Palo Alto Networks CNSE 4.1 Exam Preparation Guide

Palo Alto Networks Education

V.3

paloalto NETWORKS

Additional Study Documents and White Papers

There is a companion pack of support documents that are to be distributed with this CNSE 4.1 Exam Preparation Guide. References to these related documents will be made in red text throughout this guide.

The document pack in entitled “Palo Alto Networks CNSE Tech Notes 2012”; it can be obtained from the same source as this CNSE study guide.

General Advice

- 100 multiple-choice/multiple select questions in 2.5 hours. You can go back to previous questions, to change your answer if necessary.
- Passing score is 60%
- You need to have been working with the PA firewalls in order to get a respectable score on the test. Make sure you have completed at least one tap-mode install (see this doc for steps):
  Tech Note - PAN tap mode install.pdf
  and one Layer3 install with NAT:
  Tech Note - PAN_L3-Config guide.pdf
- When a how-to doc is listed here, it is highly recommended that you not only read that doc, but actually *go through the steps and perform the setup in that doc* (using PAN-OS 4.1 of course)
- Additional reference documents include the 4.1 Admin Guide:
  4.1_admin_guide (_beta).pdf
- and the CLI guide:
  PAN-OS_4.1_CLI_Reference_Guide.pdf

Major Exam Topics

- Administration & Management
  - Device configuration, commit workflow
- Network Architecture:
  - NAT, Packet Flow, SP3
- Security Policies/Profiles
  - WildFire, URL-Filtering, DLP
- User-ID
  - User-ID Agent, Captive Portal
- IPsec VPN
  - Configuring route-based site-to-site connectivity
- SSL Decryption
  - Inbound and outbound, SSHv2, certificates
- High Availability:
  - Active/Passive, Active/Active
- Troubleshooting
  - Connectivity, Panorama, NAT, VPN
- GlobalProtect
  - SSL VPN, Certificates, HIP Profiles, HIP matches
- Panorama
  - configuration management, commit workflow, pre and post policy, device groups, shared objects and device group objects

PA appliances as of PAN-OS 4.1: 4000, 2000, 500 Series

PA-4060

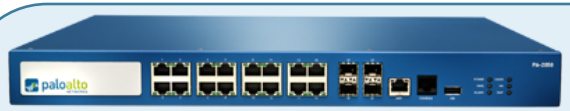
- 10 Gbps FW
- 5 Gbps threat prevention
- 2,000,000 sessions
- 4 XFP (10 Gig) I/O
- 4 SFP (1 Gig) I/O

PA-4050

- 10 Gbps FW
- 5 Gbps threat prevention
- 2,000,000 sessions
- 16 copper gigabit
- 8 SFP interfaces

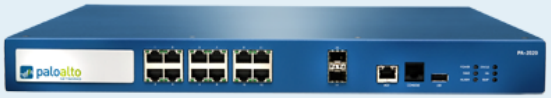
PA-4020

- 2 Gbps FW
- 2 Gbps threat prevention
- 500,000 sessions
- 16 copper gigabit
- 8 SFP interfaces



PA-2050

- 1 Gbps FW
- 500 Mbps threat prevention
- 250,000 sessions
- 16 copper gigabit
- 4 SFP interfaces



PA-2020

- 500 Mbps FW
- 200 Mbps threat prevention
- 125,000 sessions
- 12 copper gigabit
- 2 SFP interfaces

PA-500

- 250 Mbps FW
- 100 Mbps threat prevention
- 50,000 sessions
- 8 copper gigabit

paloalto NETWORKS

PA appliances as of PAN-OS 4.1: PA-5000 Series

PA-5060

- 20 Gbps FW
- 10 Gbps threat prevention
- 4 Gbps IPSec VPN
- 20,000 SSL VPN Users
- 4,000,000 sessions
- Up to 225 VSYS

(4) SFP+ (10 Gig) I/O

- (8) SFP (1 Gig) I/O
- (12) 10/100/1000

PA-5050

- 10 Gbps FW
- 5 Gbps threat prevention
- 4 Gbps IPSec VPN

10,000 SSL VPN Users

- 2,000,000 sessions
- Up to 125 VSYS
- (4) SFP+ (10 Gig) I/O
- (8) SFP (1 Gig) I/O
- (12) 10/100/1000

PA-5020

- 5 Gbps FW
- 2 Gbps threat prevention
- 2 Gbps IPSec VPN

5,000 SSL VPN Users

- 1,000,000 sessions
- Up to 20 VSYS
- (8) SFP (1 Gig) I/O
- (12) 10/100/1000

- Hot swappable fans, power supplies
- Dual, solid state hard drives
- Dedicated HA and management interfaces
- 2U standard rack mount form factor

PA Appliances as of PAN-OS 4.1: 200 Series

- 100 Mbps firewall throughput (App-ID enabled[1])
- 50 Mbps threat prevention throughput
- 50 Mbps IPsec VPN throughput
- 64,000 max sessions
- 1,000 new sessions per second
- 25 IPsec VPN tunnels/tunnel interfaces
- 25 SSL VPN Users
- 3 virtual routers
- 10 security zones
- 250 max number of policies

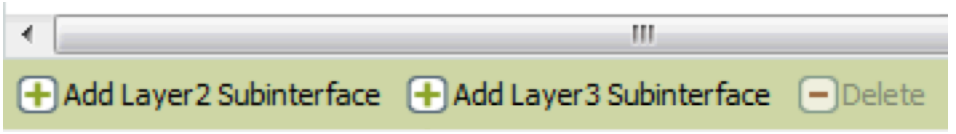
Five Physical Interface Types:

1. Tap mode interfaces simply listen to a span/mirror port of a switch
2. Virtual wire
   - EXACTLY two interfaces, what comes in one, goes out the other
   - Can be any combo (copper-copper, fiber-fiber, copper-fiber)
   - no MAC address or IP addresses on the interfaces
   - the device is still a stateful firewall and can block traffic
3. L2
   - multiple interfaces can be configured into a “virtual-switch” or VLAN in L2 mode. L2 Interfaces do not participate in STP, as Spanning Tree Protocol is not supported
4. L3
   - IP address is required, all layer-3 operations available.
5. HA (on all devices except the 4000 and 5000 series, you must configure two traffic ports as the HA ports)

Note that all interfaces, regardless of type, can be simultaneously supported.

Logical Interfaces Supported

- Subinterfaces (802.1q)
  - Up to 4094 VLAN supported per port
  - Max of 4094 VLANs per system
- Aggregate interfaces (802.3ad)
  - Only on PA-4000 and PA-5000 series
  - Up to 8 physical 1 Gig interfaces can be placed into an aggregate group
  - Up to 8 aggregate groups are supported per device
  - Each interface in a group must be the same physical media (all copper, or all fiber)
- Tunnel interfaces- for IPSec or SSL VPNs
- Loopback interfaces



Multicast Support

- Support for Multicast Filtering
  - available in Virtual Wire and L3
  - multicast IP addresses can now be used in firewall rules used with Virtual Wires and L3

- Multicast routing is supported in PAN-OS 4.1 for PIM-SM sparse mode and IGMP protocols.
- Additional information can be found in the following support document: PaloAltoNetworks_DesignGuide_RevA.pdf

Available Features in Different Interface Modes

Vwire

- No VPN
- No "auto" setting for HA passive link

L2

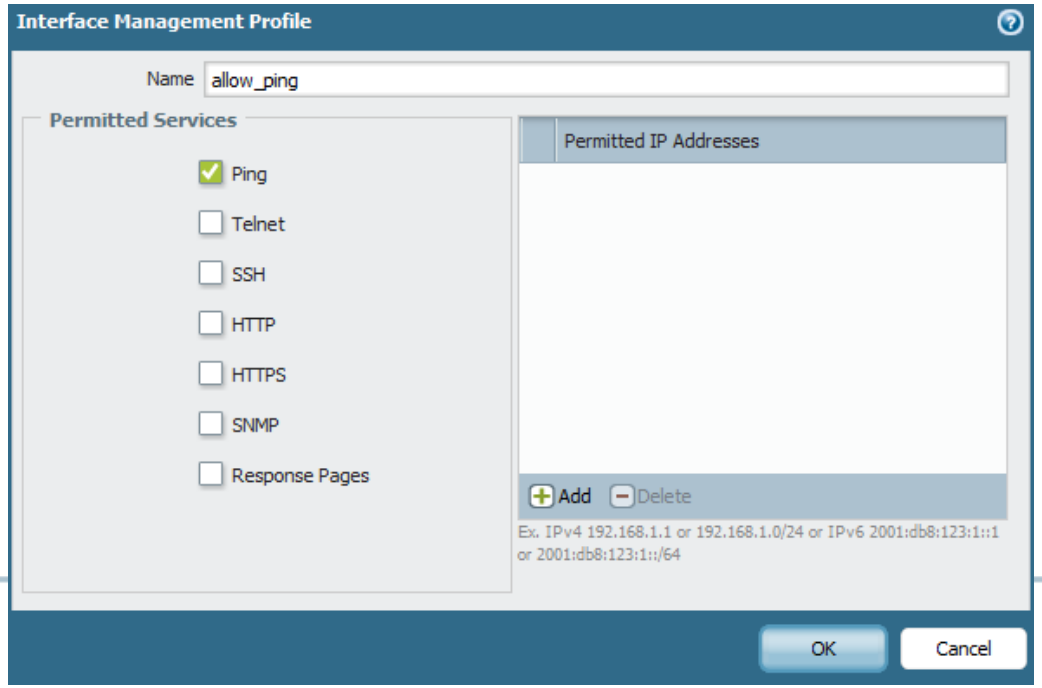
- No VPN
- No NAT (FYI in PAN-OS 4.1 you can do NAT in Vwire mode)
- No "auto" setting for HA passive link
- If IPv6 is passing, security policies can be written for this traffic
- No Multicast support

L3

- If IPv6 is passing, security policies can be written for this traffic

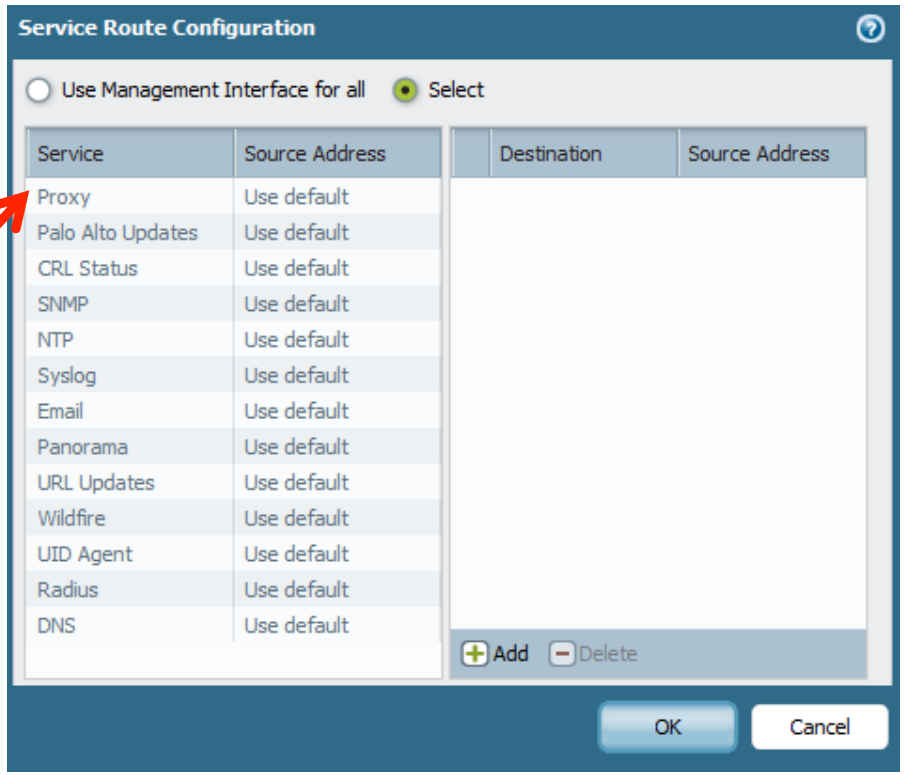
Interface Management

- An interface management profile specifies which protocols can be used to manage the firewall.
- Management profile can be assigned to:
  - L3 interfaces
  - Loopback interfaces
  - VLAN interfaces
- Configured under Network tab -> Network Profiles ->Interface Management



Device Management

- Managing the firewall (via GUI, SSH, etc.) is performed via the MGT interface on the PAN by default.
- You can specify different physical interfaces to use for specific management services via Device tab -> Setup -> Service Route Configuration.

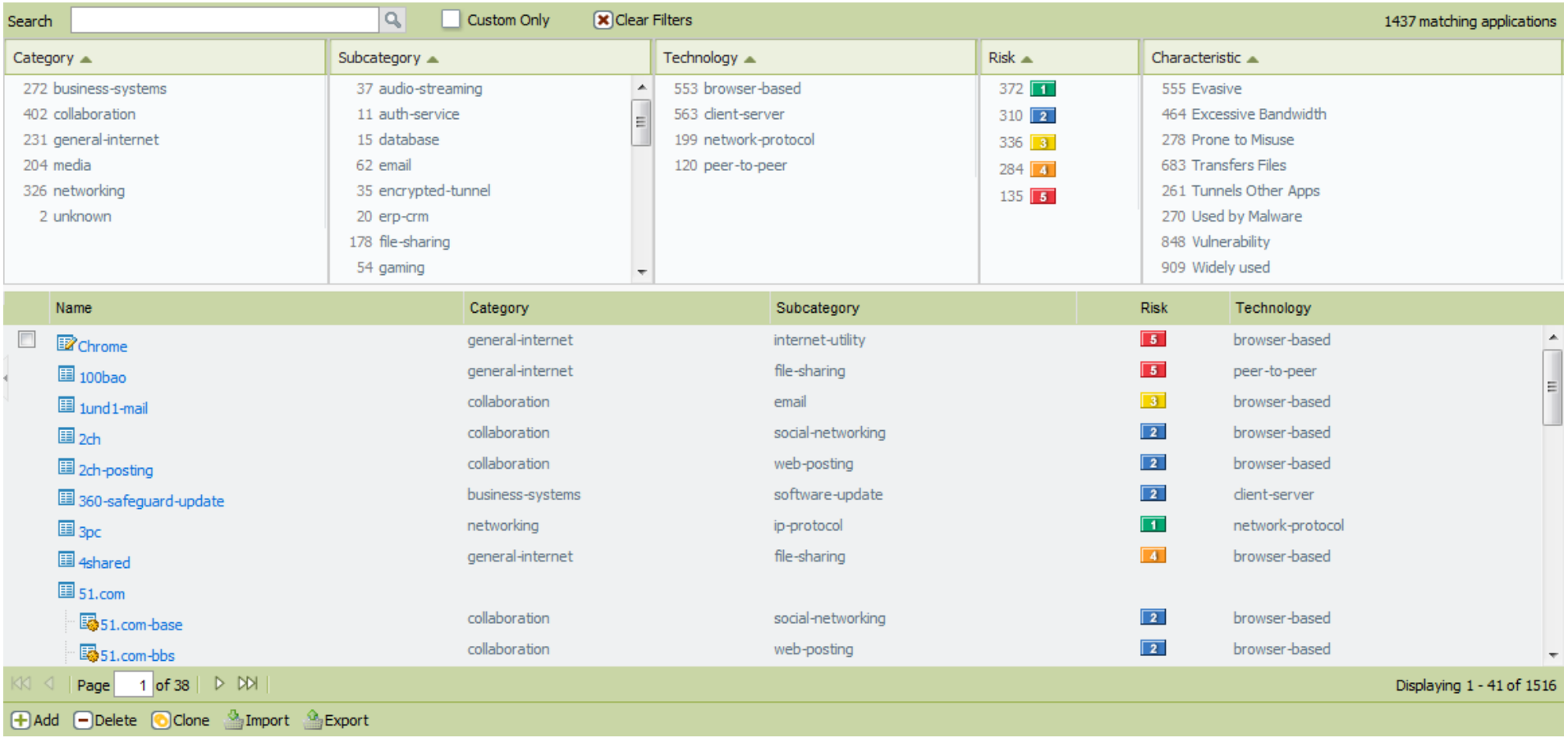


Application Identification

- App-ID provides the ability to identify applications and application functions. App-ID is a core function of the Palo Alto Networks device.
- App-ID uses various methods to determine what exactly is running in the session:
  - Protocol decoders
  - Protocol decryption
  - Application signatures
  - Heuristics are used when the above methods can not identify the application. This is the method by which applications such as the proprietarily-encrypted BitTorrent and UltraSurf are identified
- App-ID even works in these scenarios:
  - If the application is running on a different port than expected
  - If the application is being transmitted in an SSL tunnel (the firewall can forward proxy the SSL connection) or if it employs SSHv2
  - If the application is going through an HTTP proxy

