

PCNSE Bootcamp v10.1

Exam Domain #2
Deploy and Configure



2.1 Configure Management Profiles

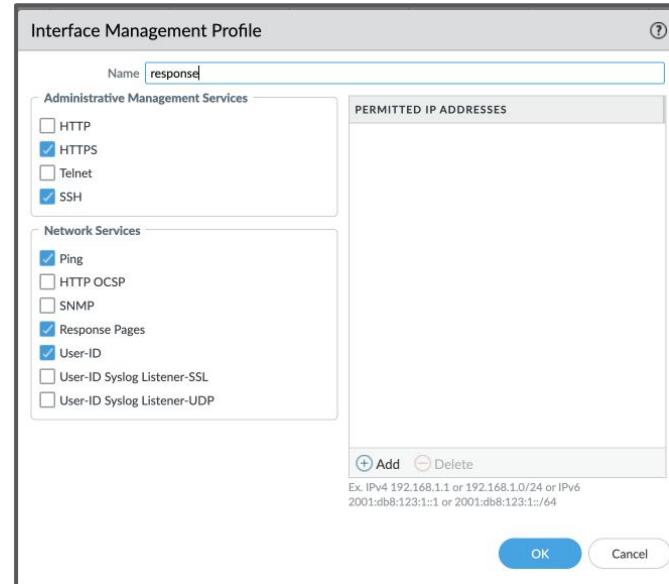
2.1.1 Interface Management Profile

The screenshot shows the PA-850 interface with the Policies tab highlighted in red. The left sidebar contains various configuration categories like Interfaces, Zones, VLANs, etc. The main pane displays a table of Interface Management Profiles. A red arrow points to the 'Interface Mgmt' item in the Network Profiles section of the sidebar.

NAME	PING	TELNET	SSH	HTTP
allow_ping	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
response	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Allow_Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

At the bottom, there are buttons for Add, Clone, and PDF/CSV.

- 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

PANORAMA DASHBOARD ACC MONITOR Device Groups Objects NETWORK DEVICE PANORAMA

Panorama Template: vm300-internet View by: Device Mode: Multi VSYS; Normal Mode; VPN Enabled

Location: Shared

6 items → >

NAME	LOCATION	CERTIFICATE	PROTOCOL VERSIONS
ssl-decrypt	Shared	ssl trust	Min Version: TLSv1.2 Max Version: Max
Global protect external fibersphere	Shared	GP External	Min Version: TLSv1.2 Max Version: Max
Global protect external ATT	Shared	GP GW ATT2	Min Version: TLSv1.2 Max Version: Max
Global protect internal	Shared	GP Internal	Min Version: TLSv1.2 Max Version: Max
Captive-Portal	Shared	vm-300-edge-CA	Min Version: TLSv1.2 Max Version: Max
<input checked="" type="checkbox"/> AdminGui	Shared	adminGui	Min Version: TLSv1.2 Max Version: Max

SSL/TLS Service Profile

SSL Decryption Exclusion
SSH Service Profile
Response Pages
Log Settings
Server Profiles
SNMP Trap
Syslog
Email
HTTP
Netflow
RADIUS
TACACS+
LDAP

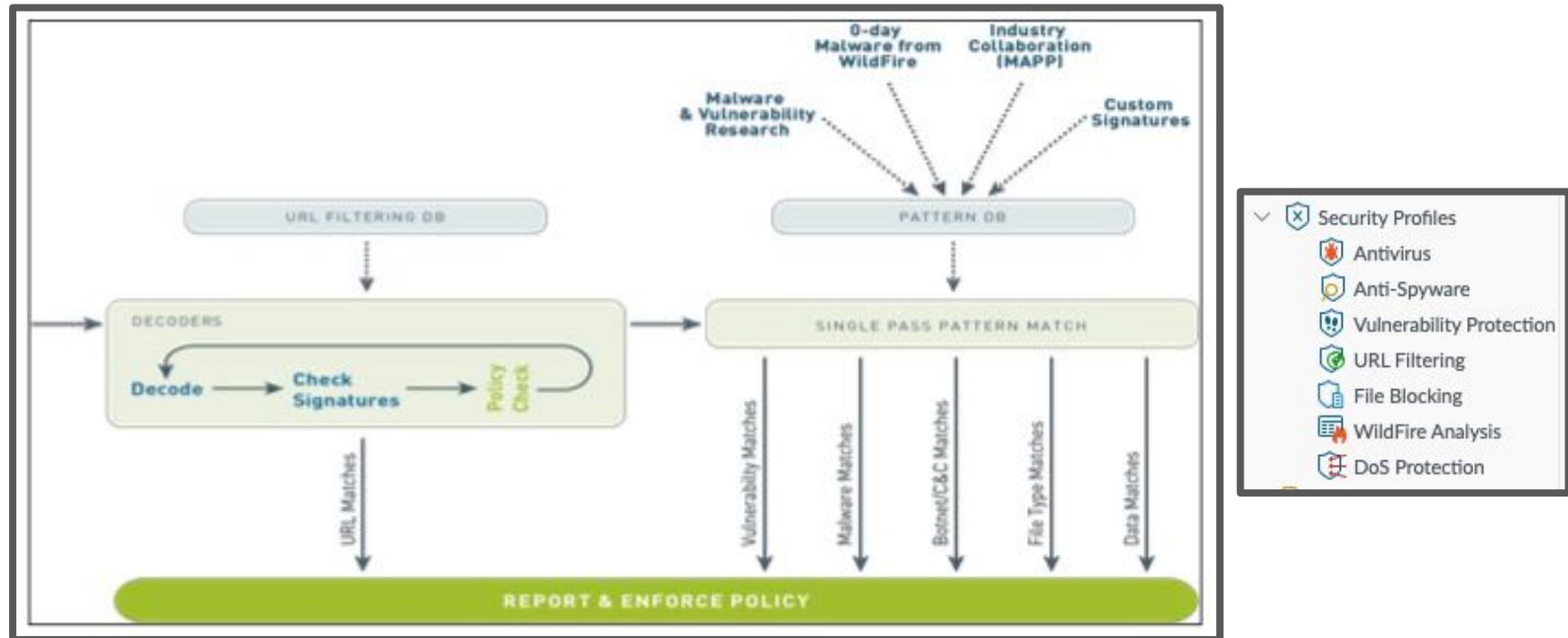
SSL/TLS Service Profile

Name: AdminGui
Certificate: adminGui
Protocol Settings:
Min Version: TLSv1.2
Max Version: Max

OK Cancel

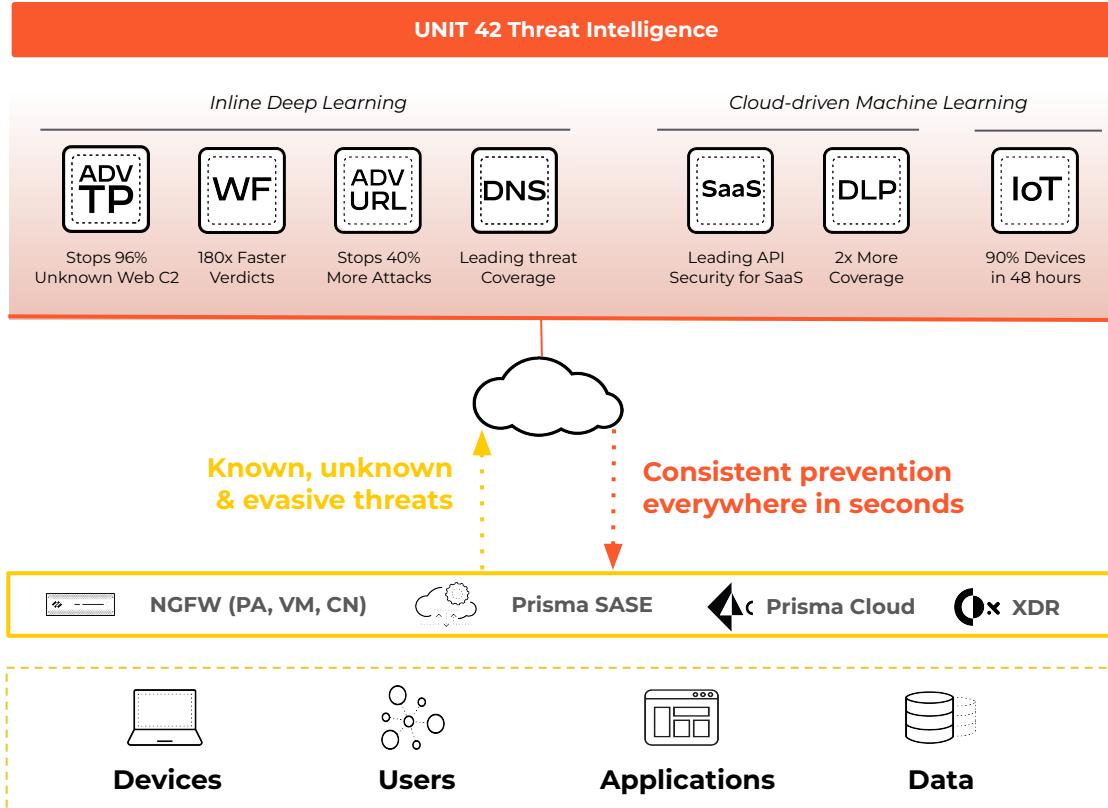
2.2 Deploy and configure Security Profiles

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

TYPE	Source					Destination			APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE							
universal	Remote	any	any	any	Home	any	any	apple-airplay	any	any	any	Allow		



Antivirus



Anti-Spyware



Vulnerability Protection



URL Filtering



File Blocking



Data Filtering



WildFire Analysis



Security Profile Group

2.2 Security Profile updates

Security Profiles



Antivirus



Anti-Spyware



Vulnerability Protection



URL Filtering



File Blocking

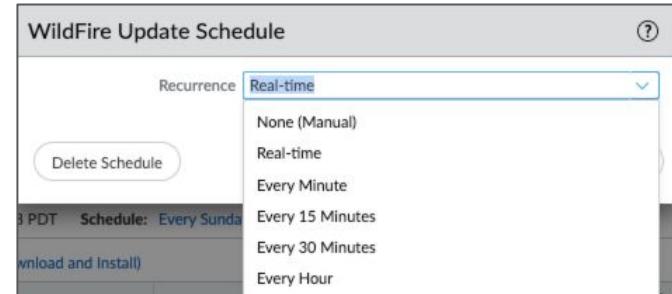


WildFire Analysis



DoS Protection

- 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

Antivirus Profile

Name: AV-Profile

Description:

Action | Signature Exceptions | WildFire Inline ML

Enable Packet Capture

Decoders

PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION
ftp	default (reset-both)	default (reset-both)	default (reset-both)
http	default (reset-both)	default (reset-both)	default (reset-both)
http2	allow	default (reset-both)	default (reset-both)
imap	alert	default (alert)	default (alert)
pop3	drop	default (alert)	default (alert)
smb	reset-client	default (reset-both)	default (reset-both)
smtp	reset-server	default (alert)	default (alert)
	reset-both		

Application Exceptions

APPLICATION	ACTION

0 items

OK Cancel

PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION
ftp	default (reset-both)	default (reset-both)	default (reset-both)
http	default (reset-both)	default (reset-both)	default (reset-both)
http2	allow	default (reset-both)	default (reset-both)
imap	alert	default (alert)	default (alert)
pop3	drop	default (alert)	default (alert)
smb	reset-client	default (reset-both)	default (reset-both)
smtp	reset-server	default (alert)	default (alert)
	reset-both		

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



The screenshot shows the "Anti-Spyware Profile" configuration window. A modal dialog box is open, titled "Anti-Spyware Policy", showing the configuration for the "AS Policy".

POLICY NAME	SEVERITY	ACTION	PACKET CAPTURE
AS Policy	any		

The "Severity" section of the dialog is highlighted with a red box, showing the following options:

- any (All severity) - Allow
- critical - Alert
- high - Drop
- medium - Reset Client
- low - Reset Server
- information - Reset Both
- Block IP

At the bottom of the dialog are "OK" and "Cancel" buttons.

2.2 Vulnerability Protection Profiles

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

Vulnerability Protection Profile (Read Only)

RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
simple-client-critical	any	any	client	critical	default	disable
simple-client-high	any	any	client	high	default	disable
simple-client-medium	any	any	client	medium	default	disable
simple-server-critical	any	any	server	critical	default	disable
simple-server-high	any	any	server	high	default	disable
simple-server-medium	any	any	server	medium	default	disable

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

Used to match any signature containing the entered text as part of the signature CVE or Vendor ID

OK Cancel

Vulnerability Protection Rule

Rule Name	Threat Name	Action	Host Type	Severity	Category
simple-client-critical	any	Default	Any	critical	any

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

Used to match any signature containing the entered text as part of the signature CVE or Vendor ID

OK Cancel

2.2 URL Filtering Profiles

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

The screenshot shows the 'URL Filtering Profile' configuration screen. At the top, there are fields for 'Name' and 'Description'. Below these are tabs: 'Categories' (which is selected and highlighted with a red box), 'URL Filtering Settings', 'User Credential Detection', 'HTTP Header Insertion', and 'Inline Categorization'. The main area displays a table of categories with columns for 'CATEGORY', 'SITE ACCESS', and 'USER CREDENTIAL SUBMISSION'. The 'USER CREDENTIAL SUBMISSION' column contains mostly 'allow' values, except for 'iTunes' which is 'alert'. A context menu is open over the 'USER CREDENTIAL SUBMISSION' column, showing options like 'Sort Ascending', 'Sort Descending', 'Columns', 'Set All Credential Submission Actions' (which is highlighted with a red box), 'Set Selected Credential Submission Actions', and 'Adjust Columns'. A red box also highlights the 'allow', 'alert', 'block', and 'continue' options listed under 'Set All Credential Submission Actions'. At the bottom of the table, there is a note about custom URL categories and external dynamic lists, and a 'Check URL Category' button.

