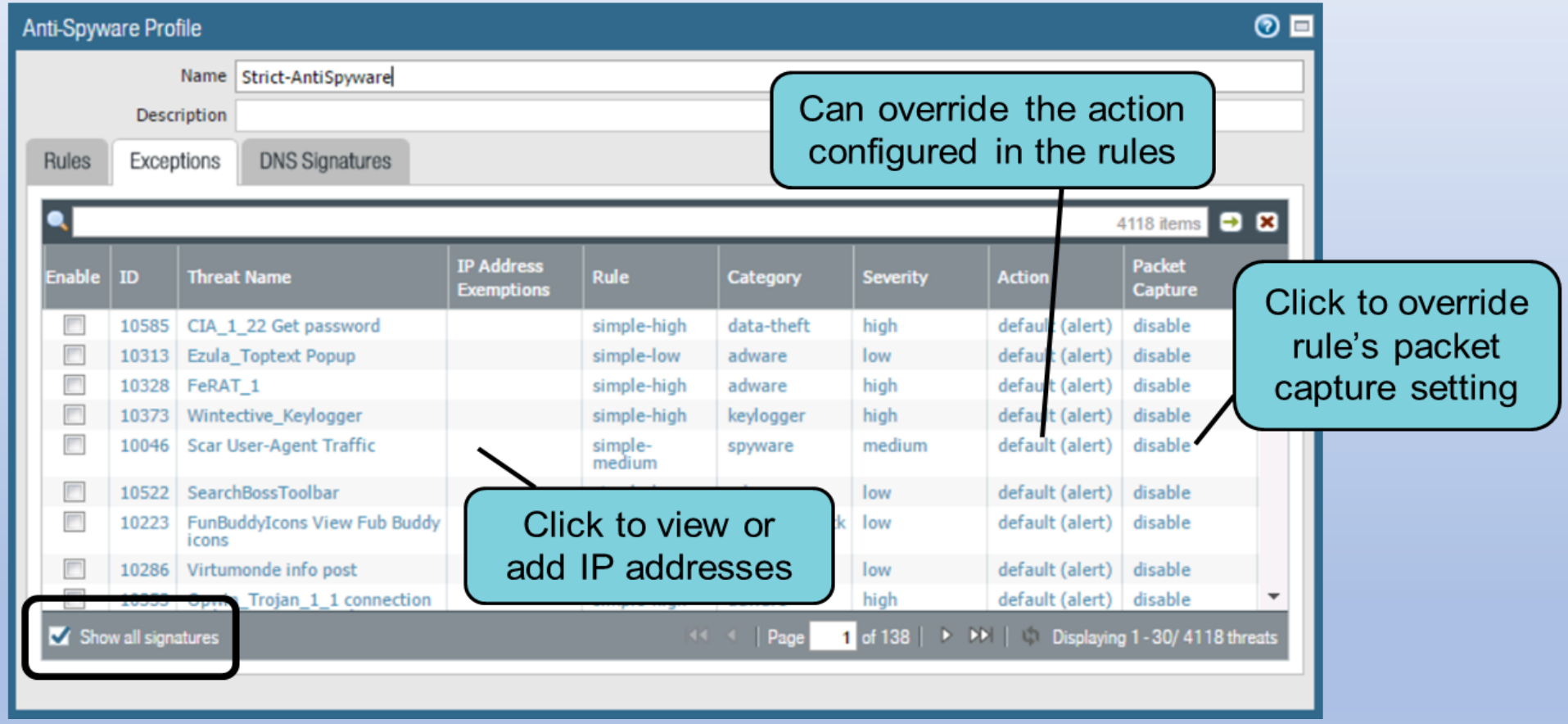
Configuring Anti-Spyware Profile Rules

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



Anti-Spyware Exceptions

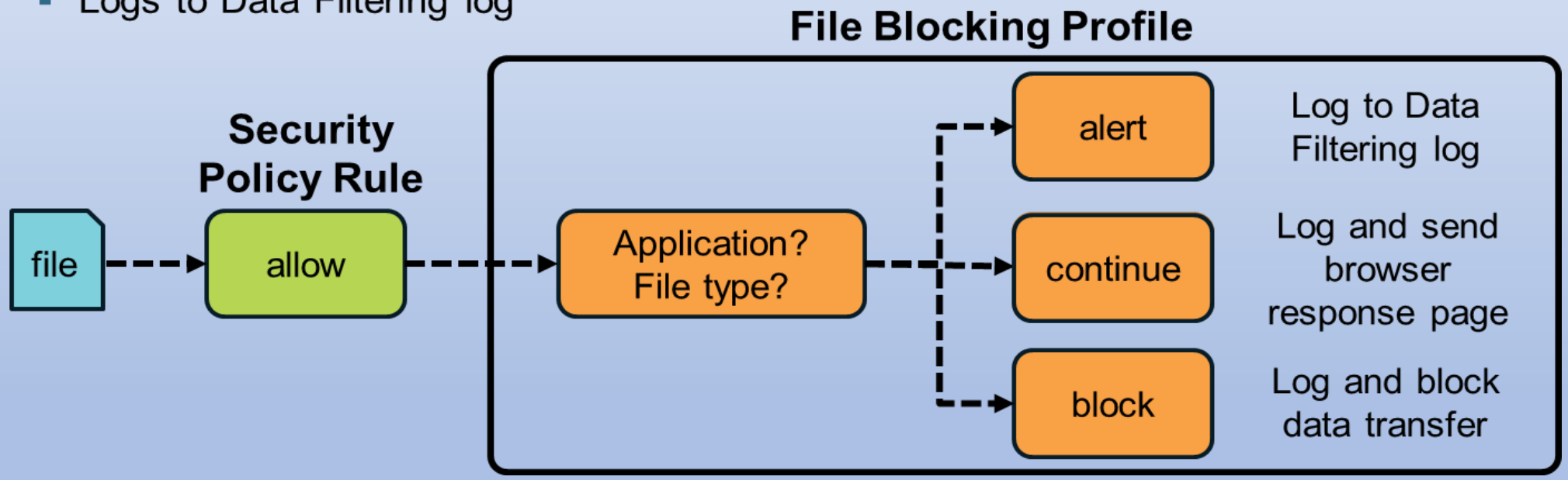
Objects > Security Profiles > Anti-Spyware > Add



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

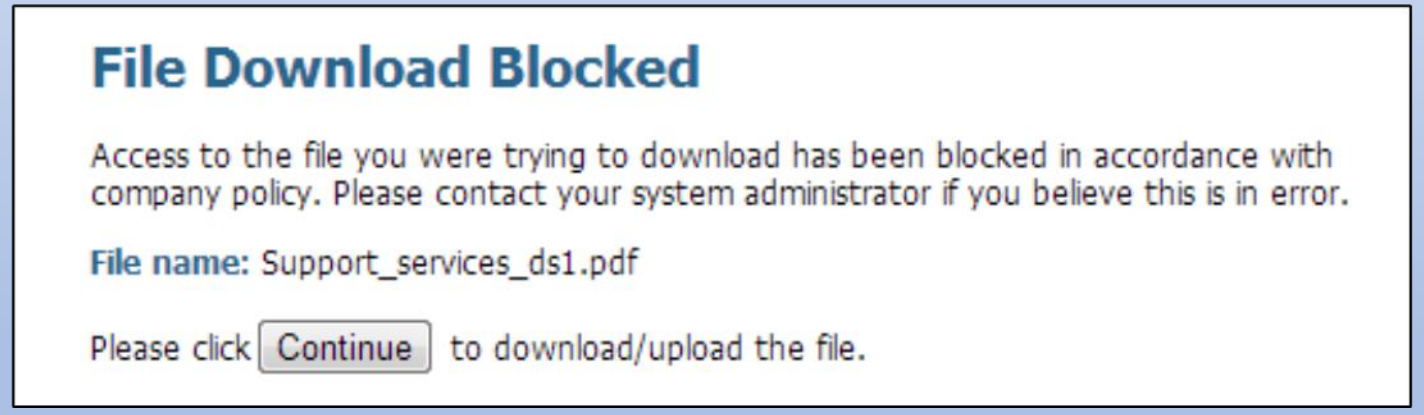
	Receive Time	File Name	Name	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
	08/12 21:24:00	44.0.2403.155_44.0.2403.130_chrome_updater.exe	Microsoft PE File	Untrust-L3	Trust-L3	74.125.170.11	192.168.14.50	61813	web-browsing	deny	General Internet
	08/12 21:23:25	44.0.2403.155_44.0.2403.130_chrome_updater.exe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

Continue Response Page

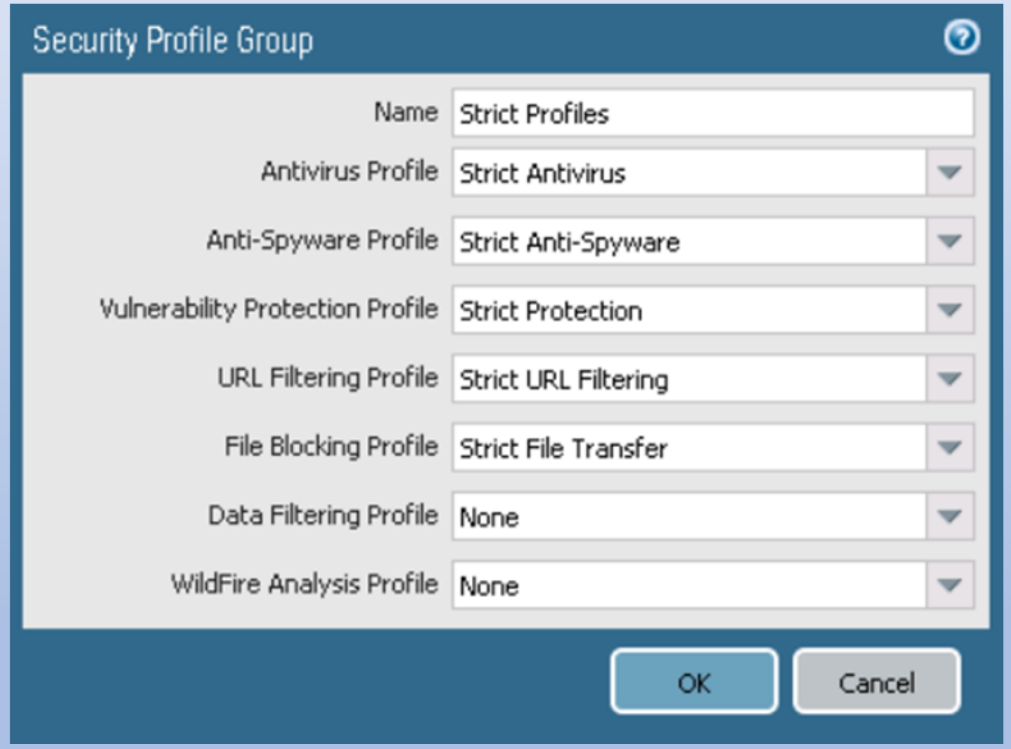
- A "continue" action requires user permission to complete file transfer.
- Only functional with web-browsing application



