CNSE 5.1 Study Guide

Version 2.2

Palo Alto Networks

Education Services

paloalto NETWORKS

the network security company™

CNSE Study Guide & Tech Documents

Palo Alto Networks Education Services site:

- https://www.paloaltonetworks.com/services/education.html

CNSE 5.1 Study Guide download:

- https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/datasheets/education/5.1-cnse-study-guide.pdf

CNSE 5.1 Tech Documents download:

- https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/zip/5.1-cnse-tech-docs.zip

CNSE 5.1 Exam Overview

- Exam offered at Kryterion testing centers
- Register at this site:
  - http://www.webassessor.com/paloaltonetworks
- Review CNSE FAQs:
  - https://www.paloaltonetworks.com/services/education/cnse-faq.html
- Exam information:
  - Based on PAN-OS 5.0 and Panorama 5.1
  - 100 questions
  - 2.5 hours duration
  - 60% minimum passing score

Exam Preparation Suggestions

- Have skill and knowledge in these subjects:
  - Administration and Management
  - Network Architecture
  - Security Architecture
  - Troubleshooting
  - User-ID
  - Content-ID
  - App-ID
  - Panorama
  - GlobalProtect

PA appliances as of PAN-OS 5.0: 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

PA appliances as of PAN-OS 5.0: PA-3000 Series

A-3050

- 4 Gbps firewall throughput (App-ID enabled[1])
- 2 Gbps threat prevention throughput
- 500 Mbps IPSec VPN throughput
- 500,000 max sessions
- 50,000 new sessions per second
- 2,000 IPSec VPN tunnels/tunnel interfaces
- 2,000 SSL VPN Users
- 10 virtual routers
- 1/6 virtual systems (base/max[2])
- 40 security zones
- 5,000 max number of policies

PA-3020

- 2 Gbps firewall throughput (App-ID enabled[1])
- 1 Gbps threat prevention throughput
- 500 Mbps IPSec VPN throughput
- 250,000 max sessions
- 50,000 new sessions per second
- 1,000 IPSec VPN tunnels/tunnel interfaces
- 1,000 SSL VPN Users
- 10 virtual routers
- 1/6 virtual systems (base/max[2])
- 40 security zones
- 2,500 max number of policies

PA appliances as of PAN-OS 5.0: 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 5.0: PA-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

Centralized Management

M-100

The M-100 allows you to deploy Panorama management and logging functions on a dedicated appliance, or you can separate the functions in a distributed manner for improved performance and scalability.

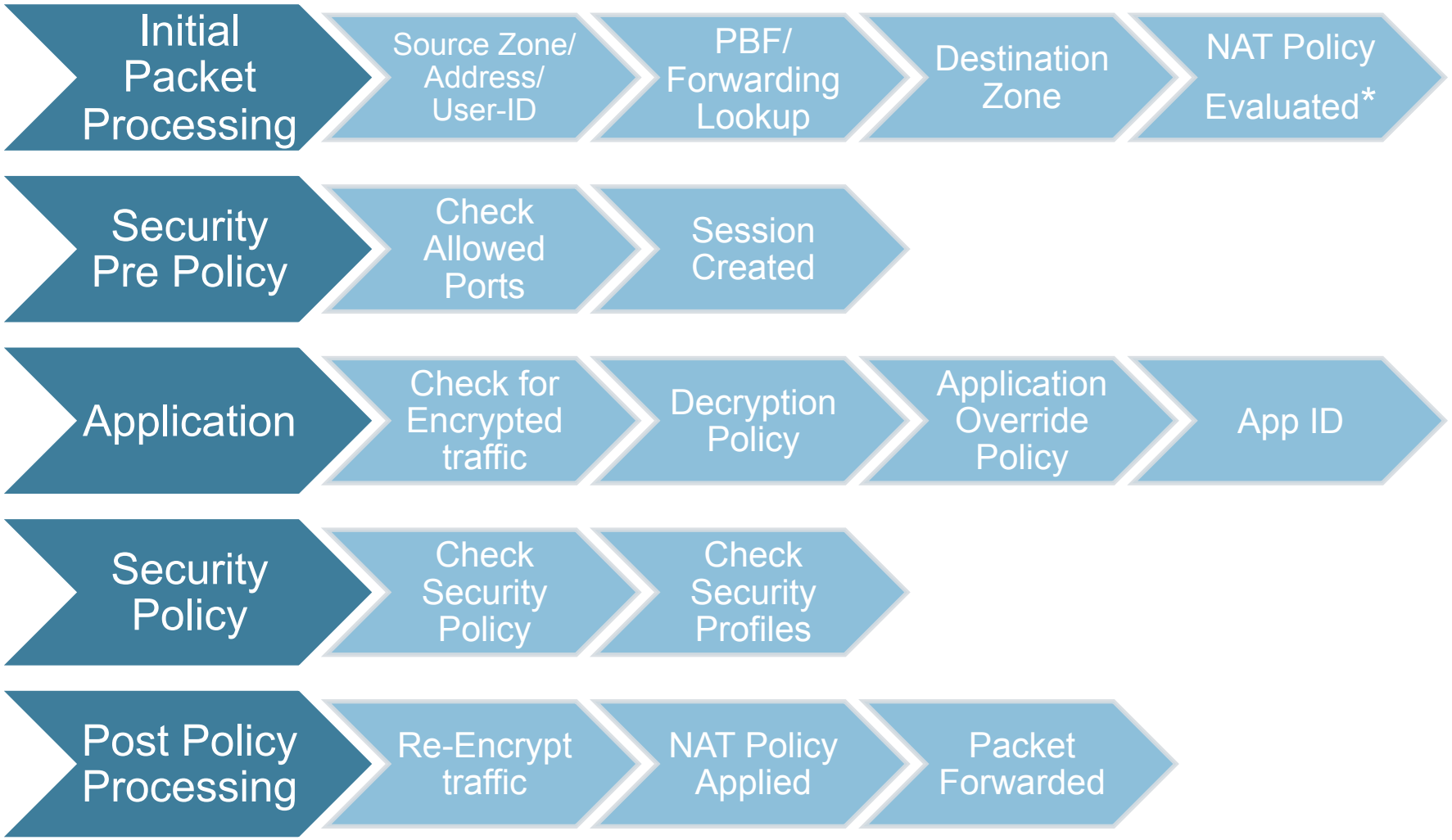
VIRTUAL APPLIANCE

You can deploy Panorama as a virtual appliance on VMware ESX(i), allowing you to support your virtualization initiatives and consolidate rack space.

Security Subscriptions

- Threat Prevention
- URL Filtering
- Global Protect
- WildFire

Flow Logic


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

Packet Flow

- Refer to this document on the packet flow in PAN-OS: 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
  - Application are indentified once a session is created on an allowed port

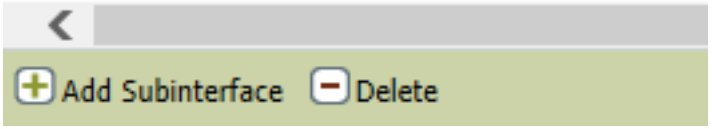
5 Physical Interface Types

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 address 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 operation available.
5. HA (on all devices except the 3000, 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 VLAN per system



- Aggregate interfaces (802.3ad)

PA-200	PA-500	PA-2000	PA-3000,4000,5000
Not Supported	4	6	8

  - Up to 8 physical 1 Gig interfaces can be placed into an aggregate group
  - Max Supported Aggregate group:
  - 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 5.0 for PIM-SM sparse mode and IGMP protocols
- Additional information can be found in the following support document:
  - PaloAltoNetworks-Designs-Guide-RevB.pdf

Available Features in Different Interface Modes

Vwire

- No VPN
- No “auto” setting for HA passive link

L2

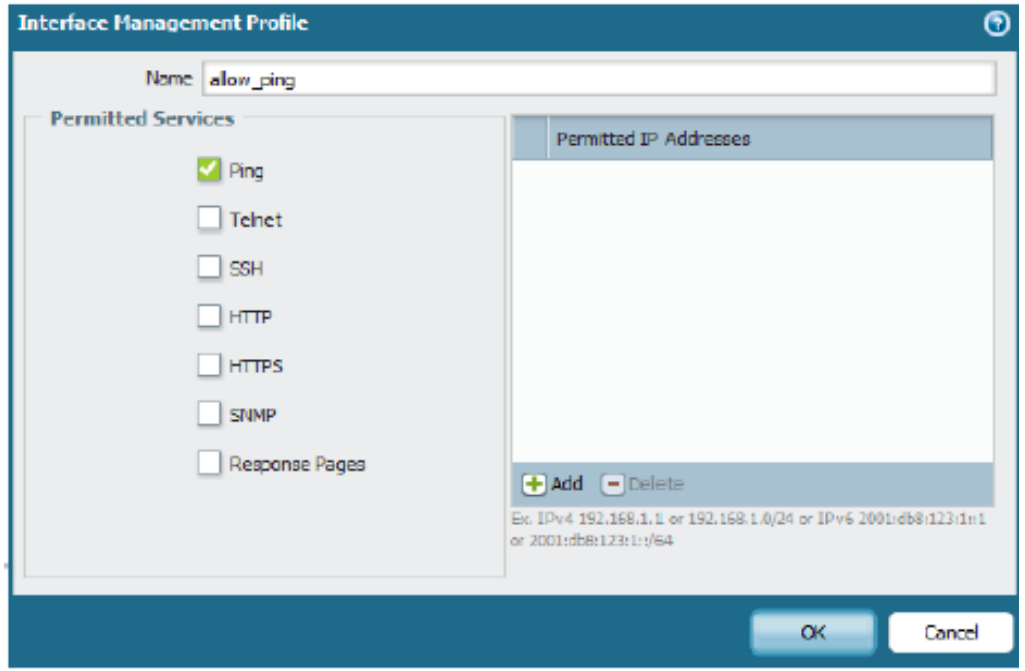
- No VPN
- No NAT (FYI Starting PAN-OS 4.1 you can do NAT in Vwire mode)
- If IPv6 is passing, security policies can be written for this traffic
- No Multicast support

L3

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

Interface Management

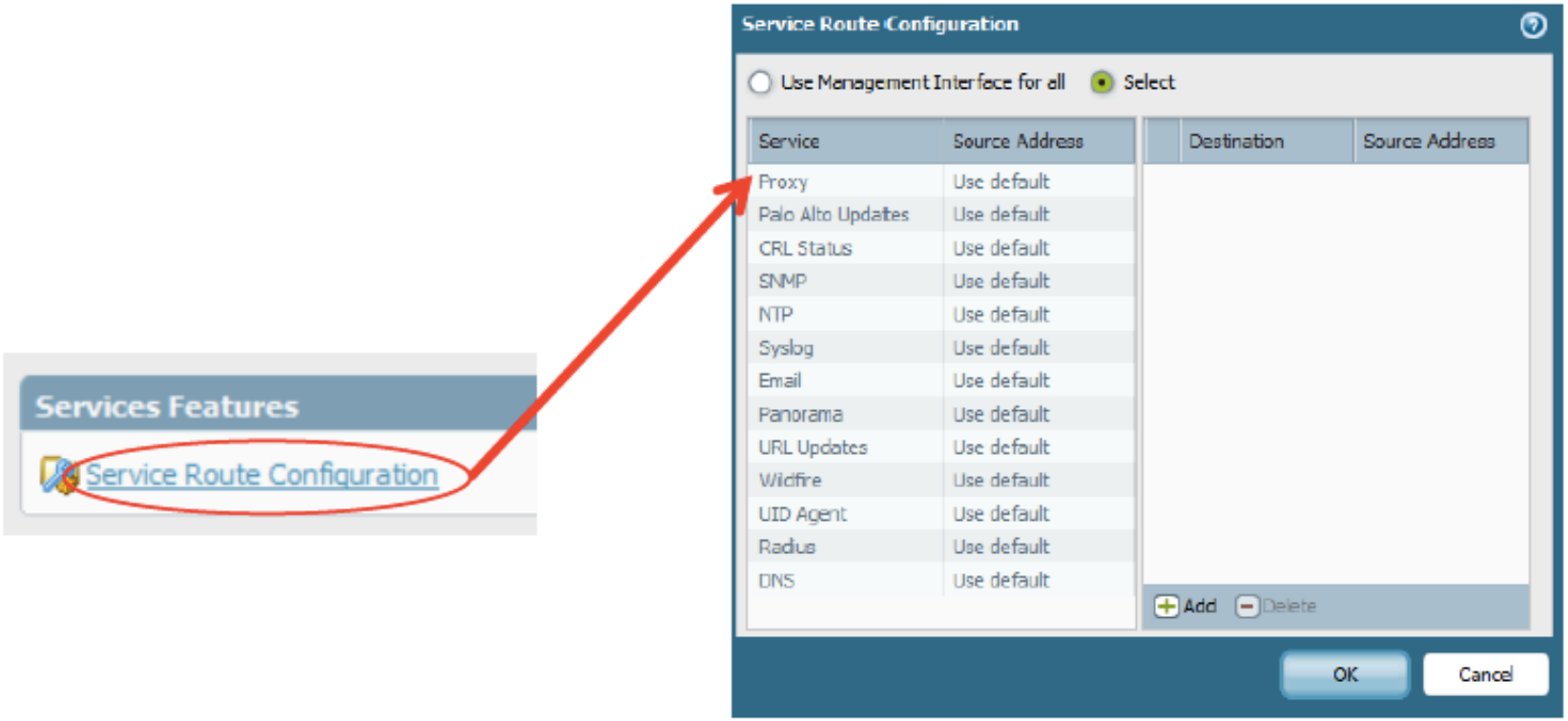
- An interface management profile specifies which protocols can be used to manage the firewall
- Management profile can be assigned to :
  - L3 interfaces
  - Loopback interfaces
  - VLAN interfaces



- Configured under
  - Network tab -> Network Profile -> Interface Management

Device Management

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



Role-based Administration

- Administrator can be given rights using the built in option or by creating new administrative roles
- There are 6 pre-defined administration 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 system 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.

Application Identification

- App-ID provides the ability to identify application 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 application such as the proprietarily-encrypted BitTorrent and UltraSurf are indentified

- App-ID even works in these scenarios:

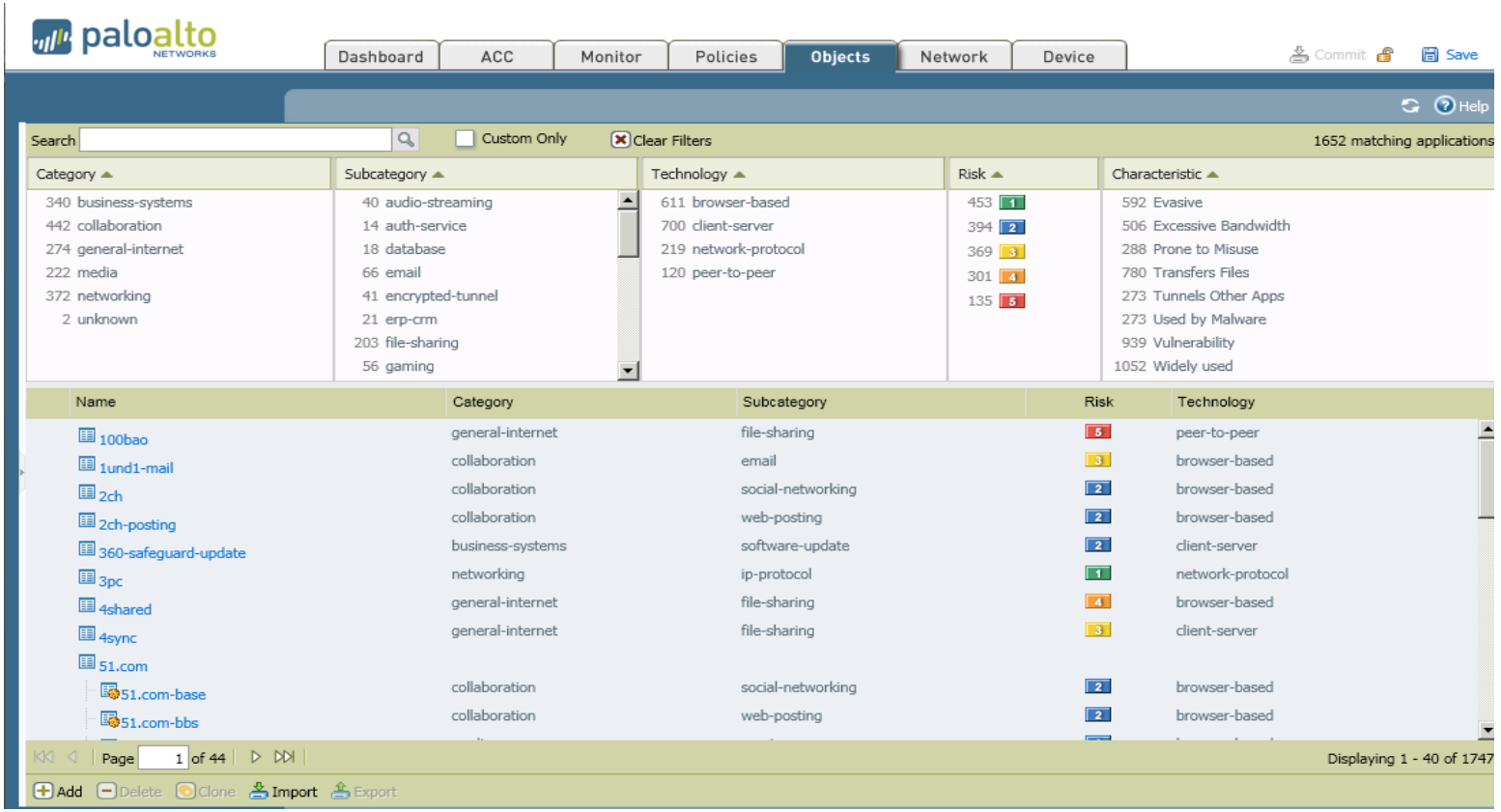
  - If the application is running on a different port than expected

  - 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

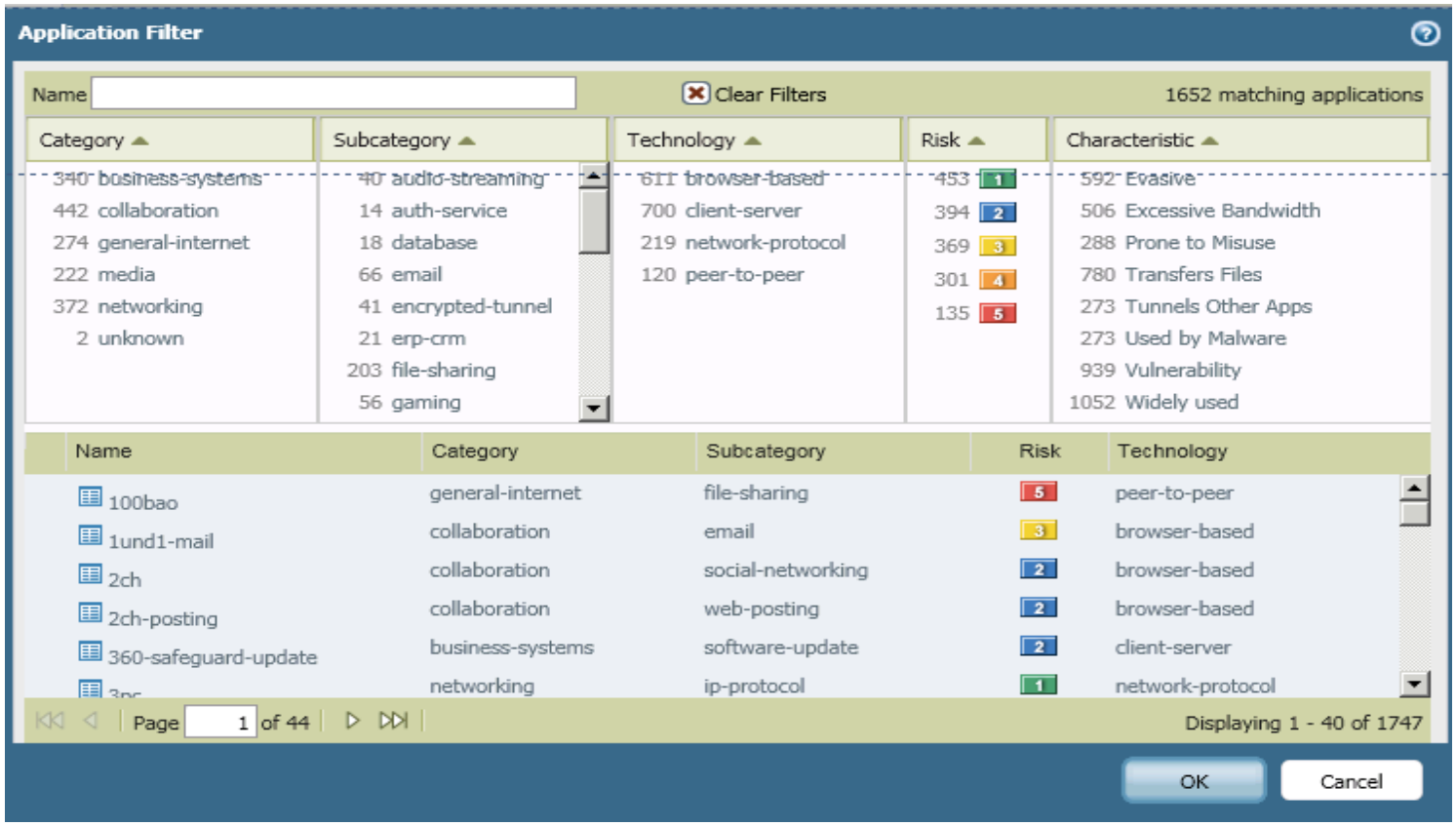
Application Selection Window

Within each policy, you can specify what applications you want to control. You can specify individual applications, or group 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

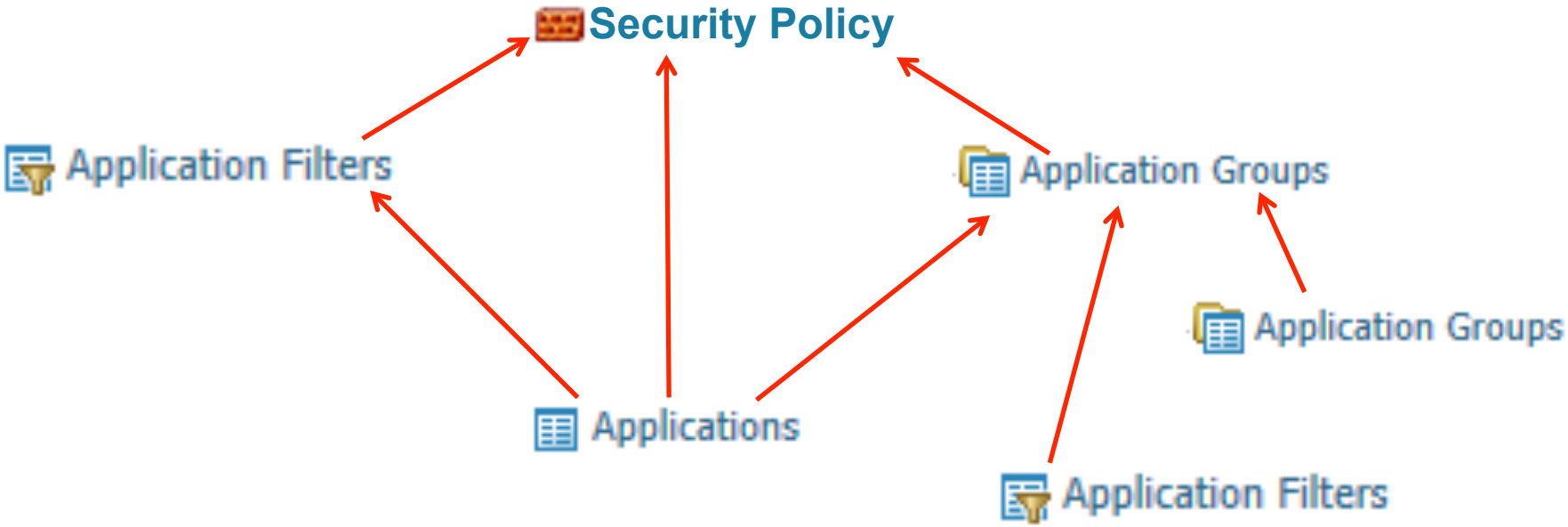
- A dynamic application filter is configured by specifying particular criteria.
- The example below is a dynamic filter to all browser-based file-sharing apps.



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

Application Group and Application Filters

- Application Group are static. Application are manually added and maintained by firewall administrators.
- Application Filters are dynamic. Application 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

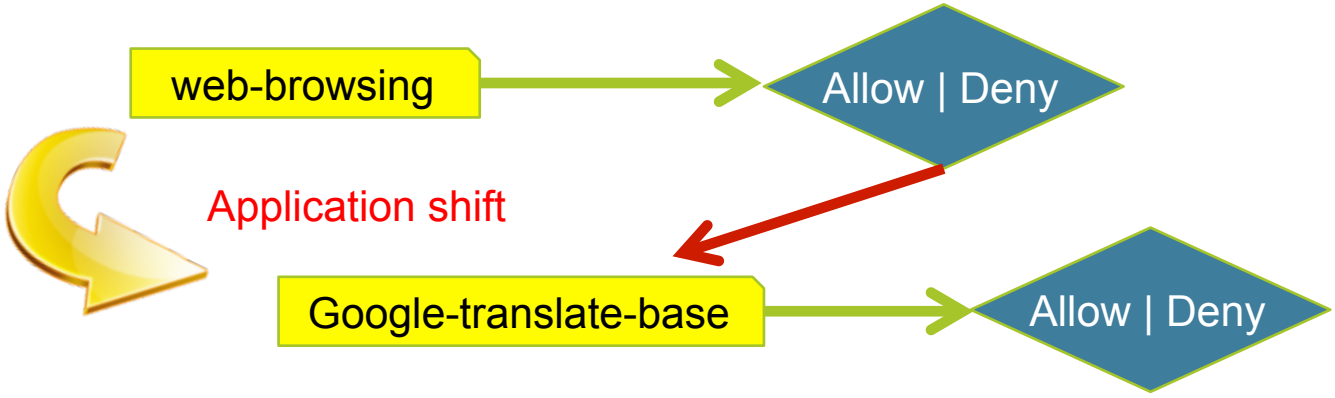
- All traffic following from one security zone to another requires a policy to allow the traffic
- The policy list is evaluated from the top down
- The first rule that matches the traffic is used
- No further rules are evaluated after the match

	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)

Security Policy Dependencies

Parent applications must also be allowed by security policy for the dependent applications to function.



Application

Name: web-browsing

Description: Web Browsing is using Hype
the World Wide Web. Its ori

Additional Information: Wikipedia Google Yahoo!

Standard Ports: tcp/80

Depends on Applications:

Application

Name: google-translate-base

Description: Google Translate is a service provided
rule-based analysis. Languages writter
automatically from phonetic equivalent

Additional Information: Wikipedia Google Yahoo!

Standard Ports: tcp/80

Depends on Applications web-browsing

Implicit Application Dependencies

PAN-OS implicitly allows parent applications for a set of commonly used applications

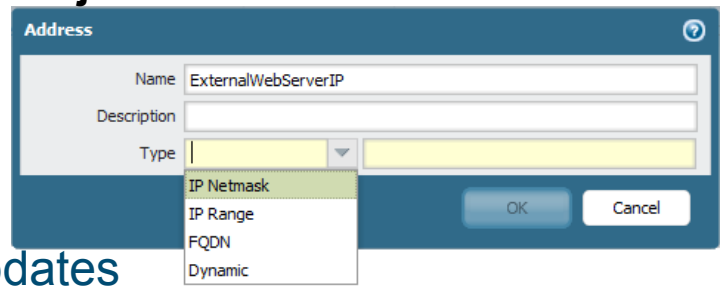
	Source			Destination					
Name	Zone	Address	User	Zone	Address	Application	Service	URL Category	Action
Allow Facebook	Trust-L3	any	any	Untrust-L3	any	facebook-base	application-default	any	✓
Allow WebBrowsing	Trust-L3	any	any	Untrust-L3	any	web-browsing	application-default	any	✓

In this example, Facebook access will work even if the **Allow WebBrowsing** policy were removed.

Address Objects & Dynamic Block Lists

- Address Object - Available types:
  - IP Netmask, IP Range, FQDN
  - Dynamic (New in 5.0)

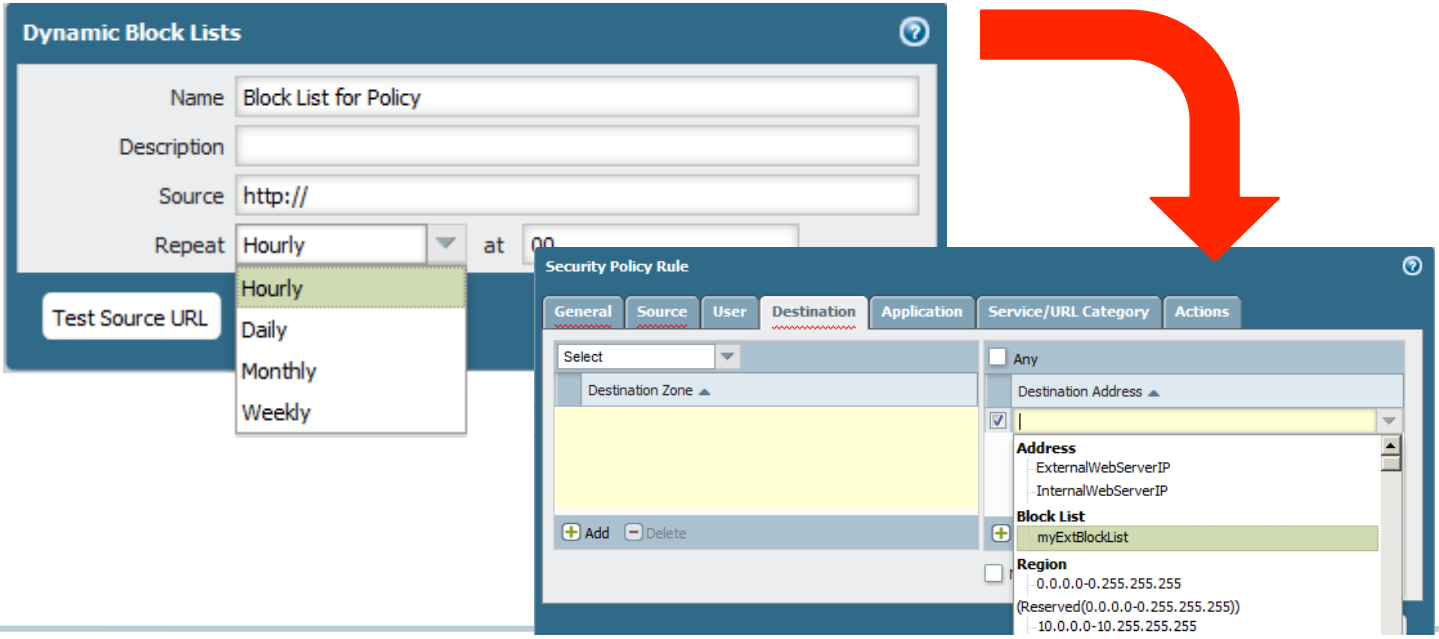
Objects > Addresses



- FQDN type changes automatically if DNS entry updates

- Allows the import of external lists of URL/IP block lists

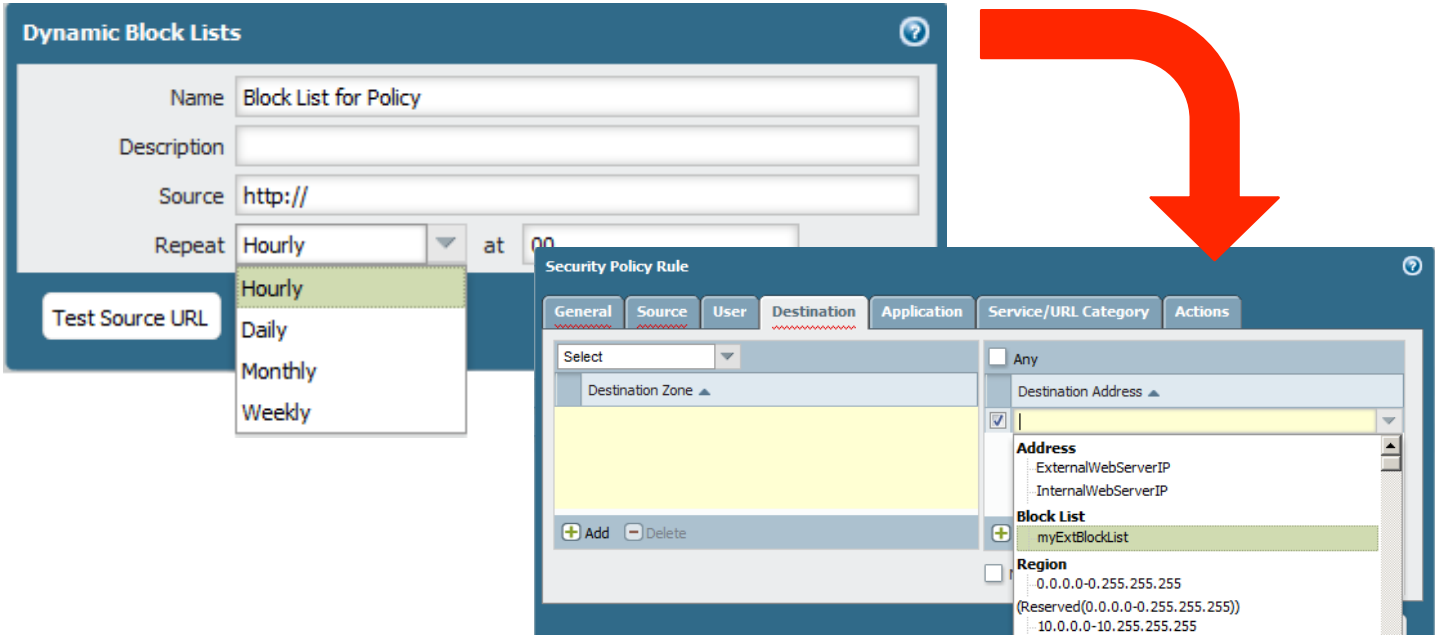
Objects > Dynamic Block Lists



Dynamic Block Lists

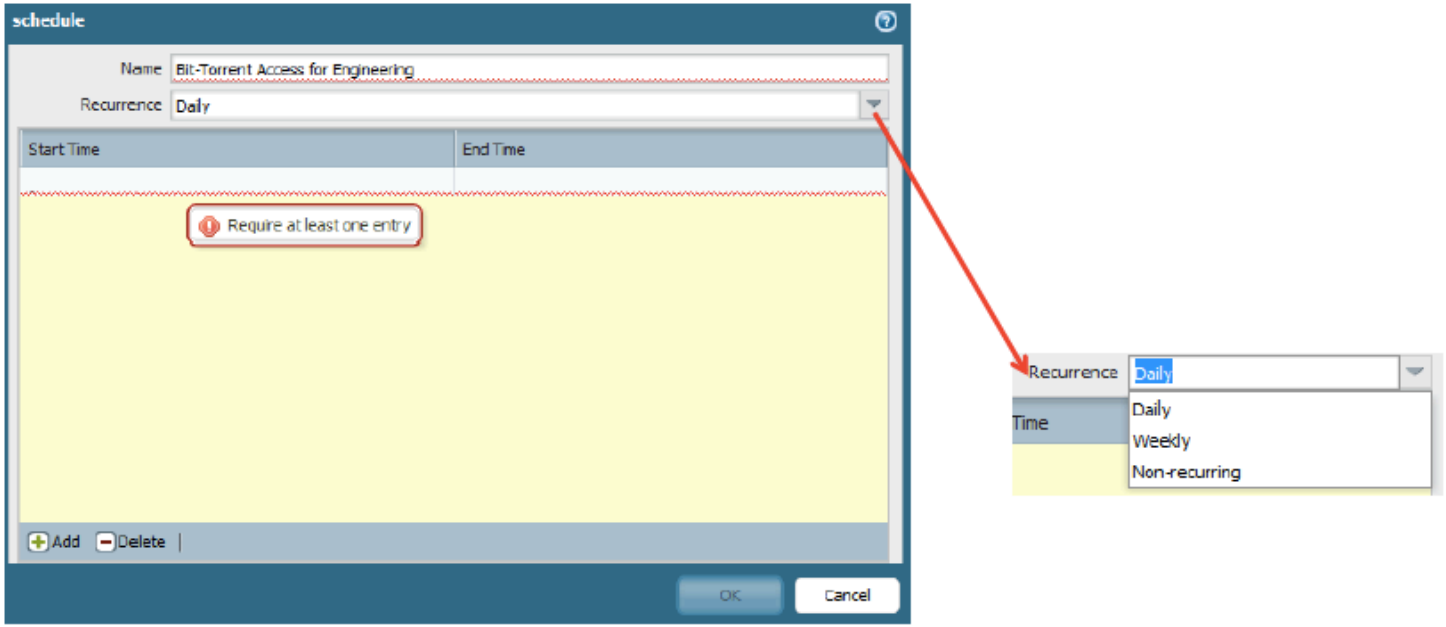
Allows the import of external lists - URL/IP block lists

Objects > Dynamic Block Lists



Scheduling Security Policies

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



- Possible schedule choices:
- Schedule are assigned under Policies tab -> Security Policy-> Option column

Blocking Skype

- The skype application is classified on the PAN device as two separate application: 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	⊘

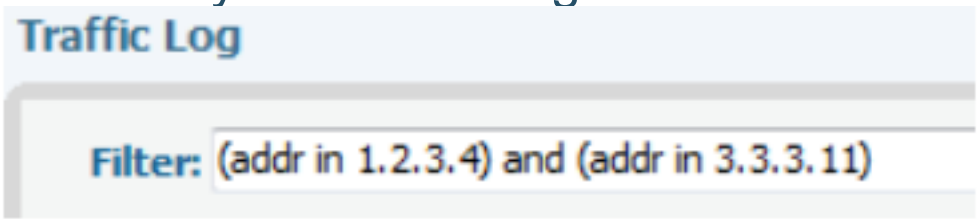
Monitoring Traffic

- 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.