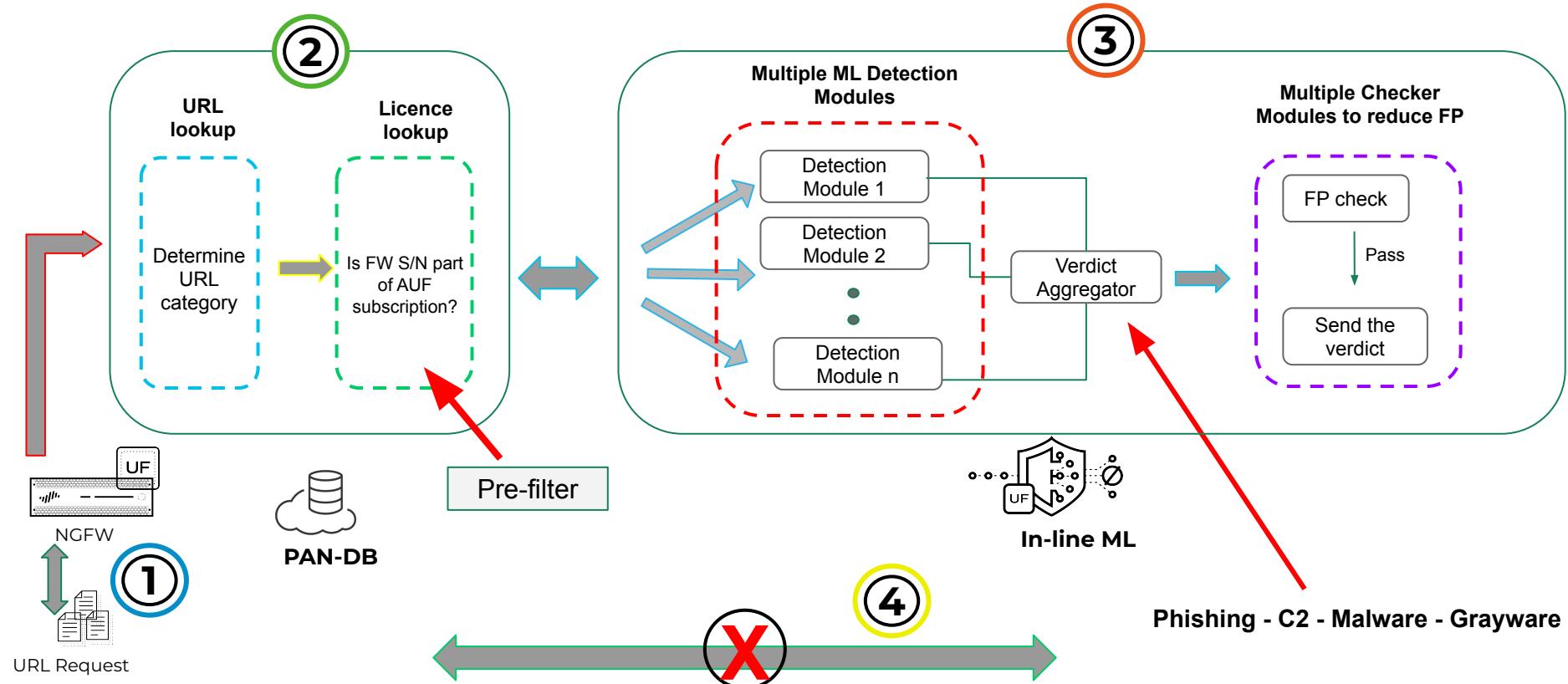
CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
Enable BingSafeSearch *	alert	allow
facebook *	alert	allow
high_sites *	alert	allow
iTunes *	alert	allow
no_decrypt *	alert	allow
PAN *	alert	allow
Search Engines *	alert	allow
SearchEngineDetection *	alert	allow

* indicates a custom URL category, + indicates external dynamic list
Check URL Category

OK Cancel

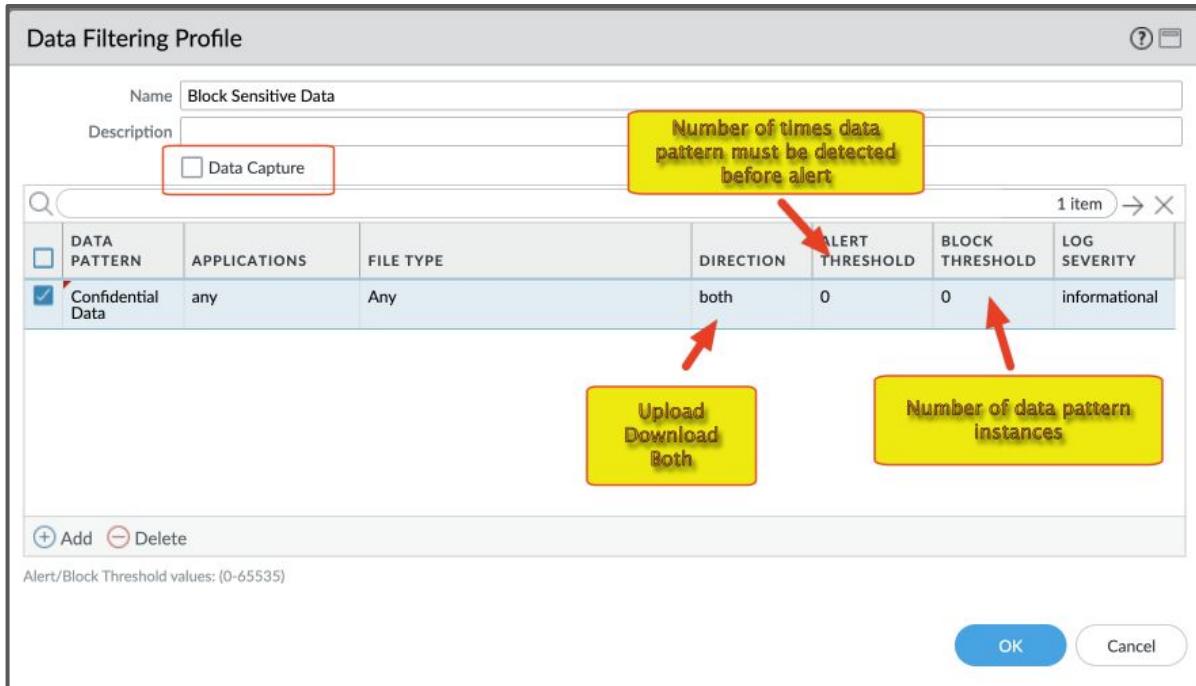
Alert Categories (84) Alert Categories (1)

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**

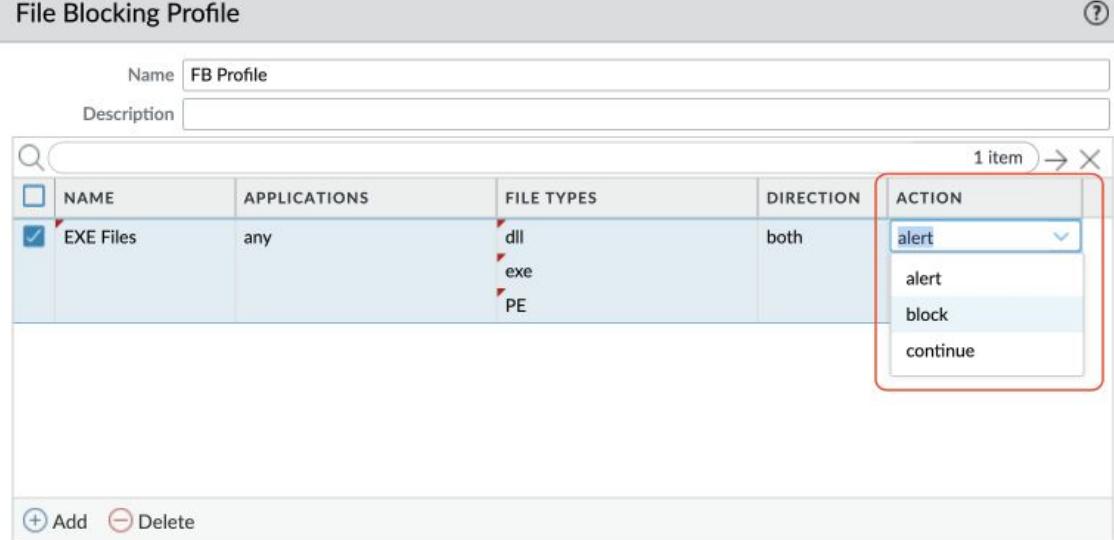
File Blocking Profile

Name	FB Profile
Description	

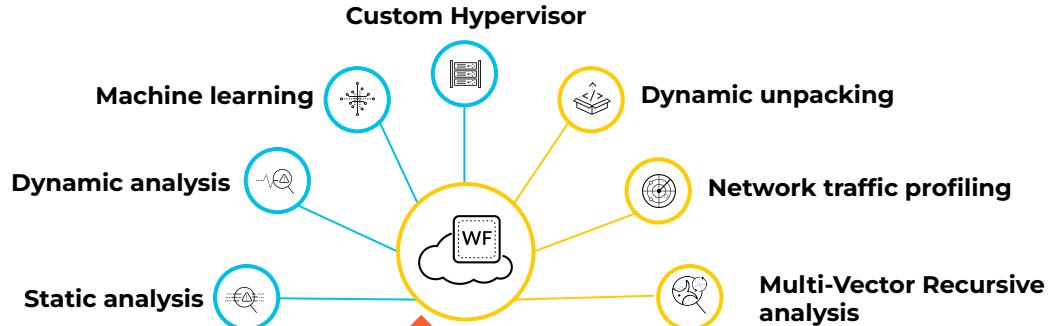
NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
EXE Files	any	dll exe PE	both	alert

+ Add - Delete

Supports custom response pages



Wildfire Security profiles



Network

Endpoint

Cloud

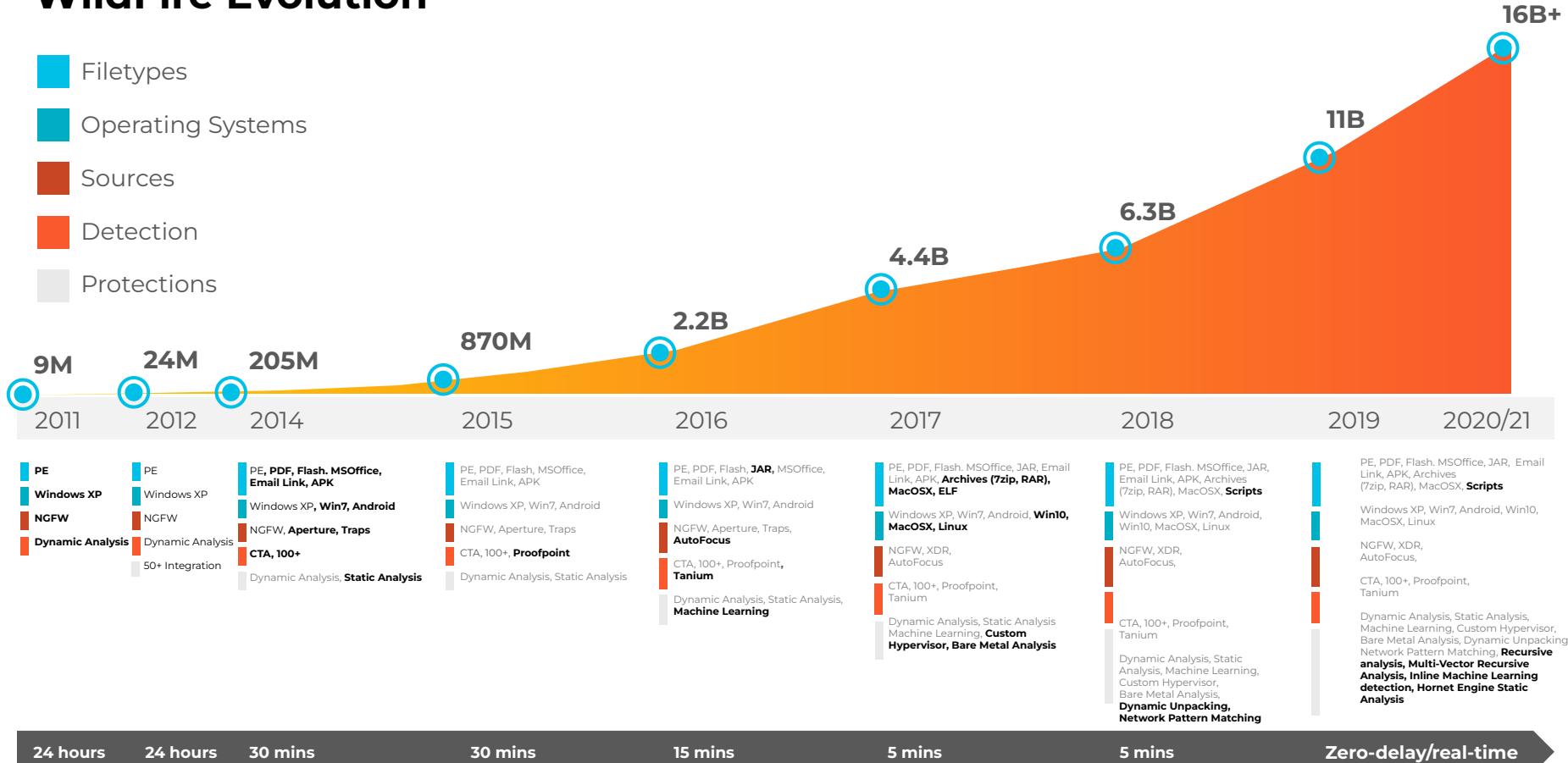
Partner
Ecosystem

Data collected from a vast
global community

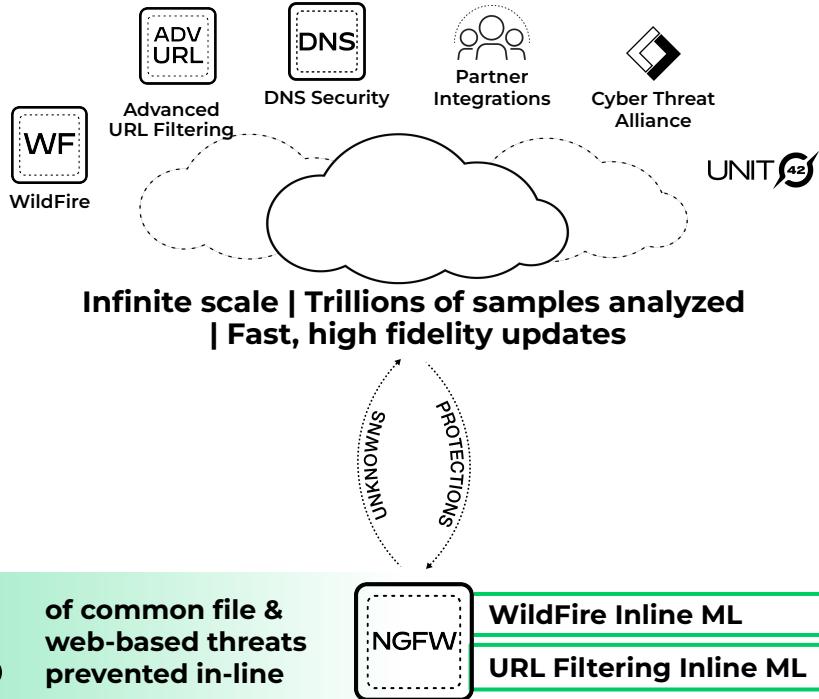
Analysis techniques far beyond
traditional sandboxing