Attaching Security Profiles to Security Policy Rules

Security Profile Groups

Objects > Security Profile Groups > Add

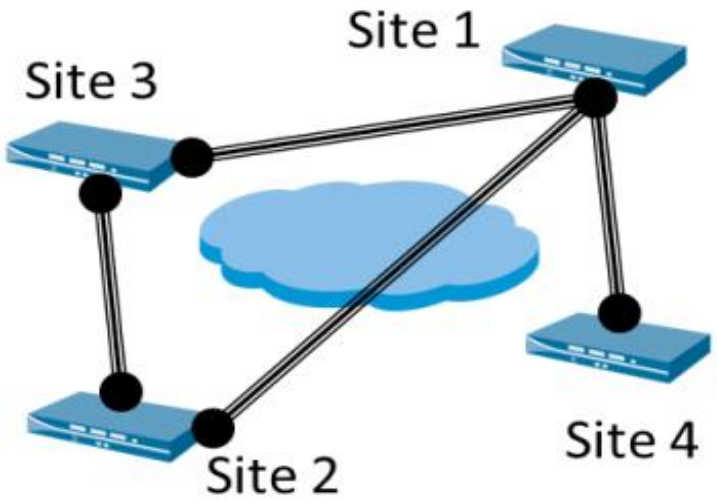


- Add Security Profiles that are commonly used together
- Simplifies Security policy rule administration

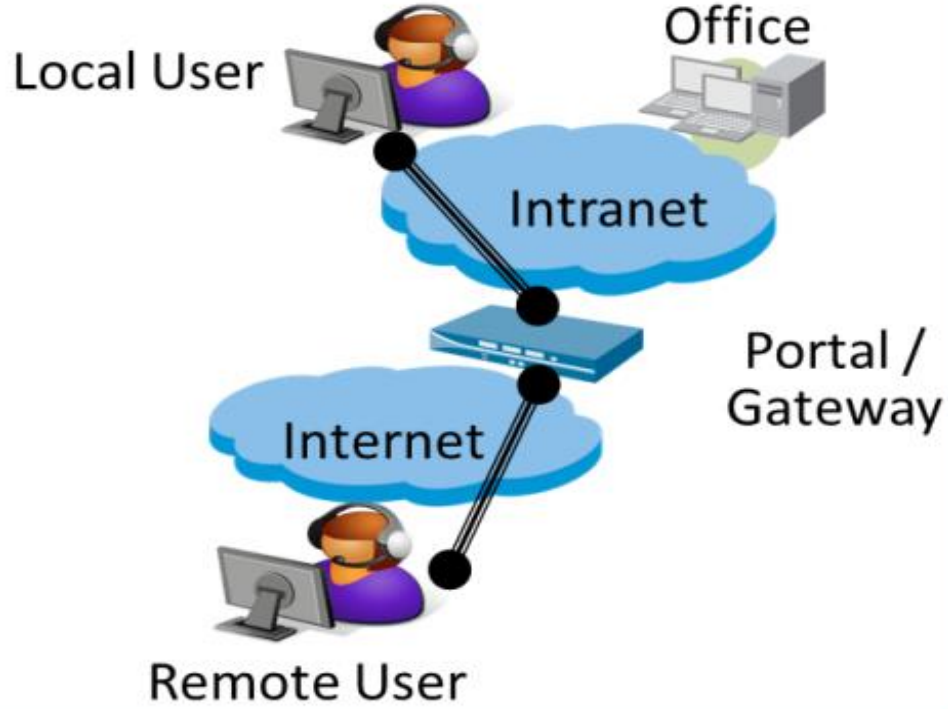
5.
Site-to-Site VPNs

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

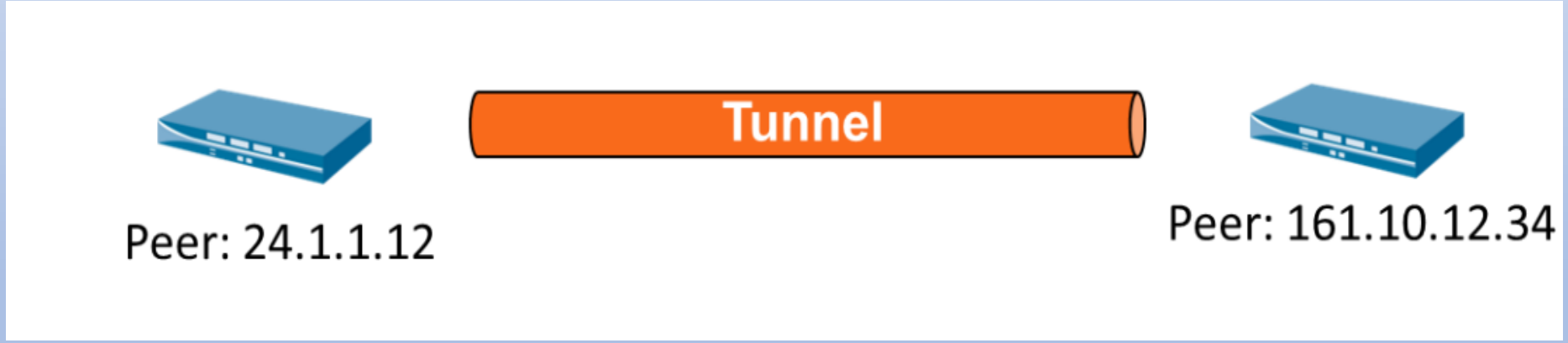
- Traffic is tunneled based on the destination of traffic
- Policy-based systems match the traffic on source and destination addresses, as well as service (port) The tunnel is represented by a logical tunnel interface
- Tunnel interface is placed into a Zone The Routing table chooses the tunnel settings

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

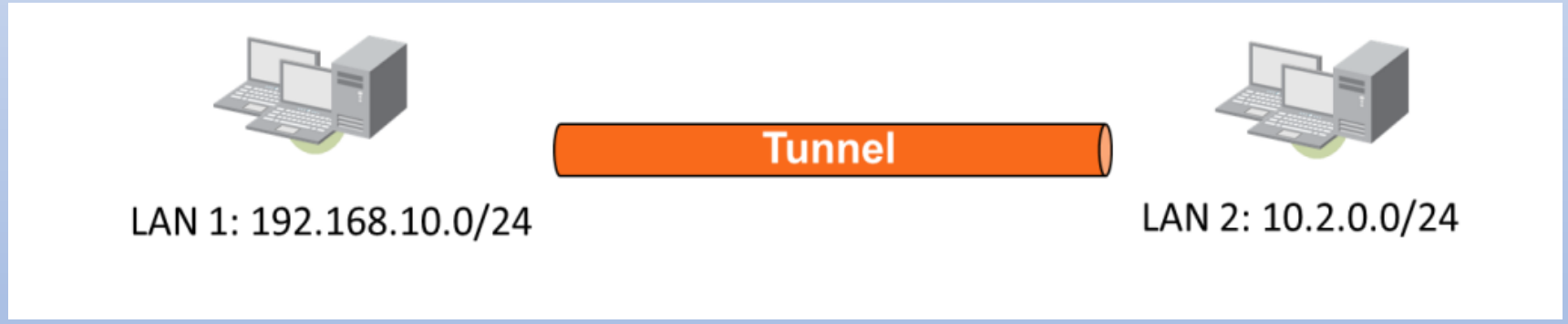
Three Settings (Modes): Aggressive, Main, Auto