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 3.3.3.1.1:



Monitoring Traffic (2)

Special Application names are used to define traffic not explicitly indentified by App-ID. (See https://live.paloaltonetworks.com/docs/DOC-1549) These will be displayed in the Traffic log as follows:

- "incomplete"
  - TCP 3-way handshake did not complete
  - TCP 3-way handshake did complete but no packets afterward
- "insufficient-data" means that either :
  - Not enough packets were seen to identify the application
- "unknown-tcp"

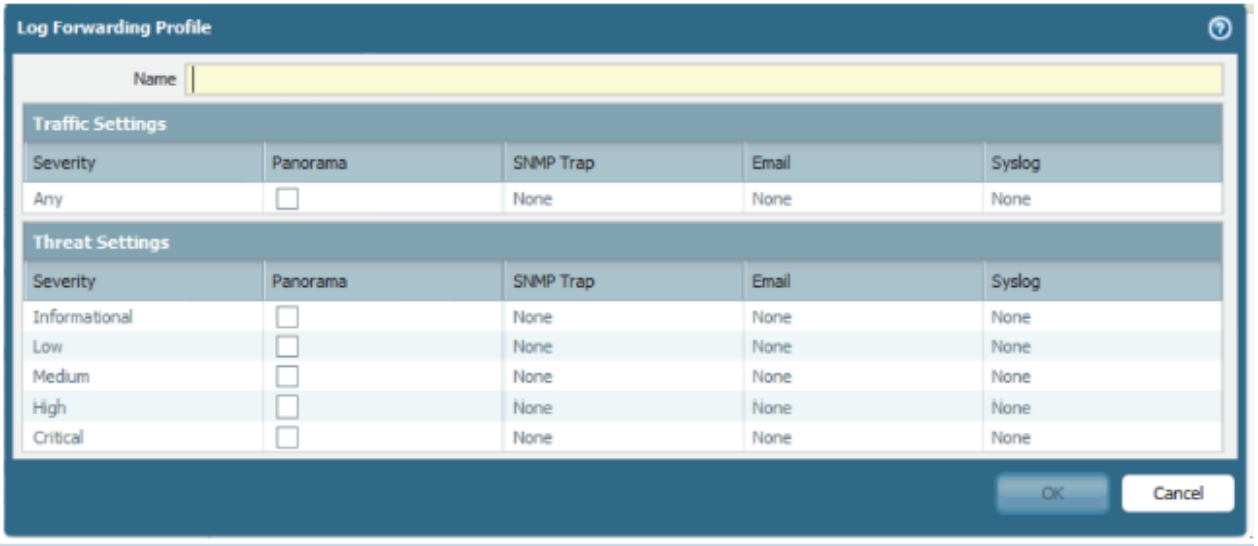
  -Application consist of unknown tcp trafic.
- unknown-udp"

  -Application consist 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 location. Upon generation of a log message, that message can be immediately forward to :
  - Syslog server
  - SNMP manager
  - Email
  - Panorama
- You configure the log message destination via a Log Forwarding Profile:



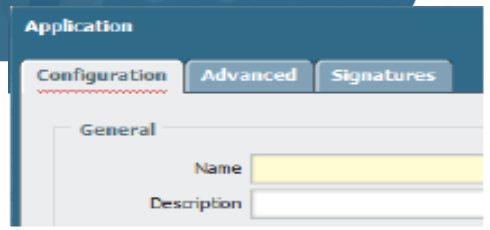
Unknown Applications

- 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	8000	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

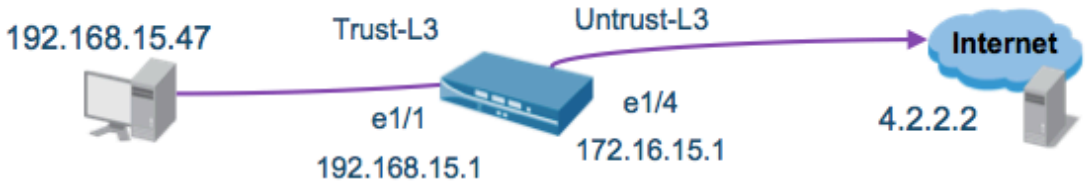
	Source			Destination				
Name	Zone	Address	User	Zone	Address	Application	Service	Action
IT Allow Override	trust	any	impressive\a...	untrust	any	Custom-app	any	✓

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



Policies > NAT

	Original Packet						Translated Packet	
Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
Source NAT	Trust-L3	Untrust-L3	any	any	any	any	dynamic-ip-and-port ethernet1/4	none

Source	Destination
192.168.15.47	4.2.2.2

Translation

Source	Destination
172.16.15.1	4.2.2.2

Policies > Security

	Source				Destination				
Name	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
Internet Usage	Trust-L3	192.168.15.0/24	any	any	Untrust-L3	any	any	any	✓

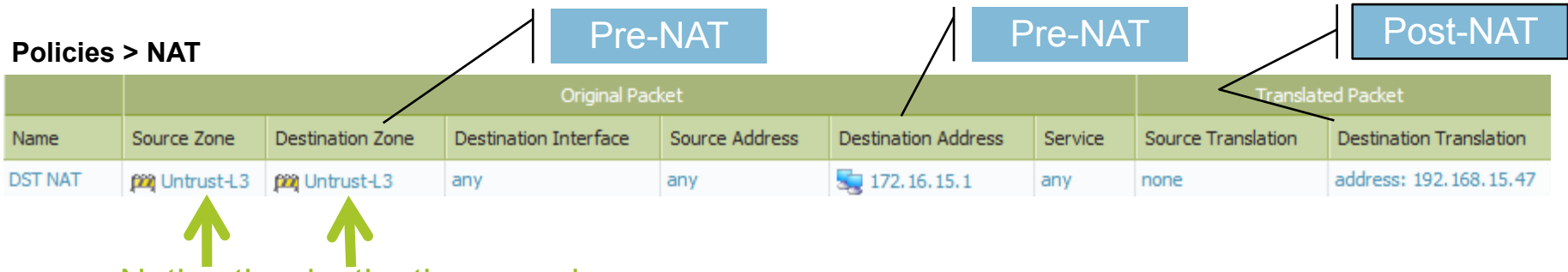
NON-translated address

Destination Address Translation

Refer to Slides Notes for scenario details

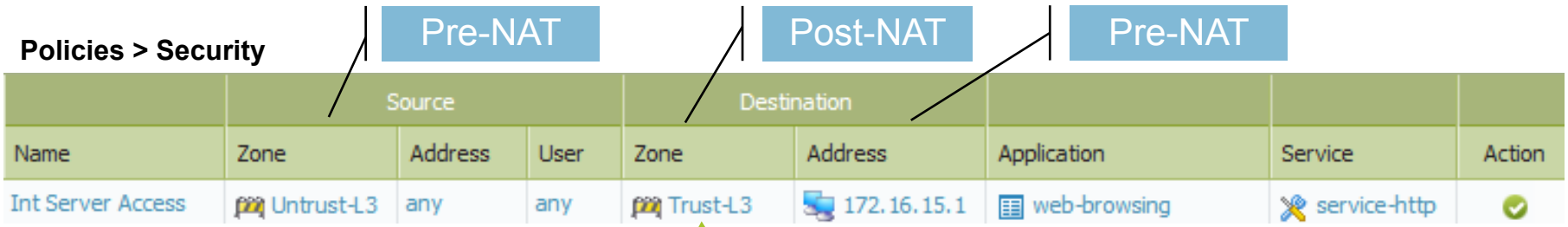
Source	Pre-NAT Destination	Post-NAT Destination
65.124.57.5	172.16.15.1	192.168.15.47
Untrust-L3	Untrust-L3	Trust-L3

Policies > NAT



Notice the destination zone is same as source zone

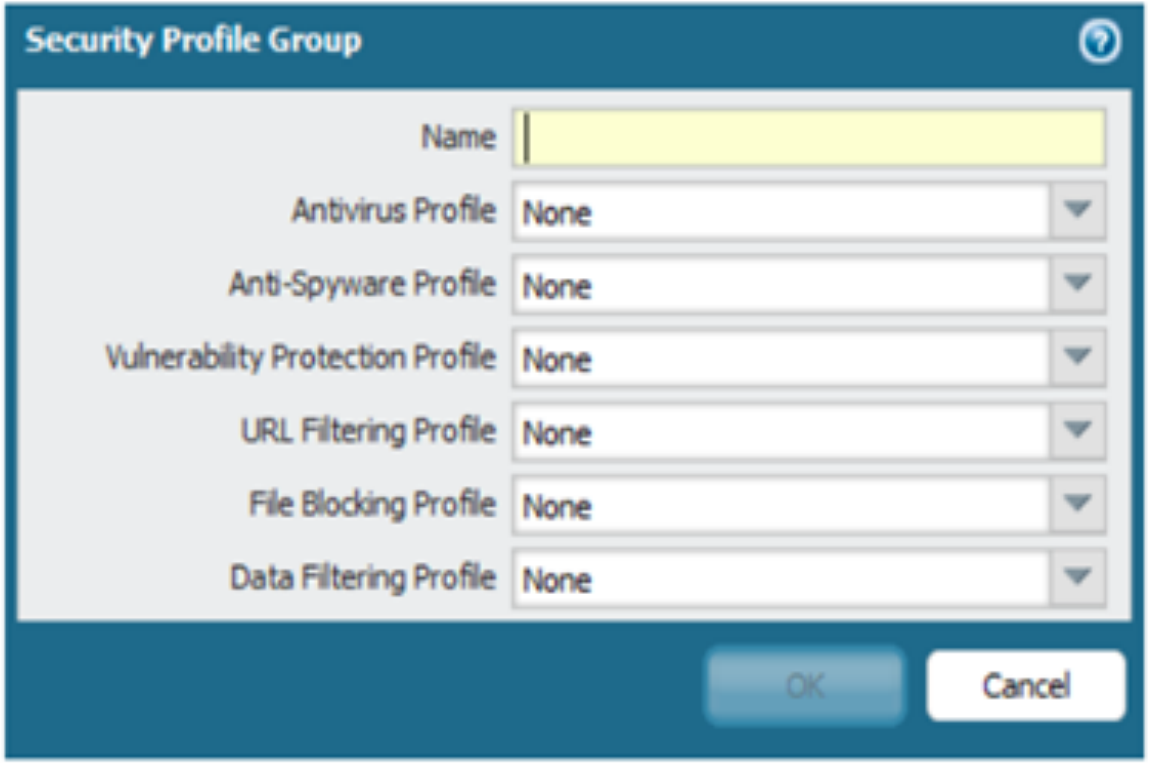
Policies > Security



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

Security Profile

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



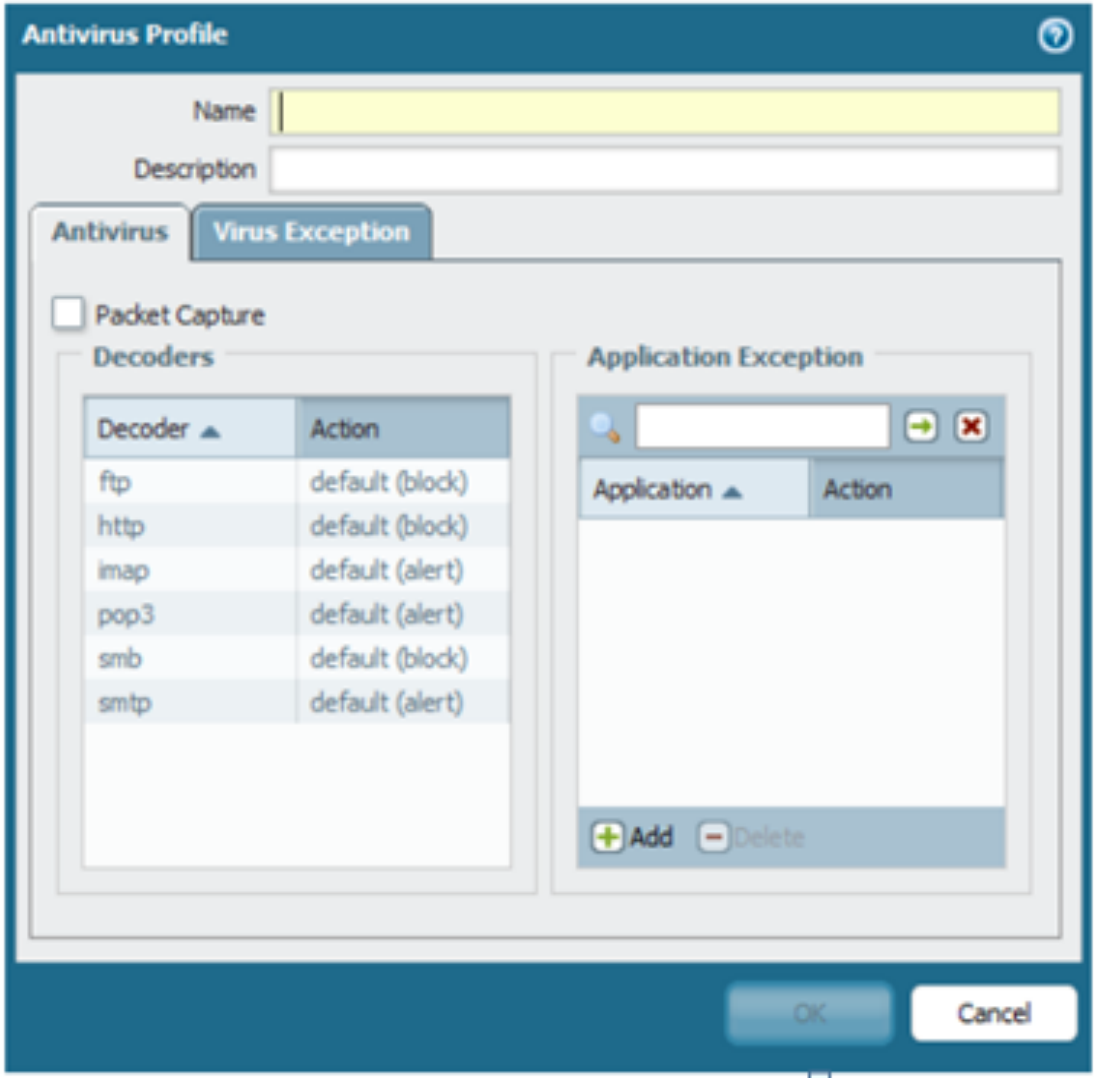
Using Security Profiles

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

	Source			Destination					
Name	Zone	Address	User	Zone	Address	Application	Service	Action	Profile
RestrictYouTube	Trust-L3	any	any	Untrust-L3	any	youtube	application-default		
Disable-FB	Trust-L3	any	...	Untrust-L3	any	facebook-base	application-default		none
General Access	Trust-L3	any	any	Untrust-L3	any	any	any		

- Disable-FB: App-ID block FaceBook for Student users , no URL filtering profile
- General Access: All other users, URL filtering to specific FaceBook URL's

Anti – Virus Profiles



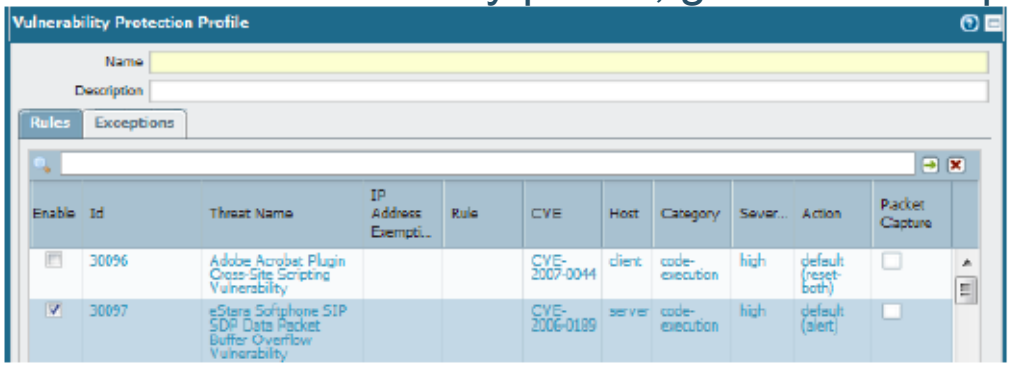
- A decoder is a software process on the firewall that interprets the protocol.
- In the antivirus and anti-spyware security profiles, you can specify actions based upon the 6 main decoders in the system, shown to the left.

Configuring Exceptions

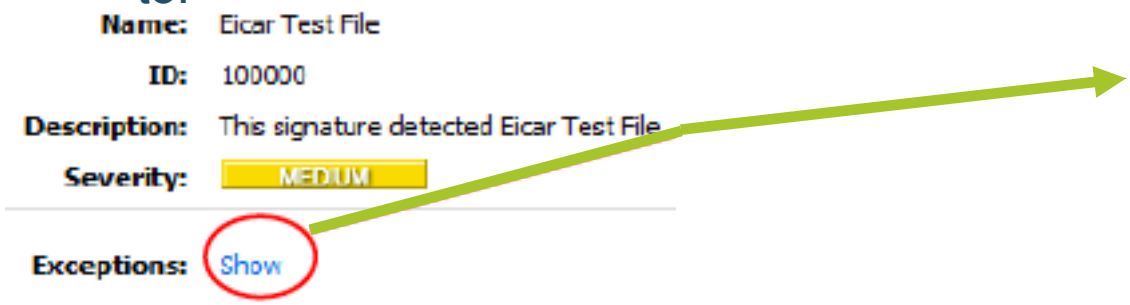
- If you have a threat or virus that you do not want to be detected, you can configure an exception

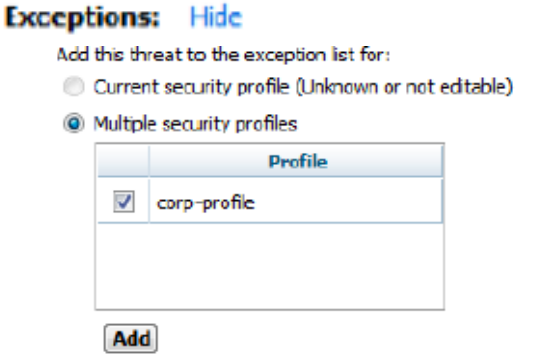
- Two ways to configure an exception:

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.



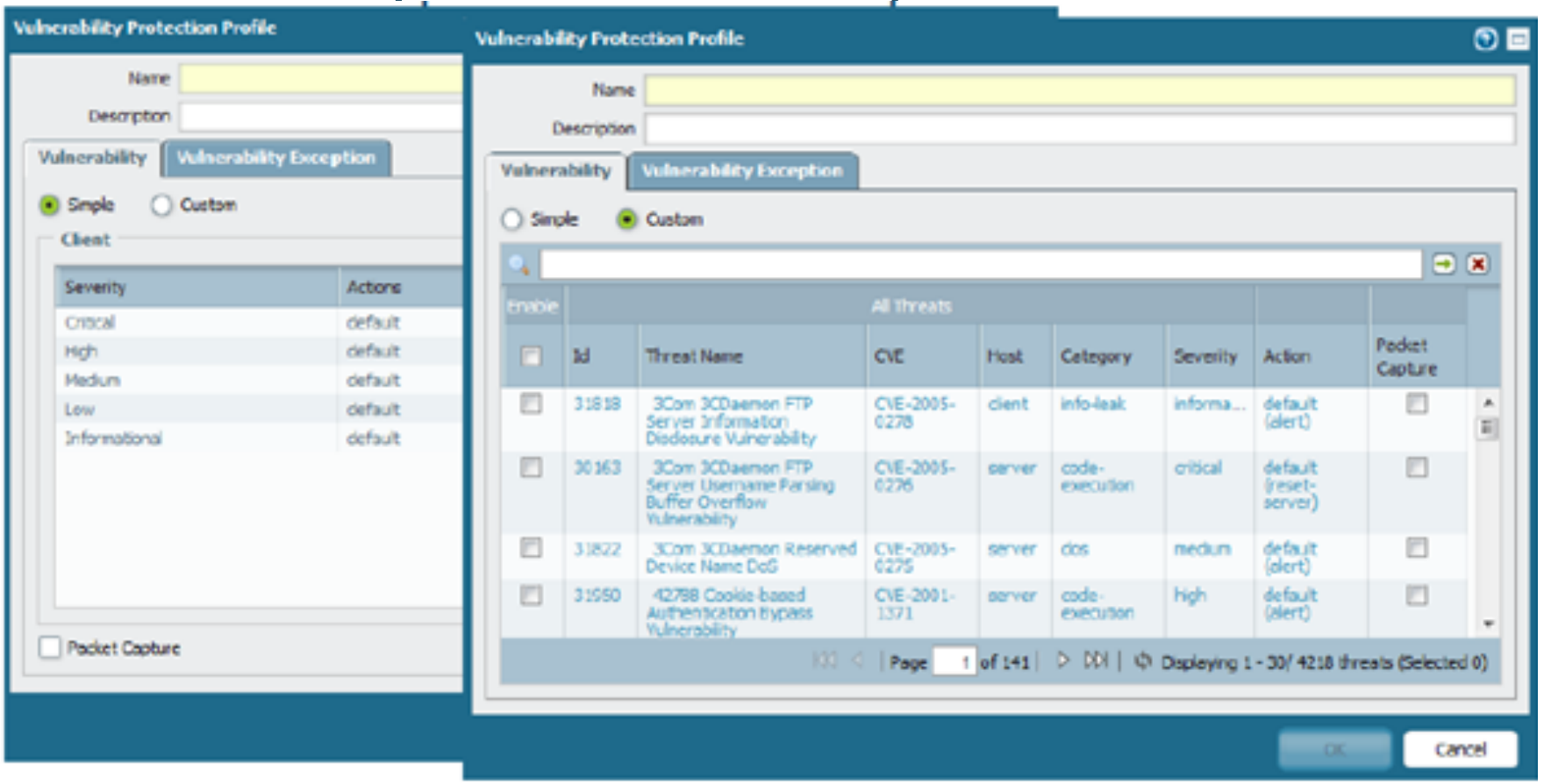


Email Protocols and AV/Spyware Protection

- 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 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

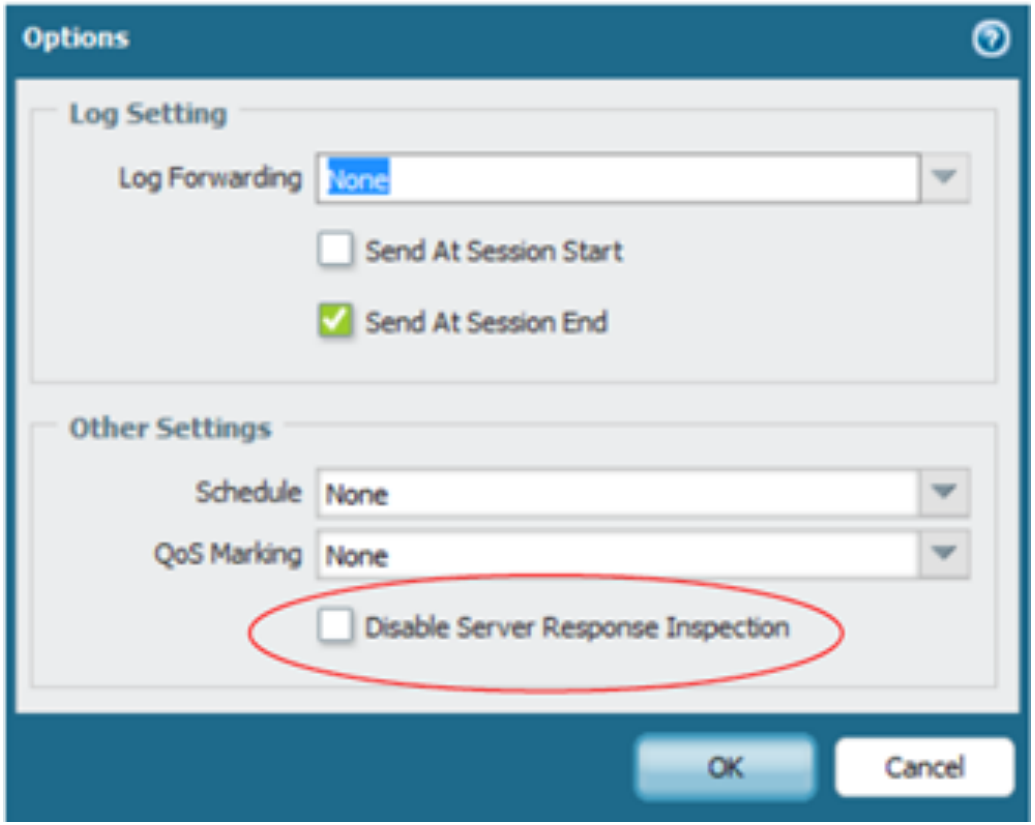


Custom Response Pages

- 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 application
    - Thus if a threat is detected during say a BitTorrent session, the response page will not appear
- Response Pages for web-based application are not enabled by default

Disable Server Response Inspection

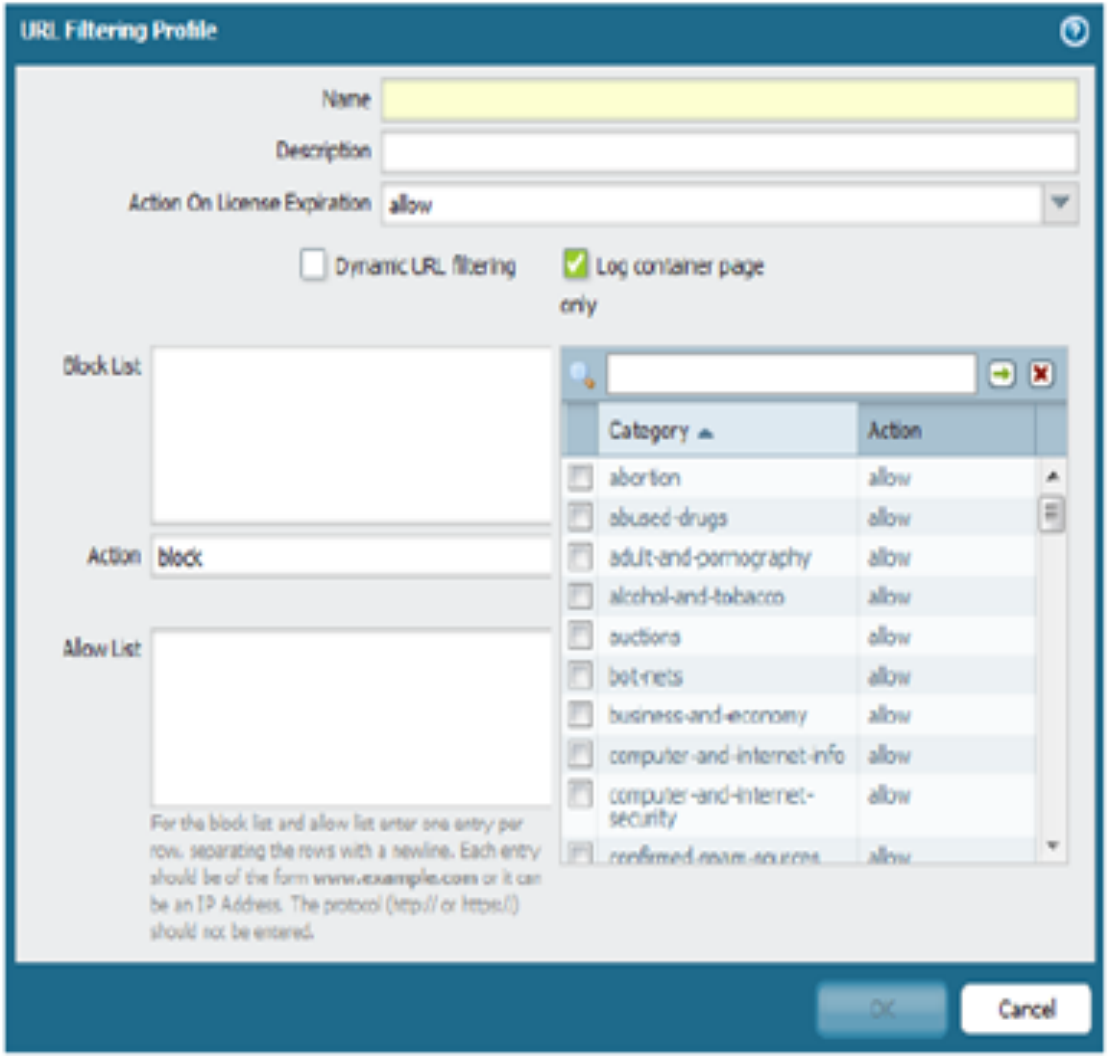
- The vulnerability protection profile by default scans traffic going in both directions (from client to server, and from server to client)
- Most IPSs only examine the traffic from the client to server.
- The way to examine traffic from only client to server on the Palo Alto firewall is to check the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

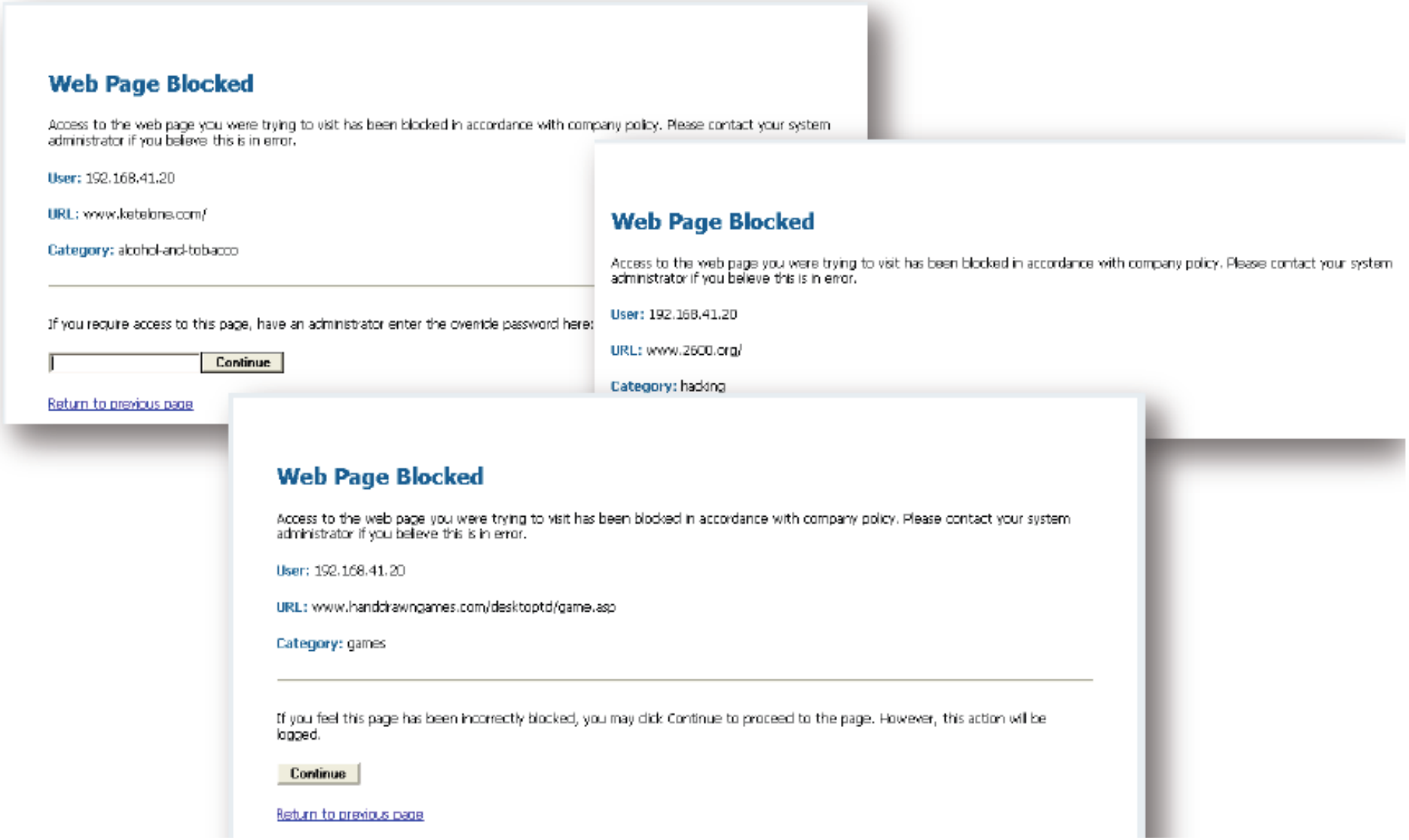
• Upon URL license expiration, URL database is no longer used; traffic is allowed or blocked based upon the “action on license expiration” field shown here.