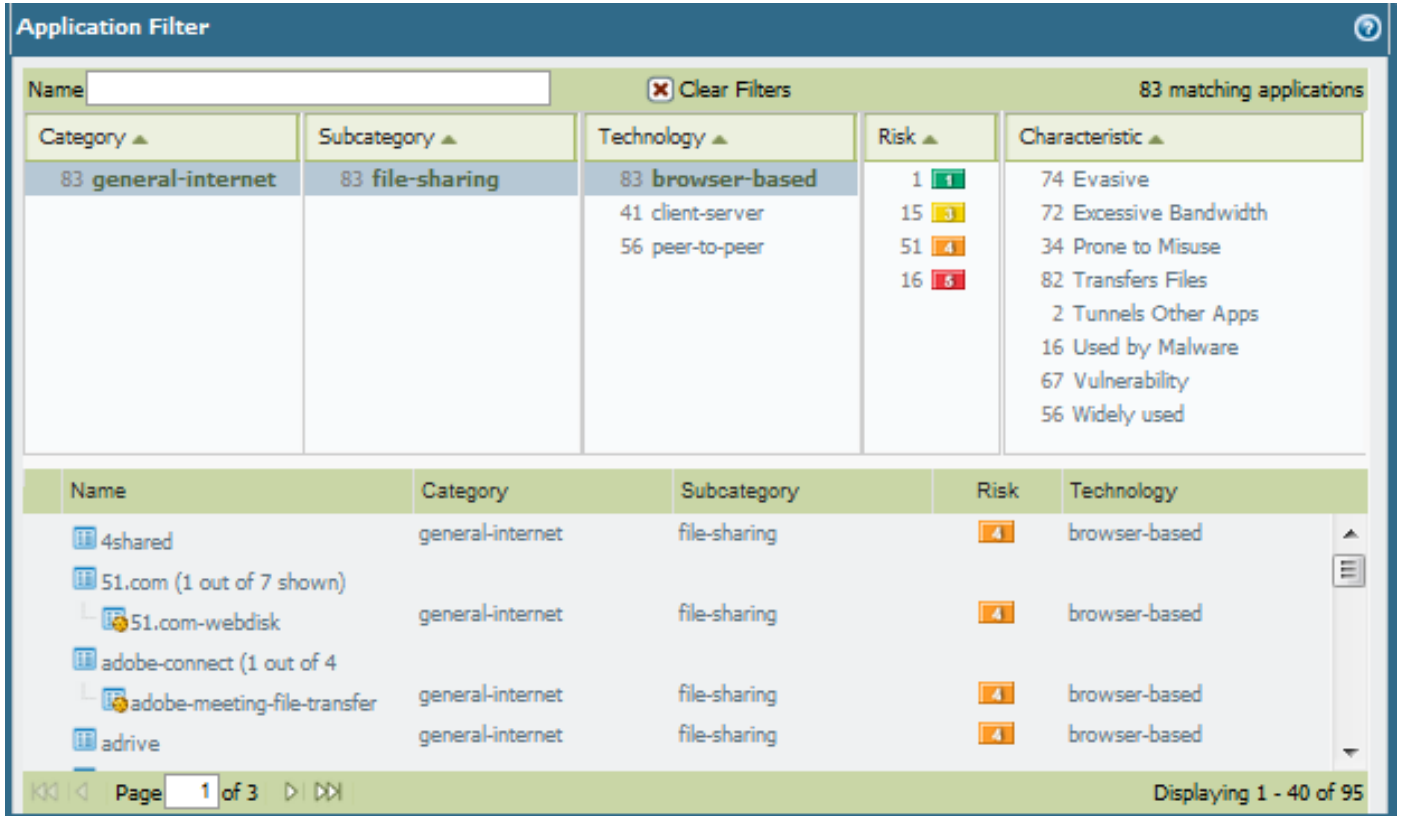
Application Selection Window

Within each policy, you can specify what applications you want to control. You can specify individual applications, or groups of applications. Some applications, such AIM instant messenger and Facebook, give you control over specific functions. Applications with Application Function Control are represented hierarchically.



Dynamic Application Filters

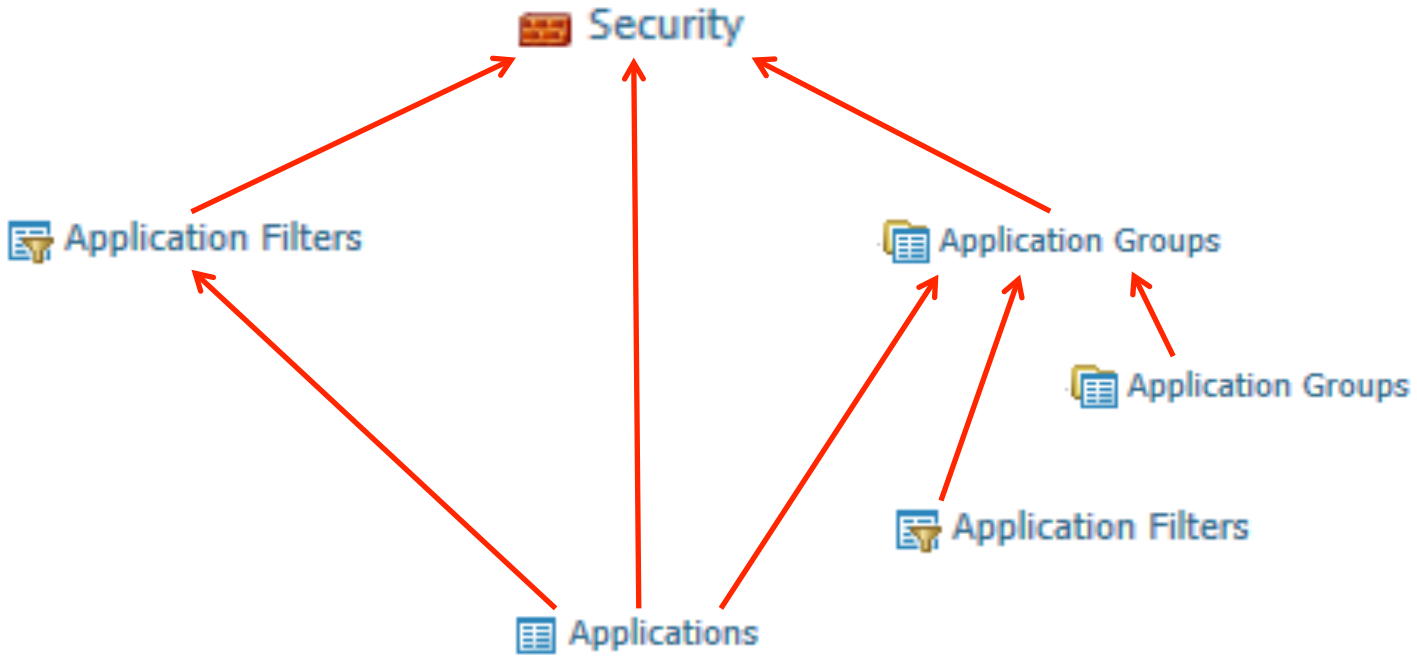
- A dynamic application filter is configured by specifying particular criteria.
- The example below is a dynamic filter of all browser-based file-sharing apps.



- Advantage of dynamic application filters: any new applications that fit into those categories will automatically be added to that dynamic filter.

Application Groups and Application Filters

- Applications Groups are static. Applications are manually added and maintained by firewall administrators.
- Applications Filters are dynamic. Applications are filtered by traits such as risk, subcategory, technology, characteristic, etc.
- If you create an Application Filter on a specific criteria, such as the subcategory of games', it will include all applications which are defined as a game. Any new games defined by an APP-ID signature will automatically be included as part of this filter.



Security Policy Operation

- All traffic flowing from one security zone to another security zone requires a policy to allow the traffic
- The policy list is evaluated from the top down
- The first rule that matches the traffic is used
- No further rules are evaluated after the match

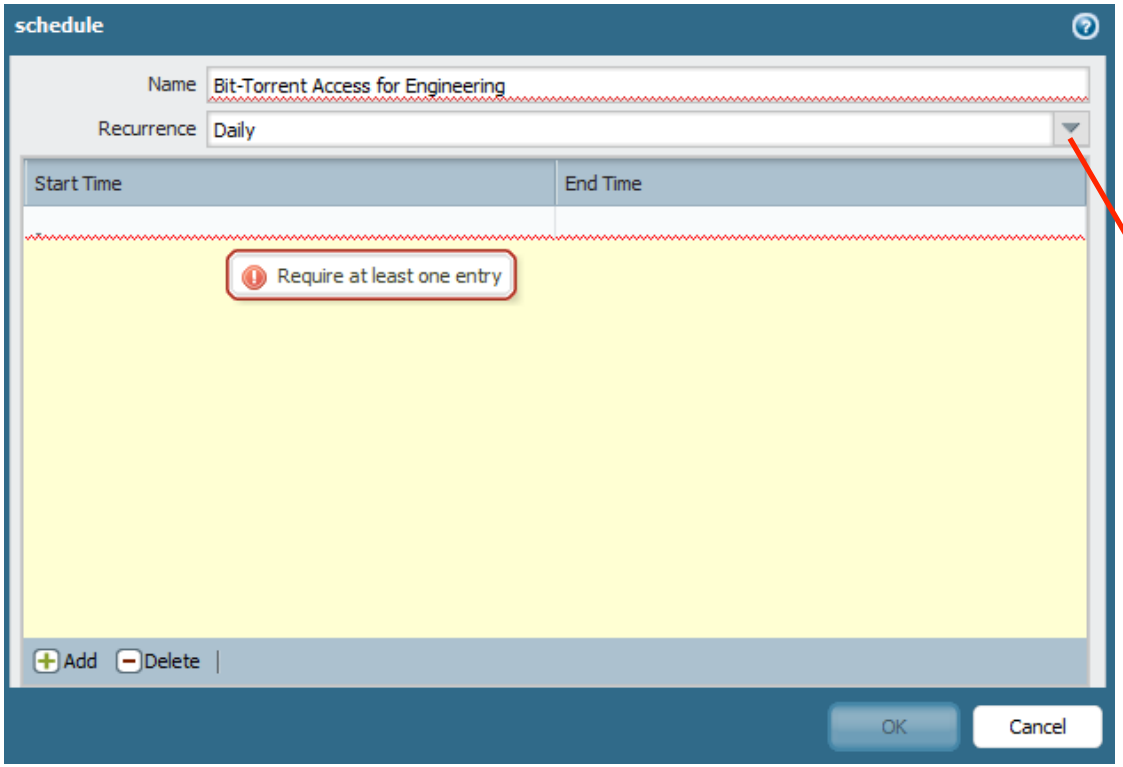
	Source			Destination					
Name	Zone	Address	User	Zone	Address	Application	Service	Action	Profile
LogAll	Tap	Mail Server	impressive\a... impressive\a...	Tap	any	facebook-chat	any		
IT Allow Override	trust	any	impressive\a...	untrust	any	Custom-app	any		
Read Only Facebook	trust	any	any	untrust	any	facebook-base	any		
Allow facebook posting	trust	any	impressive\m...	untrust	any	facebook-po...	any		

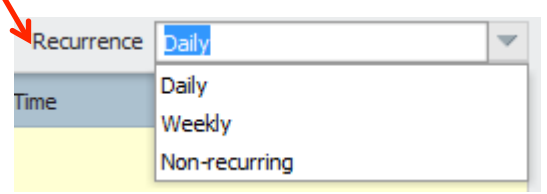
- When configuring a security to allow an application through the firewall, the service field should be set to “application-default” for inbound services. That will restrict the application to only use its standard ports (example: DNS will be restricted to only use port 53). It is a best practice to configure application-default or an explicit port(s) for increased control of the communication on the network
- Note that intra-zone traffic is allowed by default
- If you create a rule at the end of the list that says to deny (and log) all traffic, that will block intra-zone traffic (which may not be your intention)

paloalto NETWORKS

Scheduling Security Policies

- Policies can be scheduled to occur at particular times of day, or be a one-time occurrence
- Schedules are defined under Objects tab-> Schedules
  Once defined, these Schedules can be reused across multiple rules





- Possible schedule choices:
- Schedules are assigned under Policies tab -> Security Policy-> Options column

Blocking Skype

- The skype application is classified on the PAN device as two separate applications: skype-probe and skype.
- In general, think of the skype-probe application as the control channel, and “skype” application as the data channel.
- Since skype is so evasive, the way you prevent skype from sending or receiving voice or video is by allowing skype-probe, but blocking skype.
- This forces skype to use a communication that is easy to predict and block via App-ID

	Source			Destination				
Name	Zone	Address	User	Zone	Address	Application	Service	Action
Allow_skype_probe	Trust-L3	any	any	Untrust-L3	any	skype-probe	any	✓
Block_skype	Trust-L3	any	any	Untrust-L3	any	skype	any	⊘

paloalto NETWORKS

Monitoring Traffic

- The default traffic log behavior is to log all at session close. On a per-rule basis, the functionality logging at session start/session end can be selectively toggled or disabled completely
- Traffic log can be viewed under Monitor tab -> Logs -> Traffic.
- The application that was detected is shown in the log.

Traffic Log

Filter:

	Receive Time	Type	From Zone	To Zone	Source	Destination	From Port	To Port	Protocol	Application	Action
	01/25 08:40:39	end	trust	untrust	172.16.1.12	204.176.49.2	1839	80	tcp	web-browsing	allow
	01/25 08:40:32	end	trust	untrust	1.1.1.33	68.105.28.11	62892	53	udp	dns	allow
	01/25 08:40:23	end	untrust	trust	3.3.3.9	1.1.1.9	1722	139	tcp	incomplete	allow

- Filters can be created, using a syntax similar to Wireshark
  - Here is an example where you are viewing all traffic between 1.2.3.4 and 3.3.3.11:

Traffic Log

Filter: (addr in 1.2.3.4) and (addr in 3.3.3.11)

paloalto NETWORKS

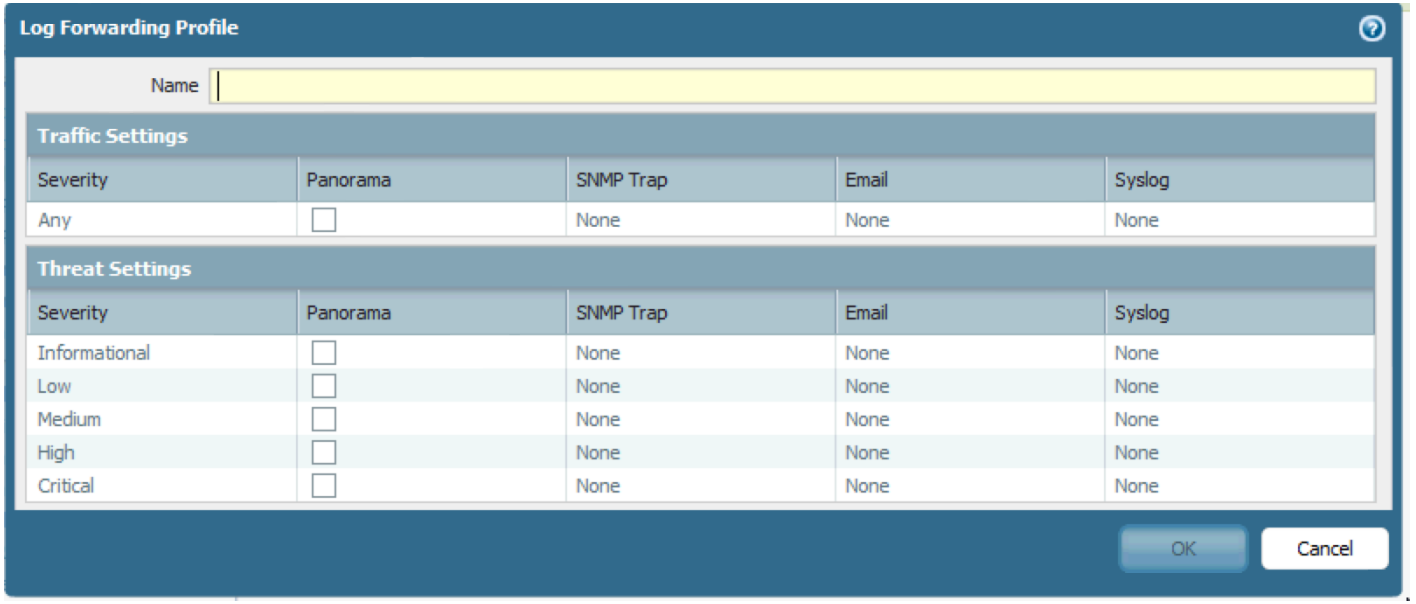
Monitoring Traffic (2)

Special Application names are used to define traffic not explicitly identified by App-ID. These application will be displayed in the Traffic log as follows:

- “incomplete”
  - SYN or SYN-SYNACK-ACK is seen, but no data packets are seen
- “insufficient-data” means that either:
  - The firewall didn’t see the complete TCP 3-way handshake, or
  - There were no data packets exchanged after the handshake
- “unknown-tcp”
  - Application consists of unknown tcp traffic.
- “unknown-udp”
  - Application consists of unknown udp trafic.
- “unknown-p2p”
  - Application matches generic p2p heuristics
- “not-applicable”
  - Session is blocked by the firewall

Log Forwarding

- The logs on the firewall can be forwarded to multiple locations. Upon generation of a log message, that message can be immediately forwarded to:
  - Syslog server
  - SNMP manager
  - Email
  - Panorama
- You configure the log message destination via a Log Forwarding Profile:



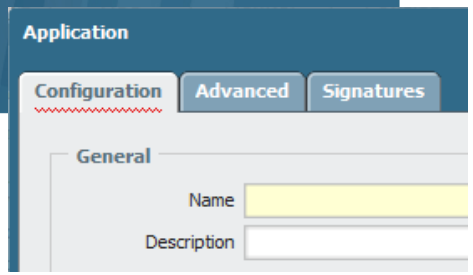
Unknown Applications

- Scenario: a network has a particular application that runs on a specific port, yet the Palo Alto firewall identifies it as “unknown-tcp” or “unknown-udp”

	Receive Time	Type	From Zone	To Zone	Source	Destination	From Port	To Port	Protocol	Application	Action
	01/26 11:46:54	end	tapzone	tapzone	10.154.3.60	72.247.247.125	1588	1935	tcp	unknown-tcp	allow
	01/26 11:43:55	end	tapzone	tapzone	10.154.5.204	72.247.247.132	2810	1935	tcp	unknown-tcp	allow

- To configure the firewall to identify this app, you will need to do three things:
  1. Create a new application
  2. Create an application override policy
  3. Make sure there is a security policy that permits the traffic

Steps to Define a New Application



1. Objects -> Applications, click New
   - Specify the application name and properties
   - On advanced tab, enter the port number that uniquely identifies the app
   - Nothing else required, click ok
2. Policies -> Application Override-> Add Rule
   - Specify port number
   - Config application to be the one you just created

	Destination				
	Zone	Address	Protocol	Port	Application
	untrust	any	tcp	8080	Custom-app

3. Policies -> Security -> Add Rule
   - Configure as appropriate: src zone/dest zone/src addr/dest addr/src user
   - Select the new app in the application column
   - For service, select “application default”
   - Select the action you want (permit/deny)
4. Commit

	Source			Destination				
Name	Zone	Address	User	Zone	Address	Application	Service	Action
IT Allow Override	trust	any	impressive\a...	untrust	any	Custom-app	any	✓

More on Unknown Applications

- App override policies are checked before security policies. The app override policy will be used in place of our App-ID engine to identify the traffic.
- Security profiles CANNOT be assigned to Application Override policies. Application Override policies bypass the Signature Match Engine entirely, which means that this also eliminates the option of performing Content-ID on this traffic. Because of this fact, the Application Override feature should be used with internal traffic only.
- The solution on the previous page is a short-term solution. If the application is a common-use application, it is recommended that the customer submit pcaps of the application to Palo Alto Support. Then our engineering team can create a new signature for the particular app.

