paloalto NETWORKS

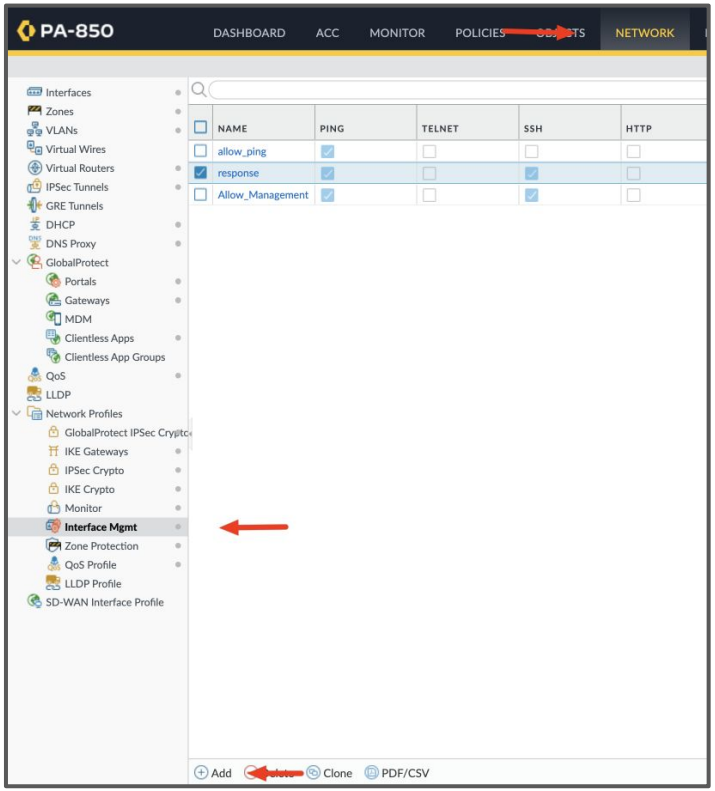
paloalto NETWORKS PCNSE

PCNSE Bootcamp v10.1

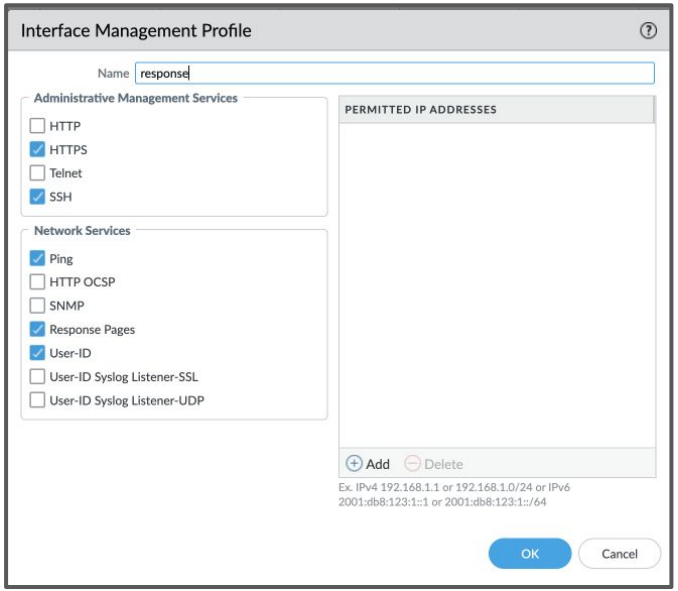
Exam Domain #2
Deploy and Configure

2.1 Configure Management Profiles

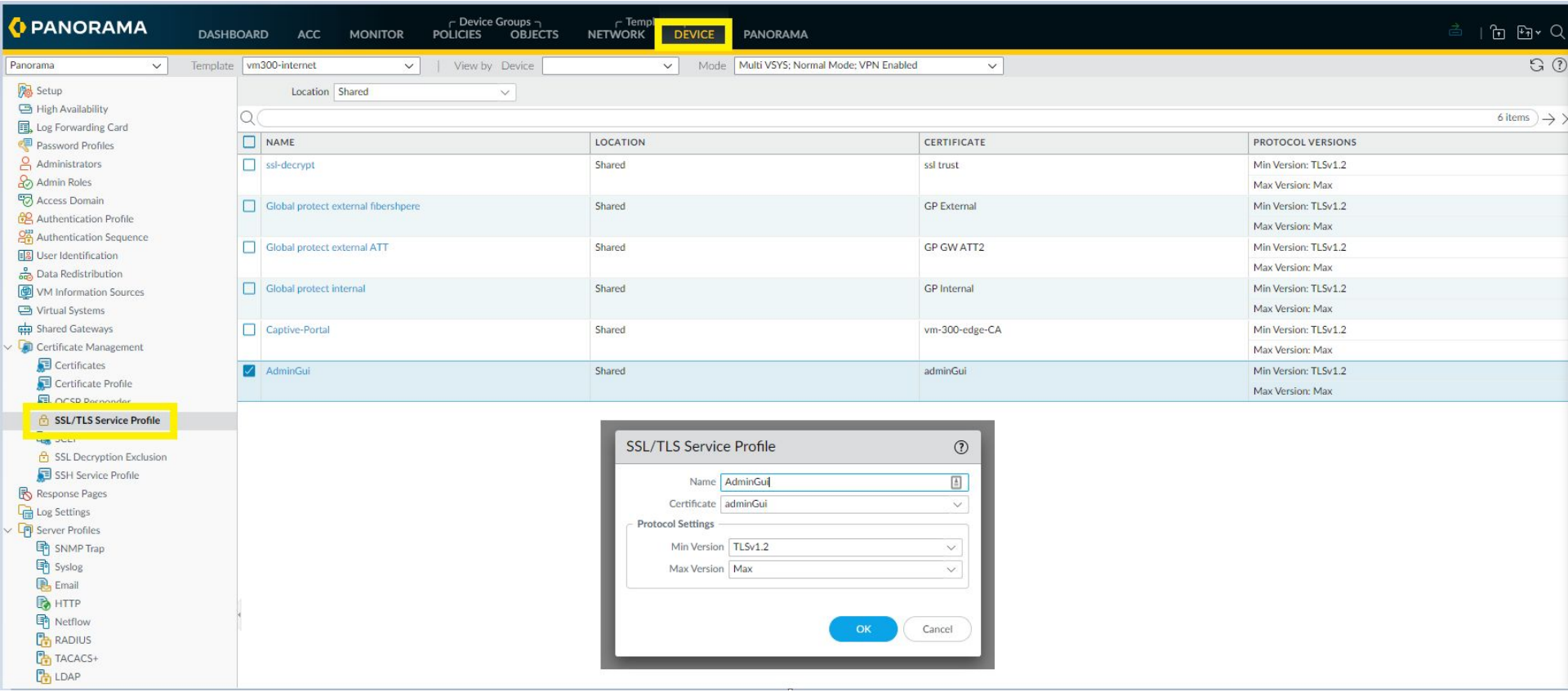
2.1.1 Interface Management Profile



- Allow you to connect to the firewall over a data interface
- It is then *applied* to the interface

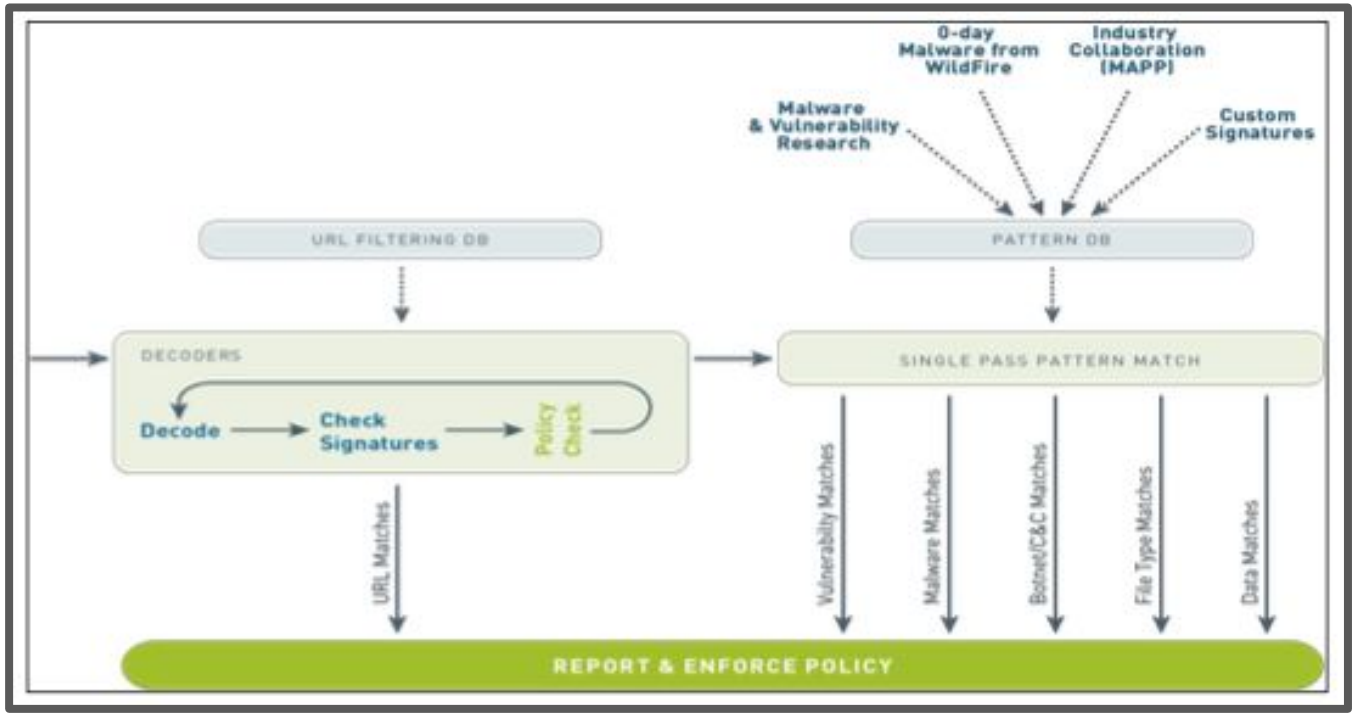


2.1.2 Configure SSL/TLS Management Profile



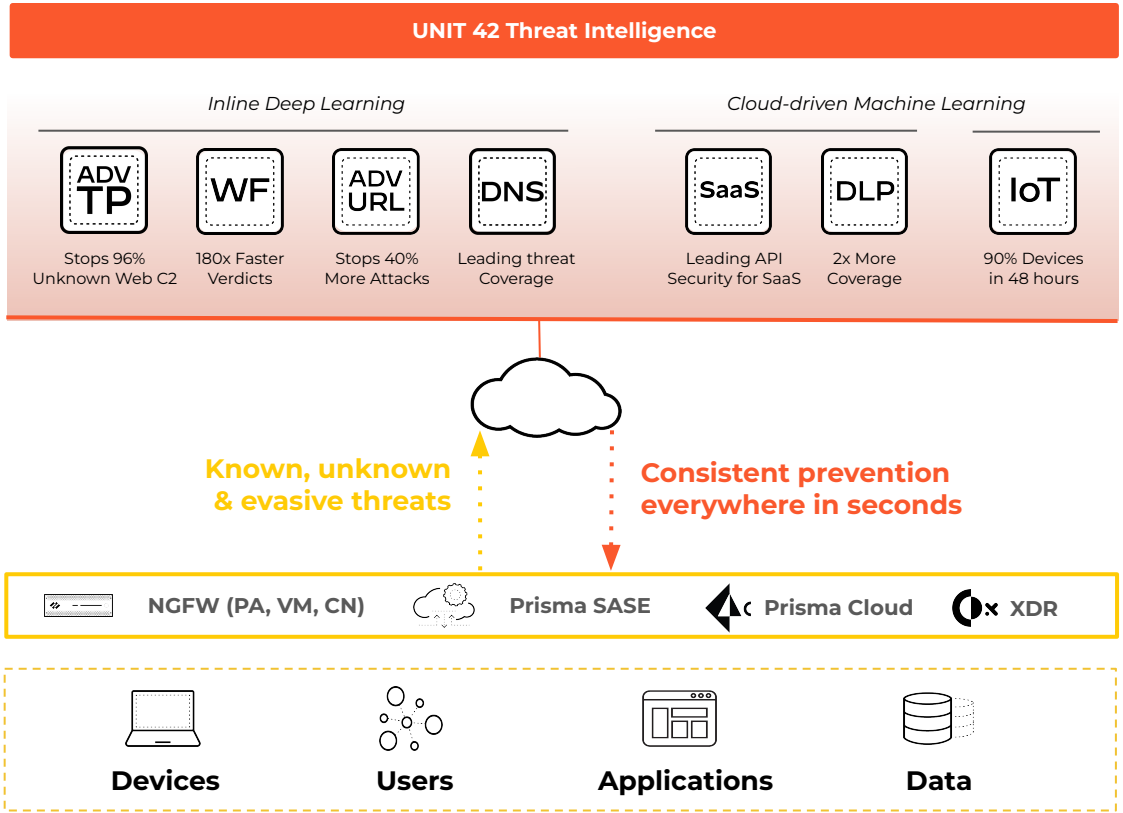
2.2 Deploy and configure Security Profiles

2.2.1 Identify and configure the different security profiles and security profile groups.



All scanning is done by signature matching on a streaming basis (not a file basis)

Palo Alto Networks' Best-In-Class Cloud-Delivered Security Services



- Industry's most comprehensive range of **proven best-in-class** security services, **delivered everywhere**.
- Shared intelligence across security product categories ensures **complete coverage across all threat vectors**, 224B threats blocked/day
- **Network effect of 85,000+ customers** turns unknown threats to prevention 180x faster and delivers over 4.3m updates/day
- **Highest efficacy and ROI** of any security vendor, providing leading security 30% faster than point solutions

2.2 Deploy and configure Security Profiles

Policies > Security

	Source				Destination								
TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
universal	Remote	any	any	any	Home Server	any	any	apple-airplay dns icmp imap ldap ping rtsp	any	any	Allow		

Antivirus

Anti-Spyware

Vulnerability Protection

URL Filtering

File Blocking

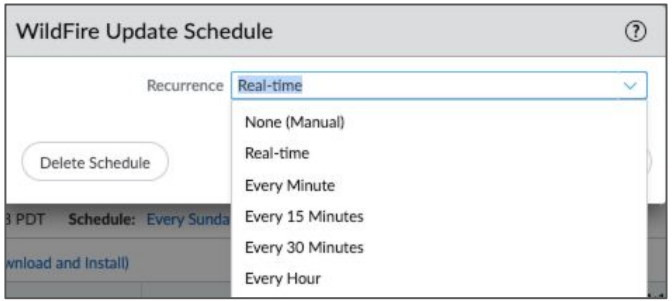
Data Filtering

WildFire Analysis

Security Profile Group

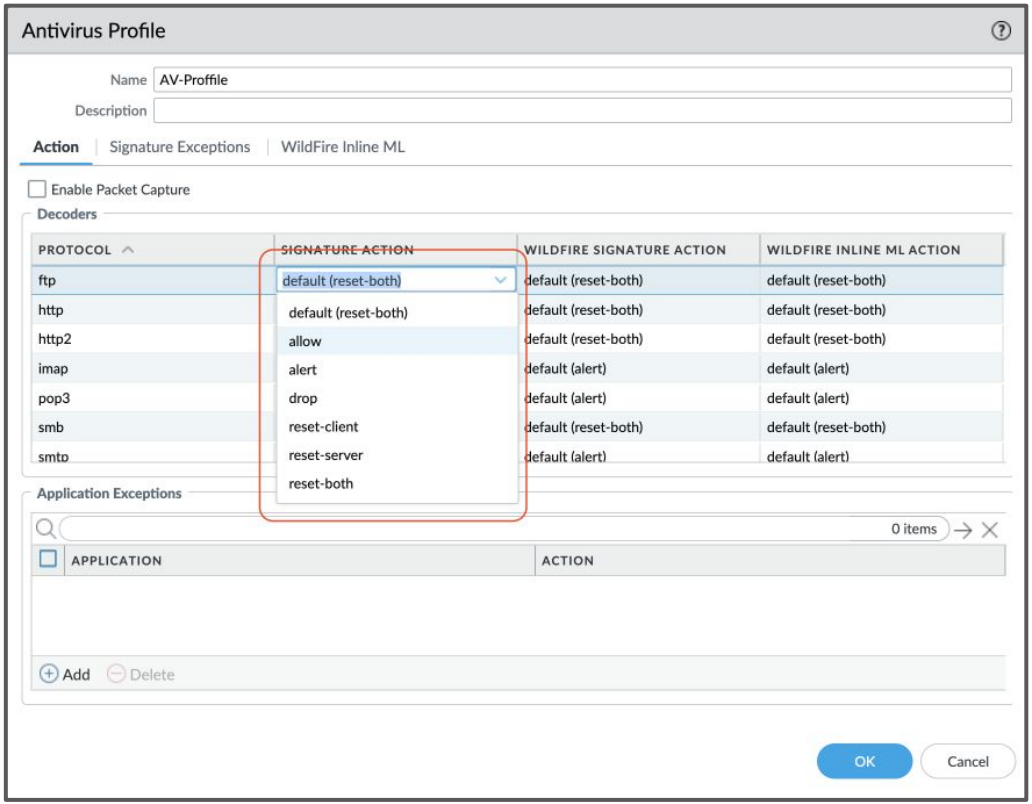
2.2 Security Profile updates

- Antivirus - updated every 24 hours (Need Threat License)
  - Includes C2 signatures
  - Updated External Dynamic Lists (high risk, bulletproof, etc)
  - DNS signatures to malicious domains
- Anti-Spyware - think C2 and DNS signatures
- URL Filtering - realtime
- Wildfire - see pict



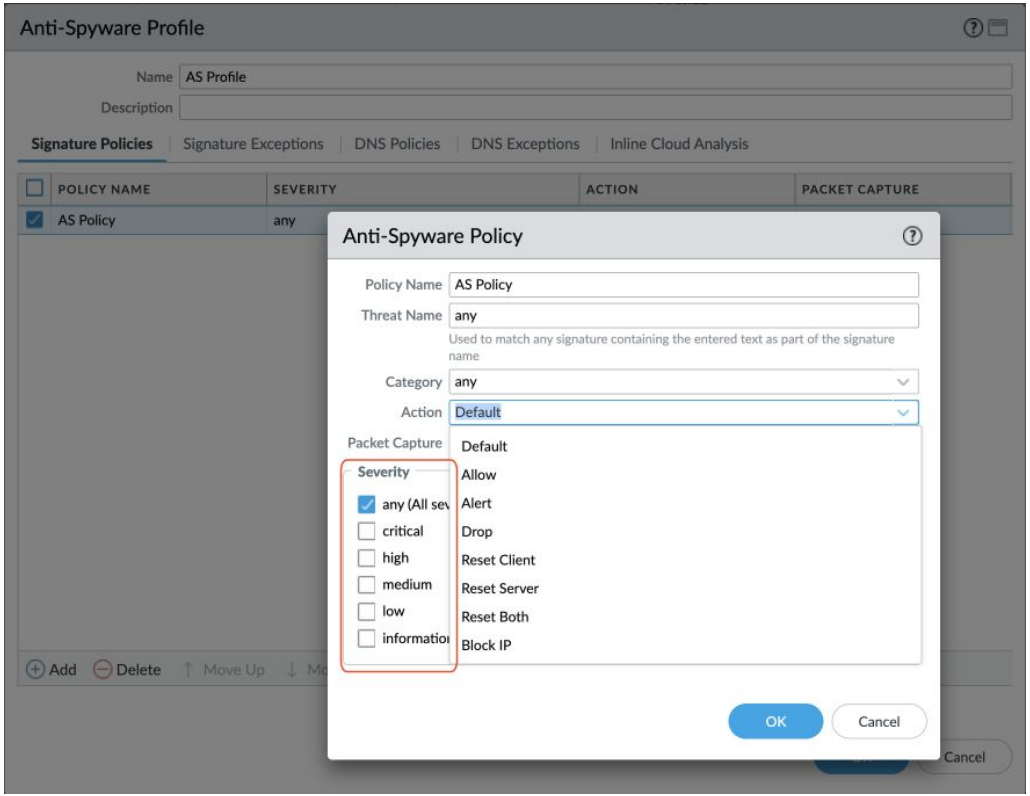
2.2 Anti-Virus

- Understand the actions
- AV is where you apply Wildfire signature actions
- Also where you apply Wildfire ML



2.2 Anti-Spyware Profiles

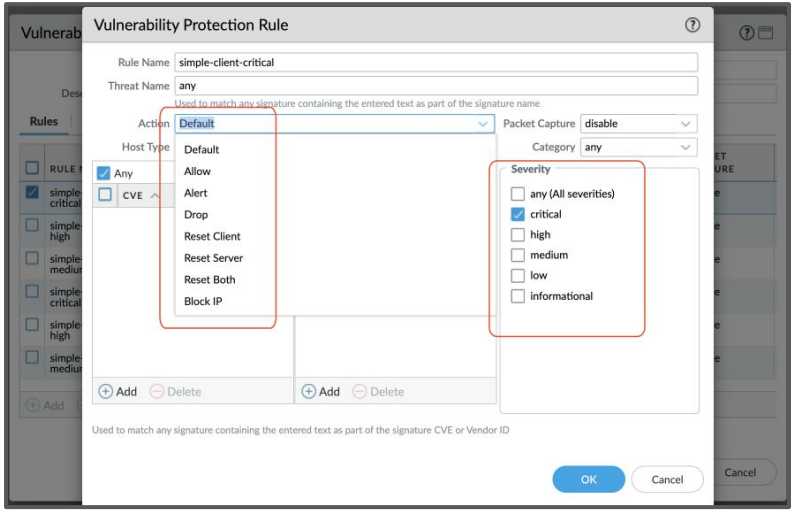
- Understand the Severity
- Know that DNS Policies are part of Anti-Spyware
- 10.2 includes the ability to inspect unknown outbound traffic

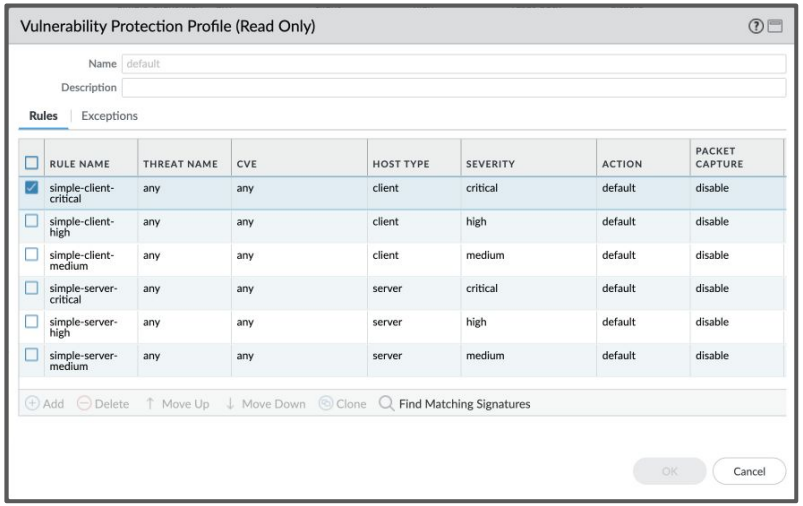


 |

2.2 Vulnerability Protection Profiles

- IPS vulnerability protection
- Understand the Actions
- Understand the Severity