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



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 sting is assigned a weight
- Alert threshold and block threshold is based upon weights

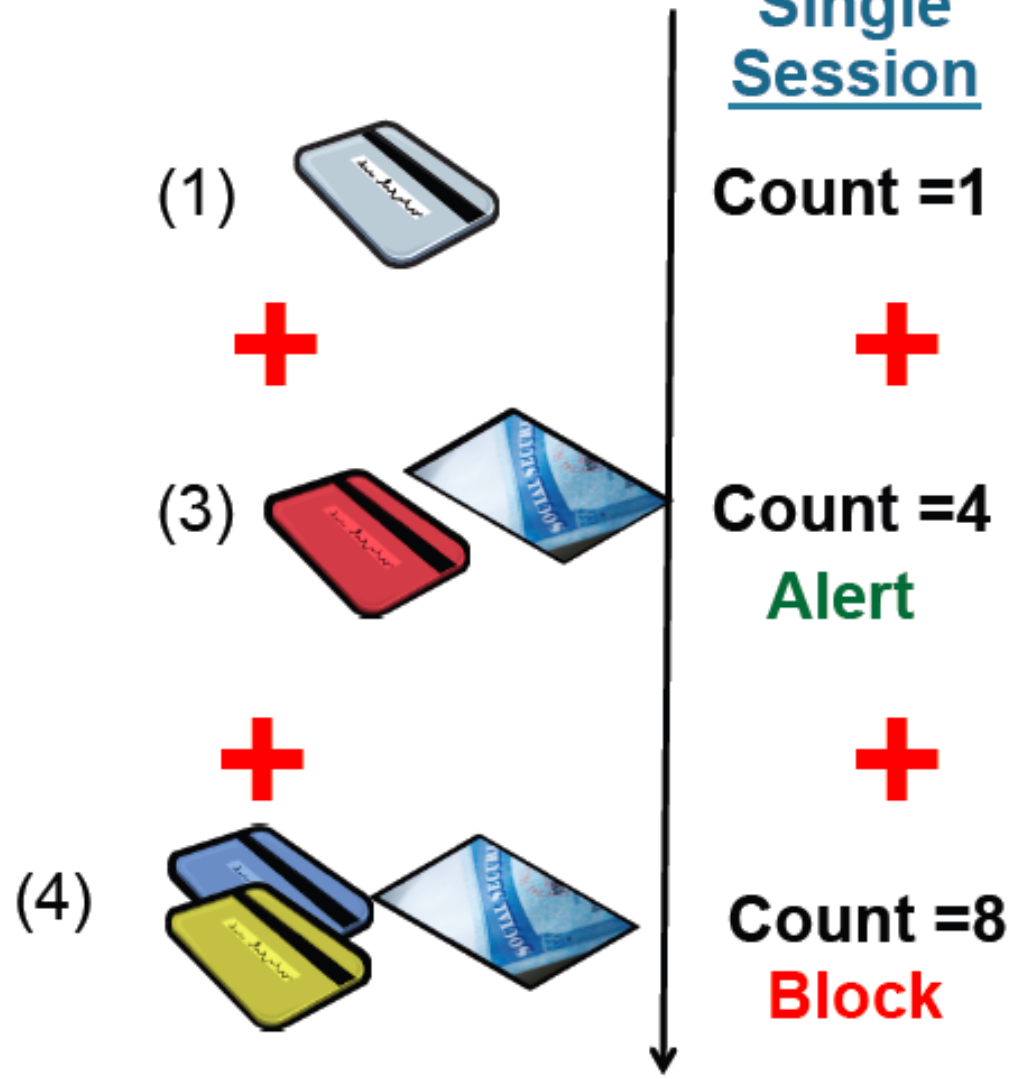
Data Filtering Example

Credit Card Weight = 1

SSN Weight = 2

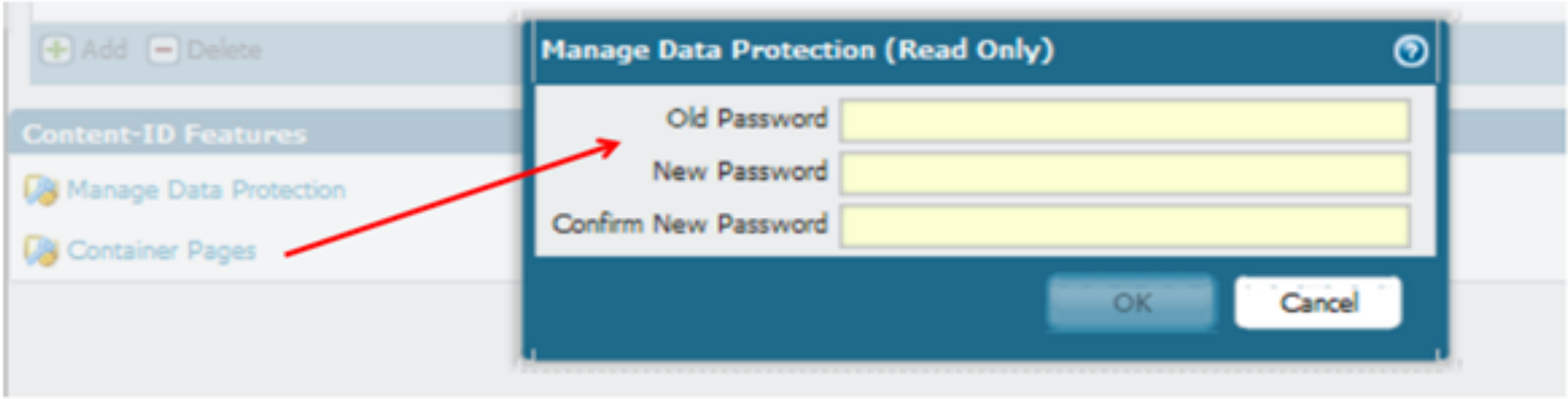
Alert Threshold = 4

Block Threshold = 8



Data Filtering Password Setup

- PCAPs on data filters requires 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



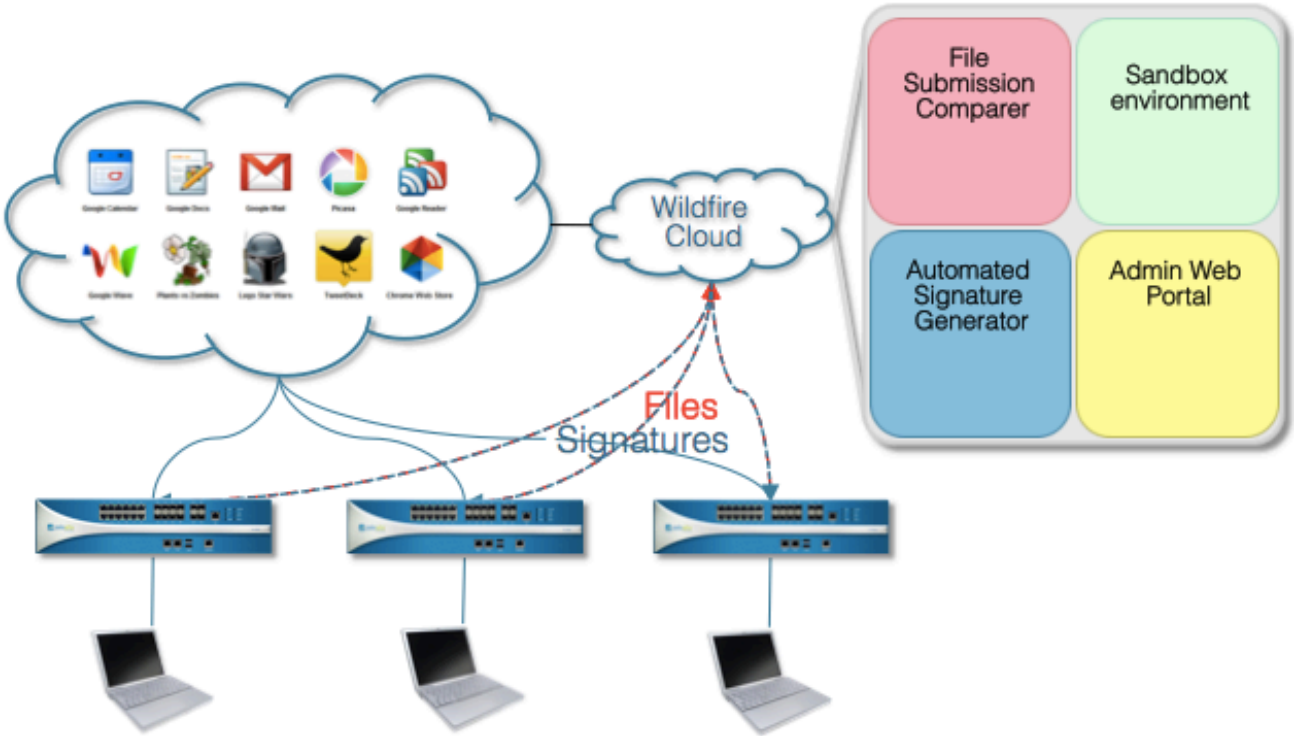
Zone Protection

- 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 againts SYN, ICMP, UDP, and other IP-based flooding attacks.
  - Reconnaissance detection – Allows you to detect and block commonly used ports 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.
- Configure under Networks tab -> Networks 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	✔		✔	✔		✔	✔	

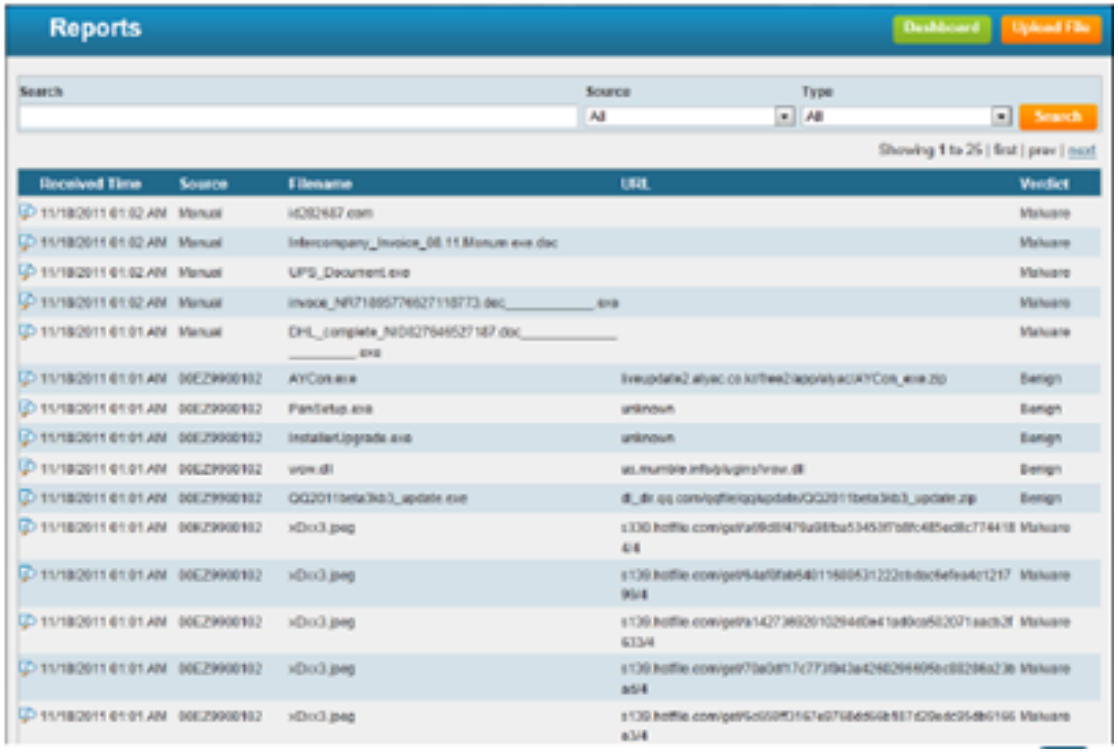
WildFire

- 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

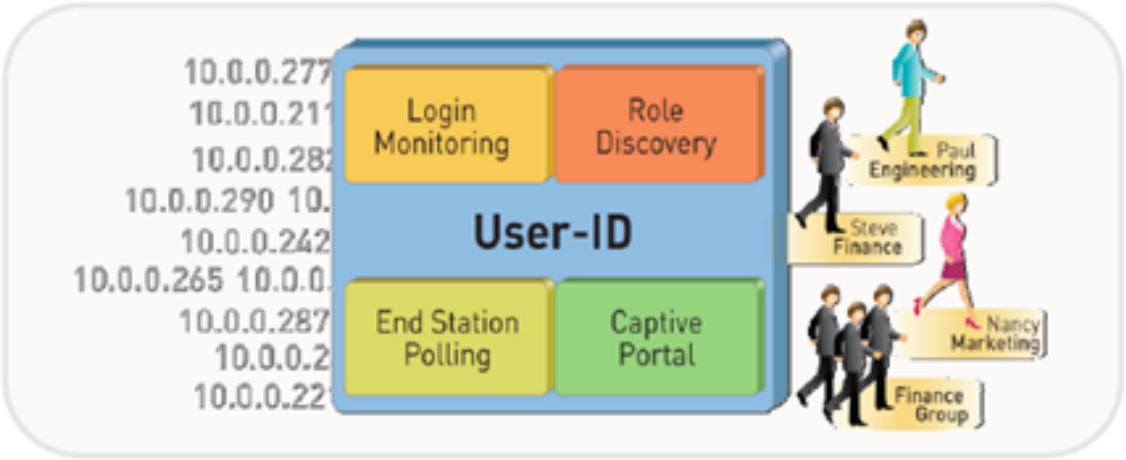


WildFire

- Provides a virtual sanbox environment for Window PE files
- A hash of each file is sent to the WildFire cloud. If no existing signature exist, 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



User-ID: Enterprise Directory Integration



- User no longer defined solely by IP address
  - Leverage existing Active Directory or LDPA 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

Where are Usernames Used?

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

To Zone	Source	Source User	Destination	Port	Application
Untrust-L3	76.103.241.215		10.154.7.14	80	web-browsing
Untrust-L3	10.154.12.204	pancademo\mary.kaler	123.138.239.140	80	qq-base
Untrust-L3	66.27.82.52		10.154.7.14	443	ssl
Trust-L3	10.154.13.15	pancademo\gerald.morales	74.86.161.118	80	web-browsing

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

Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application
CEO Apps	none	trust	any	pancademo\epasquarella	any	untrust	any	CEO Apps
Allow IT Remote Access	none	trust	EmailServer	pancademo\administrators	any	untrust	any	IT Remote Acce
Control Finance Web Po	none	trust	any	pancademo\finance	any	untrust	any	Web Posting

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

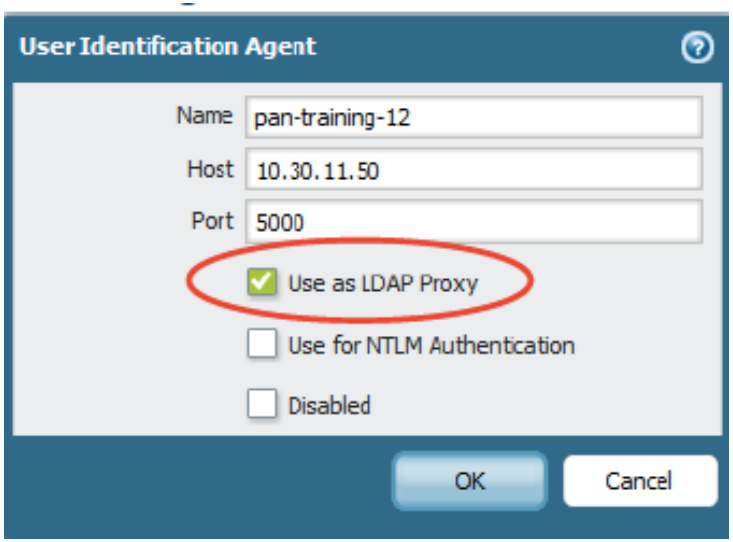
User-ID Agent Setup and Upgrade Procedure

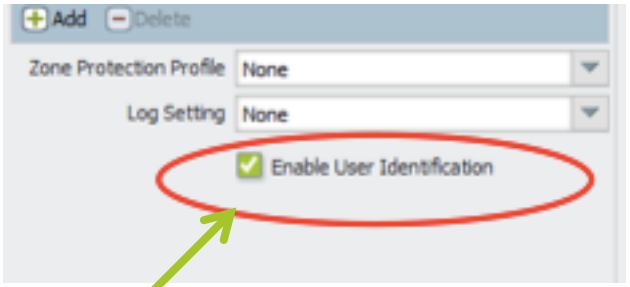
One agent is used for all directory services (AD, LDAP, eDirectory)

- The agent setup process is outlined here: User-ID-Agent_Setup-4-5.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 User-ID API can be employed when connectivity to another identity management system is required**

Installing the User-ID agent

- 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 address, 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:

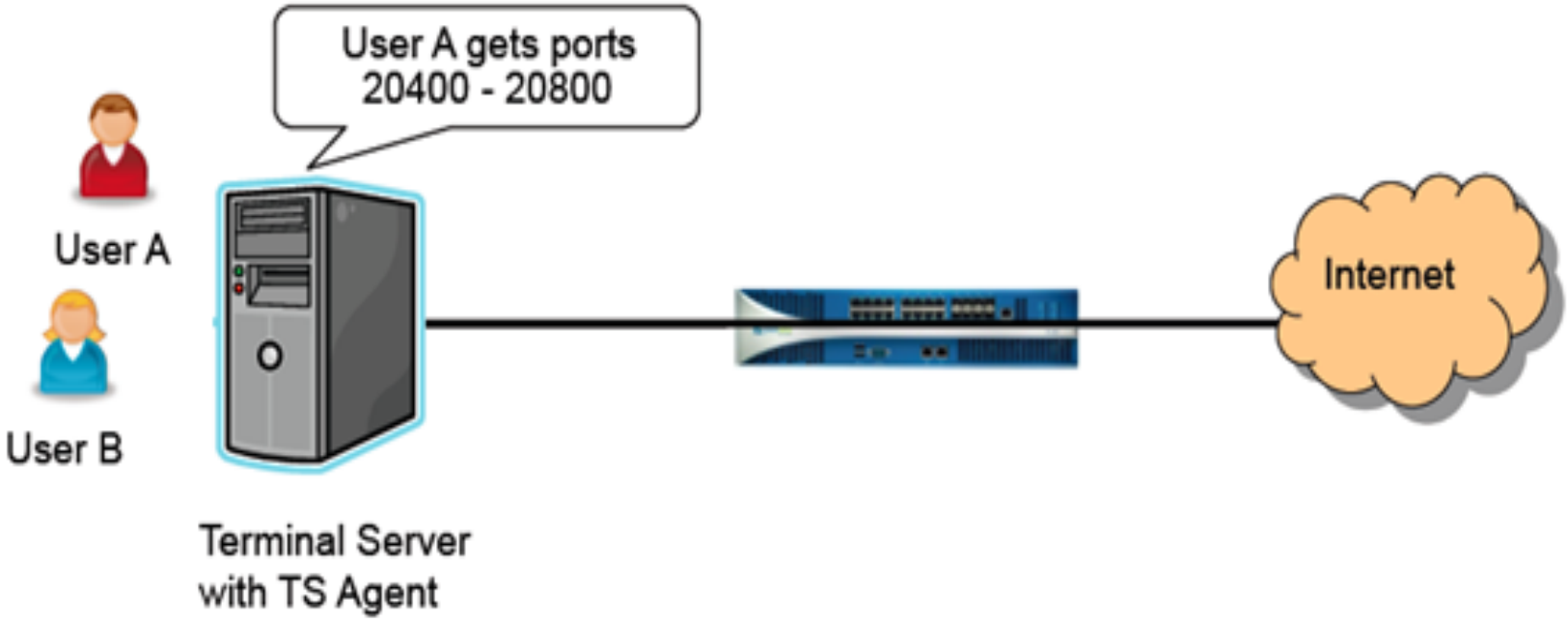




Don’t forget to enable user-ID in the zone which contains the users!

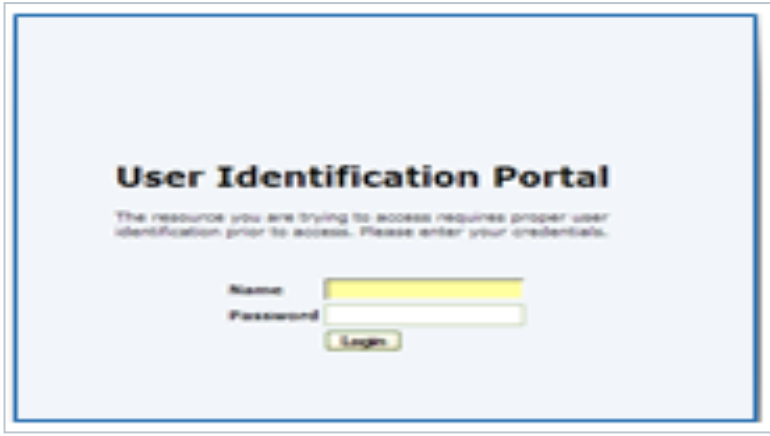
Terminal Server Agent

- 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

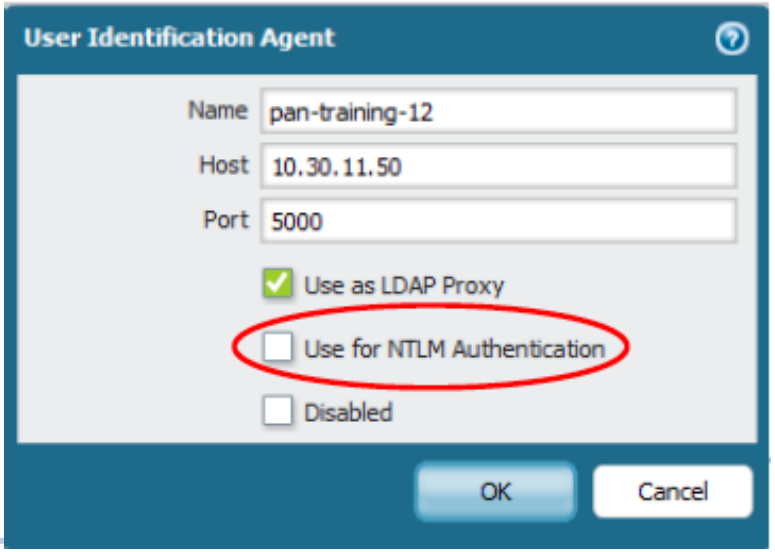
- Captive portal is a feature of the Palo Alto Networks firewall that authenticates users via an alternate source, such as a RADIUS server.
- Use captive portal when:
  - You have Window users that are not logging into the AD domain
    - ➢Authentication can be transparent if using NTML authentication
  - 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 identfication 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)

- Information on Captive Portal: Using Captive Portal.pdf
- A portion of this doc references certificate authentication; certificates are available with PAN-OS 5.0 or higher. The rest of the doc is applicable to PAN-OS 5.1
- 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.



SSL Decryption

- The Palo Alto firewall can perform SSL decryption on connection 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 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 user from seeking 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 user's browsers.

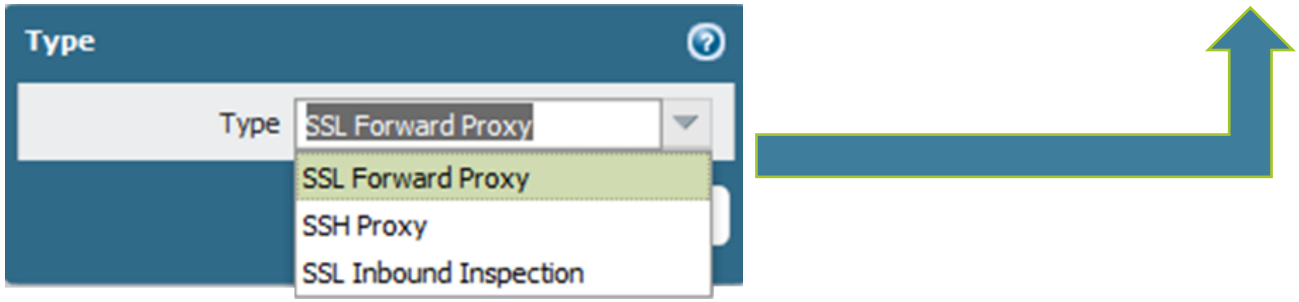
• When no internal PKI infrastructure is available, it is possible to distribute the firewall CA certificate to clients e.g. using Group Policy Objects functionality in Active Directory

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 outbound decryption, add two rules that look like this:

		Source			Destination					
Name	Tag	Zone	Address	User	Zone	Address	URL Category	Action	Type	Decryption Profile
No-Decrypt	none	Trust-L3	any	any	Untrust-L3	any	financial-services health-and-medicine shopping	no-decrypt	ssl-forward-proxy	none
Decrypt all traffic	none	Trust-L3	any	any	Untrust-L3	any	any	decrypt	ssl-forward-proxy	deny-decrypt-failures



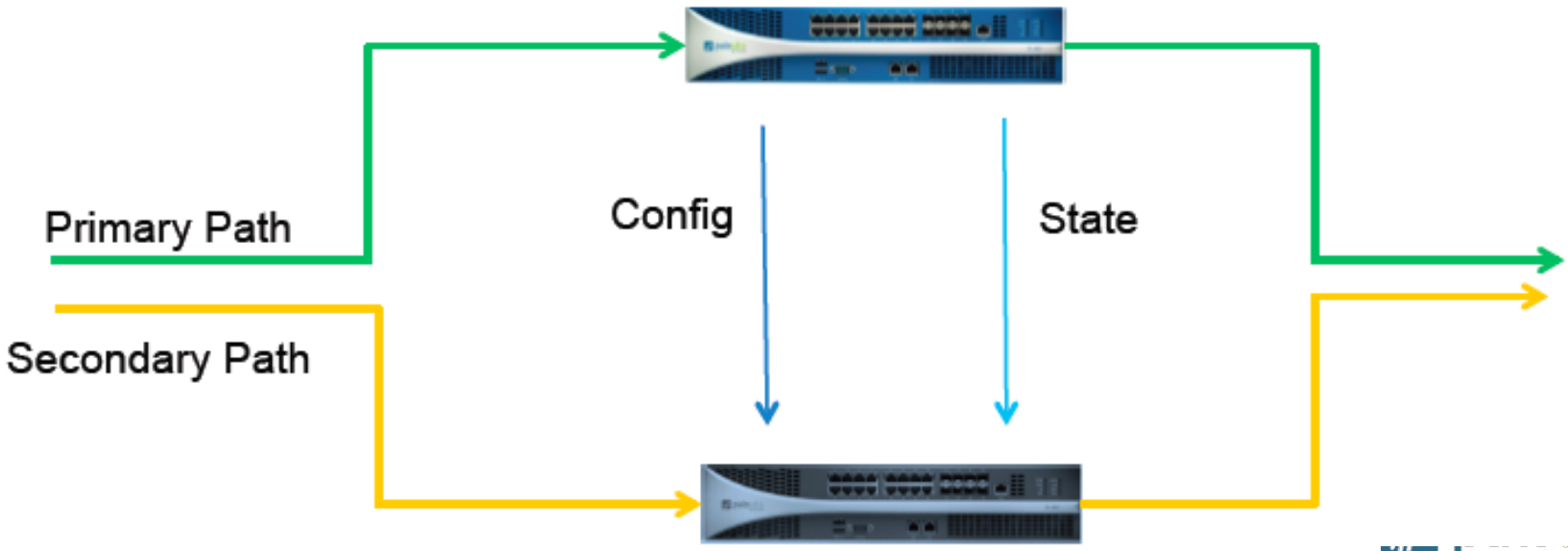
- The first rule will not decrypt any traffic going to the URL categories of finance, health, and shopping.
- The Second rule will decrypt (proxy) all other connections. Make sure to choose action “decrypt” on the second rule

Misc. SSL Decryption

- When SSL is decrypted, the app running inside the SSL session will appear in the traffic log. For example:
  - http://facebook.com, SSL decryption NOT enabled, traffic log will show application in 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

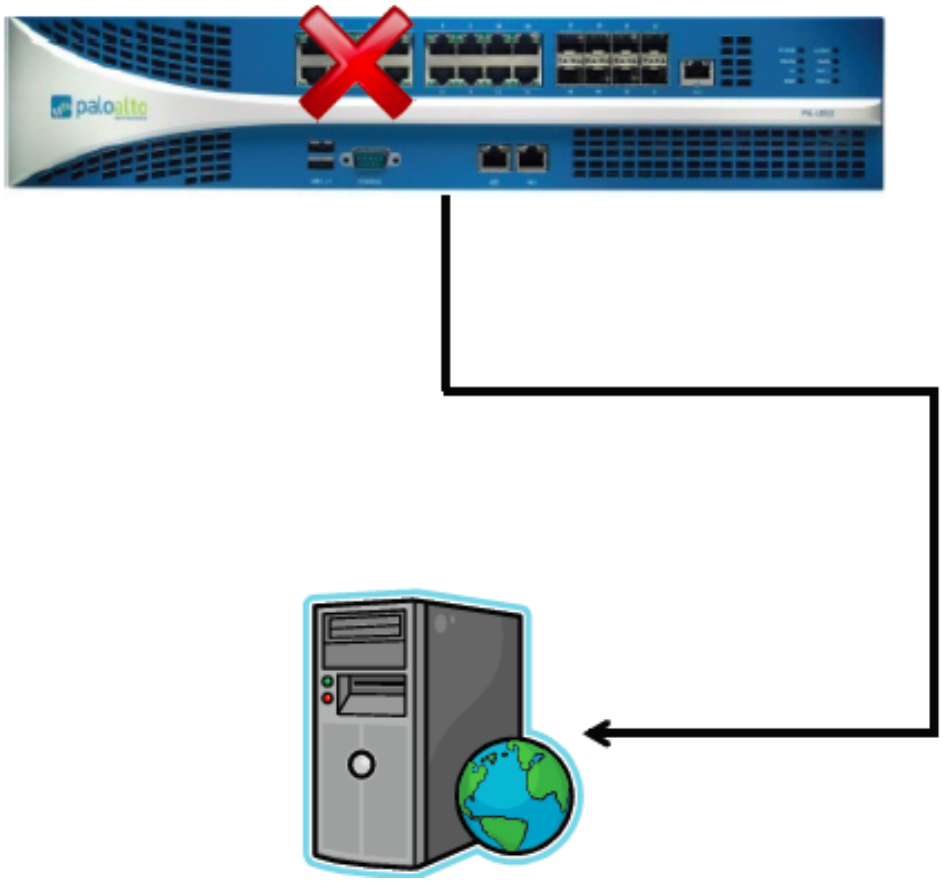
High Availability: Active/Passive

- 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



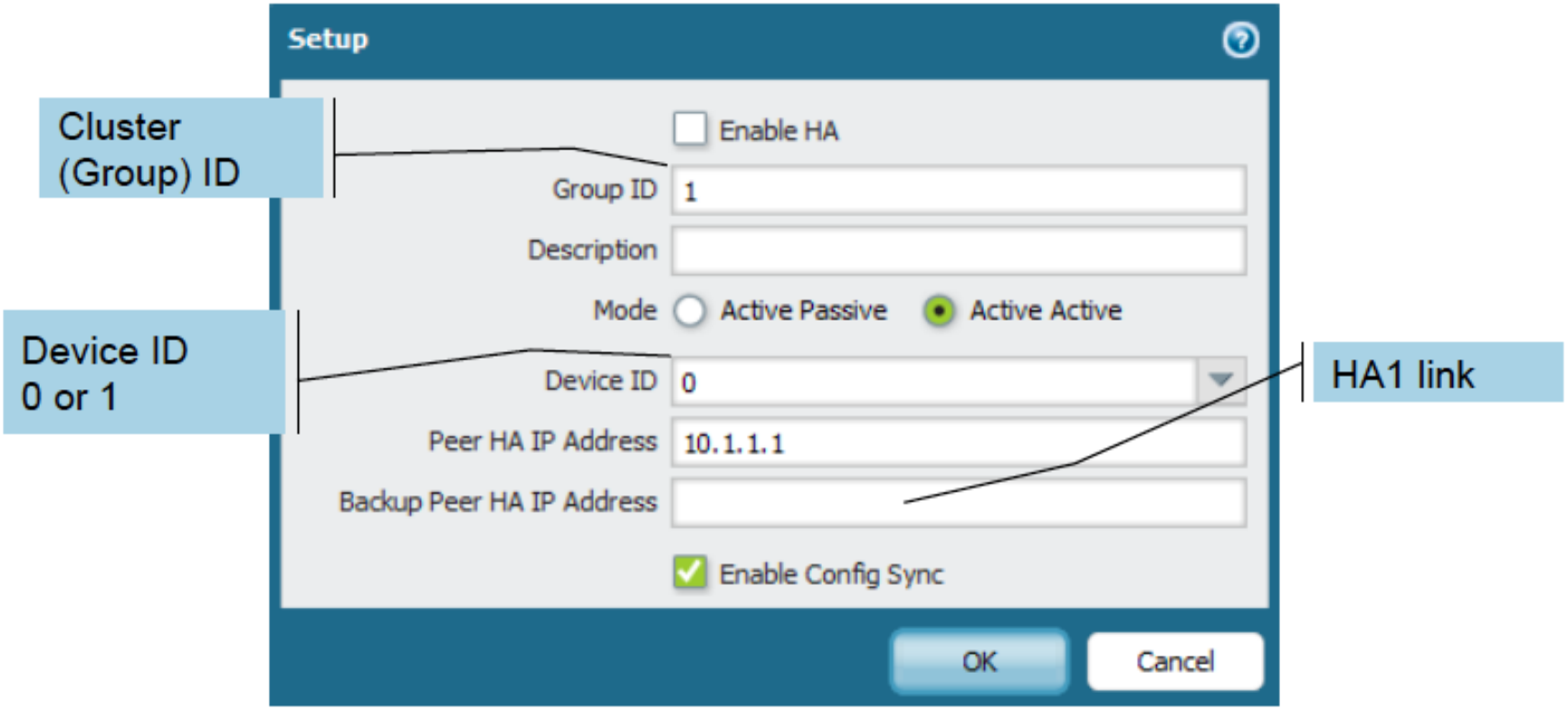
HA Failure States

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



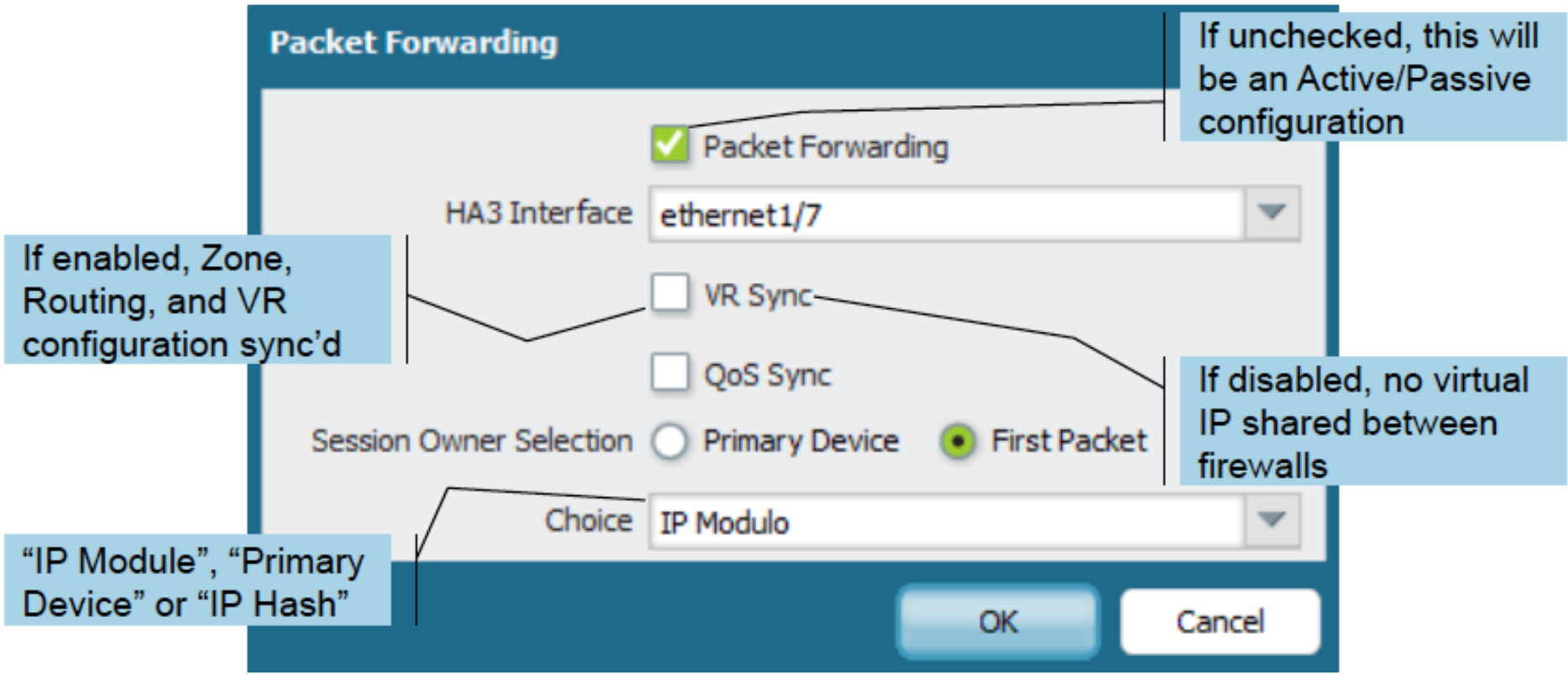
High Availability: Active/Active

- 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



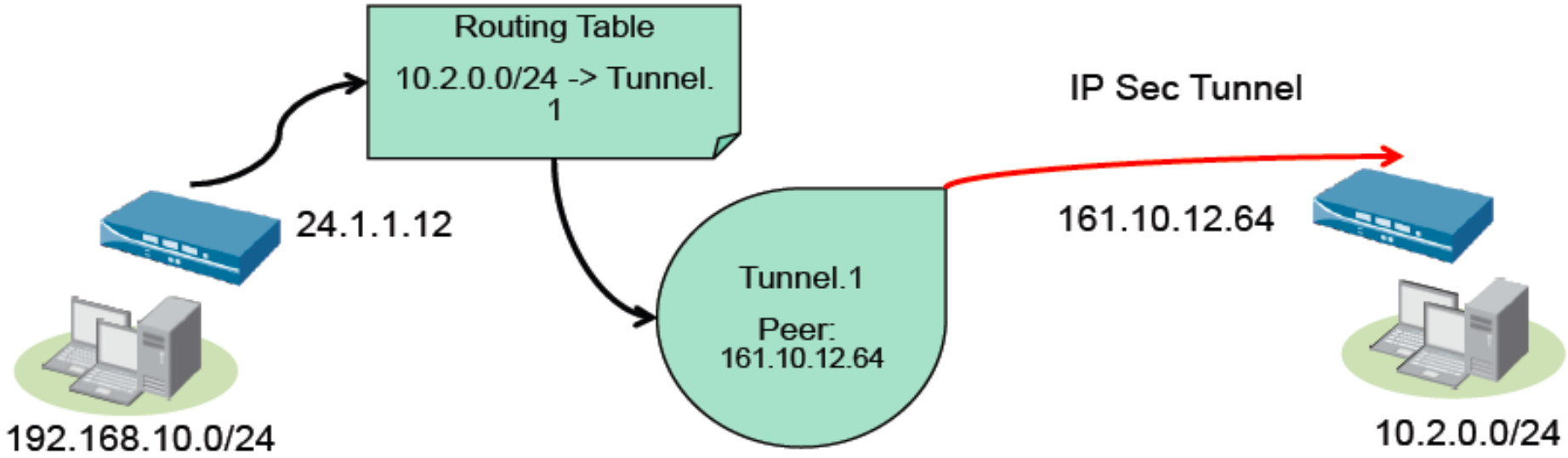
Misc HA

- 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 HA cluster

  https://live.paloaltonetworks.com/docs/DOC-4043
- 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.