Source Address Translation

- NAT rules are in a separate rulebase than the security policies.
- Palo Alto firewall can perform source address translation and destination address translation.
- Shown below is the NAT rule as well as the security rule to perform source translation
- See powerpoint notes below for more info

SA	DA	SP	DP
10.1.1.47	4.2.2.2	43778	80

Pre NAT: From L3-trust -> L3-untrust

NAT Rules

		Original Packet					Translated Packet	
	Name	Source Zone	Destination Zone	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	rule1	L3-trust	L3-untrust	any	any	any	64.3.1.22	none

Post NAT: From L3-trust -> L3-untrust

SA	DA	SP	DP
64.3.1.22	4.2.2.2	1031	80

Security Rules

	Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile	Options
30	Source NAT	L-3 Trust	L-3 Untrust	10.1.1.0/24	any	any	any	any		none	

paloalto NETWORKS

Destination Address Translation

See powerpoint notes below for description

SA	DA	SP	DP
12.67.5.2	64.10.11.103	5467	80

Pre NAT: From L3-untrust -> L3-untrust

NAT Rules

		Original Packet					Translated Packet	
	Name	Source Zone	Destination Zone	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	rule1	L3-trust	L3-untrust	any	any	any	64.3.1.22	none
2	rule2	L3-untrust	L3-untrust	any	64.10.11.103/32	service-http	none	192.168.10.100

Notice the destination zone is the same as the source zone

Post NAT: From L3-untrust -> L3-trust

SA	DA	SP	DP
12.67.5.2	192.168.10.100	5467	80

Security Rules

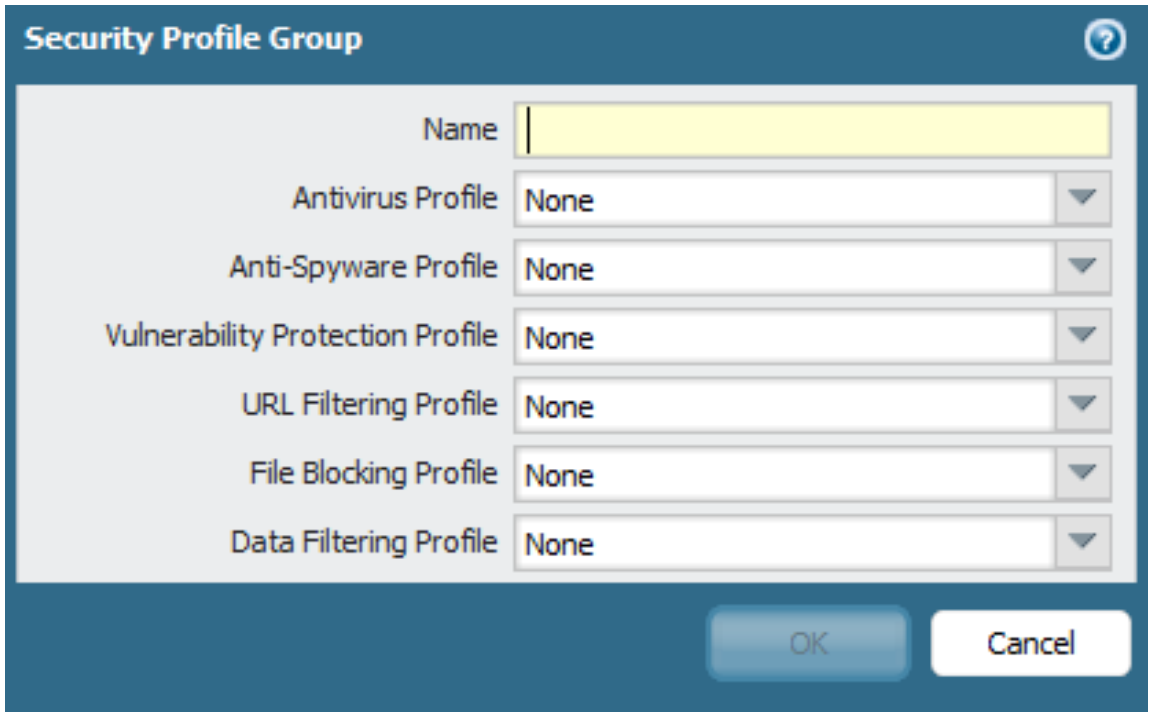
	Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action
31	Destination NAT	L-3 Untrust	L-3 Trust	any	any	64.10.11.103/32	web-browsing	application-default	

Notice the destination zone is based upon the post-NAT address

paloalto NETWORKS

Security Profiles

- Security Profiles look for malicious use of allowed applications
- Security Policies define which applications are allowed
- Profiles are applied to policies that allow traffic



paloalto NETWORKS

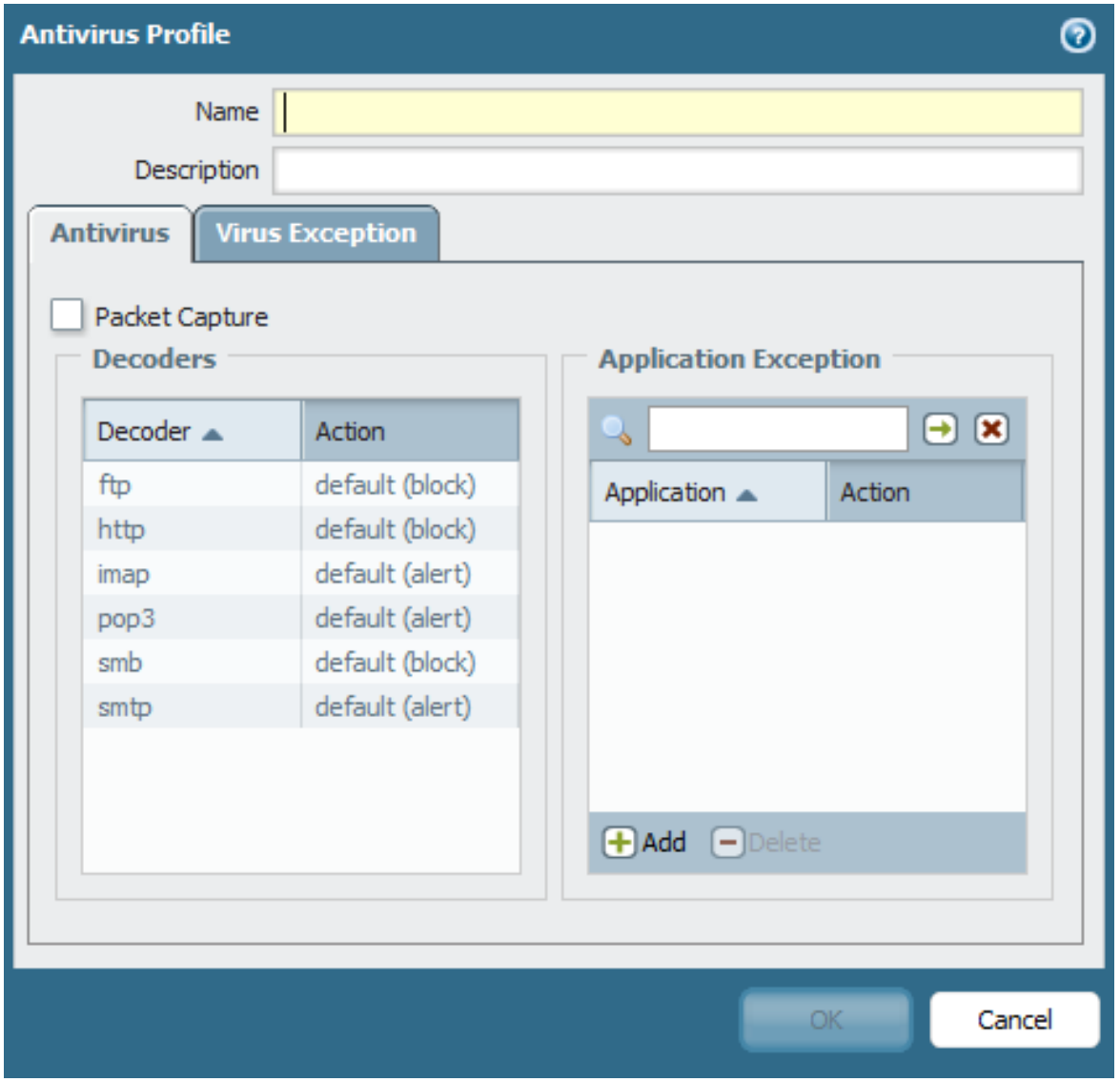
Using Security Profiles

- The profile used for traffic is based on the policy that allows the traffic
- Example:

1	Open Twitter	trust	untrust	any	pan-training\students	any	twitter	application-default	✓	none
2	Limited Twitter	trust	untrust	any	any	any	twitter	application-default	✓	

- Open Twitter: Student users, no URL filtering profile
- Limited Twitter: All other users, URL filtering to specific twitter URL's

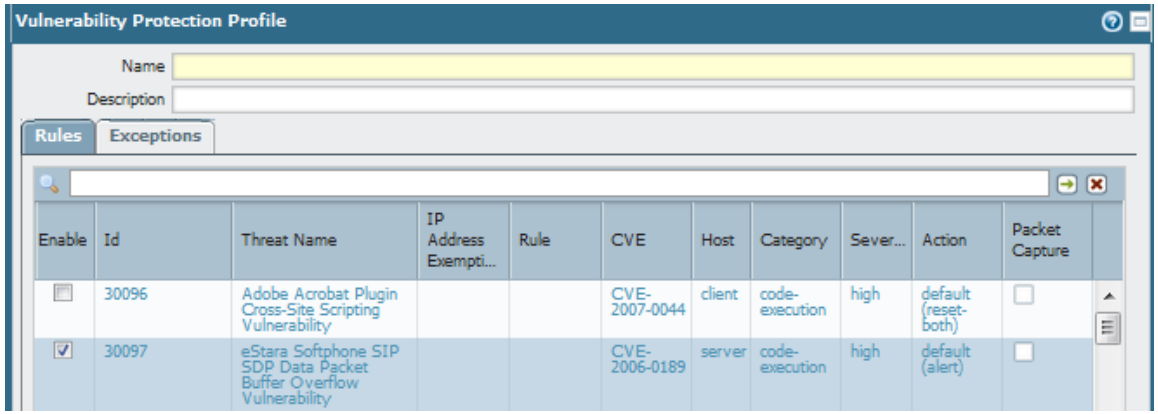
Anti-Virus Profiles



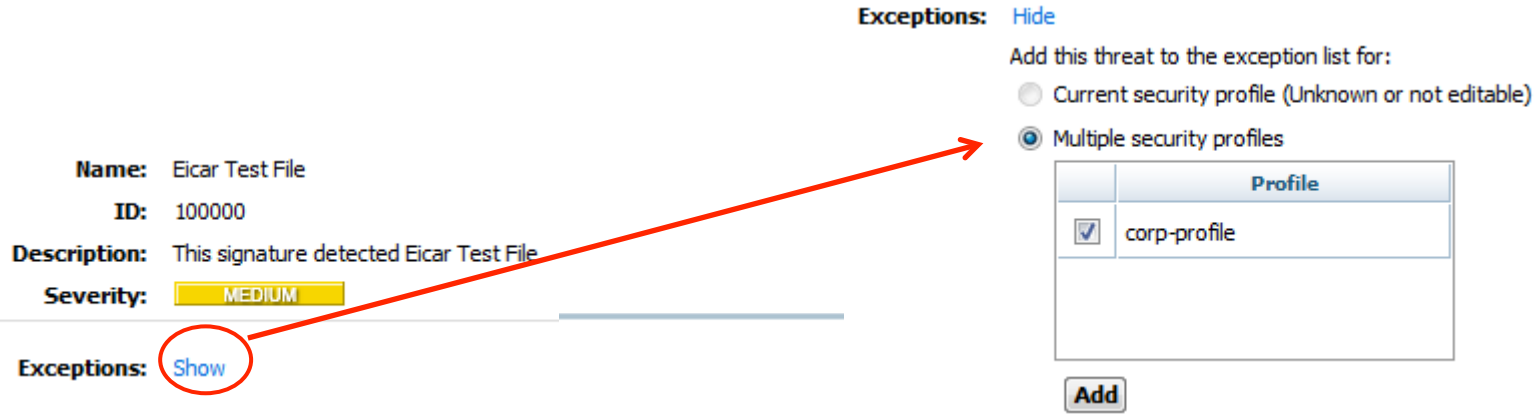
- A decoder is a software process on the firewall that interprets the protocol.
- In the antivirus and anti-spyware security profiles, you can specify actions based upon the 6 main decoders in the system, shown to the left.

Configuring Exceptions

- If you have a threat or virus that you do not want to be detected, you can configure an exception
- Two ways to configure an exception:
  1. On the security profile, go to the exceptions tab, enter the threat ID there:



  2. In the threat log, click on the threat or virus name. In the pop-up window, next to exceptions, click “show”, then select the profile to add the exception to.

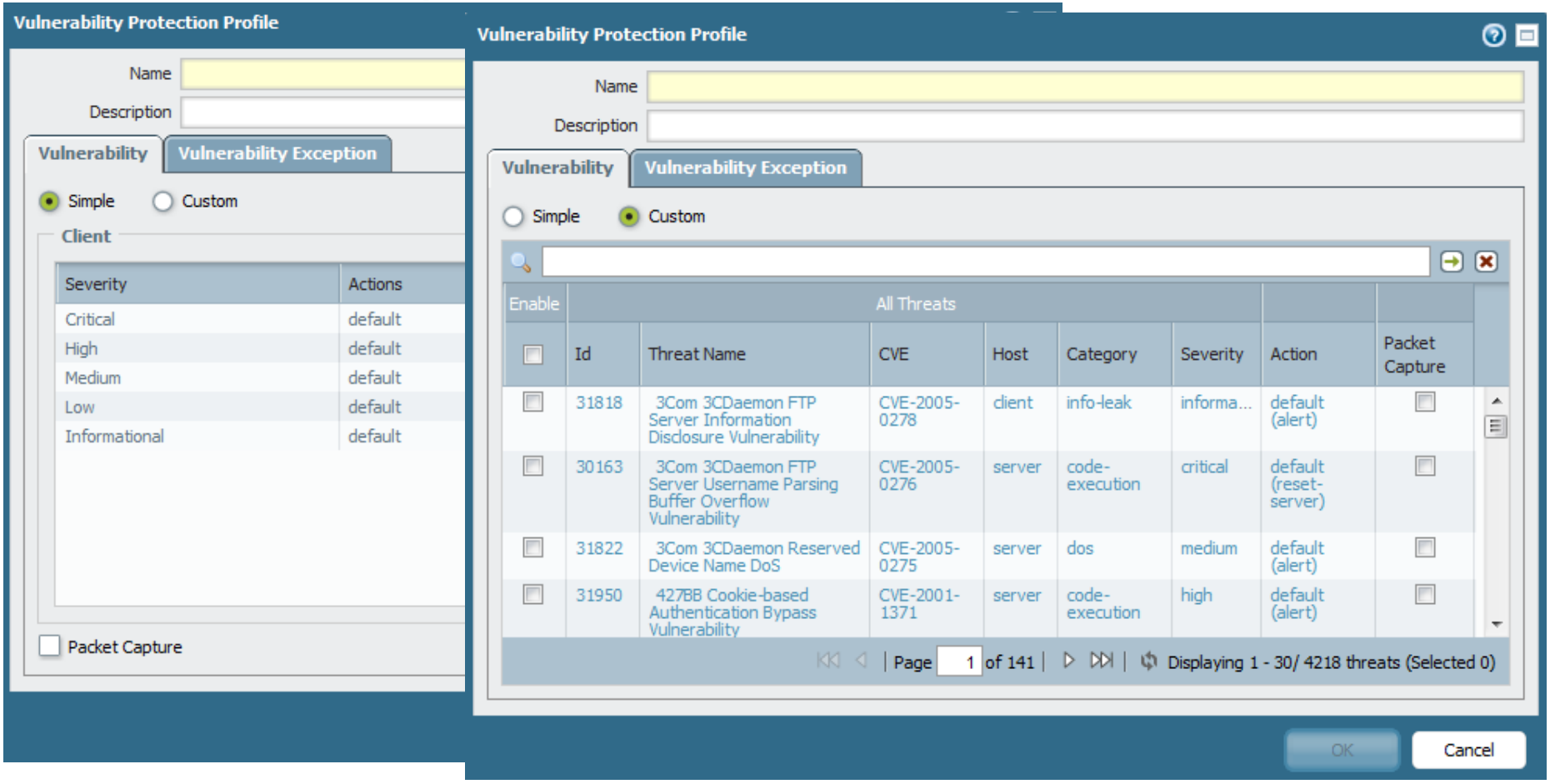


Email Protocols and AV/Spyware Protection

- If a Palo Alto Networks firewall detects a virus or spyware in SMTP, a 541 response is sent to the sending SMTP server to indicate that the message was rejected. This allows the Palo Alto Networks firewall to effectively block viruses distributed over SMTP.
- For POP3/IMAP, the only action the Palo Alto Networks device can will ever take is “alert”. The device will never block or drop for these protocols, even if you configure an action of “block”.
- The reason for this is because POP3/IMAP protocols will continue to resend the email message again and again if an intermediate device tries to close the session. This is a limitation of the POP3/IMAP protocols.