Automated protection against
multiple attack variants

WildFire Evolution



Preventing Unknown Threats Through Cloud Scale and Inline ML



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

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



File Protections: **Instant**



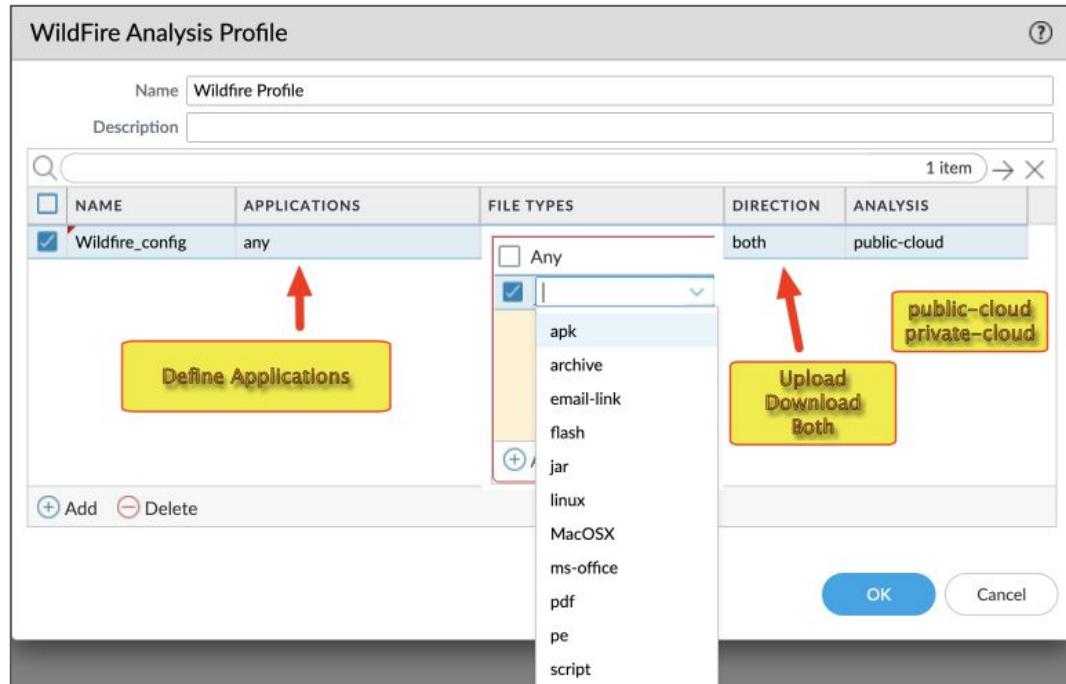
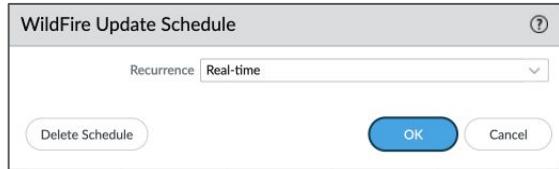
URL Protections: **Instant**



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

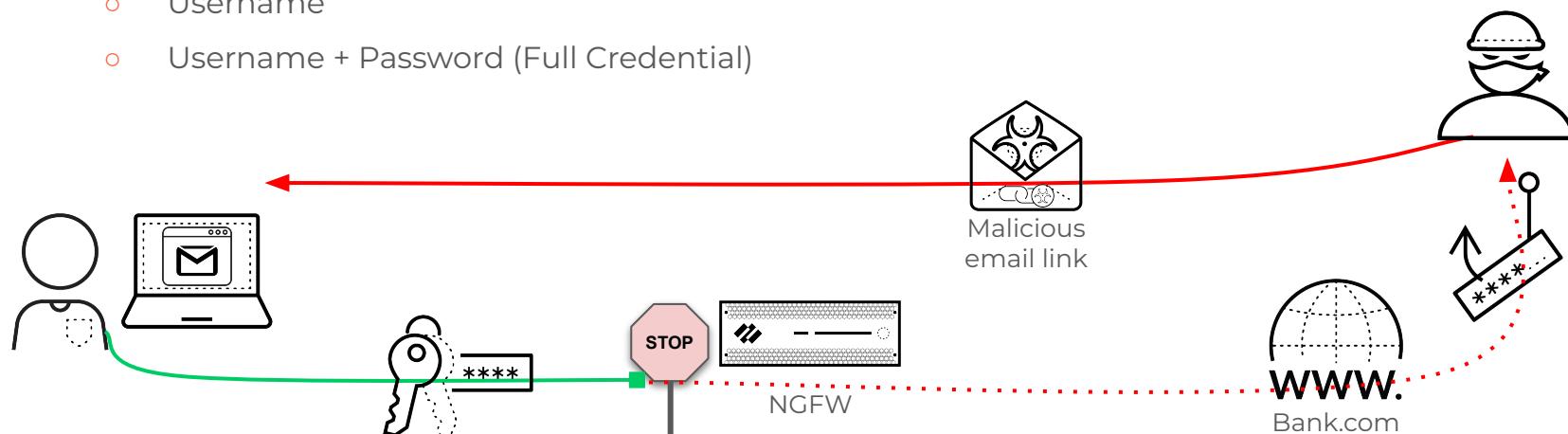
layer

The screenshot shows the 'Resources Protection' tab selected. A checkbox labeled 'Sessions' is checked. Below it, a field labeled 'Maximum Concurrent Sessions' contains the value '32768', which is highlighted with a red border.

The screenshot shows the 'DoS Protection Profile' dialog box for a profile named 'syn_cookie'. The 'Type' is set to 'Classified'. The 'Flood Protection' tab is selected, showing options for 'SYN Flood', 'UDP Flood', 'ICMP Flood', 'ICMPv6 Flood', and 'Other IP Flood'. The 'SYN Flood' checkbox is checked. The 'Action' dropdown is set to 'SYN Cookies'. Other settings include 'Alarm Rate (connections/s)' set to 'Random Early Drop', 'Activate Rate (connections/s)' set to 'SYN Cookies', 'Max Rate (connections/s)' set to '100000', and 'Block Duration (s)' set to '20'. At the bottom are 'OK' and 'Cancel' buttons.

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	<ul style="list-style-type: none">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 .	<ul style="list-style-type: none">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 .	<ul style="list-style-type: none">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

The screenshot displays the URL Filtering Profile configuration interface for a profile named "Best Practice".

Categories: A list of custom URL categories including abortion, abused-drugs, adult, alcohol-and-tobacco, auctions, and business-and-economy. Each category has associated Site Access and User Credential Submission rules.

CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
abortion	allow	allow
abused-drugs	block	block
adult	block	allow
alcohol-and-tobacco	allow	allow
auctions	allow	allow
business-and-economy	allow	allow

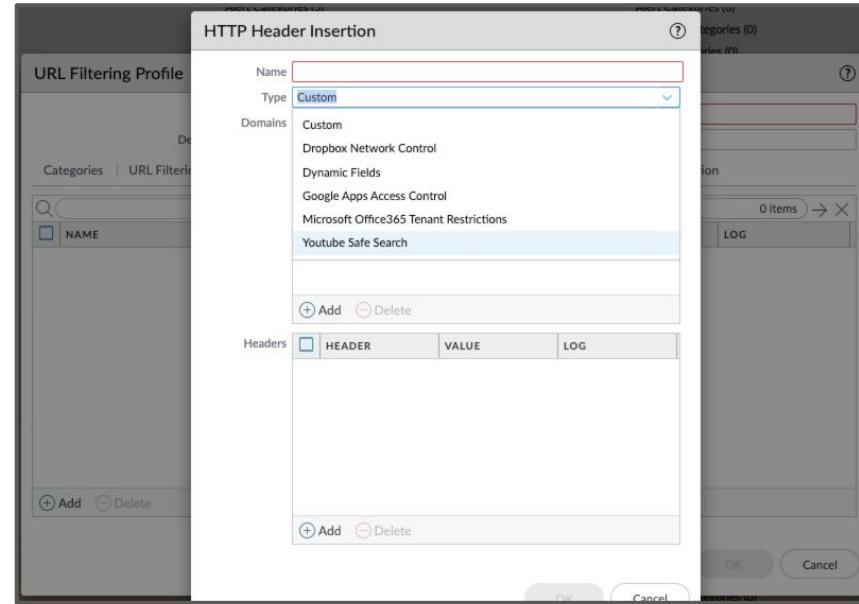
User Credential Detection: Set to "Disabled". Other options include Use IP User Mapping, Use Domain Credential Filter, and Use Group Mapping.

Inline ML: A table showing Site Access and User Credential Submission rules. The "allow" rule under Site Access is highlighted with a red box.

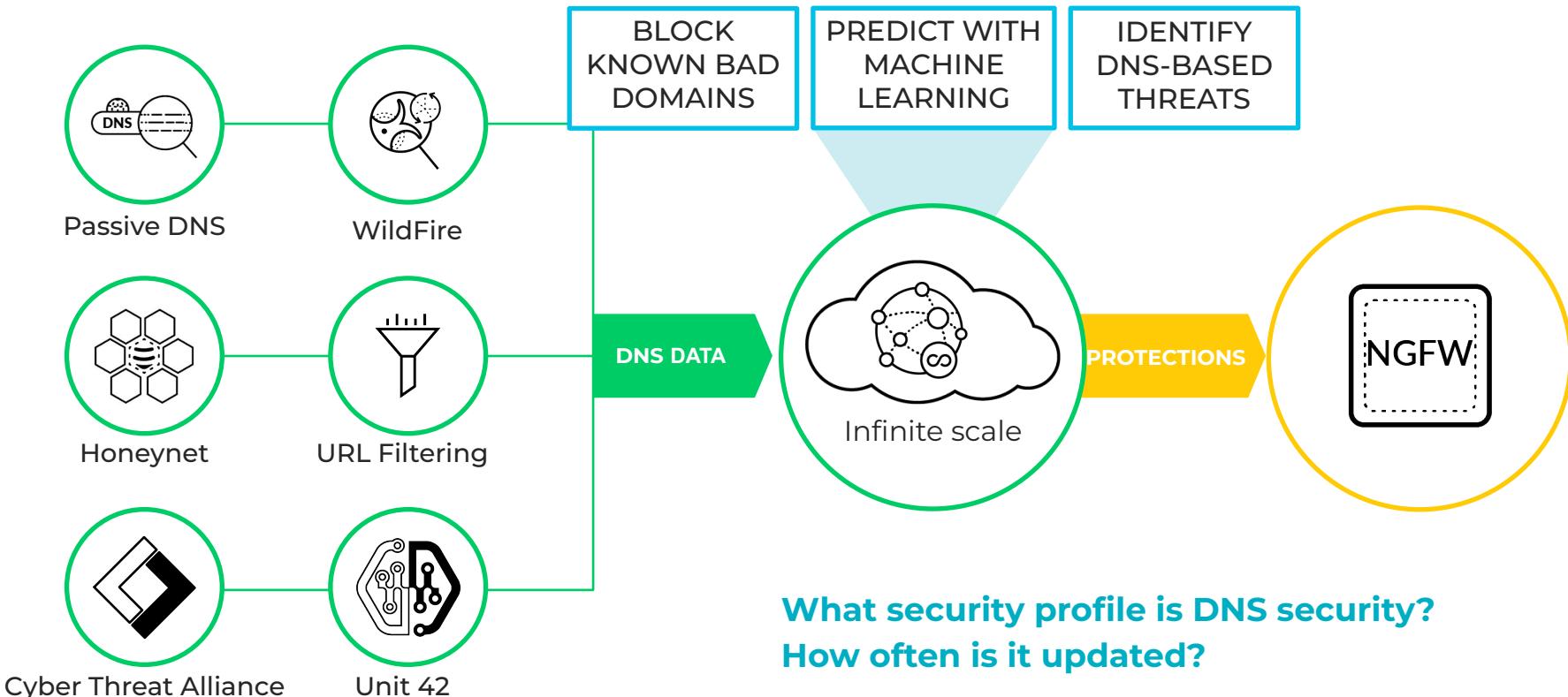
SITE ACCESS	USER CREDENTIAL SUBMISSION
allow	allow
allow	alert
allow	allow
allow	block
allow	continue
allow	none

2.2.3 Use of username and domain name in HTTP header insertion

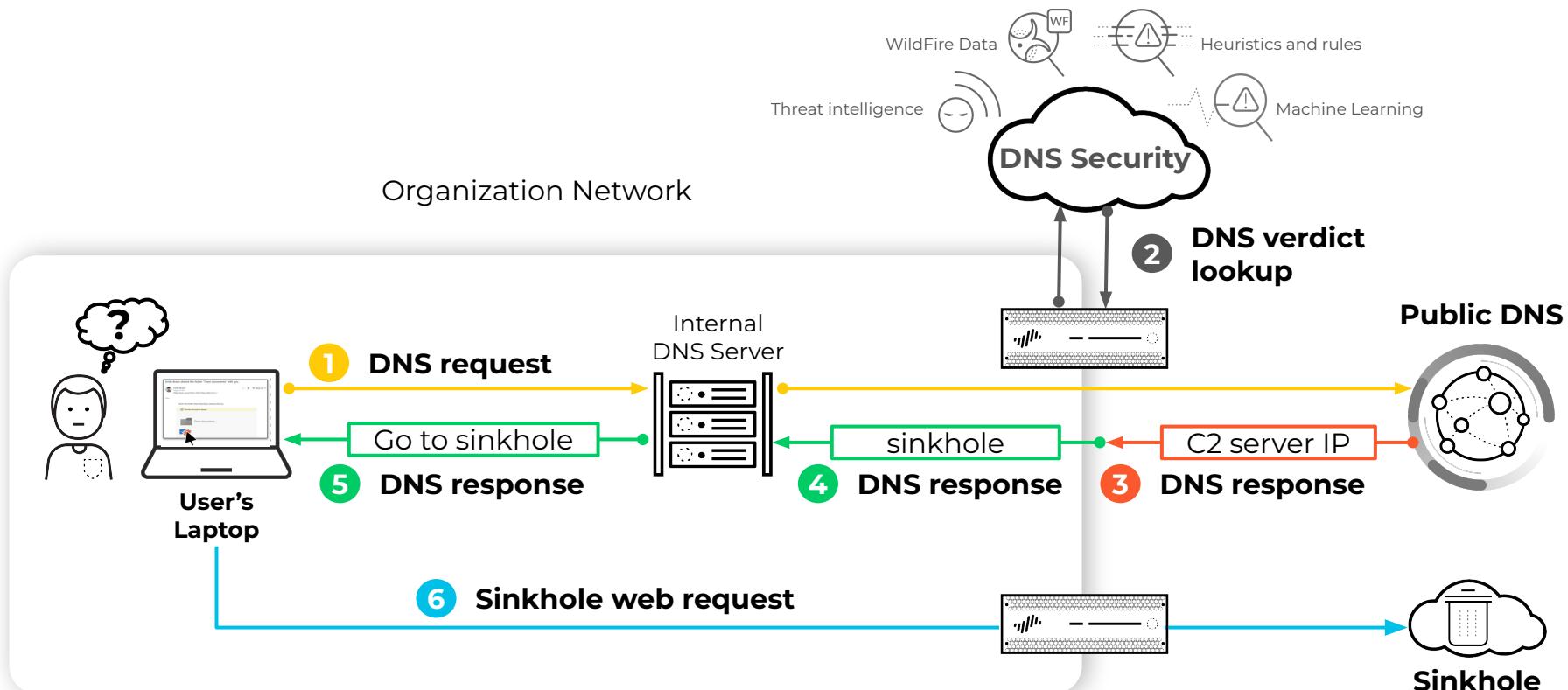
- HTTP header insertion is only available for HTTP/1.x traffic - NOT HTTP/2 traffic
- Supported for GET, POST, PUT and HEAD



2.2.4 DNS Security



DNS Security: Disrupting Attacks With Machine Learning



2.2.5 How to tune or add exceptions to a Security Profile

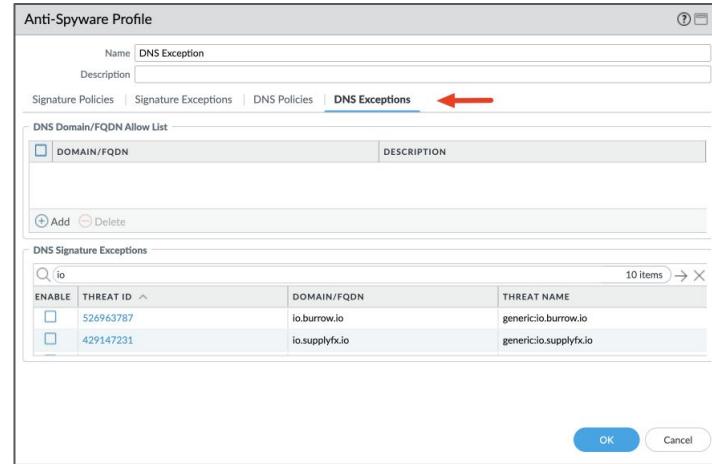
Configure threat exceptions for antivirus, vulnerability, spyware, and DNS signatures to change firewall enforcement for a threat.