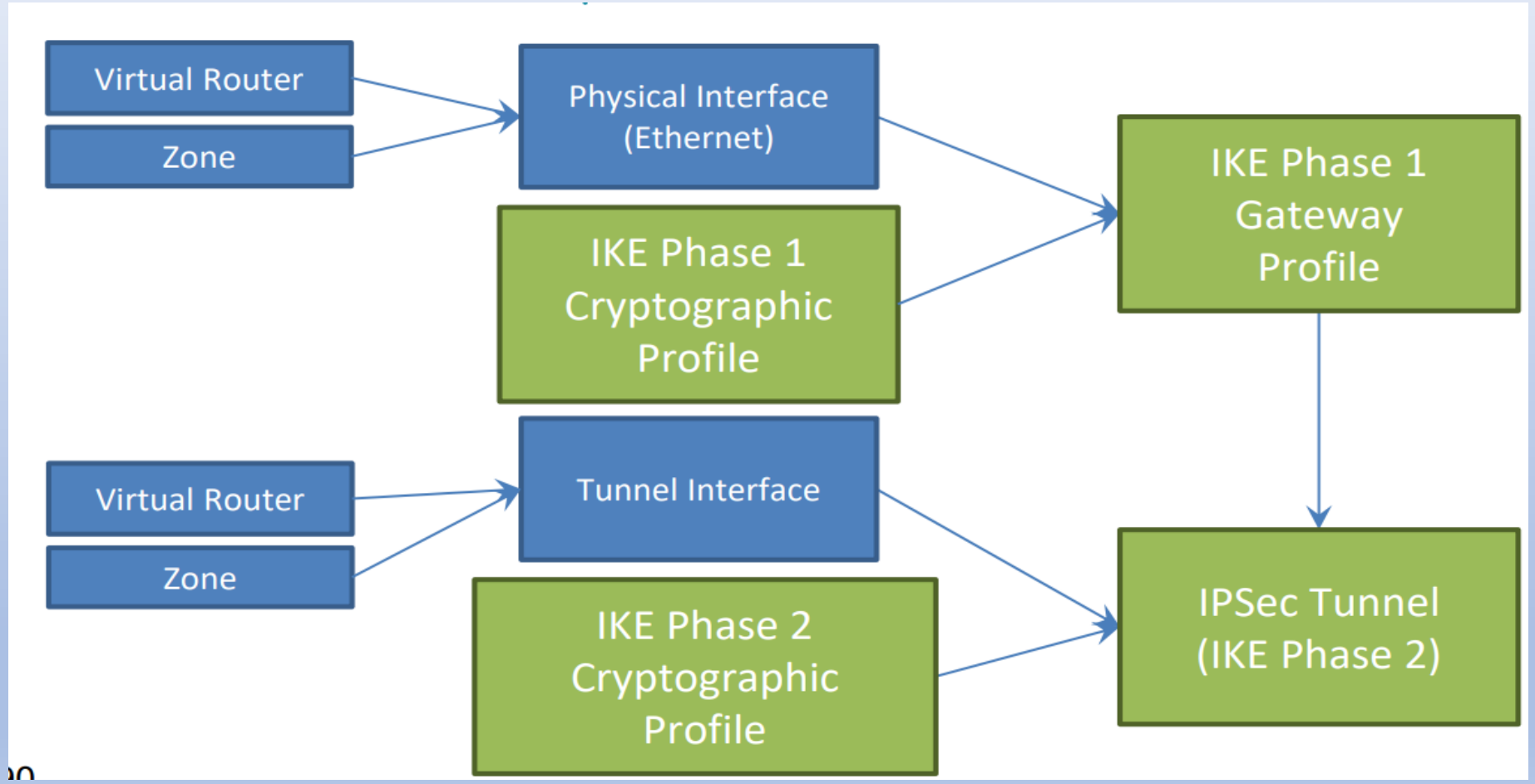
Phase 2 - IPsec

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

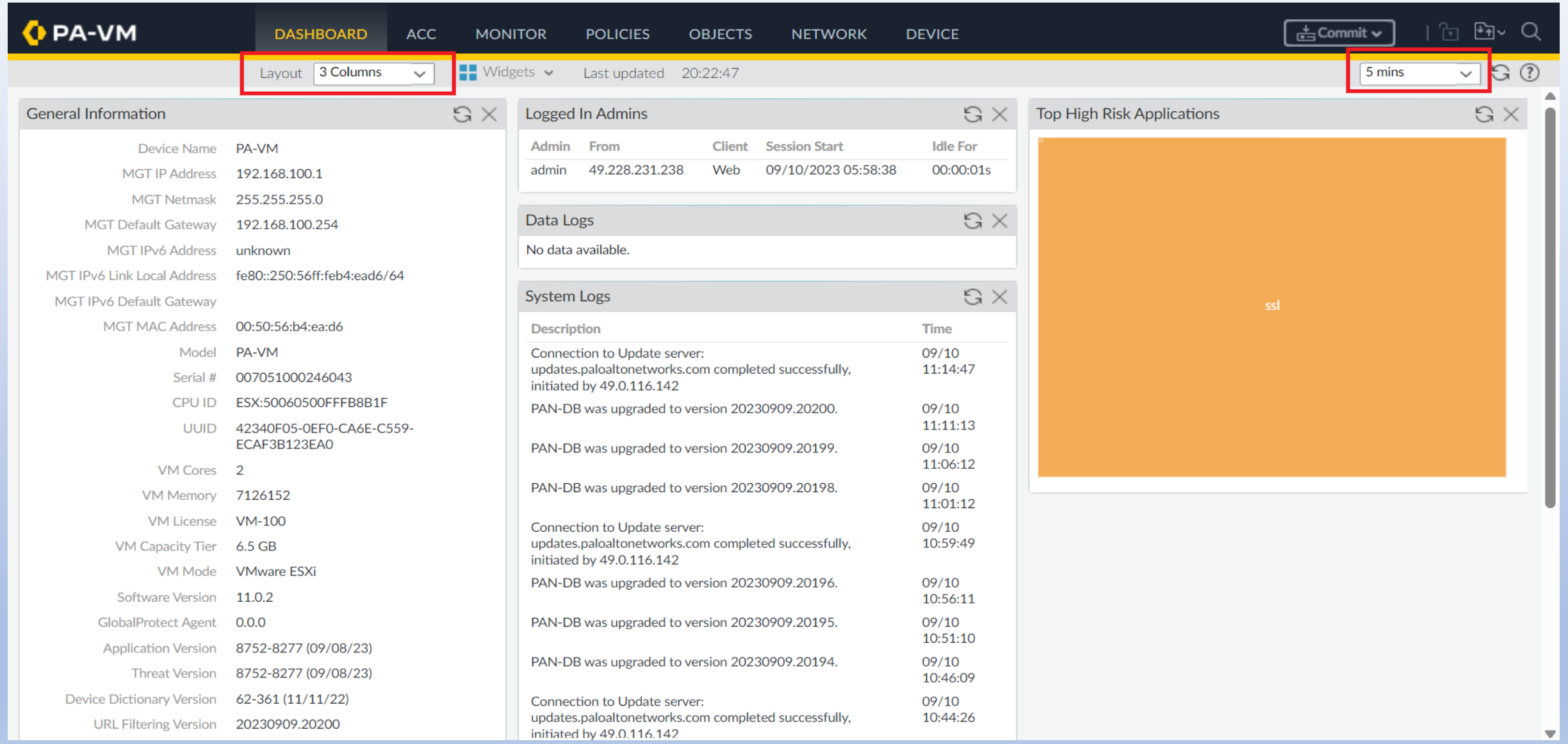


VPN Tunnel Component Interaction

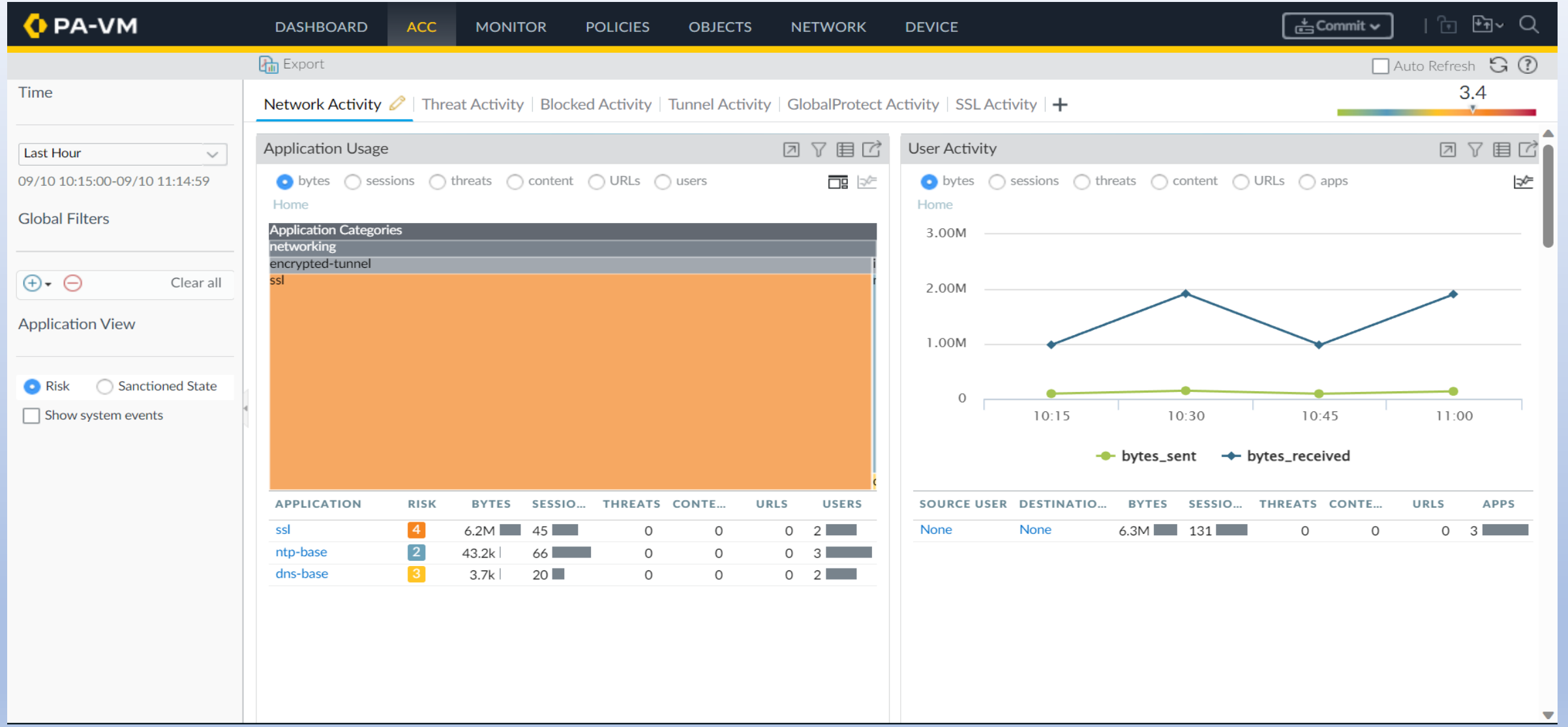


Reporting

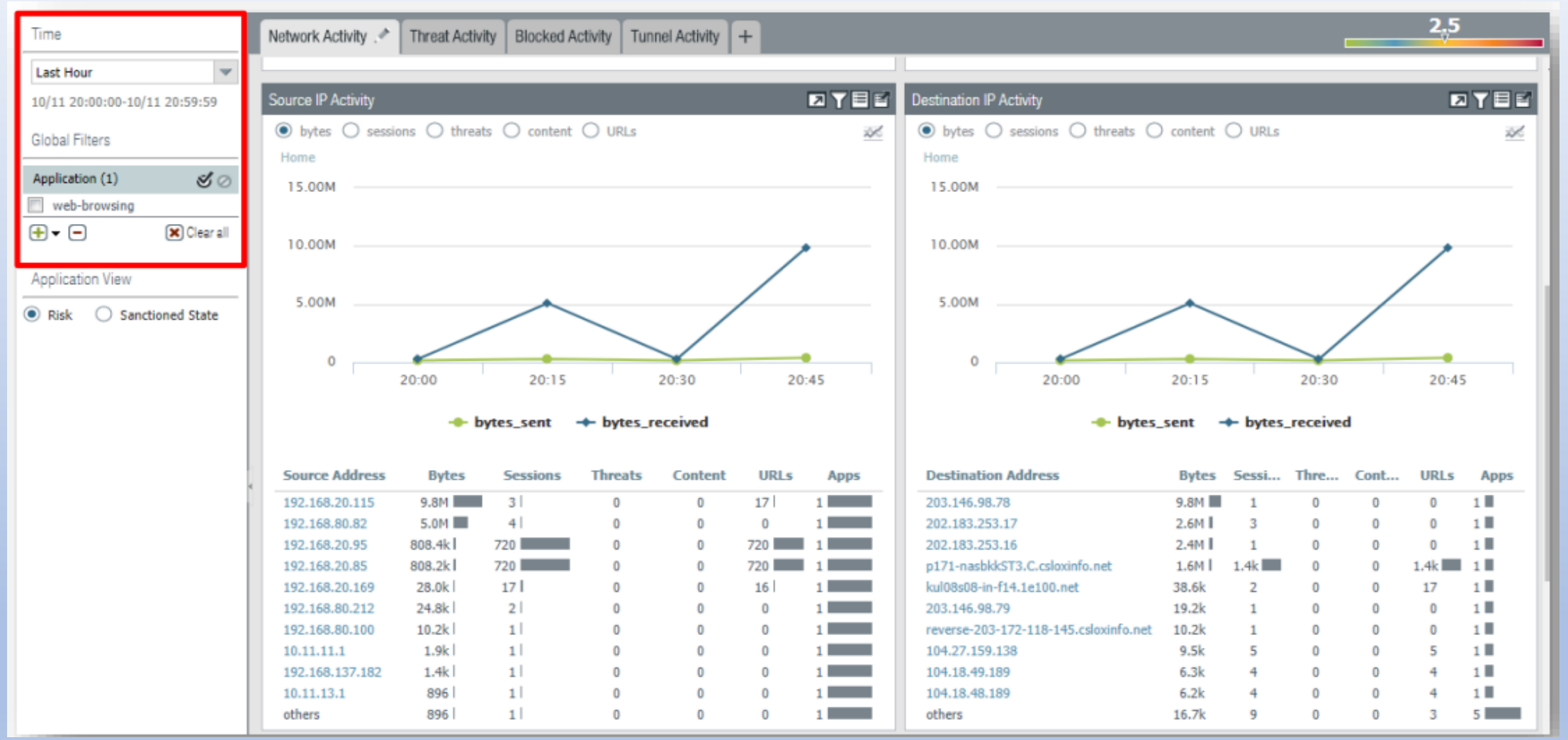
Dashboard


PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Layout
3 Columns
Widgets
Last updated
20:22:47
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:50060500FFFB8B1F
UUID 42340F05-0EF0-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
ssl

