

CNSE 5.1 Study Guide

Version 2.2

*Palo Alto Networks
Education Services*

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 enabled¹)
- 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/max²)
- 40 security zones
- 5,000 max number of policies

PA-3020



- 2 Gbps firewall throughput (App-ID enabled¹)
- 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/max²)
- 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 enabled¹)
- 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

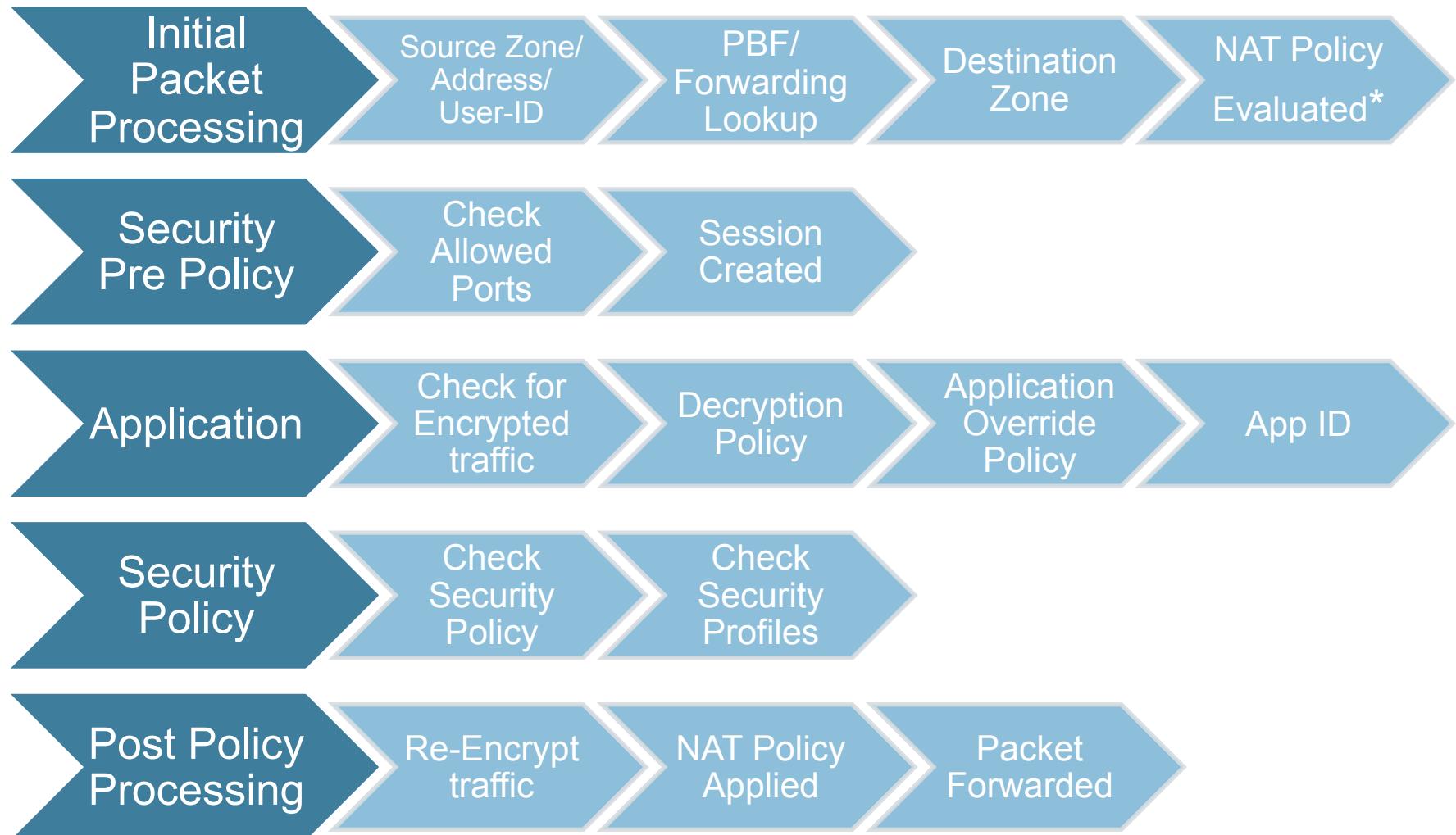


You can deploy Panorama as a virtual appliance on VMware ESX(i), allowing you to support your virtualization initiatives and consolidate rack space.

Security Subscriptions

- Threat Prevention
- URL Filtering
- Global Protect
- WildFire

Flow Logic



Packet Flow

- Refer to this document on the packet flow in PAN-OS:
[Packet Flow.pdf](#)
- Have a general understanding of how packets 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

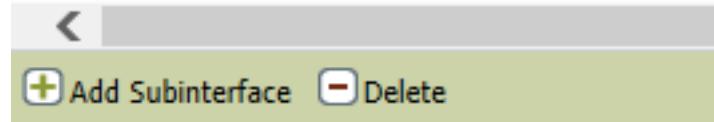
5 Physical Interface Types

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

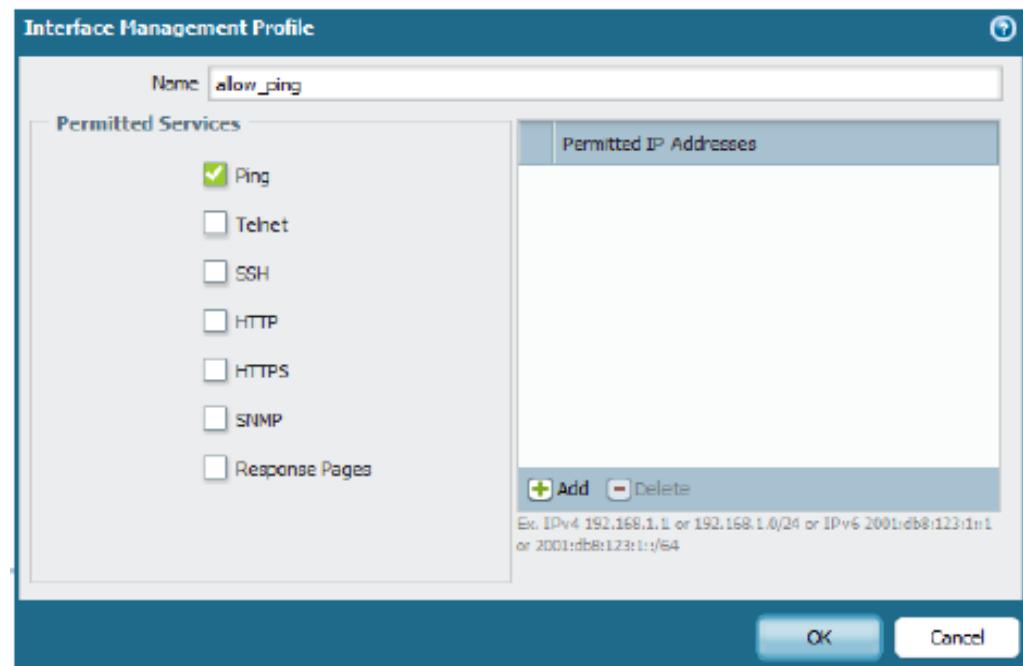
- No VPN
- No NAT (FYI Starting PAN-OS 4.1 you can do NAT in Vwire mode)
- If IPv6 is passing, security policies can be written for this traffic
- No Multicast support

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 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 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.

The screenshot shows the Palo Alto Networks Application Selection window. At the top, there are tabs for Dashboard, ACC, Monitor, Policies, Objects (selected), Network, and Device. Below the tabs, there is a search bar, a 'Custom Only' checkbox, and a 'Clear Filters' button. A message indicates '1652 matching applications'. The main area displays a table with columns: Category, Subcategory, Technology, Risk, and Characteristic. The first section of the table lists categories like business-systems, collaboration, general-internet, media, networking, and unknown, along with their respective subcategories and technologies. The second section lists individual applications with their details. At the bottom, there are navigation buttons for pages, and standard application management buttons: Add, Delete, Clone, Import, and Export.

Category	Subcategory	Technology	Risk	Characteristic
340 business-systems	40 audio-streaming	611 browser-based	453	592 Evasive
442 collaboration	14 auth-service	700 client-server	394	506 Excessive Bandwidth
274 general-internet	18 database	219 network-protocol	369	288 Prone to Misuse
222 media	66 email	120 peer-to-peer	301	780 Transfers Files
372 networking	41 encrypted-tunnel		135	273 Tunnels Other Apps
2 unknown	21 erp-crm			273 Used by Malware
	203 file-sharing			939 Vulnerability
	56 gaming			1052 Widely used

Name	Category	Subcategory	Risk	Technology
100bao	general-internet	file-sharing	5	peer-to-peer
1und1-mail	collaboration	email	3	browser-based
2ch	collaboration	social-networking	2	browser-based
2ch-posting	collaboration	web-posting	2	browser-based
360-safeguard-update	business-systems	software-update	2	client-server
3pc	networking	ip-protocol	1	network-protocol
4shared	general-internet	file-sharing	4	browser-based
4sync	general-internet	file-sharing	3	client-server
51.com				
51.com-base	collaboration	social-networking	2	browser-based
51.com-bbs	collaboration	web-posting	2	browser-based

Dynamic Application Filters

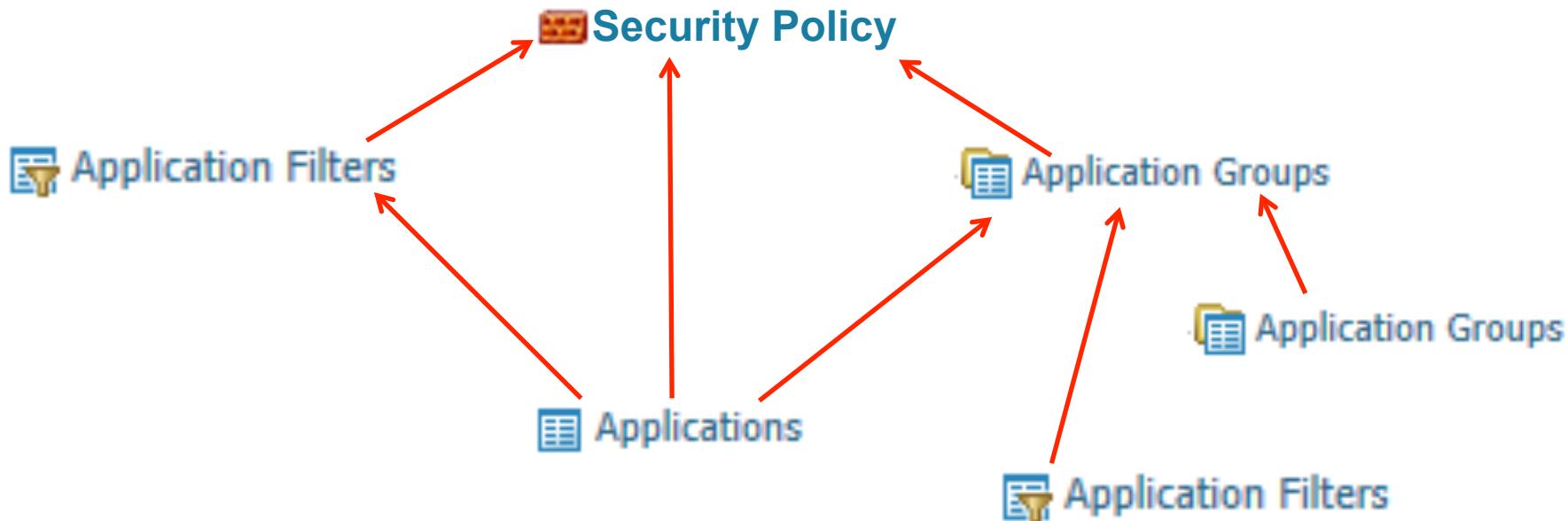
- A dynamic application filter is configured by specifying particular criteria.
- The example below is a dynamic filter to all browser-based file-sharing apps.

The screenshot shows a software interface titled "Application Filter". At the top, there is a search bar labeled "Name" and a "Clear Filters" button. To the right, it displays "1652 matching applications". The main area is a table with the following columns: Category, Subcategory, Technology, Risk, and Characteristic. The "Category" column lists various application types like business-systems, collaboration, general-internet, media, networking, and unknown. The "Subcategory" column lists specific applications such as 100bao, 1und1-mail, 2ch, 2ch-posting, 360-safeguard-update, and 3rc. The "Technology" column includes browser-based, client-server, network-protocol, peer-to-peer, and others. The "Risk" column uses colored boxes to indicate severity (green for low, yellow for medium, orange for high, red for critical). The "Characteristic" column lists various traits of the applications. Below this table is another table with columns: Name, Category, Subcategory, Risk, and Technology. It lists the same set of applications with their respective details. At the bottom, there are navigation buttons for "Page 1 of 44", a "Displaying 1 - 40 of 1747" status message, and "OK" and "Cancel" buttons.