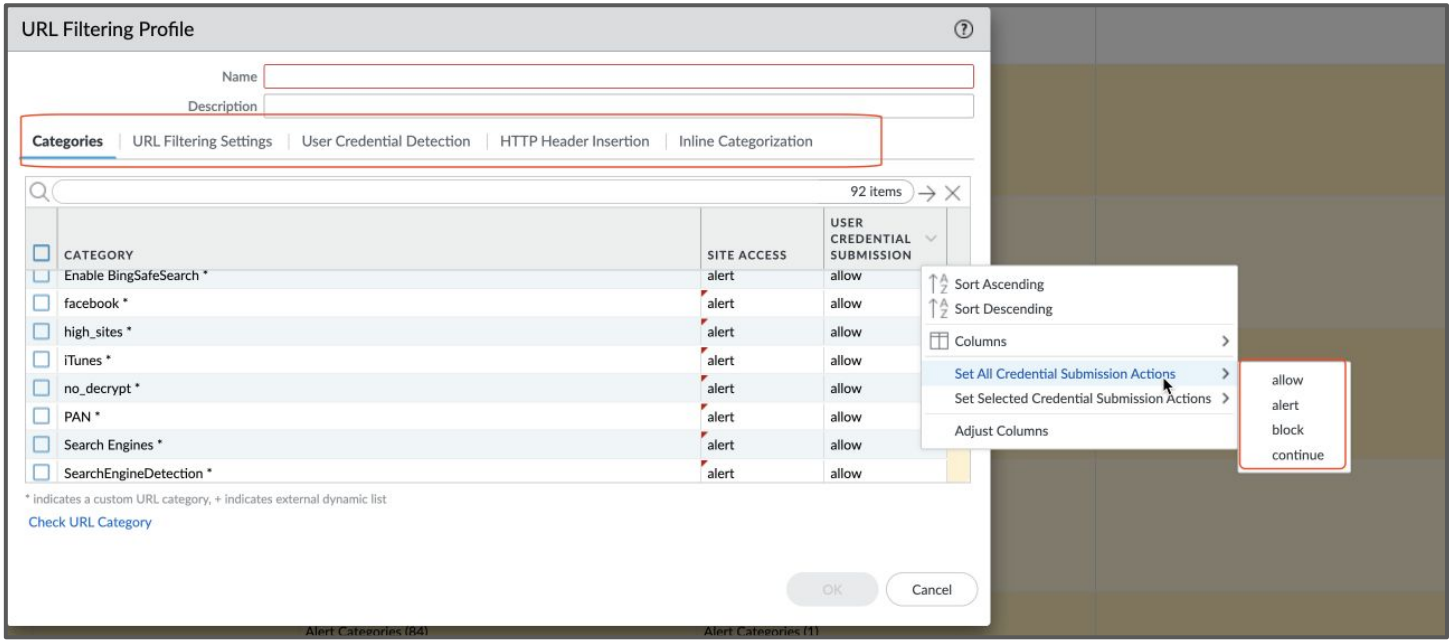




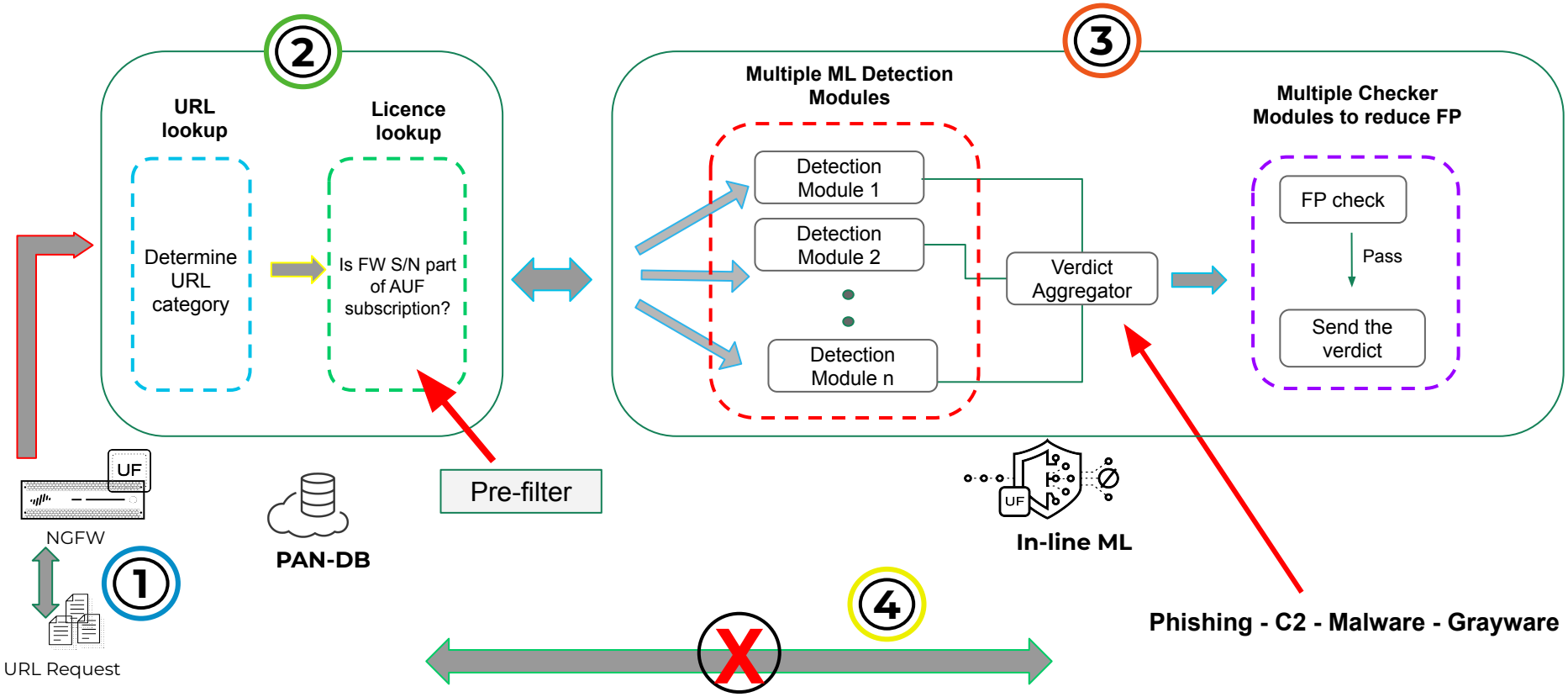
 |

2.2 URL Filtering Profiles

- Understand that there are 4 possible actions - **allow, alert, block, continue**

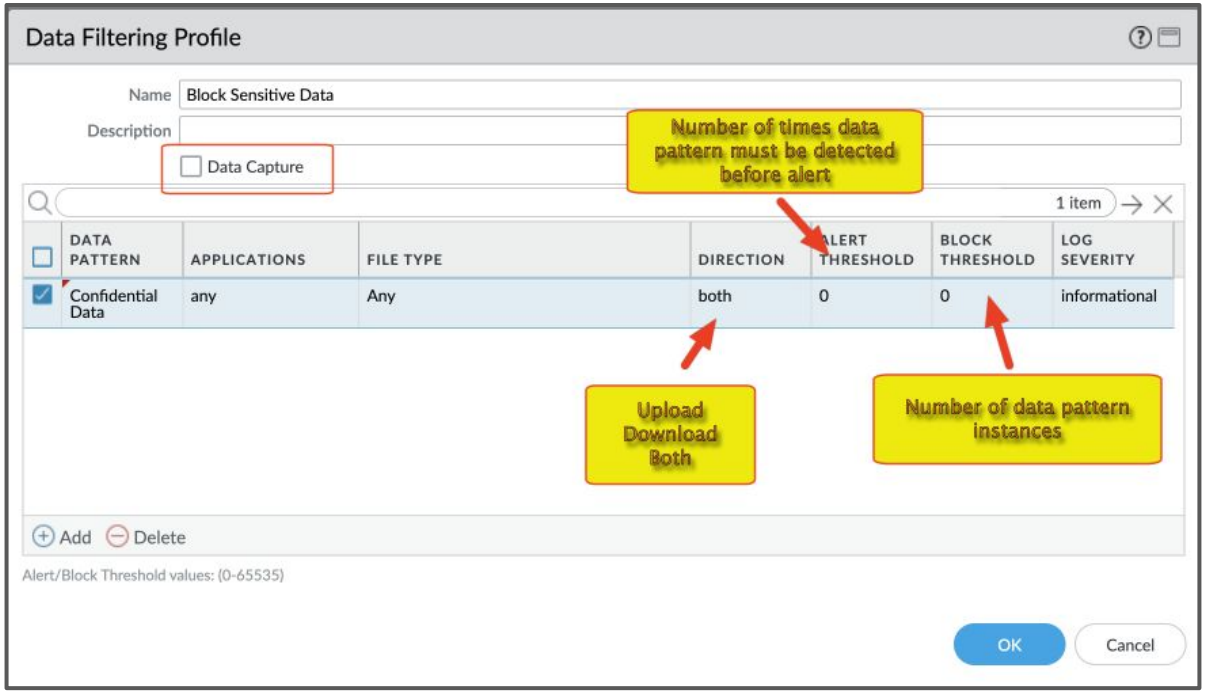


Advanced URL filtering



2.2 Data Filtering Profiles

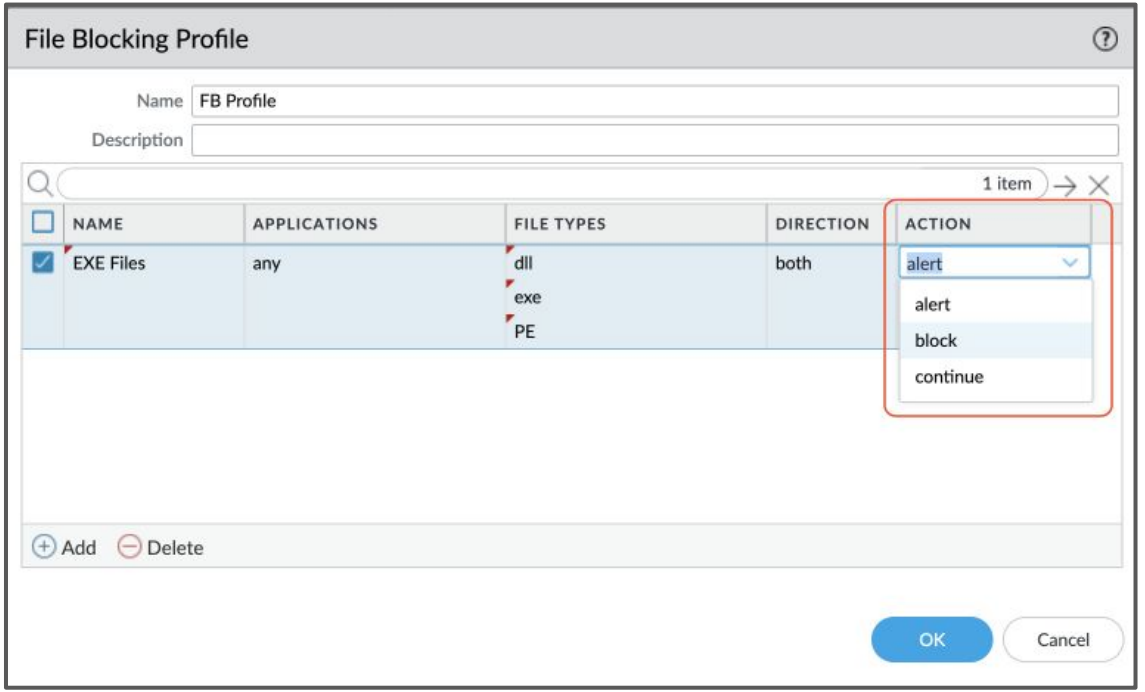
- Predefined patterns
- Regular expressions
- File properties



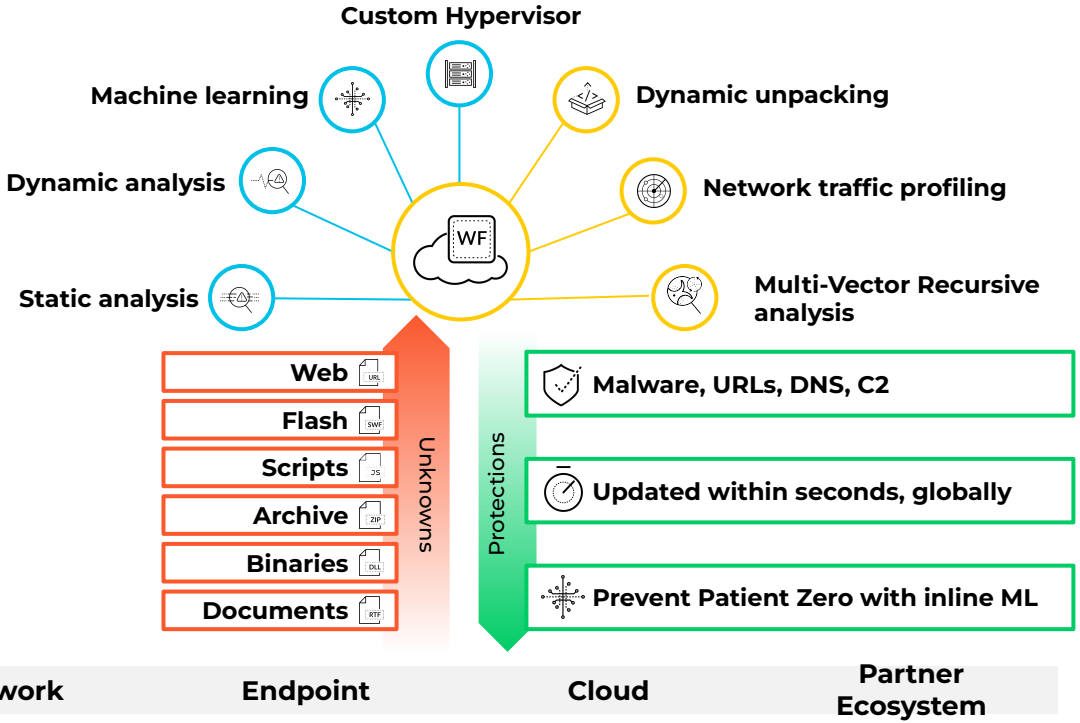
2.2 File Blocking Profiles

- Understand that there are 3 possible actions - **alert, block, continue**

Supports custom response pages



Wildfire Security profiles

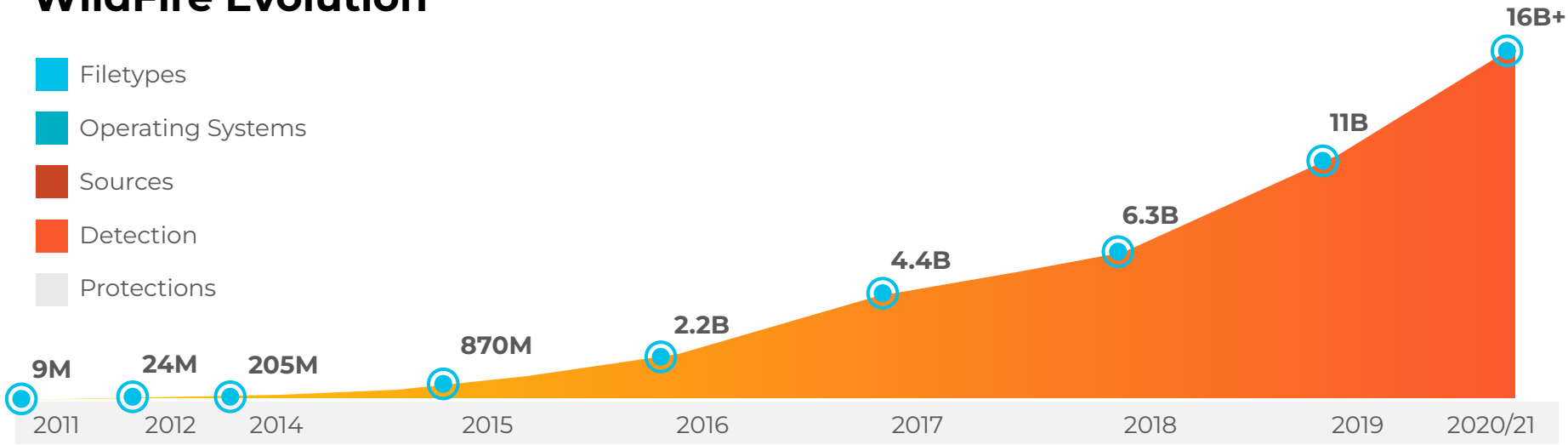


Data collected from a vast global community

Analysis techniques far beyond traditional sandboxing

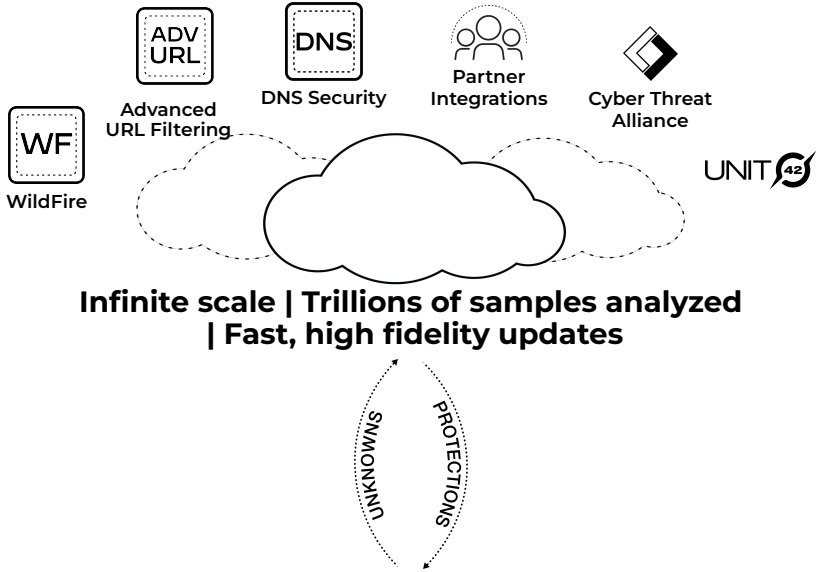
Automated protection against multiple attack variants

WildFire Evolution



2011	2012	2014	2015	2016	2017	2018	2019	2020/21
PE **Windows XP** **NGFW** **Dynamic Analysis**	PE Windows XP NGFW Dynamic Analysis 50+ Integration	PE, **PDF, Flash. MSOffice, Email Link, APK** Windows XP, **Win7, Android** NGFW, **Aperture, Traps** **CTA, 100+** Dynamic Analysis, **Static Analysis**	PE, PDF, Flash, MSOffice, Email Link, APK Windows XP, Win7, Android NGFW, Aperture, Traps CTA, 100+, **Proofpoint** Dynamic Analysis, Static Analysis	PE, PDF, Flash, **JAR,** MSOffice, Email Link, APK Windows XP, Win7, Android NGFW, Aperture, Traps, **AutoFocus** CTA, 100+, Proofpoint, **Tanium** Dynamic Analysis, Static Analysis, **Machine Learning**	PE, PDF, Flash. MSOffice, JAR, Email Link, APK, **Archives (7zip, RAR), MacOSX, ELF** Windows XP, Win7, Android, **Win10, MacOSX, Linux** NGFW, XDR, AutoFocus CTA, 100+, Proofpoint, Tanium Dynamic Analysis, Static Analysis Machine Learning, **Custom Hypervisor, Bare Metal Analysis**	PE, PDF, Flash. MSOffice, JAR, Email Link, APK, Archives (7zip, RAR), MacOSX, **Scripts** Windows XP, Win7, Android, Win10, MacOSX, Linux NGFW, XDR, AutoFocus, CTA, 100+, Proofpoint, Tanium Dynamic Analysis, Static Analysis, Machine Learning, Custom Hypervisor, Bare Metal Analysis, **Dynamic Unpacking, Network Pattern Matching**	PE, PDF, Flash. MSOffice, JAR, Email Link, APK, Archives (7zip, RAR), MacOSX, **Scripts** Windows XP, Win7, Android, Win10, MacOSX, Linux NGFW, XDR, AutoFocus, CTA, 100+, Proofpoint, Tanium Dynamic Analysis, Static Analysis, Machine Learning, Custom Hypervisor, Bare Metal Analysis, Dynamic Unpacking, Network Pattern Matching, **Recursive analysis, Multi-Vector Recursive Analysis, Inline Machine Learning detection, Hornet Engine Static Analysis**
24 hours	**24 hours**	**30 mins**	**30 mins**	**15 mins**	**5 mins**	**5 mins**	**Zero-delay/real-time**	

Preventing Unknown Threats Through Cloud Scale and Inline ML



Up to 95% of common file & web-based threats prevented in-line

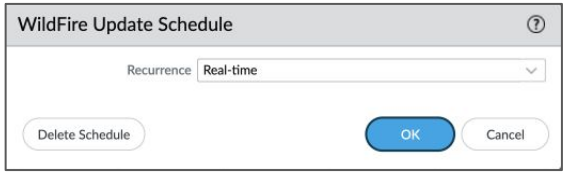
Cloud-delivered security services **scale prevention** capabilities

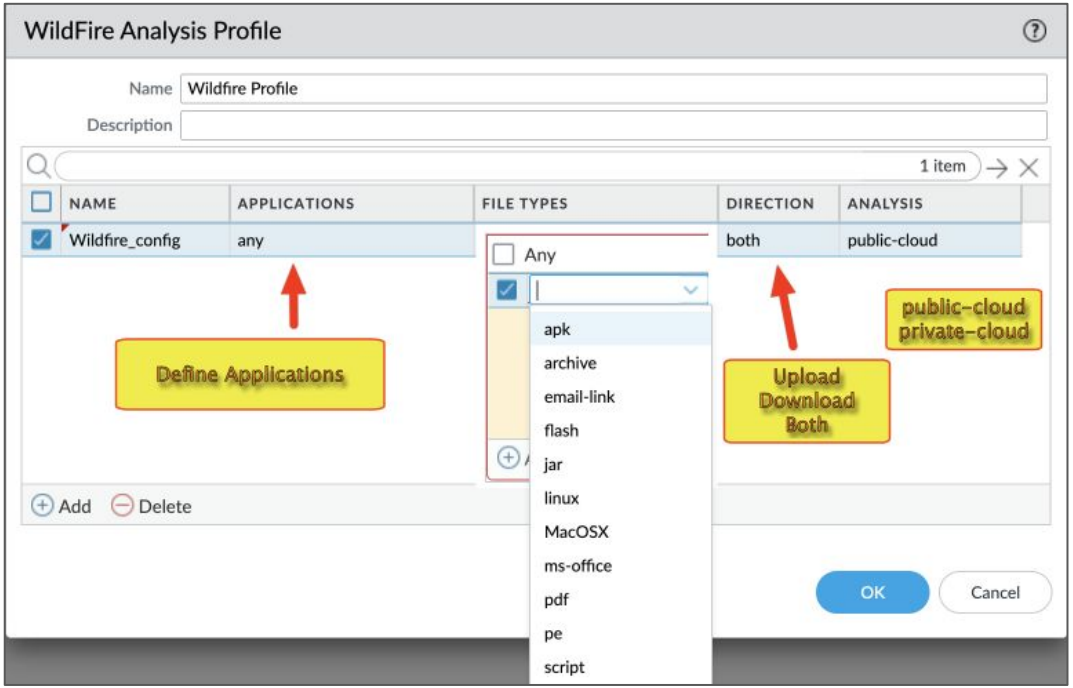
Shared intelligence allows the **fastest distribution** of protections

- File Protections: **Instant**
- URL Protections: **Instant**
- DNS Protections: **Instant**

2.2 Wildfire Profiles

- WildFire typically renders a verdict on a file within 5 to 10 minutes of receipt
- Files are installed within AV Dynamic updates are “realtime”

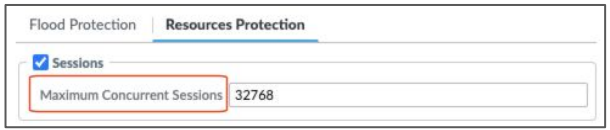


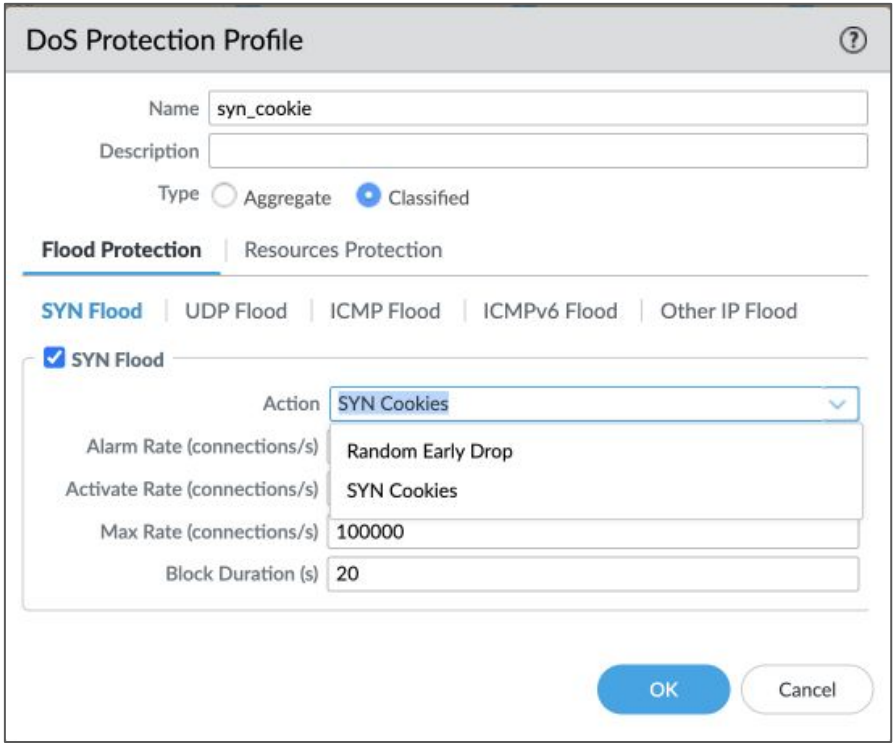


Note: Files are not quarantined pending WildFire evaluation. In cases of positive malware findings, the security engineer must use information collected on the firewall and by WildFire to locate the file internally for remediation.