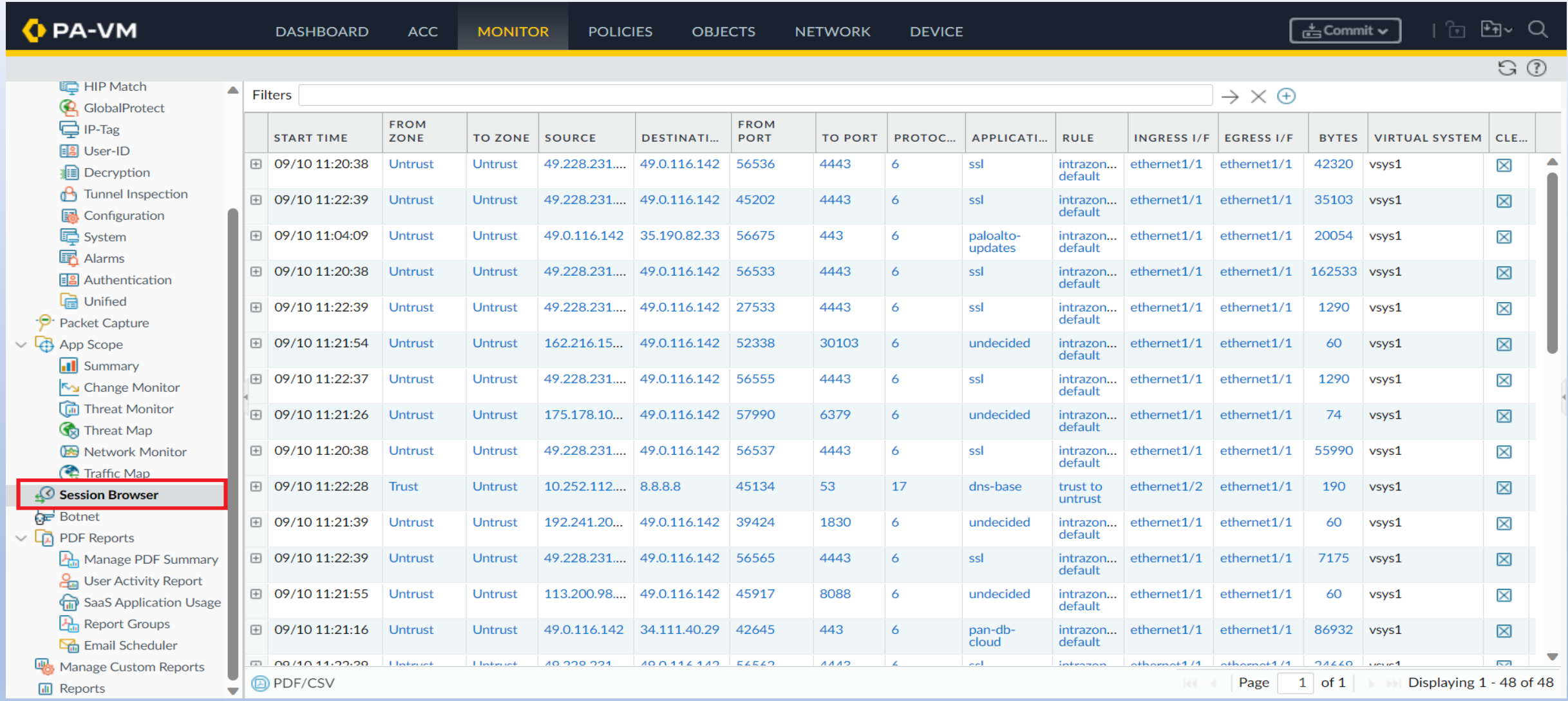
Application Command Center (ACC)



Drilling Down



Session Browser



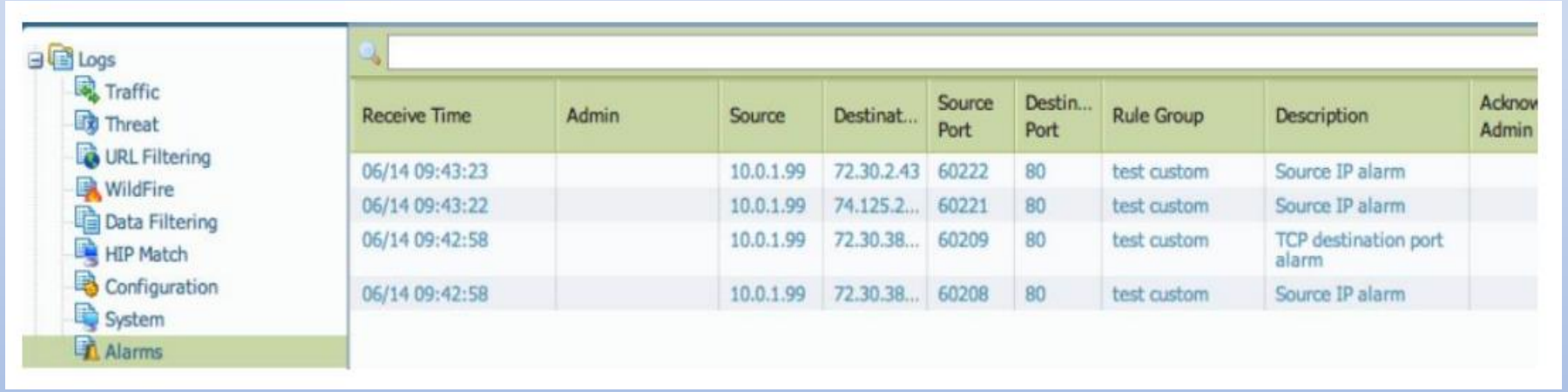
Logging

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

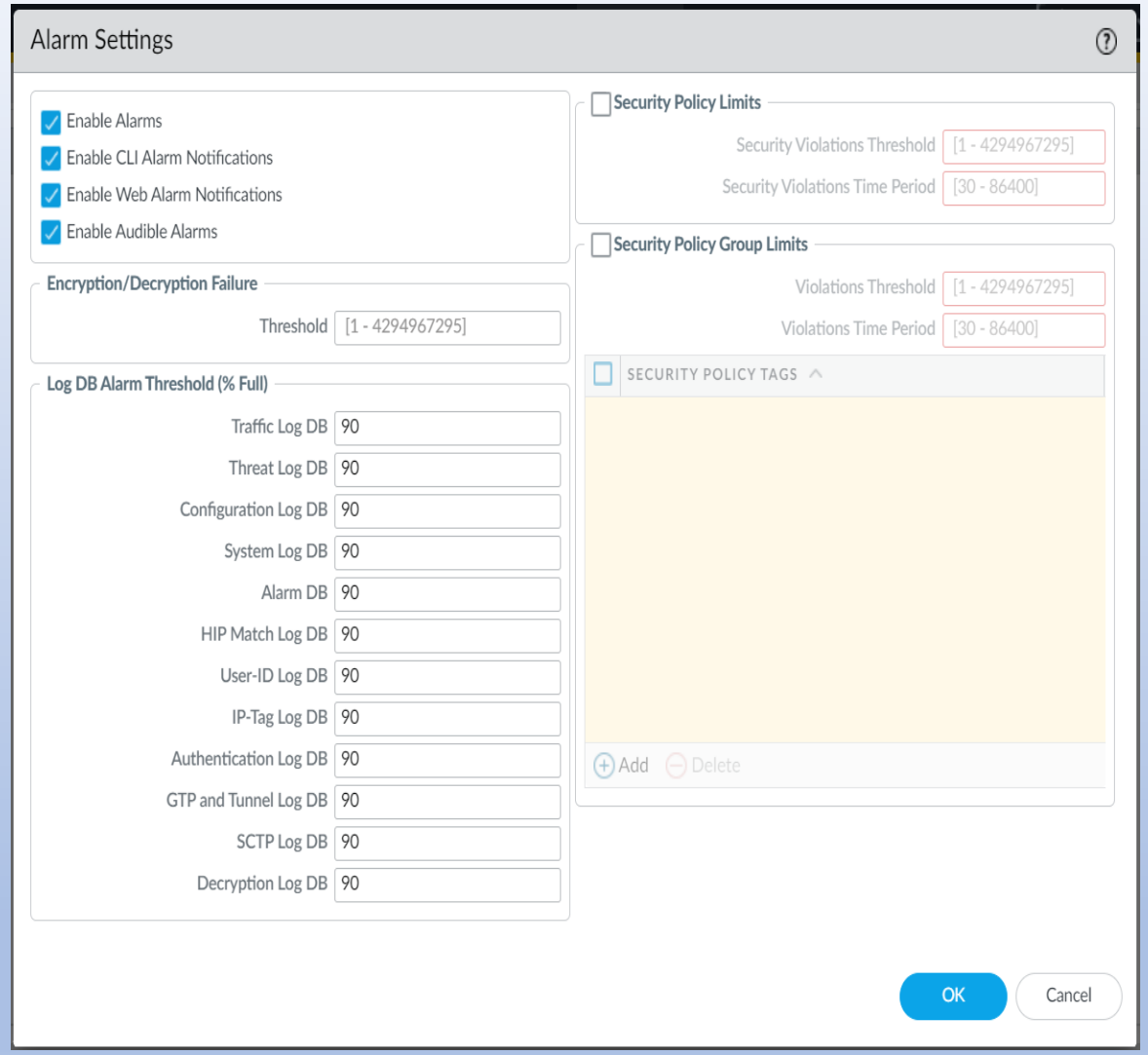
- Logs specific events
  - For example: Log DB growing too large,
    Encryption/Decryption errors, too many denies for a specific IP address
- Alarm generation be enabled is Device > Log Settings > Alarms



Receive Time	Admin	Source	Destinat...	Source Port	Destin... Port	Rule Group	Description	Acknov 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	