Vulnerability Protection

- Provides IPS functionality
- Detects attempts to use known exploits on the network

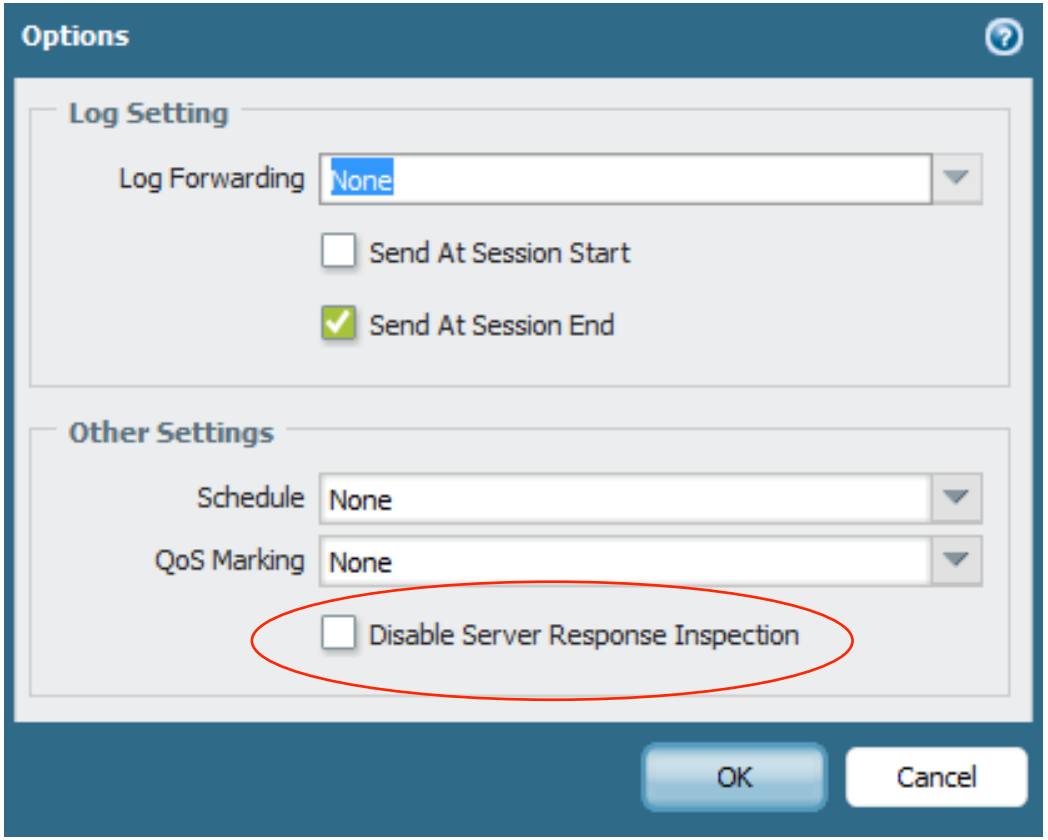


Custom Response Pages

- Response pages are configured under Device tab -> Response pages
- You can externally edit and upload those response pages to the device
- Only the html file can be uploaded to the device, images cannot be uploaded
- Response pages are displayed in the web browser only and pertain only to web-based applications
  - Thus if a threat is detected during say a BitTorrent session, the response page will not appear
- Response Pages for web-based applications are not enabled by default

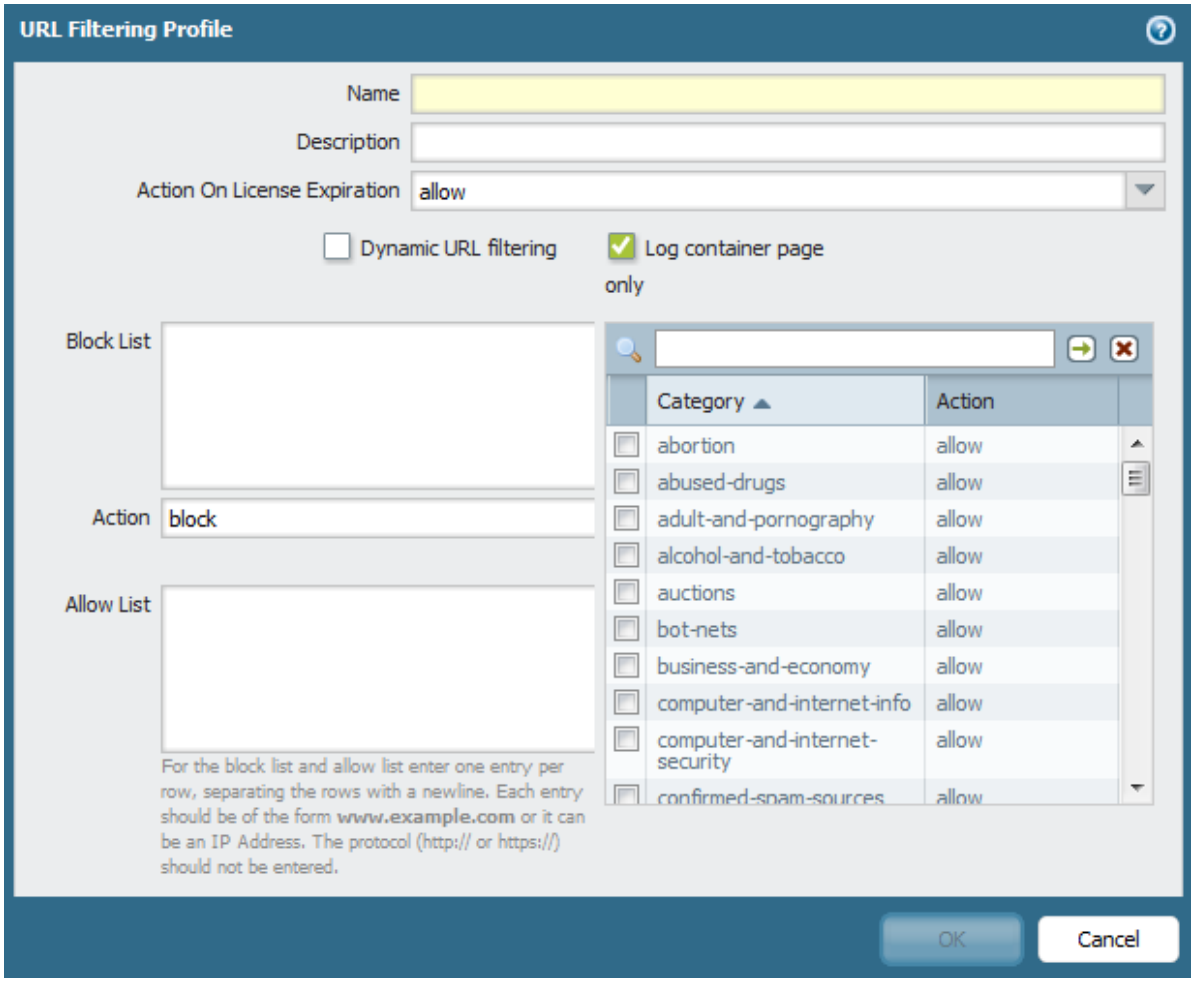
Disable Server Response Inspection

- The vulnerability protection profile by default scans traffic going in both directions (from client to server, and from server to client)
- Most IPSs only examine the traffic from the client to server.
- The way to examine traffic from only client to server on the Palo Alto firewall is to check the box to “disable server response inspection” on the security policy (options column).



URL Filtering Profile

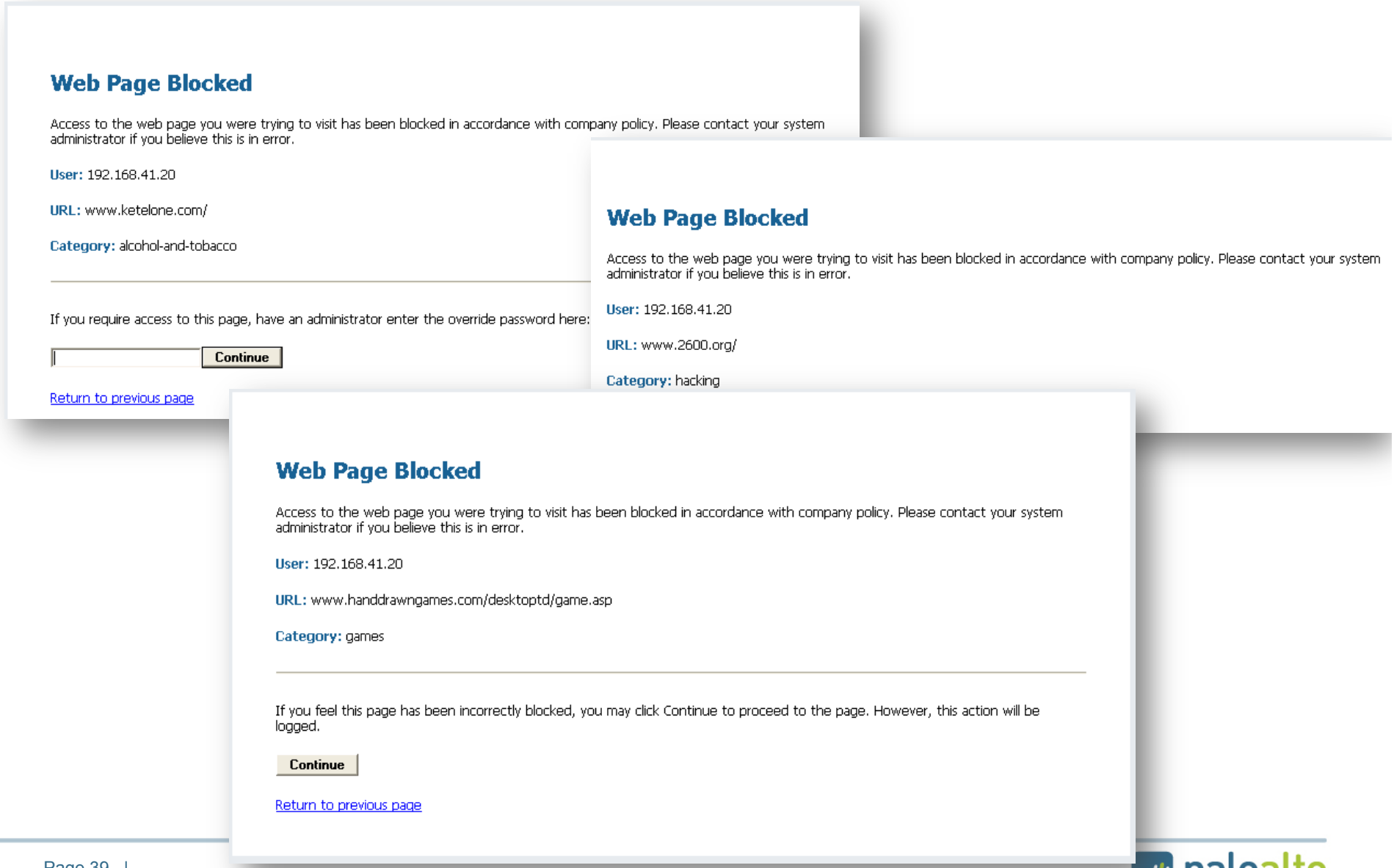
- Actions can be defined for each category
- Notification page for user can be customized
- Allow List and Block List accept wild cards
  - To specify all servers in a domain called xyz.org, two entries must be created:
    - *xyz.org*
    - **.xyz.org*
- Upon URL license expiration, URL database is no longer used; traffic is allowed or blocked based upon the “action on license expiration” field shown here.



URL Filtering Actions

- Allow – Traffic is passed, no log generated
- Block – Traffic is blocked. Block log generated
- Alert – Traffic is allowed. Allow log generated
- Continue – User is warned that the site is questionable. Block-Continue log generated
  - If user clicks through the traffic is allowed and a Continue log is generated
- Override – Traffic is blocked. User is offered chance to enter override password. Block-Override log generated
  - If user enters password the traffic is allowed and an Override log is generated

Default Block Pages



paloalto NETWORKS

Misc. URL Filtering Topics

- Order of checking within a profile:
  1. Block list
  2. Allow list
  3. Custom Categories
  4. Cached
  5. Pre-defined categories
- "Dynamic URL filtering"
  - Can be enabled on each URL filtering profile
  - If enabled, the PA device will query the cloud to resolve URLs that are not categorized by the on-box URL database
- To determine the category of an URL from the CLI:
  - **`test url <fqdn>`**

Data Filtering Overview

- Scan traffic for potentially sensitive strings of data
  - Data strings defined by regular expressions
  - Data pattern must be at least 7 bytes in length
  - Default strings are defined for SSN and credit card numbers
- Each data string is assigned a weight
- Alert threshold and block threshold is based upon weights

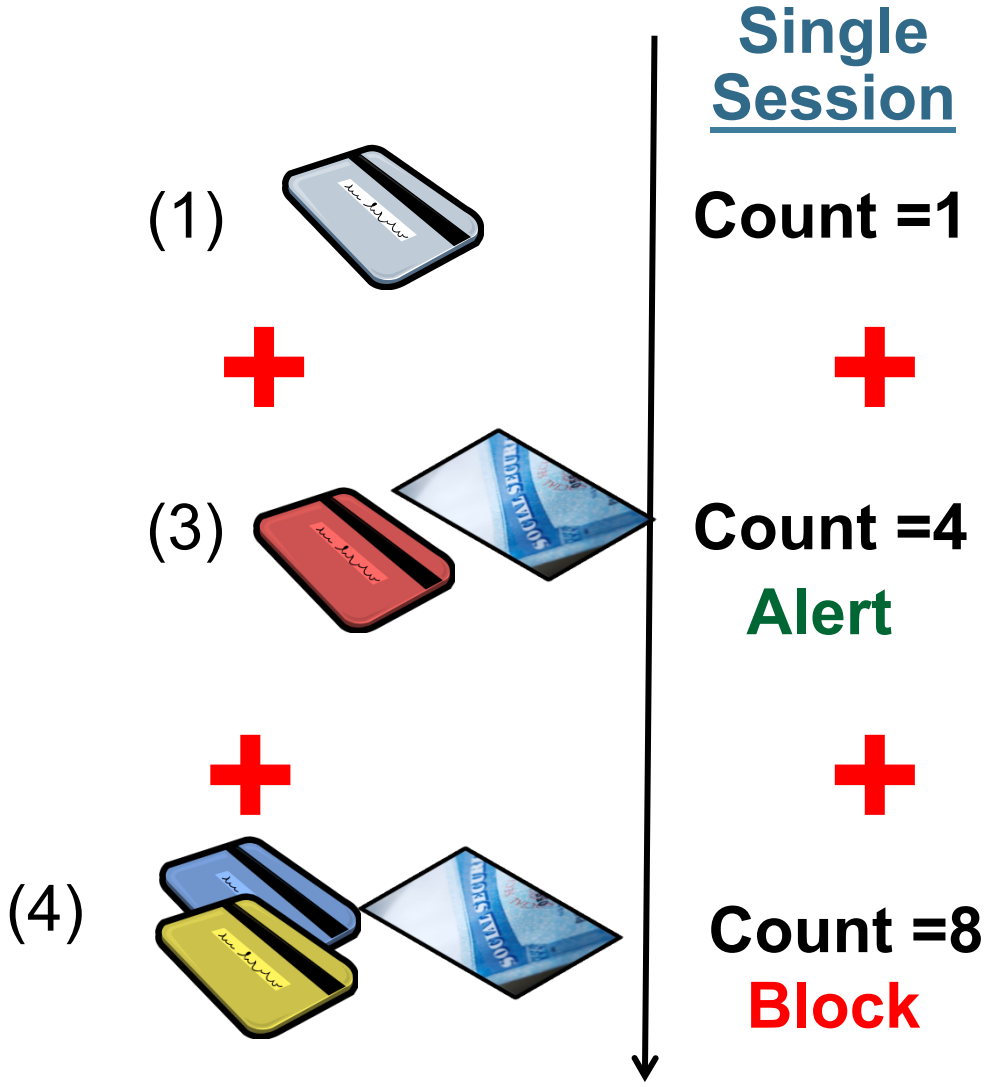
Data Filtering Example

Credit Card Weight = 1

SSN Weight = 2

Alert Threshold = 4

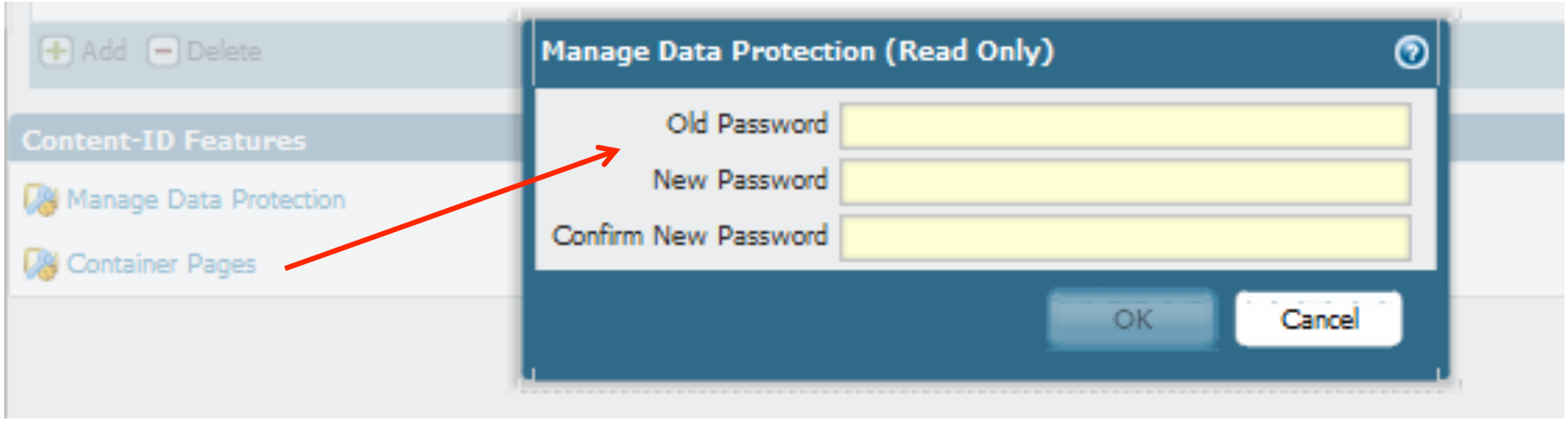
Block Threshold = 8



paloalto NETWORKS

Data Filtering Password Setup

- PCAPs on data filters require a password to be configured prior
  - Single password for firewall, stored locally, configured on Device tab-> Setup screen
- See PowerPoint notes below for more info