2.2 DOS Protection Profiles

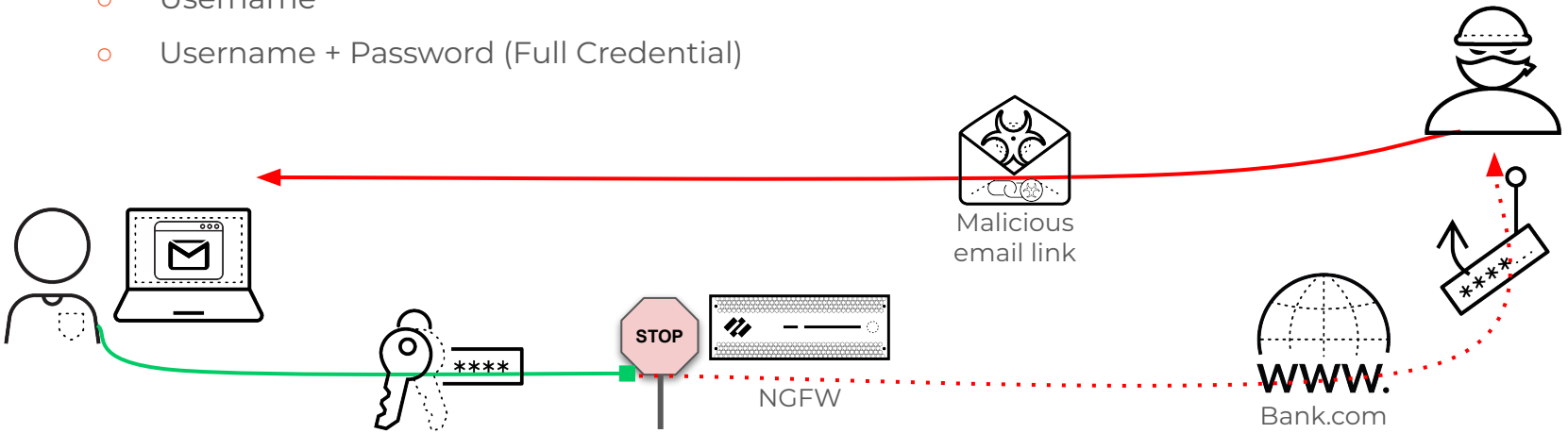
- Flood Protection
- Resources Protection
- Applied at the rule layer





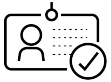
Preventing Credential Phishing with Palo Alto Networks

- URL Filtering profiles control (allow, alert, block, continue, override):
  - Site Access
  - Credential Submission
- Credential mapping by
  - User group membership
  - Username
  - Username + Password (Full Credential)



Prerequisites

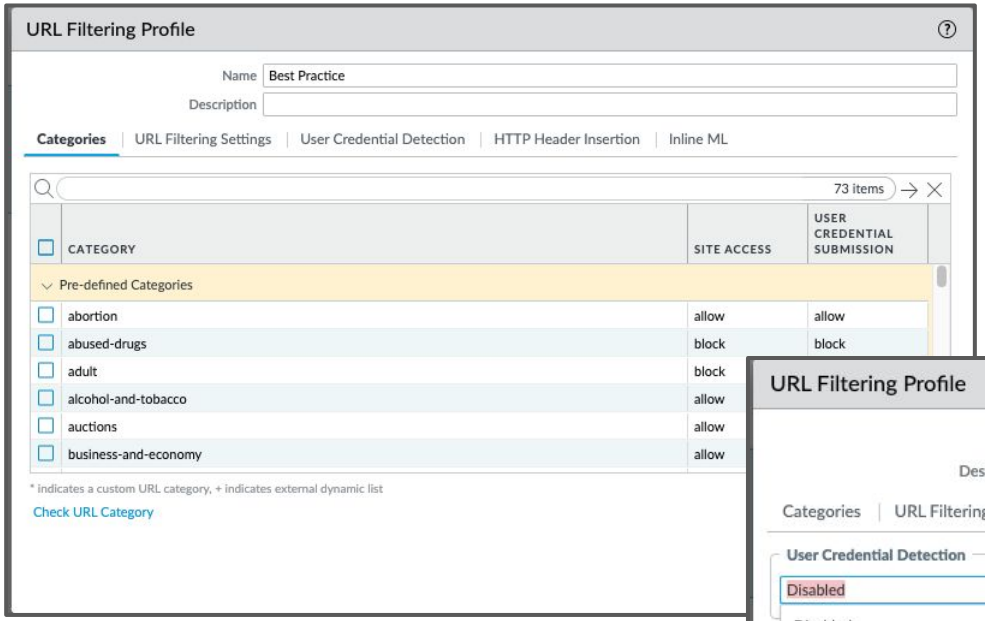
What you need in place before beginning the firewall configuration

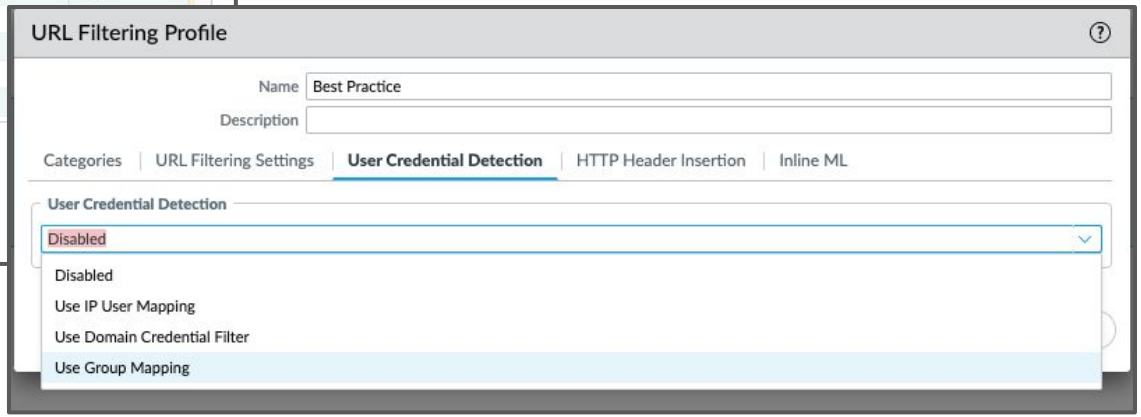
-  **Active URL Filtering Subscription**
-  **User-ID**
-  **SSL Decryption**

3 Options to Check for Credential Submissions

METHOD TO CHECK CREDENTIALS	USER-ID CONFIGURATION REQUIREMENT	HOW THIS METHOD DOES THE DETECTION
Group Mapping	Configured on Firewall	• Firewall checks if username matches any valid corporate username. • Matches to the list of usernames in its user-to-group mapping table. • This method only checks for corporate username submissions based on LDAP group membership. • **Simple to configure, but more prone to false positives**.
IP User Mapping	IP address-to- username mappings identified through User Mapping, GlobalProtect, or Authentication Policy and Authentication Portal.	• Firewall checks if username maps to the IP address of the login username. • Matches the IP address of the login username and the username submitted to a web site to its IP address-to-user mapping table. • **More of an effective method, but it does not detect password submissions**.
Domain Credential Filter	Windows User-ID agent configured with the User-ID credential service add-on -AND- IP address-to- username mappings identified through User Mapping, GlobalProtect, or Authentication Policy and Authentication Portal.	• Firewall checks if username and password match the same user's corporate username and password. • Windows User-ID agent with add-on service scans your directory (**only supported on RoDC**) for usernames and password hashes and deconstructs them into a secure bit mask known as a bloom filter. The firewall retrieves the bloom filter at regular intervals and reconstructs the bloom filter in order to look for hash matches. • **Most accurate match but would not prevent mis-typed credentials.**

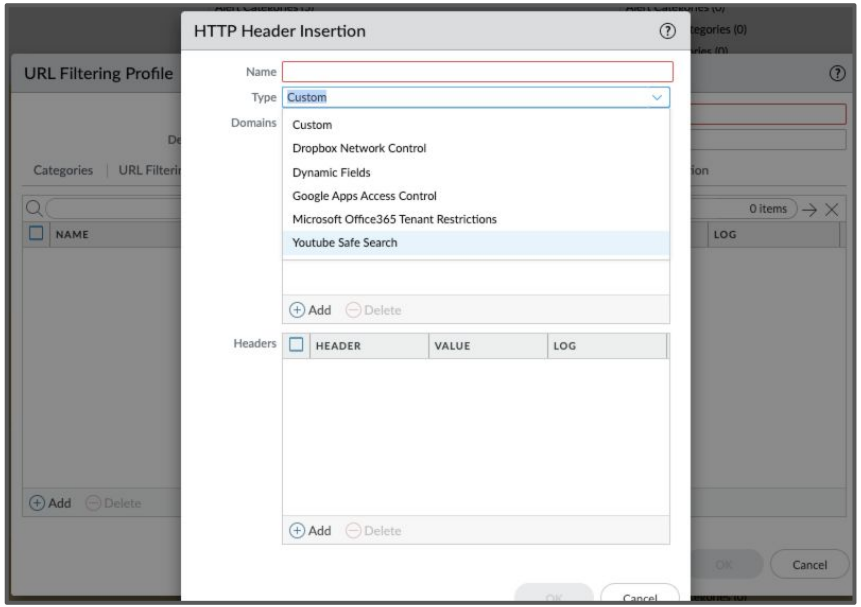
2.2.2 Relationship between URL filtering and credential theft prevention



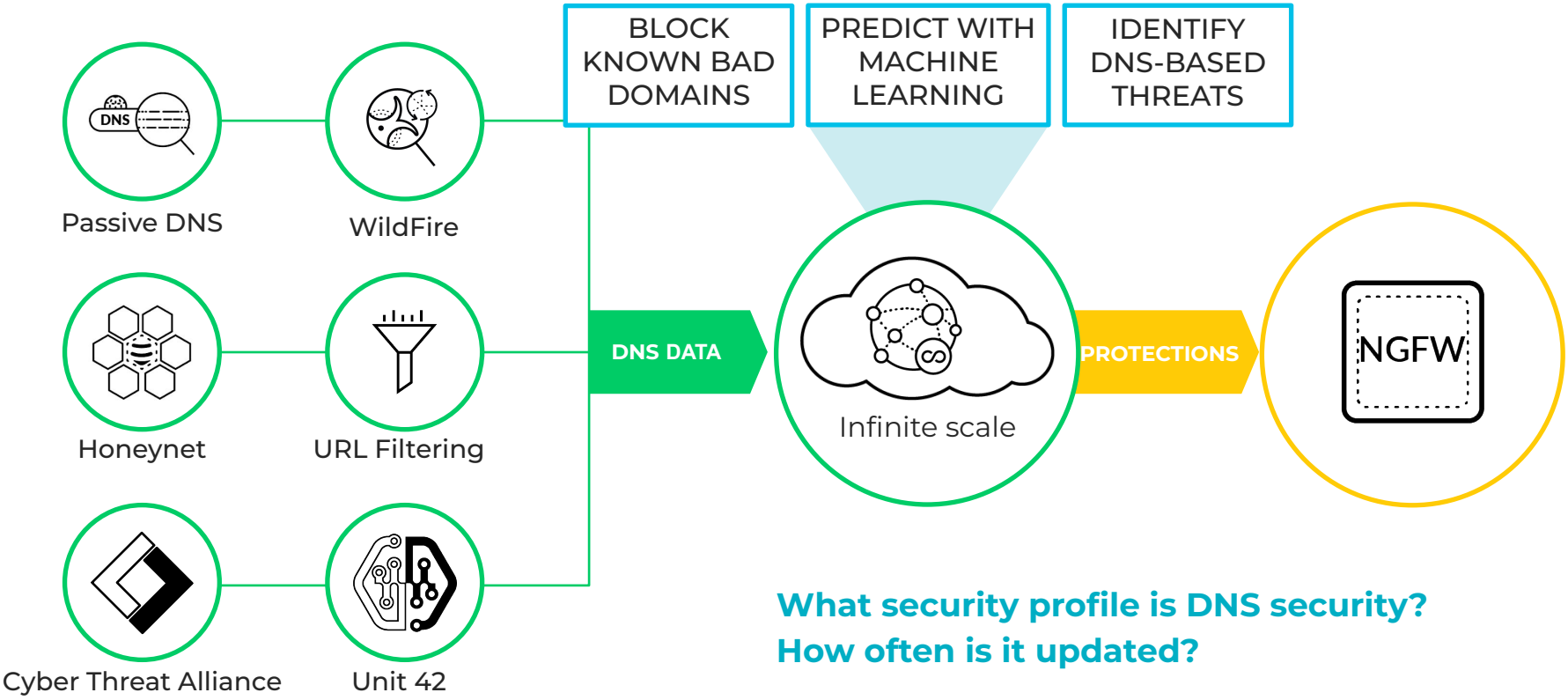


2.2.3 Use of username and domain name in HTTP header insertion

- HTTP header insertion is only available for HTTP/1.x traffic - NOT HTTP/2 traffic
- Supported for GET, POST, PUT and HEAD

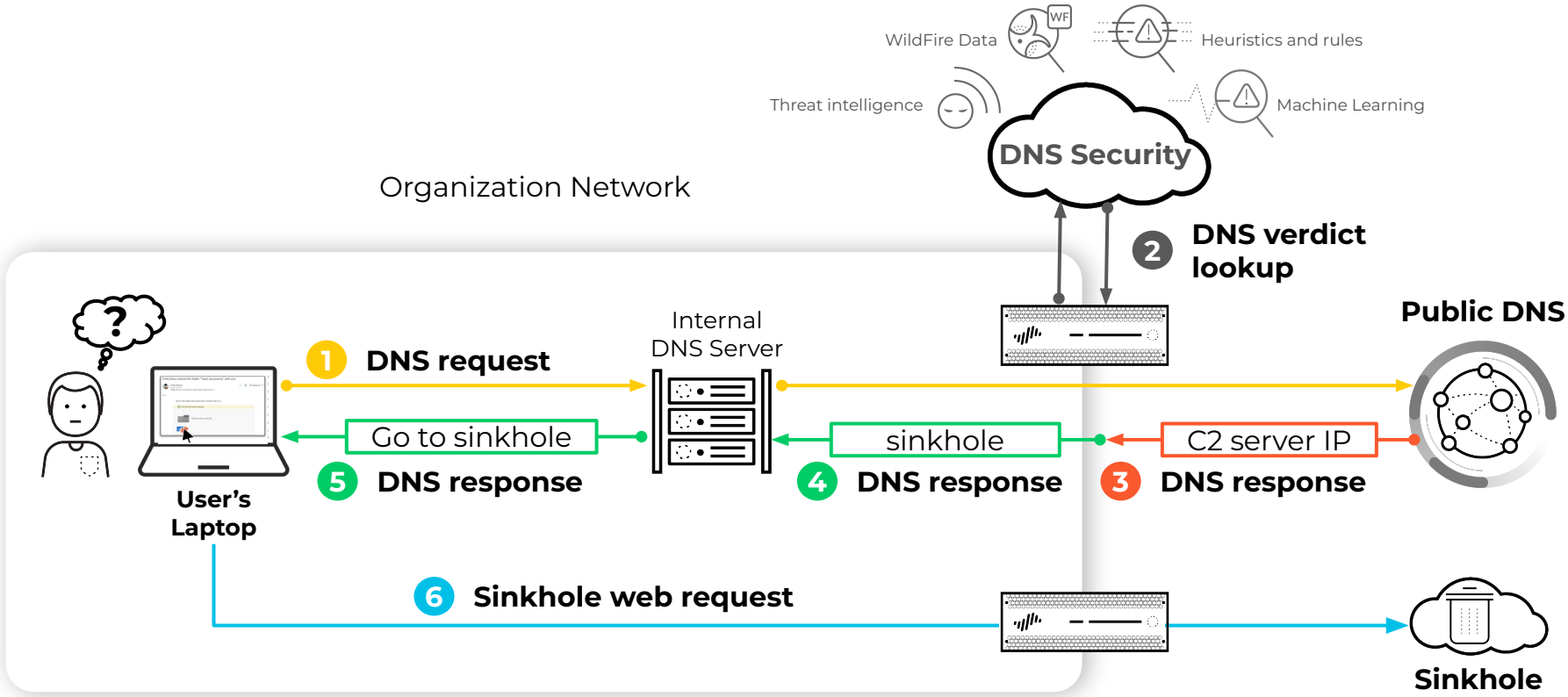


2.2.4 DNS Security



What security profile is DNS security?
How often is it updated?

DNS Security: Disrupting Attacks With Machine Learning

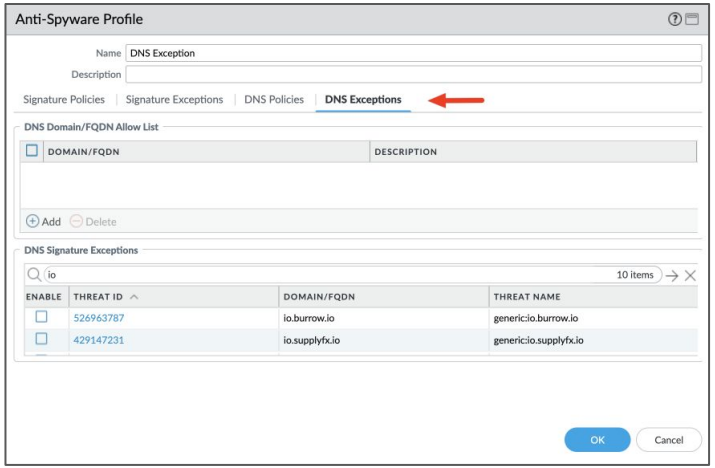


 |

2.2.5 How to tune or add exceptions to a Security Profile

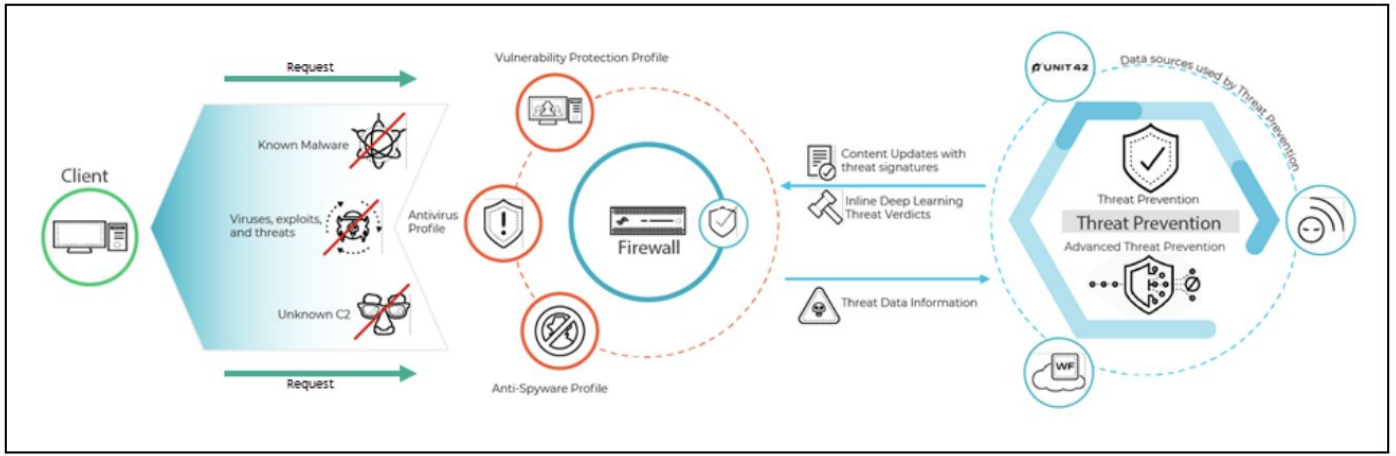
Configure threat exceptions for antivirus, vulnerability, spyware, and DNS signatures to change firewall enforcement for a threat.

Step 1: Exclude antivirus signatures from enforcement.
Step 2: Modify enforcement for vulnerability and spyware signatures. (This does not include DNS signatures;
skip to the next option to modify enforcement for DNS signatures, which are a type of spyware signature.)
Step 3: Modify enforcement for DNS signatures.



2.2.6 Compare and contrast threat prevention and advanced threat prevention

- **Antivirus** signatures detect various types of malware and viruses, including worms, Trojan horses, and spyware downloads.
- **Anti-spyware** signatures detect C2 spyware on compromised hosts that try to phone-home or beacon out to an external C2 server.
- **Vulnerability** signatures detect exploit system vulnerabilities.
- SNORT and Suricata rules, custom signatures can be created for purpose-built protection.