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



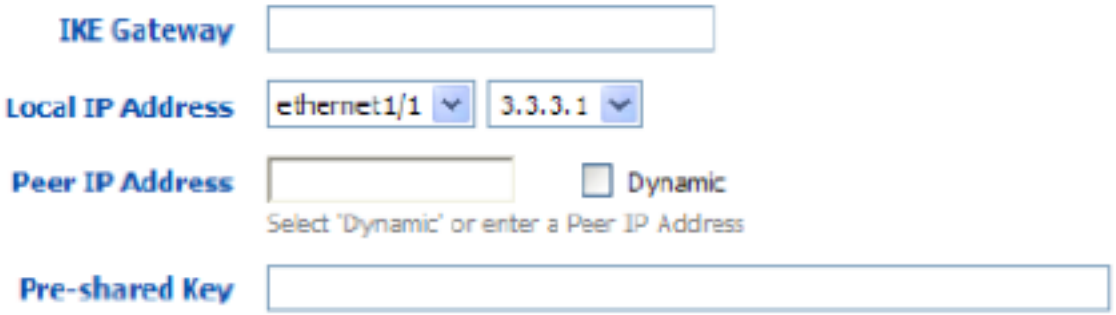
Steps to configure an IPSec site-to-site VPN

1. Create a tunnel interface
   - Under the Networks tab-> 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 advance option 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 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>`

GlobalProtect

paloalto NETWORKS

the network security company™

GlobalProtect | Overview

- License & Components
- Connection Sequence
- GlobalProtect Configuration
  1. Gateways
  2. Portal
  3. Agents
- Host Checks
- Logs

GlobalProtect Licensing

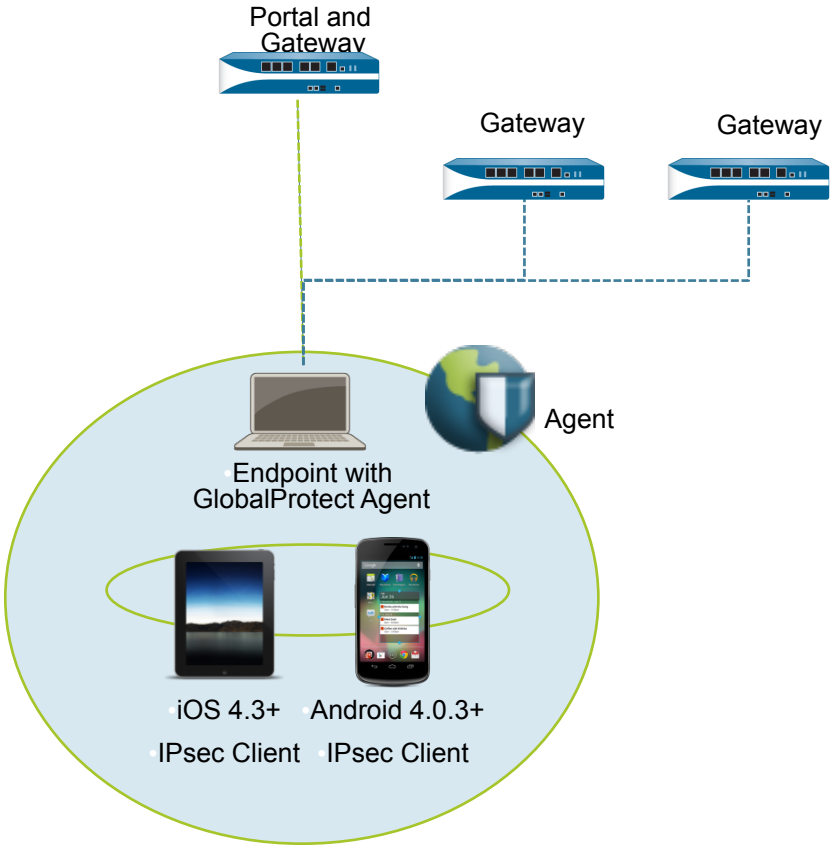
Licensing based on Portals and Gateways (firewall), not users

	Portal License	Gateway Subscription
Single Gateway		
Multiple Gateway	●	
Internal Gateway	●	
HIP check	●	●

- Portal – one-time perpetual license
  - Required on the device that would run Portal
  - Required for multi-gateway deployments
- Gateway – annual subscription
  - Required on the devices that would check host profile
  - Provides ongoing content updates to check the host profile

GlobalProtect Components

- GlobalProtect Portal
  - Central authority for GlobalProtect
  - Provides list of known gateways
  - Provides certificates to validate gateways
  - Hosts GlobalProtect agent for initial download
  - May be installed on same device as a GlobalProtect Gateway
- GlobalProtect Gateway
  - Provides tunnel termination points
  - Enforces security policy for connected users
- GlobalProtect Agent
  - Software that runs on endpoint
  - Supported on Windows 8, Windows 7, Windows Vista 32/64bit
  - Mac OS X 10.6/10.7/10.8 (PAN OS 4.1)
- Third Party IPSec Client Support
  - iOS 4.3+
  - Android 4.0.3+
  - Linux vpnc



Agent Software on the Portal

Device > GlobalProtect Client

Version	Size	Release Date	Downloaded	Currently Activated	Action		
1.2.0	21 MB	2012/11/02 18:32:22	✔	✔	Reactivate	Release Notes	☒
1.1.7	27 MB	2012/10/10 14:48:45			Download	Release Notes	
1.1.6	26 MB	2012/08/15 12:07:14			Download	Release Notes	
1.1.5	26 MB	2012/06/20 17:15:50			Download	Release Notes	
1.1.4	26 MB	2012/03/13 18:00:52			Download	Release Notes	
1.1.3	26 MB	2012/02/16 22:56:41			Download	Release Notes	
1.1.2	26 MB	2012/01/24 21:56:11			Download	Release Notes	
1.1.1	26 MB	2011/12/08 22:23:27	✔		Activate	Release Notes	☒
1.1.0	26 MB	2011/10/31 13:38:32			Download	Release Notes	

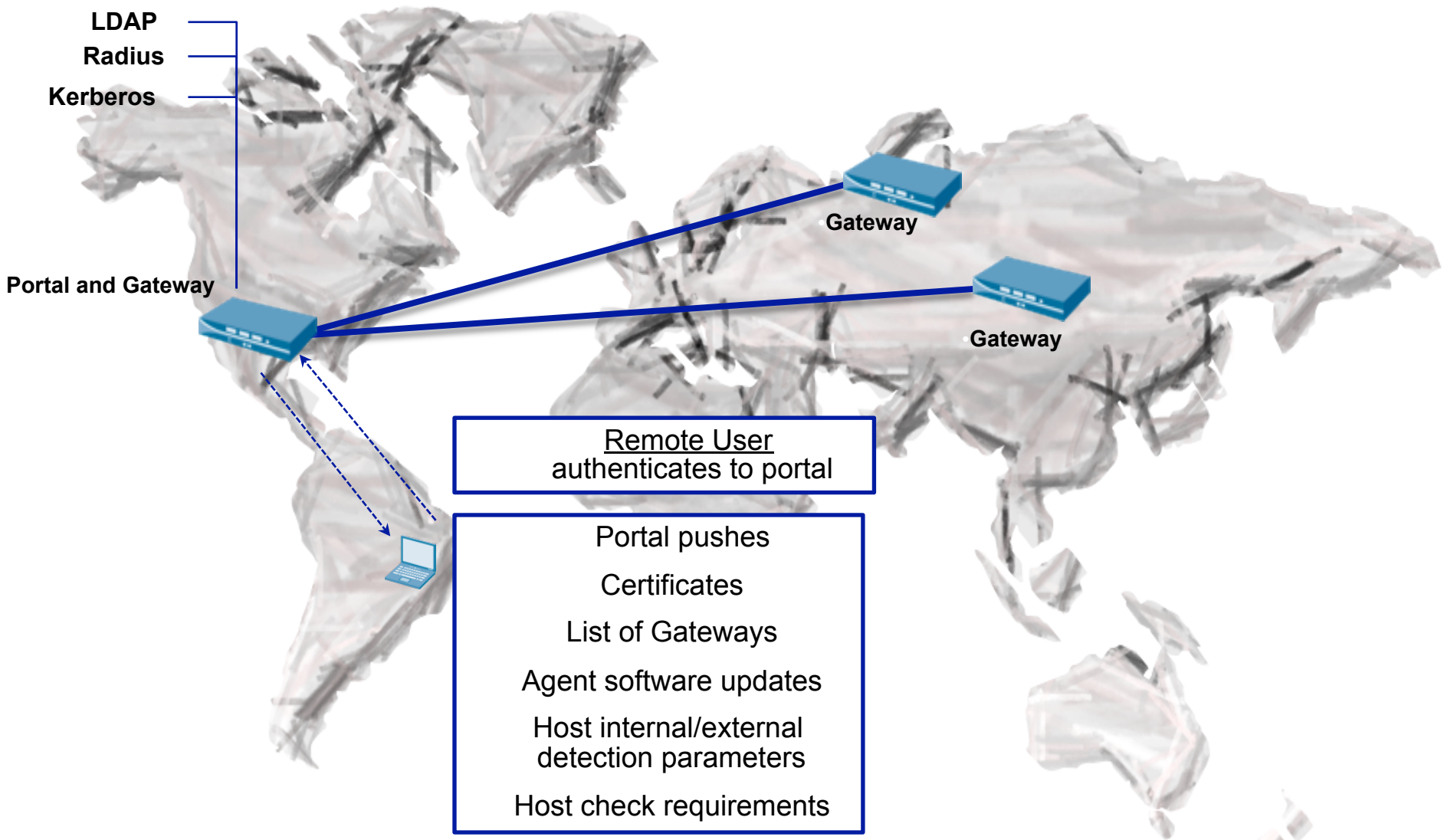
Check Now Upload Activate From File

Connection Sequence:

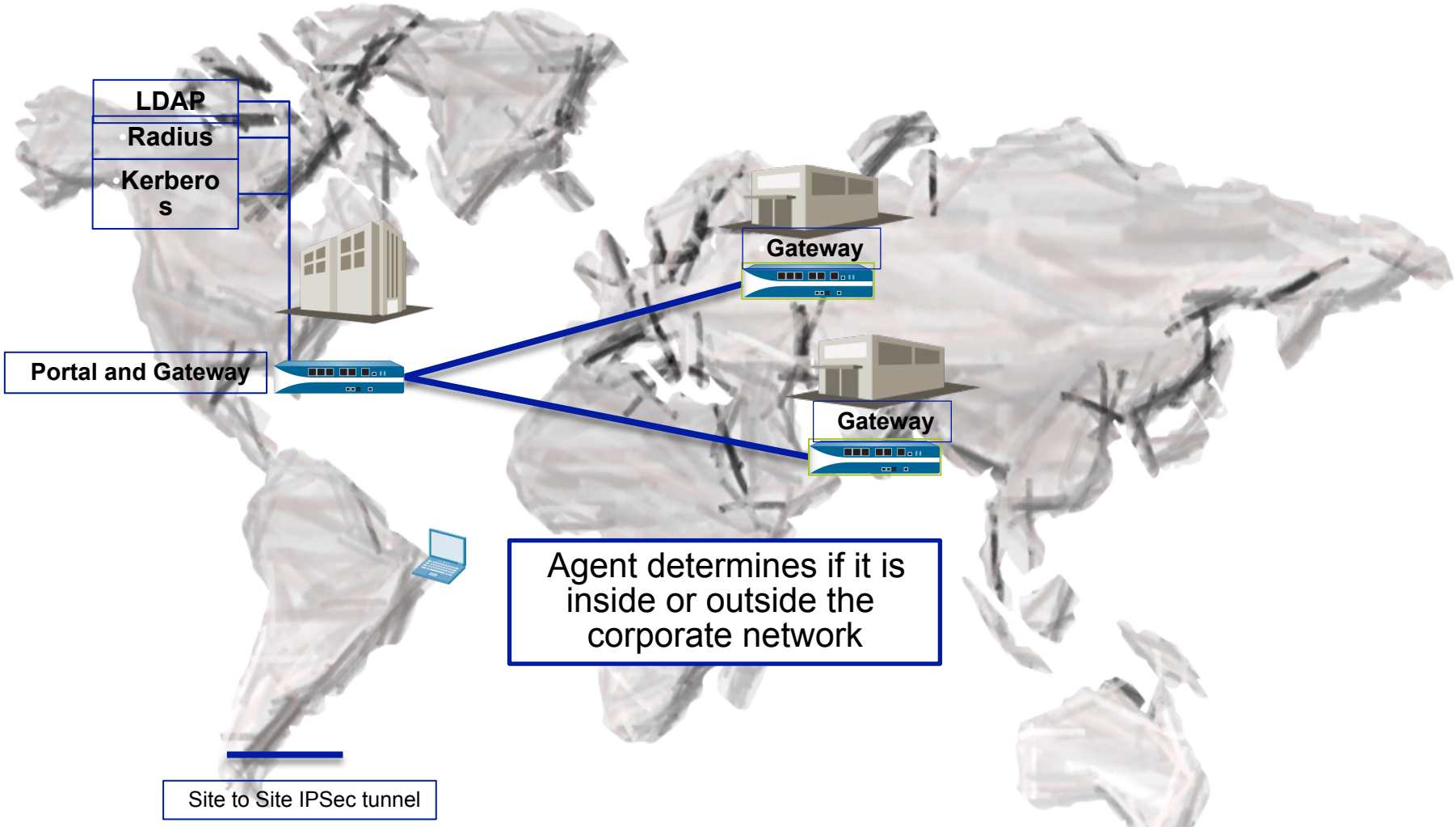
paloalto NETWORKS

the network security company™

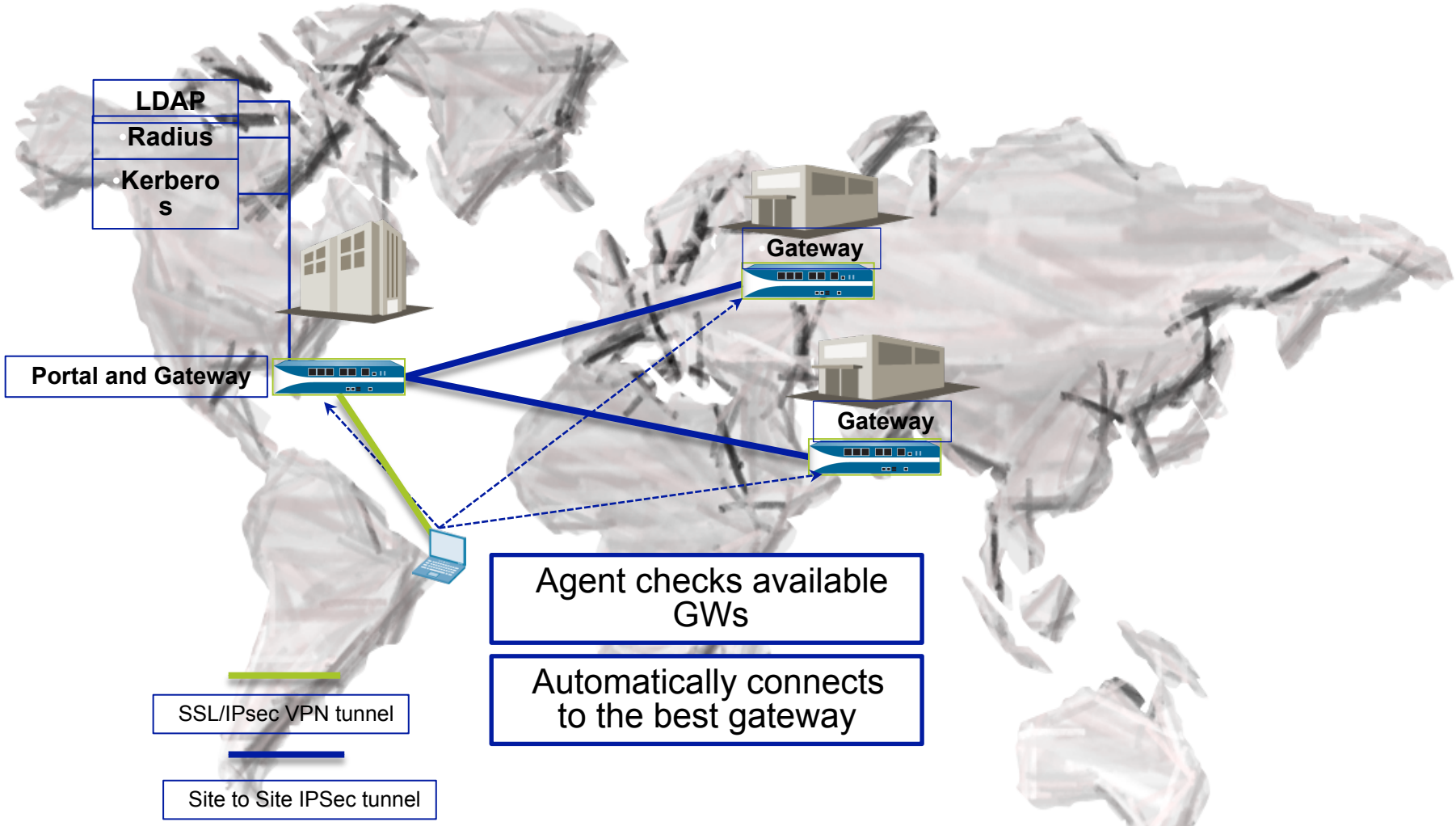
External User Sequence - Step 1



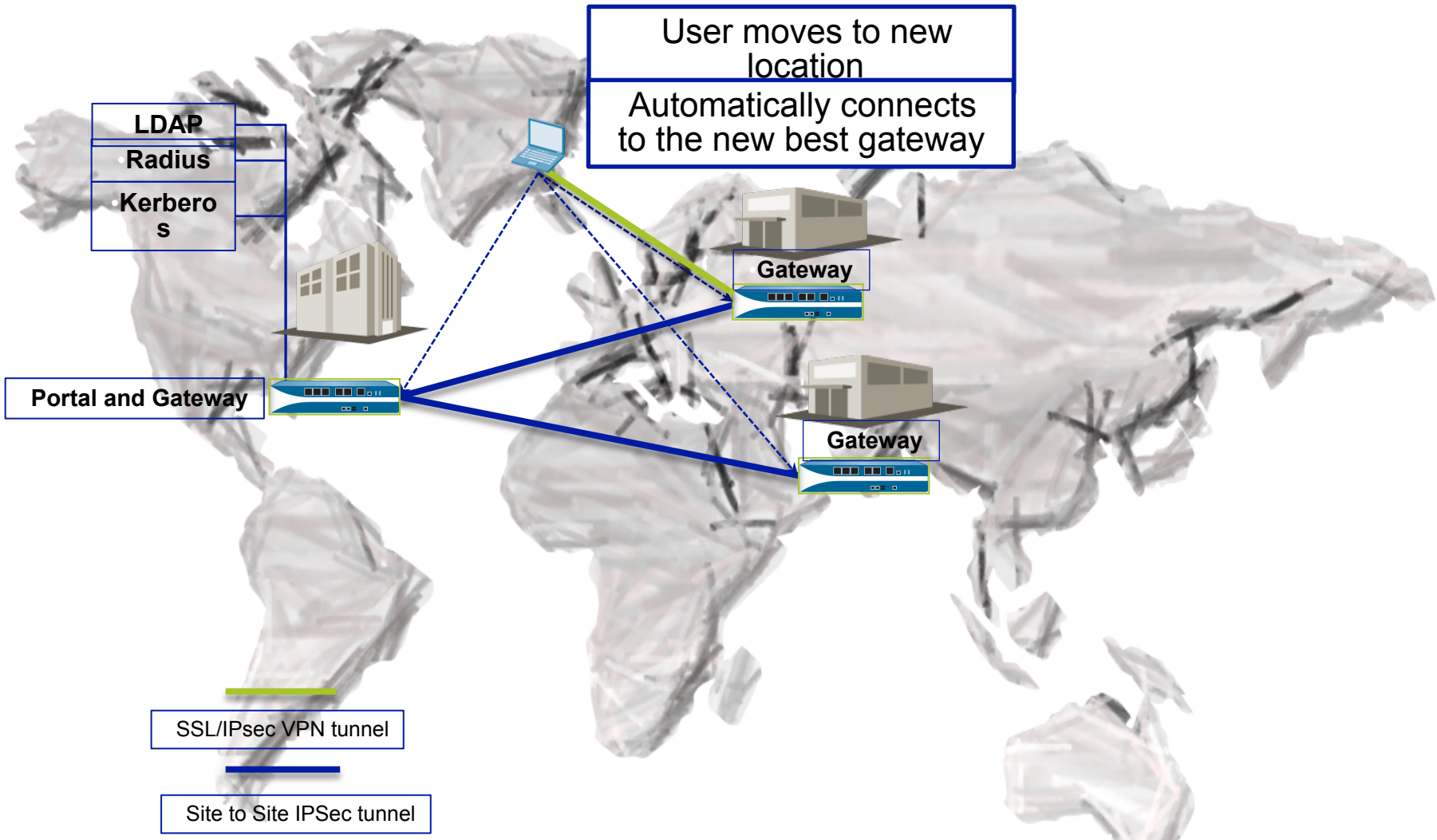
External User Sequence - Step 2



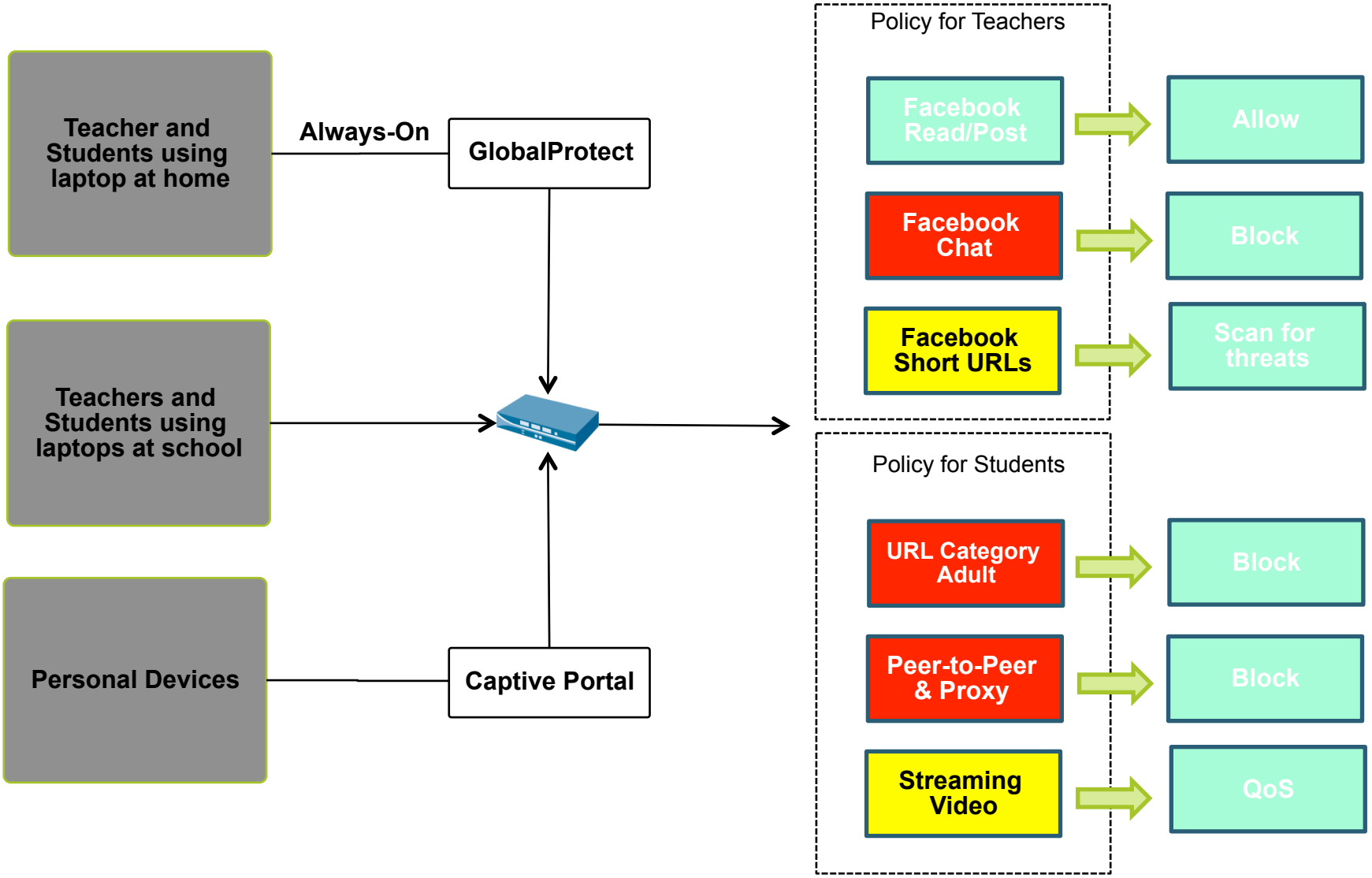
External User Sequence - Step 3



External User Sequence - Step 4



Security Policy Enforcement - Example

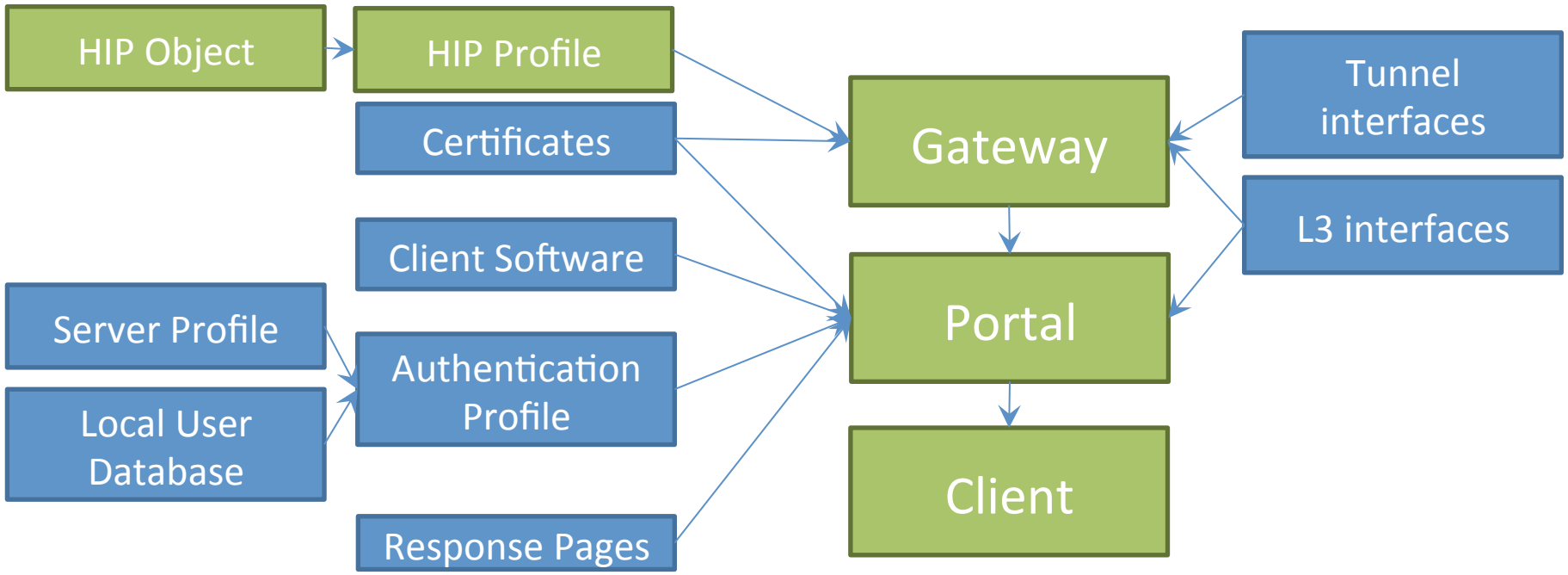


Preparing the Firewall for GlobalProtect

paloalto NETWORKS

the network security company™

Configuration Components



GlobalProtect Required Certificates

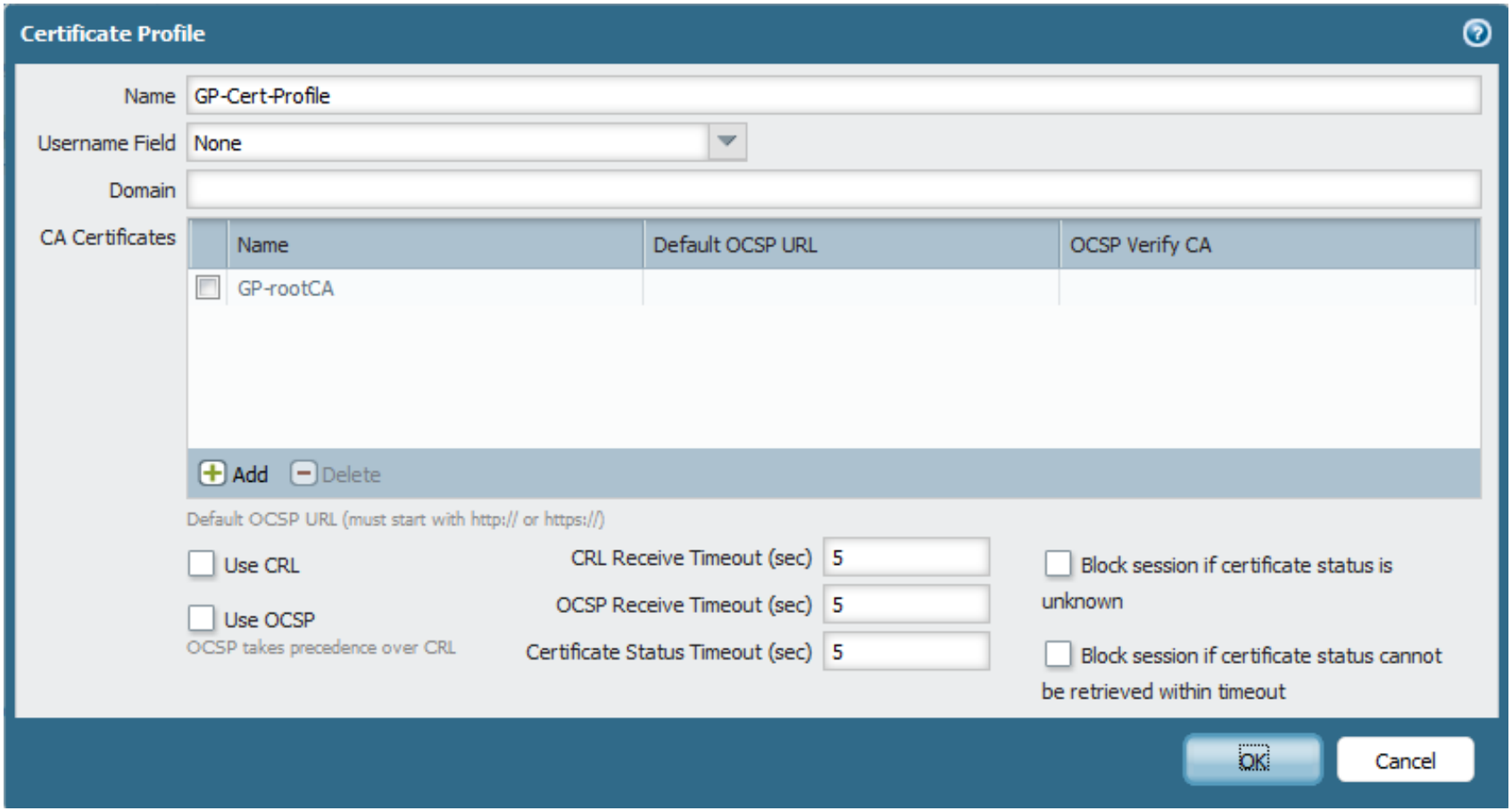
Name	Subject	Issuer	CA	Key	Expires	Status
GP-rootCA	10.30.11.15	10.30.11.15	✓	✓	Jun 25 17:09:51 2013 GMT	valid
GP-Portal	10.251.15.1	10.30.11.15		✓	Jun 25 17:10:30 2013 GMT	valid
GP-Gateway	10.2512.15.1	10.30.11.15		✓	Jun 25 17:11:08 2013 GMT	valid
GP-Client	10.253.15.1	10.30.11.15		✓	Jun 25 17:11:48 2013 GMT	valid

- Certificate Authority (CA) certificate
- GlobalProtect Portal certificate
- GlobalProtect Gateway certificate
- GlobalProtect Client certificate*

*optional

Certificate Profile

Device > Certificate Management > Certificate Profile

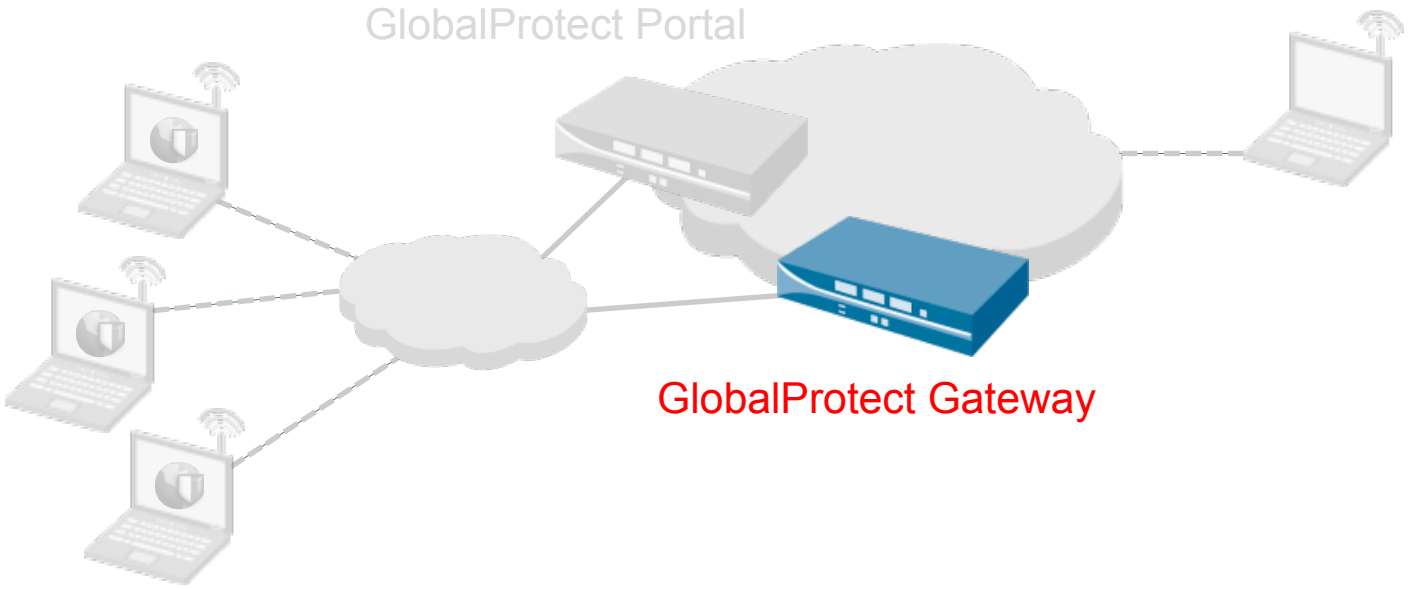


Configuration: GlobalProtect Gateway

paloalto NETWORKS

the network security company™

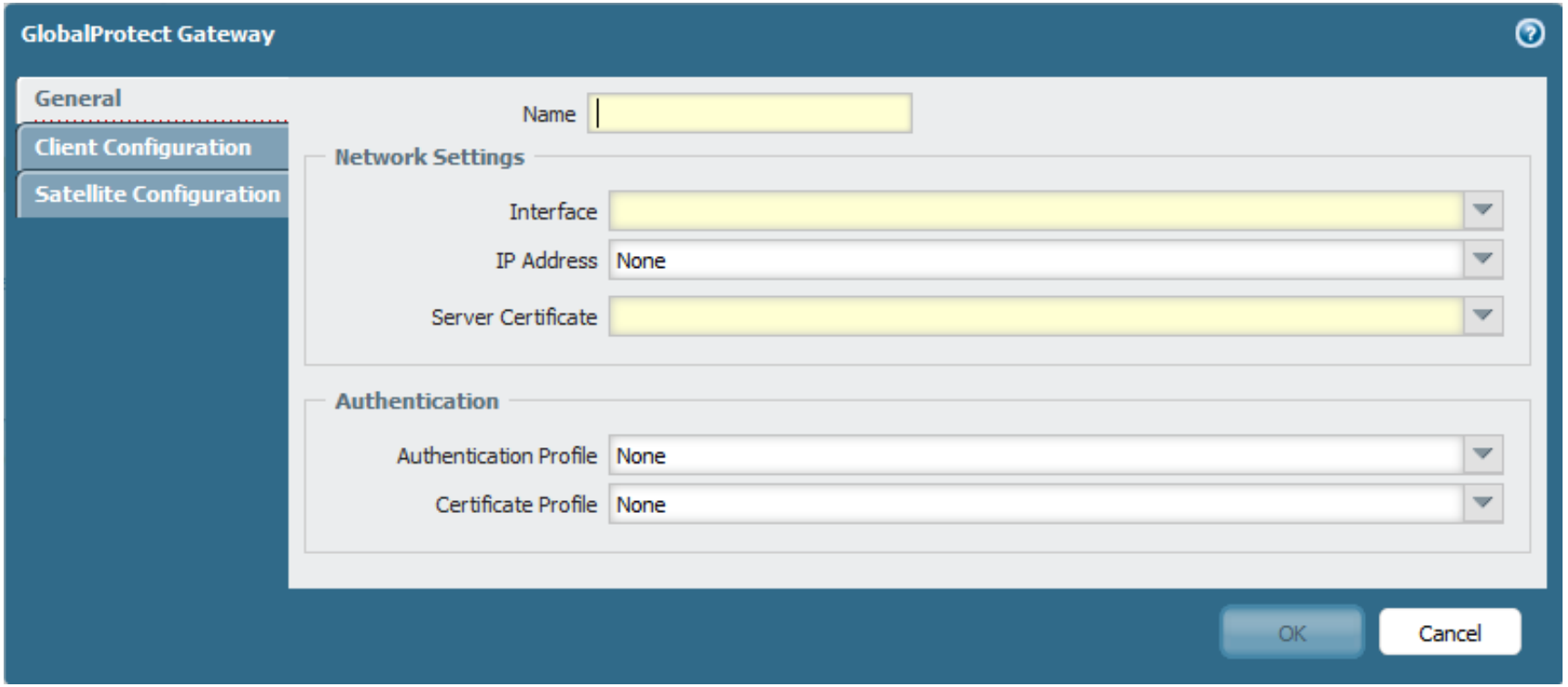
GlobalProtect Gateway



- Provides security enforcement for traffic from GlobalProtect clients
- Requires a tunnel interface for external clients
- Tunnel interfaces are optional for internal gateways