Step 1: Exclude antivirus signatures from enforcement.

Step 2: Modify enforcement for vulnerability and spyware signatures. (This does not include DNS signatures;

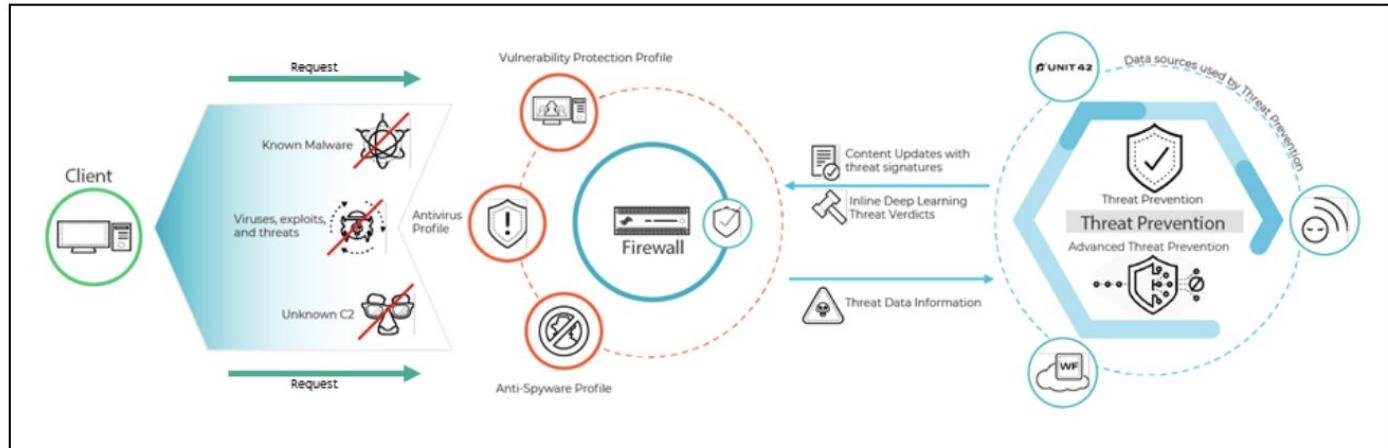
skip to the next option to modify enforcement for DNS signatures, which are a type of spyware signature.)

Step 3: Modify enforcement for DNS signatures.



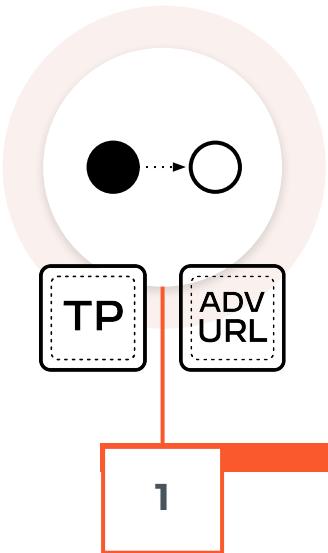
2.2.6 Compare and contrast threat prevention and advanced threat prevention

- **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.

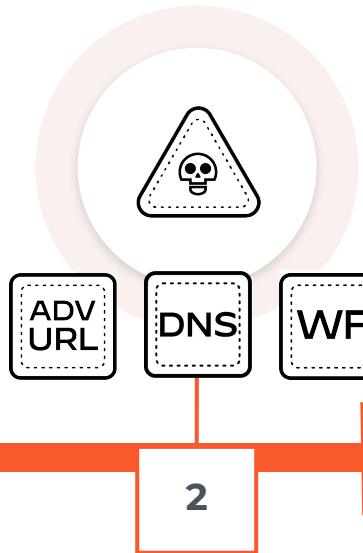


Defense in Depth across the Attack Lifecycle

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

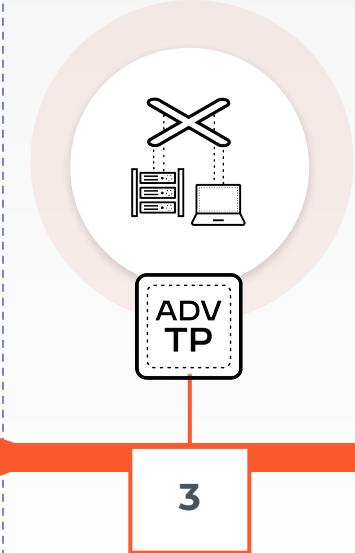


Malware download blocked by **Adv URL Filtering, DNS Security and WildFire**

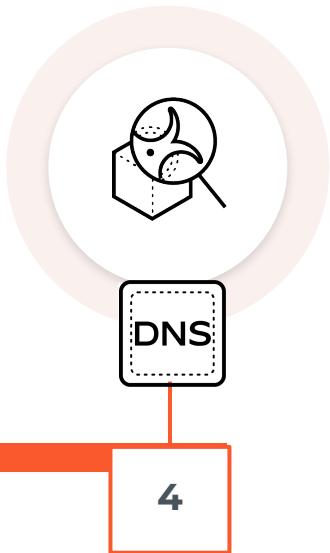


New

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 be 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

The screenshot shows the 'DEVICE' tab in the Palo Alto Networks interface. On the left, a sidebar lists various device management categories. The main area displays license details under the 'DEVICE' tab.

Advanced URL Filtering

- Date Issued: May 19, 2021
- Date Expires: September 19, 2022
- Description: Palo Alto Networks Advanced URL License

PAN-DB URL Filtering

- Date Issued: May 19, 2021
- Date Expires: September 19, 2022
- Description: Palo Alto Networks URL Filtering License
- Active: Yes

Premium

- Date Issued: May 06, 2021
- Date Expires: **October 29, 2019 (EXPIRED)**
- Description: 24 x 7 phone support; advanced replacement hardware service

Virtual Systems

- Date Issued: May 11, 2021
- Date Expires: Never
- Description: Additional 5 Virtual System Licenses

Software warranty

- Date Issued: May 06, 2021
- Date Expires: **January 29, 2019 (EXPIRED)**
- Description: 90 days for software warranty

License Management

- Retrieve license keys from license server
- Activate feature using authorization code
- Manually upload license key

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

URL Filtering Profile

Name: almas-test

Description:

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

CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
philosophy-and-political-advocacy	alert	allow
phishing	block	block
private-ip-addresses	alert	allow
proxy-avoidance-and-anonymizers	alert	allow
questionable	alert	block
real-estate	alert	allow
real-time-detection	block	block

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

Check URL Category

Real-time-detection category

Link URL Profile to the policy

The screenshot shows the Palo Alto Networks UI for managing security policies. On the left, a sidebar lists various security modules: Security, NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN. The main area displays a table of security policy rules:

NAME	TAGS	TYPE	Source				Destination			APPLICATION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	
1 Allow-dns	none	universal	any	any	any	any	any	any	any	dns
2 Deny-Quic udp	none	universal	any	any	any	any	any	any	any	any
3 Deny-Quic										
4 TEST-1										
5 TEST										

A modal window titled "Security Policy Rule" is open, showing the configuration for rule 5 (TEST). The "Actions" tab is selected. The "Action Setting" section includes "Action: Allow" and an unchecked checkbox for "Send ICMP Unreachable". The "Profile Setting" section includes "Profile Type: Profiles", "Antivirus: None", "Vulnerability Protection: None", "Anti-Spyware: None", and a red box highlights the "URL Filtering: almas-test" field. The "Log Setting" section has checkboxes for "Log at Session Start" and "Log at Session End", both checked. The "Log Forwarding" dropdown is set to "None". The "Other Settings" section includes "Schedule: None", "QoS Marking: None", and an unchecked checkbox for "Disable Server Response Inspection".

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

Logs	(url_category_list contains real-time-detection)						
	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	
URL Filtering	04/21 05:36:44	command-and-control	real-time-detection,command-and-control	cdftisan.net/banner/logo.gif?141b33d=189746469	Trust	Untrust	
	04/21 05:35:57	malware	real-time-detection,newly-registered-domain,malware	offerscreative.com/cl/1213_pd/2/3767/1739/424/06932	Trust	Untrust	
	04/21 05:35:37	phishing	real-time-detection,phishing	manusbern.gq/zaz.php	Trust	Untrust	
	04/21 05:34:37	phishing	real-time-detection,phishing	manusbern.gq/zaz.php	Trust	Untrust	
	04/21 05:33:22	malware	real-time-detection,newly-registered-domain,malware	lalemada.info/b21f534a2c9bb2c32e1afaff25a65291/getfp.exe	Trust	Untrust	
	04/21 05:14:57	malware	real-time-detection,malware	hbdry.cn/case-28-1.html/templates/default/js/css/css/main.css	Trust	Untrust	
	04/21 05:13:55	phishing	real-time-detection,phishing	biyog.info/template/valid/sub	Trust	Untrust	

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



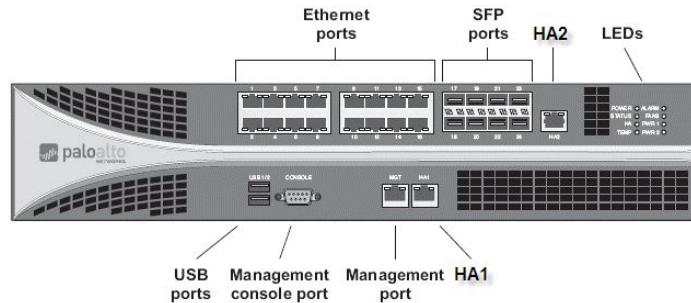
Note

With Geneve inspection enabled, the firewall is able to look inside the Geneve encapsulation to the actual traffic. If you don't enable Geneve inspection, the firewall sees traffic destined to the dataplane interface IP address with a destination port of 6081.

2.4.2 Implement an HA Pair

Overview Steps

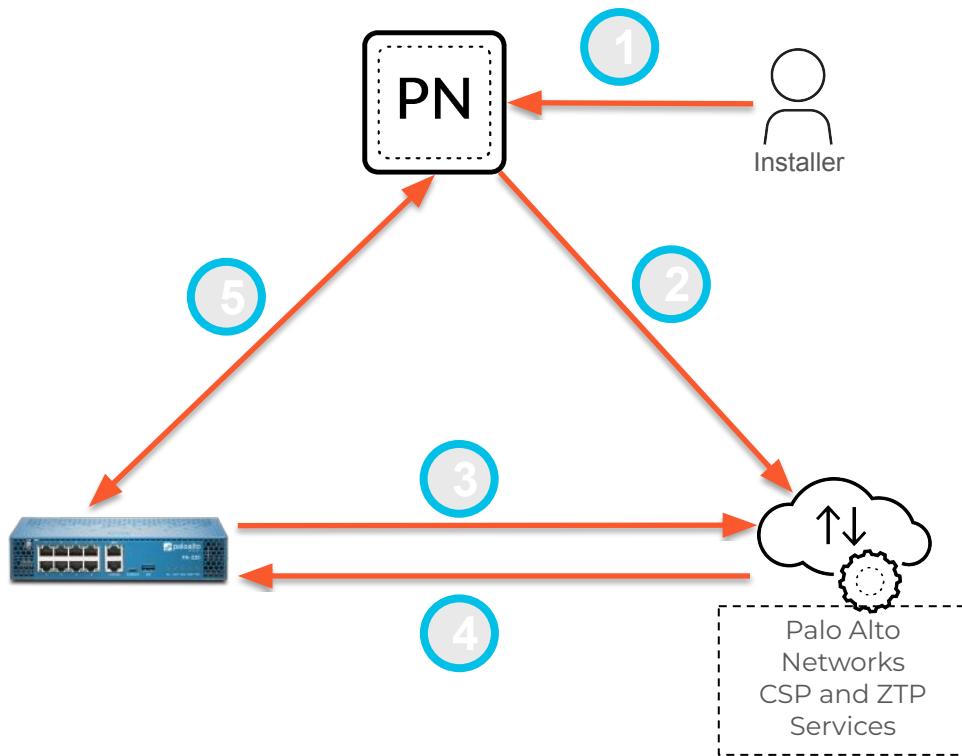
- Connect the HA ports.
- Enable ping on the management port.
- Set the HA mode and group ID.
- Set up the control link connection.
- Enable encryption for the control link connection.
- Set up the backup control link connection.
- Set up the data link connection (HA2) and the backup HA2 connection.
- 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

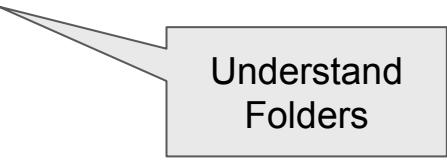
Init-cfg.txt - basic info like IP address, netmask, DG

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



Understand
Folders

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

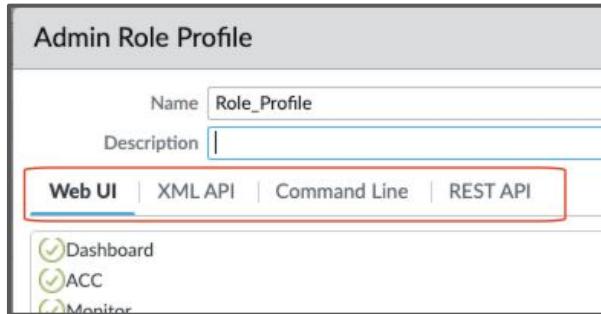
2.5 Configure authorization, authentication, and device access

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



The screenshot shows the 'Administrator' configuration screen. It includes fields for 'Name' (new_admin), 'Authentication Profile' (None), 'Password' and 'Confirm Password' (both masked), and 'Password Requirements' (Minimum Password Length (Count) 8). The 'Administrator Type' section is highlighted with a red box, showing 'Dynamic' selected over 'Role Based'. Below this are dropdowns for 'Superuser' and 'Password Profile' (None). A large callout box highlights the 'Superuser' dropdown, which lists 'Superuser', 'Superuser (read-only)', 'Device administrator', and 'Device administrator (read-only)', with 'Device administrator (read-only)' selected. Another callout box highlights the 'Profile' dropdown in a separate window, showing a list of profiles: 'auditadmin', 'cryptoadmin', 'firewalladmin', 'readonlyadmin', 'securityadmin', and 'New Admin Role Profile'.