Defense in Depth across the Attack Lifecycle

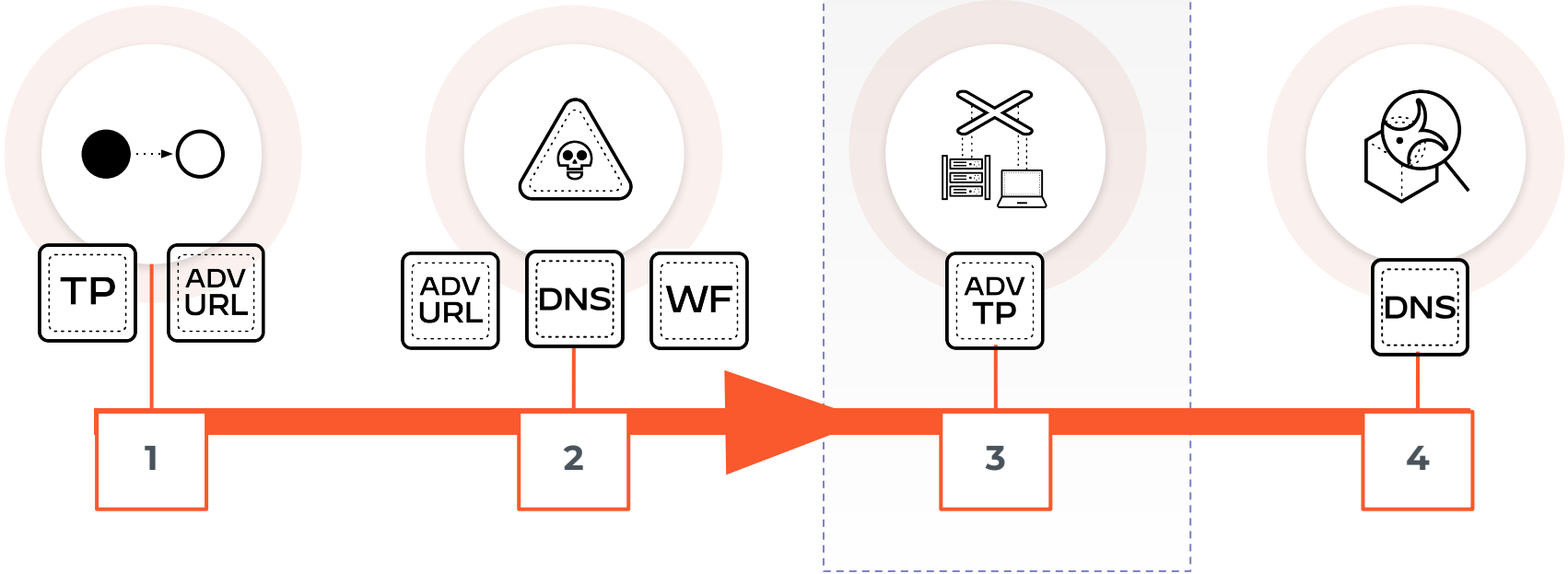
Exploit blocked by **Threat Prevention**
Evasive Phishing blocked by **Adv URL Filtering**

Malware download blocked by **Adv URL Filtering, DNS Security and WildFire**

New

Unknown C2 blocked by **Adv Threat Prevention**

Data exfil blocked by **DNS Security**



Advanced Threat Prevention - Looking for Unknown C2 traffic

Advanced Threat Prevention NEW

Threat Prevention

Best-in-class IPS

- Leading signature-based prevention for **known exploits, web threats, C2, and malware**
- Predictable performance using **single pass architecture**
- **Content updates** delivered Daily/Weekly* and customized detection with **Snort/Suricata**

Stop Unknown C2 In-line

- Prevents **unknown C2** traffic **over SSL**, HTTP, unknown-tcp and unknown-udp applications
- Stops evasive C2 derived from hack tools such as **Cobalt Strike**
- Automated **False Positive Correction** service

Infinitely Scalable Cloud-based ML

- Purpose built **Machine Learning** and **Inline Deep Learning** models
- Leverages **high fidelity** WildFire dataset from 85,000+ customers to train ML models
- **Cloud-native service** always up to date and able to expand over time

* Updates can delivered in seconds or less with additional Security Services (WildFire, etc)

2.2.7 Compare and contrast URL Filtering and Advanced URL Filtering

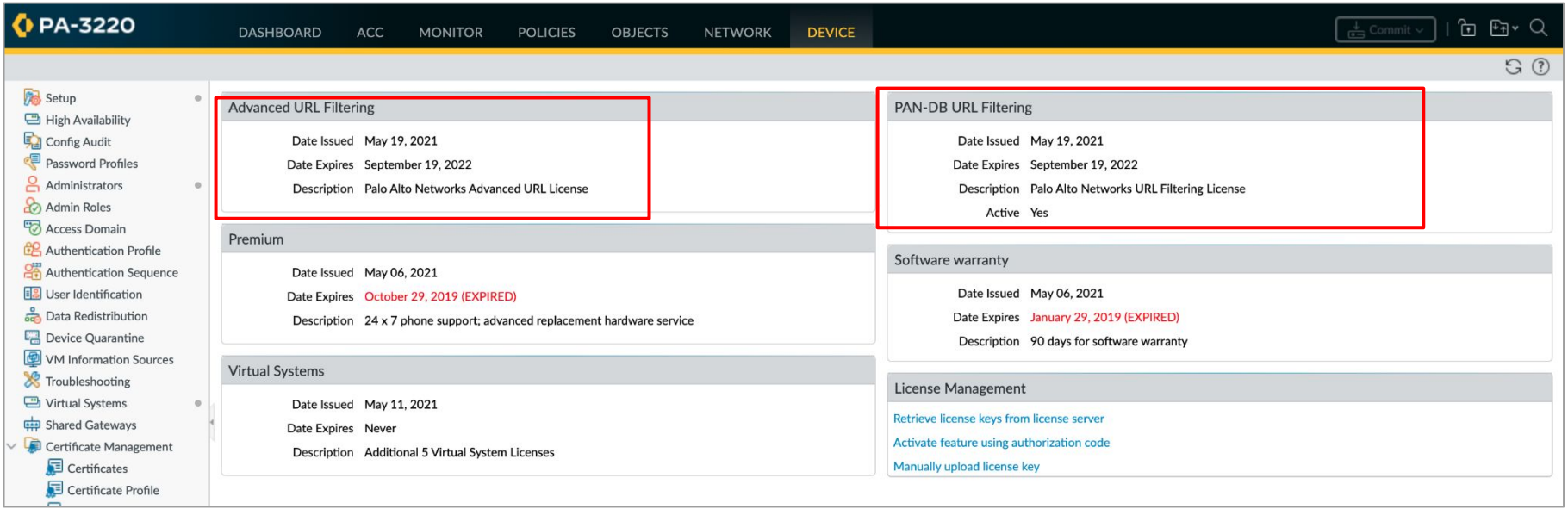
Advanced URL Filtering uses ML to analyze URLs in *real time* and classify them into benign or malicious categories, which you can easily build into your NGFW policy for total control of web traffic.

When a user visits a URL designated as risky, the firewall submits the URL to the advanced URL filtering service for machine learning analysis and searches PAN-DB for the site's category

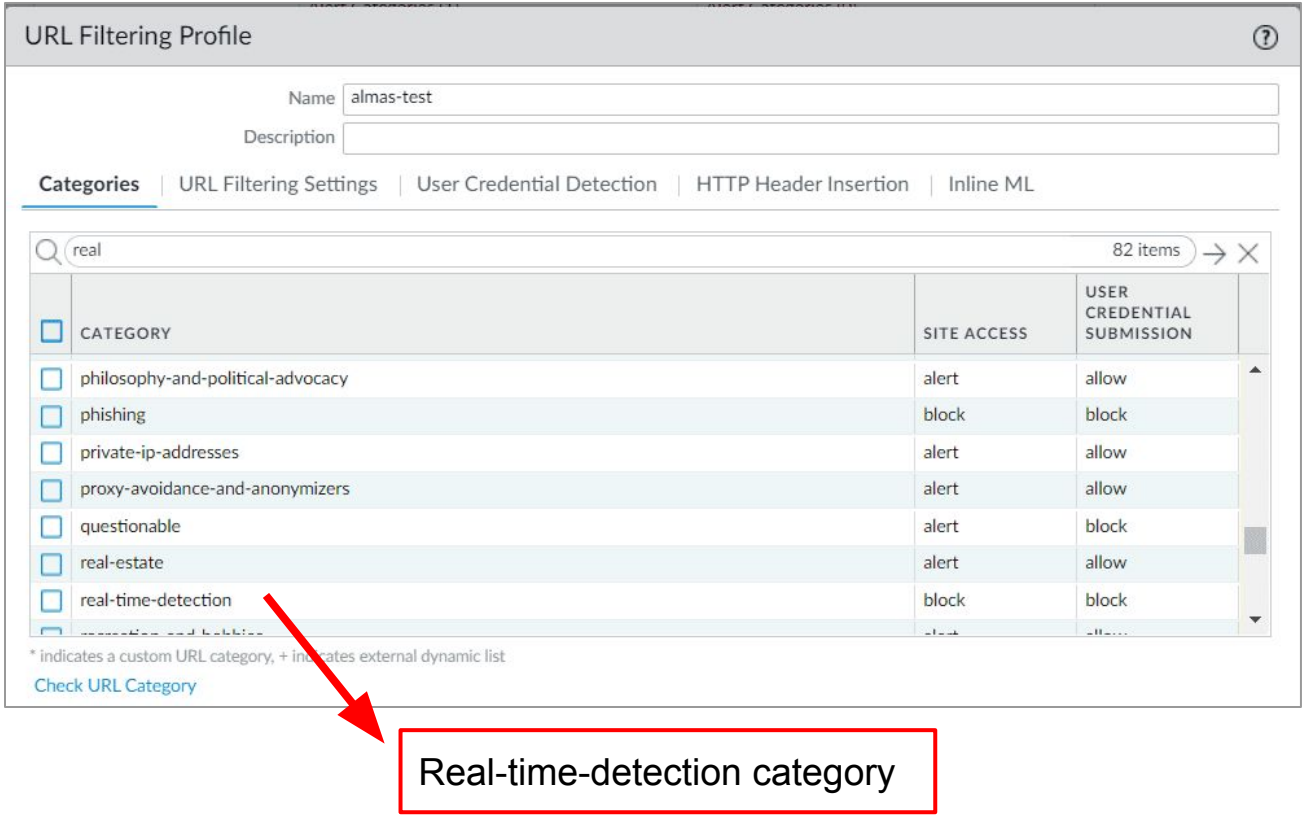
```
admin@firewall> show url-cloud status

PAN-DB URL Filtering
License :                          valid
libcurl resolver :                 threaded
Current cloud server :             serverlist2.urlcloud.paloaltonetworks.com
Cloud connection :                 connected
Cloud mode :                       public
URL database version - device :    20220920.20059
URL database version - cloud :     20220920.20059  ( last update time 2022/09/19 20:52:04 )
URL database status :              good
URL protocol version - device :    pan/2.0.0
URL protocol version - cloud :     pan/2.0.0
Protocol compatibility status :    compatible
```

License Allocation

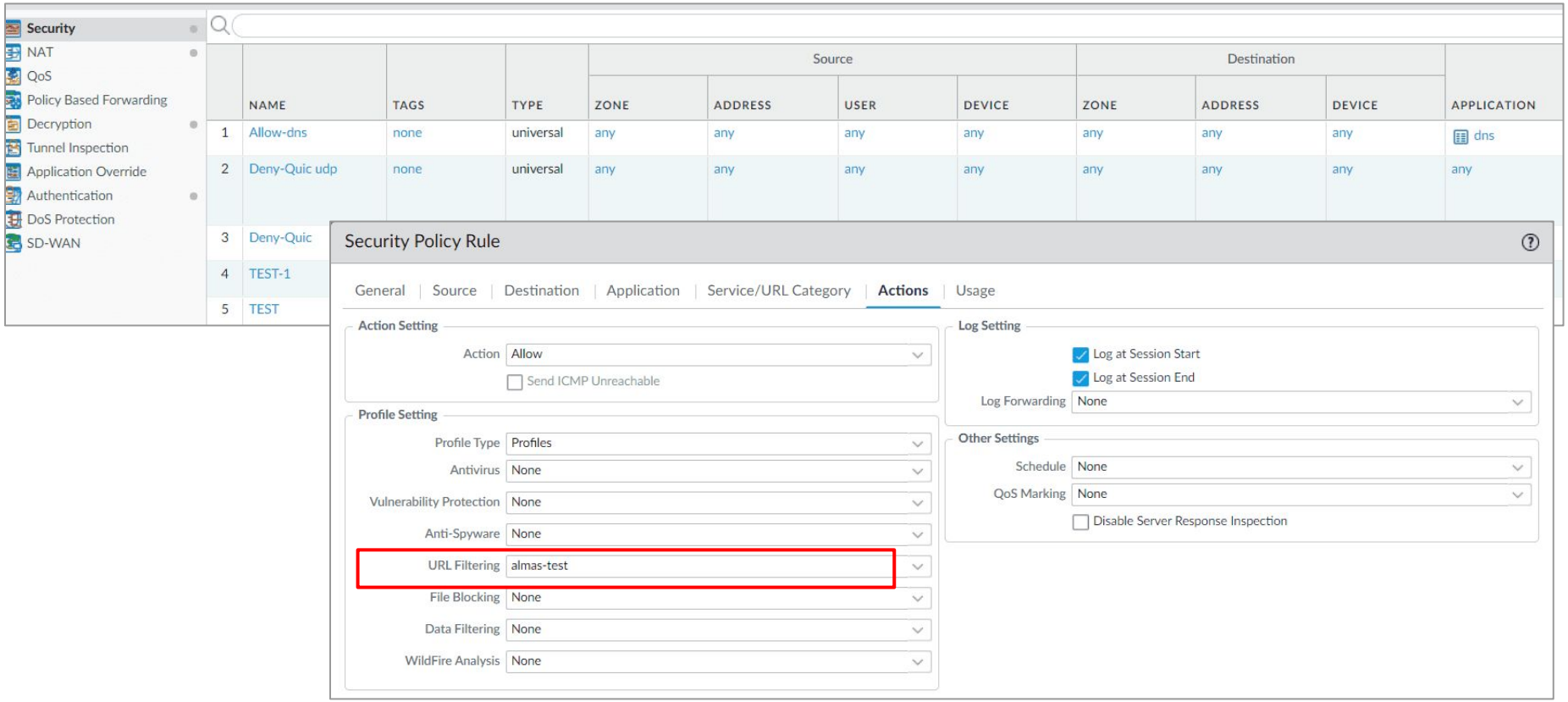


Latest content version for New “real-time-detection” category

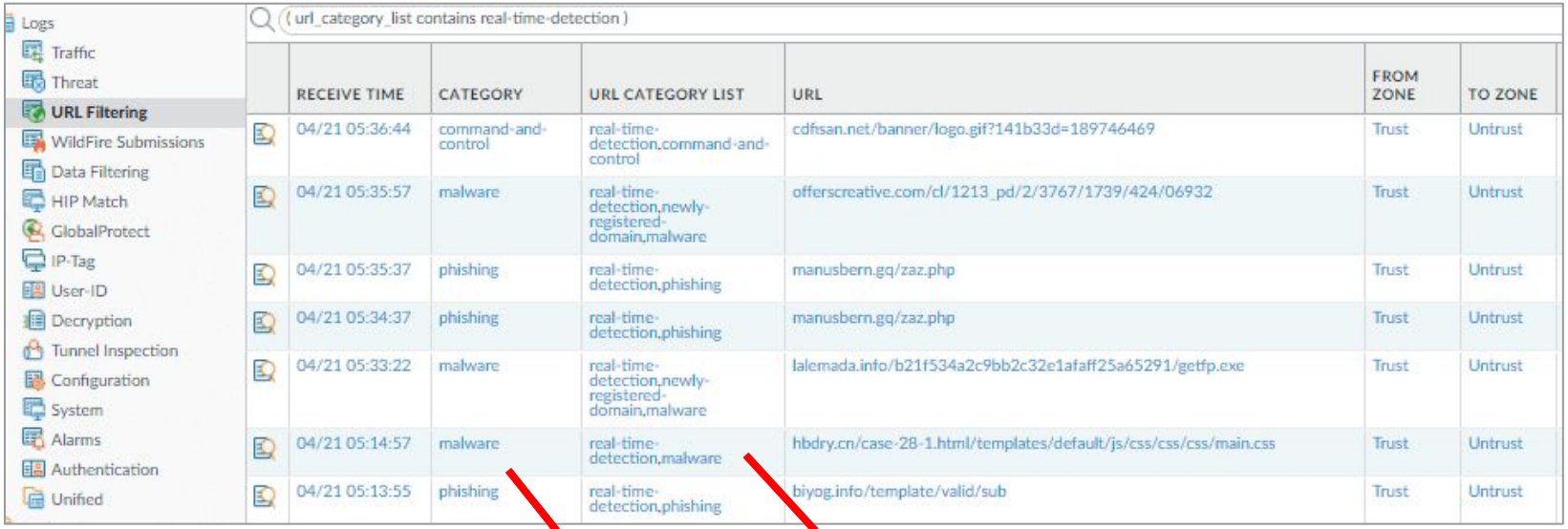


 |

Link URL Profile to the policy



Advanced URL Filtering - “It’s so easy a caveman can do it”



Category malware

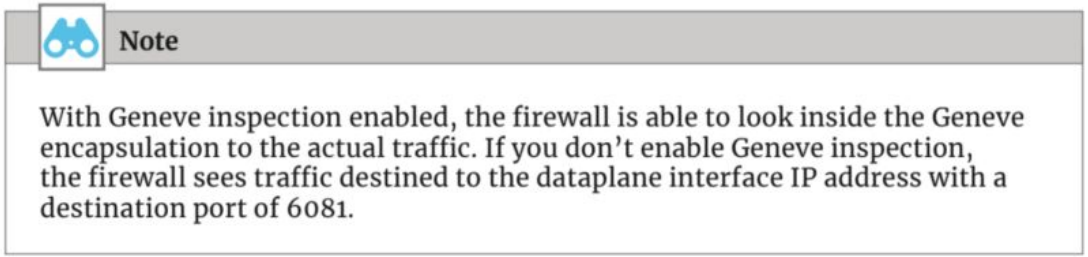
URL Category List real-time-detection,malware

2.4 Define the initial design/deployment configuration of a Palo Alto Network firewall

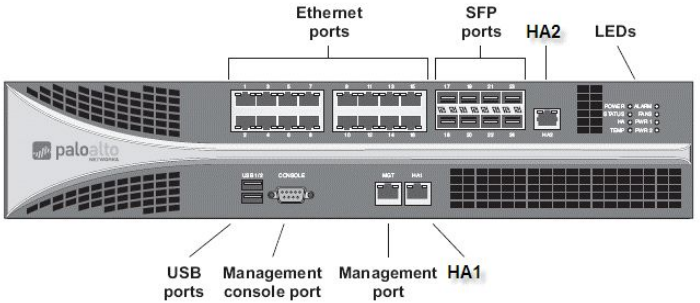
2.4.1 Considerations for Advanced HA Deployments

- HA in public cloud considerations - You can have HA in Azure - the study guide is incorrect...
  - Public cloud can only be Active/Passive HA
  - If you want Active/Active - you use a load balancer and **not** PAN-OS HA

- AWS now has GWLB which uses GENEVE to send flows to the firewall



2.4.2 Implement an HA Pair



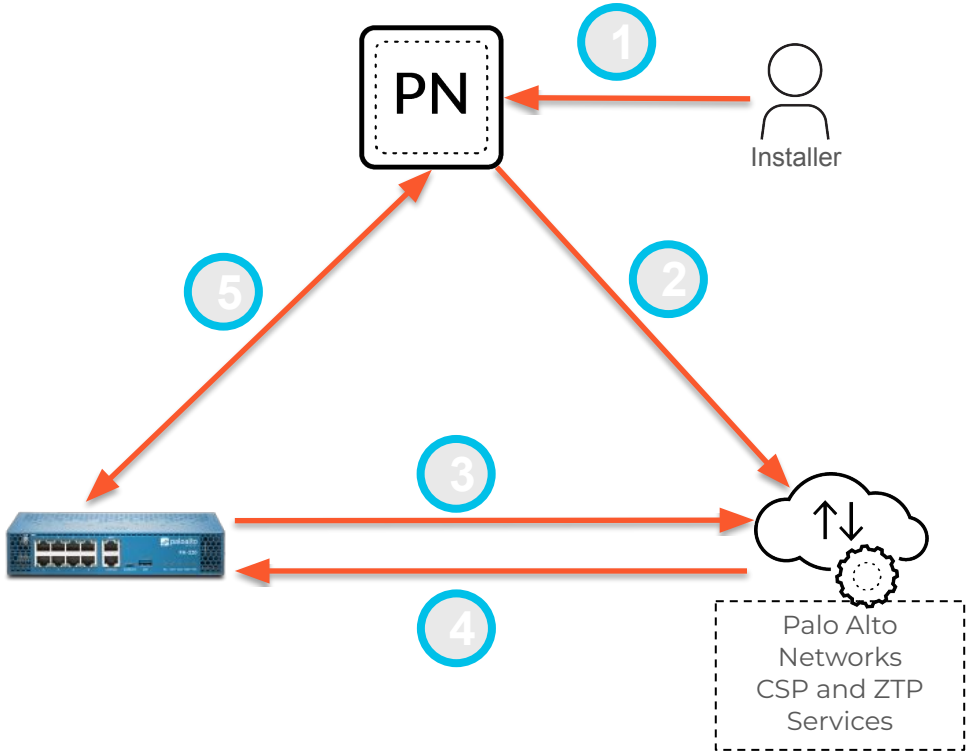
Overview Steps

- Connect the HA ports.
- Enable ping on the management port.
- Set the HA mode and group ID.
- Set up the control link connection.
- Enable encryption for the control link connection.
- Set up the backup control link connection.
- Set up the data link connection (HA2) and the backup HA2 connection.
- Enable heartbeat backup.
- Set the device priority, and enable preemption.
- Modify the HA timers.
- Modify the link status of the HA ports on the passive device.
- Enable HA.

HA 1 - Control
HA2 - Data
HA3 - Packet Forwarding
HA4 - Session Sync

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/ha-links-and-backup-links

2.4.3 Implement Zero Touch Provisioning



1. Installer or IT admin registers device via a ZTP page on Panorama (PN)
2. PN registers the device with the Customer Support Portal (CSP) and Zero Touch Provisioning Service (ZTP)
3. Firewall with factory config connects with ZTP service
4. ZTP service provides the IP/FQDN for customer's Panorama
5. Firewall connects to Panorama and receives its config

2.4.3 Implement Zero Touch Provisioning

To set up your firewall for Zero Touch Provisioning (ZTP), perform the following using Panorama:

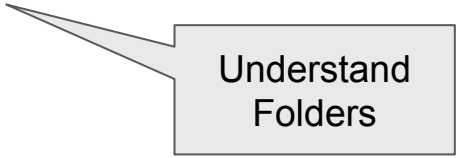
- Select Panorama > Plugins to Download. Install the most recent version of the ZTP plugin.
- Install the Panorama device certificate.
- Register Panorama with the ZTP service.
- Create a default device group and template to connect your ZTP firewalls to Panorama.
- Select Panorama > Zero Touch Provisioning. Sync Panorama with the ZTP service.
- Set up the ZTP installer administrative account.
- Add ZTP firewalls to Panorama.

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/ha-links-and-backup-links

2.4.4 Configure Bootstrapping

The bootstrap process is initiated only when the firewall starts up in a factory default state.