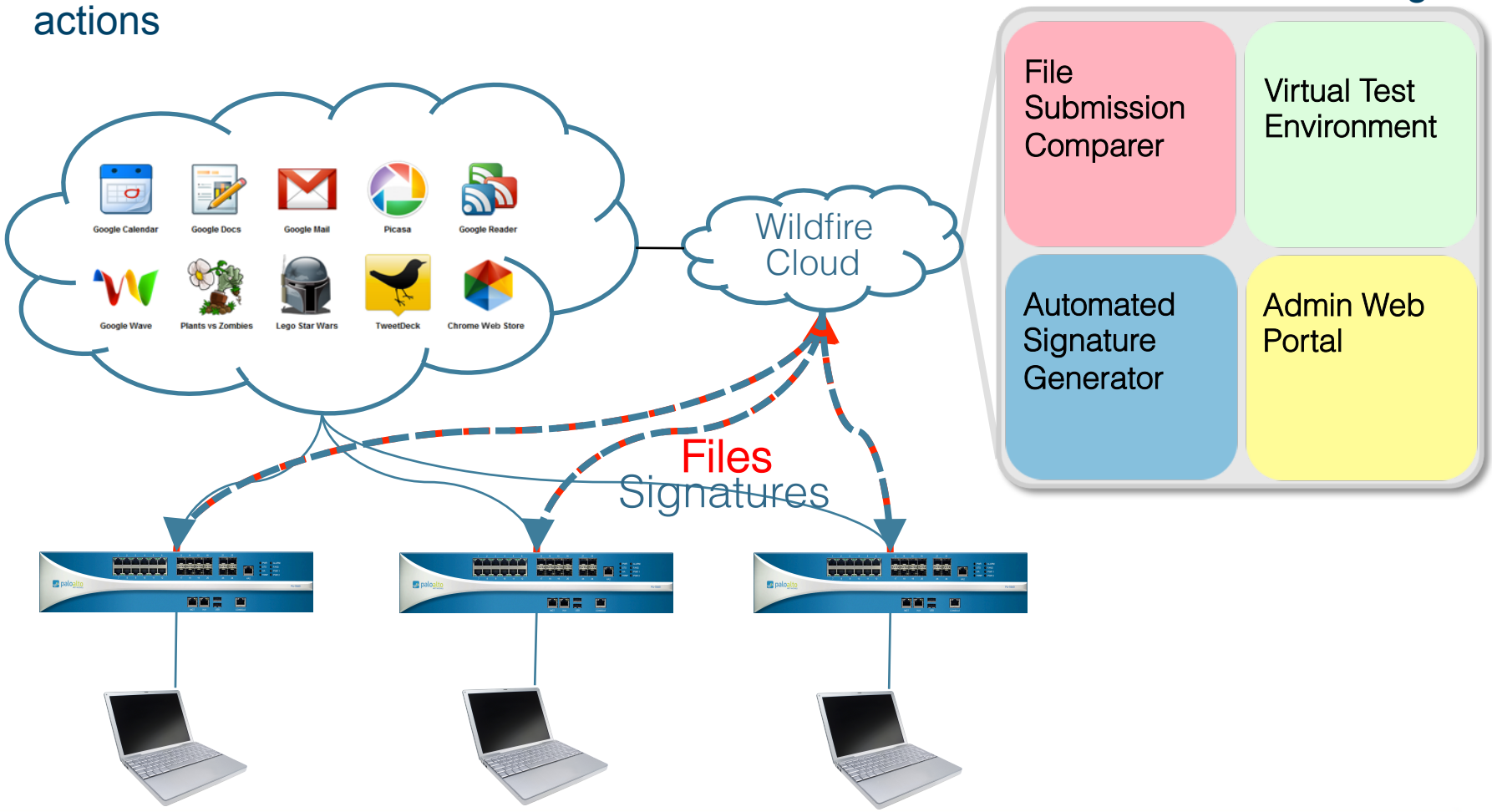
Zone Protection

- For each security zone, you can define a zone protection profile that specifies how the security gateway responds to attacks from that zone.
- The same profile can be assigned to multiple zones.
- The following types of protection are supported:
  - Flood Protection—Protects against SYN, ICMP, UDP, and other IP-based flooding attacks.
  - Reconnaissance detection—Allows you to detect and block commonly used port scans and IP address sweeps that attackers run to find potential attack targets.
  - Packet-based attack protection—Protects against large ICMP packets and ICMP fragment attacks.
- Configured under Network tab -> Network Profiles -> Zone protection

		Flood Protection					Reconnaissance Protection		
	Name	SYN Flood	UDP Flood	ICMP Flood	ICMPv6 Flood	Other IP Flood	TCP Port Scan	UDP Port Scan	Host Sweep
☐	External_Zone-Pen-Protect	✔		✔	✔		✔	✔	

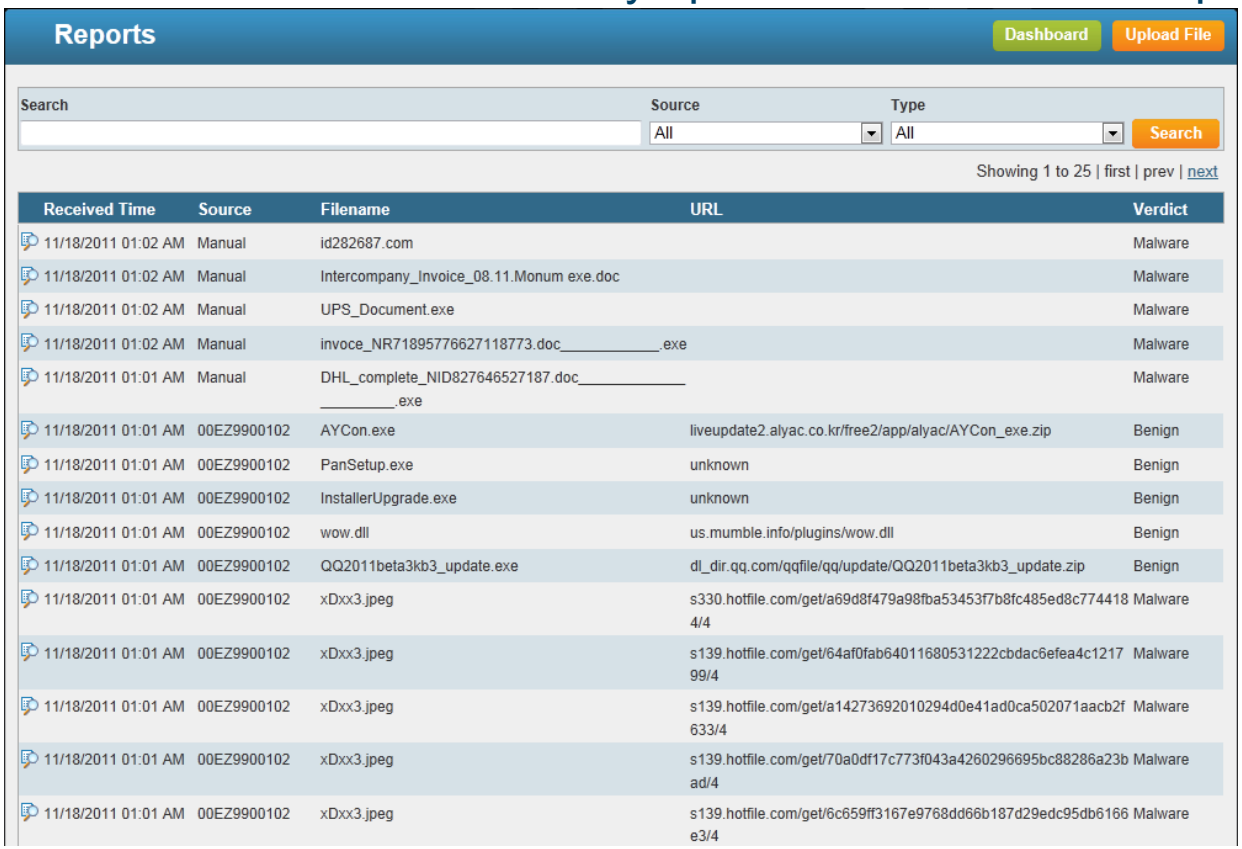
WildFire

- WildFire relies upon two main technologies: a virtual sandbox environment and a malware signature generator
- WildFire is enabled via the “Forward” and “Continue-and-Forward” file-blocking actions



WildFire

- Provides a virtual sandbox environment for Windows PE files
- A hash of each file is sent to the WildFire cloud. If no existing signature exists, the file is uploaded. The new signature will be made available as part of the next AV Update
- Files up to 10 MB in size can be manually uploaded to the WildFire portal for inspection



Received Time	Source	Filename	URL	Verdict
11/18/2011 01:02 AM	Manual	id282687.com		Malware
11/18/2011 01:02 AM	Manual	Intercompany_Invoice_08.11.Monum exe.doc		Malware
11/18/2011 01:02 AM	Manual	UPS_Document.exe		Malware
11/18/2011 01:02 AM	Manual	invoce_NR71895776627118773.doc_____.exe		Malware
11/18/2011 01:01 AM	Manual	DHL_complete_NID827646527187.doc_____ _____.exe		Malware
11/18/2011 01:01 AM	00EZ9900102	AYCon.exe	liveupdate2.alyac.co.kr/free2/app/alyac/AYCon_exe.zip	Benign
11/18/2011 01:01 AM	00EZ9900102	PanSetup.exe	unknown	Benign
11/18/2011 01:01 AM	00EZ9900102	InstallerUpgrade.exe	unknown	Benign
11/18/2011 01:01 AM	00EZ9900102	wow.dll	us.mumble.info/plugins/wow.dll	Benign
11/18/2011 01:01 AM	00EZ9900102	QQ2011beta3kb3_update.exe	dl_dir.qq.com/qqfile/qq/update/QQ2011beta3kb3_update.zip	Benign
11/18/2011 01:01 AM	00EZ9900102	xDxx3.jpeg	s330.hotfile.com/get/a69d8f479a98fba53453f7b8fc485ed8c774418 4/4	Malware
11/18/2011 01:01 AM	00EZ9900102	xDxx3.jpeg	s139.hotfile.com/get/64af0fab64011680531222cbdac6efea4c1217 99/4	Malware
11/18/2011 01:01 AM	00EZ9900102	xDxx3.jpeg	s139.hotfile.com/get/a14273692010294d0e41ad0ca502071aacb2f 633/4	Malware
11/18/2011 01:01 AM	00EZ9900102	xDxx3.jpeg	s139.hotfile.com/get/70a0df17c773f043a4260296695bc88286a23b ad/4	Malware
11/18/2011 01:01 AM	00EZ9900102	xDxx3.jpeg	s139.hotfile.com/get/6c659ff3167e9768dd66b187d29edc95db6166 e3/4	Malware

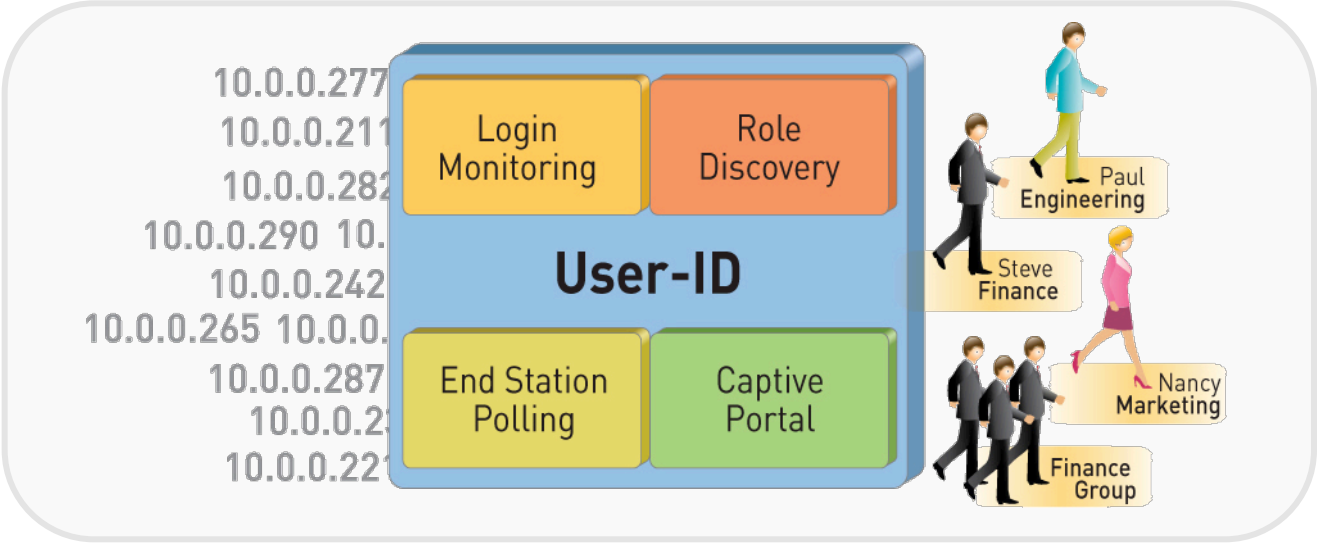
Packet Flow

- Refer to this document on the packet flow in PAN-OS: PANOS Packet Flow.pdf
- Have a general understanding of how packet are processed by the Palo Alto Networks firewall
  - Determine which of the following is checked first: NAT rules, security rules, PBF rules, app-ID
  - Prior to the session being established, a forward lookup is performed to determine what the post-NATed zone will be.
  - The packet flow process is intrinsically tied to the Single Pass Parallel Processing (SP3) hardware architecture of the Palo Alto Networks next-generation firewall.
  - Applications are identified once a session is created on an allowed port.

Role-based Administration

- Administrators can be given rights using the built in options or by creating new administrative roles
- There are 6 pre-defined administrator roles:
  - Superuser – All access to all options of all virtual systems.
  - Superuser (read-only)
  - Device Admin – Full access to the device except for creation of virtual systems and administrative accounts.
  - Device admin (read-only)
  - Vsys Admin – Full access to a specific virtual system.
  - Vsys admin (read-only)
- To provide a more granular level of control, additional roles can be created.

User-ID: Enterprise Directory Integration



- Users no longer defined solely by IP address
  - Leverage existing Active Directory or LDAP infrastructure without complex agent rollout
  - Identify Citrix users and tie policies to user and group, not just the IP address
- Understand user application and threat behavior based on actual username, not just IP
- Manage and enforce policy based on user and/or AD group
- Investigate security incidents, generate custom reports

paloalto NETWORKS

Where are Usernames Used?