2.5.2 Different methods used to authenticate

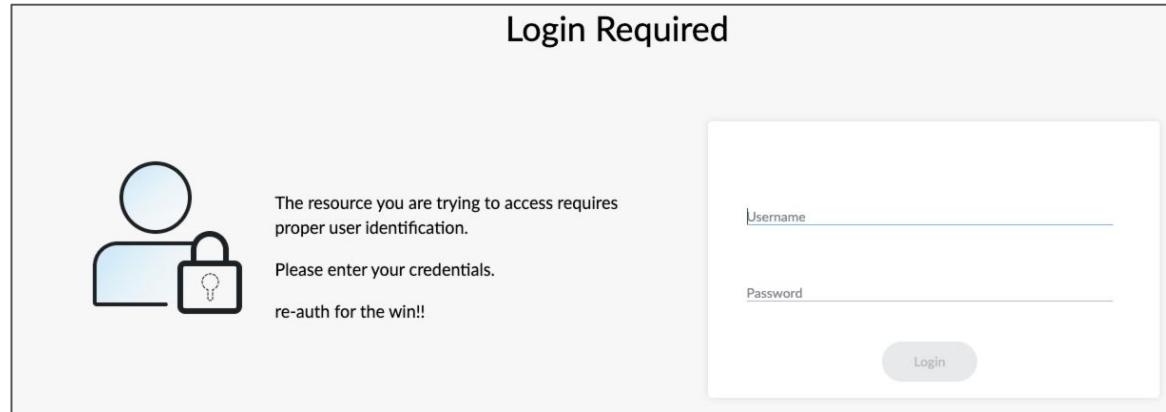
Supported authentication types include the following:

- 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*



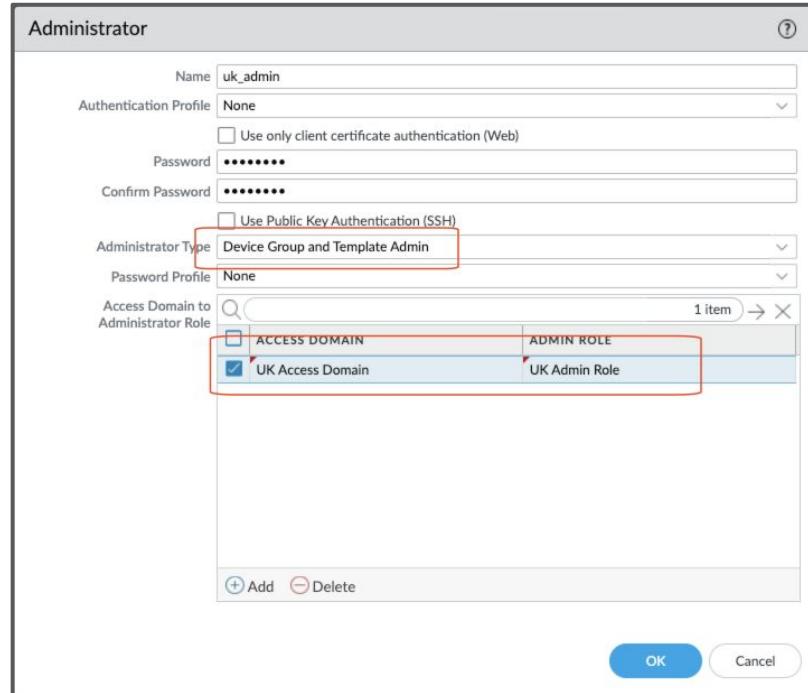
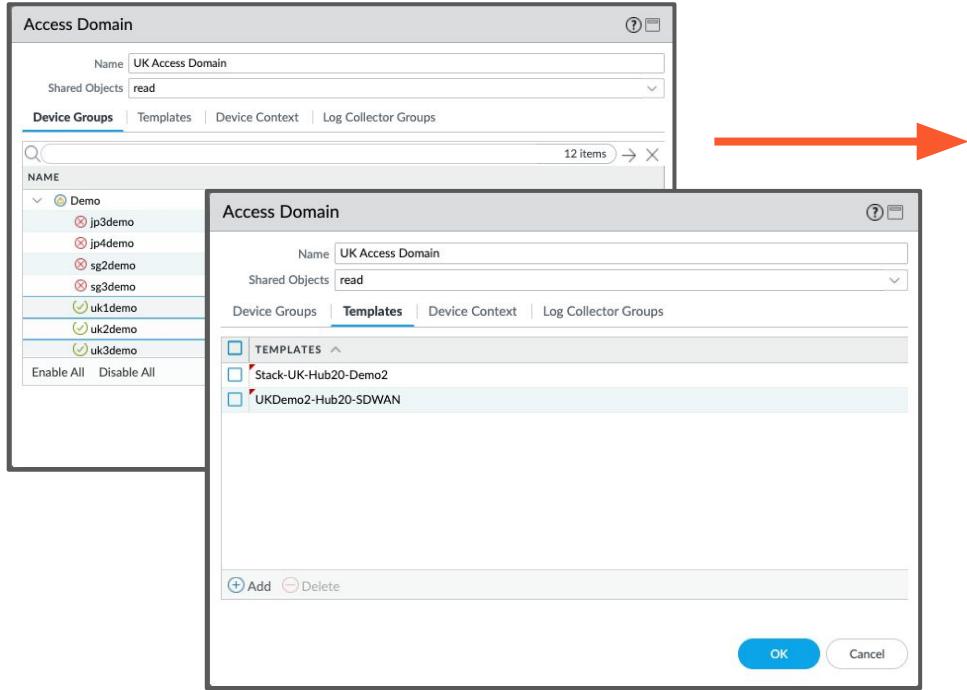
2.5.3 The Authentication Sequence

The screenshot shows the Palo Alto Networks PA-220 device configuration interface. The left sidebar contains a navigation tree with the following items:

- Setup
- High Availability
- Config Audit
- Password Profiles
- Administrators
- Admin Roles
- Authentication Profile
- Authentication Sequence** (selected)
- User Identification
- Data Redistribution
- Device Quarantine
- VM Information Sources
- Troubleshooting
- Certificate Management
 - Certificates
 - Certificate Profile
 - OCSP Responder
 - SSL/TLS Service Profile
 - SCEP
 - SSL Decryption Exclusion
 - SSH Service Profile
- Response Pages
- Log Settings
- Server Profiles
 - SNMP Trap
 - Syslog

The main content area displays the "Authentication Sequence" configuration dialog. The "NAME" field is set to "auth-sequence". Under "Authentication Sequence Settings", there is a checked checkbox labeled "Use domain to determine authentication profile". The "AUTHENTICATION PROFILES" section lists three profiles: "Idap" and "local-2" (which is currently selected). At the bottom of the dialog are buttons for "+ Add", "- Delete", "Move Up", "Move Down", "OK", and "Cancel".

2.5.4 The device access method - for Panorama Access Domains



2.5.4 Understand the Different Methods to Authenticate

The screenshot shows the PANORAMA interface with the following details:

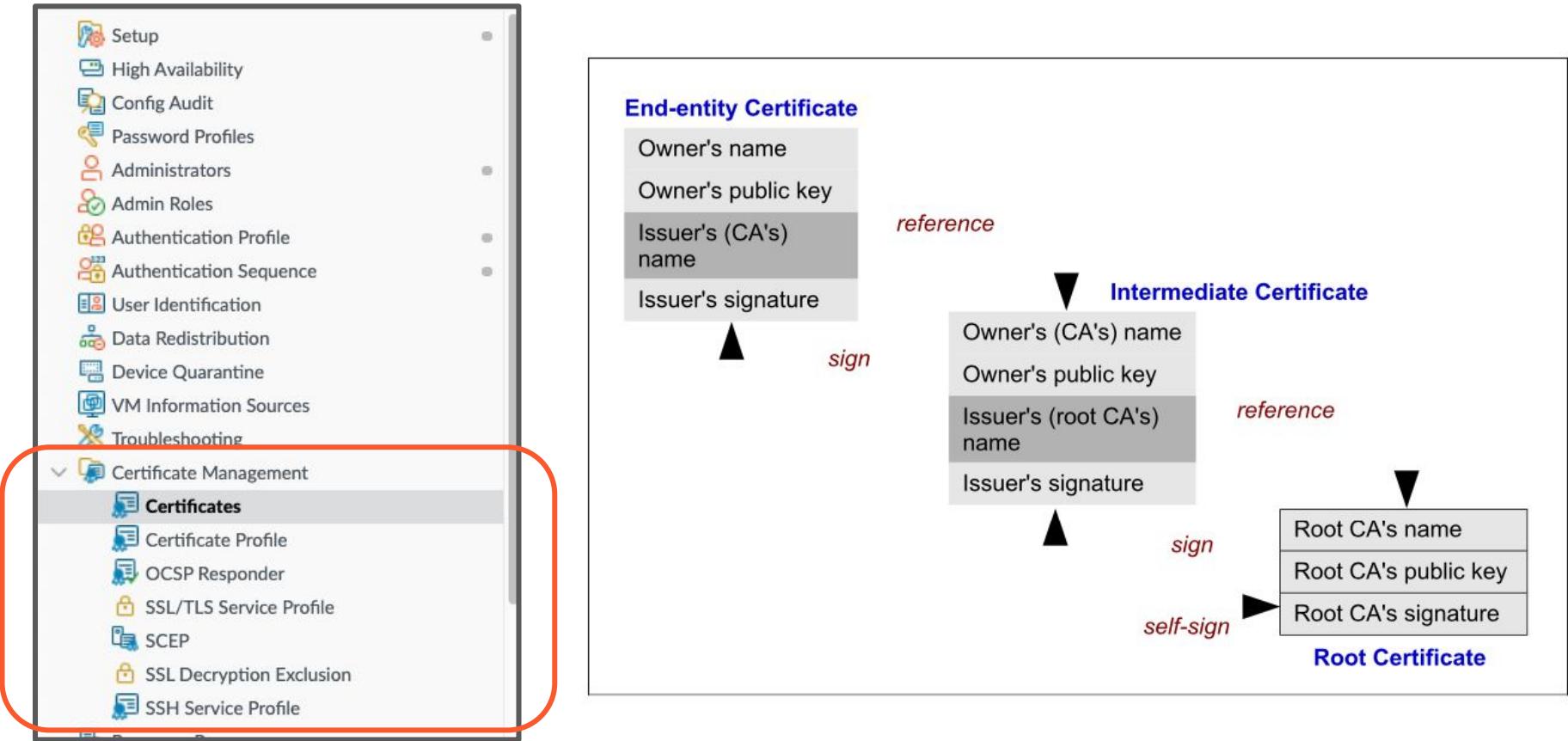
- Left Sidebar:** Shows navigation links including Setup, High Availability, Log Forwarding Card, Password Profiles, Administrators, Admin Roles, Access Domain, Authentication Profile, Authentication Sequence, and User Identification. The "Administrators" link is highlighted with a red box.
- Top Bar:** Includes tabs for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE (highlighted), and PANORAMA. It also shows the current template (vm300-internet), view by (Device), mode (Multi VSYS; Normal Mode; VPN Enabled), and a search bar.
- Main Content Area:** A table listing users. The columns are NAME, ROLE, AUTHENTICATI... PROFILE, PASSWORD PROFILE, CLIENT CERTIFICATE AUTHENTICATI... (WEB), PUBLIC KEY AUTHENTICATI..., and Administer/(View). The table shows three rows:
 - jared (Superuser, No Profile, No Certificate)
 - jaulsen (Superuser, plsn ldap, No Certificate)
 - jaredani (Custom role-, No Profile, No Certificate)
- Bottom Modal:** A "Local User" dialog box with fields for Profile Name (gptest), Location (Shared), Mode (Password selected), Password, Confirm Password, and Enable checkbox. Buttons for OK and Cancel are at the bottom.
- Right Sidebar:** Shows a list of authentication methods:
 - Server Profiles (SNMP Trap, Syslog, Email, HTTP, Netflow)
 - RADIUS
 - TACACS+
 - LDAP (highlighted with a red box)
 - Kerberos
 - SAML Identity Provider
 - DNS
 - Multi Factor Authentication

Annotations:

- Users vs. Administrators:** A callout pointing to the left sidebar.
- Local vs. External:** A callout pointing to the right sidebar.

2.6 Configure and manage certificates

2.6.1 Certificate Usage



2.6.2 Certificate Profiles

The screenshot shows the Palo Alto VM (PA-VM) interface. The top navigation bar includes links for Dashboard, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE, and a highlighted 'DEVICE' tab. A sidebar on the left lists various configuration categories such as Setup, High Availability, and Certificates. The main content area displays the 'Device Certificates' section under 'Default Trusted Certificate Authorities'. A modal window titled 'Generate Certificate' is open, containing fields for Certificate Type (Local selected), Certificate Name, Common Name, Signed By (with checkboxes for Certificate Authority and Block Private Key Export), Cryptographic Settings (Algorithm RSA, Number of Bits 2048, Digest sha256, Expiration May 31), and Certificate Attributes. At the bottom of the modal are 'Generate' and 'Cancel' buttons. Three numbered callouts point to specific elements: '1' points to the 'Signed By' dropdown; '2' points to the 'Certificate Attributes' table; and '3' points to the 'Generate' button.

1 Blank to designate the certificate as self-signed

2 Checkbox determines whether this certificate will have the rights to sign other certificates.

3

Generate Certificate

Certificate Type Local SCEP

Certificate Name

Common Name

Signed By External Authority (CSR)

Certificate Authority

Block Private Key Export

2.6.1 Certificate Usage

Import Certificate ?