/config folder - init-cfg.txt and bootstrap.xml
    Init-cfg.txt - basic info like IP address, netmask, DG
    bootstrap.xml - contains a complete configuration for the firewall
/license folder - license keys or authorization codes
/software folder - software images
/content folder - Applications and Threats updates and WildFire updates



https://docs.paloaltonetworks.com/vm-series/10-2/vm-series-deployment/bootstrap-the-vm-series-firewall

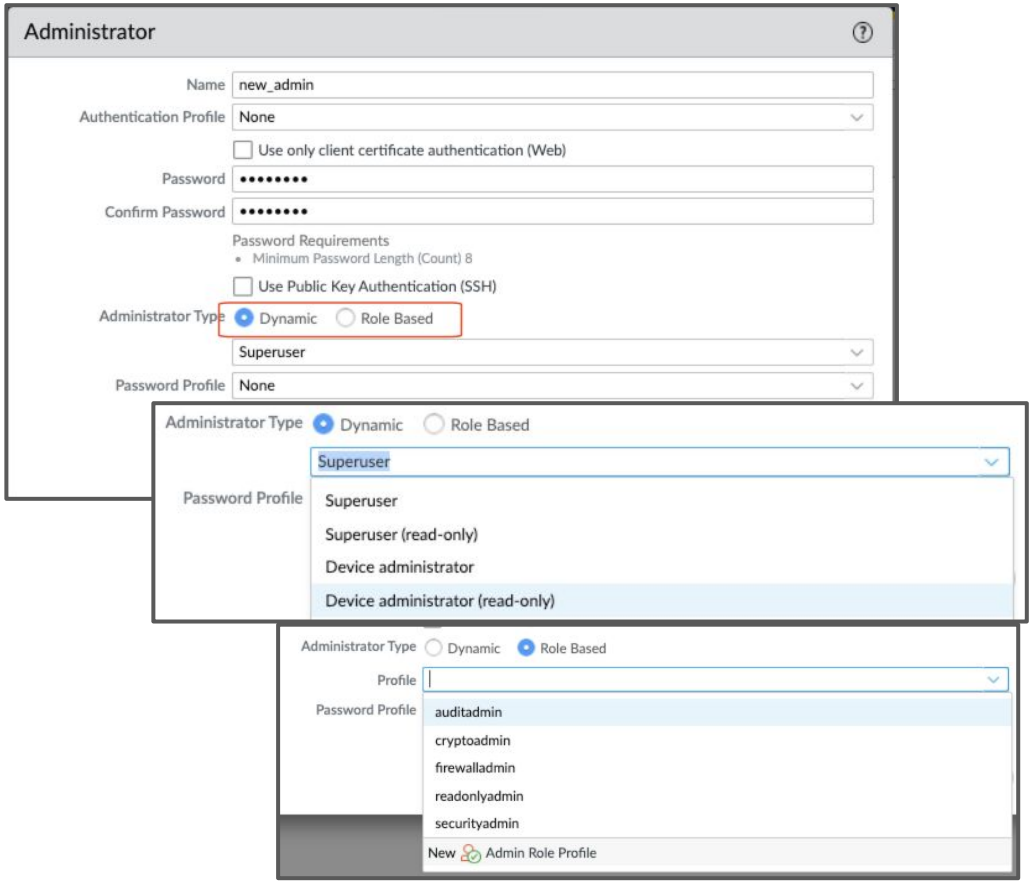
2.5 Configure authorization, authentication, and device access

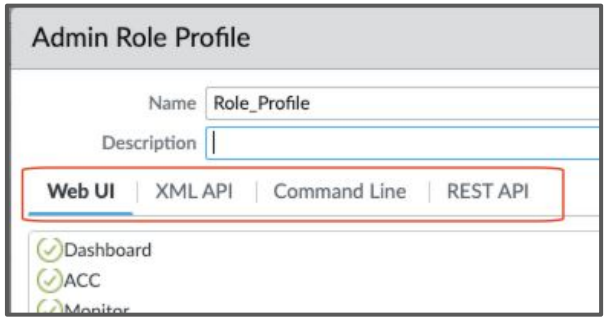
2.5.1 Role-based access control for authorization

Dynamic

- Superuser
- Superuser (Read-only)
- Device Administrator
- Device administrator (read-only)

Role Based - Based on a *Admin Role Profile*, can configure access to CLI, XML and REST API along with WebUI





2.5.2 Different methods used to authenticate

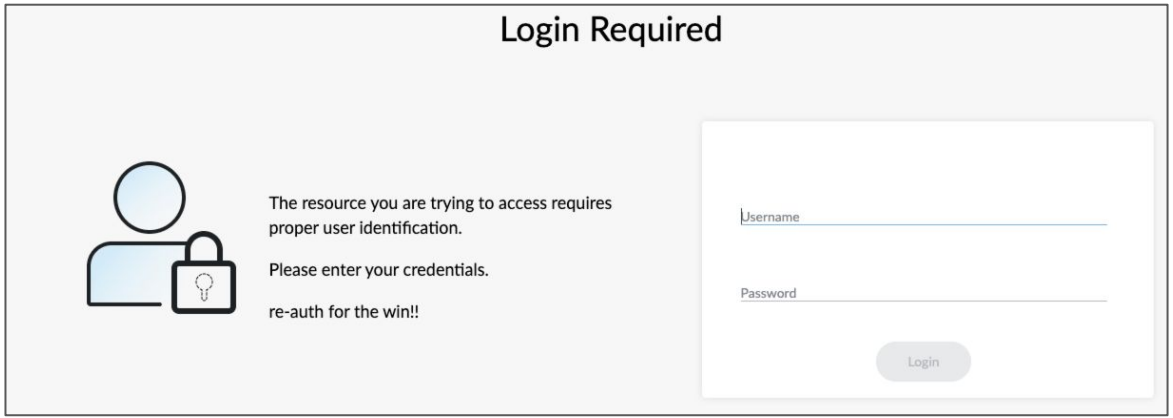
Supported authentication types include the following:

- MFA
- SAML
- SSO
- Kerberos
- TACACS+
- RADIUS
- LDAP
- Local

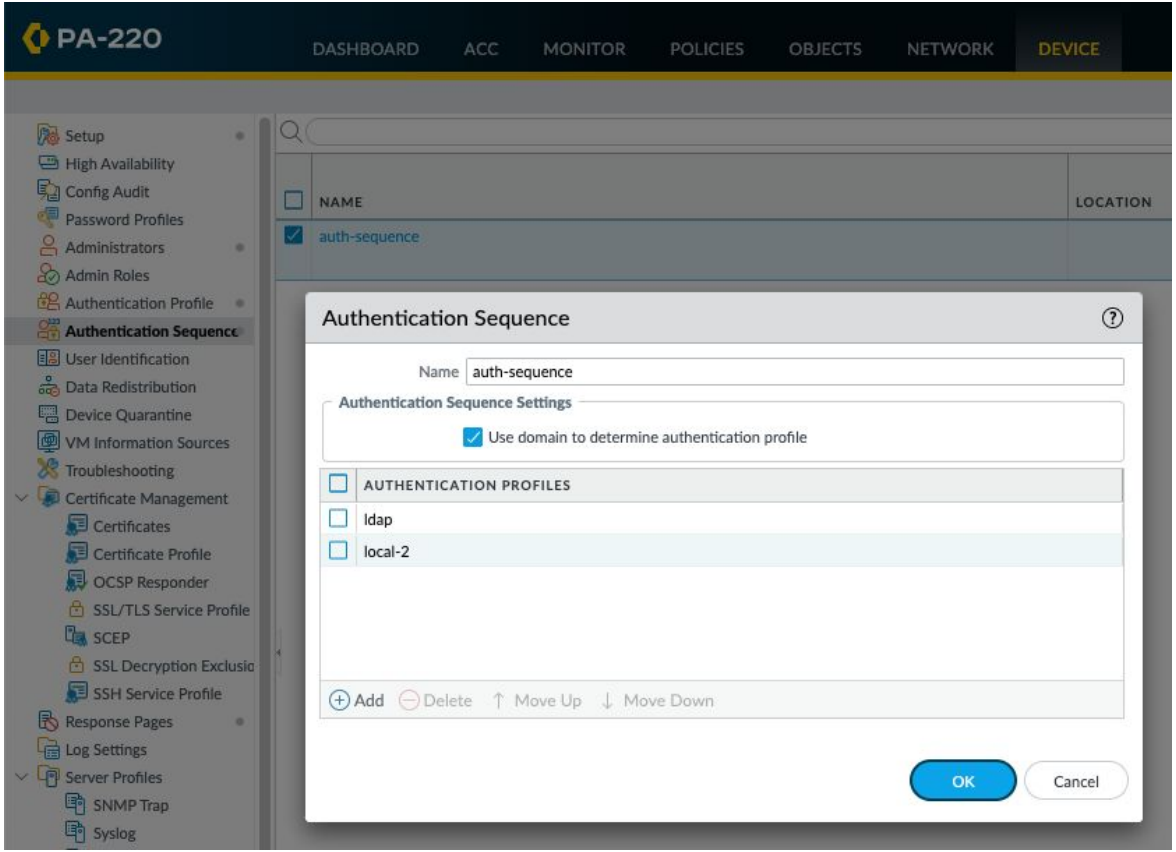
1. Create Auth Profile
2. Create Authentication method
3. Create an Auth Policy to match traffic

Protecting Service Access Through the Firewall

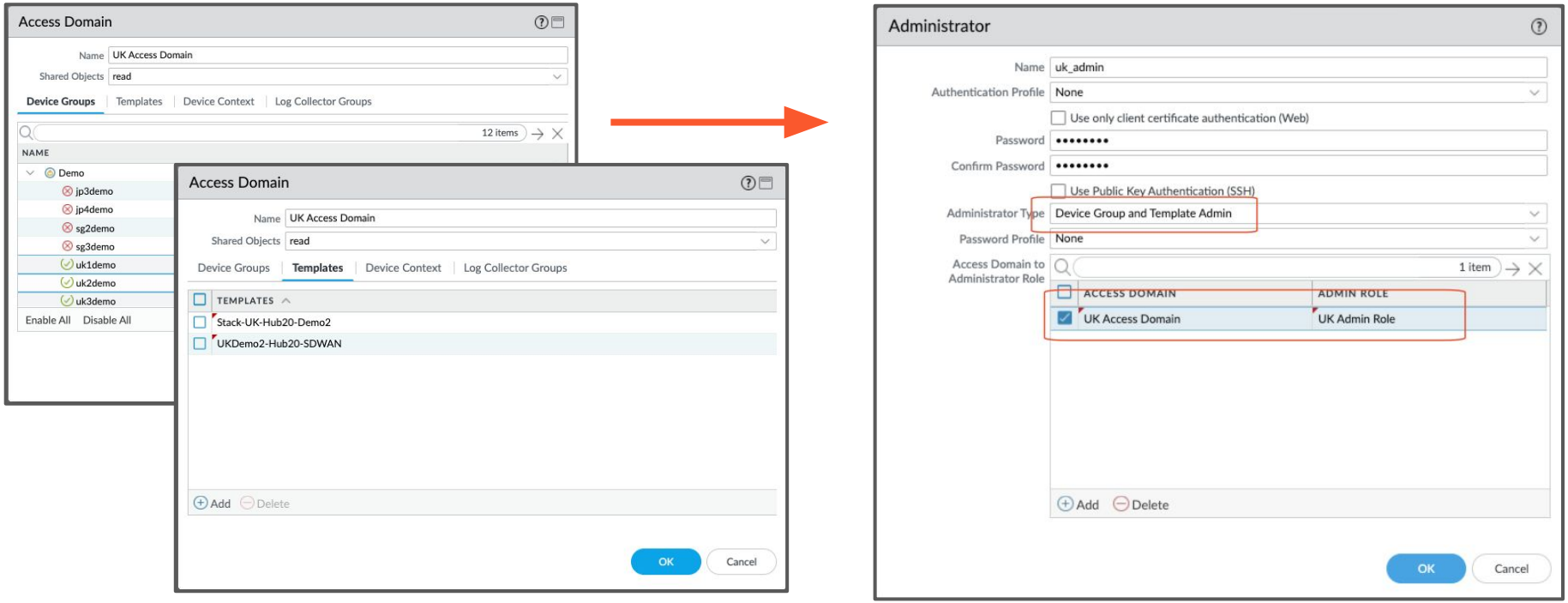
- ***UserID***
- ***Authentication Policy - Captive Portal***