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 Groups are static. Applications are manually added and maintained by firewall administrators.
- Application 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

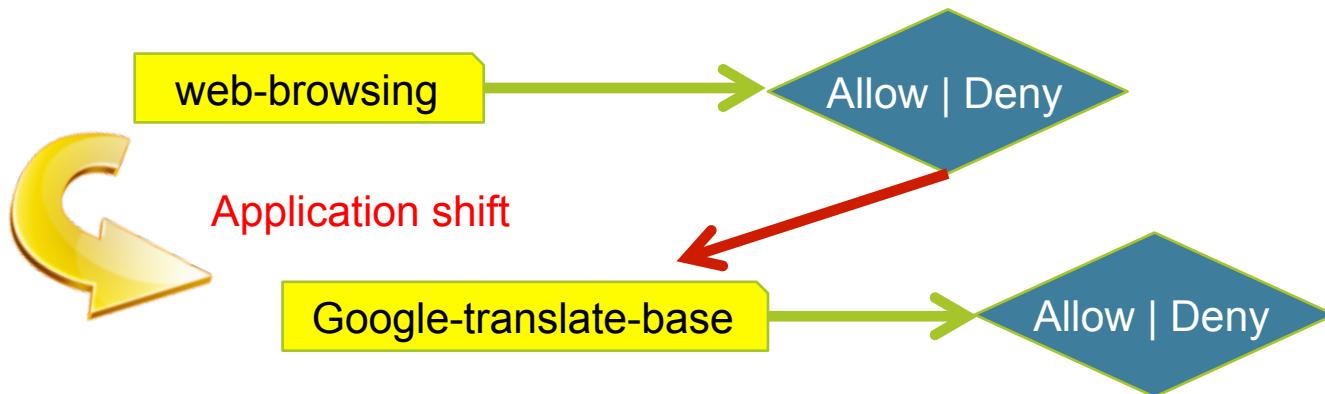
- All traffic following from one security zone to another requires a policy to allow the traffic
- The policy list is evaluated from the top down
- The first rule that matches the traffic is used
- No further rules are evaluated after the match

Name	Source			Destination			Application	Service	Action	Profile
	Zone	Address	User	Zone	Address					
LogAll	Trust	Mail Server	impressive\at... impressive\at...	Trust	any		facebook-chat	any	🚫	🔗 📥 📤 📲 📱
IT Allow Override	trust	any	impressive\at...	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 HyperText Transfer Protocol (HTTP) to access the World Wide Web. Its original purpose was to provide a graphical user interface for reading hypertext documents.
Additional Information:	Wikipedia Google Yahoo!
Standard Ports:	tcp/80
Depends on Applications:	

Application	
Name:	google-translate-base
Description:	Google Translate is a service provided by Google that translates text from one language to another. It uses rule-based analysis. Languages written in different scripts are converted automatically from phonetic equivalents.
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

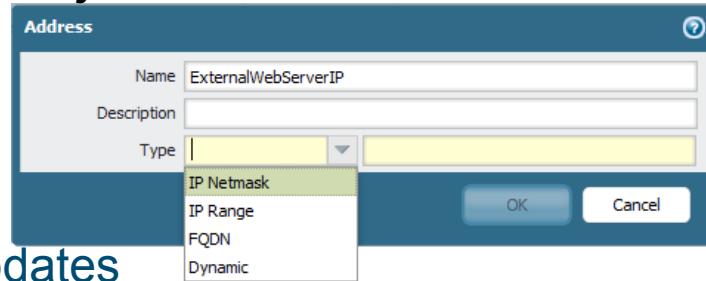
Name	Source			Destination		Application	Service	URL Category	Action
	Zone	Address	User	Zone	Address				
Allow Facebook	 Trust-L3	any	any	 Untrust-L3	any	 facebook-base	 application-default	any	
Allow WebBrowsing	 Trust-L3	any	any	 Untrust-L3	any	 web-browsing	 application-default	any	

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)
- FQDN type changes automatically if DNS entry updates
- Allows the import of external lists of URL/IP block lists

Objects > Addresses



Objects > Dynamic Block Lists

A screenshot of the Palo Alto Networks UI for managing dynamic block lists. On the left, a 'Dynamic Block Lists' dialog shows a list with one item: 'Block List for Policy'. Below it, a 'Test Source URL' button is visible. On the right, a 'Security Policy Rule' dialog is open, specifically the 'Destination' tab. In the 'Address' dropdown, the 'ExternalWebServerIP' address is selected. A large red curved arrow points from the 'Dynamic' option in the 'Address Object' dropdown above to the 'myExtBlockList' entry in the 'Block List' dropdown here.

Dynamic Block Lists

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

Objects > Dynamic Block Lists

The screenshot illustrates the configuration of a Dynamic Block List and its application in a security policy rule.

Dynamic Block Lists (Left Panel):

- Name: Block List for Policy
- Description: (empty)
- Source: http://
- Repeat: Hourly (selected)
- at: 00
- Test Source URL: (button)

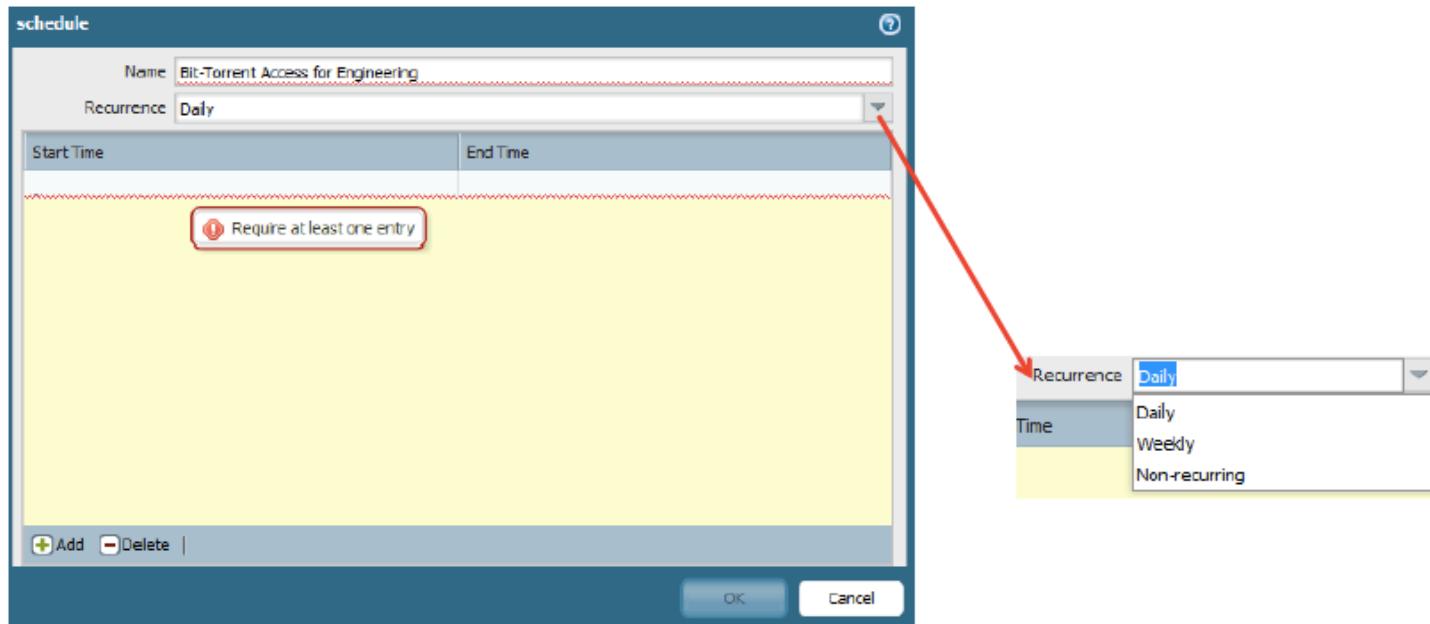
Security Policy Rule (Right Panel):

- General tab selected.
- Destination tab selected.
- Destination Zone: Select dropdown (empty).
- Address: ExternalWebServerIP, InternalWebServerIP (checkboxes)
- Block List: myExtBlockList (checkbox selected, highlighted green)
- Region: 0.0.0.0-255.255.255 (Reserved(0.0.0.0-255.255.255)), 10.0.0.0-10.255.255.255 (checkboxes)

A large red curved arrow points from the Dynamic Block List panel to the Security Policy Rule panel, indicating the flow of configuration.

Scheduling Security Policies

- Policies can be scheduled to occur at particular times of day, or be a one-time occurrence
- Schedules are defined under Object tab-> Schedules. Once defined, these schedules 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.

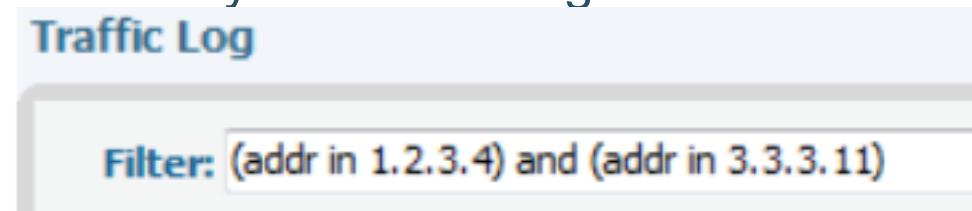
Name	Source			Destination			Application	Service	Action
	Zone	Address	User	Zone	Address				
Allow_skype_probe	 Trust-L3	any	any	 Untrust-L3	any		 skype-probe	any	
Block_skype	 Trust-L3	any	any	 Untrust-L3	any		 skype	any	

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: <input type="text"/>											
	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:



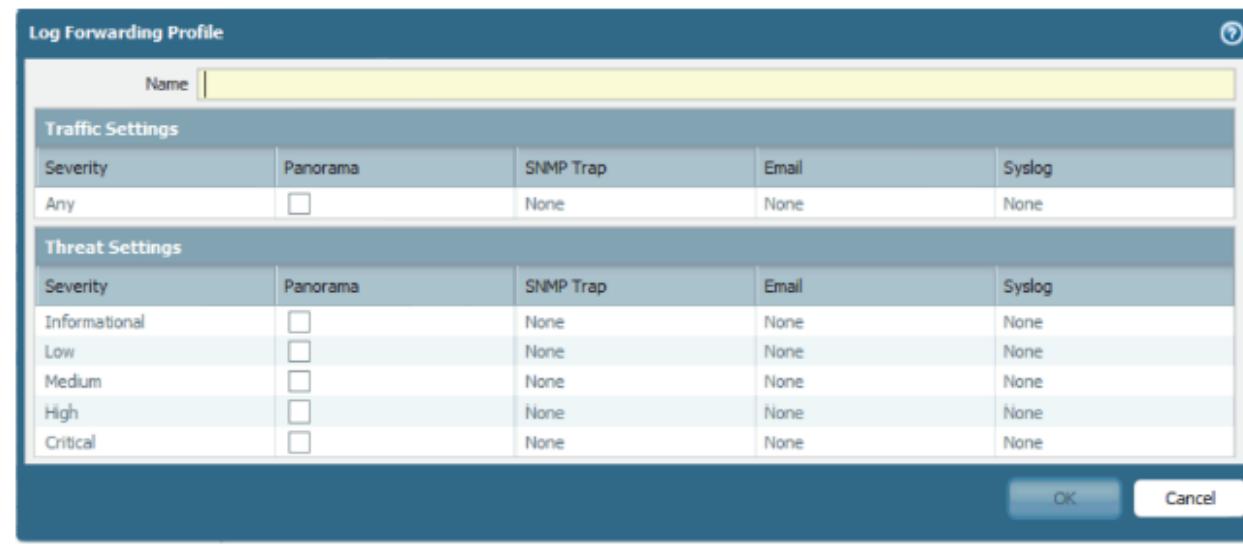
Monitoring Traffic (2)

Special Application names are used to define traffic not explicitly identified 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”

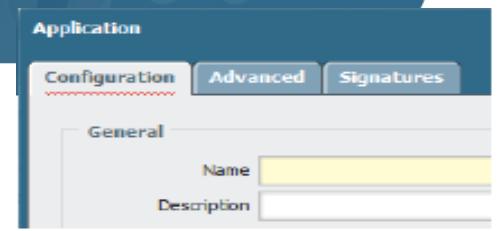
	Receive Time	Type	From Zone	To Zone	Source	Destination	From Port	To Port	Protocol	Application	Action
	01/26 11:46:54	end	tapzone	tapzone	10.154.3.60	72.247.247.125	1588	1935	tcp	unknown-tcp	allow
	01/26 11:43:55	end	tapzone	tapzone	10.154.5.204	72.247.247.132	2810	1935	tcp	unknown-tcp	allow

- 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		Protocol	Port	Application
	Zone	Address			
	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

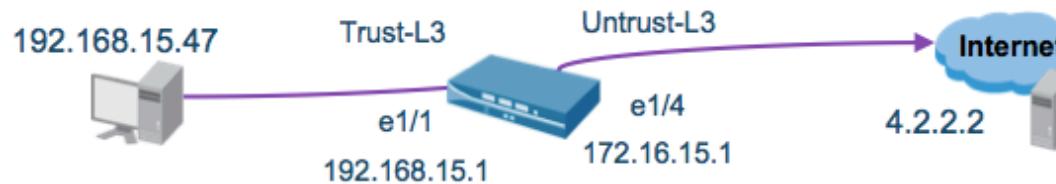
Name	Source			Destination			Application	Service	Action
	Zone	Address	User	Zone	Address				
IT Allow Override	trust	any	impressive\all	untrust	any		Custom-app	any	✓

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

Name	Original Packet						Translated Packet	
	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