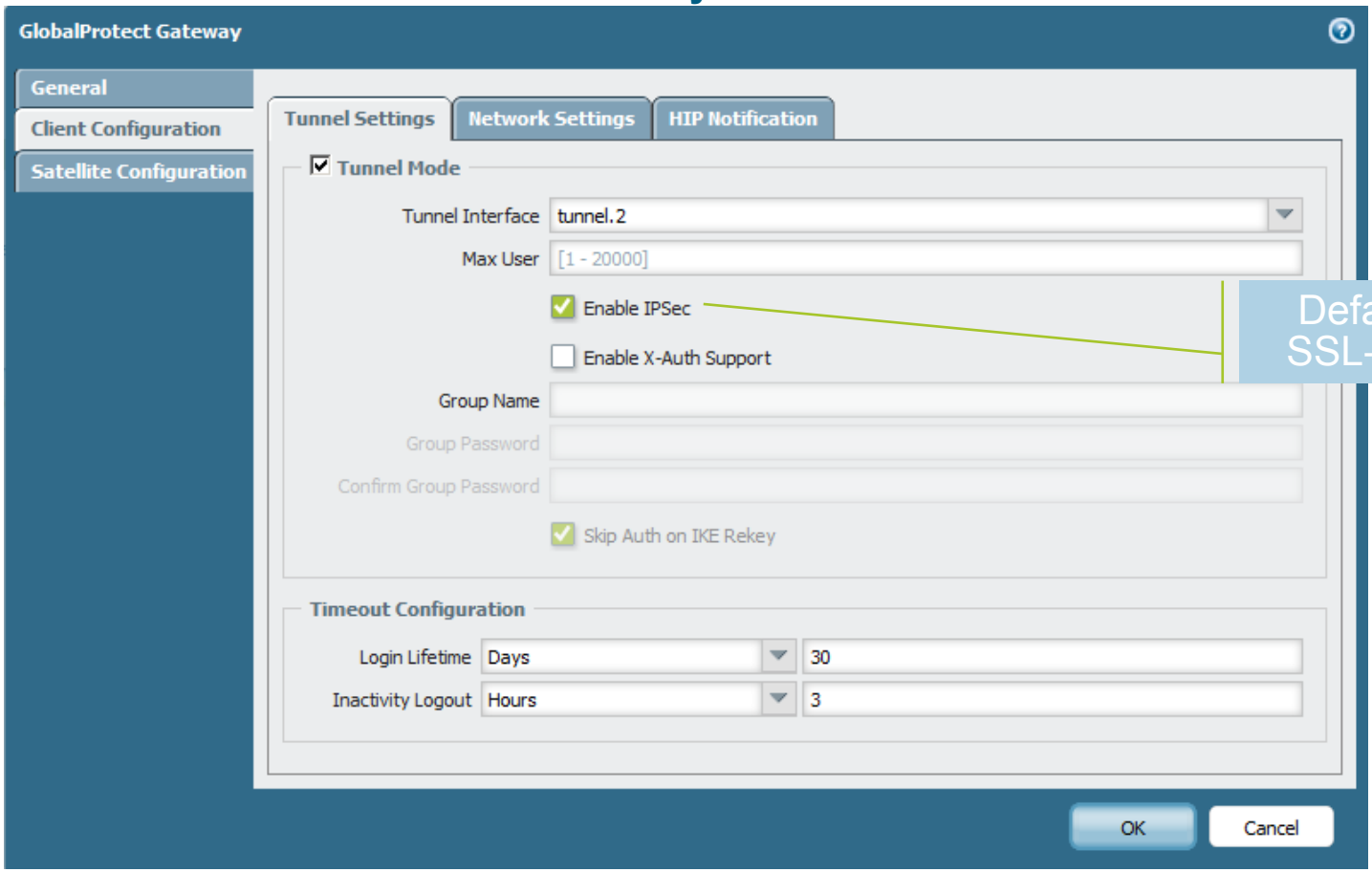
GP-Gateway | General Tab

Network > GlobalProtect > Gateways



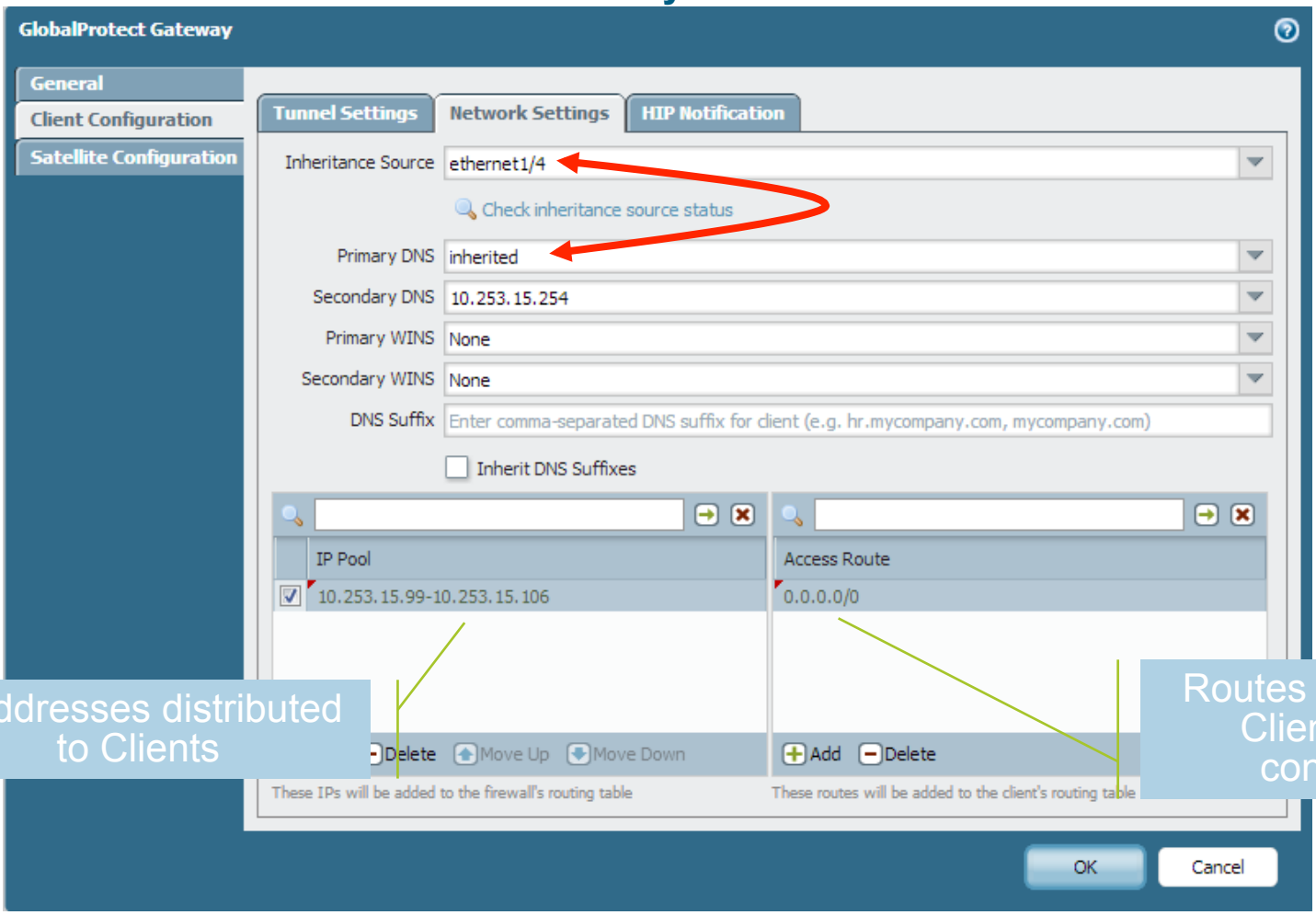
GP-Gateway | Tunnel Settings

Network > GlobalProtect > Gateways



GP-Gateway | Network Settings

Network > GlobalProtect > Gateways



IP addresses distributed to Clients

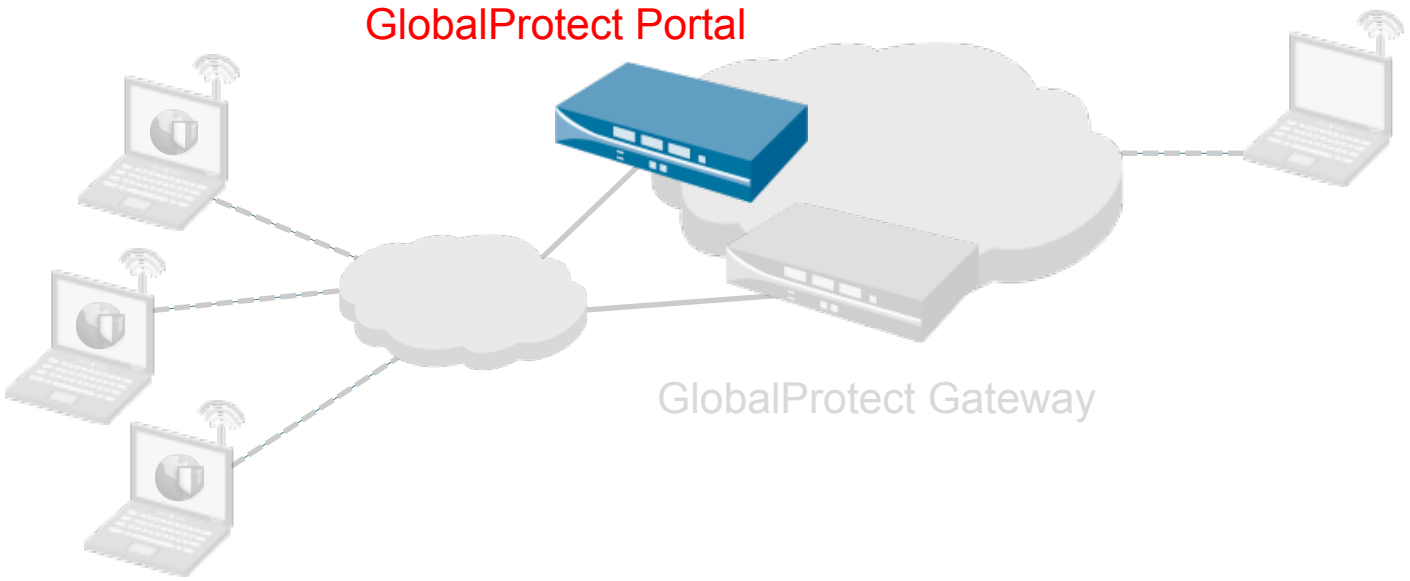
Routes installed on Clients' VPN connection

Configuration: GlobalProtect Portal

paloalto NETWORKS

the network security company™

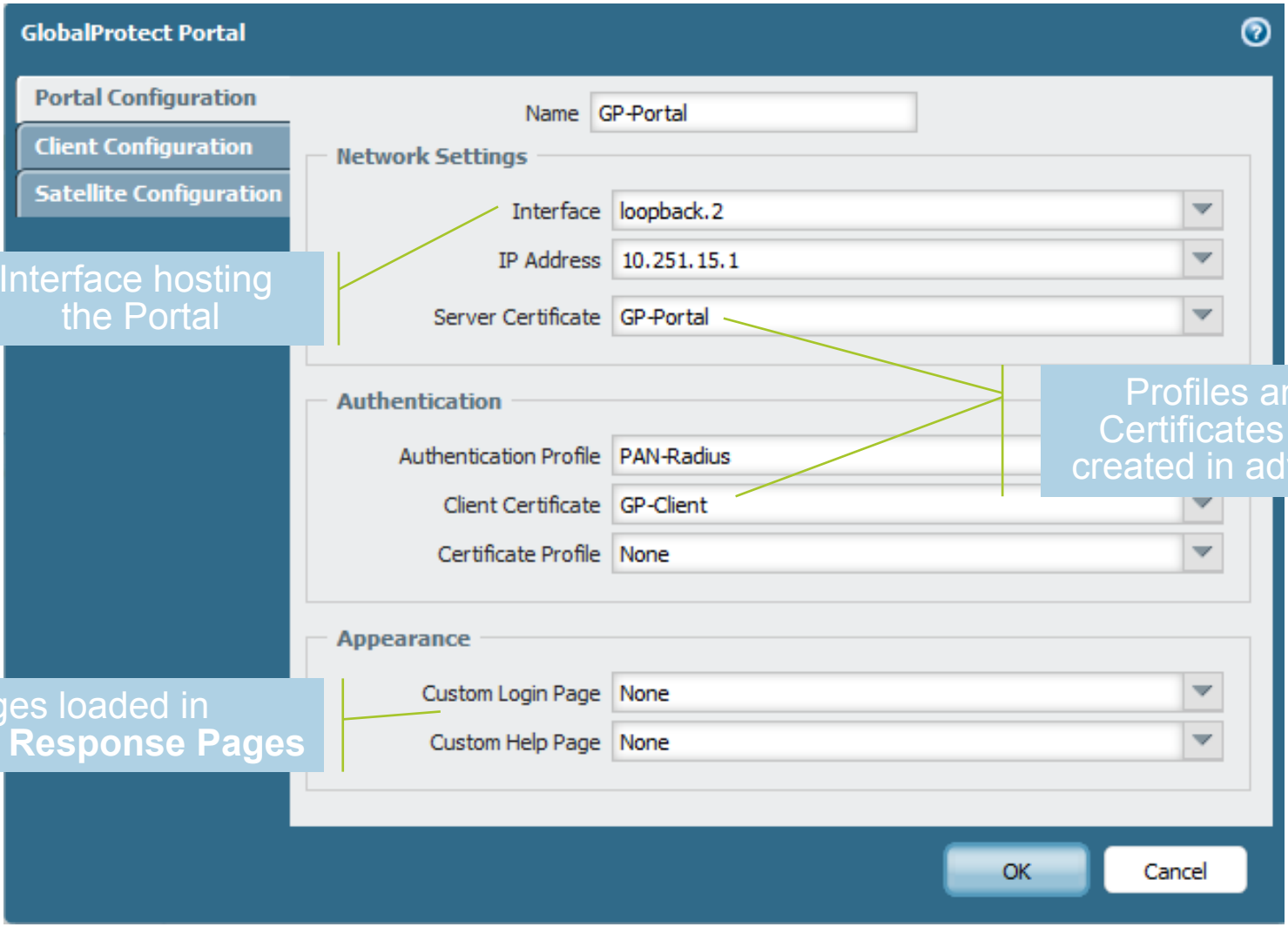
GlobalProtect Portal



- Authenticates users initiating connections to GlobalProtect
- Stores client configurations
- Maintains lists of internal and external gateways
- Manages CA certificates for client validations of gateways

GP-Portal | Portal Configuration tab

Network > GlobalProtect > Portals



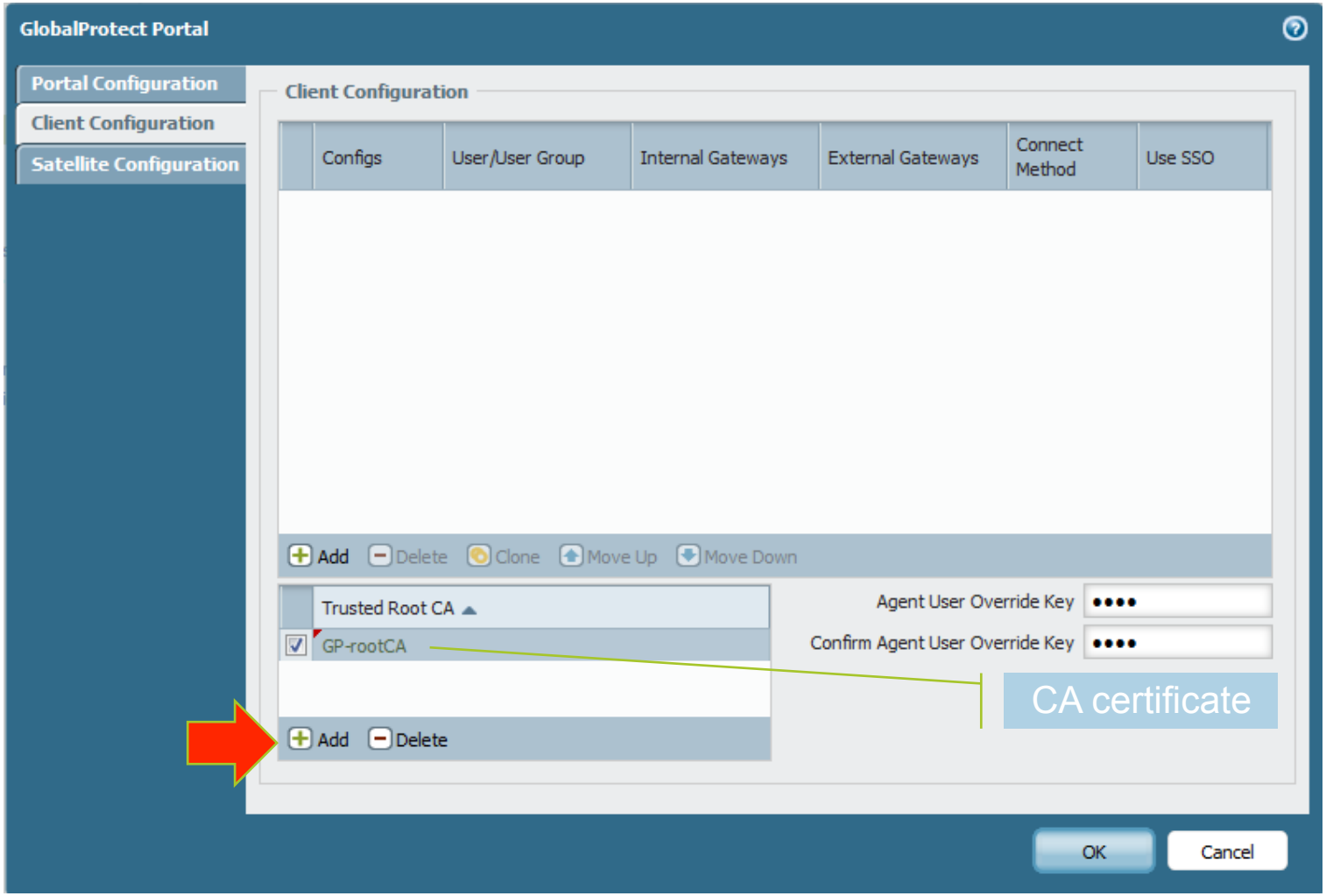
Interface hosting the Portal

Profiles and Certificates are created in advance

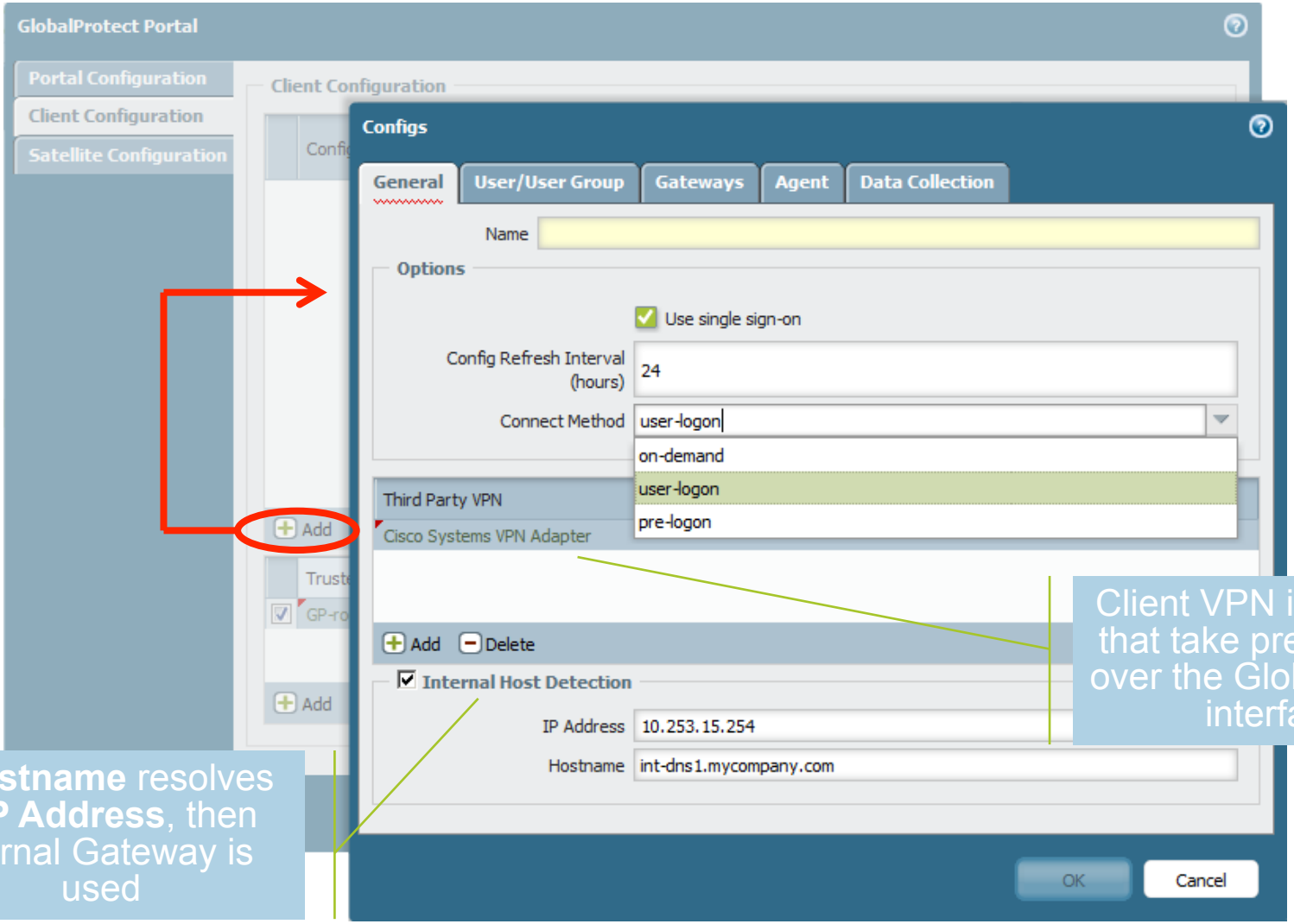
Pages loaded in **Device > Response Pages**

GP-Portal | Client Configuration - Certificates

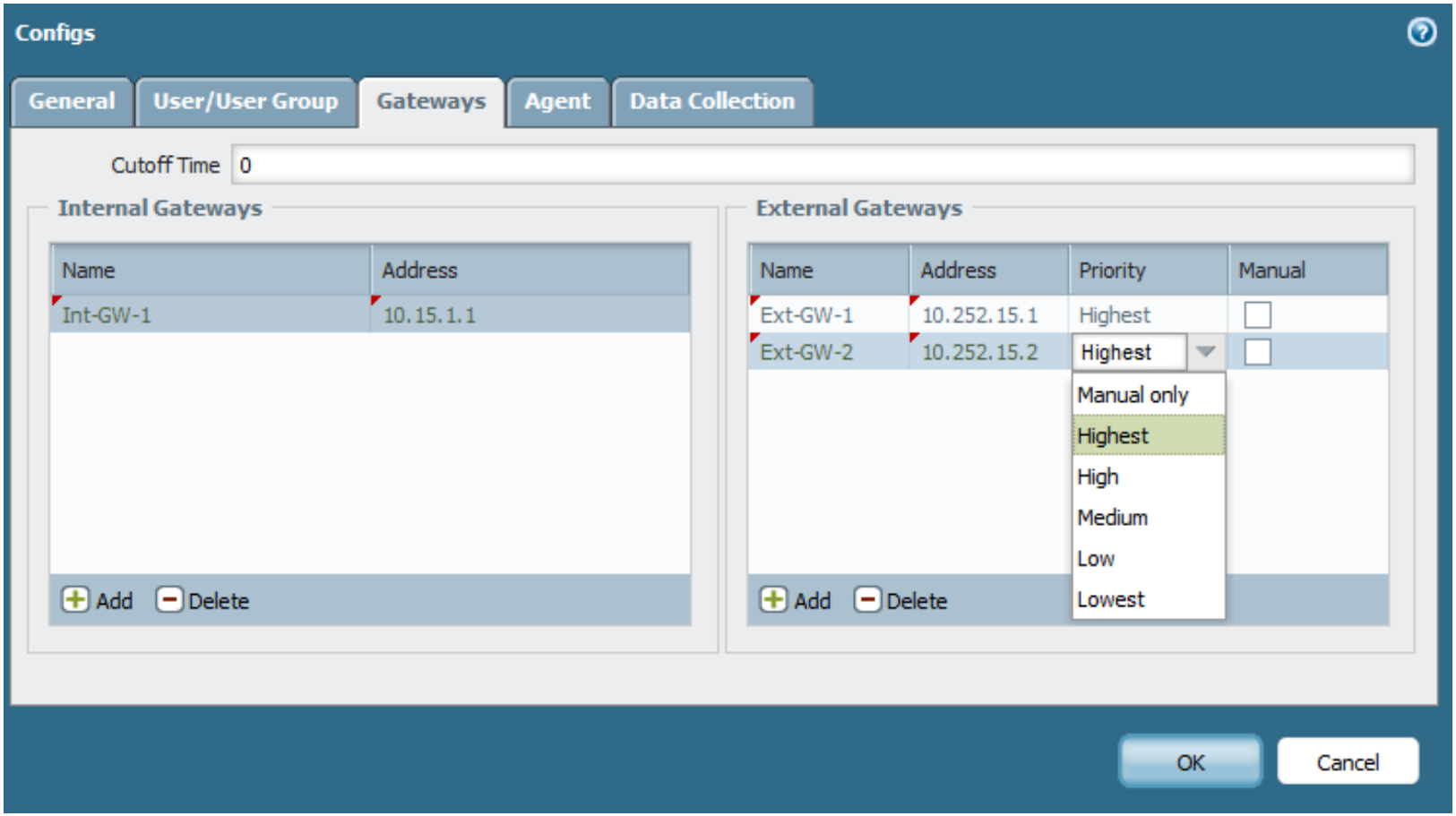
Network > GlobalProtect > Portals



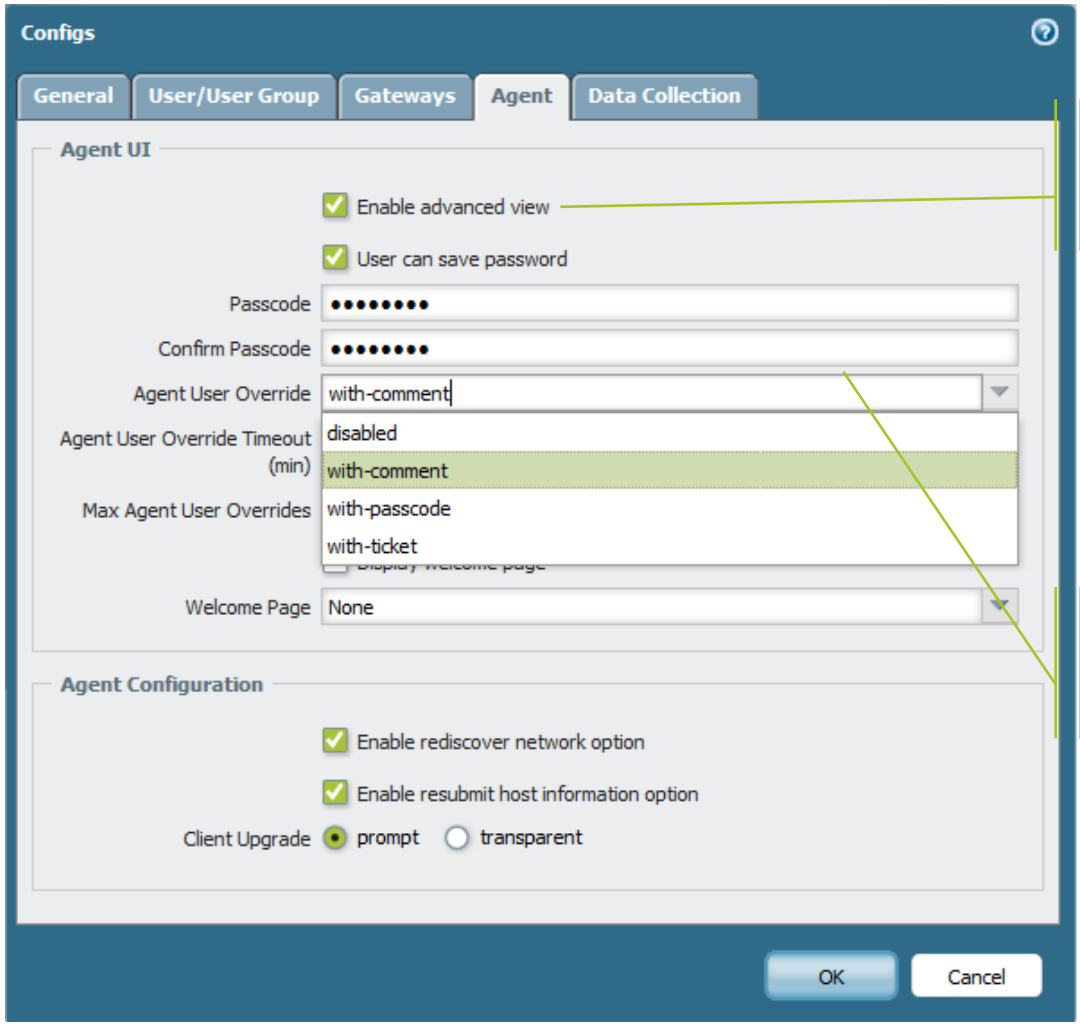
GP-Portal | Client Configurations – General tab



GP-Portal | Client Configuration – Gateways Tab



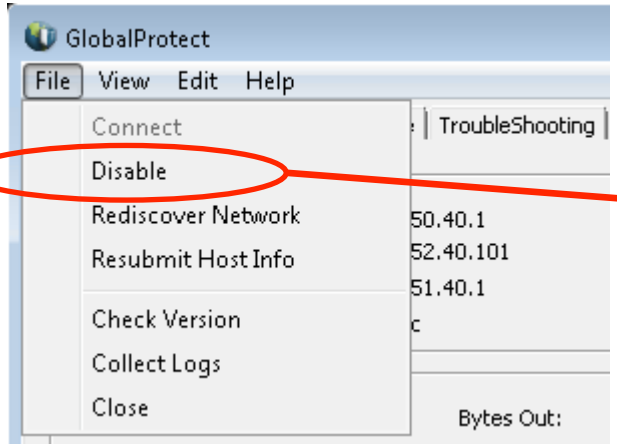
Client Configuration – Agent Tab



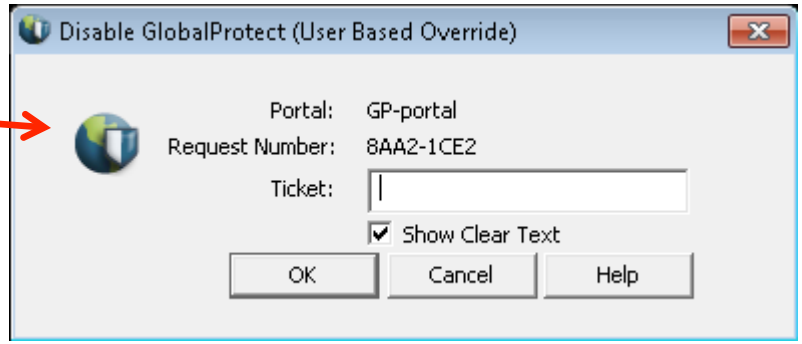
Can view the **Troubleshooting** tab in the Agent

End-user can disable the installed Agent

Disabling the GlobalProtect Agent - Ticket

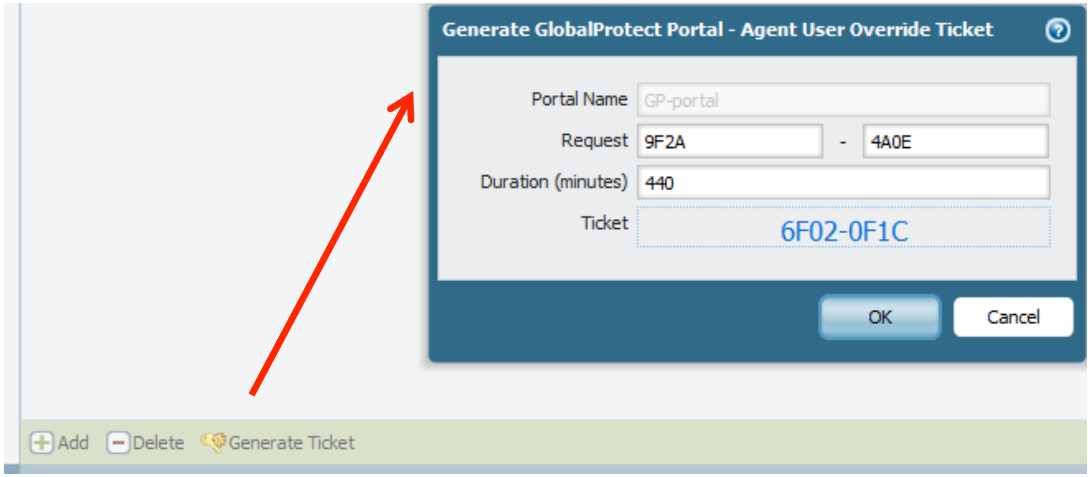


On the Client system



On the portal firewall

Network > GlobalProtect Portal

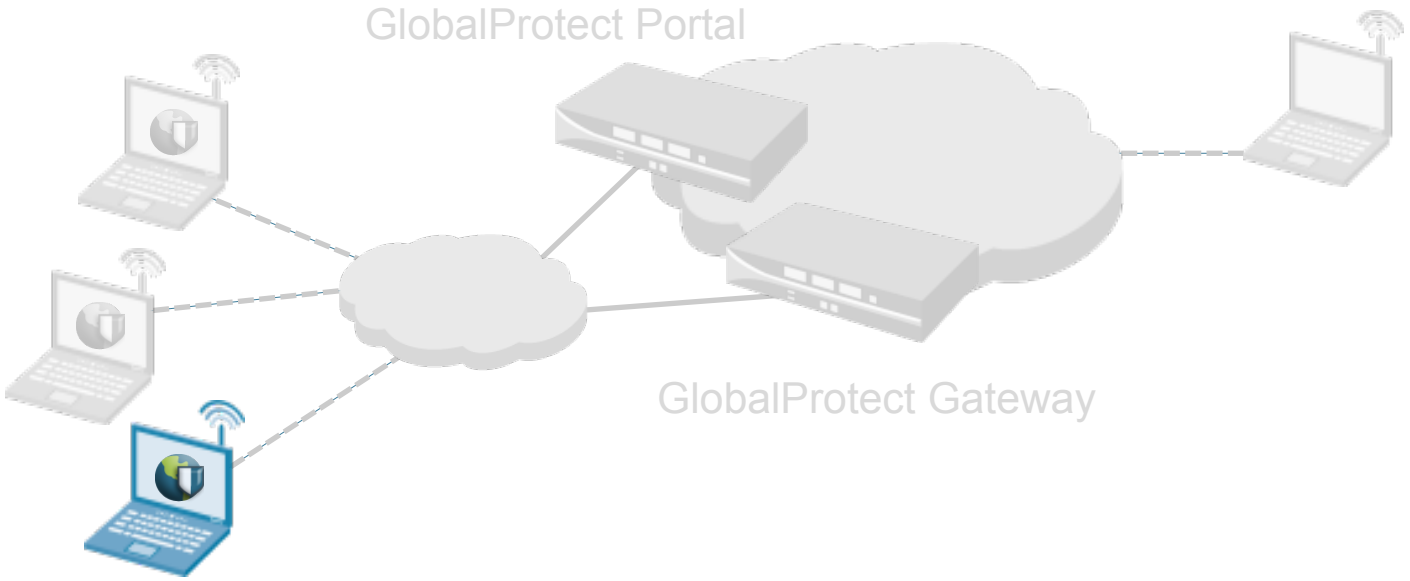


Configuration: GlobalProtect Agent

paloalto NETWORKS

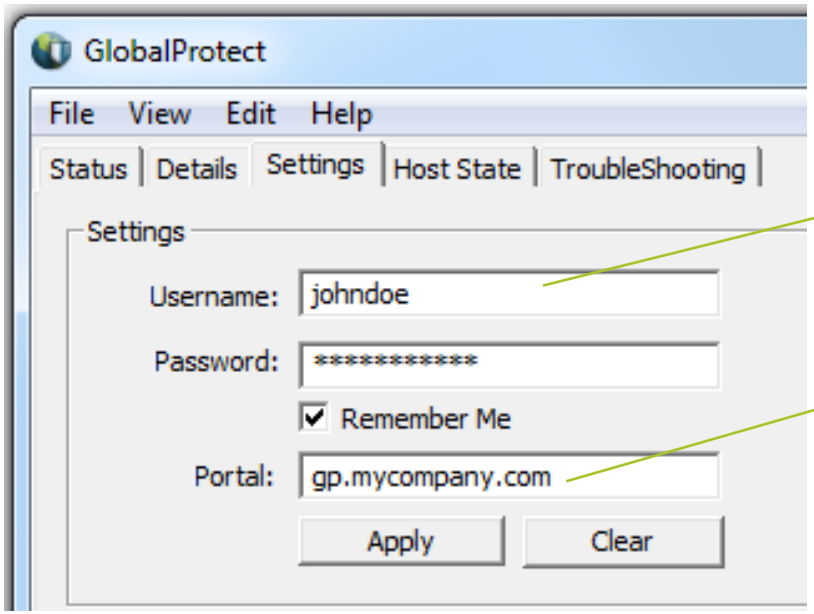
the network security company™

GlobalProtect Agent



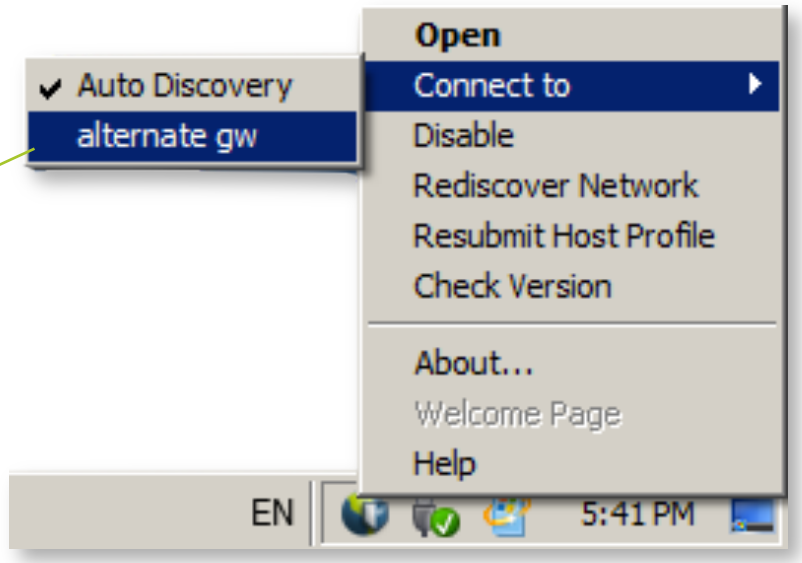
- Authenticates connection against the portal
- Establishes connection with gateways
- Sends HIP reports
- Allows users varying levels of control over the connections

Client Configuration



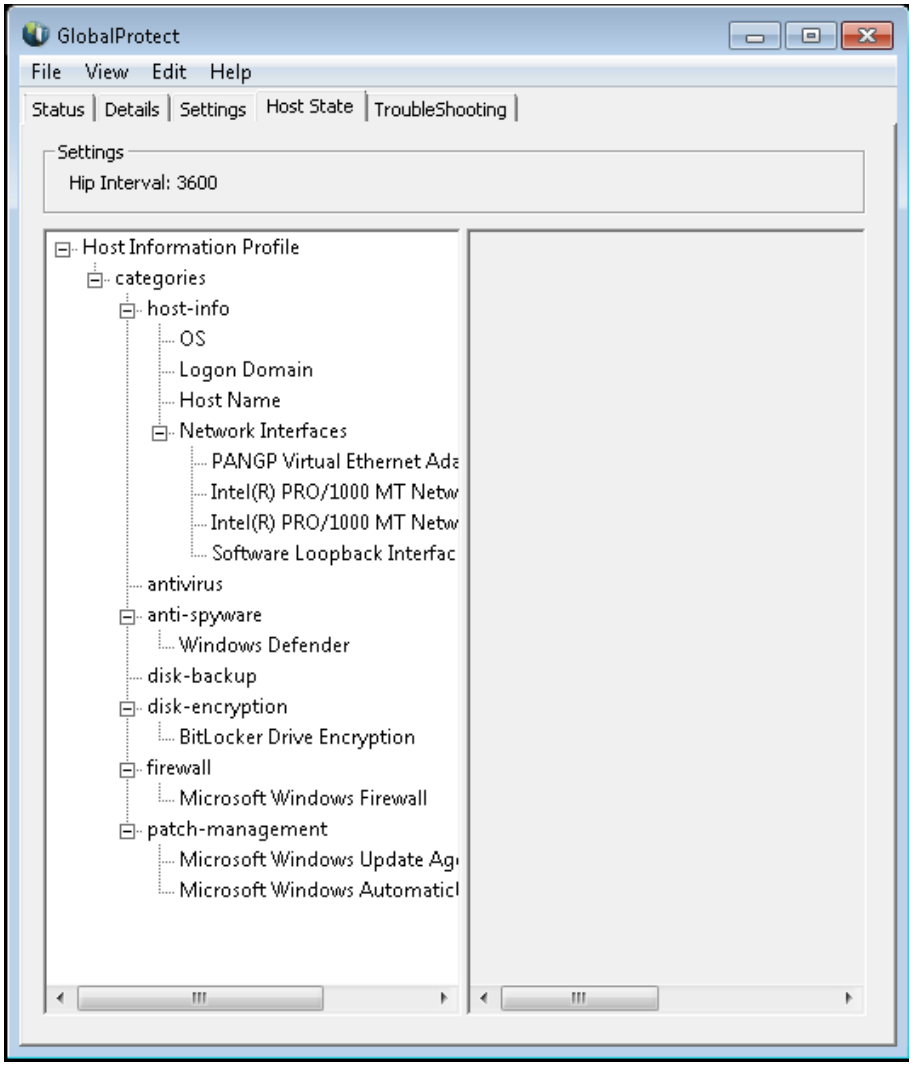
Can be left blank if using single sign-on

Do not include HTTP:// or HTTPS:// in the portal name!