1. Stored in Logs
   - Sort log data by User / Group
   - Filter logs by User

From User	To User	From Port	To Port	Protocol	Application
tlewis		49764	53	udp	dns
	mellison	1150	137	udp	netbios-ns
tlewis		49763	53	udp	dns
	rrosa	1150	137	udp	netbios-ns
	nburt	4140	3184	udp	emule
bbrown7		4981	80	tcp	limelight
tlewis		49785	53	udp	dns

2. As a Value to Match in Security Policy
   - Control application use by group
   - Separate unknown user traffic from known user traffic

Source User	Destination Address	Application	Service	Action
pancademo\administrators	any	Remote Access	any	✓
pancademo\jstoller	any	worldofwarcraft	any	✓

3. In URL-Filtering Response pages, User Name will be displayed

paloalto NETWORKS

User-ID Agent Setup and Upgrade Procedure

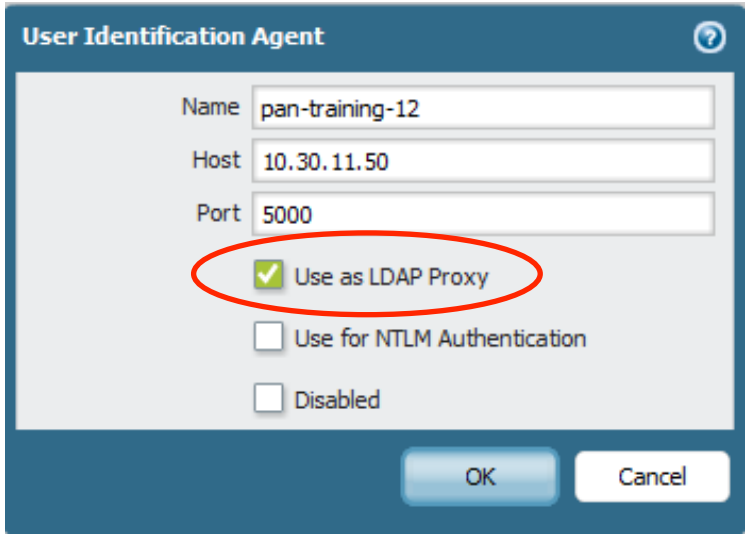
One agent is used for all directory services (AD, LDAP, eDirectory)

- The agent setup process is outlined here:
  Tech Note - PAN User-ID Agent install steps.pdf
- The most recent version of User-ID agent should always be used. PAN-OS will auto-detect the agent version and change it's behavior accordingly. The best practices when implementing the agent are outlined here:
  Tech Note - User Identification Best Practises PANOS 4.1.pdf
- When upgrading from a previous agent version to the 4.1 User-ID agent, use the following procedure:
  Tech Note - User-ID_Upgrade_4.1.pdf

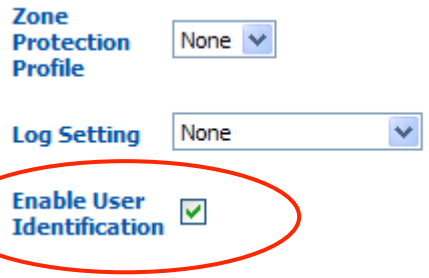
The User-ID API can be employed when connectivity to another identity management system is required

Installing the User-ID agent

- For detailed instructions on the operation of the User-ID Agent, read this document in detail: User-Identification-Operations-4.0.pdf
- Note that a best practice would be to install two User-ID Agents for each domain in the forest (for redundancy)
- In addition to mapping IP addresses, the User-ID agent can also act as an LDAP proxy, to assist in the enumeration process. This behavior is enabled through the selection of the “Use as LDAP Proxy” checkbox:

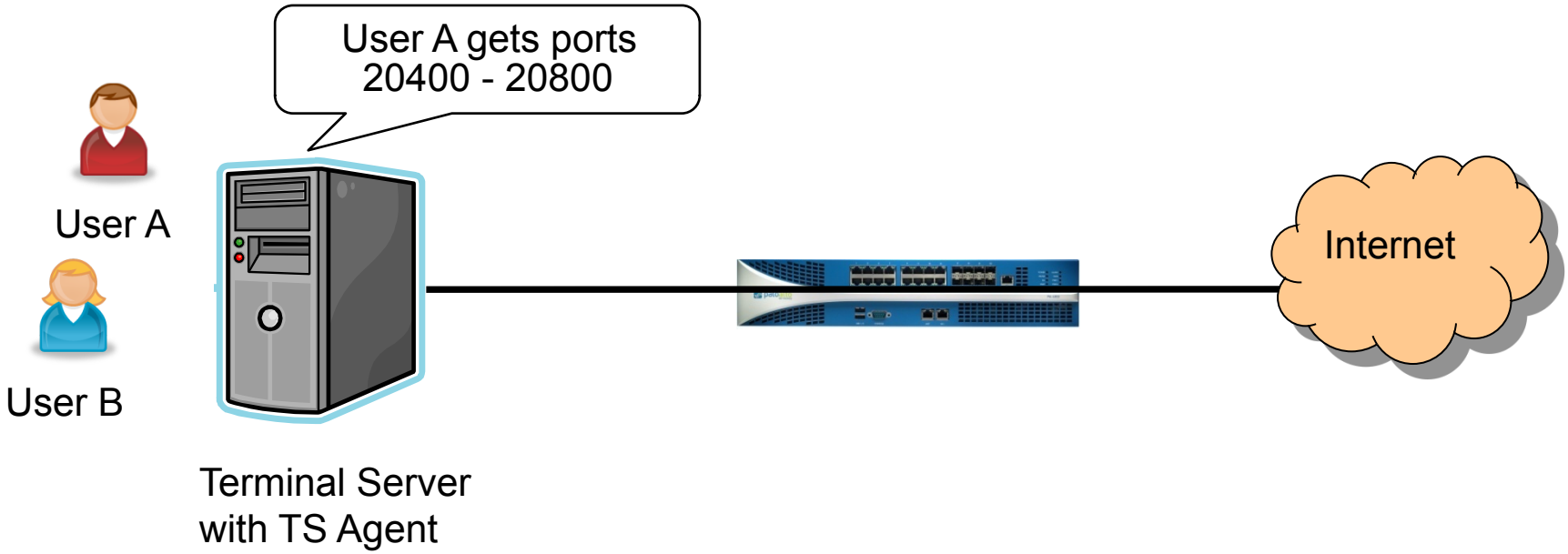


- Don’t forget to enable user-ID in the zone which contains the users!



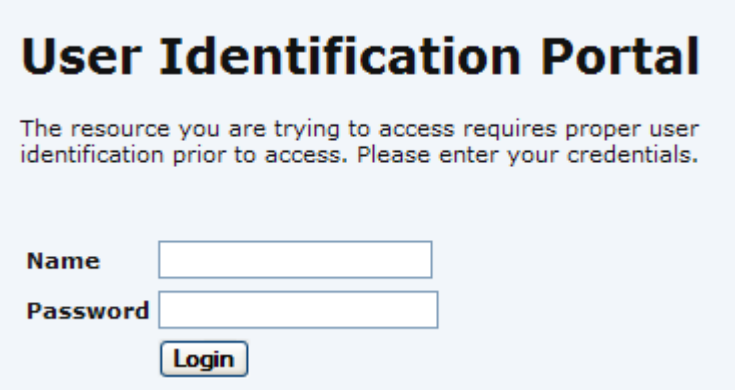
Terminal Server Agent

- Runs on the Terminal or Citrix Metaframe server
- TS Agent modifies the client port number from each user
- Firewall tracks user by source port, not by IP address



Captive Portal

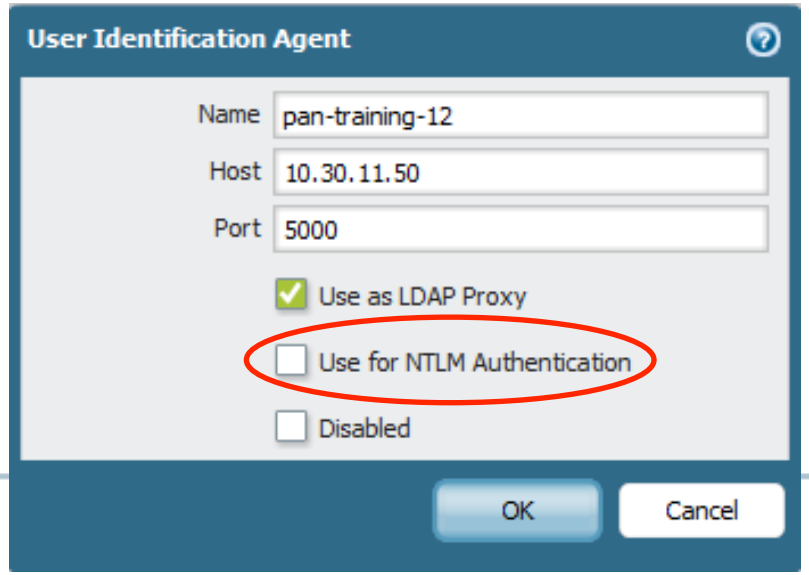
- Captive portal is a feature of the Palo Alto Networks firewall that authenticates users via an alternate source, such as a RADIUS server.
- Use captive portal when:
  - You have Windows users that are not logging into the AD domain
    - Authentication can be transparent if using NTLM authentication
  - You have Mac or Unix workstations
    - Users will see a login prompt
    - Users using captive portal without transparent NTLM authentication can be authenticated against RADIUS, Kerberos, LDAP, AD, or the local firewall.
  - You wish to invoke user identification for users that were not identified via one of the other user identification methods



- Once users authenticate with the firewall, user-based policies can be applied to the user's traffic.

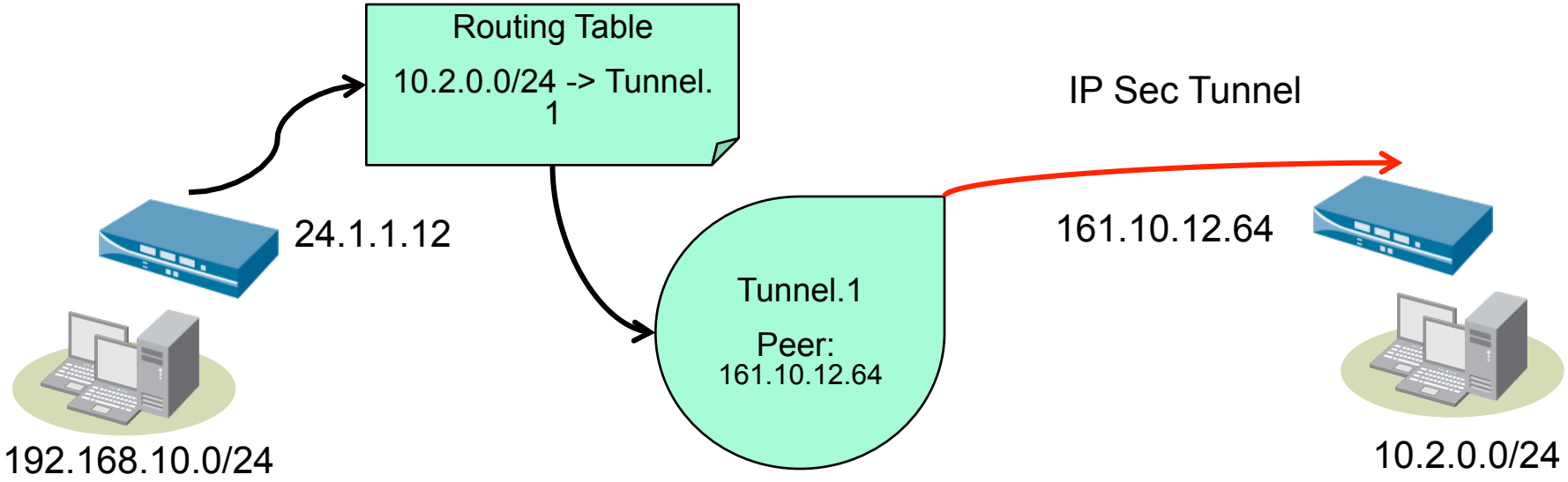
Captive Portal (2)

- How to configure Captive Portal:
  Tech Note - Captive Portal Transparent vs Redirect mode v3.1.pdf
  Tech Note - How to configure Captive Portal in PANOS 3.1.x L3.pdf
  Tech Note - How to Configure Captive Portal in PANOS 3.1.x Vwire.pdf
- A portion of this doc references certificate authentication; certificates are available with PAN-OS 4.0 or higher. The rest of the doc is applicable to PAN-OS 3.1
  - Captive Portal NTLM authentication requires the User ID Agent to be installed. The User ID agent must have the “Use for NTLM Authentication” checkbox selected.



Implementation of IPSec in PAN-OS

- PAN-OS implements route-based site to site IPSec VPN's
  - No IPSec client software available (use SSL VPN instead)
- The destination of the traffic determines if a VPN is required
- The tunnel is represented by a logical tunnel interface
  - One tunnel interface can support 10 IPSec tunnels
- The routing table chooses the tunnel to use



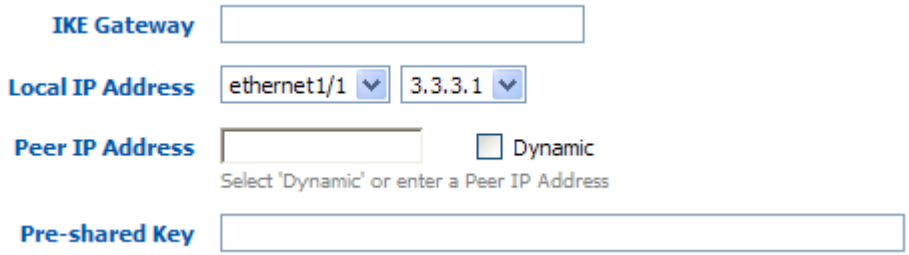
Steps to Configure an IPSec site-to-site VPN

1. Create a tunnel interface
   - Under the Networks tab-> Interfaces-> New Tunnel Interface
   - Assign it to a L3 Zone and a Virtual Router
2. Configure the IPSec Tunnel
   - Under Networks tab, IP Sec Tunnel
   - If site to site with another PAN-OS device use simple configuration
   - Set advanced options if required
3. Add static route to the appropriate Virtual Router or enable dynamic routing protocol
   - Under Networks tab, Virtual Router
   - Create a route for the remote private network using the tunnel interface

Dynamic routing protocols will traverse the tunnel if you assign a static IP to the tunnel interface

Notes about IPSec site-to-site VPNs

- Possible IKE phase 1 authentication methods:
  - Pre-shared key only



- It is possible to configure multiple phase 2 IP IPSec tunnels to use the same phase 1 gateway, as long as each phase 2 config uses different proxy IDs on that same tunnel interface.
- You can attempt to bring up all ipsec tunnels on the device via:

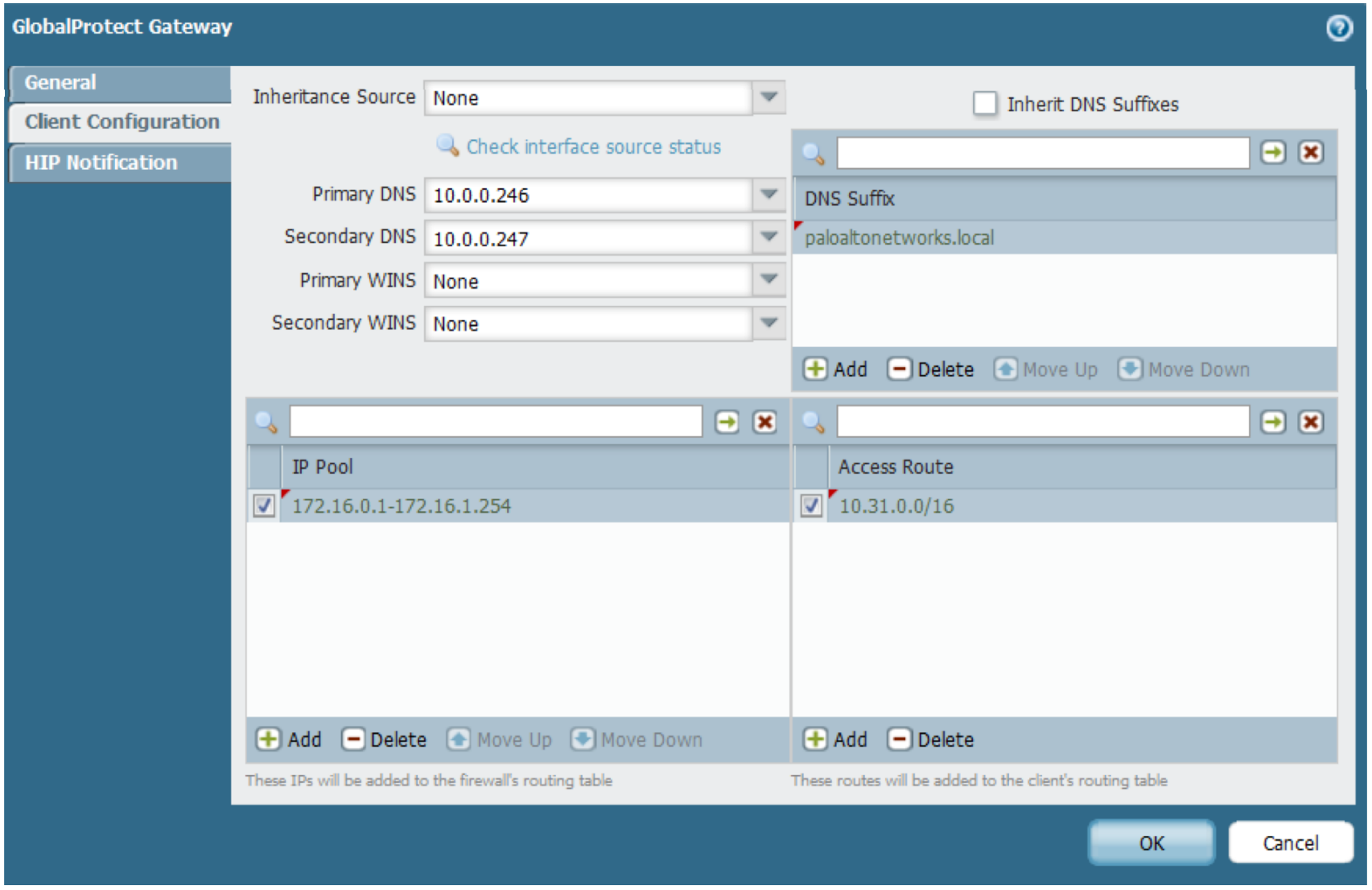
```
test vpn ipsec-sa <multiple arguments follow>
```

- How-to configure IPSec VPNs:
  Tech Note - How to configure site2site IPSec 4.0.pdf
- There are two docs, read the one titled “How to Configure an IPSec VPN”
  - There are a number of questions on IPsec, you should definitely follow this doc to configure a tunnel.