Source	Destination
192.168.15.47	4.2.2.2

Translation

Source	Destination
172.16.15.1	4.2.2.2

Policies > Security

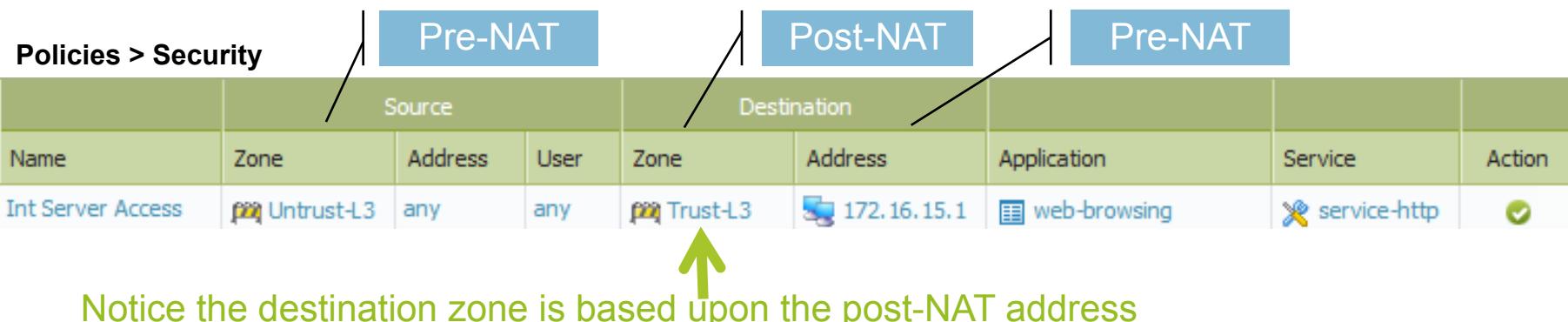
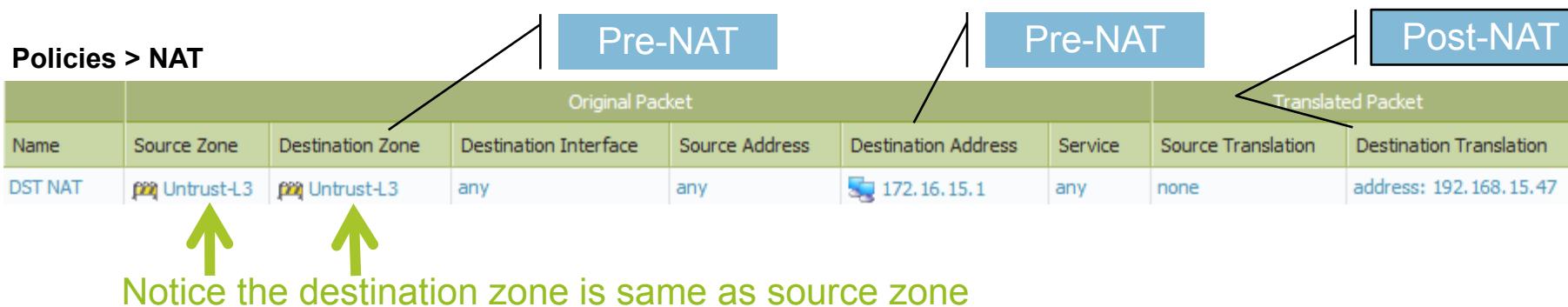
Name	Zone	Source		Destination		Action	
		Address	User	HIP Profile	Zone	Address	
Internet Usage	Trust-L3	192.168.15.0/24	any	any	Untrust-L3	any	any

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



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

The screenshot shows the Palo Alto Networks Panorama interface. On the left, there is a sidebar with a tree view under the 'Security Profiles' node, listing Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, Data Filtering, and DoS Protection. To the right, a modal dialog titled 'Security Profile Group' is displayed, containing fields for configuring profiles for each of these categories. The 'Name' field is empty, and the other fields (Antivirus Profile, Anti-Spyware Profile, Vulnerability Protection Profile, URL Filtering Profile, File Blocking Profile, Data Filtering Profile) all show 'None' selected. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Name	Antivirus Profile	Anti-Spyware Profile	Vulnerability Protection Profile	URL Filtering Profile	File Blocking Profile	Data Filtering Profile
	None	None	None	None	None	None

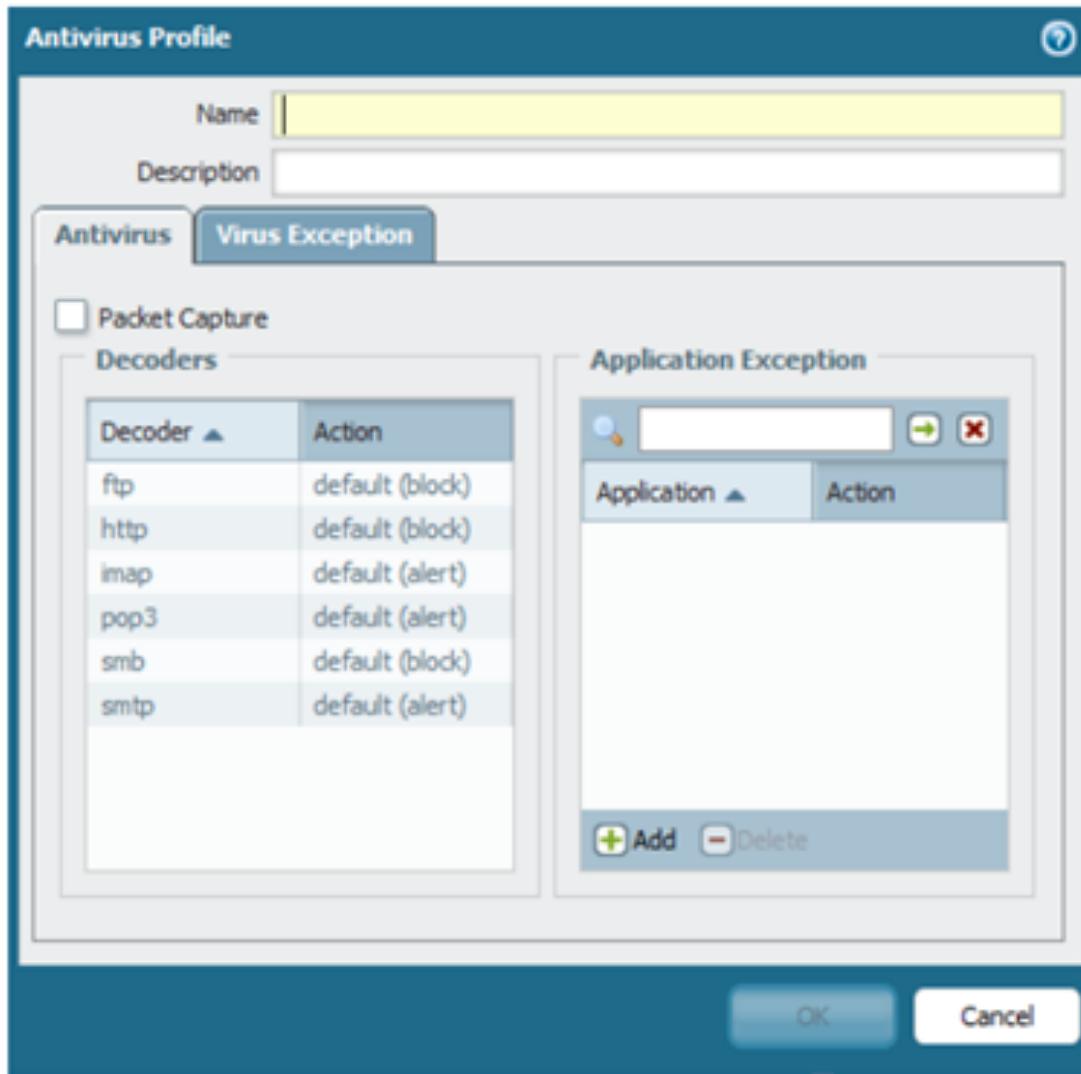
Using Security Profiles

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

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

Enable	Id	Threat Name	IP Address Exempt..	Rule	CVE	Host	Category	Sever..	Action	Packet Capture
<input type="checkbox"/>	30096	Adobe Acrobat Plugin Cross-Site Scripting Vulnerability			CVE-2007-0044	client	code-execution	high	default (reset-both)	<input type="checkbox"/>
<input checked="" type="checkbox"/>	30097	eStars Softphone SIP SDP Data Packet Buffer Overflow Vulnerability			CVE-2006-0189	server	code-execution	high	default (alert)	<input type="checkbox"/>

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.

Name: Eicar Test File
ID: 100000
Description: This signature detected Eicar Test File
Severity: MEDIUM
Exceptions: **Show**

Exceptions: Hide

Add this threat to the exception list for:

Current security profile (Unknown or not editable)

Multiple security profiles

Profile
<input checked="" type="checkbox"/> corp-profile

Add

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

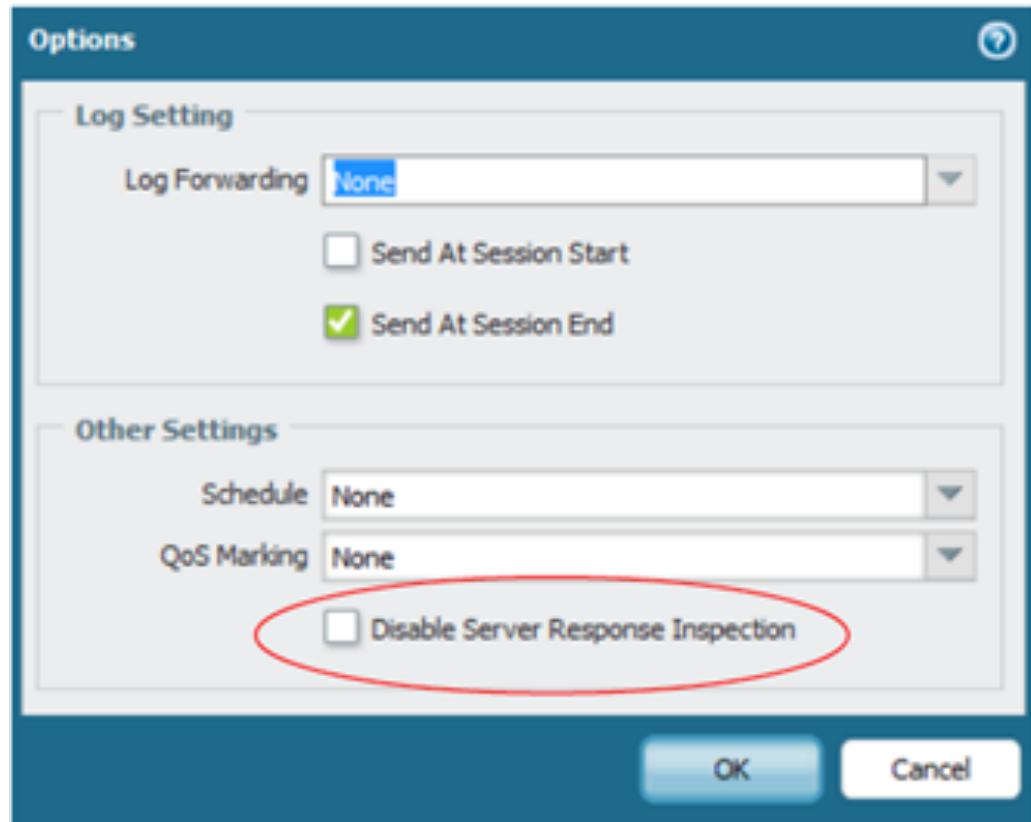


Custom Response Pages

- 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

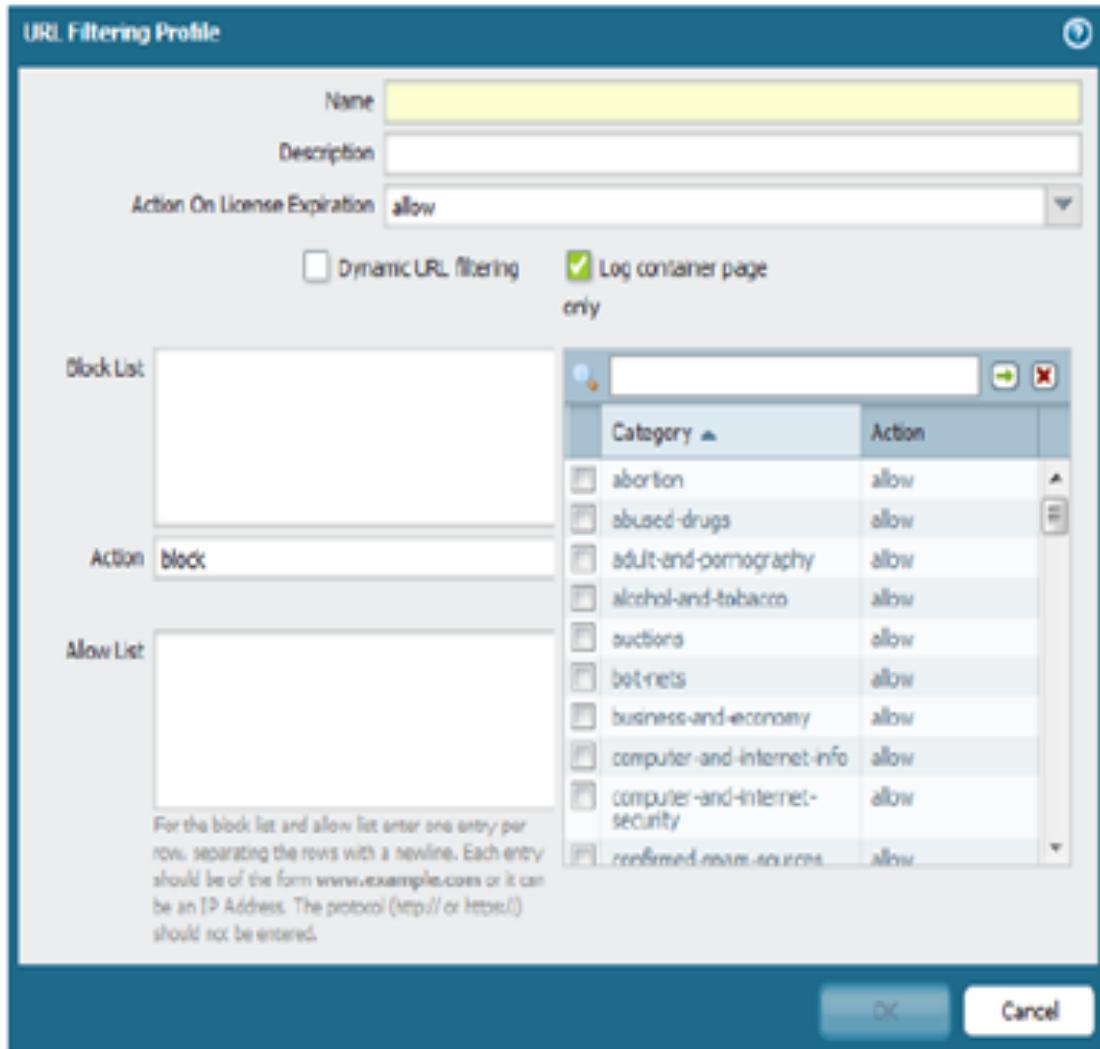
Disable Server Response Inspection

- 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

Web Page Blocked

Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: 192.168.41.20

URL: www.ketelone.com/

Category: alcohol-and-tobacco

If you require access to this page, have an administrator enter the override password here:

Continue

[Return to previous page](#)

Web Page Blocked

Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: 192.168.41.20

URL: www.2600.org/

Category: hacking

Web Page Blocked

Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: 192.168.41.20

URL: www.handdrawinggames.com/desktoptd/game.asp

Category: games

If you feel this page has been incorrectly blocked, you may click Continue to proceed to the page. However, this action will be logged.