Certificate Type Local SCEP

Certificate Name

Certificate File [Browse...](#)

File Format ▼

Private key resides on Hardware Security Module

Import Private Key

Block Private Key Export

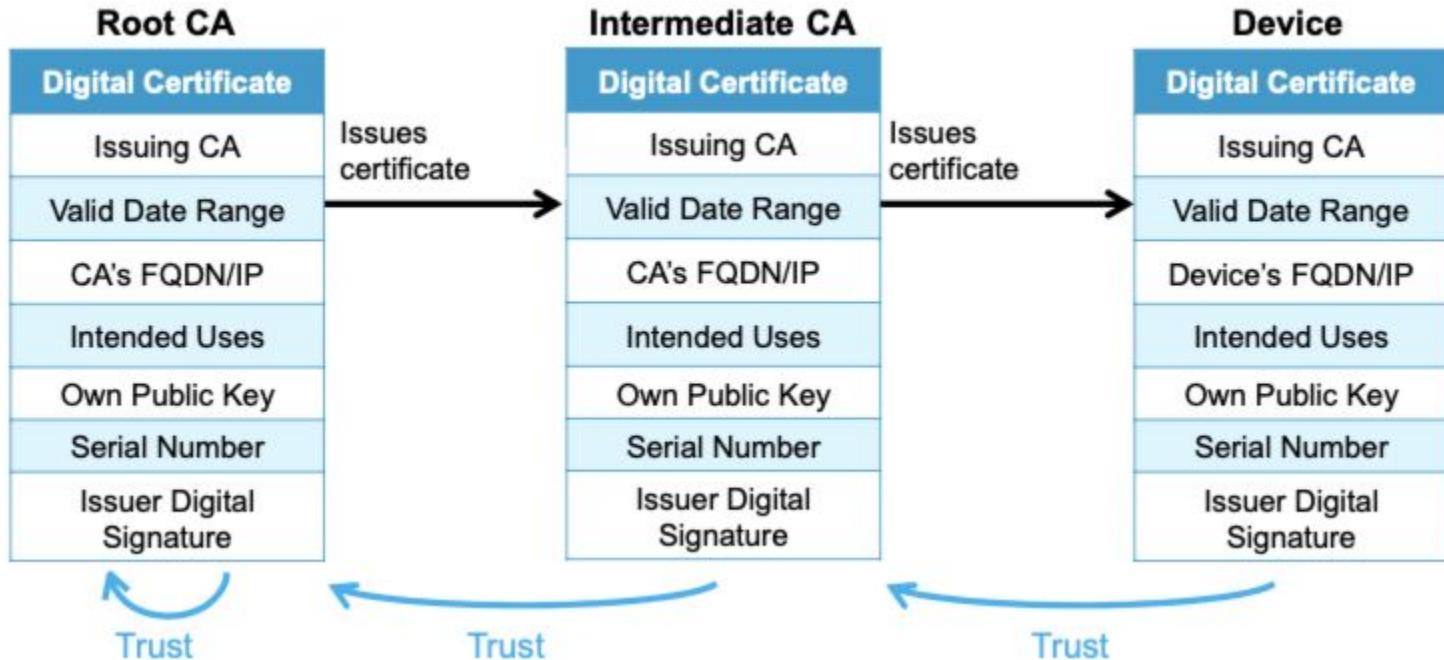
Key File [Browse...](#)

Passphrase

Confirm Passphrase

OK Cancel

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

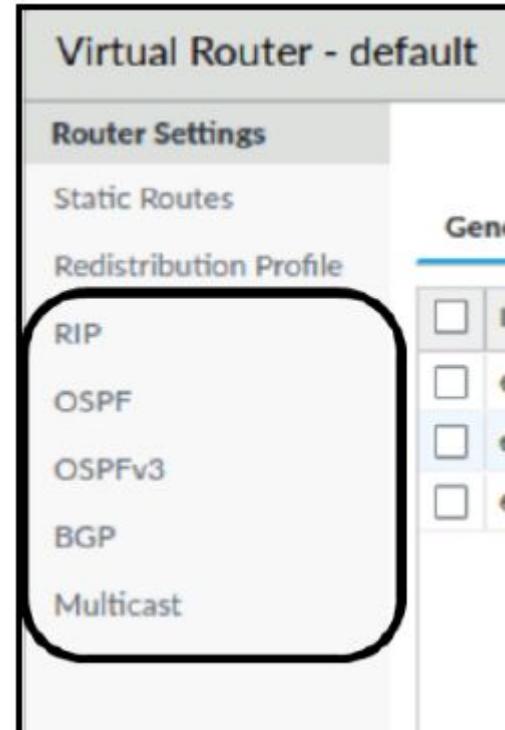
The screenshot shows the Palo Alto PA-220 interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, and NETWORK, with NETWORK being the active tab. On the left, a sidebar lists various network objects: Interfaces, Zones, VLANs, Virtual Wires, Virtual Routers (which is currently selected), and IPSec Tunnels. The main content area displays a table for managing Virtual Routers. The table has columns for NAME, INTERFACES, and CONFIGURATION. A row for 'default' is selected, indicated by a blue highlight. The 'CONFIGURATION' column for this row shows 'ECMP status: Disabled'. A search bar is located above the table.

NAME	INTERFACES	CONFIGURATION
default		ECMP status: Disabled

Configure Dynamic Routing

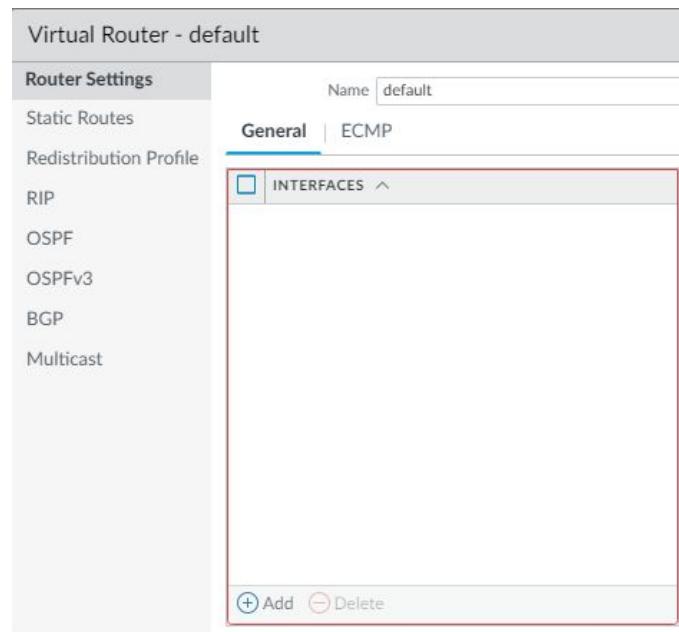
Router Types(PAN-OS 10.1)

- 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 Administrable 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



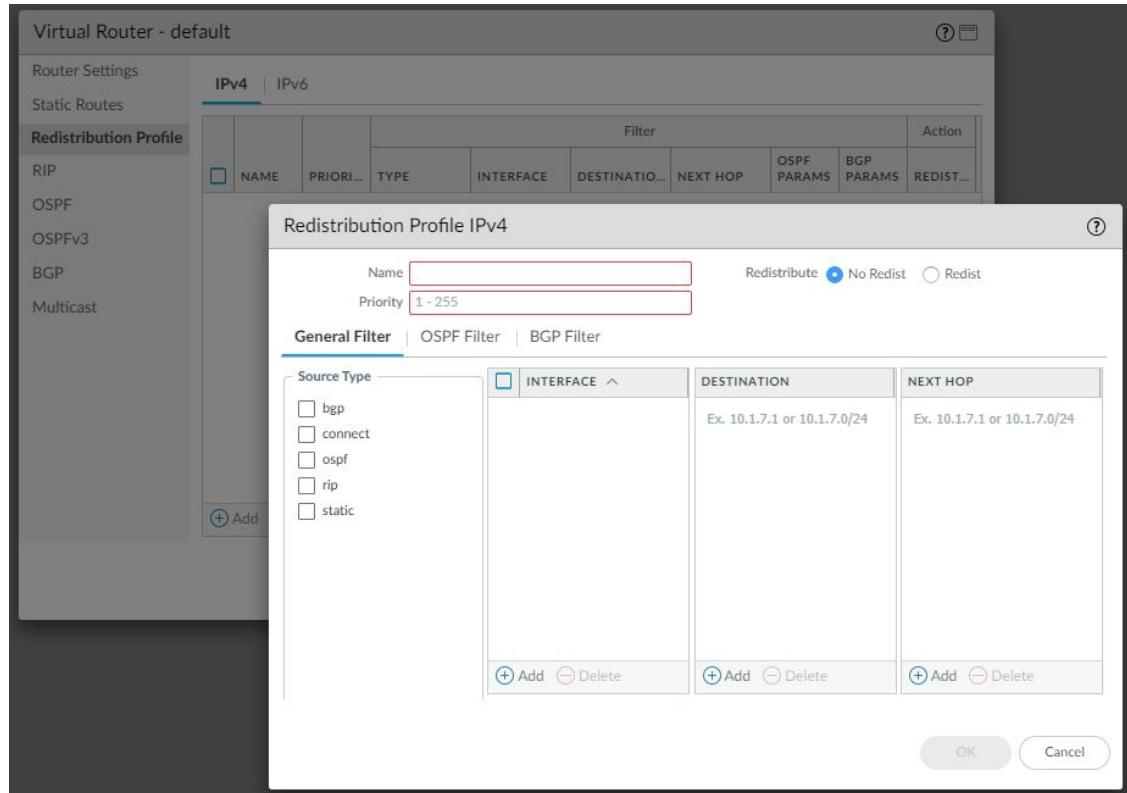
Configure Dynamic Routing

- 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

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

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 its 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

Virtual Router - Static Route - IPv4

Name	default
Destination	0.0.0.0/0
Interface	None
Next Hop	IP Address 10.0.0.254
Admin Distance	10 - 240
Metric	10
Route Table	Unicast

Path Monitoring

Failure Condition		<input checked="" type="radio"/> Any	<input type="radio"/> All	Preemptive Hold Time (min)	2	
	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT
<input type="checkbox"/>						
<input type="button"/> Add <input type="button"/> Delete						

OK Cancel

2.7.4 Route Monitoring

Virtual Router - Static Route - IPv4

Name	default1
Destination	0.0.0.0/0
Interface	None
Next Hop	IP Address
	10.0.0.254
Admin Distance	10 - 240
Metric	10
Route Table	Unicast

Path Monitoring

Failure Condition	<input checked="" type="radio"/> Any	<input type="radio"/> All				
Preemptive Hold Time (min)						
2						
	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT
<input type="checkbox"/>	monitor-1	<input checked="" type="checkbox"/>	10.0.0.1/24	8.8.8.8	3	5

Add Delete

OK Cancel

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

The screenshot shows the Palo Alto Networks UI for managing security policies. On the left, a sidebar lists categories: Security, NAT, QoS, Policy Based Forwarding (selected), Decryption, and Tunnel Inspection. The main area displays a table of policy-based forwarding rules. The table has columns for NAME, TAGS, ZONE/INTERFACE, ADDRESS, USER, ADDRESS, APPLICATION, SERVICE, ACTION, EGRESS I/F, and NEXT HOP. One rule is listed:

NAME	TAGS	Source			Destination		APPLICATION	SERVICE	ACTION	EGRESS I/F	NEXT HOP
		ZONE/INTERFACE	ADDRESS	USER	ADDRESS						
1 PBF	none	in	10.0.1.111/32	any	8.8.8.8/32	X	TCP-53		forward	ethernet1/8	172.31.67.254

This screenshot shows the 'Policy Based Forwarding Rule' configuration dialog with the 'Source' tab selected. The dialog is divided into several sections: General, Source, Destination/Application/Service, and Forwarding. The Source section contains fields for Type (set to Zone) and Zone (set to 'in'). It also includes source address and user selection dropdowns, each with an 'Any' option and a specific IP/Port entry ('10.0.1.111/32'). There are 'Add' and 'Delete' buttons for each row, and a 'Negate' checkbox at the bottom.

This screenshot shows the 'Policy Based Forwarding Rule' configuration dialog with the 'Forwarding' tab selected. The Forwarding section contains fields for Action (set to 'Forward'), Egress Interface (set to 'ethernet1/8'), and Next Hop (set to 'IP Address 172.31.67.254'). It also includes a 'Monitor' section with a 'Profile' dropdown and a checkbox for 'Disable this rule if nexthop/monitor ip is unreachable'. There is also an 'Enforce Symmetric Return' checkbox and a 'NEXT HOP ADDRESS LIST' input field.

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

Welcome
PAN-OS 10.2
“NEBULA”

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 Enabled/Reboot Required

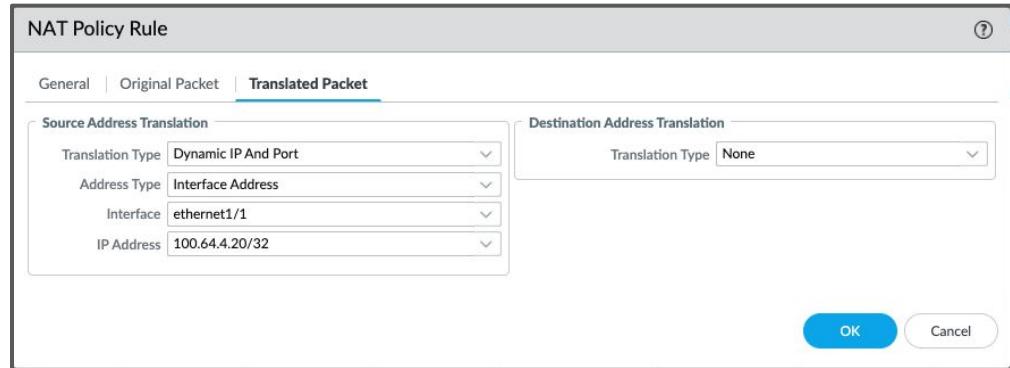
2.8 Configuring NAT

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.

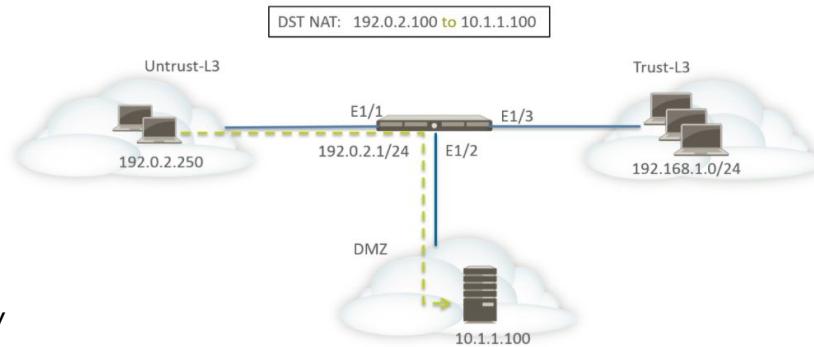


Slack Channel: Understanding_NAT-4.1-RevC.pdf

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

The screenshot shows the PA-VM interface with the following navigation bar:

DASHBOARD ACC MONITOR POLICIES

The left sidebar contains the following menu items:

- Setup
- High Availability
- Config Audit
- Administrators
- Admin Roles
- Authentication Profile
- Authentication Sequence
- User Identification
- Data Redistribution
- Device Quarantine
- VM Information Sources
- Troubleshooting** (selected)
- Certificate Management
 - Certificates
 - Certificate Profile
 - OCSP Responder
 - SSL/TLS Service Profile
 - SCEP

The main area displays the "Test Configuration" dialog for "NAT Policy Match". The dialog fields are:

- Select Test: NAT Policy Match
- From: None
- To: None
- Source: (red box)
- Destination: (red box)
- Source Port: [1 - 65535]
- Destination Port: [1 - 65535] (red box)
- Protocol: TCP
- To Interface: None
- Ha Device ID: [0 - 1]

At the bottom are "Execute" and "Reset" buttons.