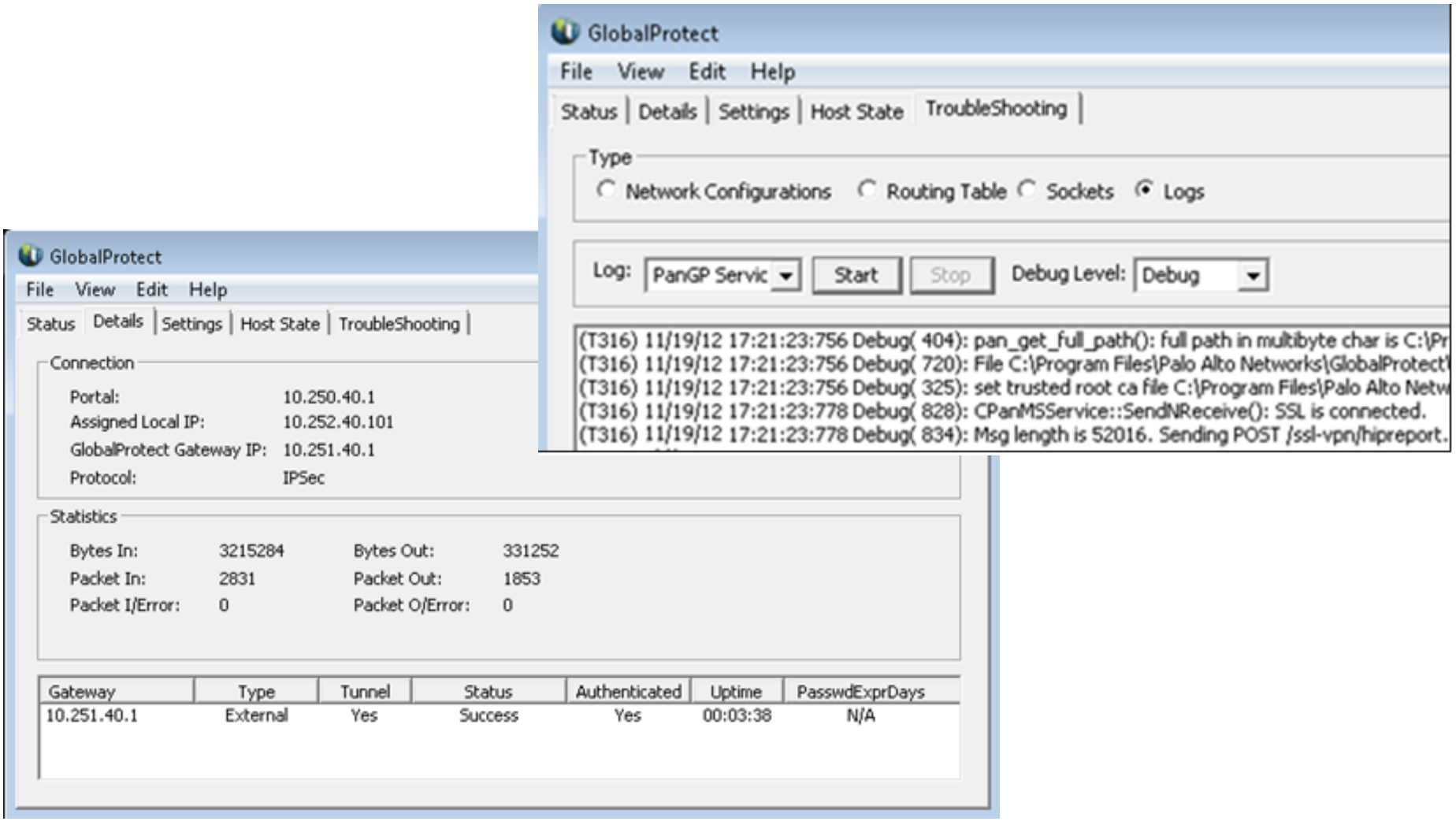


Manual gateway selection

Advanced View



Troubleshooting GlobalProtect Agent

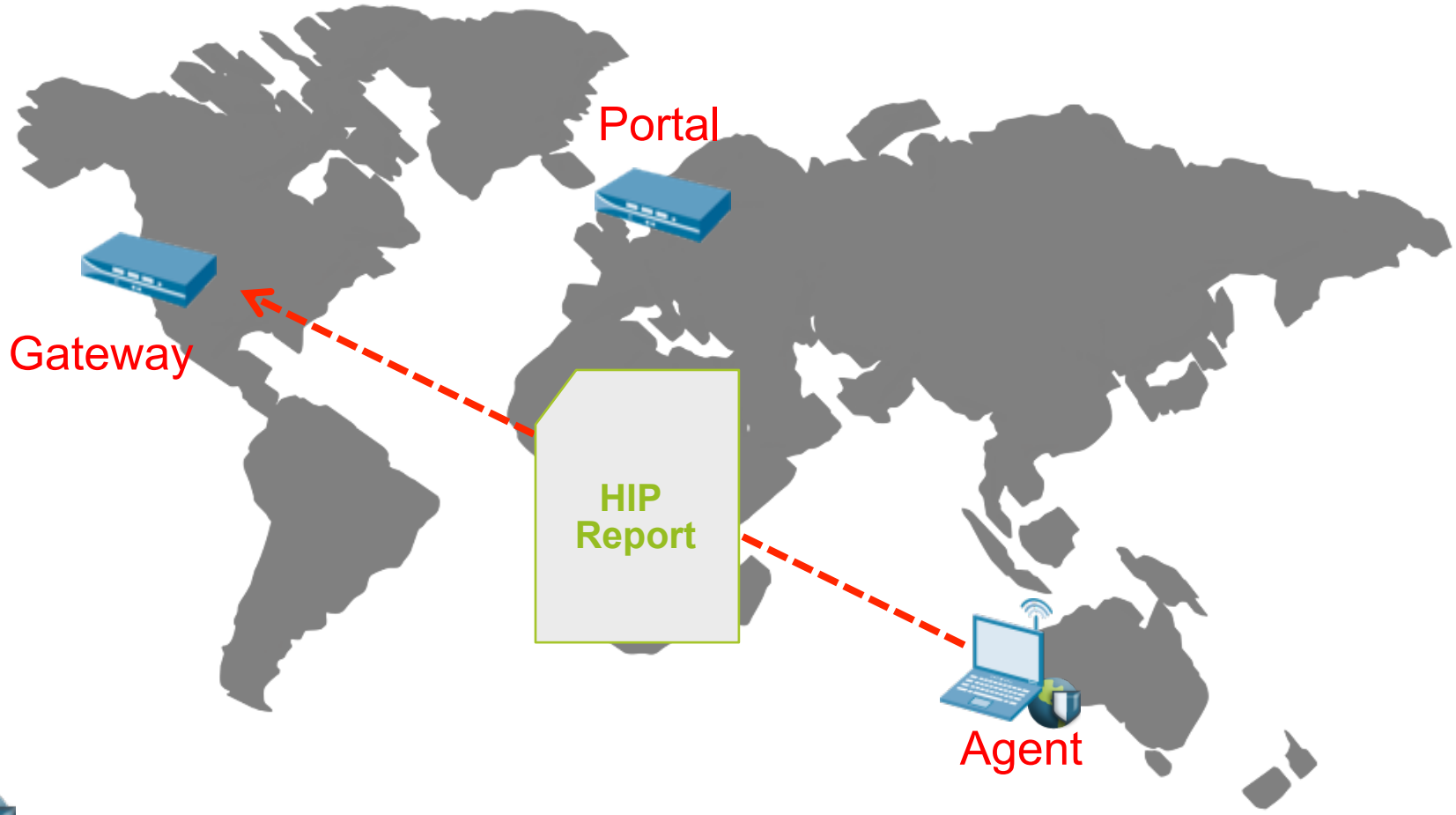


Host Checks

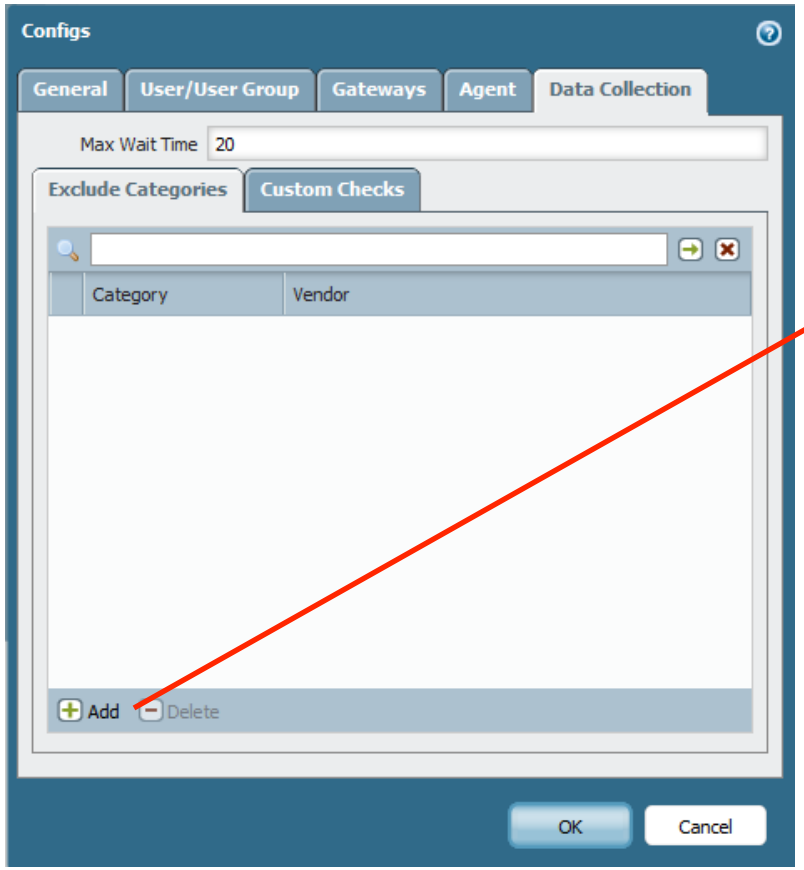
paloalto NETWORKS

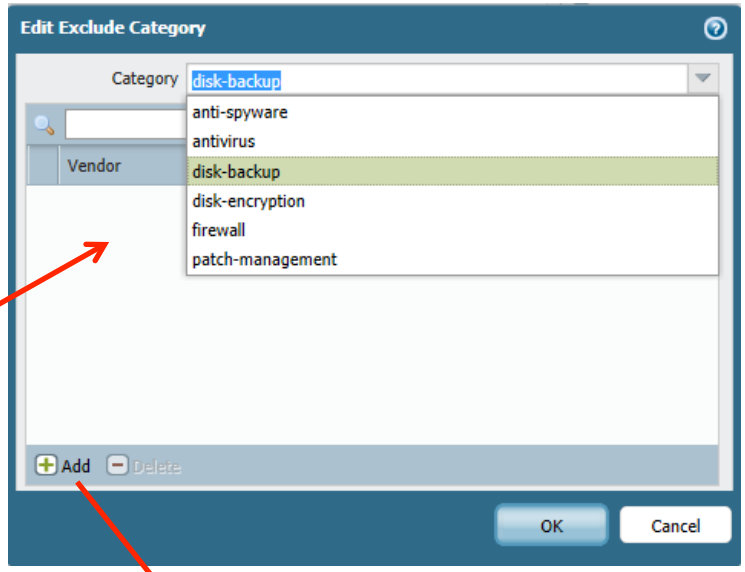
the network security company™

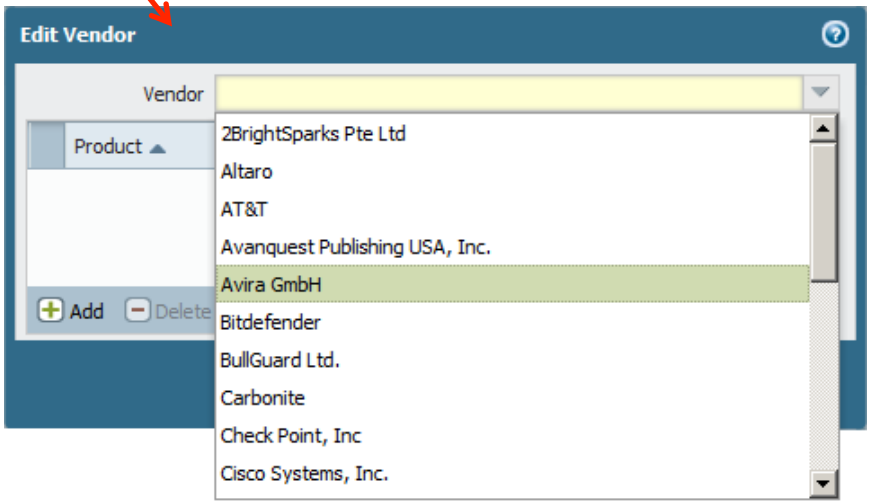
Host Information Profile (HIP)



Portal: Client Configuration – Data Collection

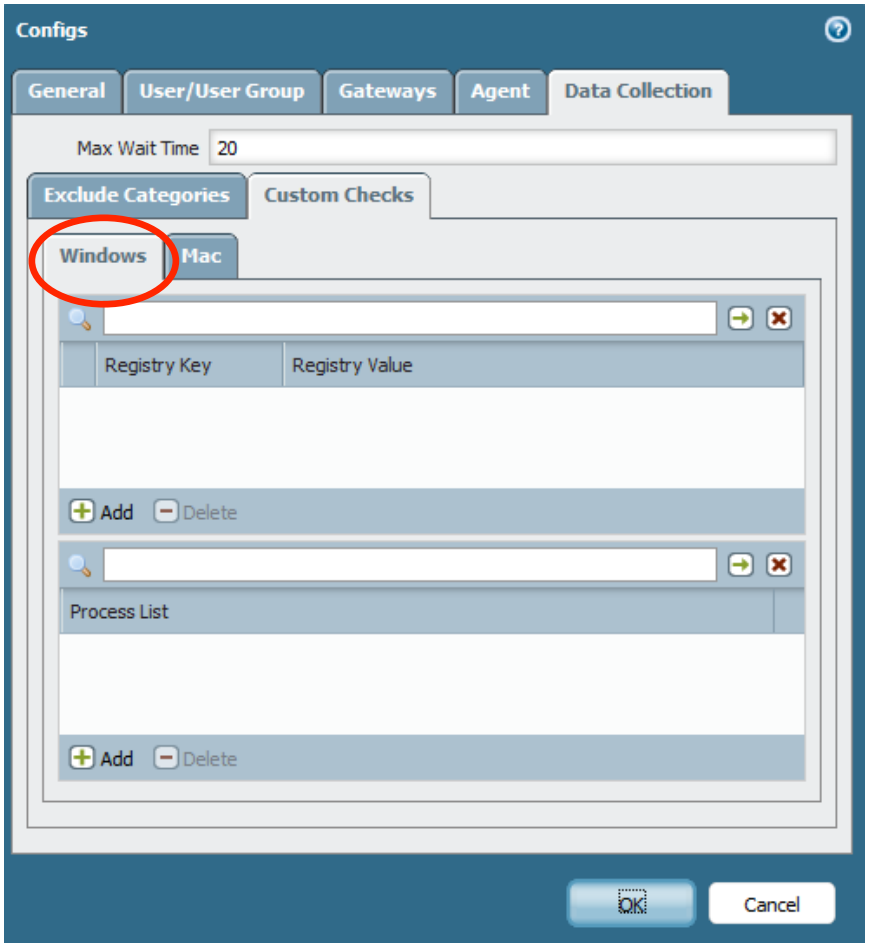


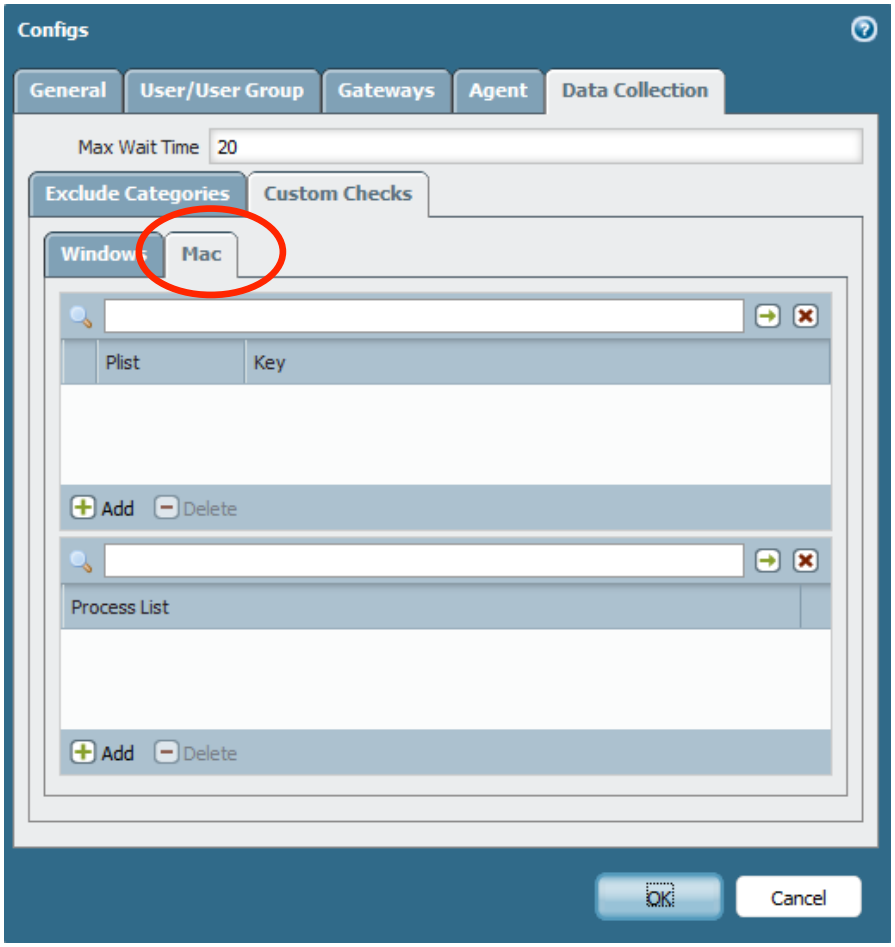




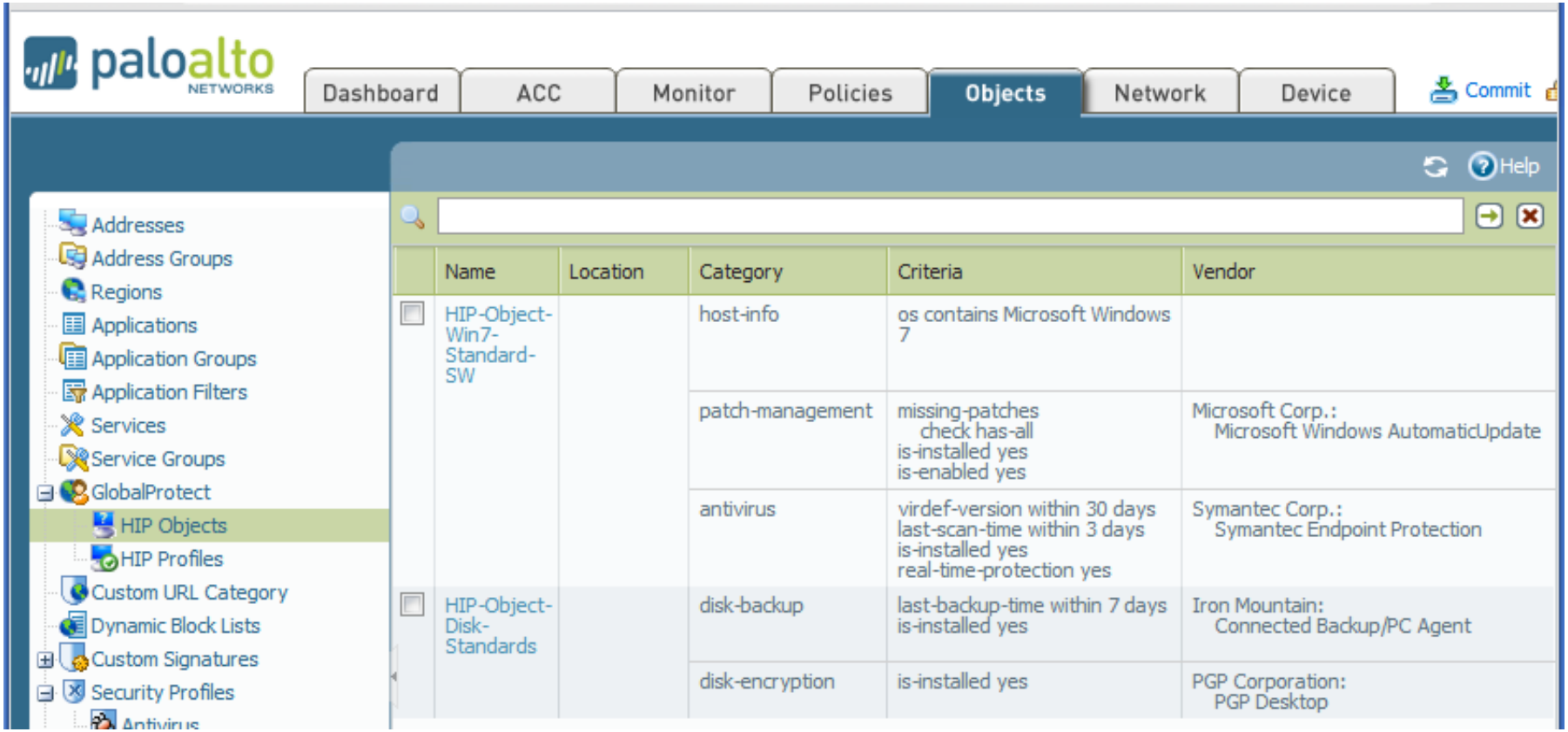
Reduces the amount of information being passed by the client to the gateway

Portal: Client Configuration – Custom Checks





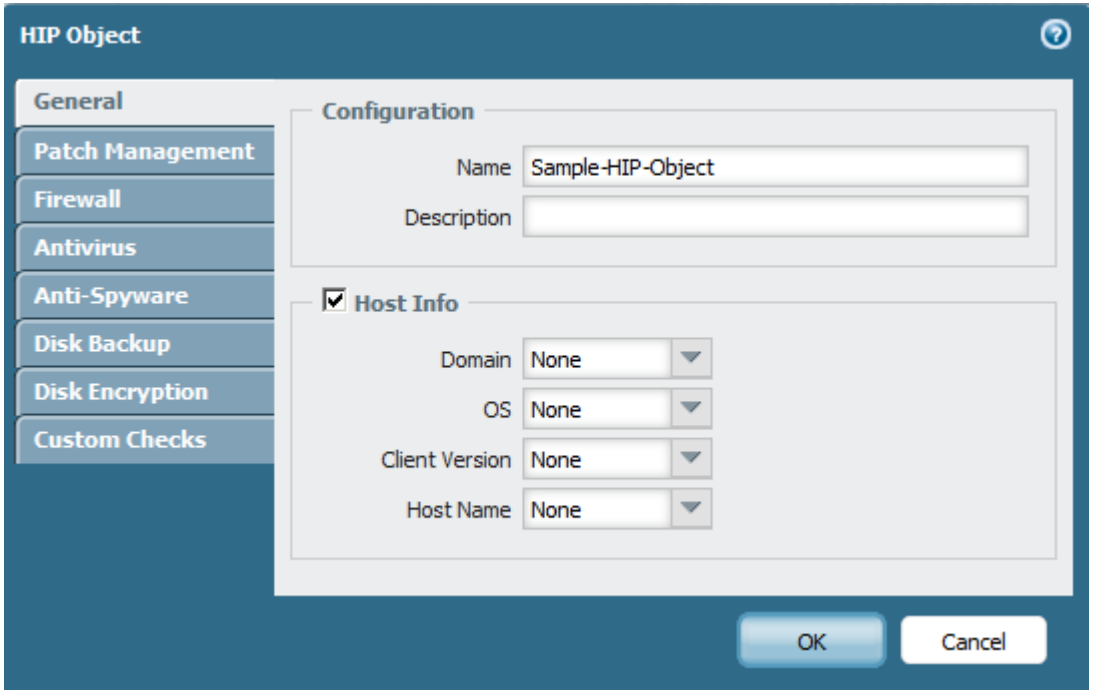
HIP Objects



HIP Objects are used to define match criteria for GlobalProtect Clients

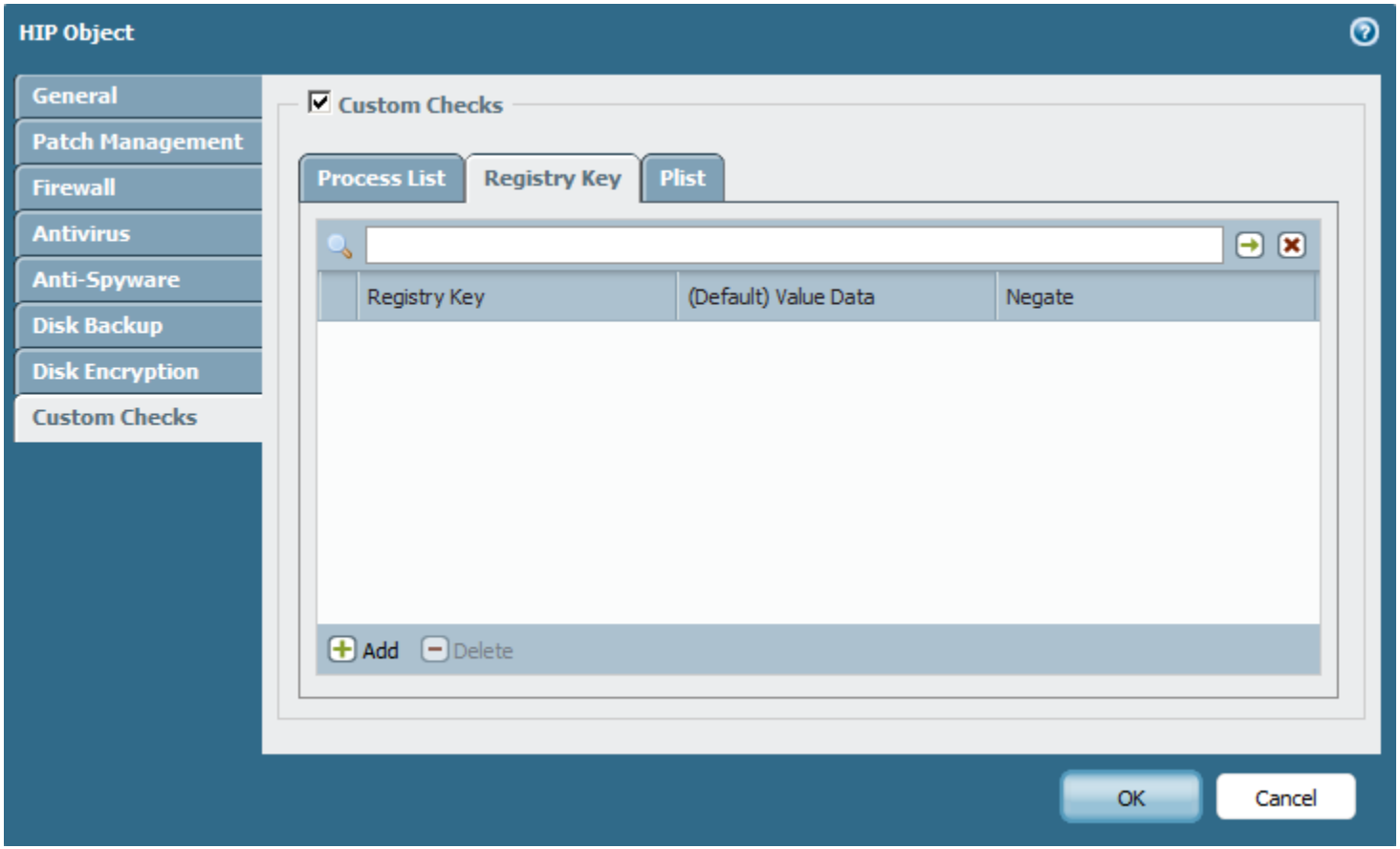
Configuring HIP Objects

Objects > GlobalProtect > HIP Objects



- Host Info
- Patch Management
- Firewall
- Antivirus
- Anti-Spyware
- Disk Backup
- Disk Encryption
- Custom Checks

Custom Checks



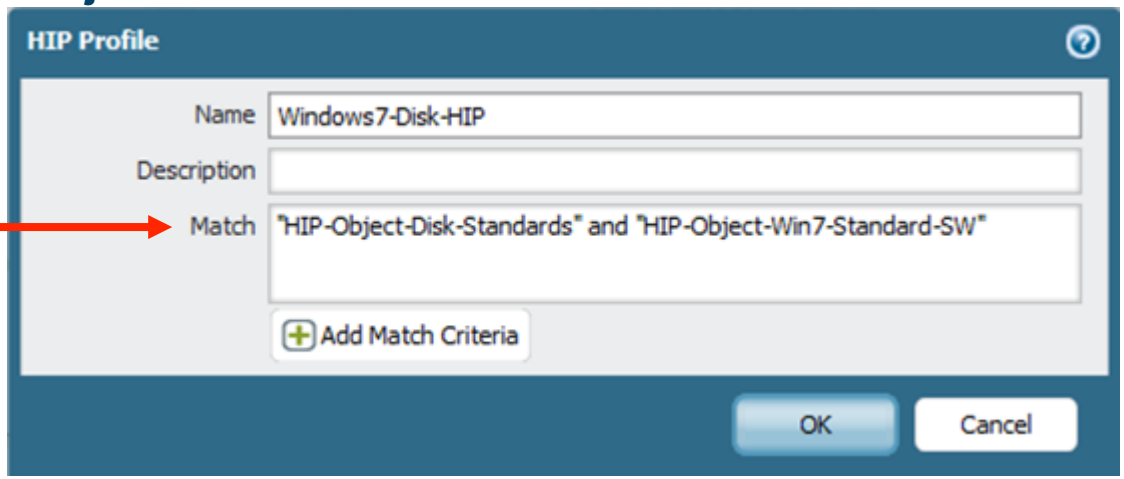
HIP objects can check for specific Registry Keys (Windows) or Plist values (Mac)

Example - HIP Objects and Profiles

Objects > GlobalProtect > HIP Objects

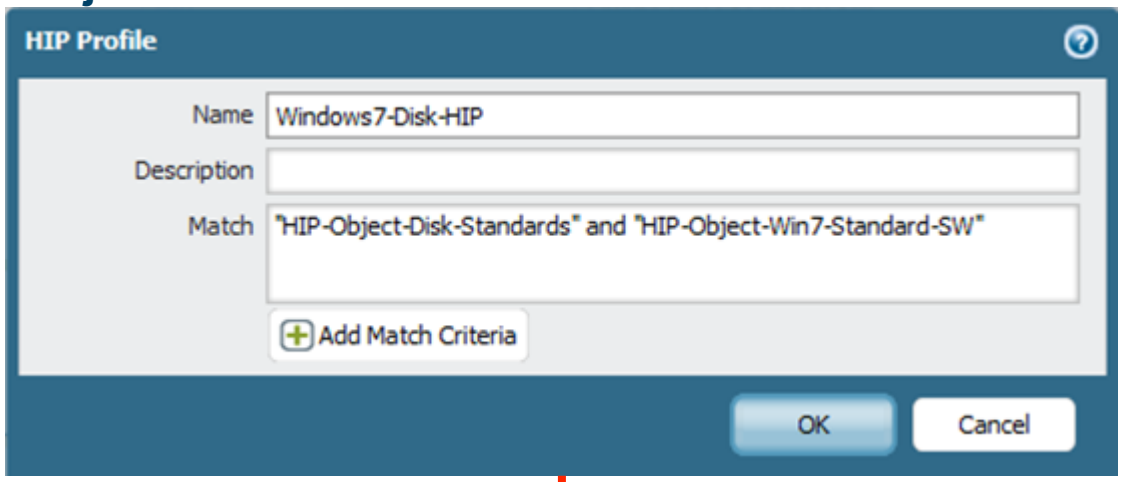
	Name	Location	Category	Criteria	Vendor
☐	HIP-Object-Win7-Standard-SW		host-info	os contains Microsoft Windows 7	
			patch-management	missing-patches check has-all is-installed yes is-enabled yes	Microsoft Corp.: Microsoft Windows AutomaticUpdate
			antivirus	last-scan-time within 3 days is-installed yes real-time-protection no	Symantec Corp.: Symantec Endpoint Protection
☐	HIP-Object-Disk-Standards		disk-backup	last-backup-time within 7 days is-installed yes	Iron Mountain: Connected Backup/PC Agent
			disk-encryption	is-installed yes	PGP Corporation: PGP Desktop