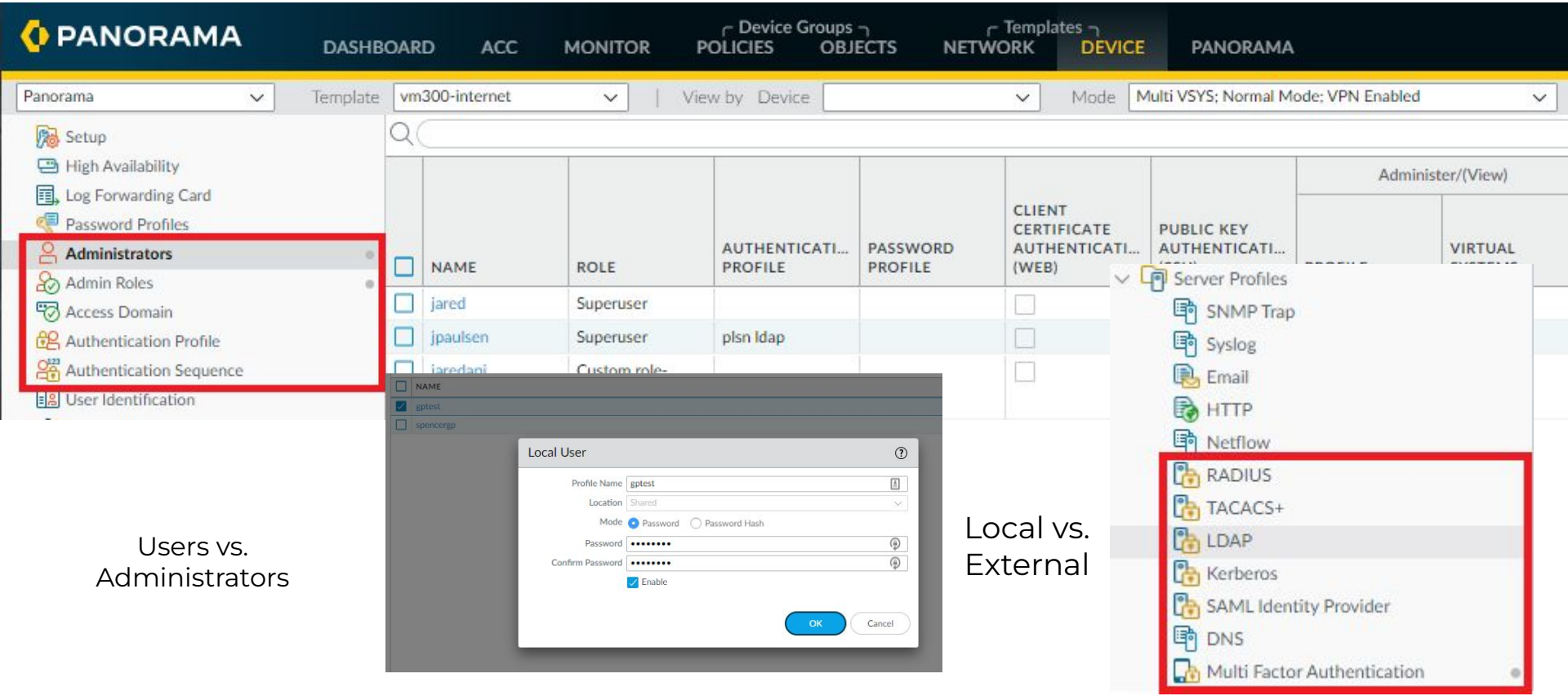
2.5.3 The Authentication Sequence



2.5.4 The device access method - *for Panorama Access Domains*



2.5.4 Understand the Different Methods to Authenticate

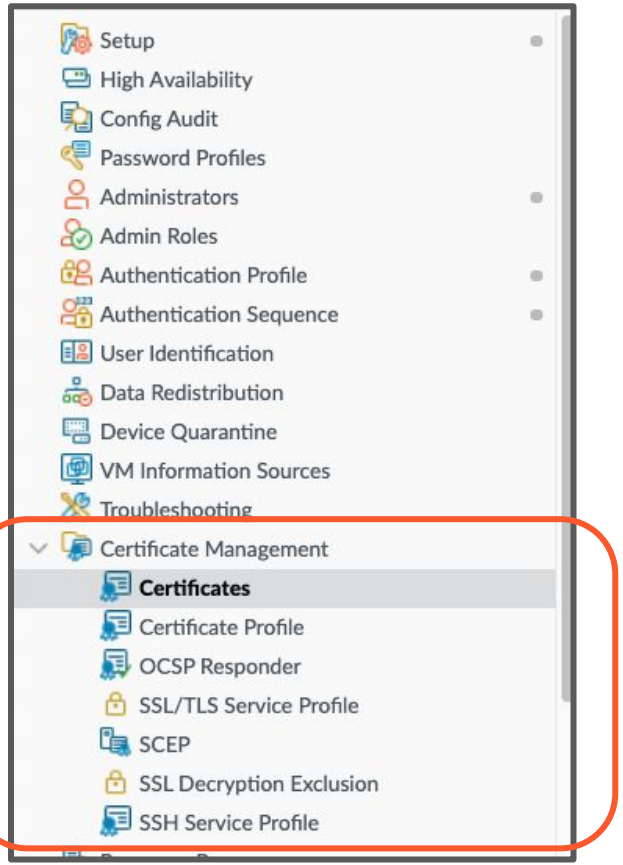


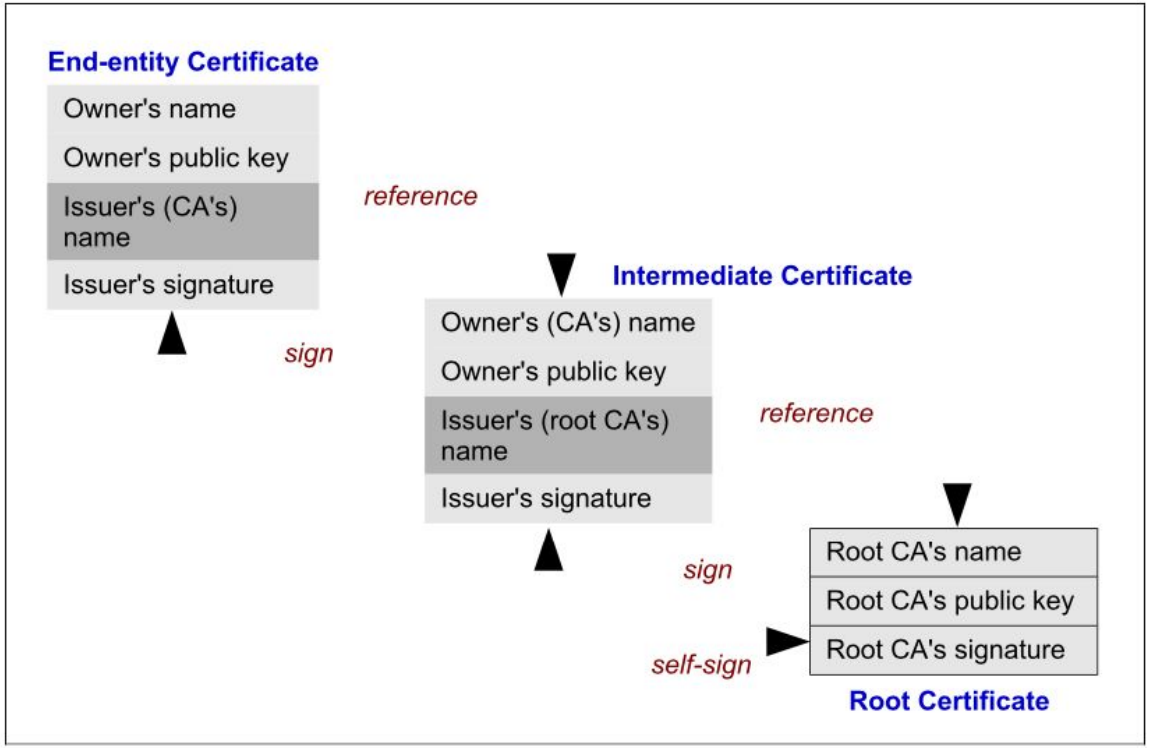
Users vs. Administrators

Local vs. External

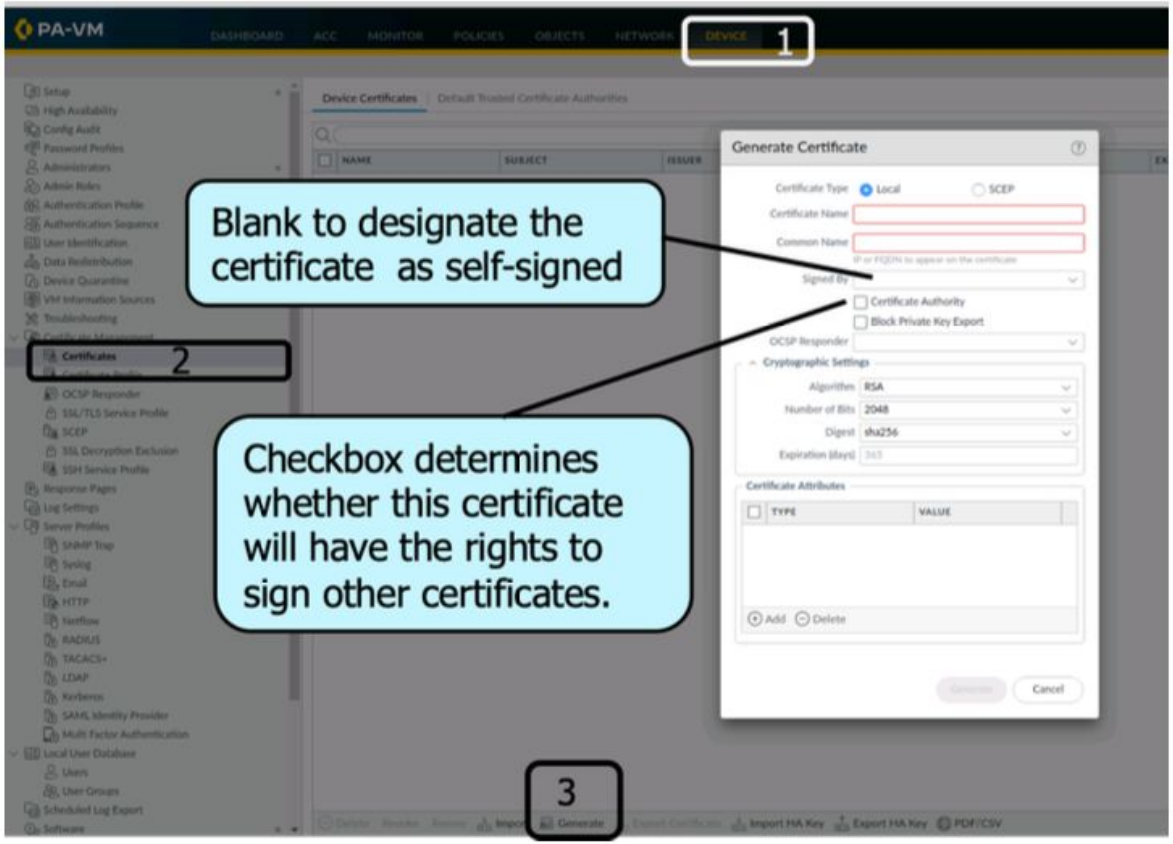
2.6 Configure and manage certificates

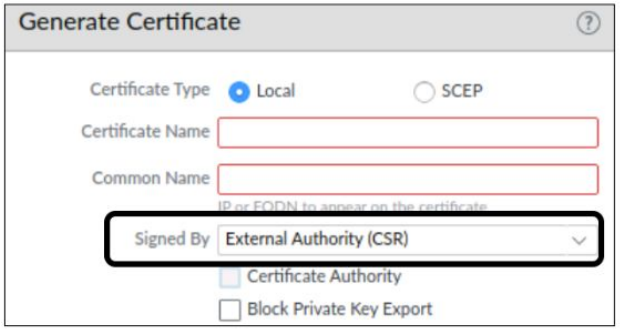
2.6.1 Certificate Usage





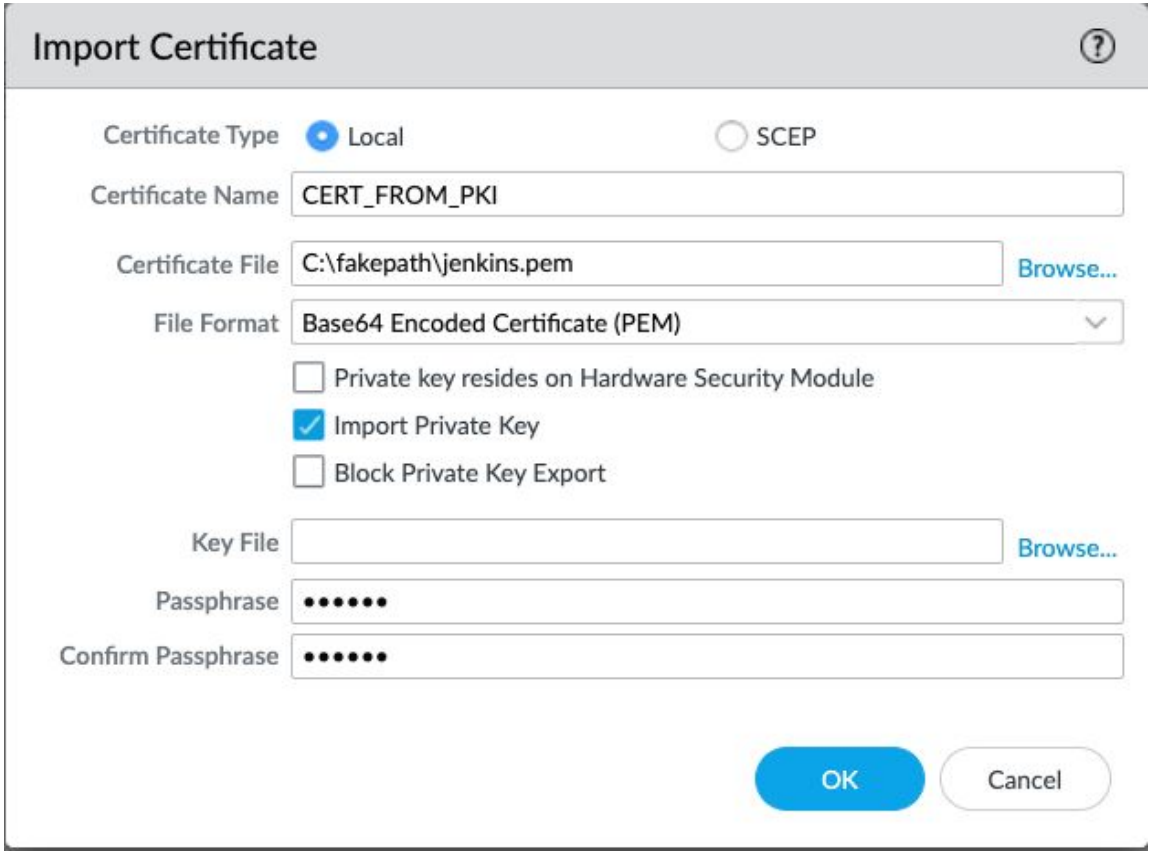
2.6.2 Certificate Profiles



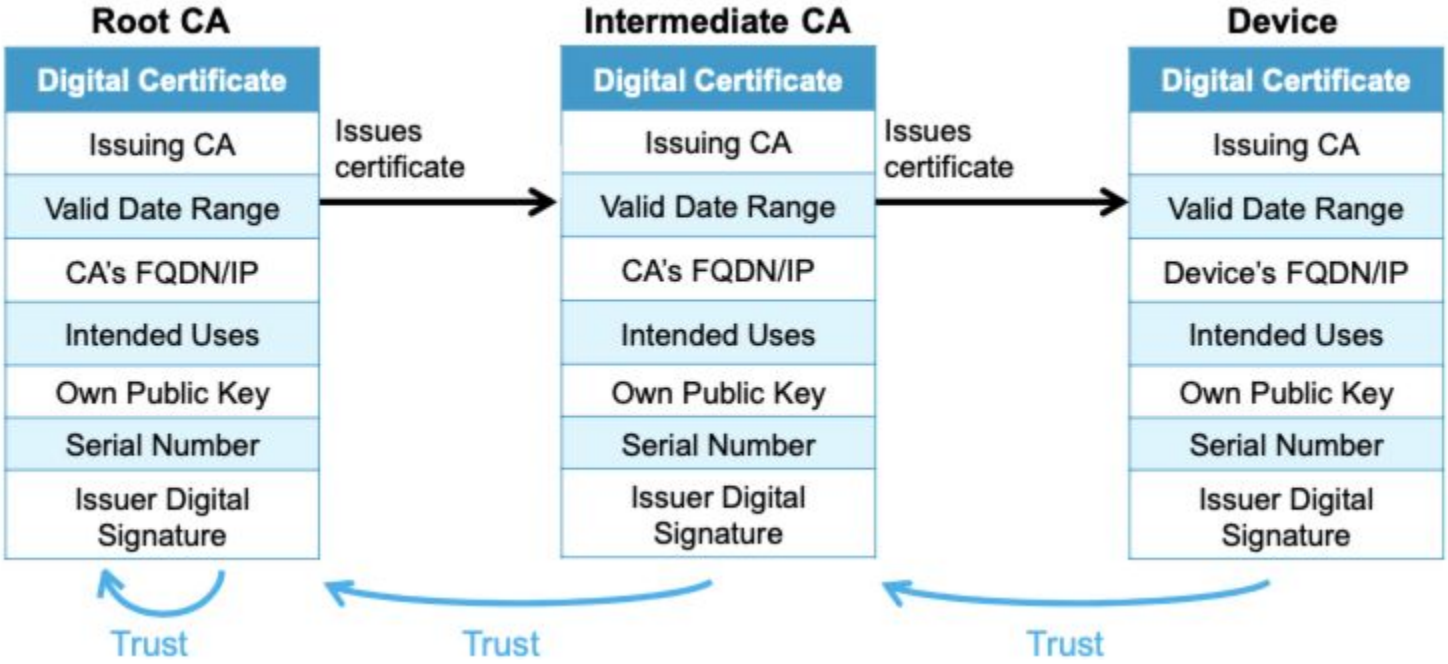


 |

2.6.1 Certificate Usage



2.6.3 Certificate Chains



2.6.3 Firewall CA Certificate Deployment Choices

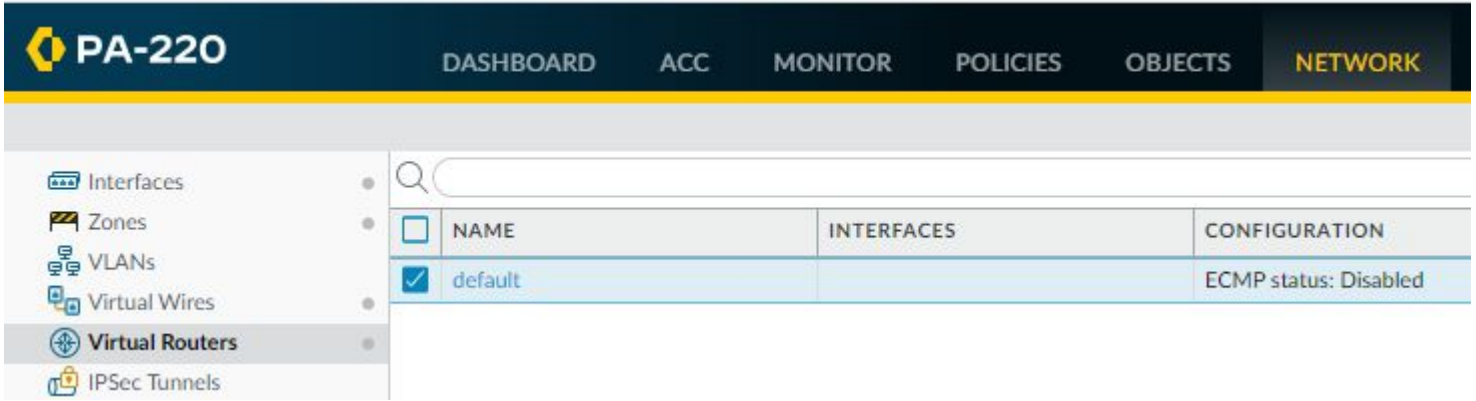
- Signing certificates are authorized to sign other certificates.
- A signing certificate must be a CA certificate.
- Three choices for obtaining a firewall CA certificate:
  - Import a firewall CA certificate
  - Generate a firewall CA certificate using a CSR
  - Generate a firewall self-signed CA certificate

In order to decrypt outbound SSL traffic, what kind of certificate needs to be defined on the firewall?

2.7 Configuring Routing

2.7.1 - Configure Dynamic Routing

- > Network > Virtual Routers > Select Virtual Router



 |

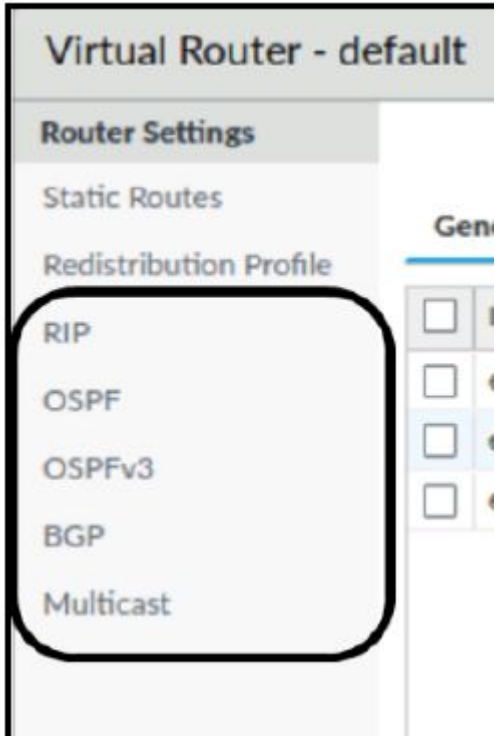
Configure Dynamic Routing

Router Types(PAN-OS 10.1)

- Legacy Virtual Router
  - Enabled by default
  - Supports Static Routes, RIP, OSPF, BGP, Multicast
  - Will be used in most cases
  - Can Create Multiple Virtual Routers (VR)
    - Each VR has its own Routing Table

- Combine with vSYS to Get Admistratable L3 NGFW

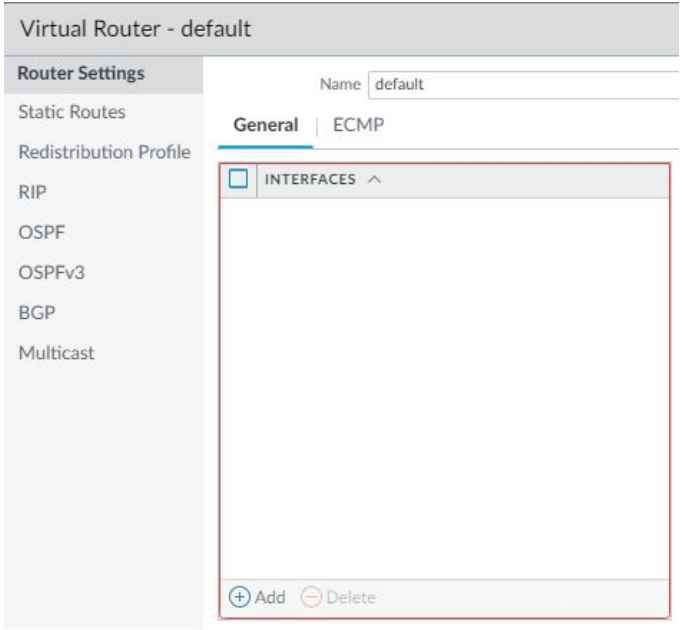
- VR Can be a Next Hop in a Route
  - This Allows You to Route Between Route Tables and Solve Problems Creatively
    - Duplicate IP Address Space Problems
    - Facilitate Weird NAT Tricks



 |

Configure Dynamic Routing

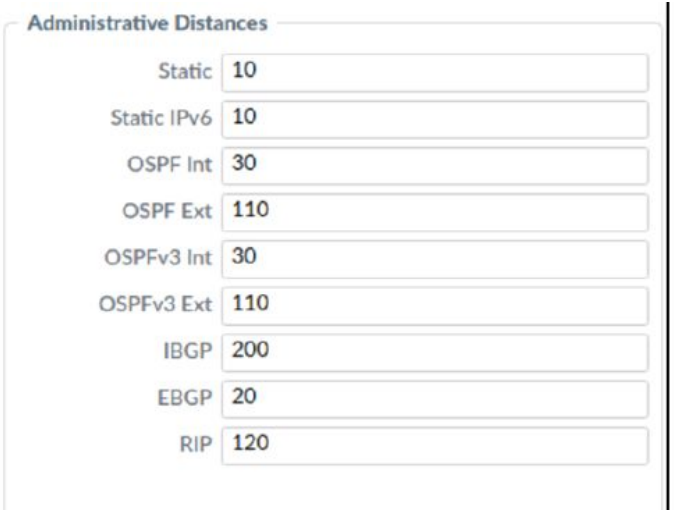
- Each Virtual Router Must Have the Following
  - Name
  - Assigned Interface(s)
  - Routing Protocol Configured “Optional”
- Note - All Layer 3 Interfaces Must Be Assigned to a Virtual Router
- Administrative Distance
- Notable Terminology
  - RIB (Routing Information Based) - Management Plane
  - FIB (Forwarding Information Based) - Data Plane
- Equal Cost Multipathing(ECMP)
  - Add multiple routes to RIB/FIB & Load Balance



 |

Configure Dynamic Routing

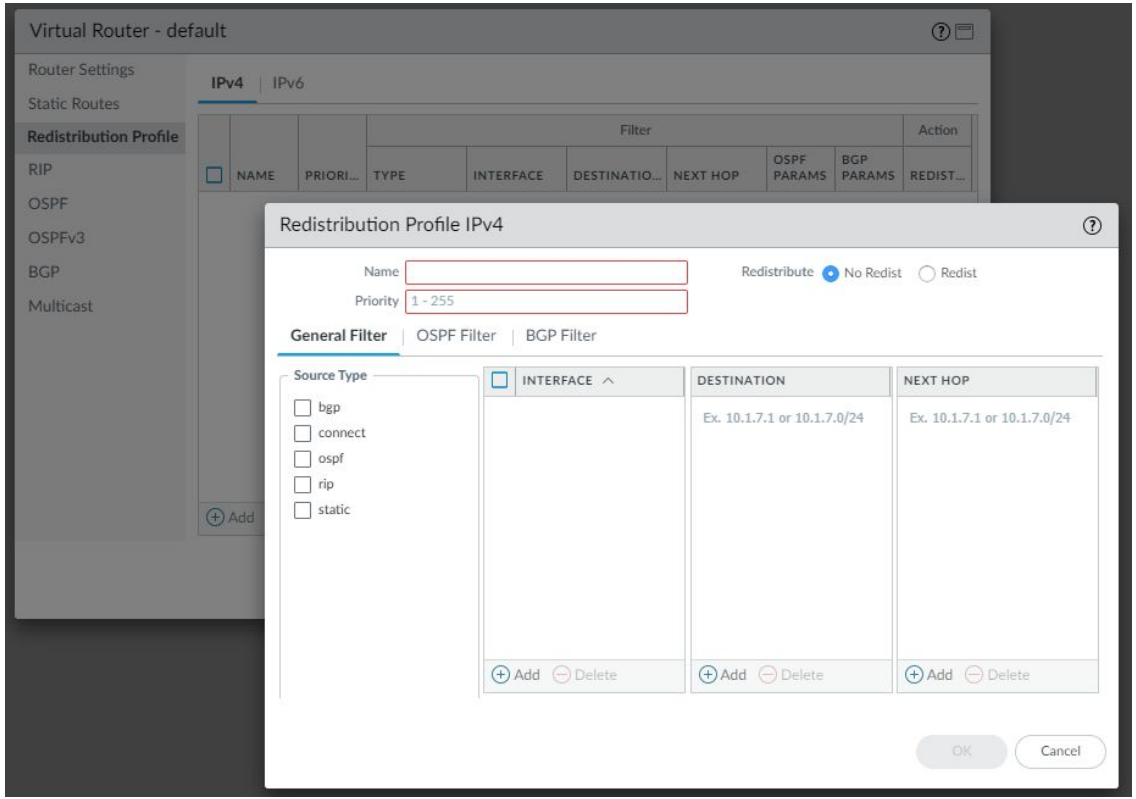
- Each Virtual Router Must Have the Following
  - Name
  - Assigned Interface(s)
  - Routing Protocol Configured “Optional”
- Note - All Layer 3 Interfaces Must Be Assigned to a Virtual Router
- Administrative Distance
- Notable Terminology
  - RIB(Routing Information Based)
  - FIB (Forwarding Information Based)
- Equal Cost Multipathing(ECMP)
  - Add multiple routes to RIB/FIB & Load Balance



 |

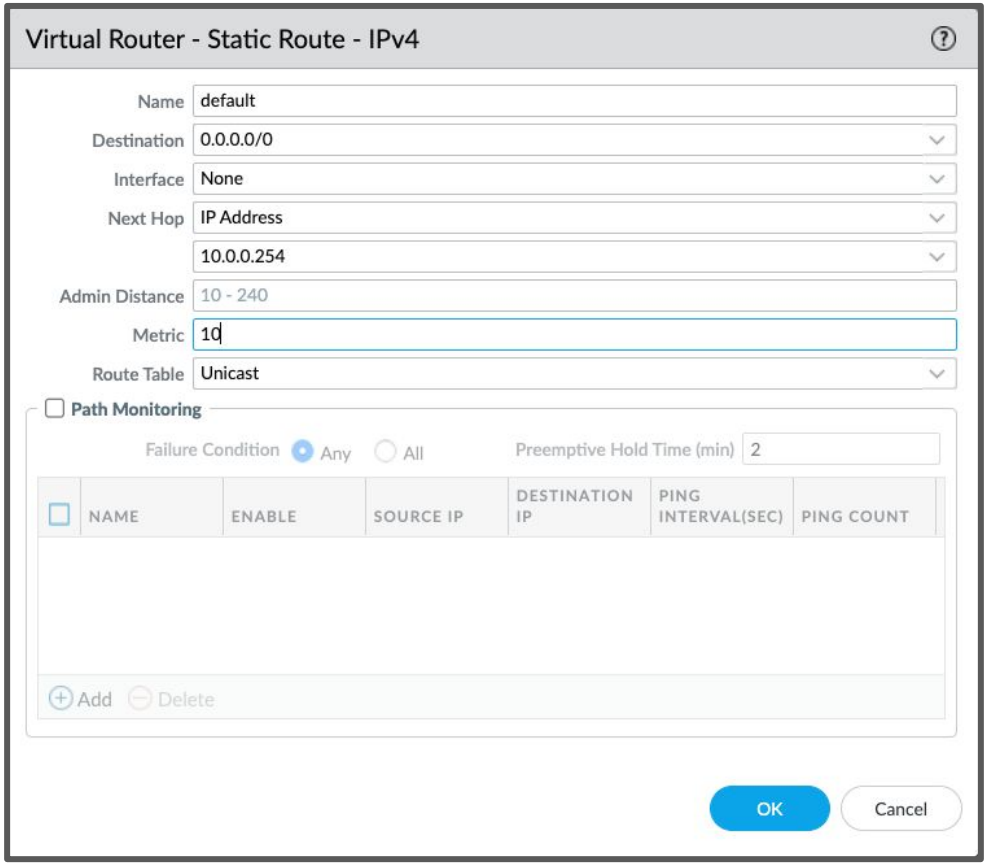
2.7.2 - Redistribution Profiles

- By Default Routes are not Shared Between Routing Protocols
  - Example: If a route is known via OSPF, BGP will not send information to it's peers
- How to Configure
  - Name - example: "OSPF to BGP"
  - Select a Source Protocol Type
  - Filtering Options (how to decide what routes to send)
    - Interface
    - Destination
    - Next Hop

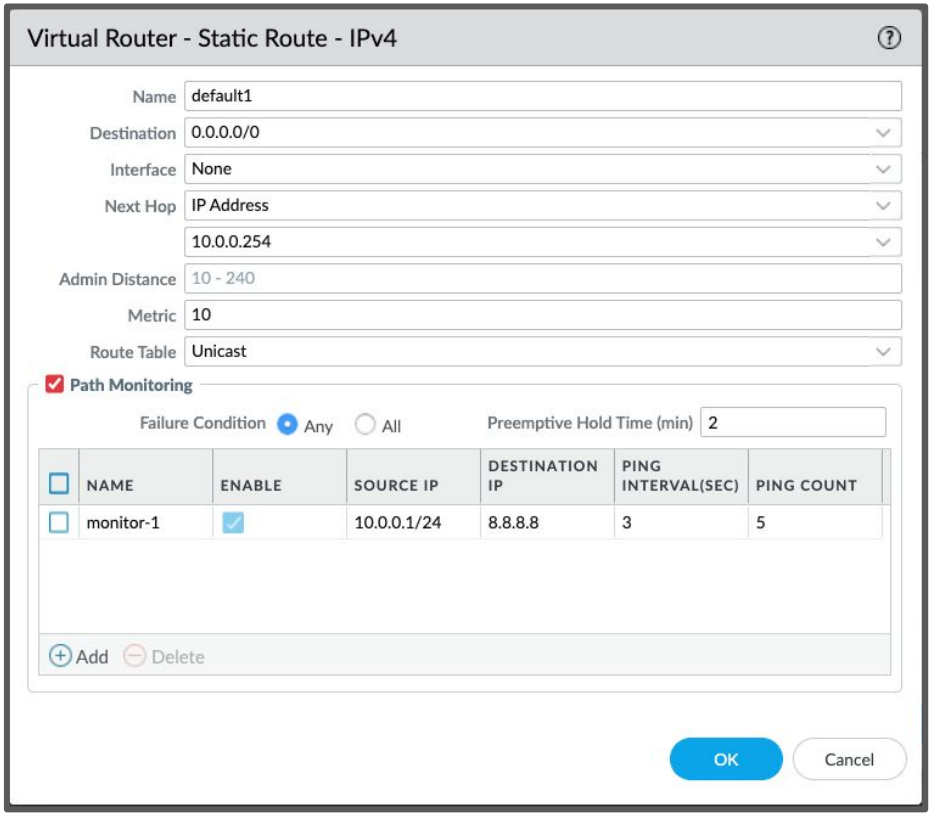


 |

2.7.3 Configure Static Routes

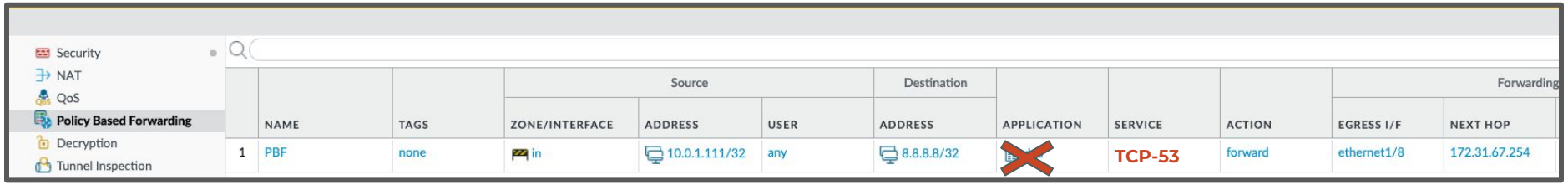


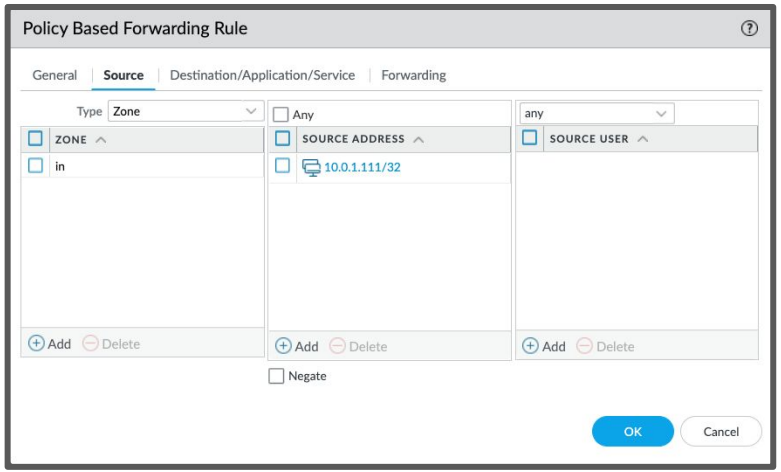
2.7.4 Route Monitoring

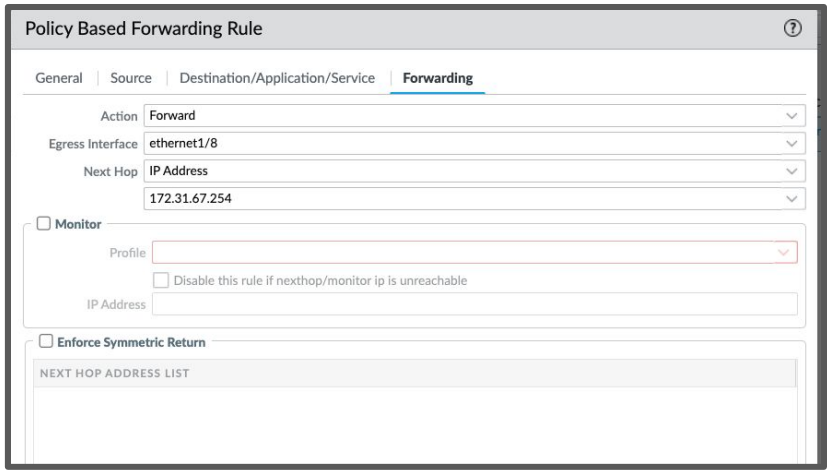


 |

2.7.5 Configure Policy-Based Forwarding and How it Affects Routing and Firewall Security







2.7.6 - Virtual Router vs Logical Routers

Legacy Route Engine

- Multi Virtual router Support
- Dynamic Routing Protocols
  - BGP, OSPF, OSPFv3 & RIPv2
  - Not a Dynamic Routing Protocol but Static Routes are Supported

Advanced Route Engine

- Single Virtual Router Support
- Dynamic Routing Protocols
  - BGP
  - Not a Dynamic Routing Protocol but Static Routes are Supported
- Preview Mode on v10.1
- Use Case
  - Large Data Centers, Enterprises, ISPs & Cloud Services

Note: PAN-OS v10.2 of Advanced Routing Engine Supports BGP, OSFP, OSPFv3 & **RIPv2 (Not a Correct Answer for This Test)** - Full Release

- Only One Type Can Be Enable/Reboot Required

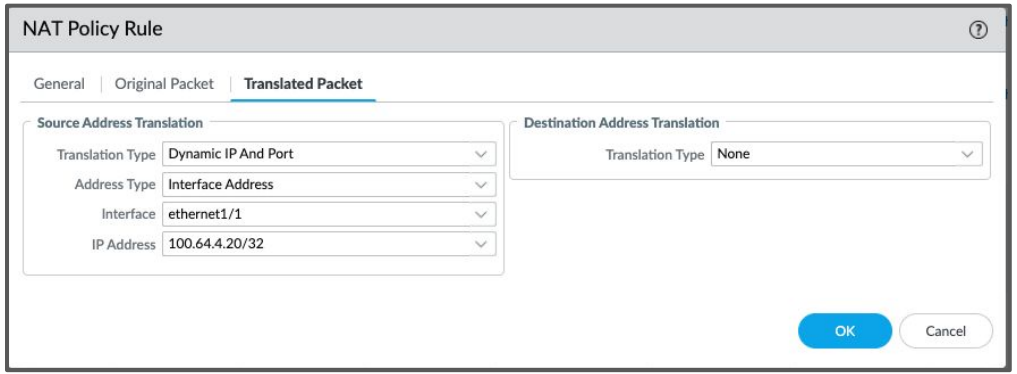
2.8 Configuring NAT

2.8.3 Source NAT

8	SNAT	none	L3-Trust	L3-Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1 100.64.4.20/32

Source NAT Translation is the simplest configuration - its also referred to as DIPP in the study guide (Dynamic IP & Port)

Be familiar with oversubscription mentioned in study guide.