The screenshot shows the "NAT Policy Rule" configuration dialog with the "Translated Packet" tab selected. The tabs include General, Original Packet, and Translated Packet. The "Translated Packet" tab has two sections: Source Address Translation and Destination Address Translation, both set to "None". At the bottom are "OK" and "Cancel" buttons.

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

The screenshot shows the PA-VM interface with the 'MONITOR' tab selected. The left sidebar contains a tree view of monitoring modules: Logs (Traffic, Threat, URL Filtering, WildFire Submissions, Data Filtering, HIP Match, GlobalProtect, IP-Tag, User-ID, Decryption, Tunnel Inspection, Configuration, System, Alarms, Authentication, Unified, Packet Capture), App Scope (Summary, Change Monitor, Threat Monitor, Threat Map, Network Monitor, Traffic Map), and Session Browser (Botnet). The 'Session Browser' module is highlighted.

The main area displays two network flows in a table:

Flow	Session ID	Source	Destination	Protocol	From Port	To Port	Application	Rule	Ingress I/F	Egress I/F	Bytes	Virtual System	Action
Flow 1	159835	10.154.12.89	74.217.1.83	6	3763	80	hotmail	Allowed Personal Apps	ethernet1/4	ethernet1/4	10733	vsys1	Edit
Flow 2	159835	10.154.12.89	74.217.1.83	6	50052	80	web-browsing	Unknown User SSL and Web	ethernet1/4	ethernet1/4	2052	vsys1	Edit

Below the table, detailed information is provided for each flow:

Flow 1:

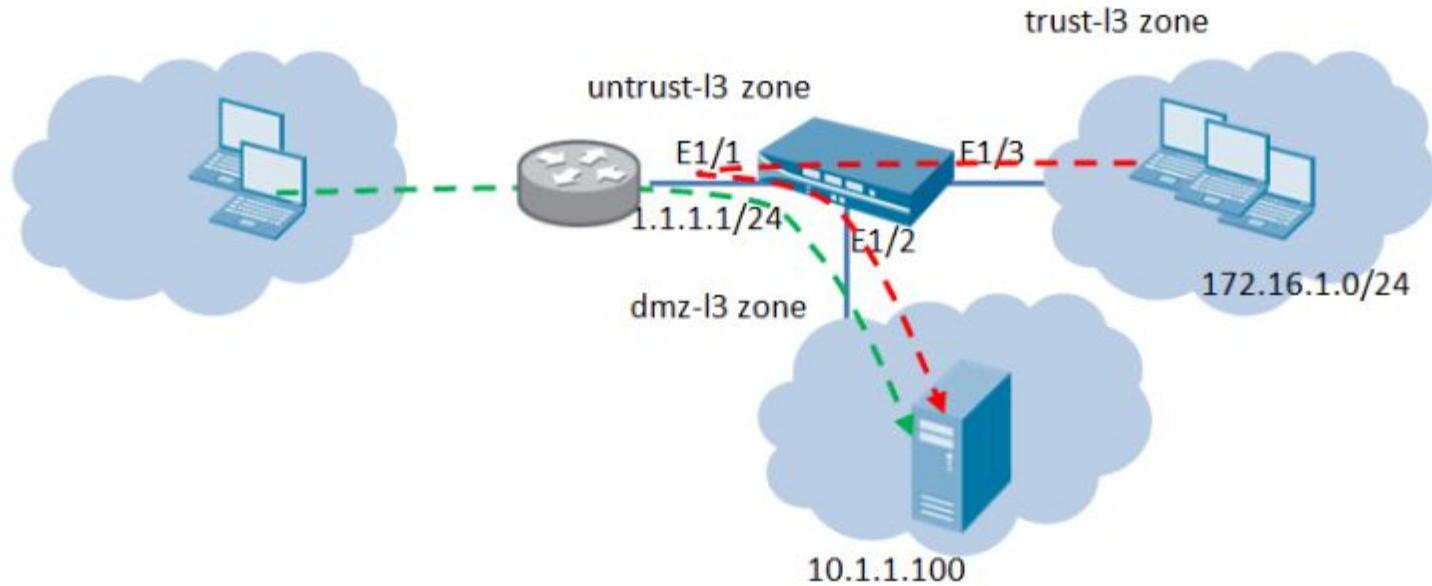
Session ID	159835
Timeout	7
Time To Live	6
Virtual System	vsys1
Application	web-browsing
Protocol	6
Security Rule	Unknown User SSL and Web
URL Category	license-expired
QoS Rule	N/A
QoS Class	4
Created By Syn Cookie	False
To Host Session	False
Traverse Tunnel	False
Captive Portal	False
Session End Log	True
Session In Ager	True
Session From HA	False
End Reason	tcp-rst-from-server
Tracker Stage Firewall	TCP RST - server

Flow 2:

Session ID	159835
Timeout	7
Time To Live	6
Virtual System	vsys1
Application	web-browsing
Protocol	6
Security Rule	Unknown User SSL and Web
URL Category	license-expired
QoS Rule	N/A
QoS Class	4
Created By Syn Cookie	False
To Host Session	False
Traverse Tunnel	False
Captive Portal	False
Session End Log	True
Session In Ager	True
Session From HA	False
End Reason	tcp-rst-from-server
Tracker Stage Firewall	TCP RST - server

2.8.6 U-Turn NAT

Slack Channel: Understanding_NAT-4.1-RevC.pdf



2.8.7 Check HIT Counts

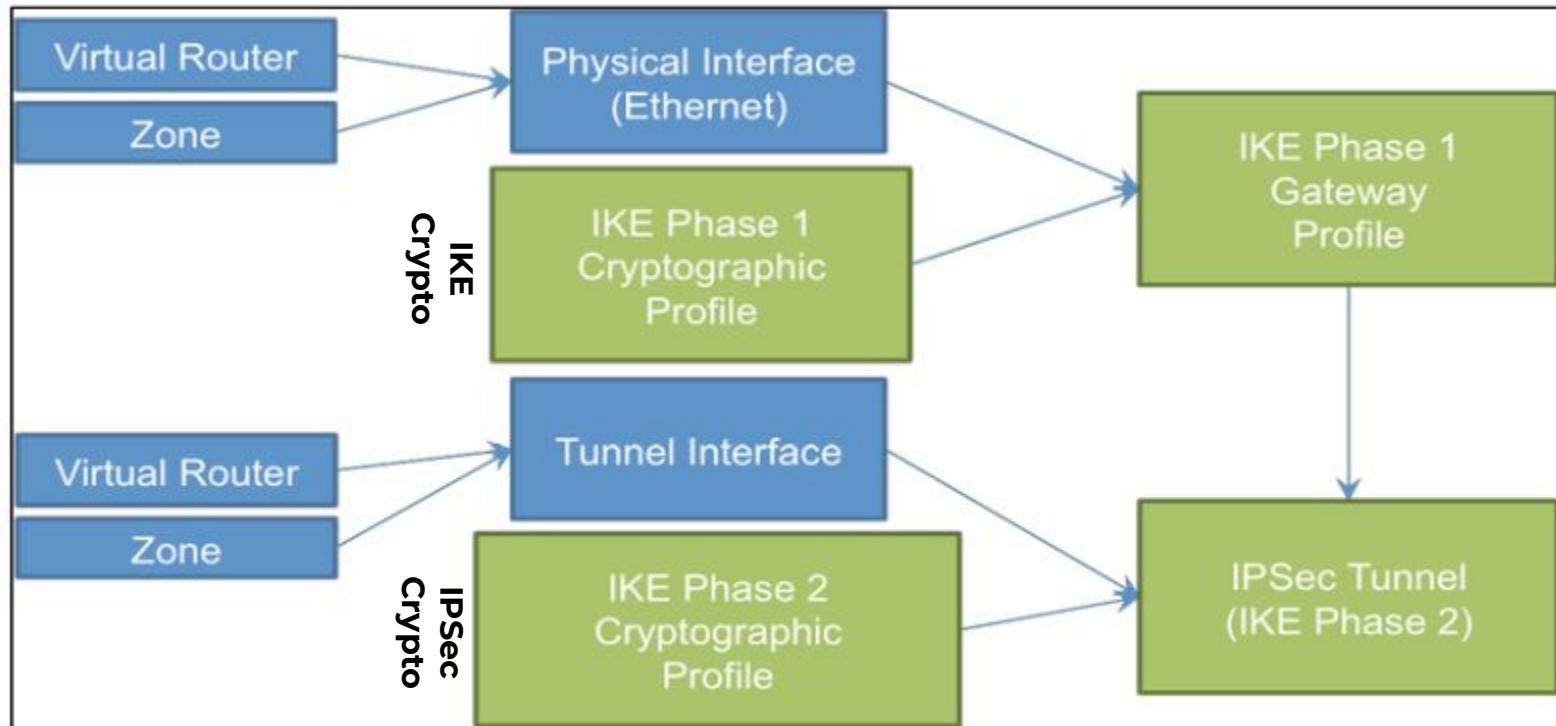
Use Fuel Virtual Lab & PCNSE Study Guide Section - Make this Section a Lab

The screenshot shows the Palo Alto Networks Policy Manager interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES (which is highlighted in yellow), OBJECTS, NETWORK, and DEVICE. On the right side of the header are buttons for Commit, Undo, Redo, and Search. The main content area has a sidebar on the left with sections for Security (NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, SD-WAN) and Policy Optimizer (New App Viewer, Rules Without App Controls, Unused Apps, Log Forwarding for Security Services). The main table is titled "Rule Usage" and displays 74 items. The columns are: CATEGORY, ACTION, PROFILE, OPTIONS, HIT COUNT, LAST HIT, FIRST HIT, APPS SEEN, MODIFIED, and CREATED. The data in the table includes various rule configurations such as Allow and Drop actions, different profiles, and varying hit counts (e.g., 0, 11616, 2197439, 8254, 2088, 269886, 634, 3144, 4564). The last few rows under Policy Optimizer show rules for New App Viewer, Rules Without App Controls, Unused Apps, and Log Forwarding for Security Services.

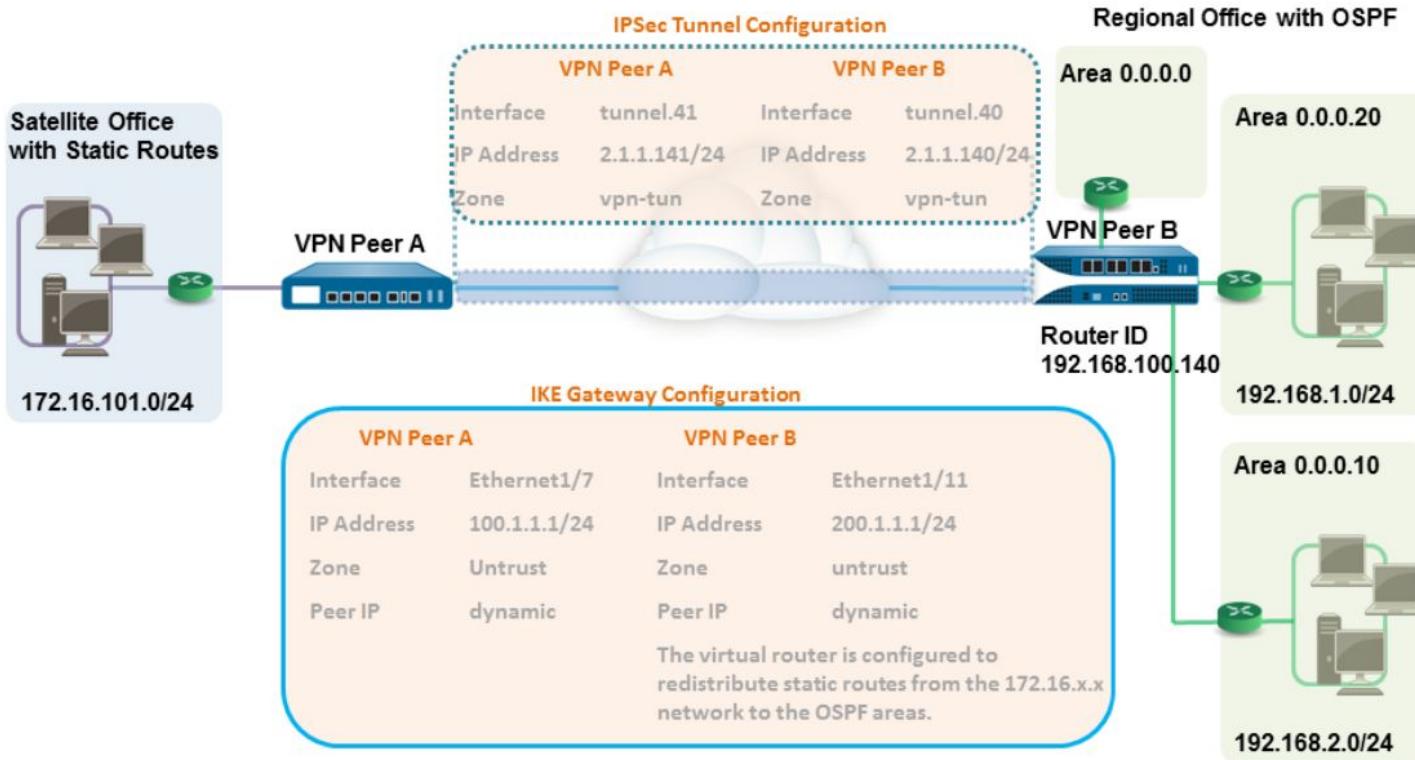
CATEGORY	ACTION	PROFILE	OPTIONS	Rule Usage				MODIFIED	CREATED	
				HIT COUNT	LAST HIT	FIRST HIT	APPS SEEN			
Security	Allow	Locked	Table	0	-	-	21	2022-08-30 14:14:20	2022-11-02 16:24:56	
	Allow	Shielded	Table	0	-	-	-	2022-08-30 14:14:20	2022-06-10 00:29:32	
	Allow	Shielded	Table	11616	2022-09-18 01:26:46	2022-08-10 01:12:46	1	2022-08-30 14:14:20	2022-10-22 11:54:52	
	Allow	Shielded	Table	2197439	2022-09-21 18:35:44	2022-07-28 14:24:50	28	2022-08-30 14:14:20	2022-06-10 00:29:32	
	Drop	none	Table	0	-	-	-	2022-08-30 14:14:20	2022-06-10 00:29:32	
	Allow	Shielded	Table	8254	2022-09-21 16:25:13	2022-07-28 16:25:12	2	2022-08-30 14:14:20	2020-10-22 11:54:52	
	Allow	Shielded	Table	2088	2022-09-21 16:25:10	2022-07-28 16:25:08	1	2022-08-30 14:14:20	2020-10-22 11:54:52	
		Allow	Shielded	Table	269886	2022-09-21 16:25:11	2022-07-28 16:25:09	3	2022-08-30 14:14:20	2020-10-22 11:54:52
	Policy Optimizer	Allow	Shielded	Table	634	2022-09-21 16:25:10	2022-07-28 16:25:08	1	2022-08-30 14:14:20	2020-10-22 11:54:52
		Allow	Shielded	Table	3144	2022-09-21 16:25:11	2022-07-28 16:25:09	1	2022-08-30 14:14:20	2020-10-22 11:54:52
Allow		none	Table	4564	2022-09-21 16:30:35	2022-07-28 16:30:33	1	2022-08-30 14:14:20	2022-06-10 00:29:32	