Objects > GlobalProtect > HIP Profiles



Security Policy with HIP Profile

Objects > GlobalProtect > HIP Profiles

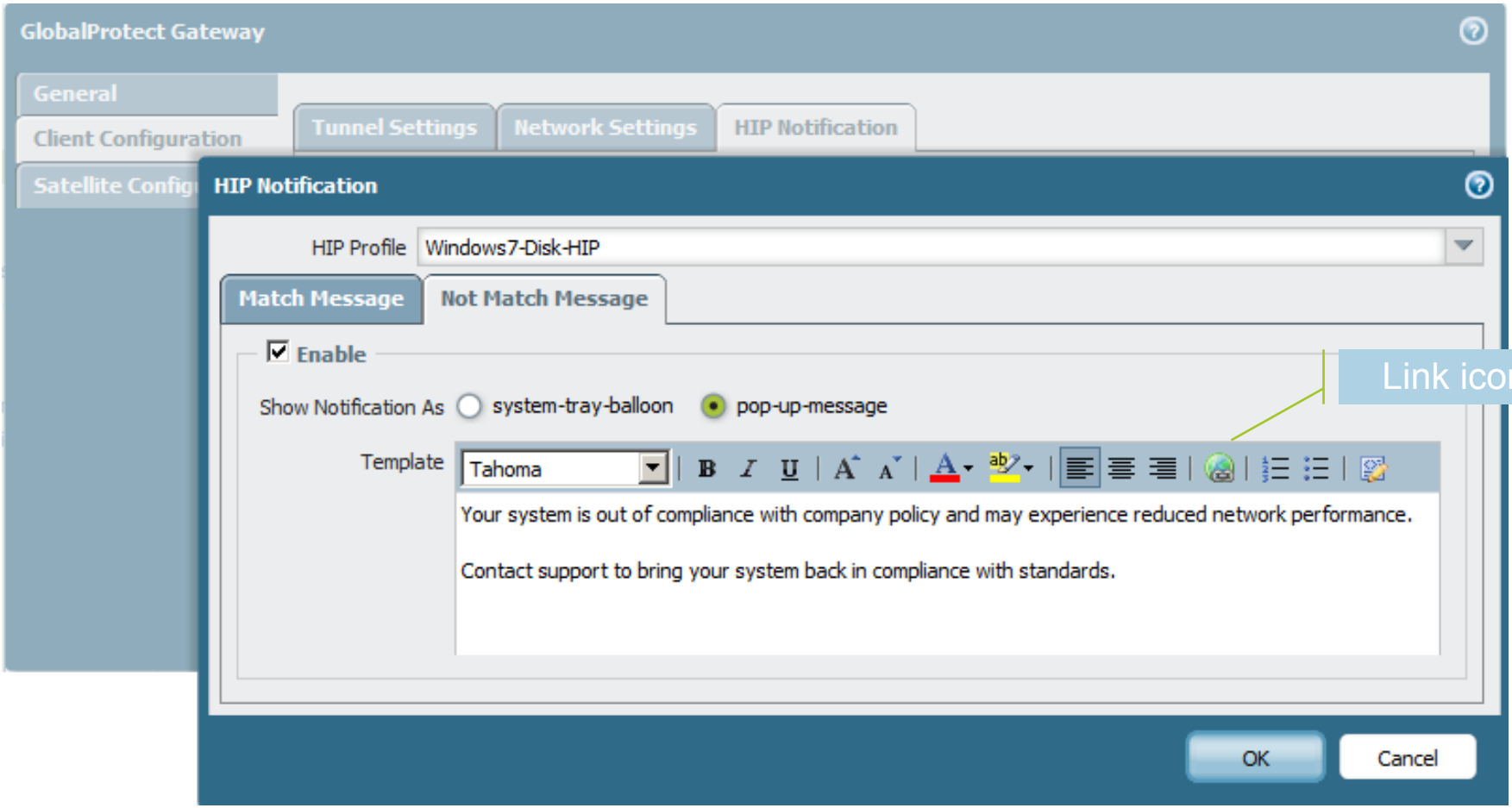


Policies > Security

	Source			Destination			
Name	Zone	User	HIP Profile	Zone	Application	Service	Action
General Internet	Trust-L3	any	Windows7-Disk-HIP	Trust-L3	Known-Good	any	

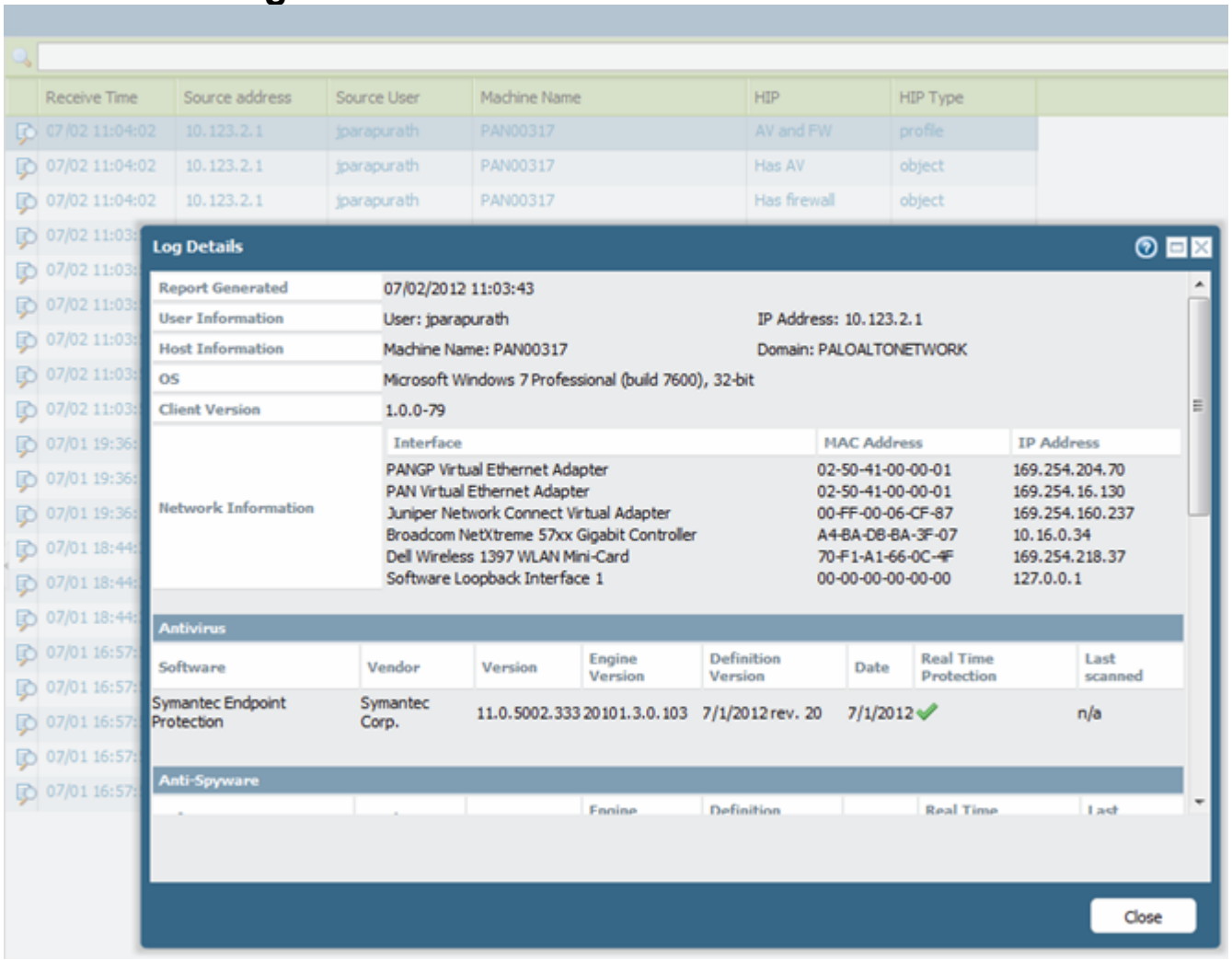
Gateway: HIP Notification

Network > GlobalProtect > Gateways

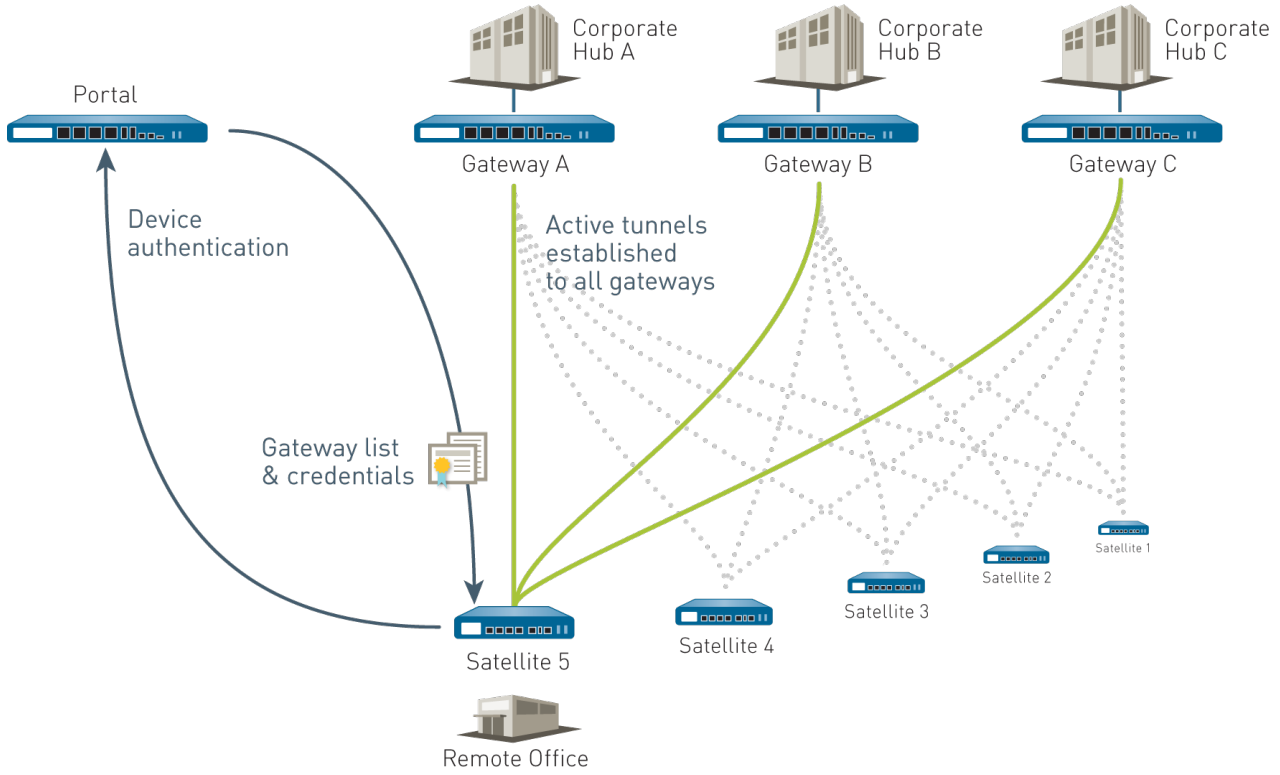


HIP Match Log

Monitor > Logs > HIP Match



Large-Scale VPNs with GlobalProtect Satellites

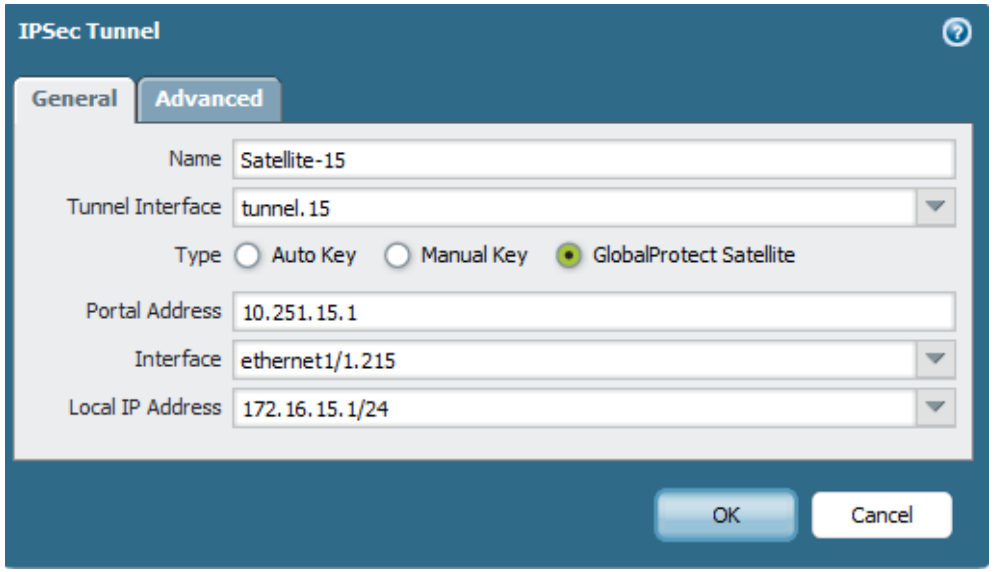


- GlobalProtect Satellites connect to existing Portal and Gateways
- Receive network and routing information from Portal like standard clients
- Minimal deployment tasks on Satellite device
- Satellites can be connected to multiple gateways simultaneously

Satellite Deployment

- Satellite devices can be easily deployed once Portal and Gateways are in place
- Deployment effort on the Satellite side is minimal
  - Get device connected to the internet
  - Create a tunnel interface
  - Add GlobalProtect Portal hostname to the IPSec Tunnel satellite configuration

Network > IPSec Tunnels



Panorama

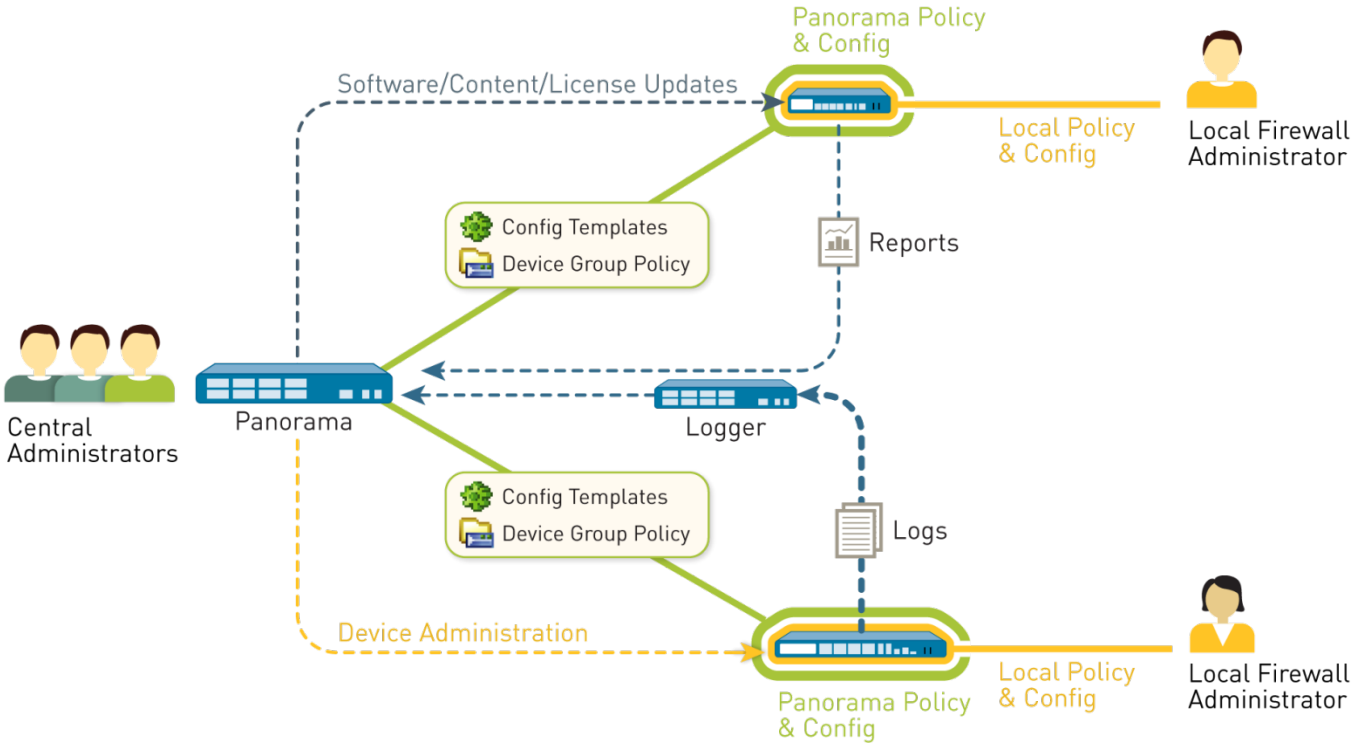
CNSE Bootcamp

Panorama

paloalto NETWORKS

the network security company™

Panorama Benefits



Panorama is designed to provide three benefits:

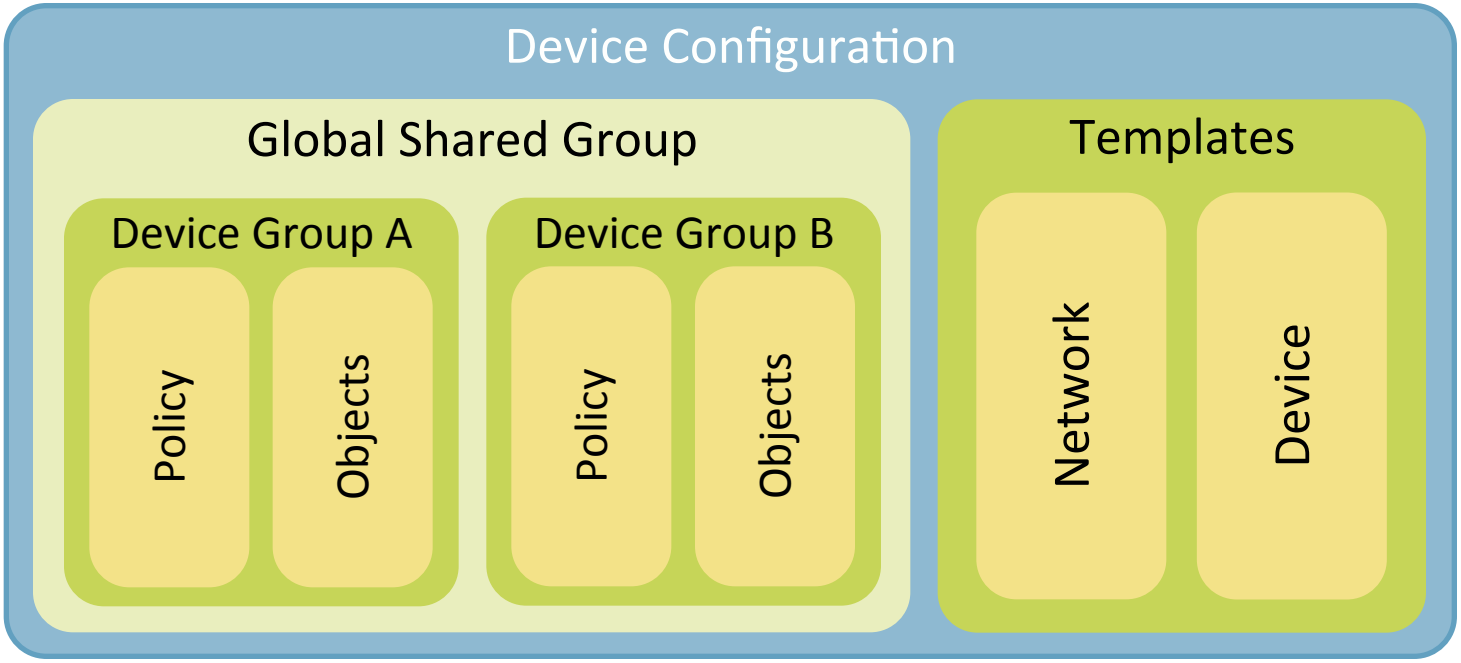
- Centralized configuration management
- Centralized logging and reporting
- Centralized deployment management

Deployment

- Virtual Machine Appliance
  - Simple installation and maintenance
  - Allows for tailored hardware and operating system
  - Disks and CPU can be sized to fit deployment requirements
  - Minimum: VMware ESX(i) 3.5+ or VMware Server 1.0.6+
- Physical Appliance (M-100)
  - Simple, high-performance, dedicated appliance for Panorama
  - Simplifies deployment and support for non-VMware environments
  - Includes distributed log collection capability for large scale deployments
- Licensed by number of managed devices: 25, 100, 1000

Device Groups and Templates

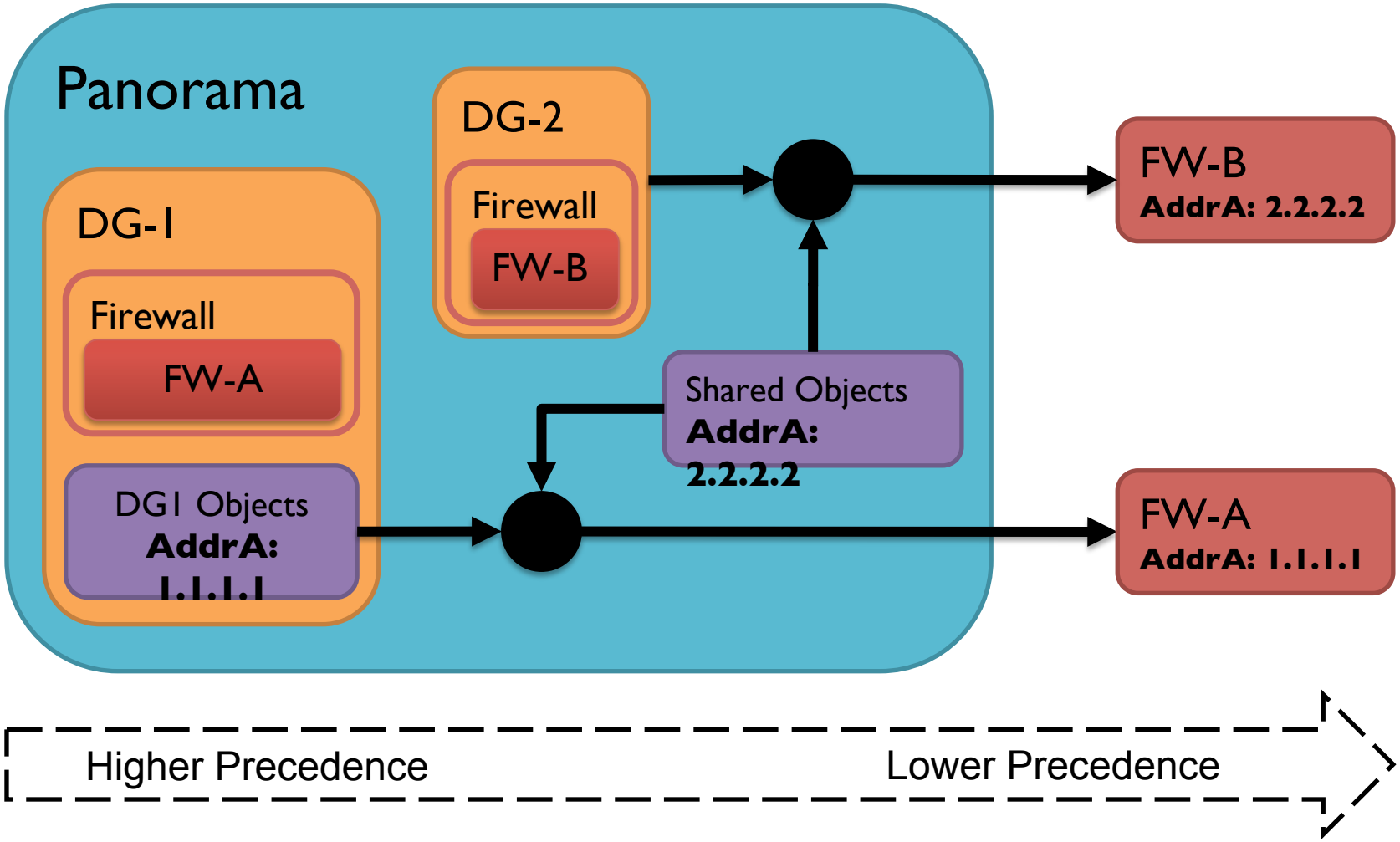
- Device Groups manage shared Policies and Objects
- Templates manage Network and Device configurations



Objects

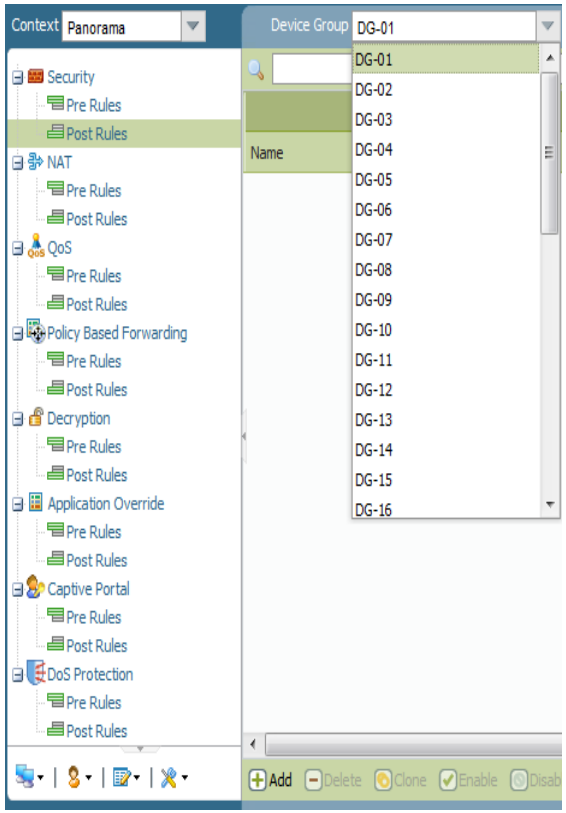
- Types of Objects
  - “Objects” tab objects (e.g. Address groups)
  - Server Profiles (SNMP, Syslog, Email, RADIUS, LDAP, Kerberos)
  - Auth Profile/Sequence
  - Client Cert Profile
  - Certificates
  - Block Pages

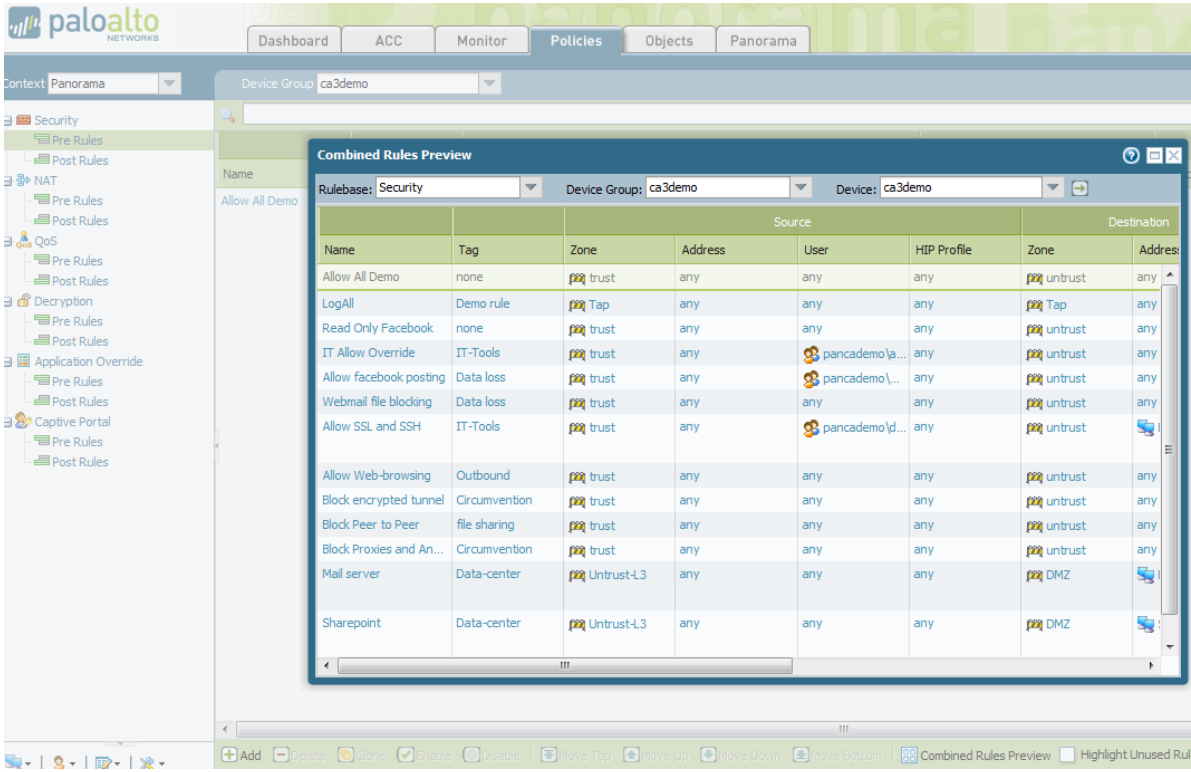
Objects | Precedence

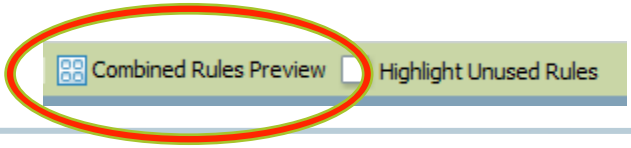


Shared Policy | Pre and Post Policy Config

- Device Groups manage shared Policy and Objects
- Policy can be targeted to groups or specific firewalls
- Pre/Post-rules **cannot** be edited inside firewall once pushed



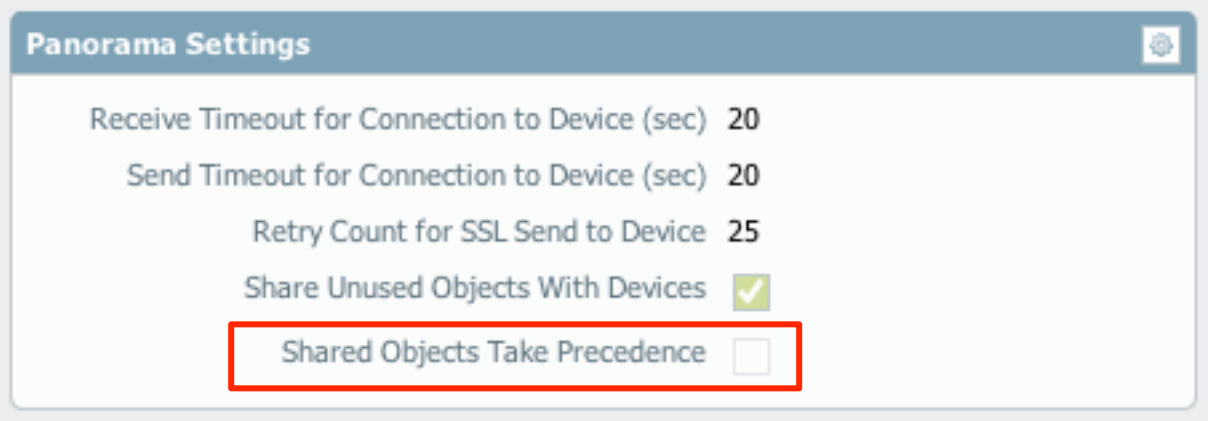




Managing Shared Objects

- Shared objects can be overridden by creating device group objects with the same name
- Use the **Shared Objects Take Precedence** option in the Panorama WebUI to turn off the capability for a device group administrator to override objects used in shared policy

Panorama > Setup > Management > Panorama Settings



Managing Policy with Panorama

- Panorama Policy are tied to Device Groups
  - Policy can be targeted to be pushed to device groups or specific firewalls
- Panorama rules **cannot** be edited inside firewall once pushed

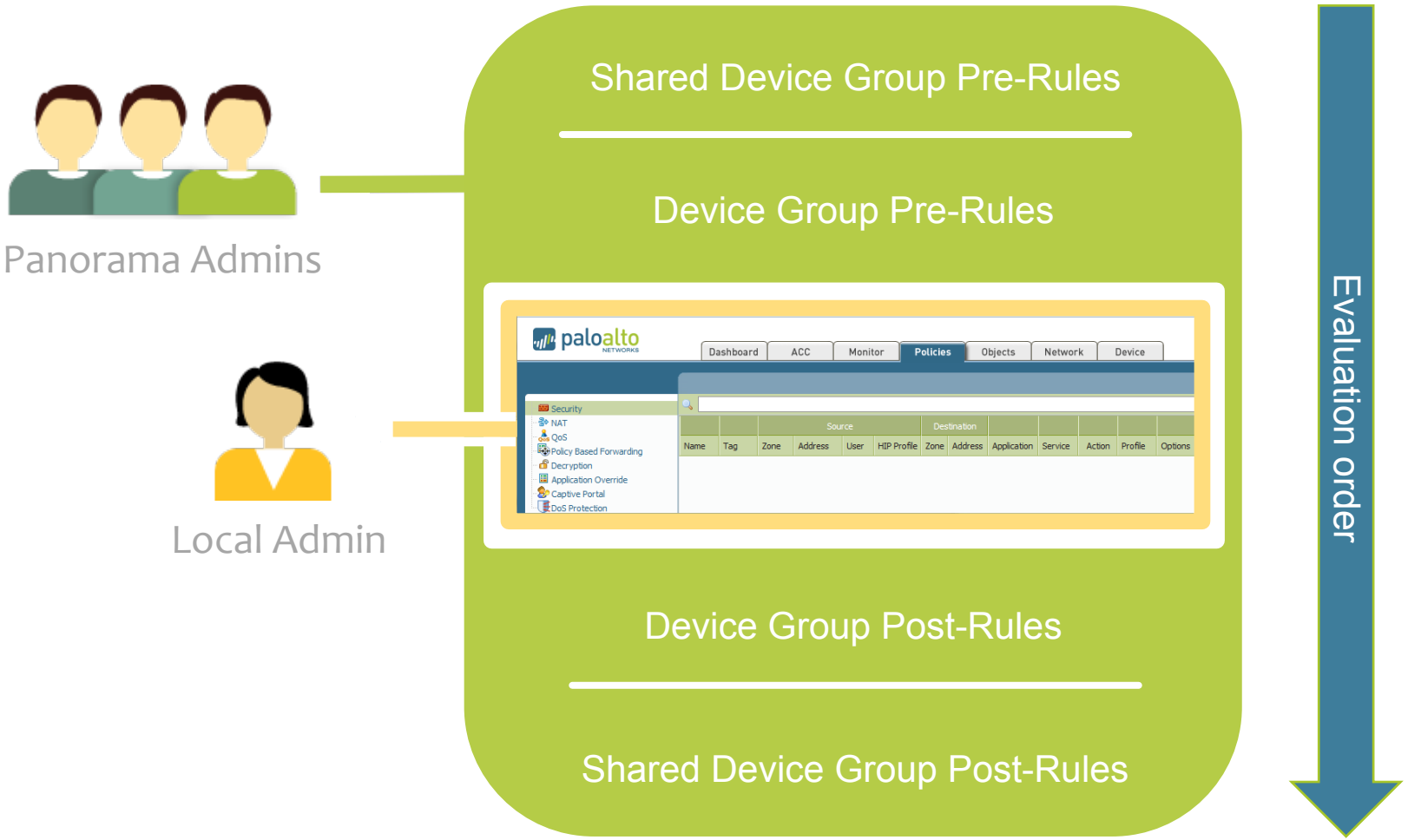
Policies > Security

Panorama Pre Rules

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

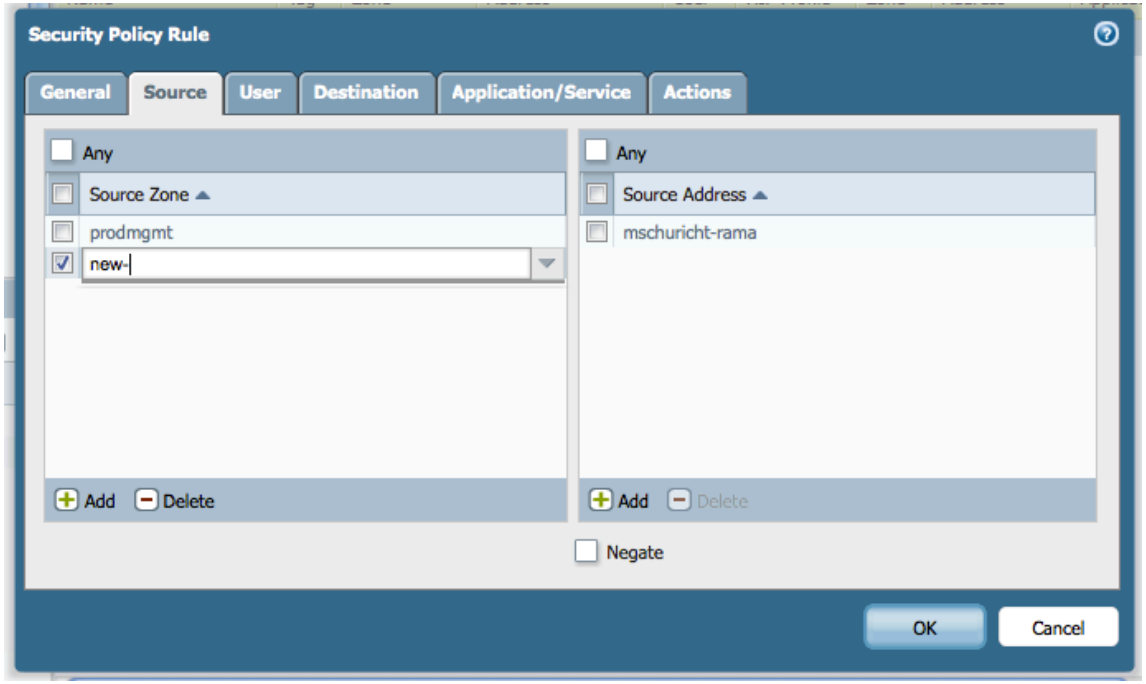
Panorama Post Rule

Policy Evaluation Order

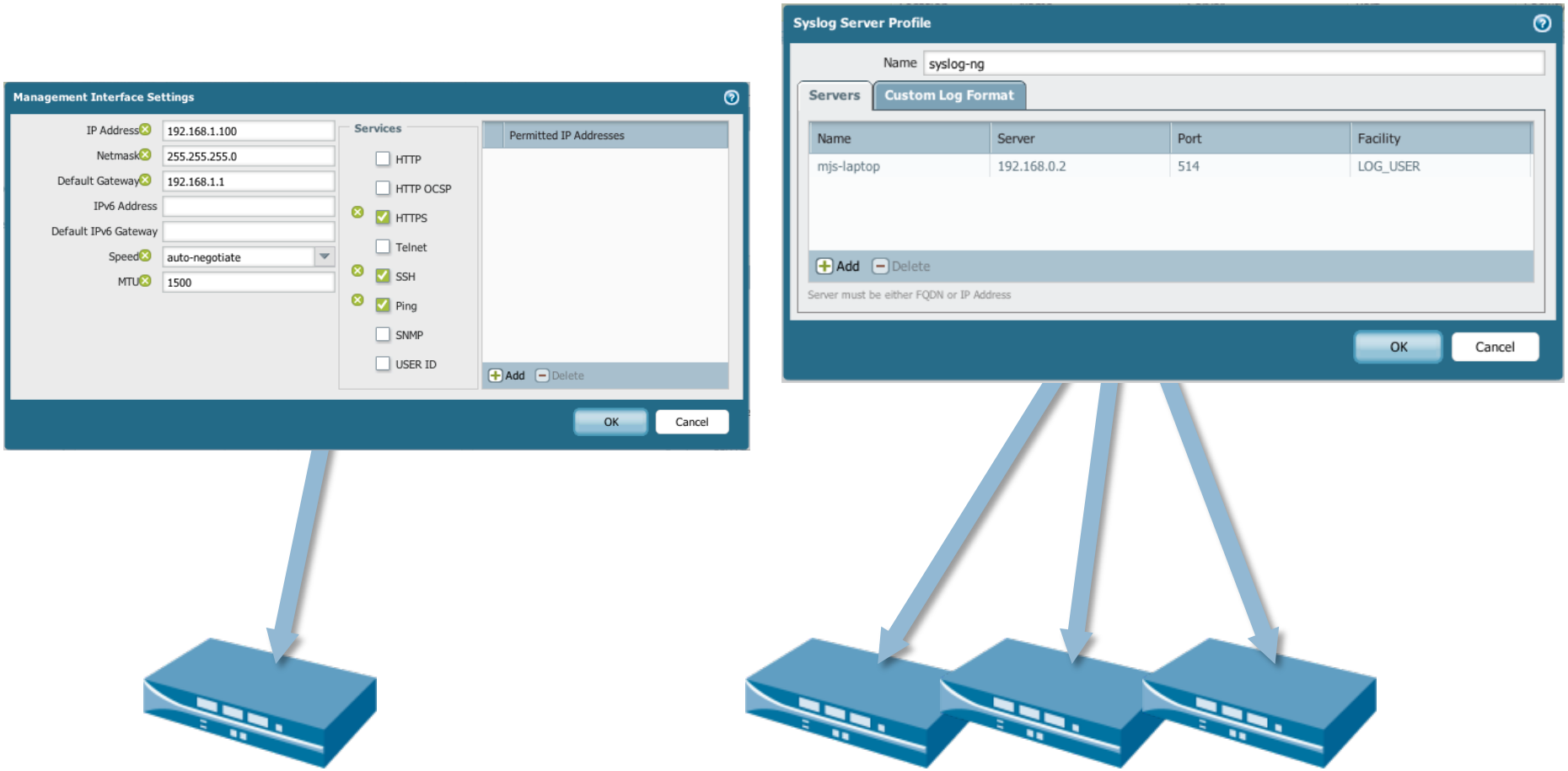


Shared Policy | Zones

- Zones are required to be manually entered once
  - Commit All will fail if Zone does not exist on firewall
- Deletion occurs when no references or wrong reference (e.g. Missing, misspellings, case sensitivity) exists to a Zone string
  - No Zone management table like other “objects”