GlobalProtect - SSL VPN

- PAN-OS supports not only IPSec site-to-site VPNs, but SSL VPNs. SSL VPN's are provided via the GlobalProtect agent
- The GlobalProtect agent will run on Win32/Win64 and OS X 32-bit/64-bit clients
- The native VPN client on Apple iOS devices is officially supported via XAuth
- Interface types that can be used for the SSL VPN portal:
  - L3 interface
  - Loopback interface
- Prior to PAN-OS 4.1 NetConnect was the VPN client employed for SSL VPN's. To migrate NetConnect to GlobalProtect, follow this procedure: Tech Note - NC to GP Migration.pdf
- GlobalProtect can be installed as a basic Ipsec/SSL VPN or configured to make use of HIP profiles and HIP matches. Quickstart GlobalProtect guide: Quick Start Guide Global Protect ver2.pdf

SSL VPN Client Configuration Screen

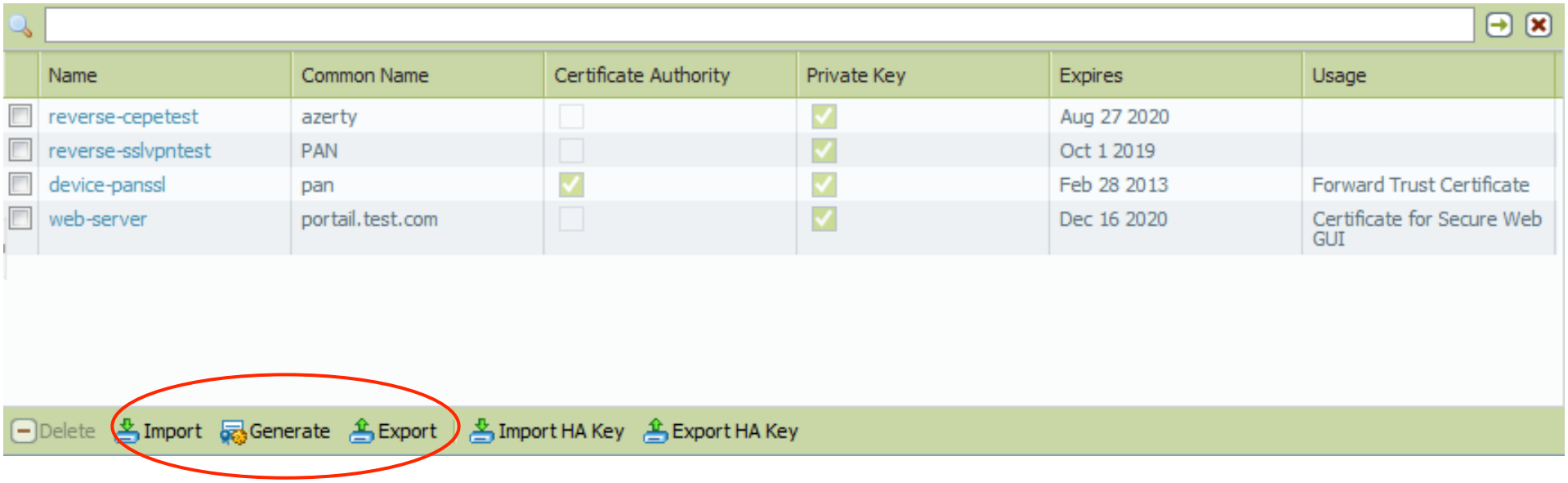


SSL Decryption

- The Palo Alto firewall can perform SSL decryption on connections that are initiated inbound or outbound, so that the traffic can be inspected for threats or restricted apps
- Inbound decryption:
  - Use when you want to intercept and decrypt users traffic coming from the Internet to your DMZ servers
  - You must load onto the firewall the same certificates that are on your DMZ servers
- Outbound decryption:
  - Use when you want to decrypt users traffic coming from the internal network and going to the external network
  - You need to have a PKI infrastructure in place for this to be transparent to the user
  - This is referred to as “forward-proxy”

Configuring SSL Inbound Decryption Certificate

- All certificates on the device (inbound/outbound/admin UI/etc) are centrally managed under the “Certificates” node on the “Device” tab



- You can add edit a certificate to establish it as an SSL inbound certificate. You should create one certificate for each DMZ server that you will be decrypting traffic for
- You can establish different SSL inbound certificates for different inbound SSL decryption rules.

Configuring SSL Outbound Decryption Certificate

- You can either generate a self-signed certificate (good for testing purposes), or import a certificate from your company's certificate server.

- In order to prevent users from seeing a browser certificate error, it is recommended that you have a PKI infrastructure deployed in your organization. Therefore you will be able to import into the firewall a certificate that is trusted by the users' browsers.
- When no internal PKI infrastructure is available, it is possible to distribute the firewall CA certificate to clients e.g. using Group Policy Objects functionality in Active Directory.

Configuring SSL Inbound or Outbound Policies

Once the appropriate certificates are imported/created, SSL Decryption policies can be created. For either inbound or outbound decryption, the policies are configured under Policies tab -> SSL Decryption.

- For inbound decryption, add a rule that looks like the following. This will decrypt traffic from the Internet to the public web server.

SSL Decryption Rules

	Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Category	Certificate	Action
1	rule1	Internet	DMZ	any	any	public web server	any	inbound_cert	decrypt

- For outbound decryption, and add two new rules that look like this:

2	rule2	Internal	Internet	any	any	any	financial-services health-and-medicine shopping	forward proxy	no-decrypt
3	rule3	Internal	Internet	any	any	any	any	forward proxy	decrypt

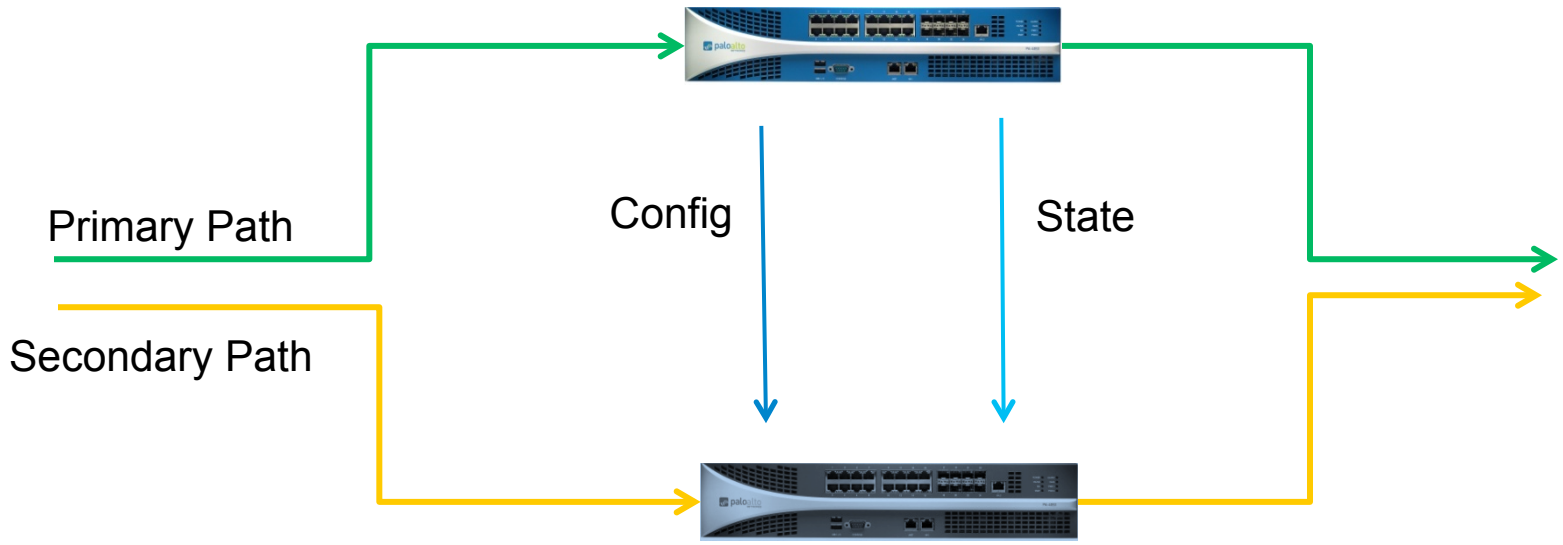
  - The first rule will not decrypt any traffic going to the URL categories of finance, health, and shopping.
  - The second rule will decrypt (proxy) all other connections. Make sure to choose action “decrypt” on the second rule

Misc. SSL Decryption

- When SSL is decrypted, the app running inside the SSL session will appear in the traffic log. For example:
  - https://facebook.com, SSL decryption NOT enabled, traffic log will show application is SSL
  - https://facebook.com, SSL decryption enabled, traffic log will show application is facebook
- The firewall will NOT send a response page for a virus detected with decrypted SSL traffic

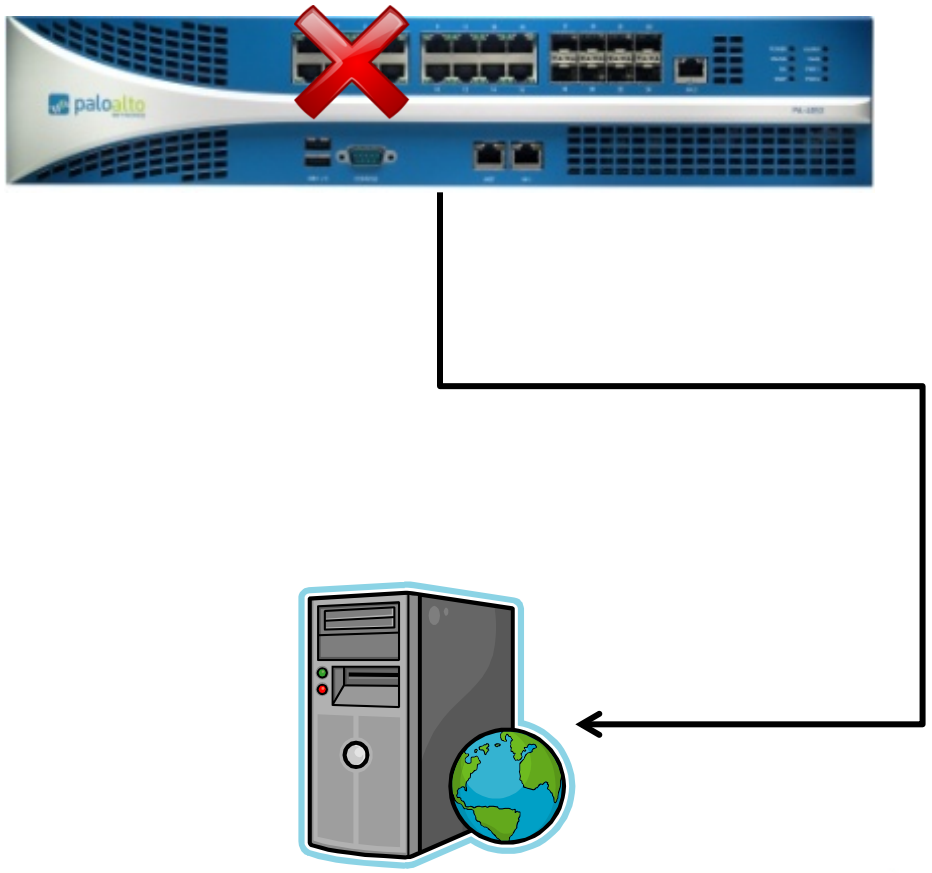
High Availability: Active/Passive

- 2 unit cluster provides Stateful synchronization
- HA 1 syncs certificates, response pages, and configuration
  - Communications can be encrypted by swapping the HA keys on both firewalls
- HA 2 syncs are Stateful session information between both devices
- Split-brain, in which both firewalls are attempting to take control as the Active device, can be controlled by enabling HA1 backup and/or enabling Heartbeat backup



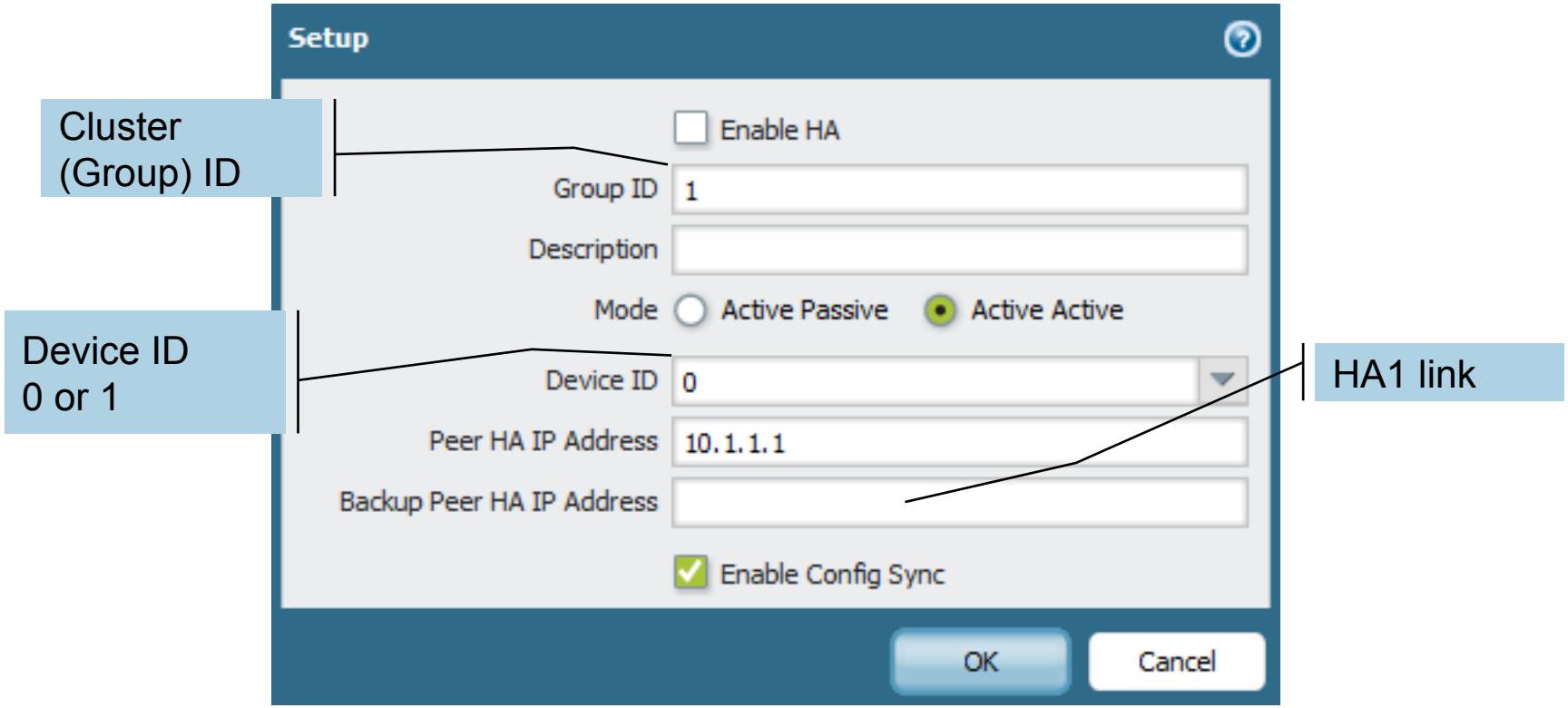
HA Failure States

- Link Failure
  - One or more physical links go down
- Path Failure
  - IP Address connectivity
- Combinations
  - Multiple possible failure states



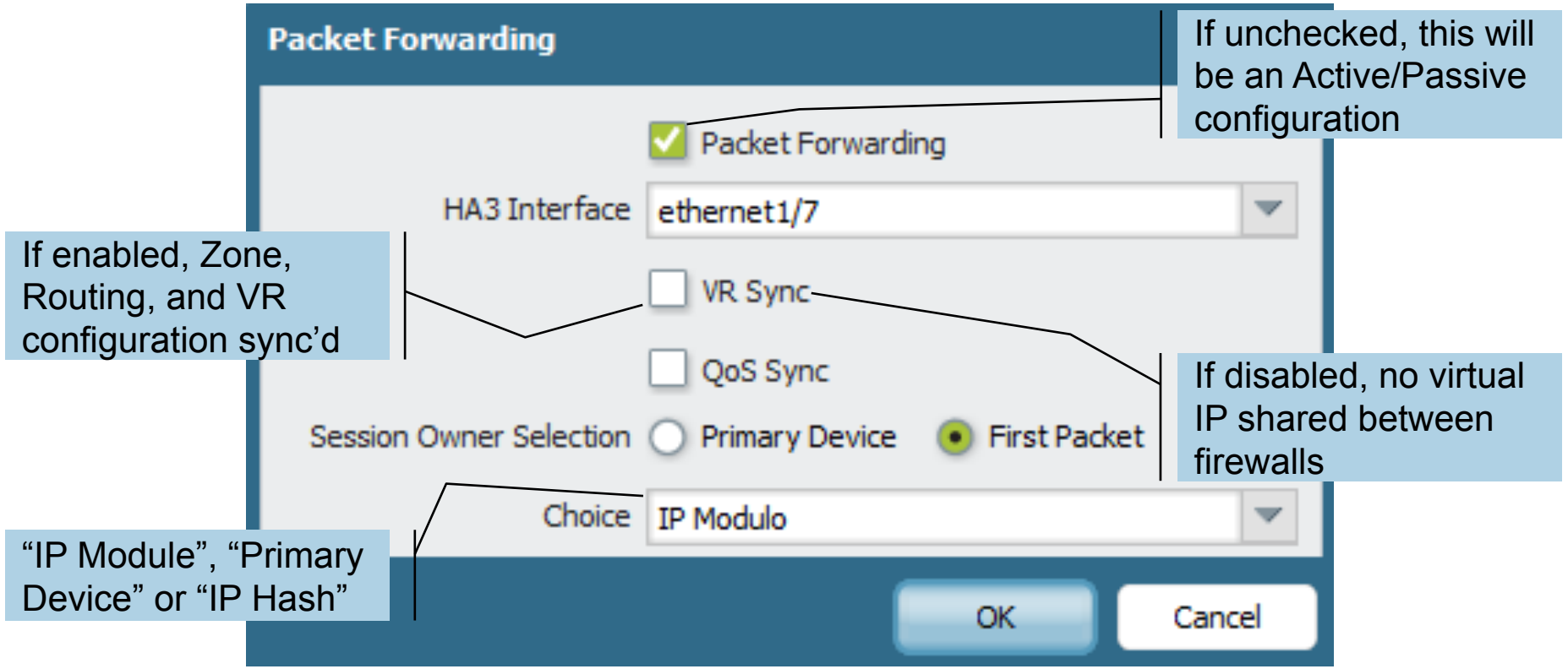
High Availability: Active/Active

- Requires a Group ID to uniquely identify both Devices within an HA Cluster
- Requires the selection of Active Active mode
- Requires the “Enable Config Sync” checkbox to be selected