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
```

Monitor Profile

Name: **vpn_monitor**

Action: Wait Recover Fail Over

Interval (sec): **3**

Threshold: **5**

OK **Cancel**

IPSec Tunnel

General | Proxy IDs

Name: **vpn_tunnel**

Tunnel Interface: **tunnel.201**

Type: Auto Key Manual Key GlobalProtect Satellite

Address Type: IPv4 IPv6

IKE Gateway: **gw_0101_007058000139887_0101**

IPSec Crypto Profile: **default**

Show Advanced Options
Enable Replay Protection
 Copy ToS Header
 Add GRE Encapsulation

Anti Replay Window: **1024**

Tunnel Monitor

Destination IP: **1.1.1.1**
Profile: **vpn_monitor**

Comment: _____

OK **Cancel**

2.9.4 IPSEC Tunnel Testing

IKE Phase 1

test vpn ike-sa gateway <gateway_name>
show vpn ike-sa gateway <gateway_name>

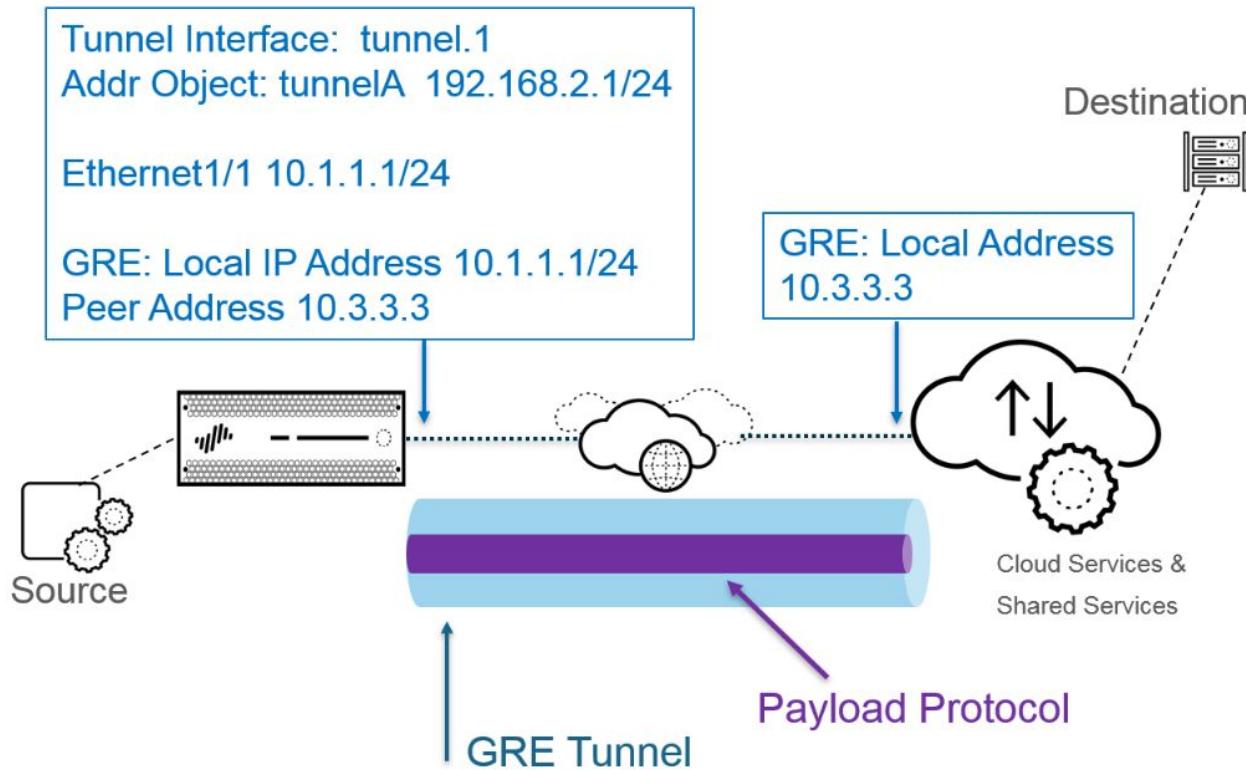
IKE Phase 2

test vpn ike-sa tunnel <tunnel_name>
show vpn ike-sa tunnel <tunnel_name>

To See IPSEC Tunnel Flow

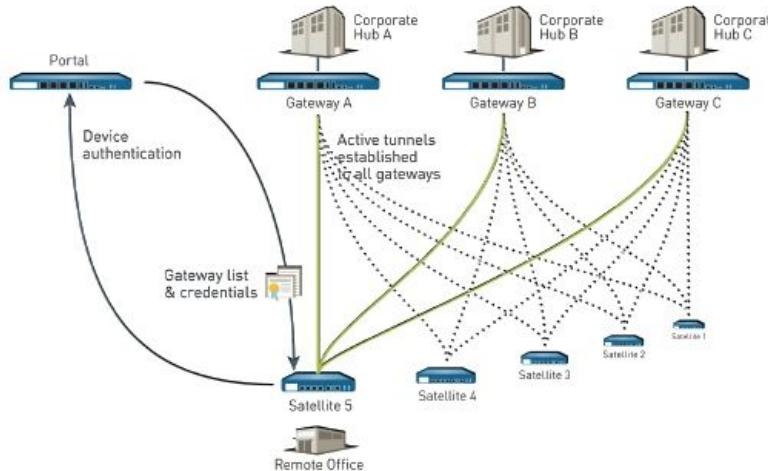
show vpn flow

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 LVPN 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=kA10g000000PLTICAO>

Tips & Tricks: Why Use a VPN Proxy ID?

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIUFCA0>

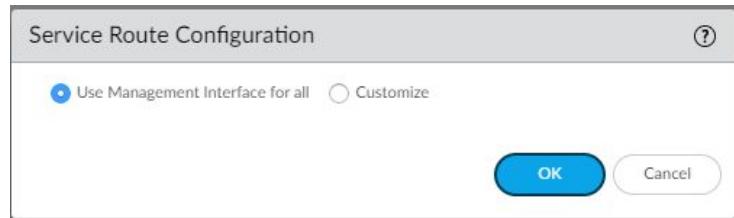
How to Build an IPsec Tunnel Between a Palo Alto Networks Firewall and a Cisco ASA (Adaptive Security Appliance)

<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



The screenshot shows the PA-220 management interface with the "Services" tab selected. In the "Services" section, the "Update Server" is set to "updates.paloaltonetworks.com". Under "DNS Servers", "Primary DNS Server" is listed as "8.8.8.8". "Proxy Server" is configured with "Primary NTP Server Address" as "pool.ntp.org". In the "Services Features" section, the "Service Route Configuration" option is highlighted with a red box.

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

Service Route Configuration

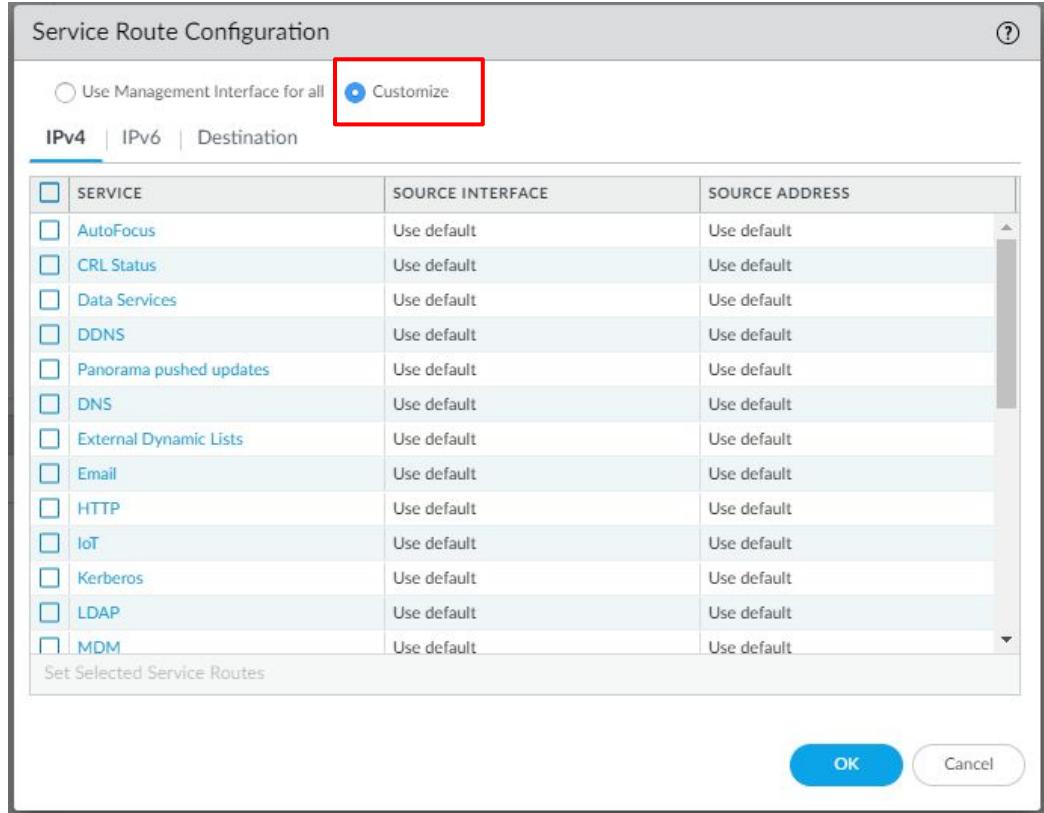
Use Management Interface for all Customize

IPv4 | IPv6 | Destination

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

Set Selected Service Routes

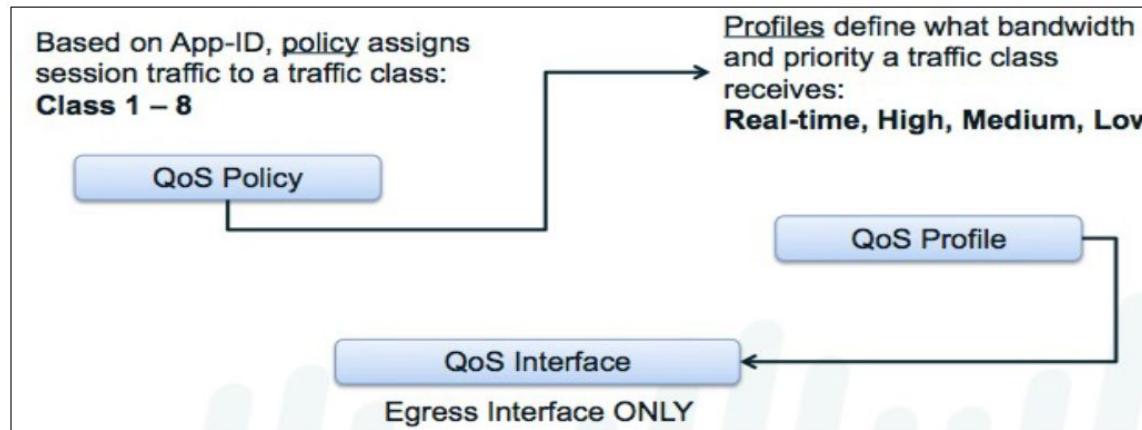
OK Cancel



2.11 Configure Application-Based QoS

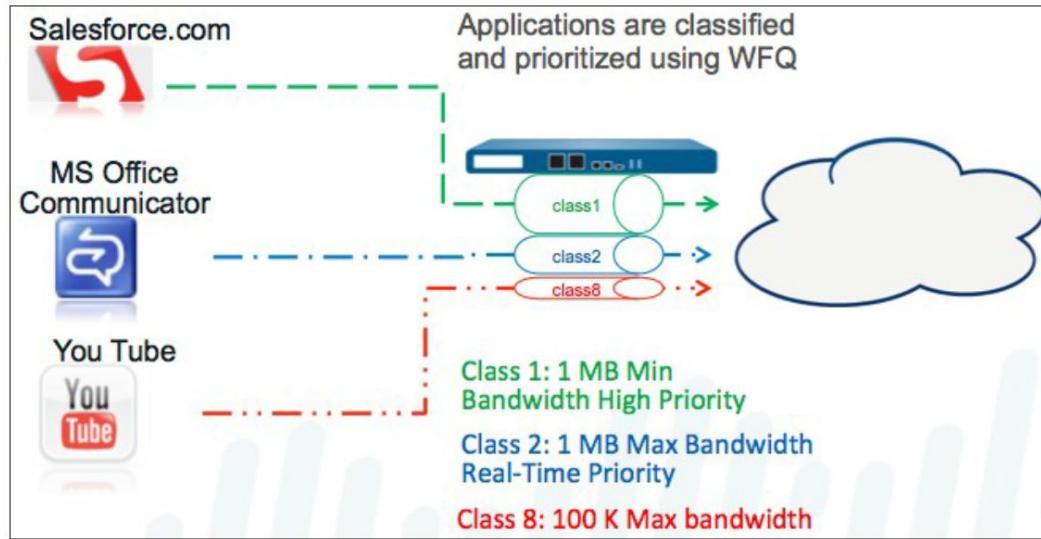
2.11.1 Select/Identify the Application

- 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

The screenshot shows the QoS Profile configuration table. The left sidebar lists various network profiles, with 'QoS Profile' selected. The main area displays a table with columns: Class, Min Rate (Mbps), Max Rate (Mbps), and Priority.

Class	Min Rate (Mbps)	Max Rate (Mbps)	Priority
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