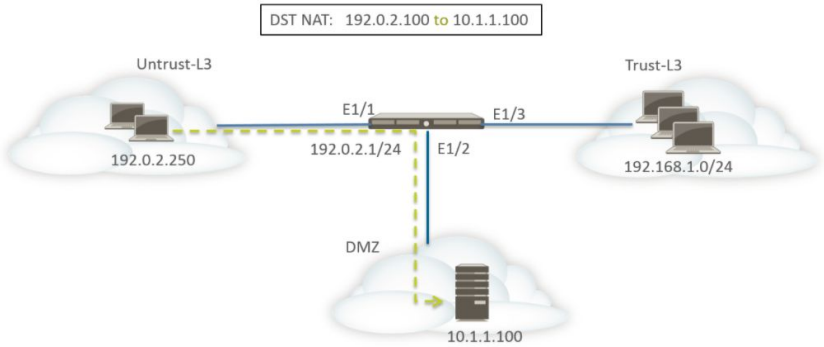


Slack Channel: Understanding_NAT-4.1-RevC.pdf

2.8.1 NAT Policy Rules & 2.8.2 Security Rules

NAT Policy

NAME	TAGS	Original Packet						Translated Packet	
		SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Webserver-public	any	none	destination-translation address: webserver-private



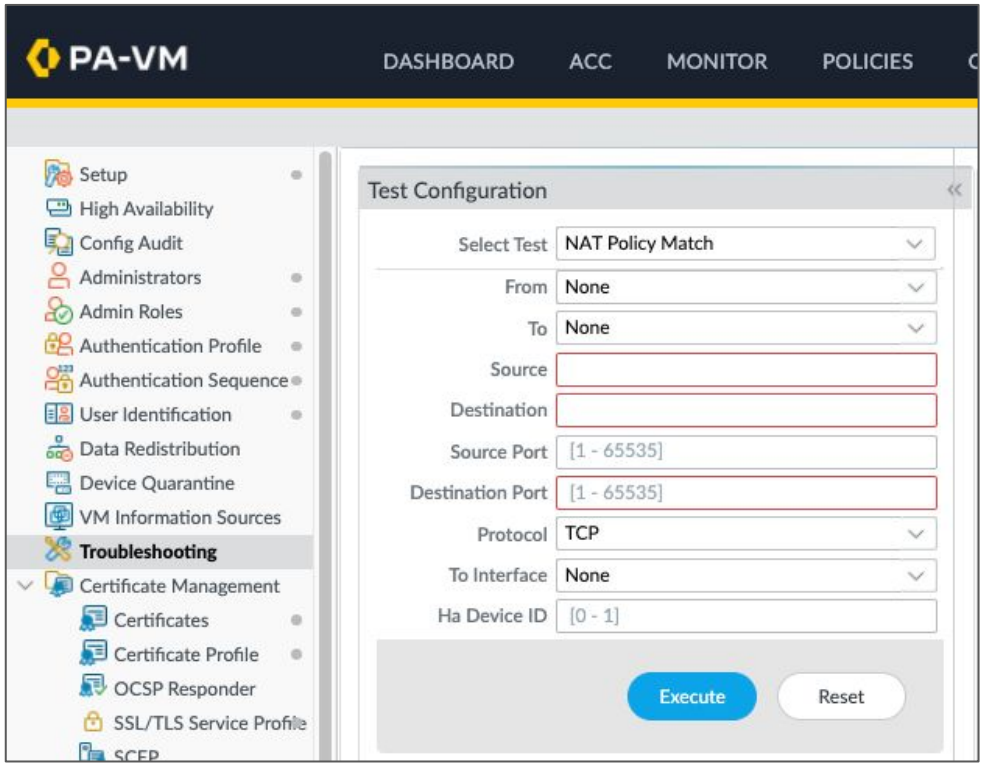
Slack Channel:
Understanding_NAT-4.1-RevC.pdf

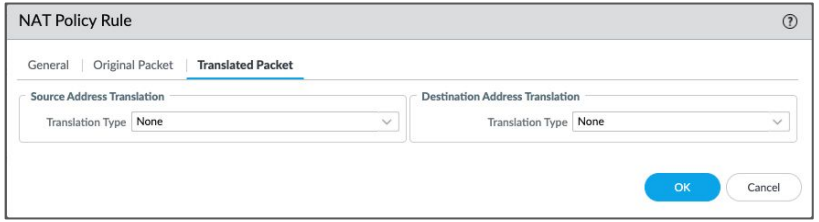
Security Policy

NAME	Source		Destination		APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
	ZONE	ADDRESS	ZONE	ADDRESS					
Webserver access	Untrust-L3	any	DMZ	Webserver-pu...	web-browsing	any	Allow	none	

 |

2.8.4 No-NAT Policies





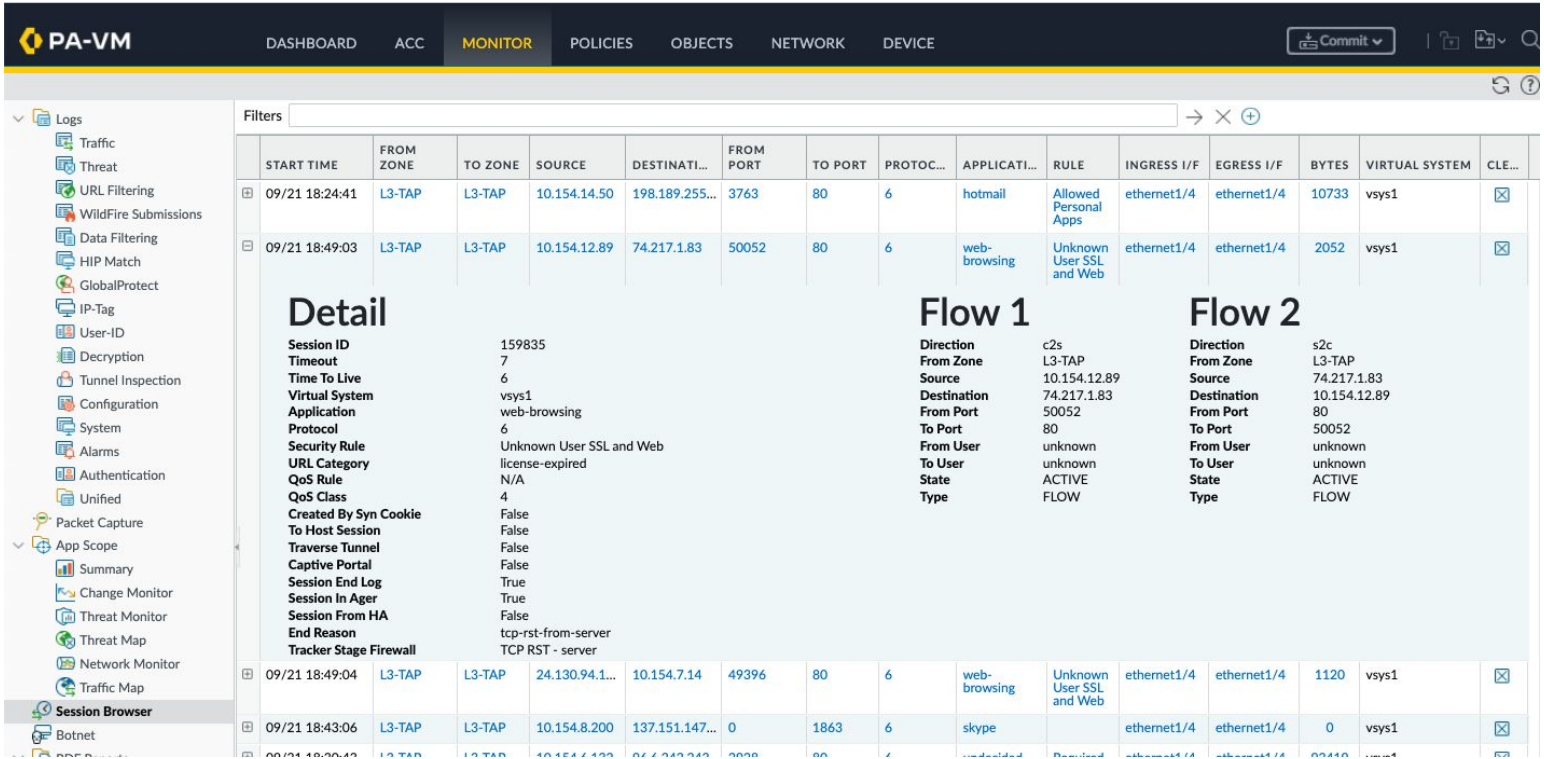
Some NAT Scenarios Require Traffic to be Exempted from NAT. Use No-NAT Policies to Exempt Traffic From NAT.

You Can Debug this with the **Device → Troubleshooting** Widget

Use the FUEL Virtual Lab to Practice Using this Tool

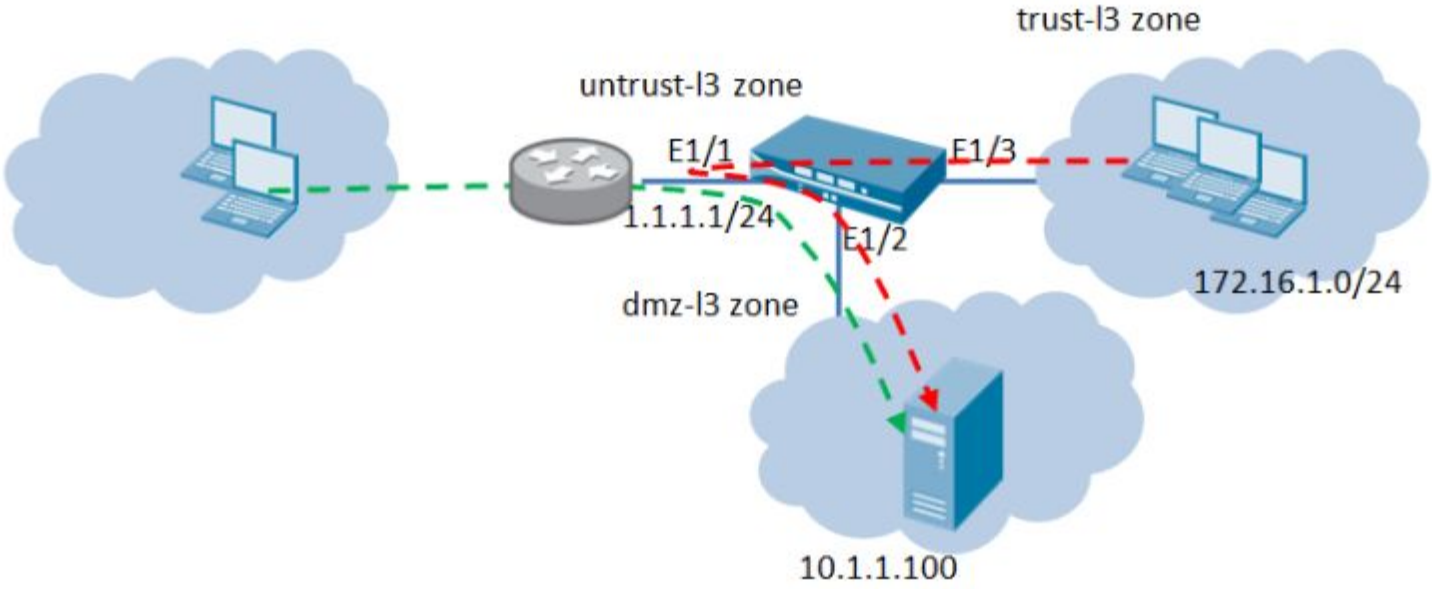
2.8.5 Use Session Browser to Find NAT Rule Name

Use the FUEL Virtual Lab - Surf to the Internet and Use the Session Browser to Analyze Your Traffic



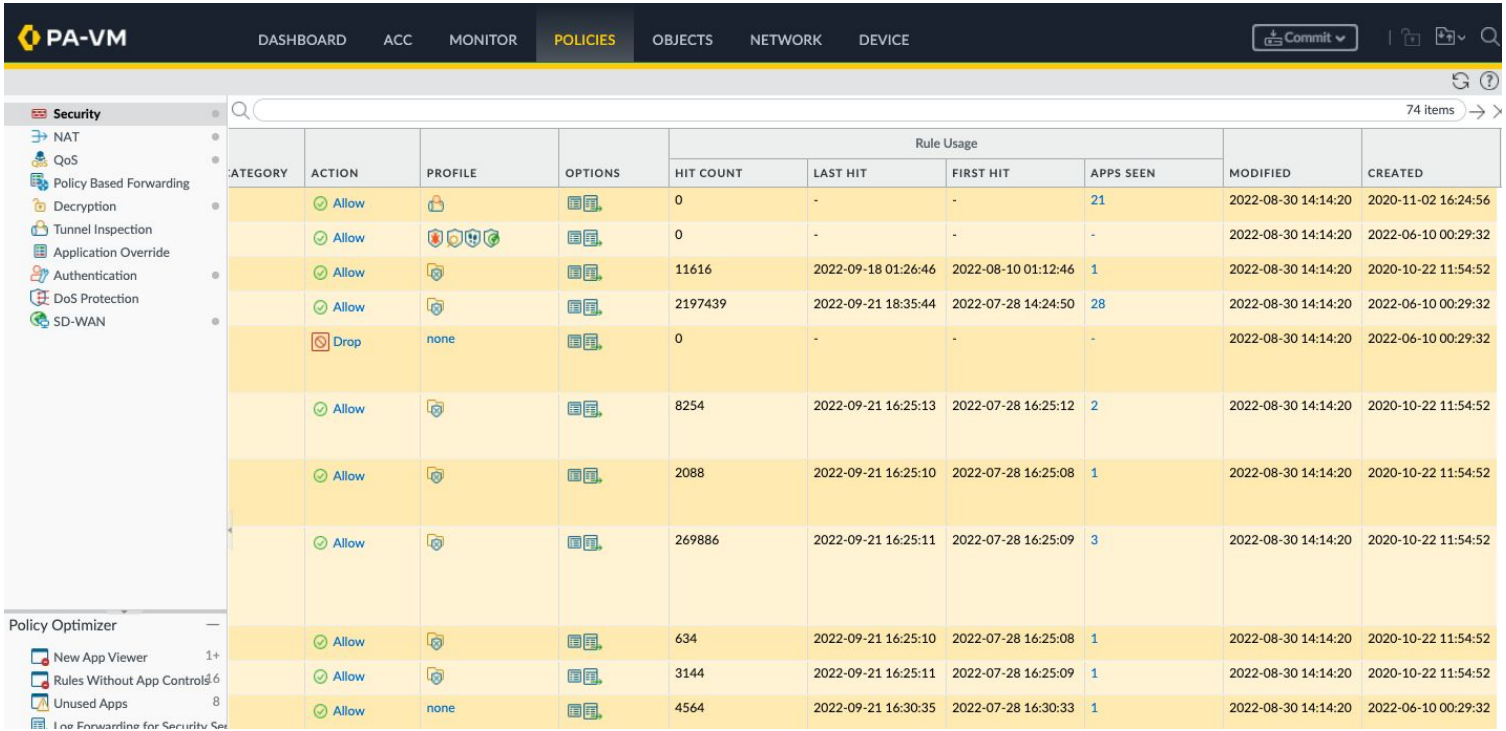
2.8.6 U-Turn NAT

Slack Channel: Understanding_NAT-4.1-RevC.pdf



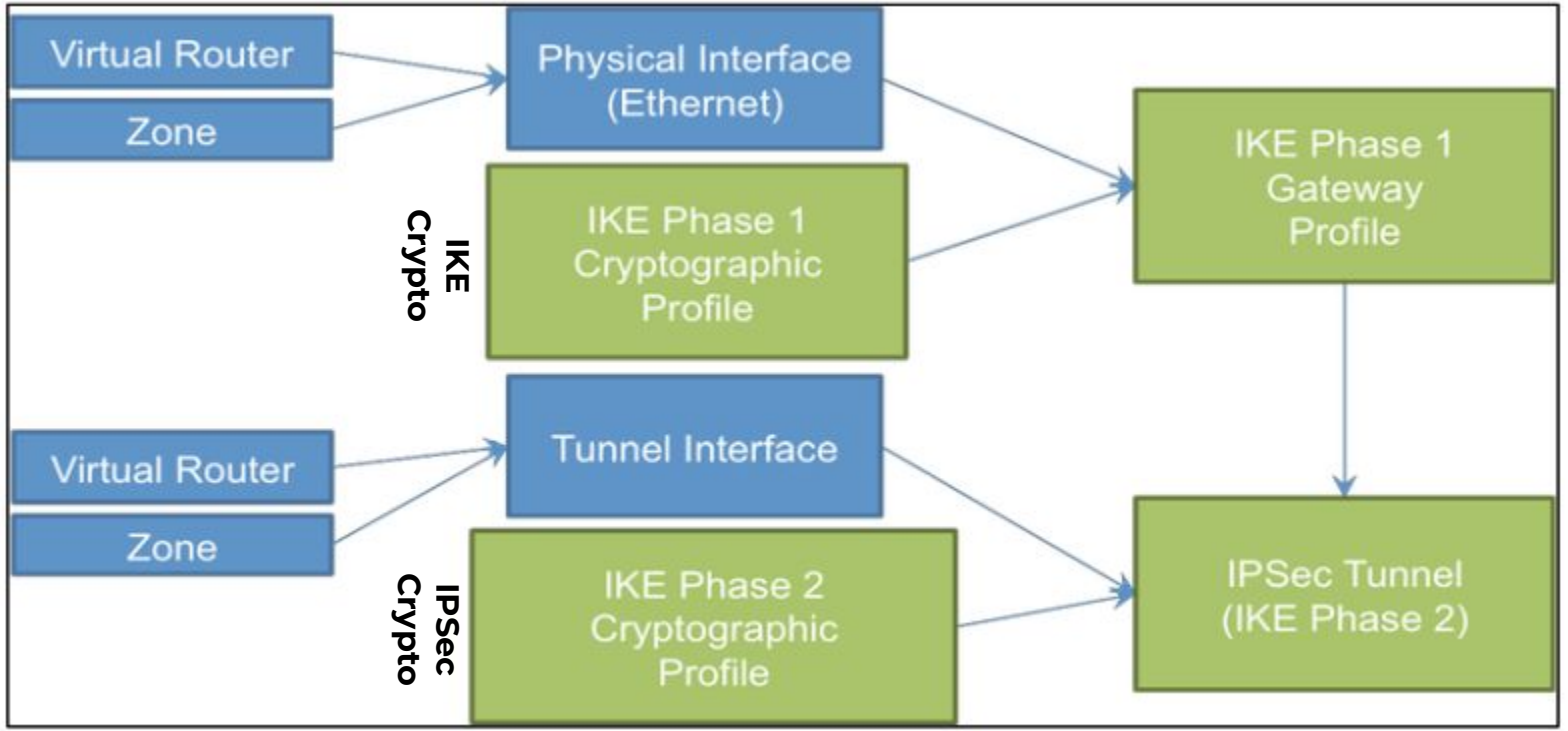
2.8.7 Check HIT Counts

Use Fuel Virtual Lab & PCNSE Study Guide Section - Make this Section a Lab

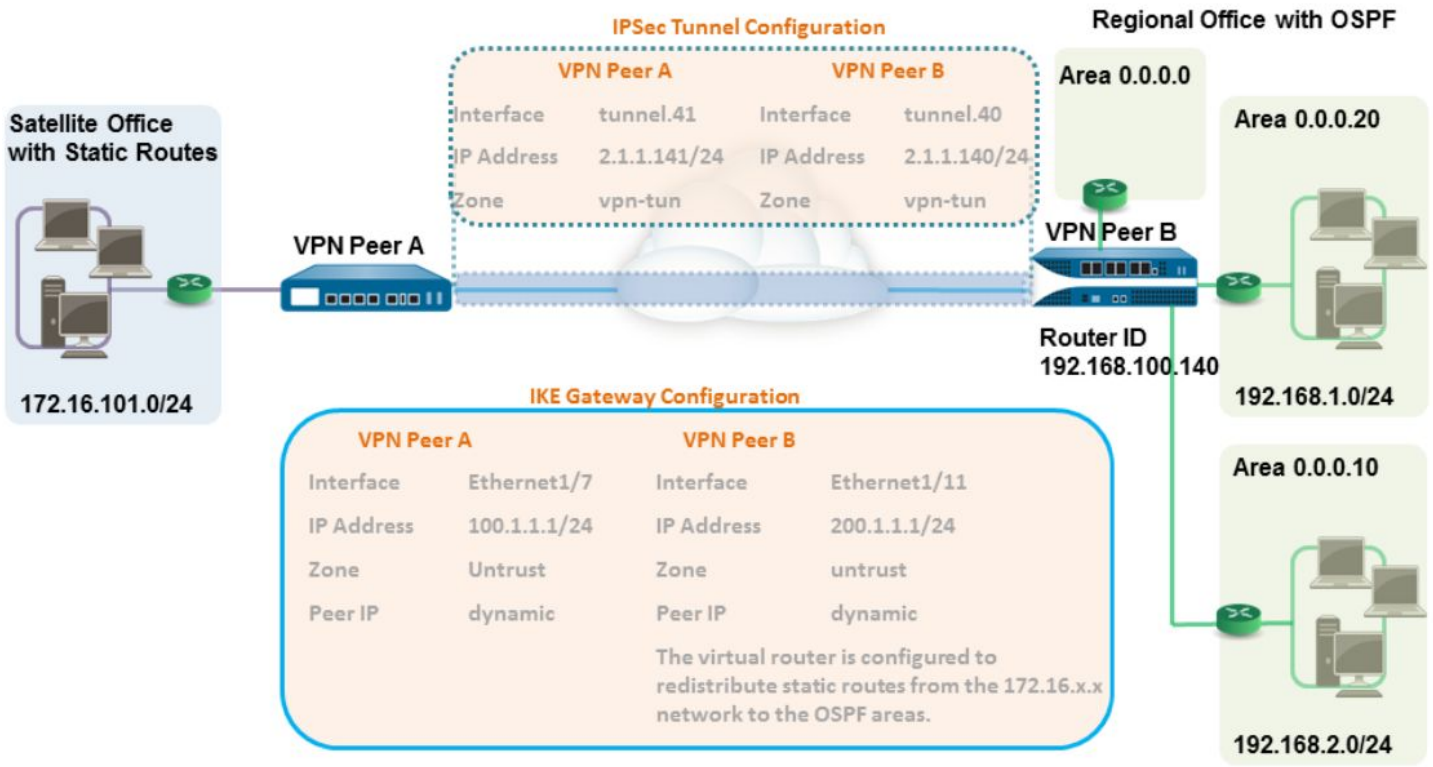


2.9 Configure Site-2-Site Tunnels

2.9.1 Configure IPSEC, GRE

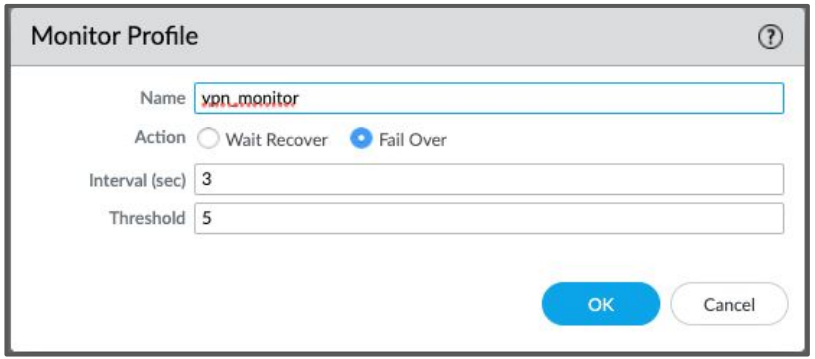


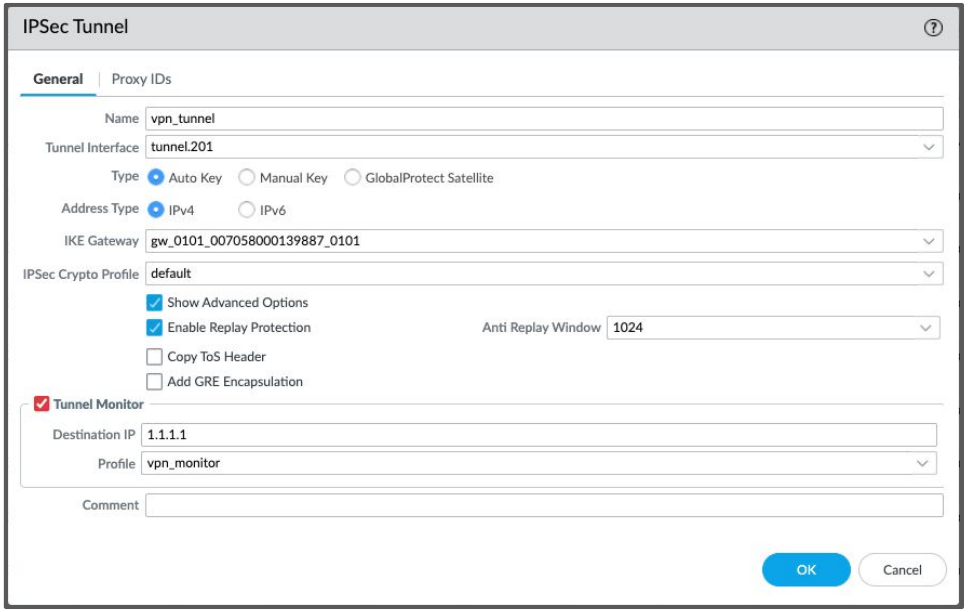
2.9.2 Static Peers & Dynamic Peers for IPSEC