Continue

[Return to previous page](#)

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

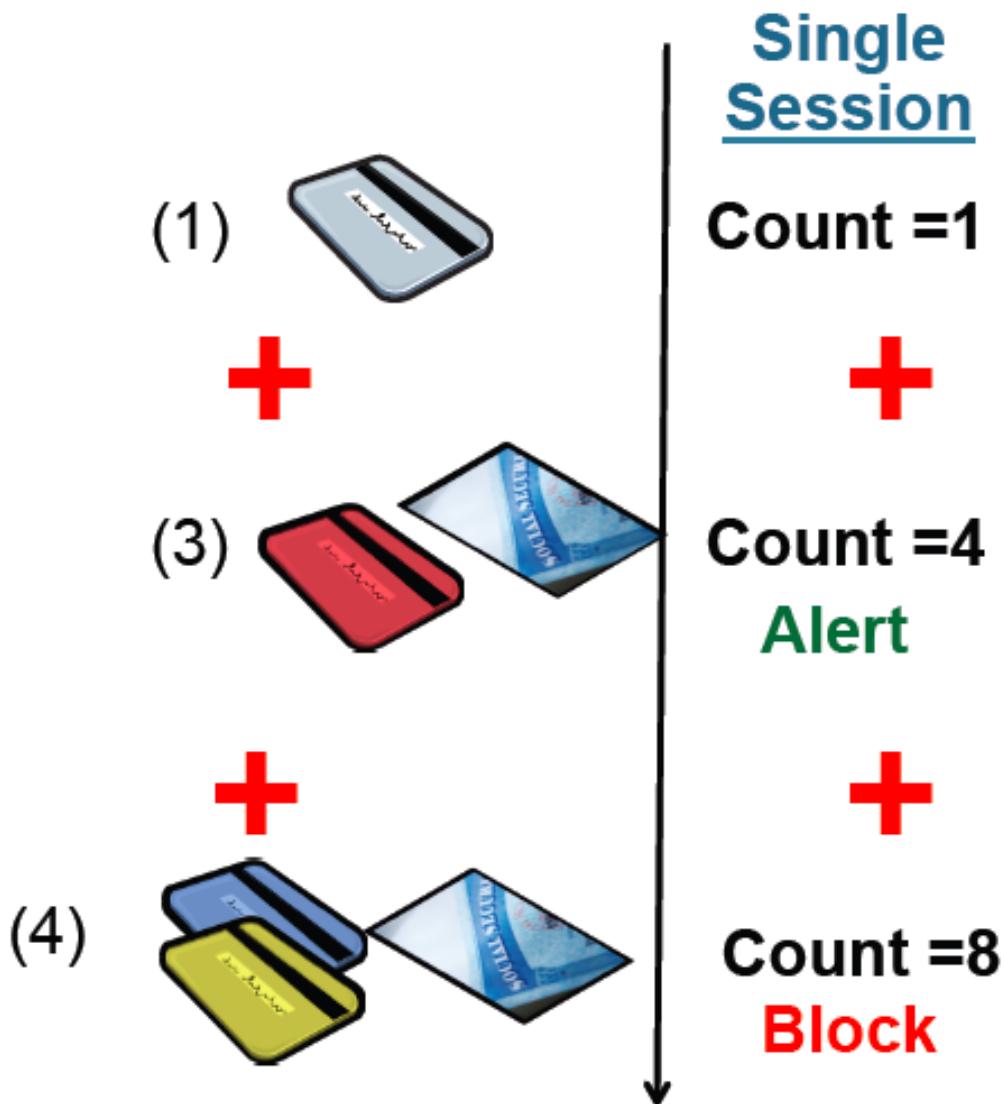
Data Filtering Example

Credit Card Weight = 1

SSN Weight = 2

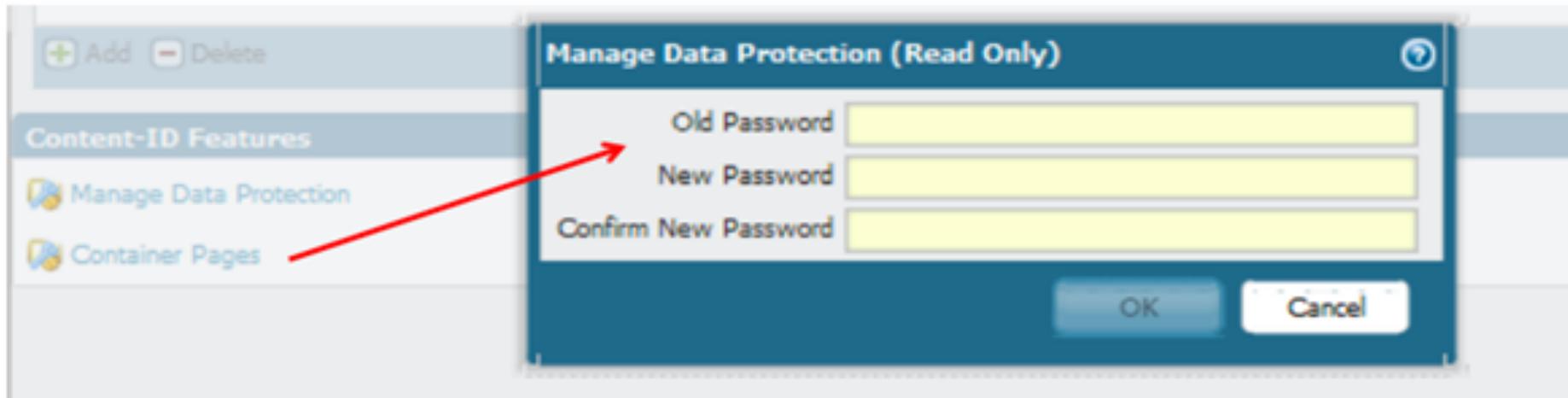
Alert Threshold = 4

Block Threshold = 8



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



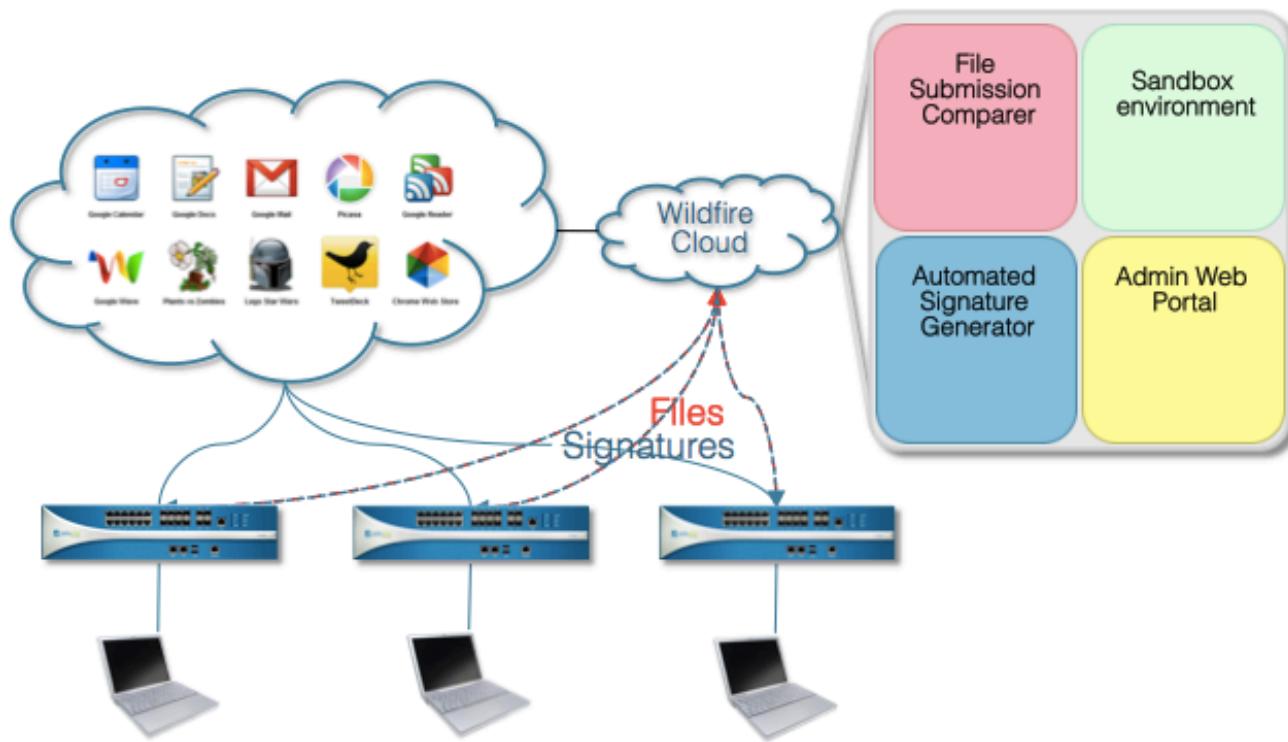
Zone Protection

- 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 against 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

Name	Flood Protection					Reconnaissance Protection		
	SYN Flood	UDP Flood	CMP 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



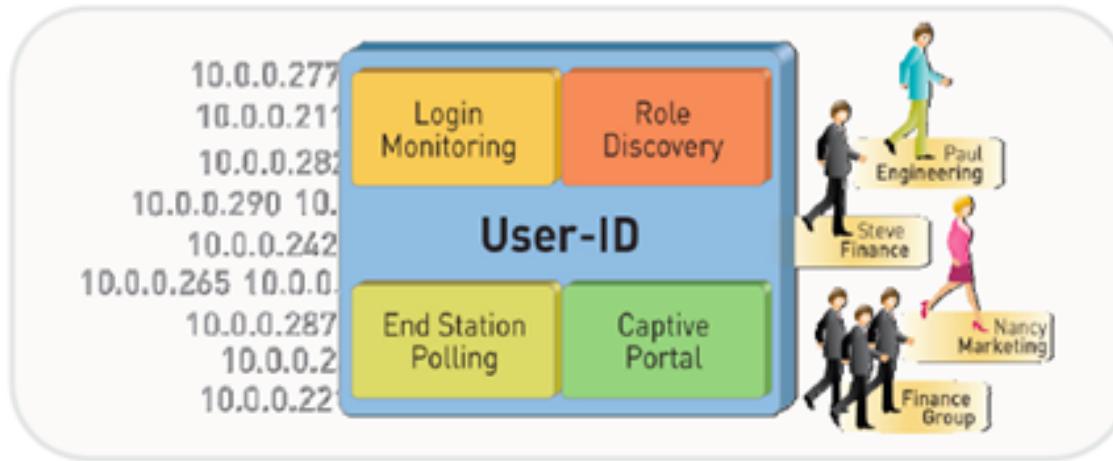
WildFire

- Provides a virtual sandbox environment for 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

The screenshot shows a web-based interface for the WildFire portal. At the top, there's a navigation bar with tabs for 'Dashboard' and 'Upload File'. Below the navigation is a search bar and filters for 'Source' (set to 'All') and 'Type' (set to 'All'). A 'Search' button is located to the right of the search bar. Below the search area, a message says 'Showing 1 to 25 | first | prev | next'. The main content is a table with columns: 'Received Time', 'Source', 'Filename', 'URL', and 'Verdict'. The table lists 25 entries, each with a small blue circular icon followed by a timestamp, source, filename, URL, and verdict (e.g., Malware, Benign, or Unknown). Some URLs are truncated with ellipses.

Received Time	Source	Filename	URL	Verdict
11/18/2011 01:02 AM	Manual	i402467.com		Malware
11/18/2011 01:02 AM	Manual	Intercompany_Invoice_08.11.Maniure.exe.doc		Malware
11/18/2011 01:02 AM	Manual	UPS_Document.xls		Malware
11/18/2011 01:02 AM	Manual	invoice_NR71885776627118773.xls_____exe		Malware
11/18/2011 01:01 AM	Manual	CHI_complete_ND027946527187.xls_____exe		Malware
11/18/2011 01:01 AM	00E29900102	AyCor.exe	livelupdate2.alyc.co.kitwew2ap0nlyacAYCor_4000.zip	Benign
11/18/2011 01:01 AM	00E29900102	FanSetup.exe	unknown	Benign
11/18/2011 01:01 AM	00E29900102	InstallerUpgrade.exe	unknown	Benign
11/18/2011 01:01 AM	00E29900102	win.dll	us.muraro.infisyalgen/share.dll	Benign
11/18/2011 01:01 AM	00E29900102	QQ2011beta3k3_update.exe	d_dz_qq_comqqfileqqupdate/QQ2011beta3k3_update.zip	Benign
11/18/2011 01:01 AM	00E29900102	xOx3.jpeg	s130 hoffle.com/qfufu/af9d8479a88fbu53458ff8ff485edfc7744/18_Malware/4/8	Malware
11/18/2011 01:01 AM	00E29900102	xOx3.jpeg	s130 hoffle.com/qfufu/af9d8479a85401160453122/18dc4efea4c1217_Malware/954	Malware
11/18/2011 01:01 AM	00E29900102	xOx3.jpeg	s130 hoffle.com/qfufu/14273802010294d0e4fad0ca502071aaeb2f_Malware/6334	Malware
11/18/2011 01:01 AM	00E29900102	xOx3.jpeg	s130 hoffle.com/qfufu/7ba08mt7c773f943a4246294605e088296a236_Malware/634	Malware
11/18/2011 01:01 AM	00E29900102	xOx3.jpeg	s130 hoffle.com/qfufu/c500f3167e071a6ed548817429edc95-d86196_Malware/634	Malware