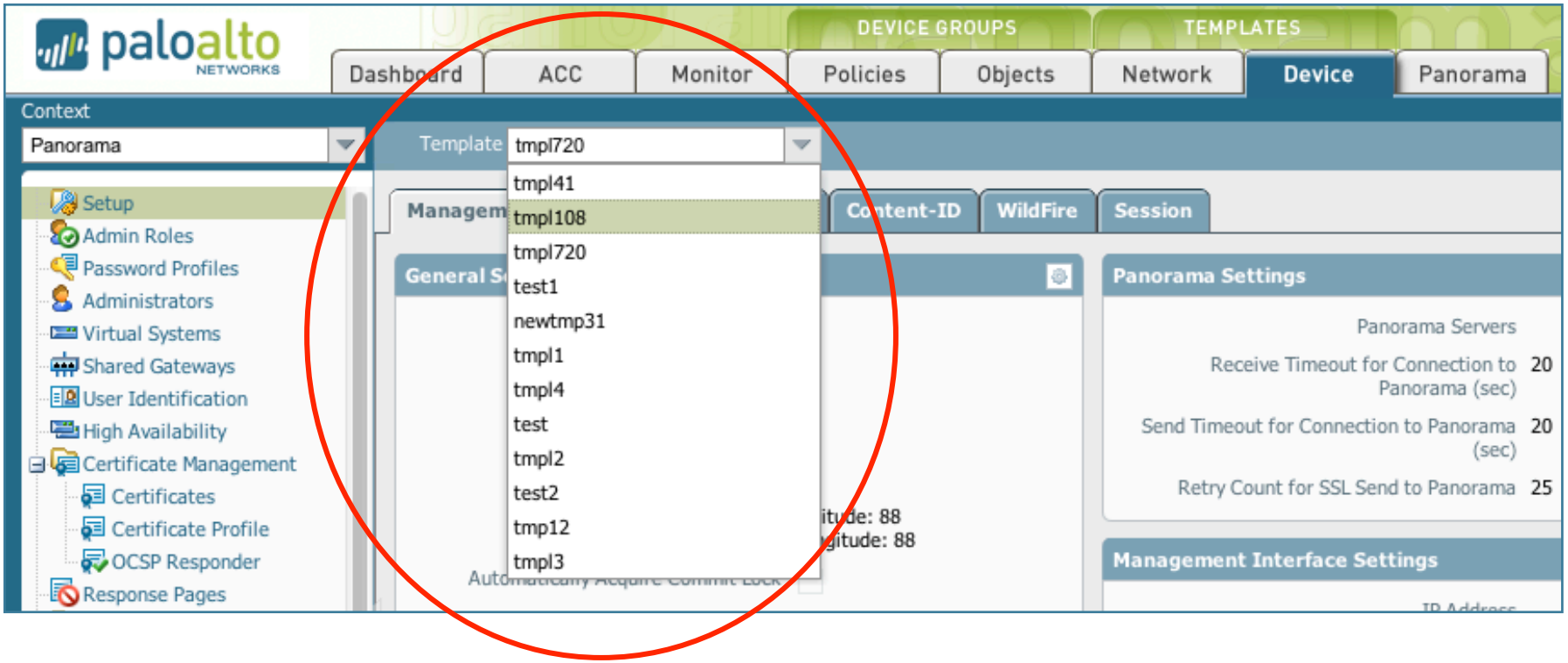


How to Use Templates



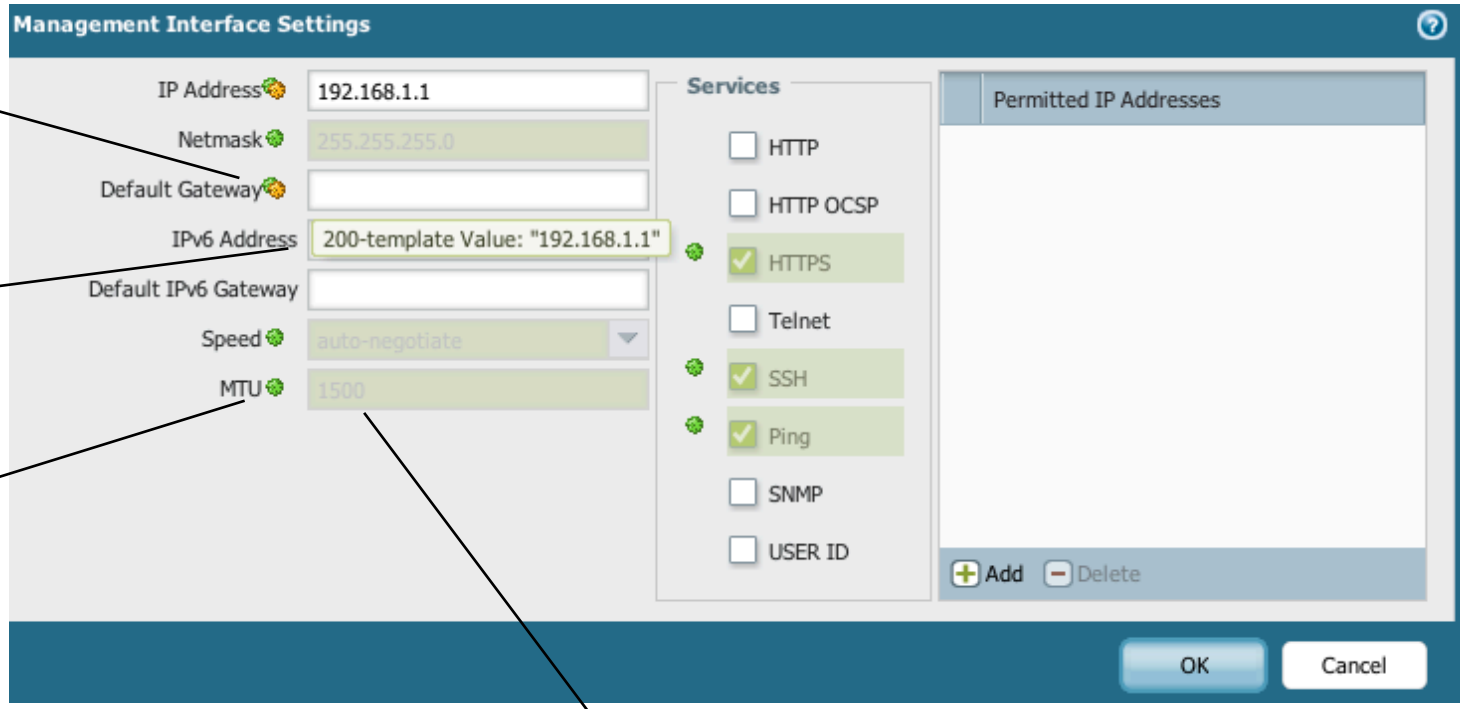
- Device specific settings applied to only one device
- Common settings spread across multiple devices

Select Template in Device and Network Tabs



Override Values on Managed Device

Individual fields can be overridden where granularity is needed
e.g., **Device > Setup**, User Identification, High Availability



Indicates overridden value

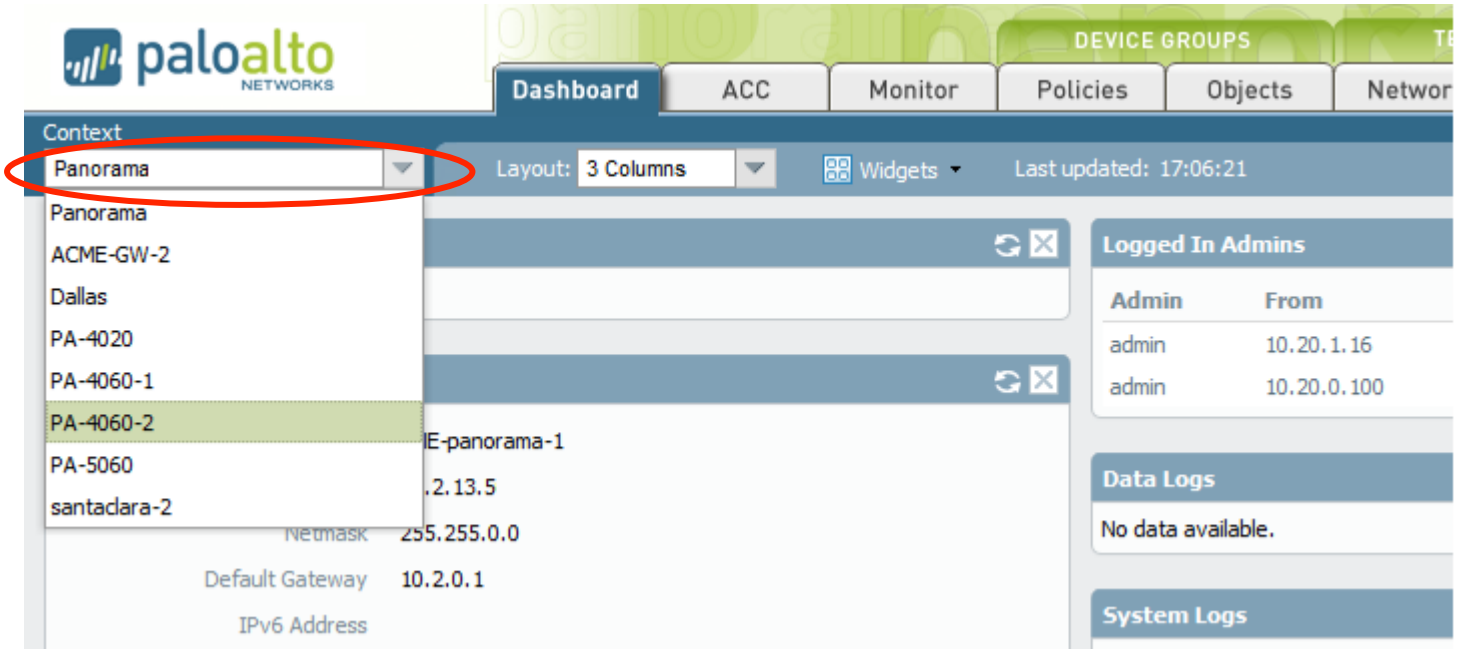
Template name and value upon revert

Indicates templated value

Templated value

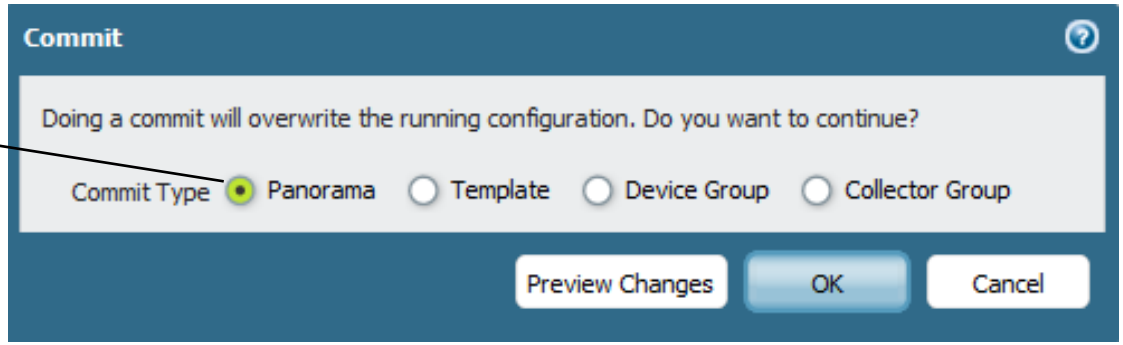
Context Switch

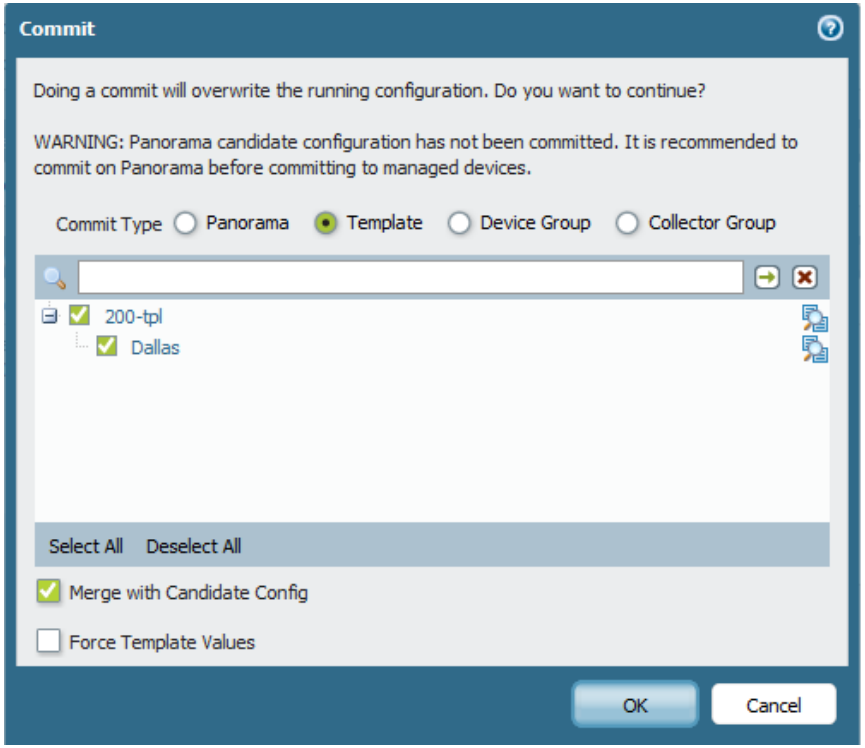
- Device configuration editing is done through **Context** switch
  - Controlled via “Administrator” and “Access Domain”
  - Panorama proxies the management connection
- Access can be given to admins based on Device[/VSYS]

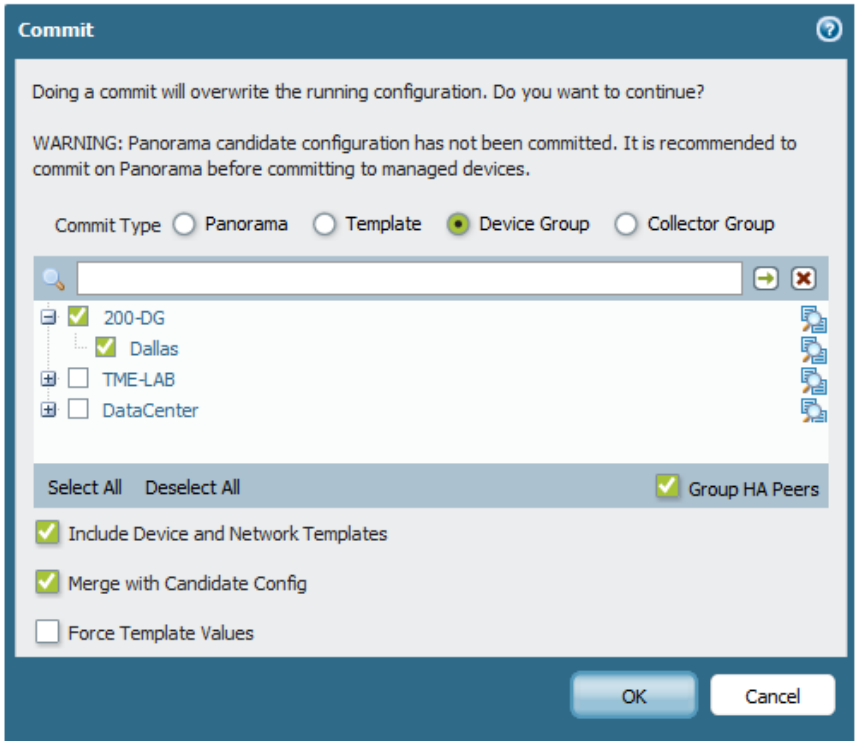


Commit Workflow

A Panorama commit must happen before any other type of commit can run

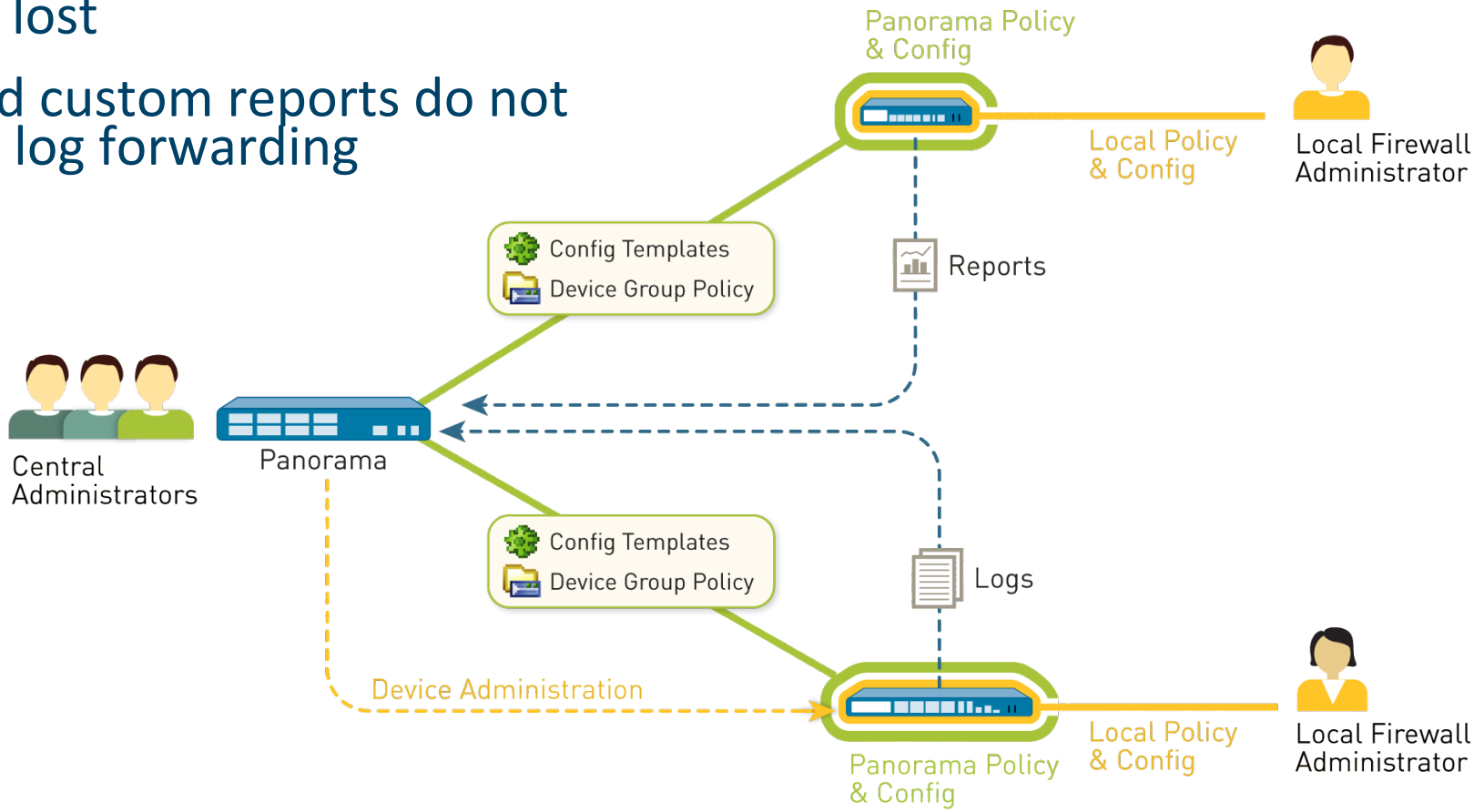






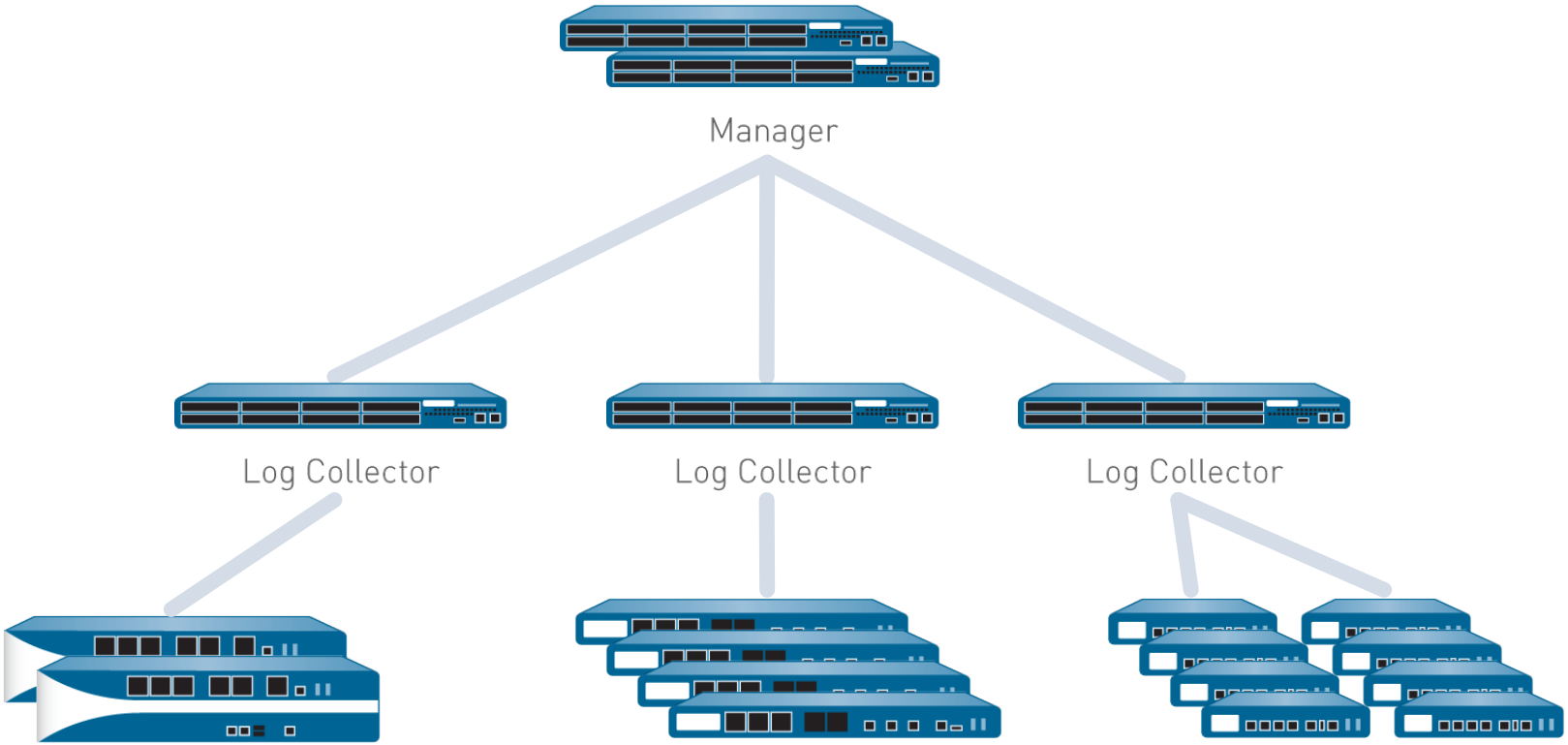
Logging and Reporting

- Panorama aggregates logs from entire deployment
- Device log buffering occurs so logs are not lost
- ACC and custom reports do not require log forwarding

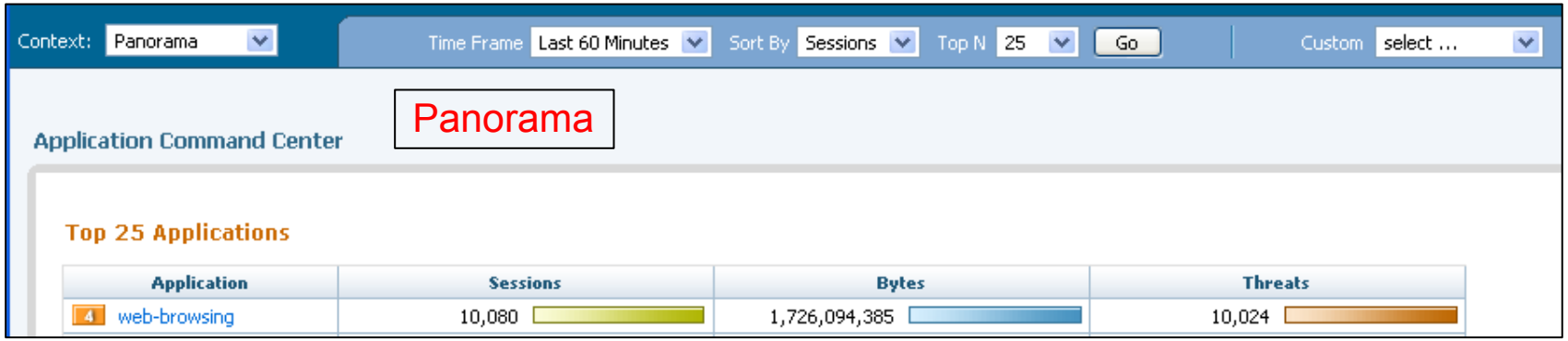


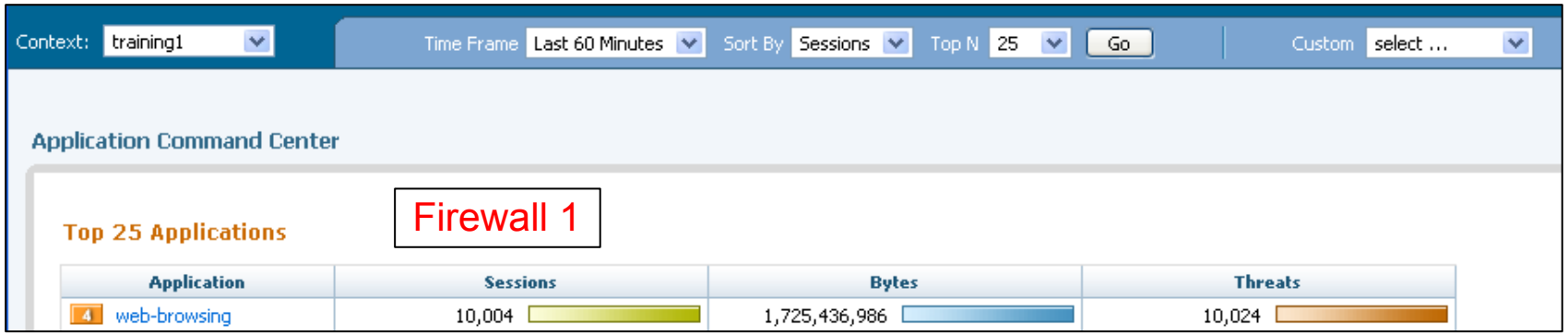
Panorama Distributed Architecture

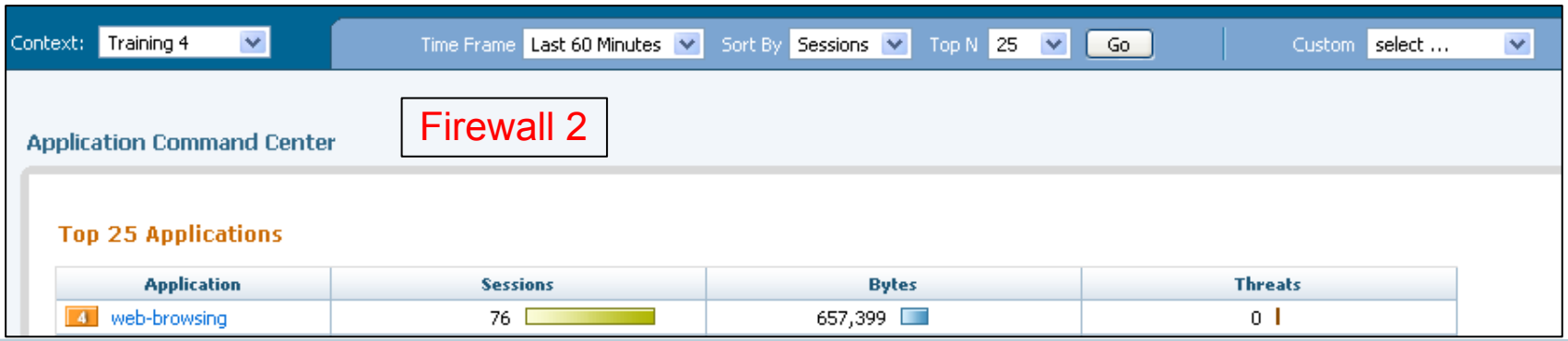
- With the M-100, manager and log collector functions can be split
- Deploy multiple log collectors to scale collection infrastructure
  - Log collection can only be run on the M-100 platform



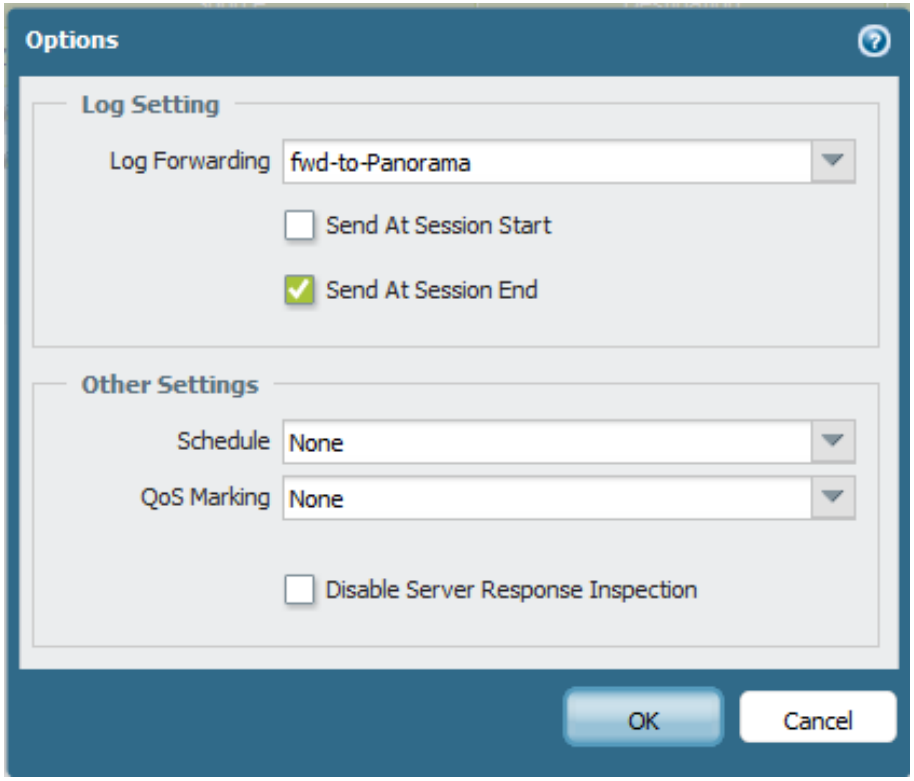
Aggregate Logging







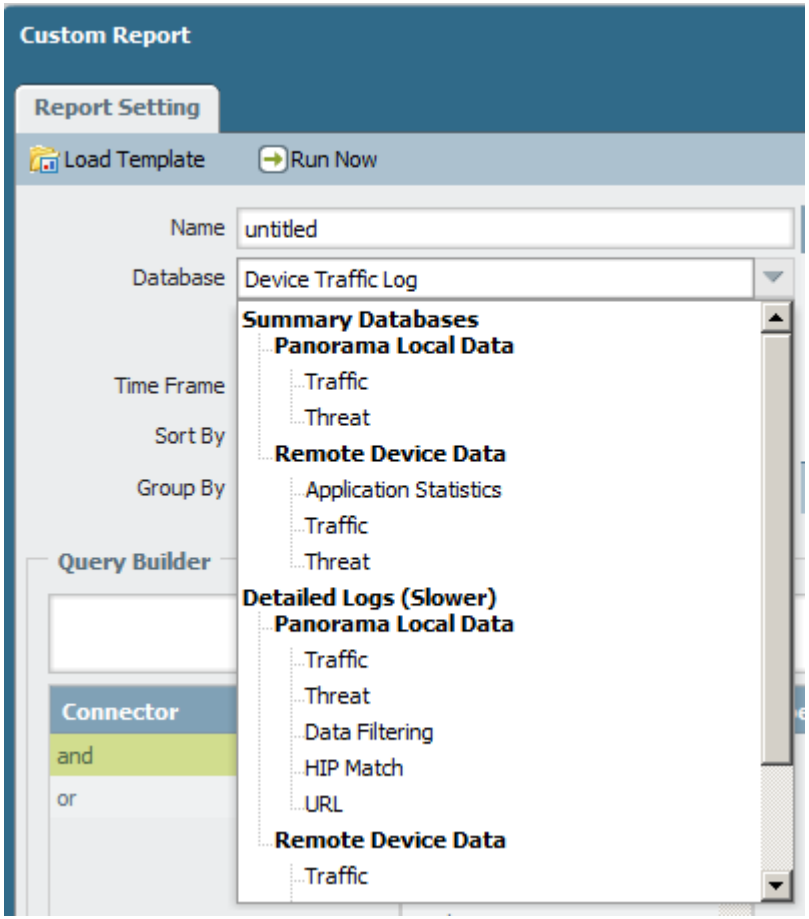
Logging and Reporting Configurations



- Long term log storage and local reporting require log forwarding
- ACC browsing and Reports do not require explicit log forwarding

Logging and Reporting Data Types

- Scheduled reports (Built-in & User defined)
  - Utilize 60min statistics files
  - Aggregate file data when schedule is executed
- Built-in reports – database selection
  - Panorama vs. Firewall <logDB>
  - “Run Now” with Firewall DB pulls data dynamically
- All logs are sent with serial number of the individual firewalls



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)

Questions?

paloalto NETWORKS

the network security company™