Active/Active | HA3 interface

- A third HA interface is required for Active/Active HA. This interface provides Packet forwarding for Session Setup and L7 processing (App-ID and Content-ID) in asymmetrically-routed environments

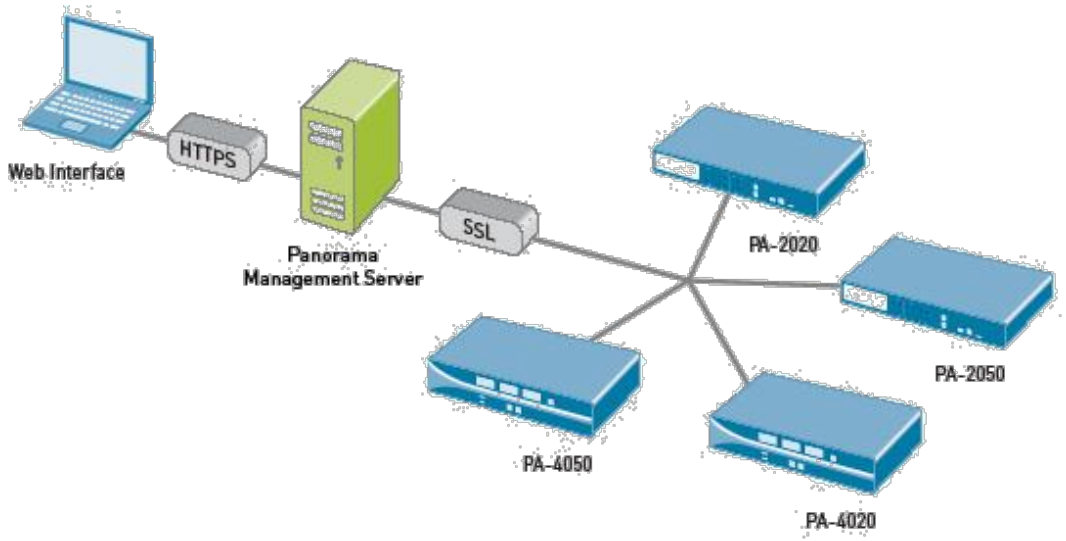


Misc HA

- How to configure Active/Passive HA in PAN-OS 4.x:
  Tech Note - HA Active Passive 4.0.pdf
- How to configure Active/Active HA in PAN-OS 4.x:
  Tech Note - HA Active Active 4.0.pdf
- HA failover can be triggered by the following three mechanisms:
  - Link failure
  - Path failure
  - Heartbeat loss
- Command to view the HA settings/status:
  - **`show high-availability state`**
- Upgrading a PAN-OS 3.1 HA cluster to PAN-OS 4.0
  https://live.paloaltonetworks.com/docs/DOC-1751
- If Pre-emptive mode is enabled, the firewall with the lowest priority setting will become master. Pre-emptive mode must be enabled on both firewalls.

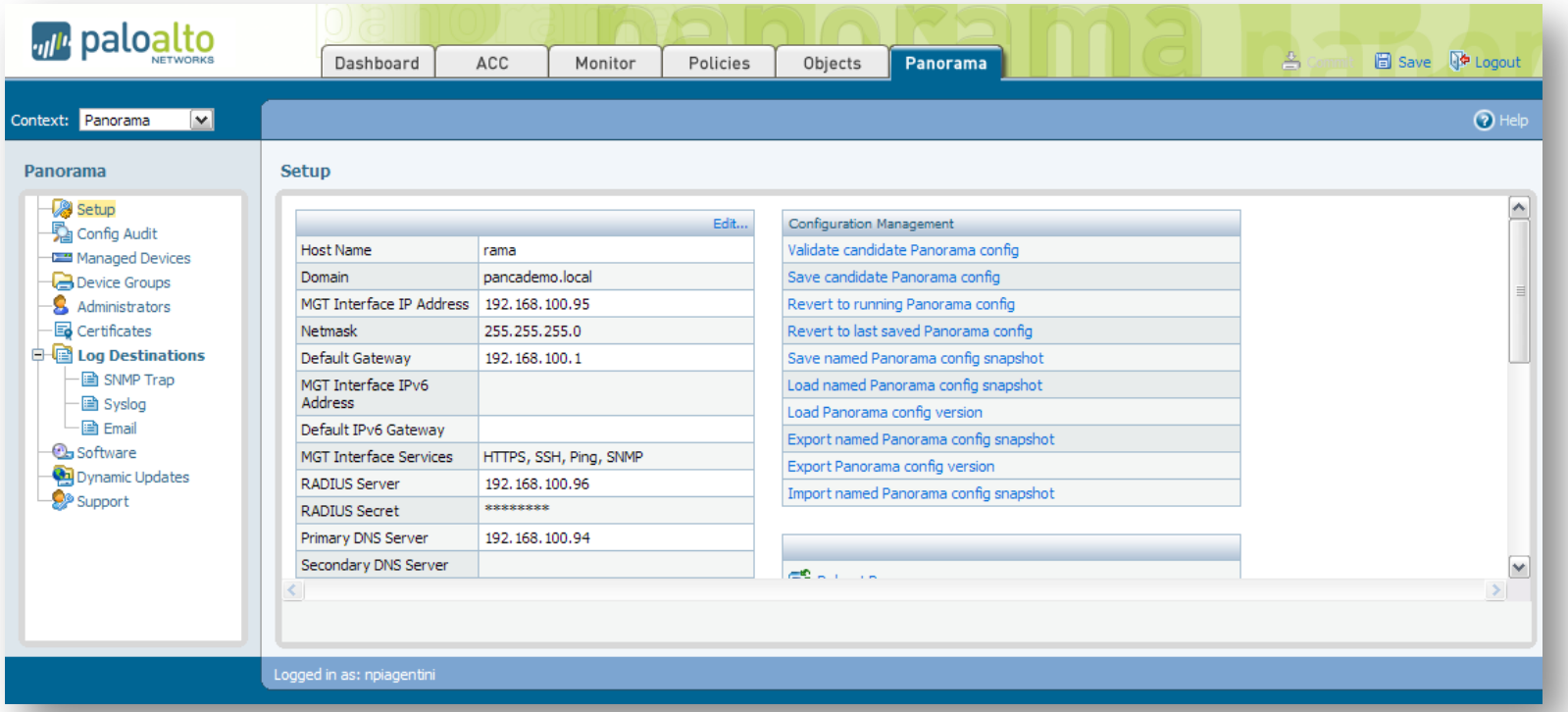
Panorama

- Central source to view log / report data, as well as to centrally manage the firewalls
- Virtual Appliance (on Vmware)
- Supports shared policies
- Connects to firewall using SSL
- Panorama is sold separately from the firewalls in 25/100/1000 license versions (licensed by firewall, not by virtual system)
- Firewalls are managed in Device Groups. Pre and post policies are pushed to Device Groups by selecting the appropriate Device Group/s as a “Target” when creating new rules within Panorama



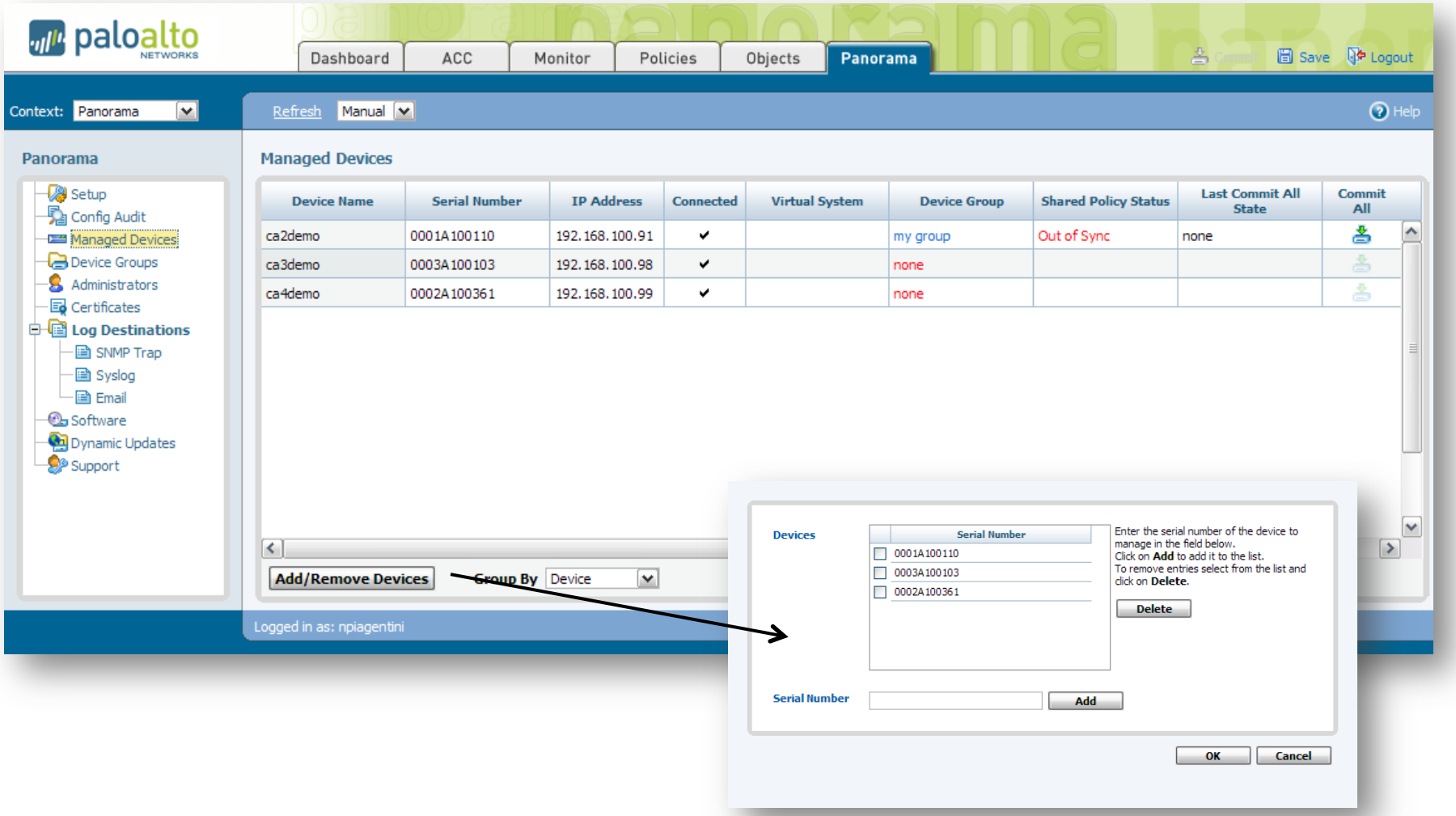
Panorama GUI

- Uses similar GUI as devices
- “Panorama” tab provides management options for Panorama



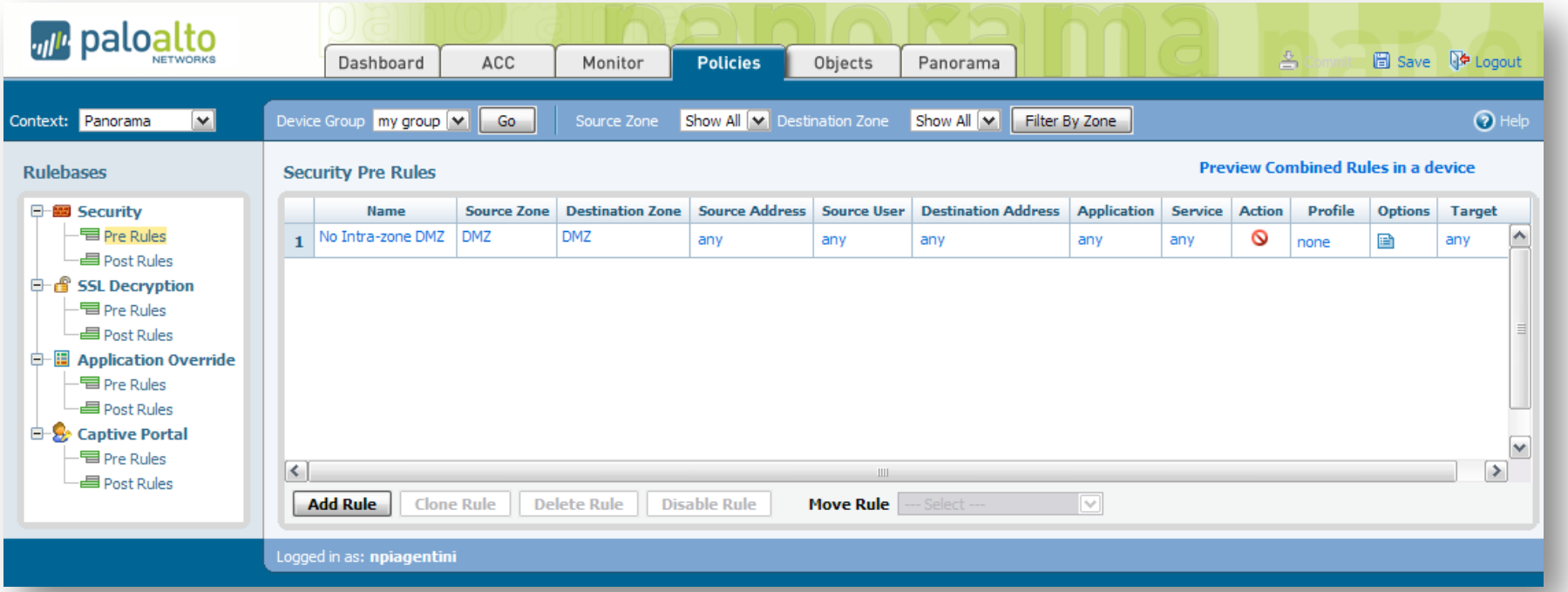
paloalto NETWORKS

Adding Devices to Panorama



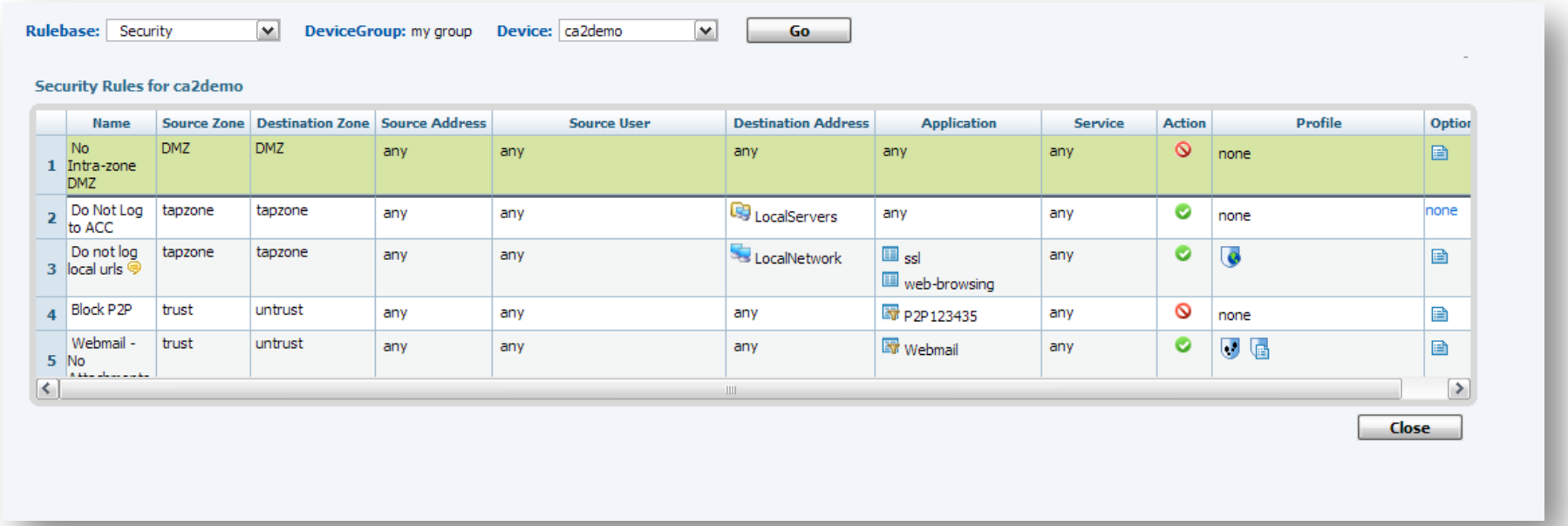
Shared Policy

- Rules can be added before or after device rules
  - Called pre-rules and post-rules
- Rules can be targeted to be installed on specific devices

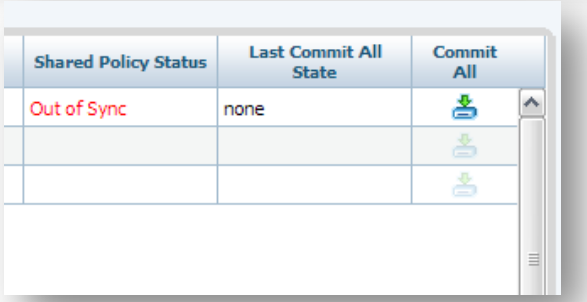


View and Commit

You can view a combined policy for any device



You can push policy changes via Panorama managed devices screen



Additional Notes on Panorama

- The firewall uses the config on the device itself. Panorama can store a backup copy of each firewall's config.
- The only thing that affects each firewall's config are the pre-rules and post-rules.
- When you make a change locally on the firewall, and that device is being managed by Panorama, you do NOT need to re-import the device, or synchronize the config between panorama and the firewall. The pre and post rules are still maintained on the firewall.
- The connection between a firewall and Panorama can be severed by selecting the "Disable Shared Config" option on the firewalls' Device tab.

Topics that have minimal or no questions

- Dynamic routing
- QoS
- Policy-based forwarding
- CLI commands (there will be questions testing the ability to read CLI command output, but not the commands themselves)