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

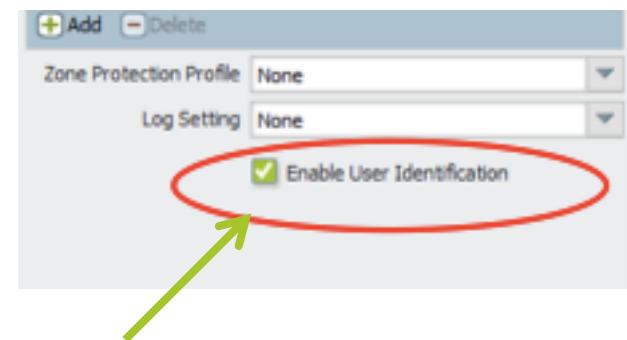
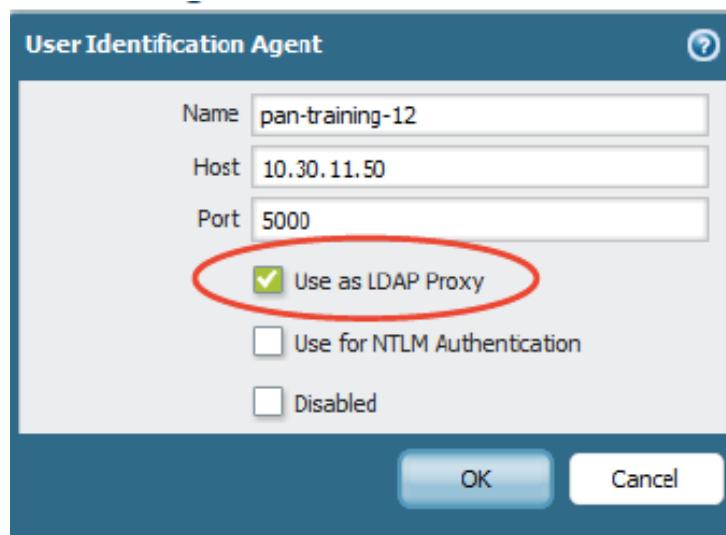
User-ID Agent Setup and Upgrade Procedure

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

Installing the User-ID agent

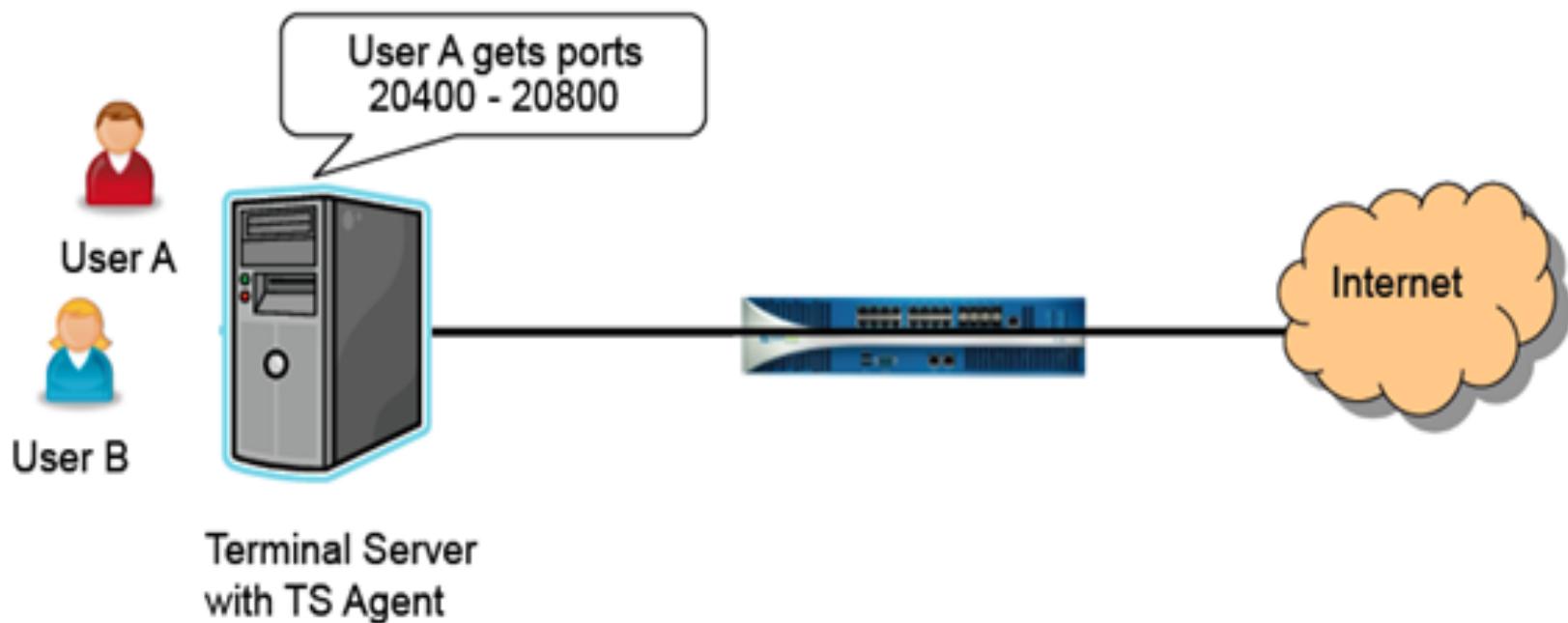
- Note that a best practice would be to install two User-ID Agents for each domain in the forest (for redundancy)
- In addition to mapping IP address, the User-ID agent can also act as an LDAP proxy, to assist in the enumeration process. This behavior is enabled through the selection of the “Use as LDAP Proxy” checkbox:



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

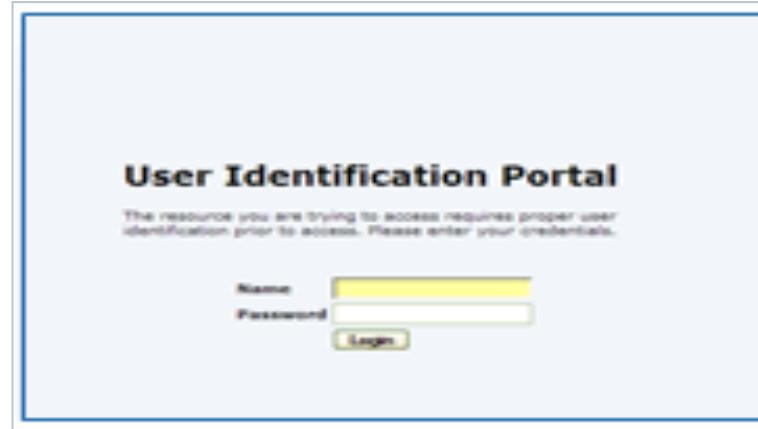
Terminal Server Agent

- 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



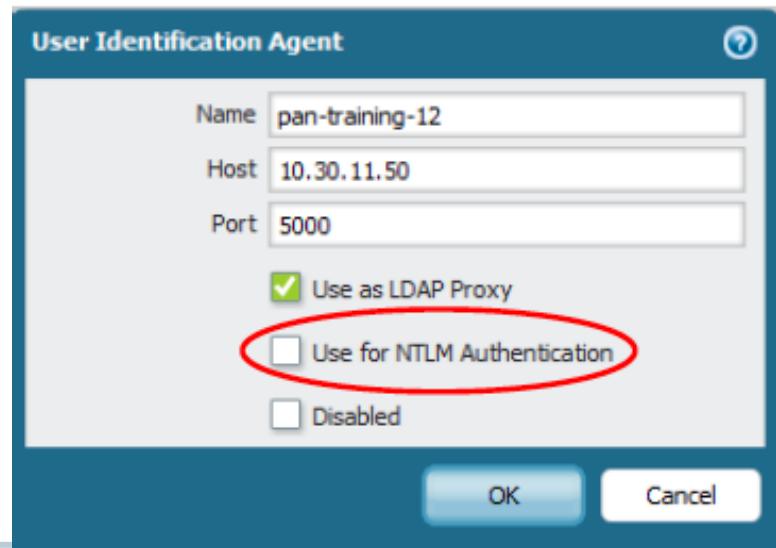
Captive Portal

- 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 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)

- 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 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 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

The screenshot shows a table listing certificates. The columns are: Name, Common Name, Certificate Authority, Private Key, Expires, and Usage. The usage for the last two entries is explicitly mentioned in the table.

Name	Common Name	Certificate Authority	Private Key	Expires	Usage
reverse-cepetest	azerty	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Aug 27 2020	
reverse-sslpnptest	PAN	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Oct 1 2019	
device-panel	pan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 28 2013	Forward Trust Certificate
web-server	portail.test.com	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Dec 16 2020	Certificate for Secure Web GUI

Below the table is a toolbar with the following buttons: Delete, Import, Generate, Export, Import HA Key, and Export HA Key. The Import, Generate, and Export buttons are circled in red.

- 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.

The screenshot shows a table of certificates with columns: Name, Common Name, Certificate Authority, Private Key, Expires, and Usage. The usage for the last two entries is explicitly mentioned in the table. Below the table is a toolbar with several buttons: Delete, Import, Generate, Export, Import HA Key, and Export HA Key. The 'Import' and 'Generate' buttons are highlighted with a red oval.

Name	Common Name	Certificate Authority	Private Key	Expires	Usage
reverse-cepetect	azerty	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Aug 27 2020	
reverse-sslvptest	PAN	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Oct 1 2019	
device-panssl	pan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 28 2013	Forward Trust Certificate
web-server	portal.test.com	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Dec 16 2020	Certificate for Secure Web GUI

Toolbar buttons: Delete, Import, Generate, Export, Import HA Key, Export HA Key

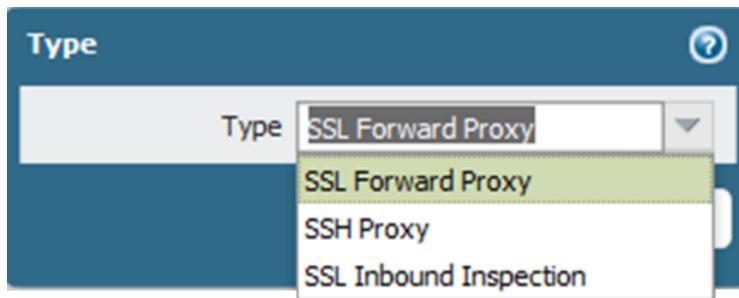
- In order to prevent user from seeking a browser certificate error, it is recommended that you have a PKI infrastructure deployed in your organization. Therefore you will be able to import into the firewall a certificate that is trusted by the user's browsers.
- When no internal PKI infrastructure is 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:

Name	Tag	Source		Destination					Type	Decryption Profile
		Zone	Address	User	Zone	Address	URL Category	Action		
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



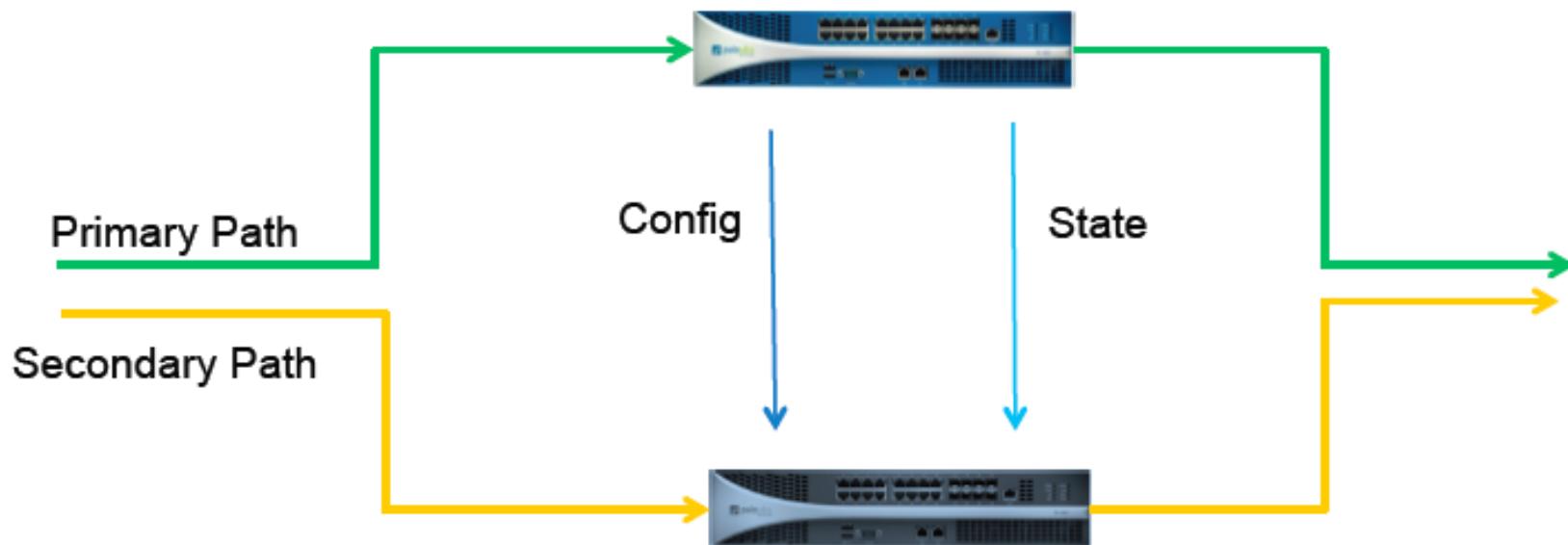
- The first rule will not decrypt any traffic going to the URL categories of finance, health, and shopping.
- The Second rule will decrypt (proxy) all other connections. Make sure to choose action “decrypt” on the second rule