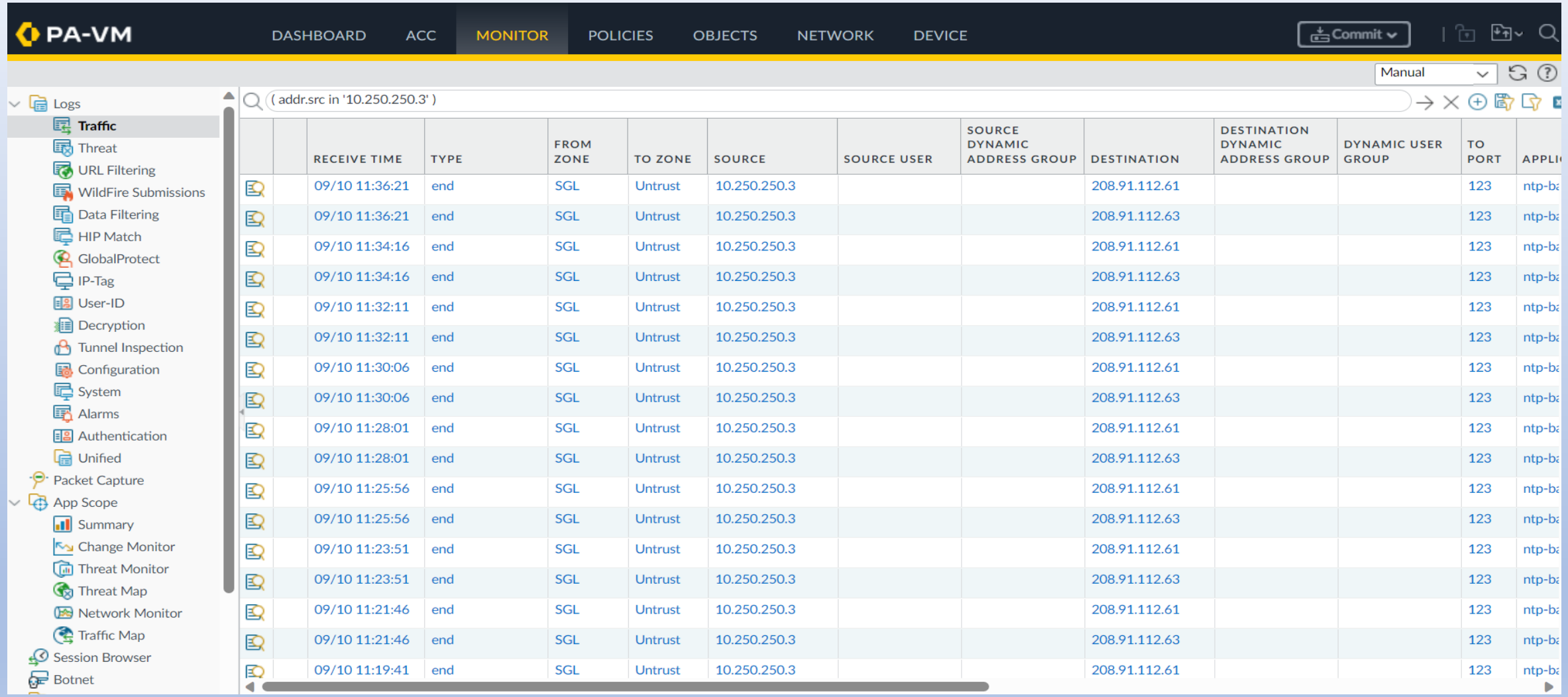
Enabling Alarm Settings

- 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



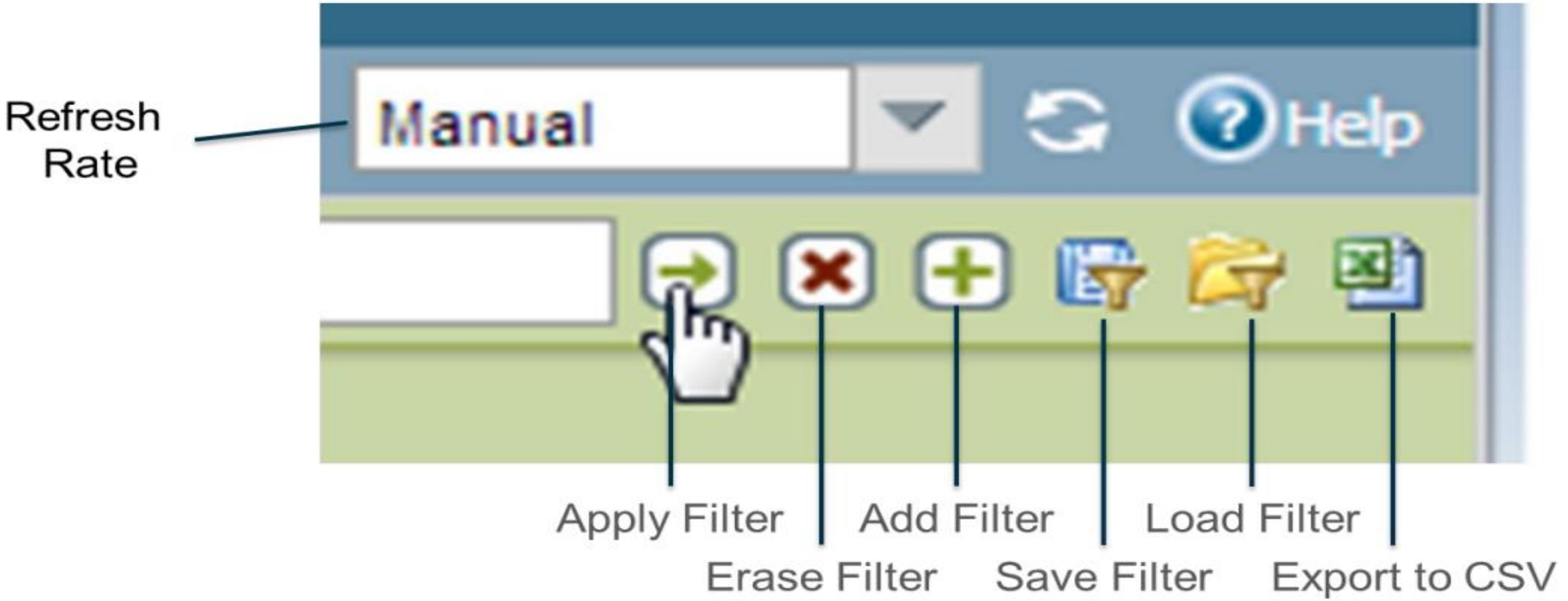
Viewing and Filtering Logs

Constructing a Log Filter



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

Filter Buttons



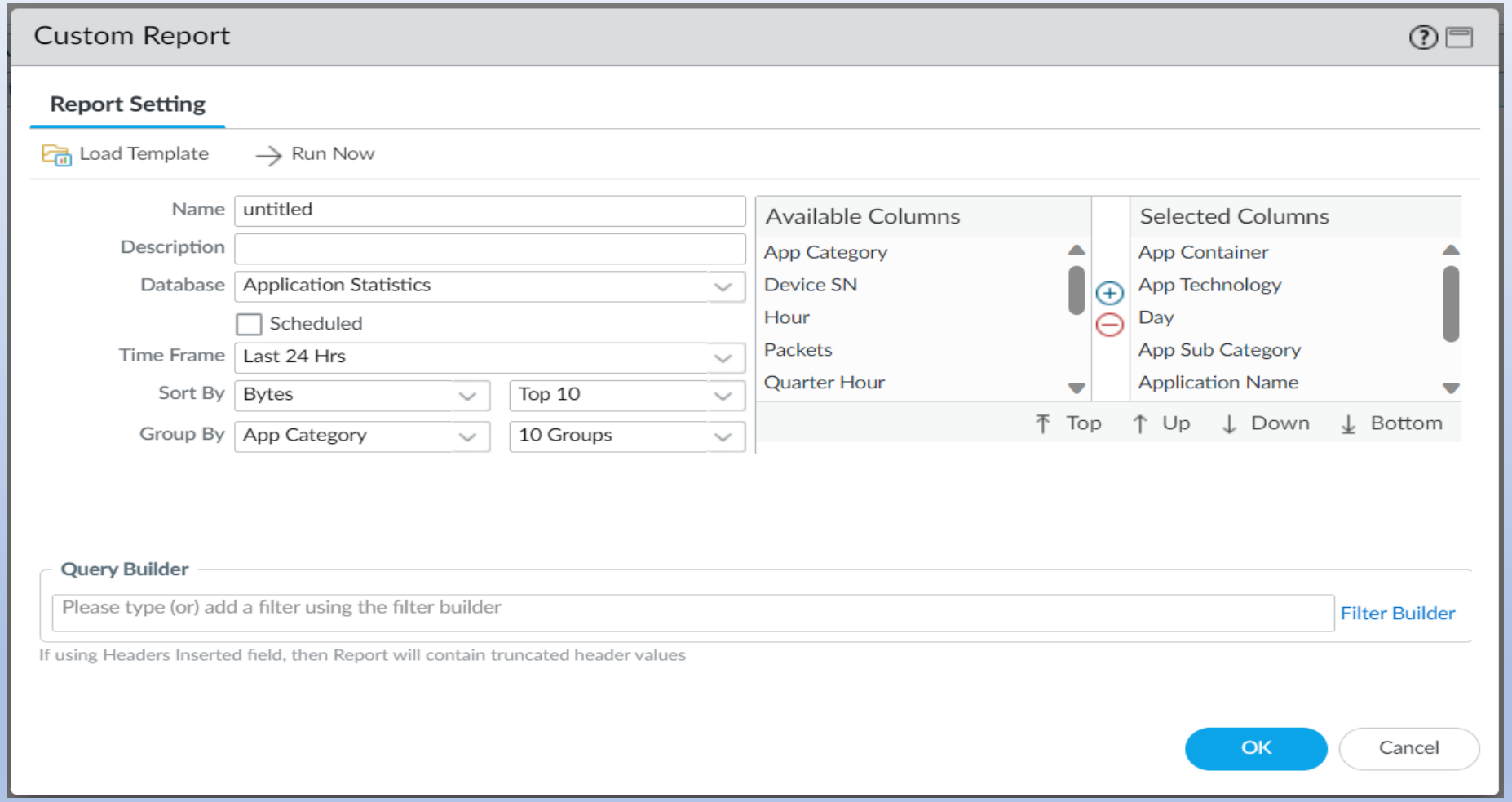
Reports

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

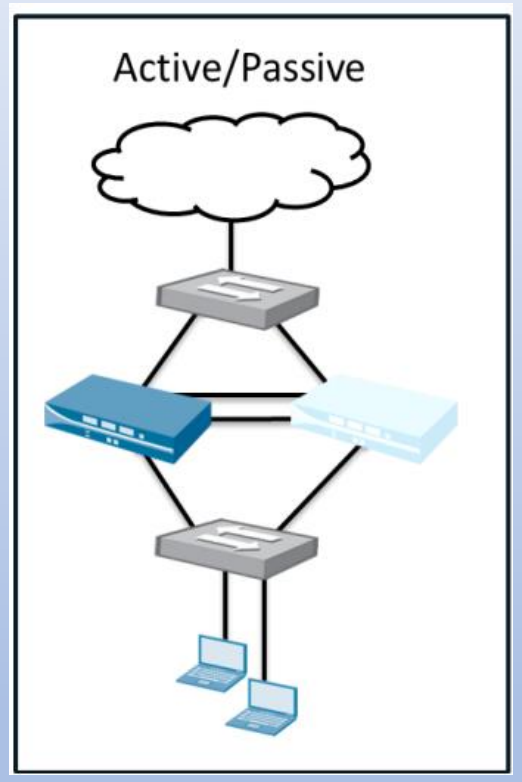
PDF Summary Reports
  - Aggregate reports
- Report Groups
  - Compile reports into a single emailed PDF