2.9.3 IPSEC Tunnel Monitor Profiles

```
show vpn flow
1  tunnel-to-remote active    up        10.66.24.94
show vpn flow tunnel-id 1
monitor:            on
monitor status:     up
```





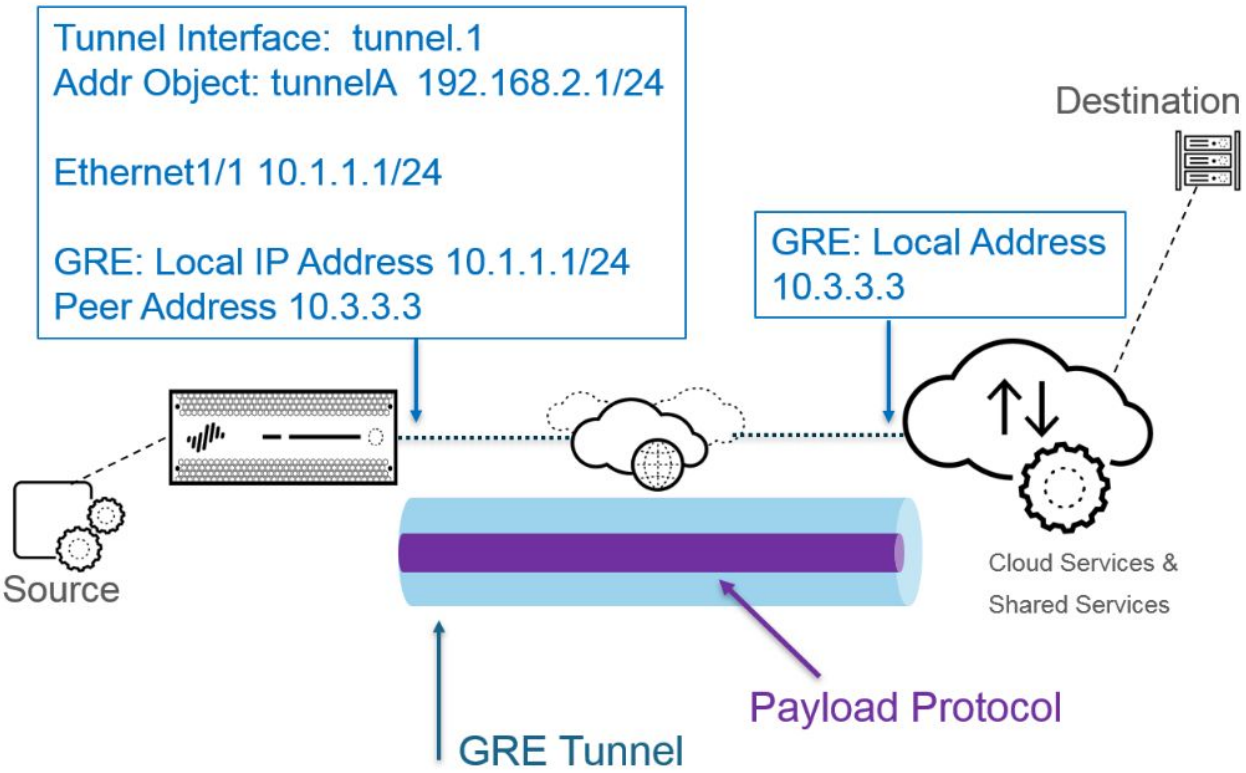
2.9.4 IPSEC Tunnel Testing

IKE Phase 1
test vpn ike-sa gateway <gateway_name>
show vpn ike-sa gateway <gateway_name>

IKE Phase 2
test vpn ike-sa tunnel <tunnel_name>
show vpn ike-sa tunnel <tunnel_name>

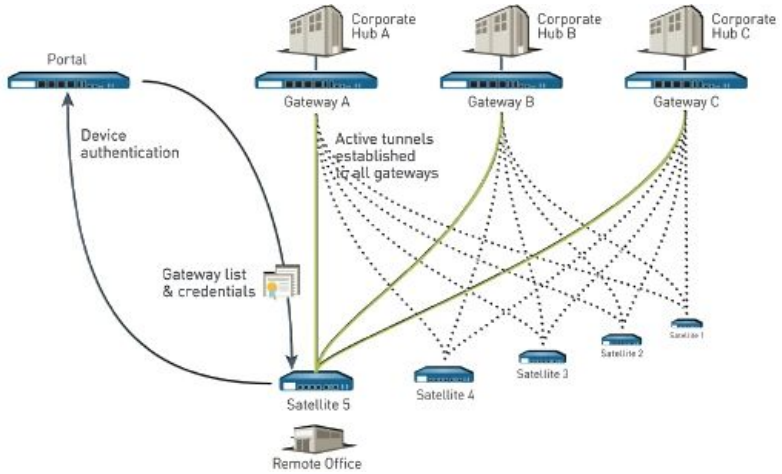
To See IPSEC Tunnel Flow
show vpn flow

2.9.5 Generic Routing Encapsulation (GRE)



2.9.6 One-to-one & One-to-Many Tunnels

- **Site-to-Site VPN**: Central site to remote site tunnel. Also commonly referred to as hub-and-spoke VPN that connects central (gateway) with multiple remote (branch) sites.
- **Remote-user-to-site VPN**: Endpoint client that uses GlobalProtect agent for secure remote user access through NGFW gateway.
- **Large Scale VPN (LSVPN)**: Deployment using Palo Alto Networks LSVPN provides scalable mechanism for hub-and-spoke VPN for up to 1,024 branch offices zero-touch provisioning.



2.9.7 Determine When to Use Proxy IDs

Multi-Vendor Compatibility - That All I'm Going to Say !

Configure Multiple Proxy IDs in VPN Tunnel with Overlapping Subnet Ranges (KB article):
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PLTlCAO

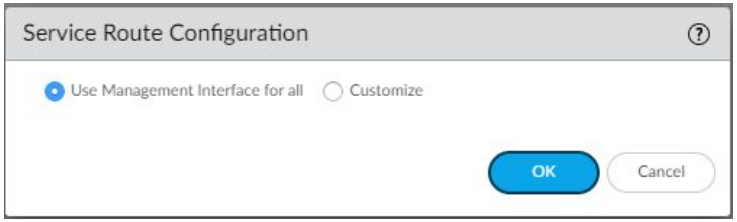
Tips & Tricks: Why Use a VPN Proxy ID?
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClUFCA0

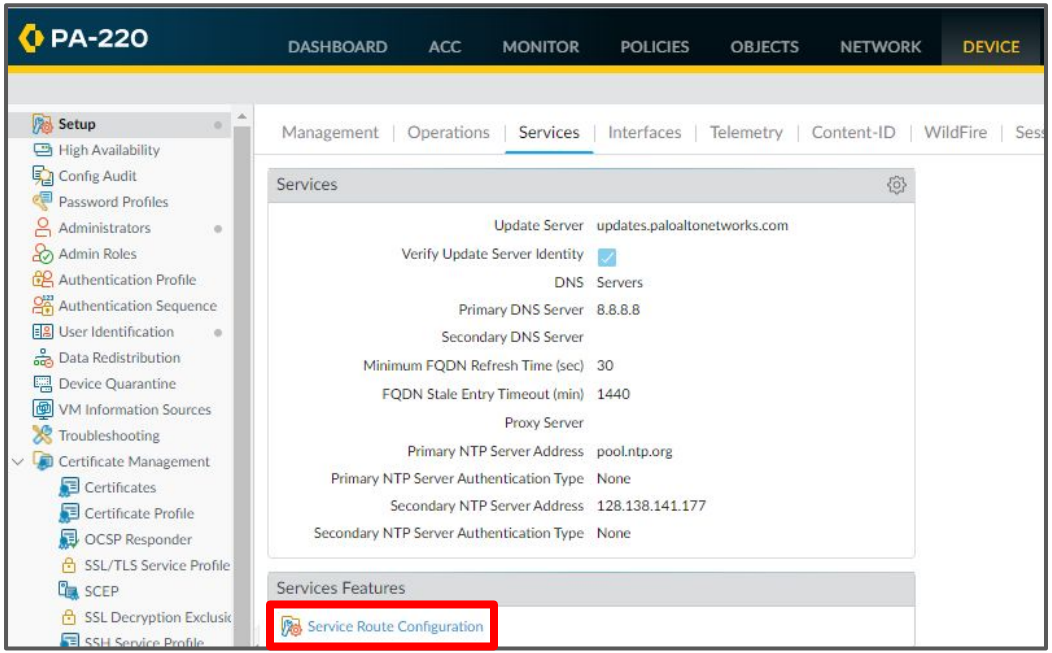
How to Build an IPSec Tunnel Between a Palo Alto Networks Firewall and a Cisco ASA (Adaptive Security Appliance)
https://blog.fuelusergroup.org/how-to-build-an-ipsec-tunnel-between-a-palo-alto-networks-firewall-and-a-cisco-asa

2.10 Configure Service Routes

2.10.1 Configure Default Routes

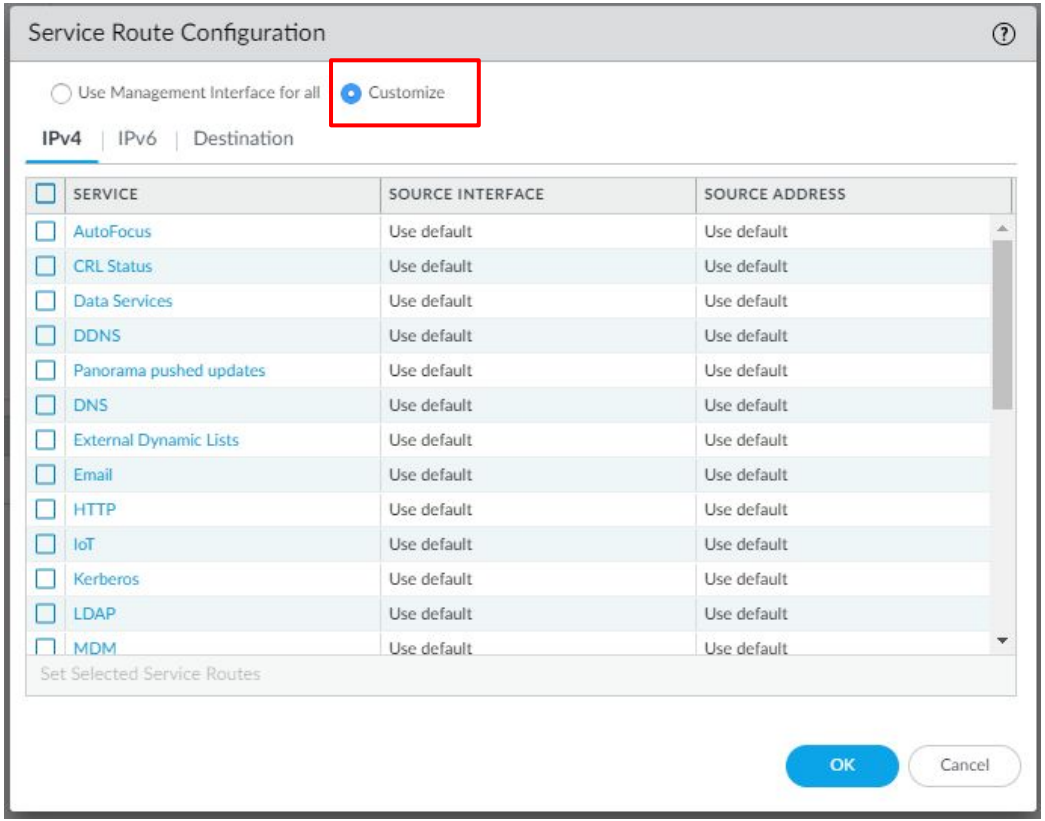
- > Device > Setup > Services > Service Routes
- Default Setting is to use Management Interface for all routes





2.10.2 Custom Service Routes

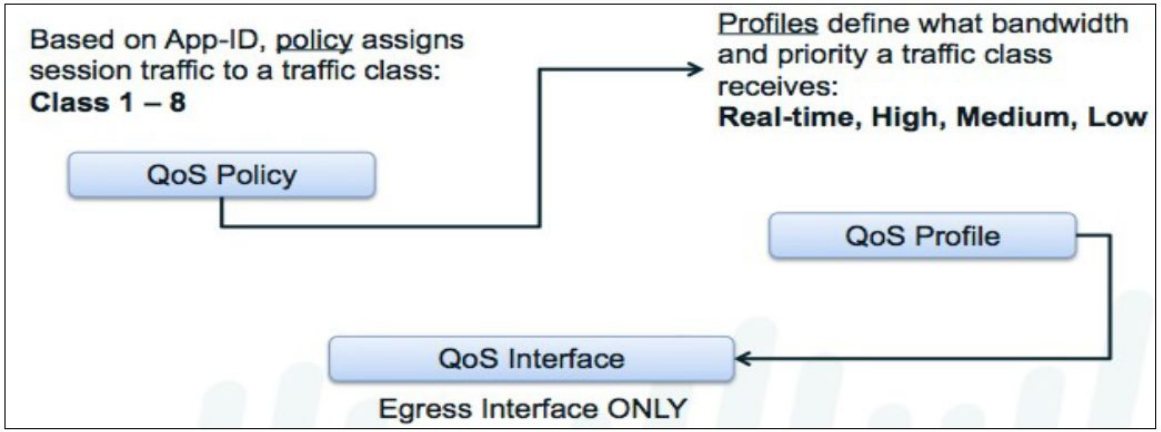
- > Device > Setup > Services > Service Routes
- Customize give you the ability to send traffic out another interface
- Example: use the untrusted (Internet) interface of a NGFW instead of the management interface



2.11 Configure Application-Based QoS

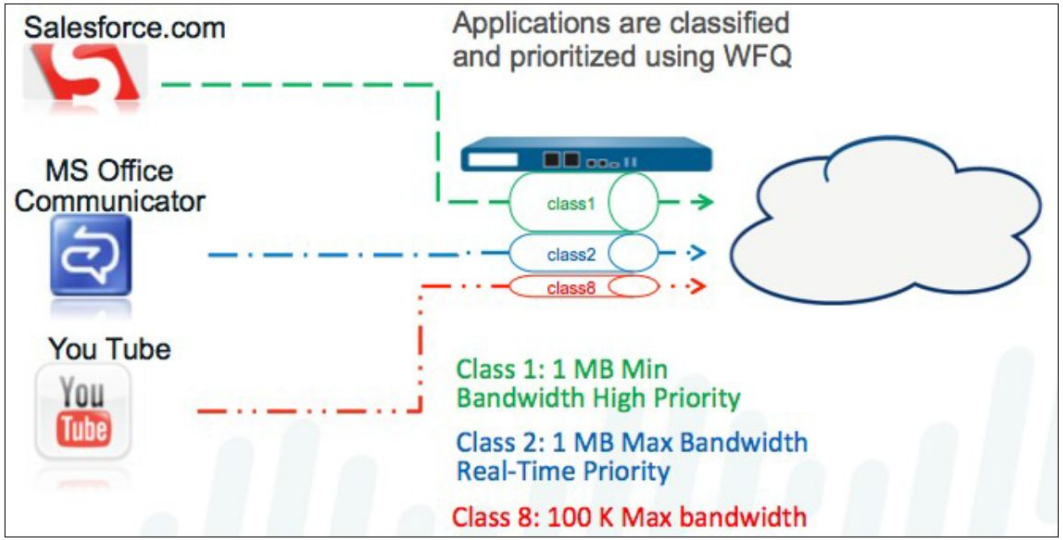
2.11.1 Select/Identify the Application

- Quality of Service(QoS)
- QoS Profiles assigned to egress interfaces
- PAN-OS Supports up to 8 QOS classes per policy
- PAN-OS Supports 4 Priority types
- Default Class is 4
- Requires QoS Policy, QoS Profile and QoS Egress Interface



2.11.2 Select Egress Interface (& Turn QoS on After Configuring it)

- Quality of Service(QoS)
- QoS Profiles assigned to egress interfaces
- PAN-OS Supports up to 8 QOS classes per policy
- PAN-OS Supports 4 Priority types
- Default Class is 4
- Requires QoS Policy, QoS Profile and QoS Egress Interface



 |

2.11.3 Add DSCP/TOS Markings

This can be very complicated. For the Purposes of the Test This is What You Should try to Remember

DSCP Markings:

EF = Expedited Forwarding (Typically Real-time Voice & Video Traffic)

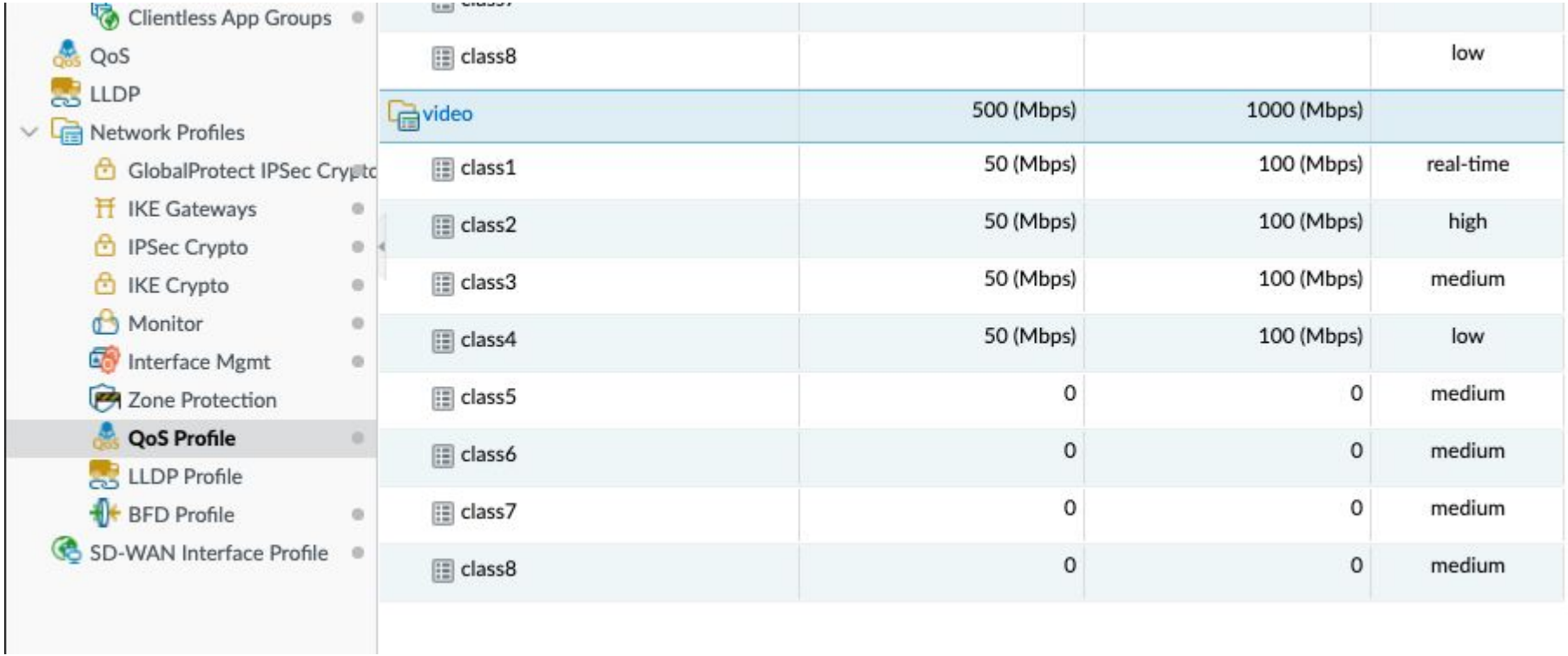
AF = Assured Forwarding (Typically Near Real Time Traffic Voice/Video Signaling & Playback Traffic also used for Priority Application Traffic)

BE = Best Effort (Typically Bulk Internet Traffic goes into this Queue)

DSCP is a newer way of coding QoS in IP Packets and replaced ToS some time ago. The above should get you through the test (and the rest of your career for that matter).

2.11.4 Configure QoS Profile

- > Network > QoS Profile



class8			low
video	500 (Mbps)	1000 (Mbps)	
class1	50 (Mbps)	100 (Mbps)	real-time
class2	50 (Mbps)	100 (Mbps)	high
class3	50 (Mbps)	100 (Mbps)	medium
class4	50 (Mbps)	100 (Mbps)	low
class5	0	0	medium
class6	0	0	medium
class7	0	0	medium
class8	0	0	medium

2.11.5 Determine How to Control Bandwidth on a Per-Application Basis

PCNSE MASTER CHALLENGE

Use the FUEL Virtual Lab - Use the PCNSE Study Guide Section 2.11.5 and an Application of Your Choice to Control Bandwidth on a Per-Application Basis