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

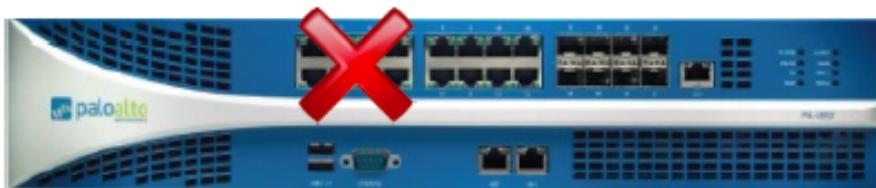
High Availability: Active/Passive

- 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



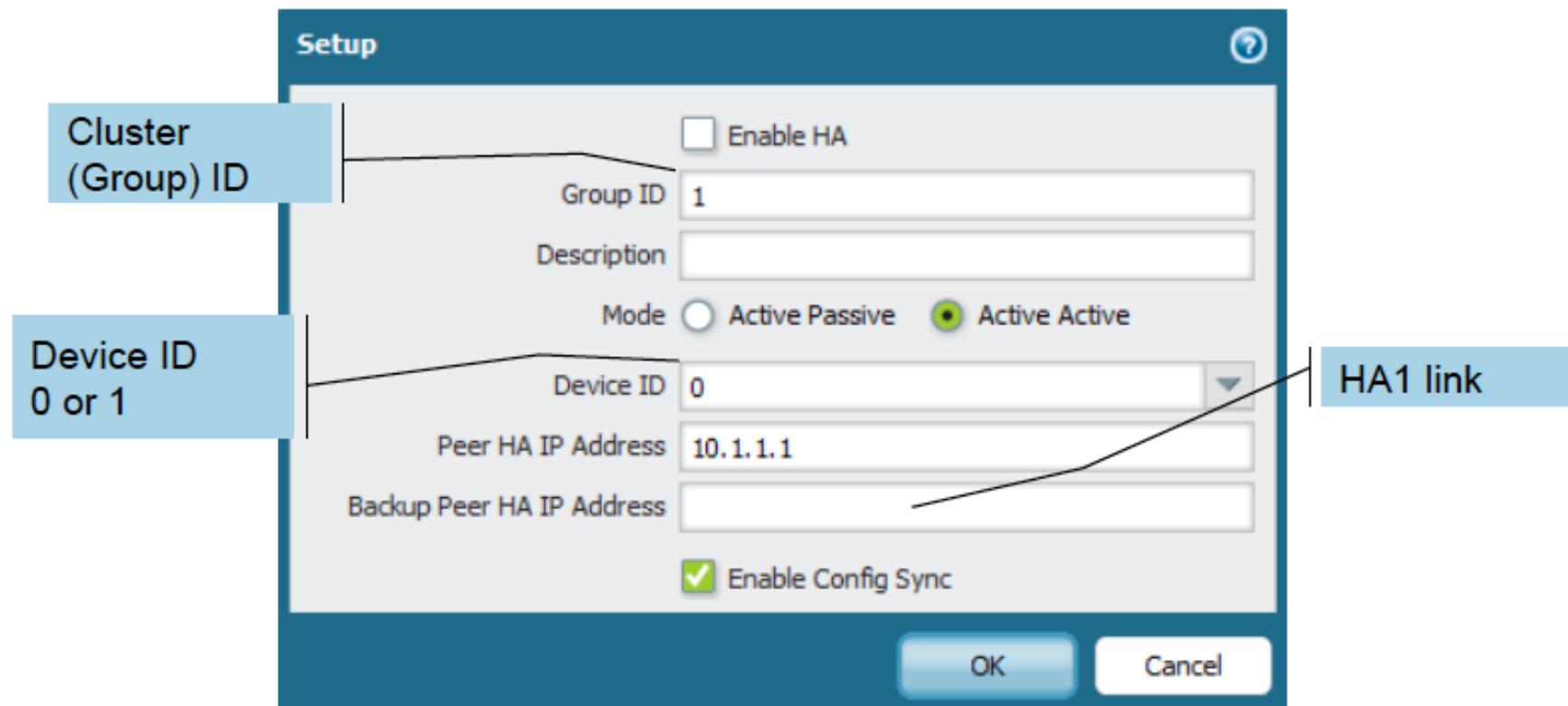
HA Failure States

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



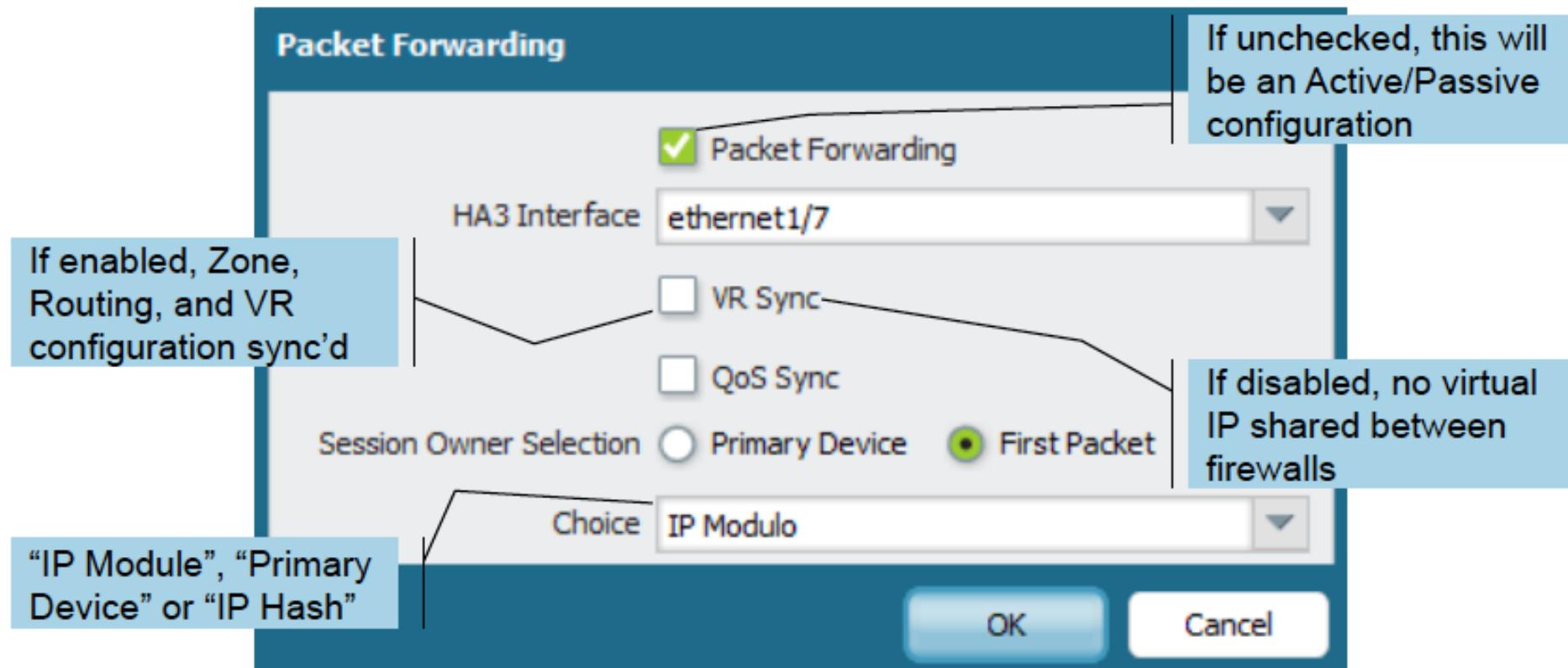
High Availability: Active/Active

- 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

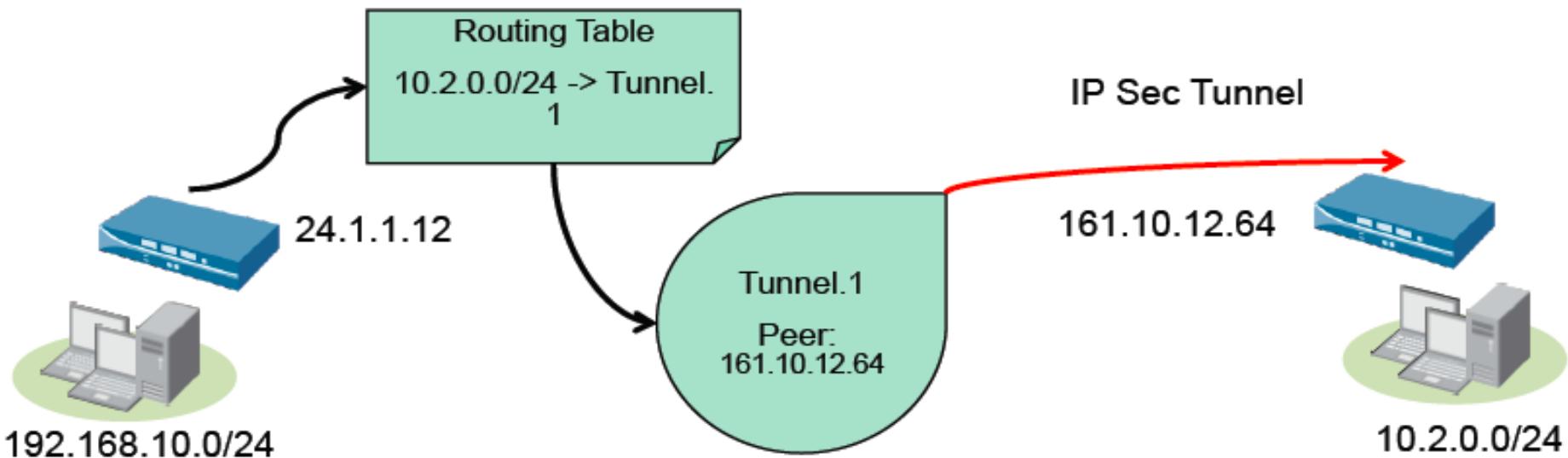


Misc HA

- 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

The screenshot shows a configuration interface for an IKE Phase 1 gateway. It includes fields for the IKE Gateway (empty), Local IP Address (selected as 'ethernet1/1' with IP '3.3.3.1'), Peer IP Address (empty with a note to 'Select 'Dynamic' or enter a Peer IP Address' and a 'Dynamic' checkbox), and a Pre-shared Key field (empty).

- 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

GlobalProtect | Overview

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

GlobalProtect Licensing

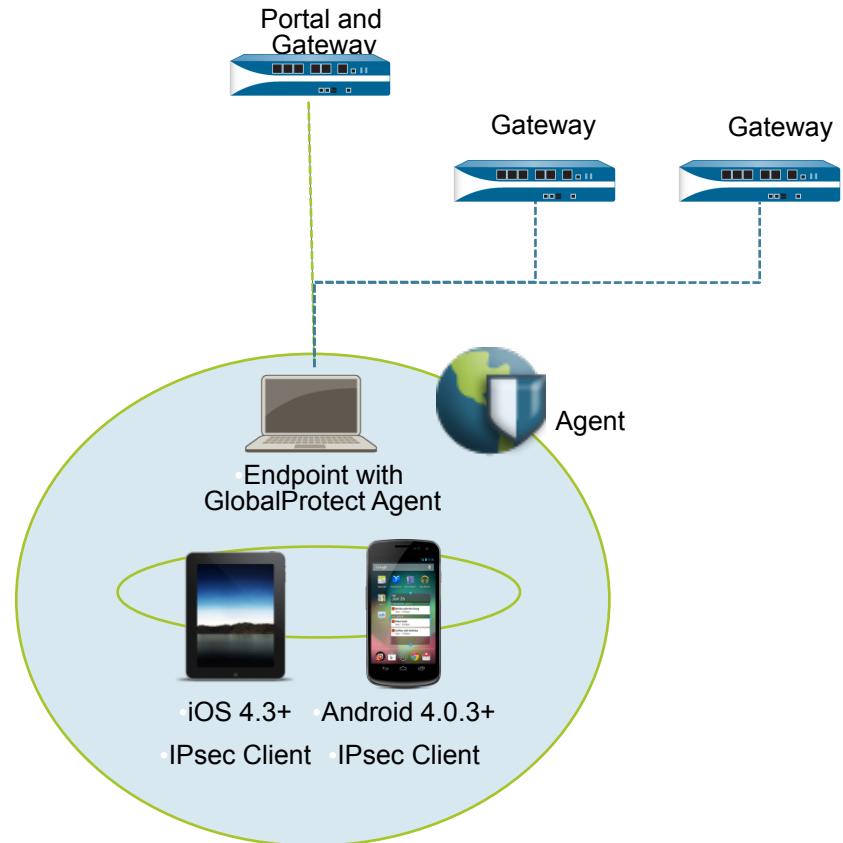
Licensing based on Portals and Gateways (firewall), not users

	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

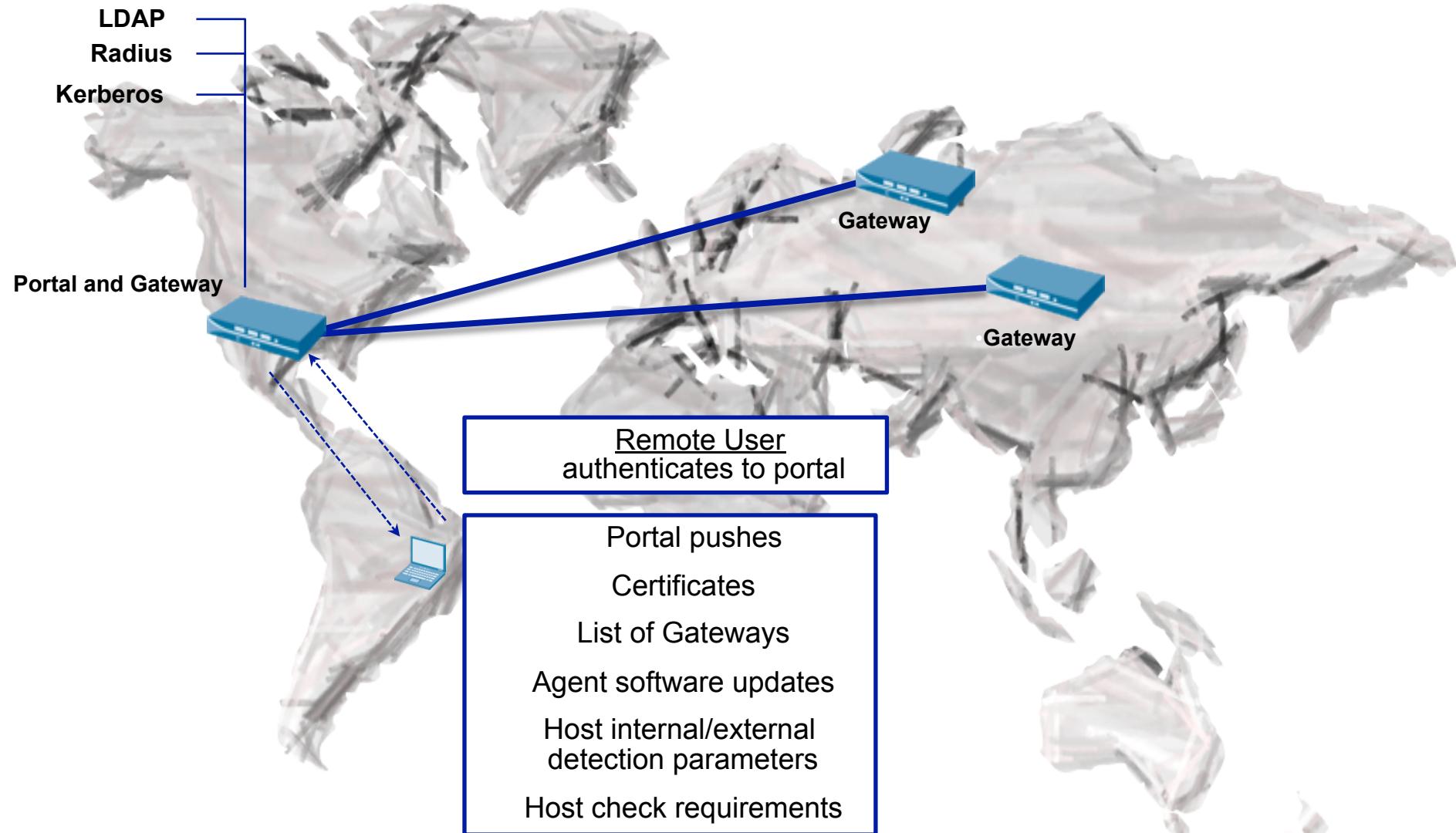
Device > GlobalProtect Client

Version	Size	Release Date	Downloaded	Currently Activated	Action	Release Notes	
1.2.0	21 MB	2012/11/02 18:32:22	✓	✓	Reactivate	Release Notes	<input checked="" type="checkbox"/>
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	<input checked="" type="checkbox"/>
1.1.0	26 MB	2011/10/31 13:38:32			Download	Release Notes	