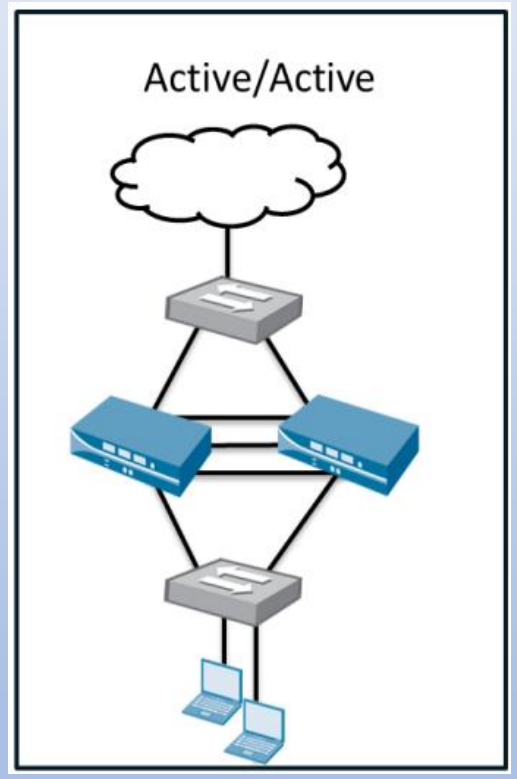
Custom Reports



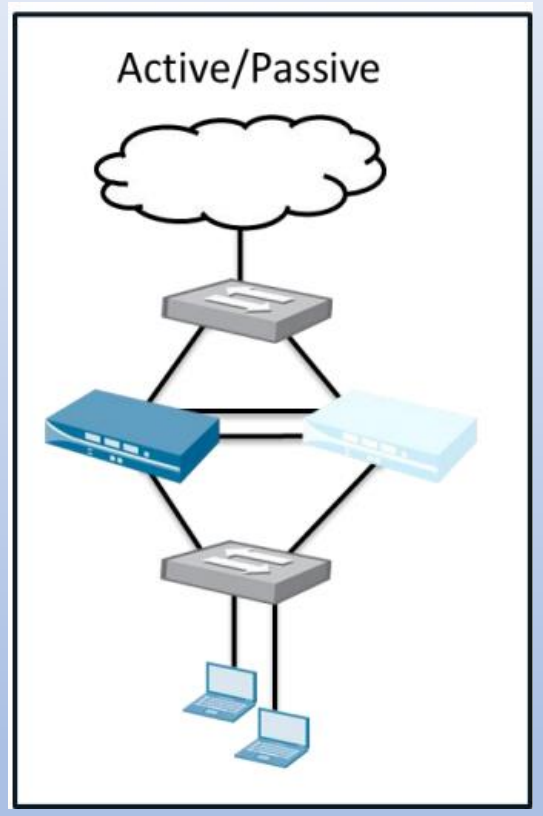
High Availability (HA) Overview

High Availability (HA)





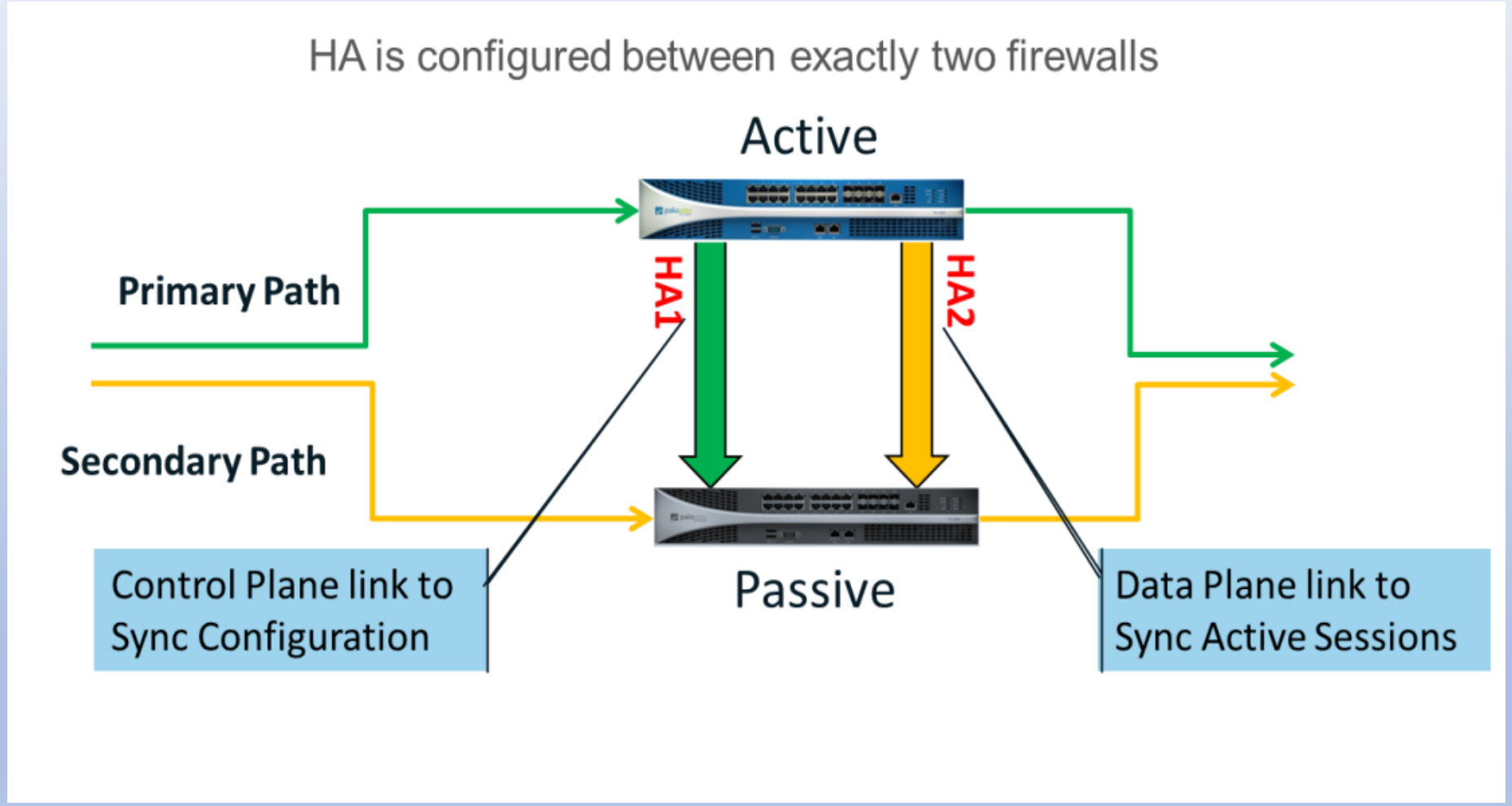
Active/Passive Overview



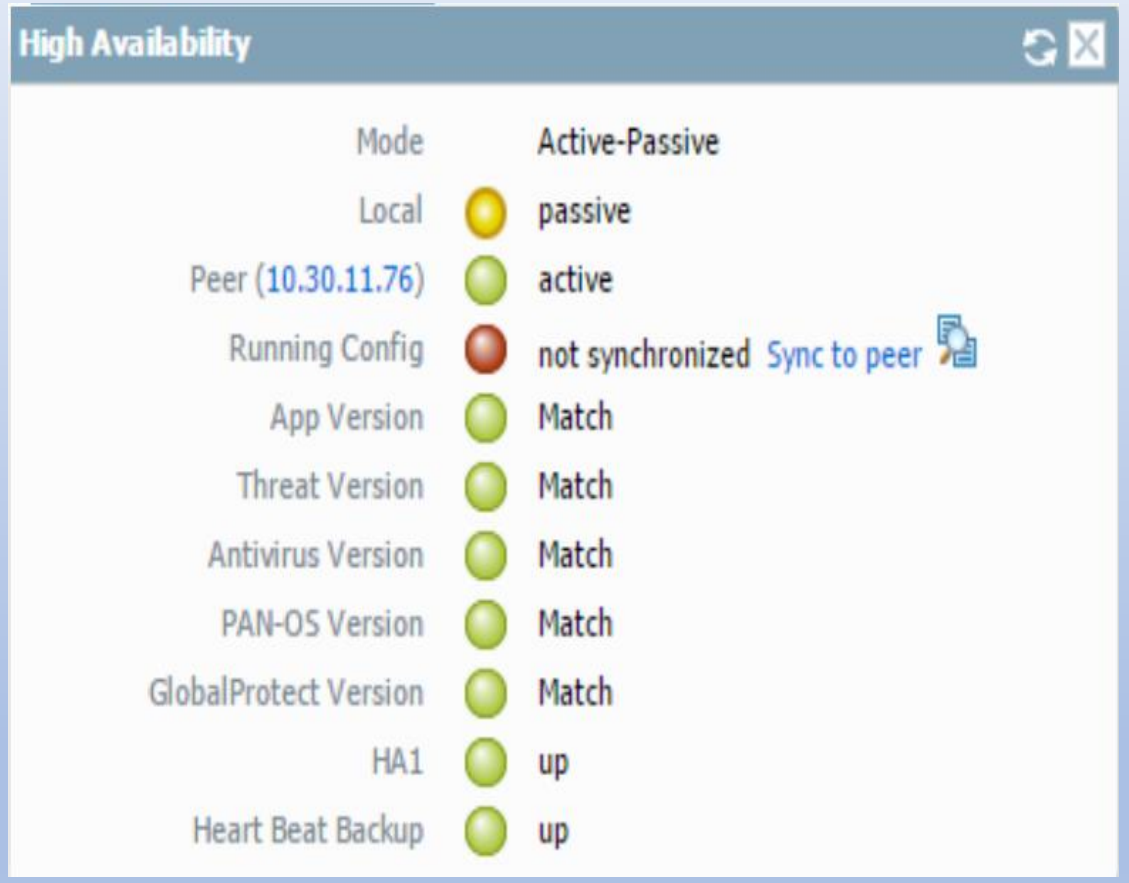
Supported Modes:

- 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



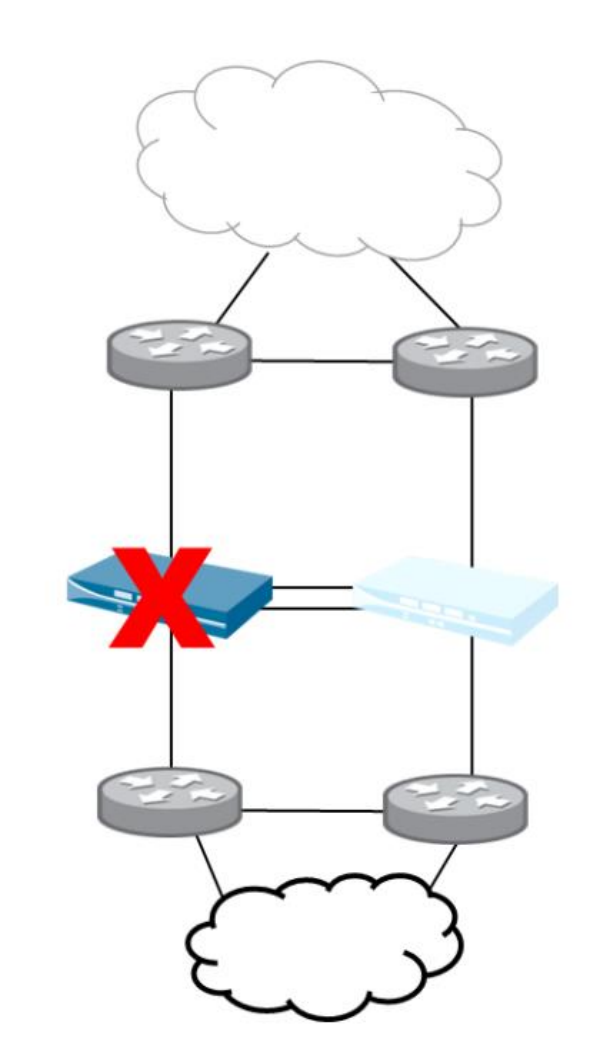
Device States



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

Device States

- Heartbeat Polling
- Path Monitoring
- Link Monitoring

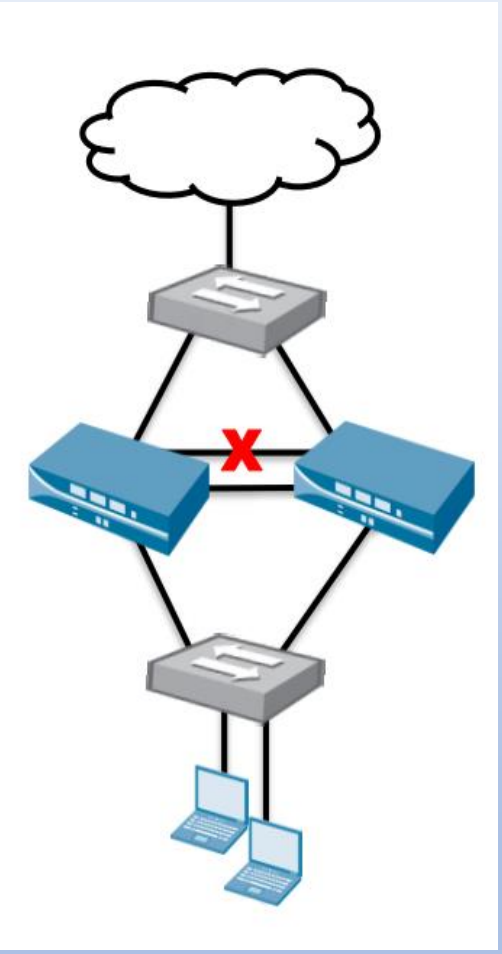


Split Brain

“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.

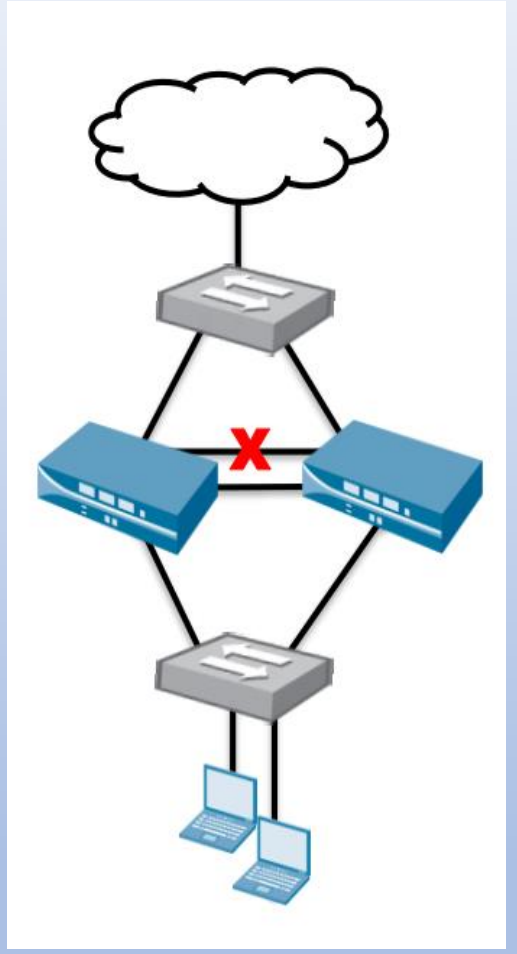
If the Active device loses connection to the Passive device, path and link monitoring will not be honored as the Active device doesn’t know that the peer will take over.



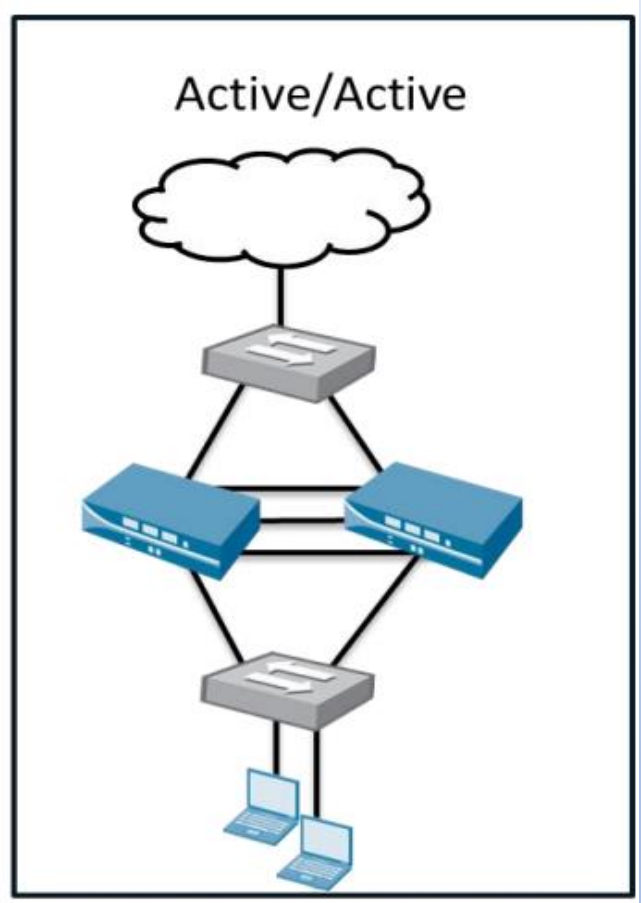
Split Brain Solutions

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

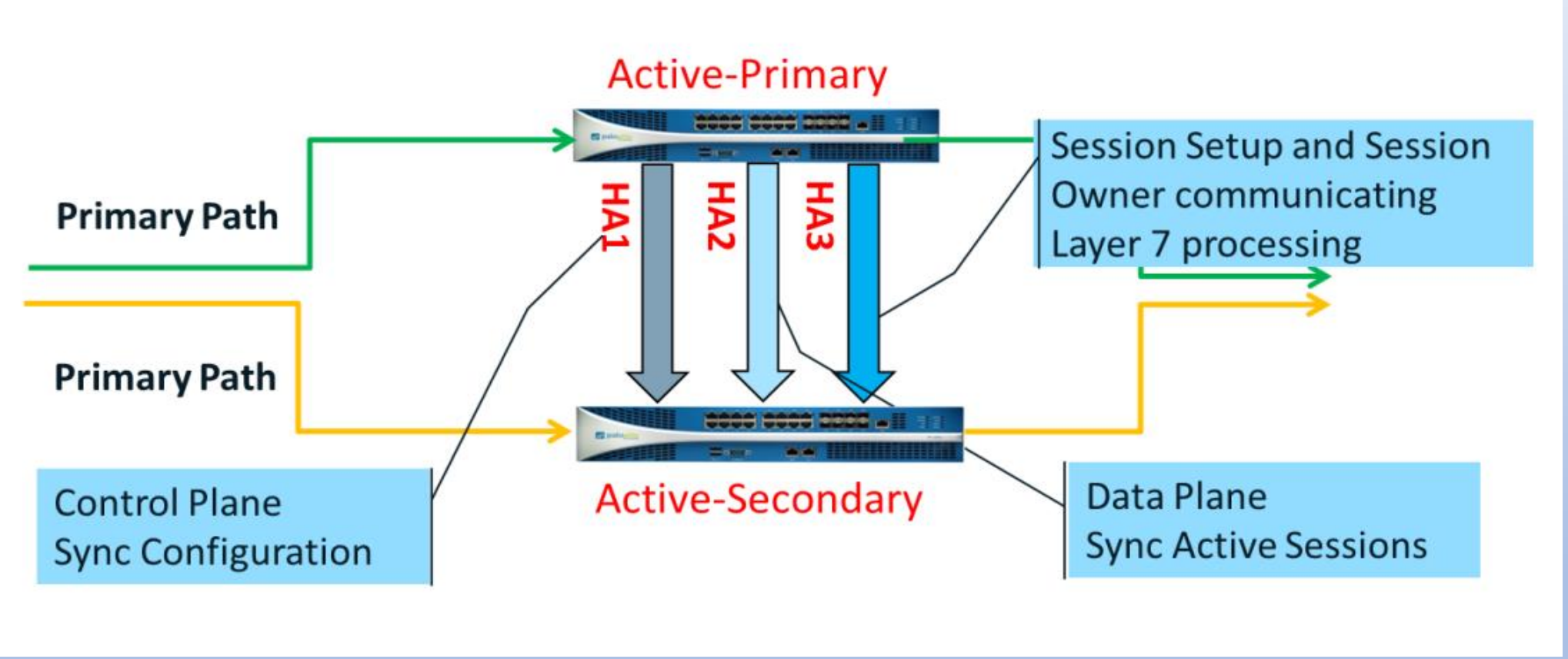
Both devices in the cluster are:

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

No increase in session capacity

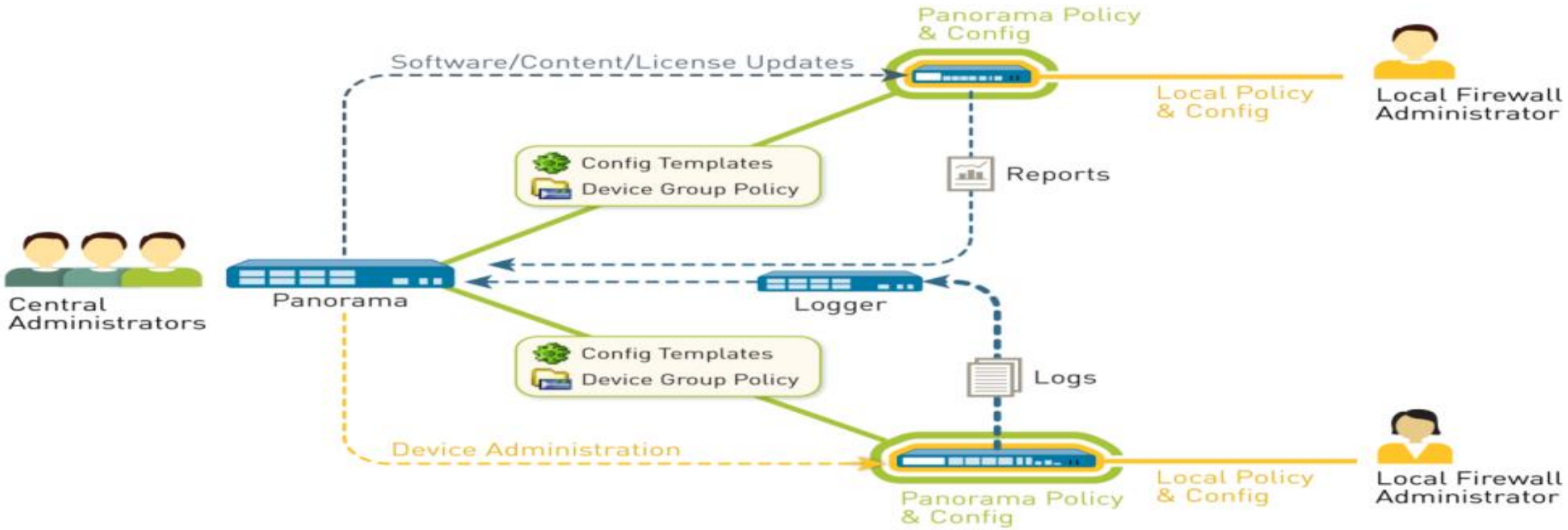
Not designed to increase throughput

Active/Active Links



Panorama

Panorama Benefits



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

Panorama Platforms

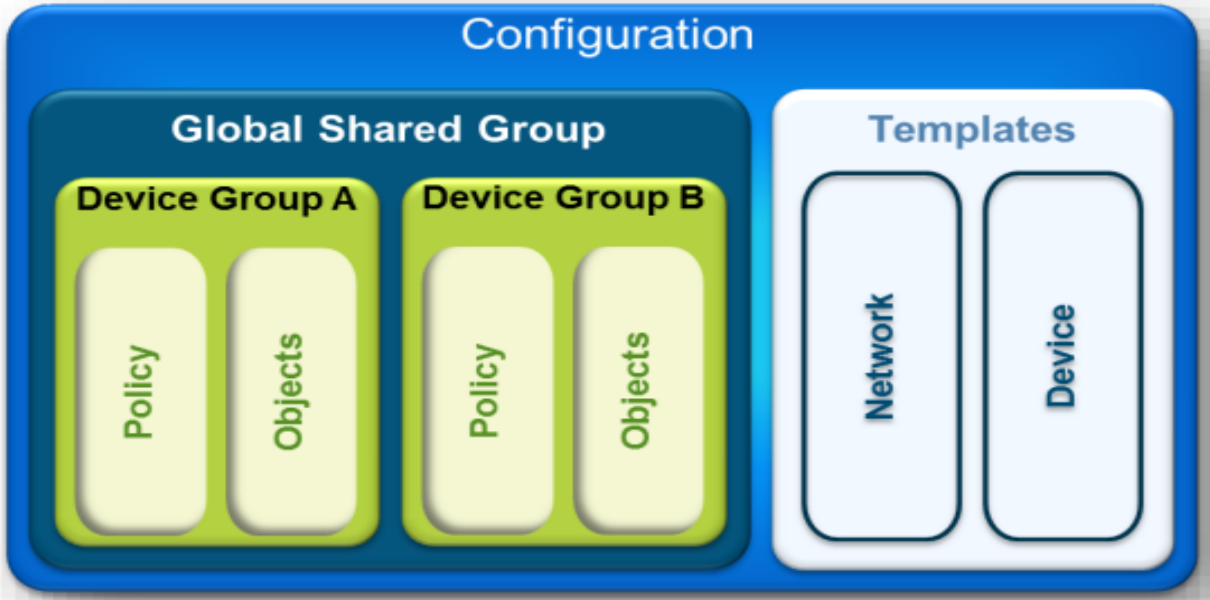
Installed on VMware, Amazon AWS or KVM

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

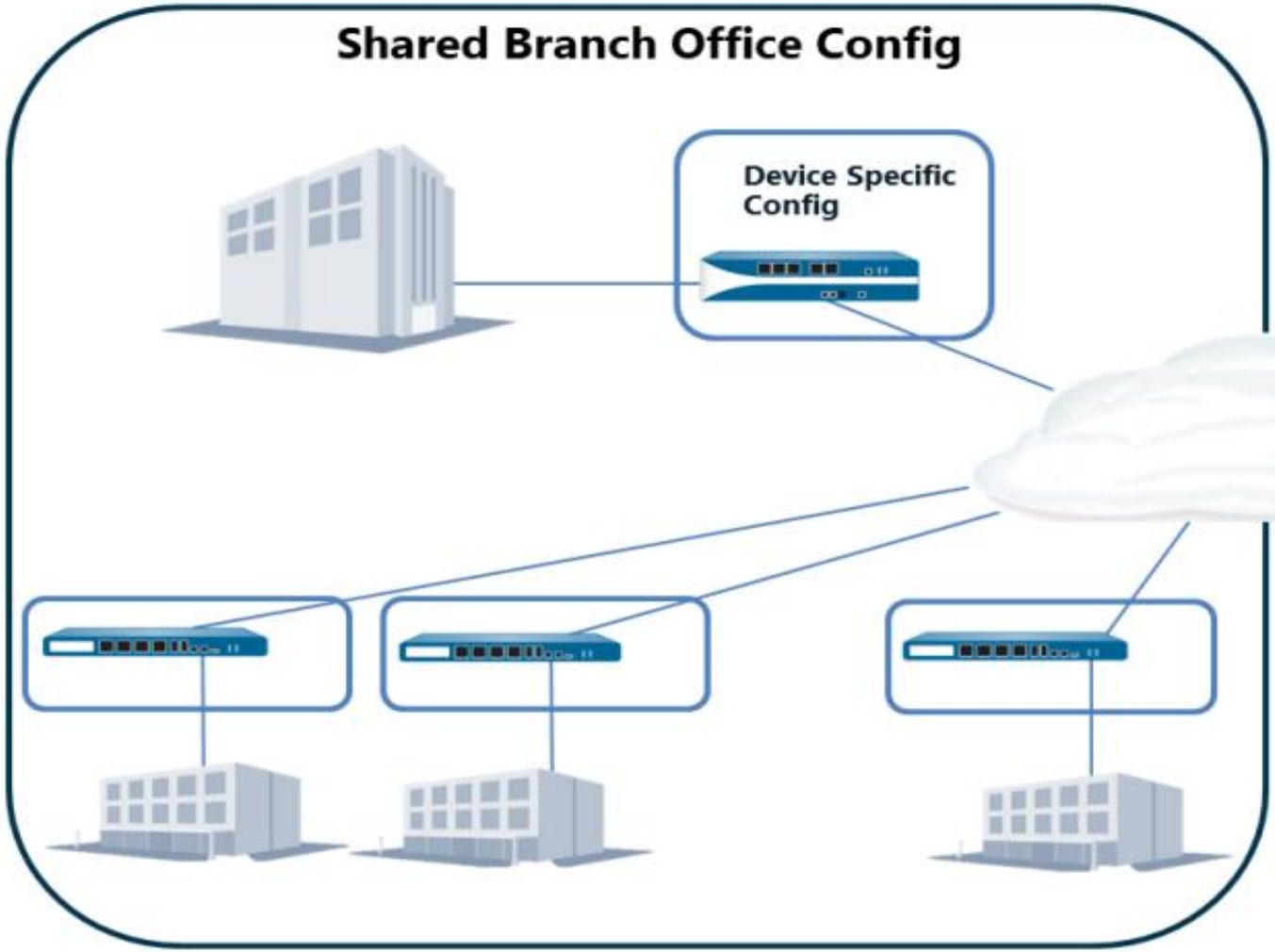
- Supports up to 100 firewalls and 10,000 logs/sec
- Can be put into distributed log architecture with dedicated Log Collectors
  - Up to 1000 firewalls
  - > 10,000 logs/sec (Max
    (Max 50,000 logs/sec per collector)

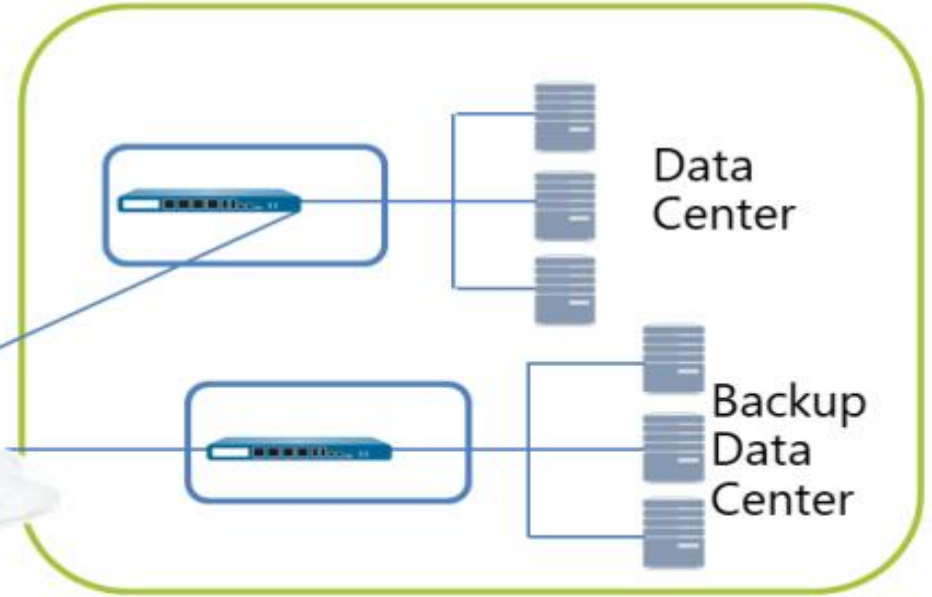
Centralized Configuration and Deployment

- 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





Most deployments have a configuration that is common between devices, as well as some device-specific configurations

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

	Source			Destination				
Name	Zone	Address	User	Zone	Address	Application	Service	Action
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	⊘


Thank you!