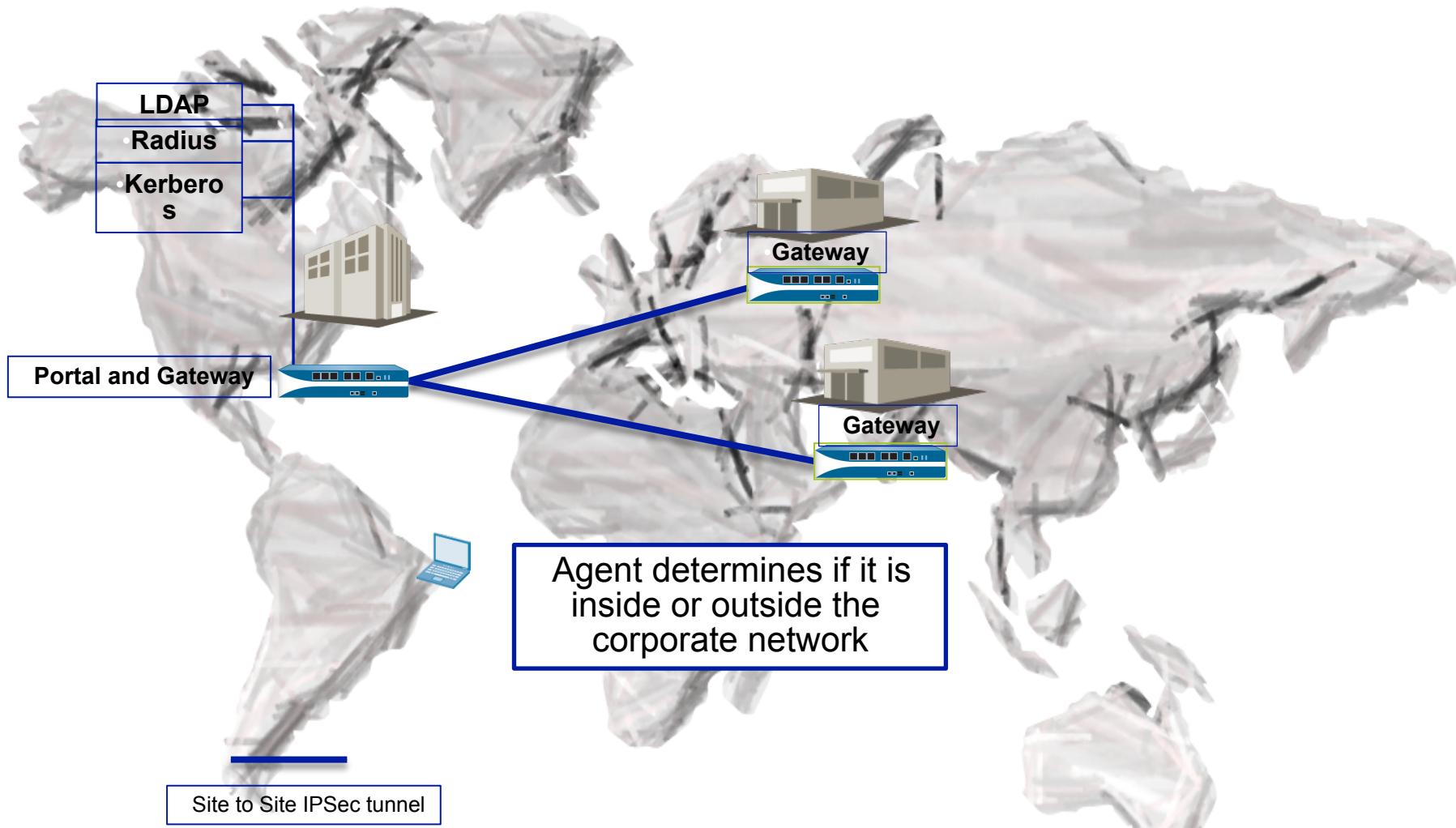
 Check Now  Upload  Activate From File

Connection Sequence:

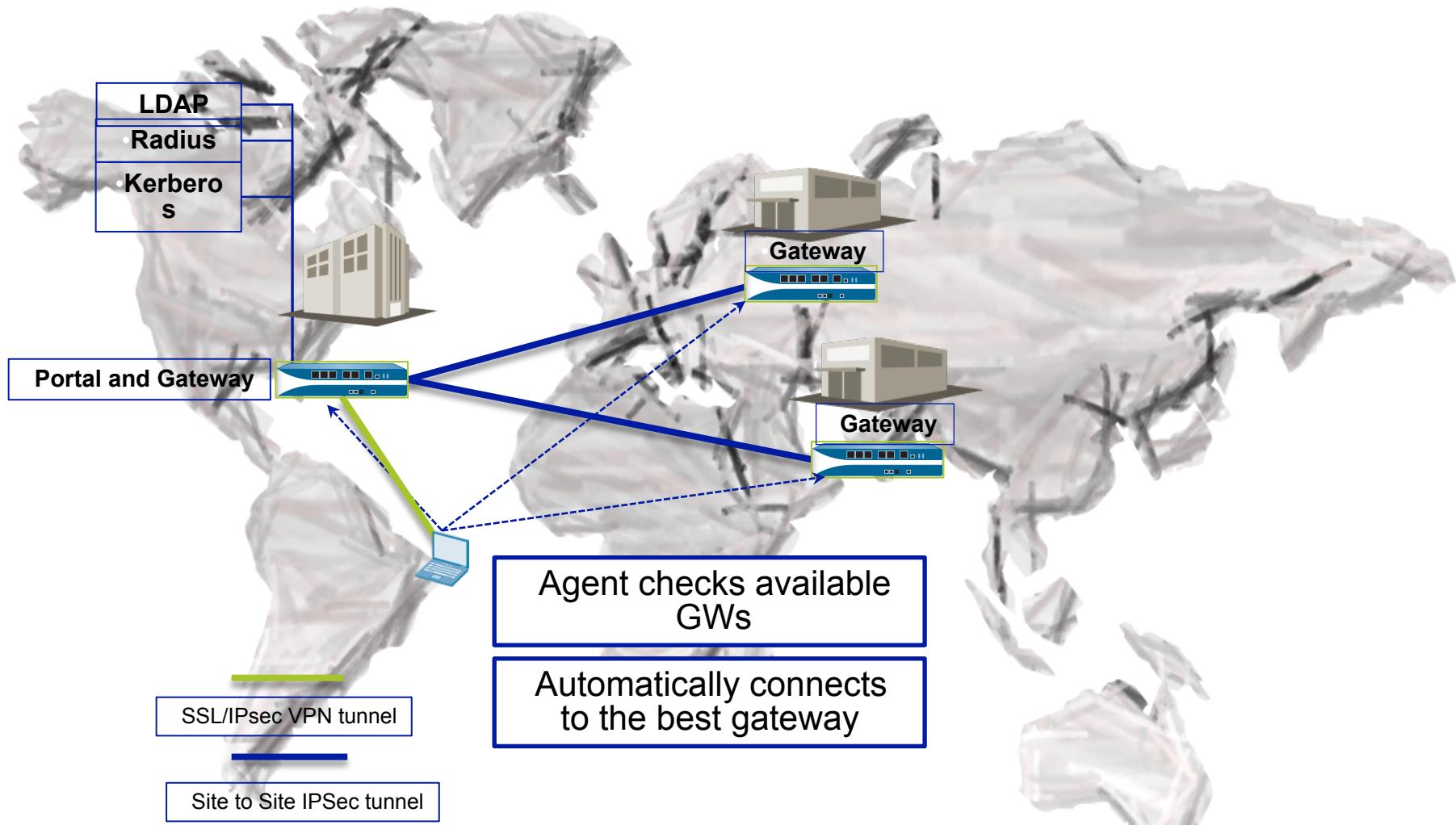
External User Sequence - Step 1



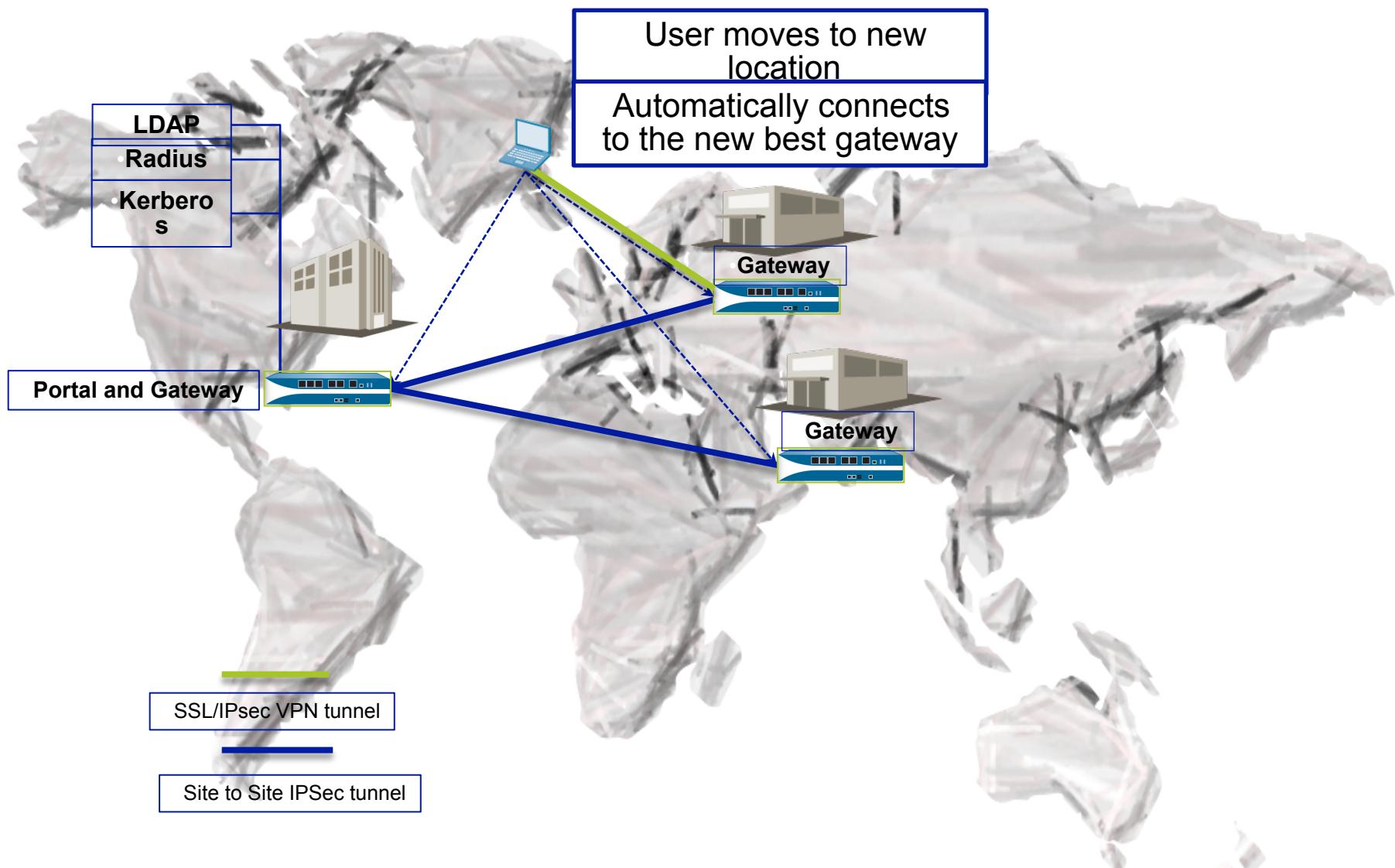
External User Sequence - Step 2



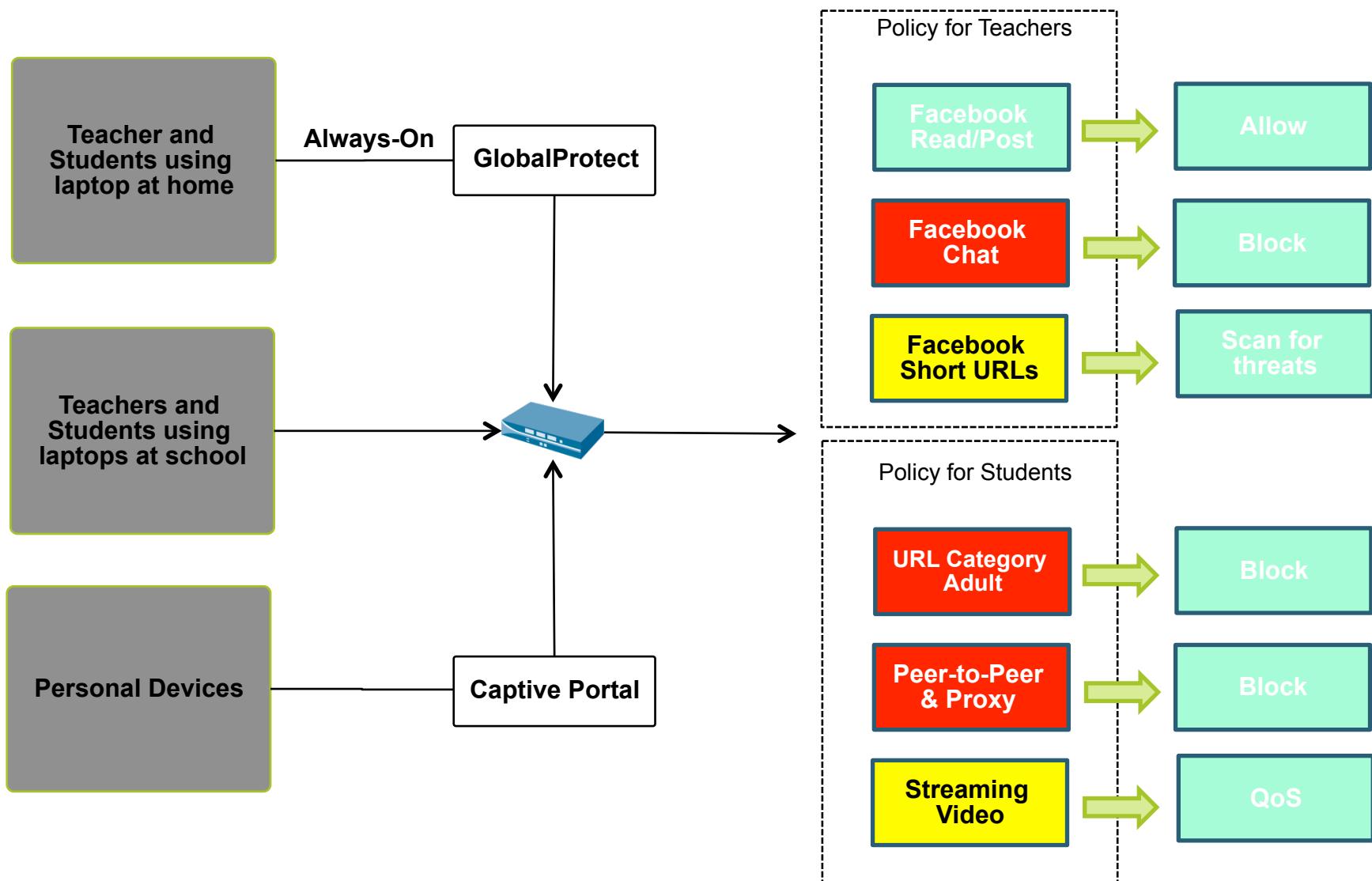
External User Sequence - Step 3



External User Sequence - Step 4

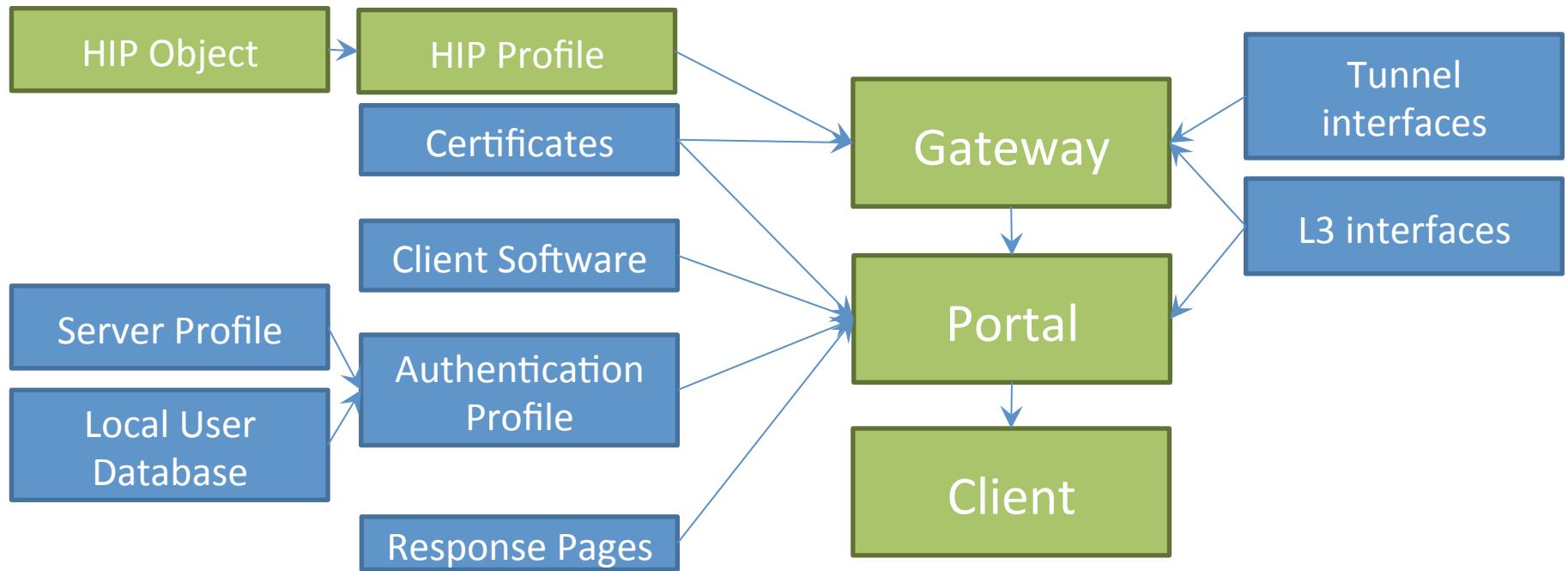


Security Policy Enforcement - Example

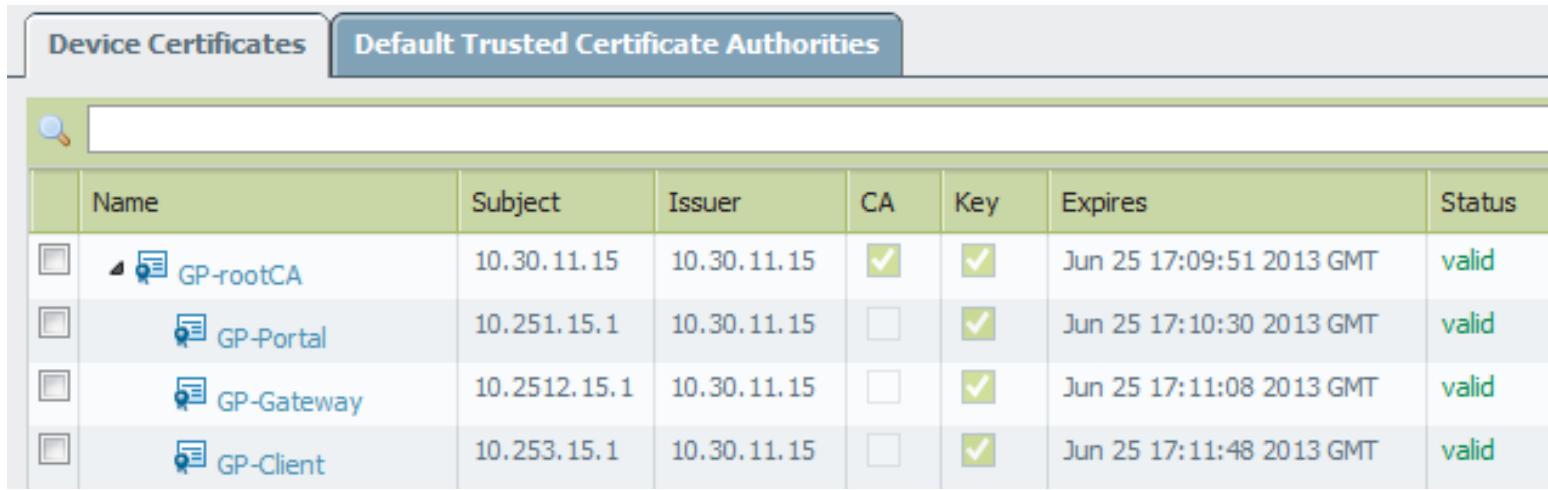


Preparing the Firewall for GlobalProtect

Configuration Components



GlobalProtect Required Certificates



The screenshot shows a user interface for managing certificates. At the top, there are two tabs: "Device Certificates" and "Default Trusted Certificate Authorities". The "Default Trusted Certificate Authorities" tab is selected, indicated by a blue background. Below the tabs is a search bar with a magnifying glass icon. The main area is a table with the following columns: Name, Subject, Issuer, CA, Key, Expires, and Status. There are four rows in the table, each representing a certificate:

	Name	Subject	Issuer	CA	Key	Expires	Status
<input type="checkbox"/>	GP-rootCA	10.30.11.15	10.30.11.15	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 25 17:09:51 2013 GMT	valid
<input type="checkbox"/>	GP-Portal	10.251.15.1	10.30.11.15	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 25 17:10:30 2013 GMT	valid
<input type="checkbox"/>	GP-Gateway	10.2512.15.1	10.30.11.15	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 25 17:11:08 2013 GMT	valid
<input type="checkbox"/>	GP-Client	10.253.15.1	10.30.11.15	<input type="checkbox"/>	<input checked="" type="checkbox"/>	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

Certificate Profile

Name	GP-Cert-Profile						
Username Field	None						
Domain							
CA Certificates	<table border="1"><thead><tr><th>Name</th><th>Default OCSP URL</th><th>OCSP Verify CA</th></tr></thead><tbody><tr><td>GP-rootCA</td><td></td><td></td></tr></tbody></table>	Name	Default OCSP URL	OCSP Verify CA	GP-rootCA		
Name	Default OCSP URL	OCSP Verify CA					
GP-rootCA							
Add Delete							

Default OCSP URL (must start with http:// or https://)

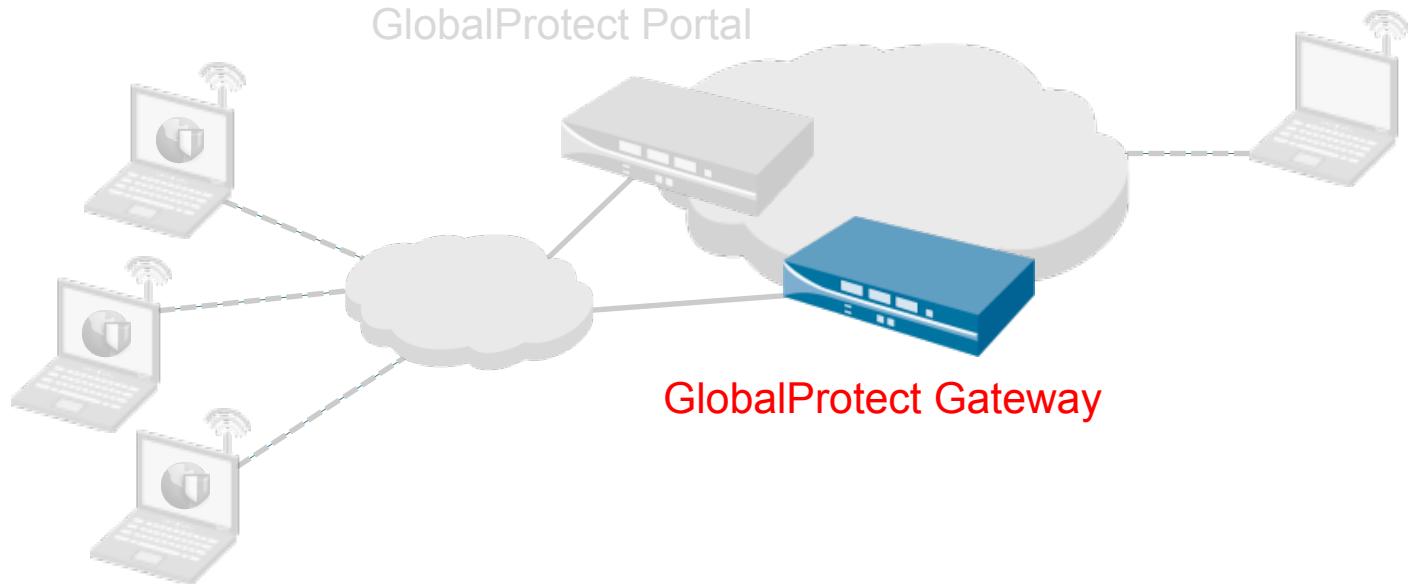
Use CRL CRL Receive Timeout (sec)
 Use OCSP OCSP Receive Timeout (sec)
OCSP takes precedence over CRL Certificate Status Timeout (sec)

Block session if certificate status is unknown
 Block session if certificate status cannot be retrieved within timeout

OK **Cancel**

Configuration: GlobalProtect Gateway

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

GlobalProtect Gateway

General Client Configuration Satellite Configuration

Name

Network Settings

Interface

IP Address None

Server Certificate

Authentication

Authentication Profile None

Certificate Profile None

OK Cancel

This screenshot shows the 'GlobalProtect Gateway' configuration dialog box. The left sidebar has tabs for 'General', 'Client Configuration', and 'Satellite Configuration', with 'General' being the active tab. The main area contains fields for 'Name' (empty), 'Network Settings' (Interface set to empty, IP Address set to 'None', Server Certificate set to empty), and 'Authentication' (Authentication Profile and Certificate Profile both set to 'None'). At the bottom are 'OK' and 'Cancel' buttons.

GP-Gateway | Tunnel Settings

Network > GlobalProtect > Gateways

GlobalProtect Gateway

General Client Configuration Satellite Configuration

Tunnel Settings Network Settings HIP Notification

Tunnel Mode

Tunnel Interface: tunnel.2

Max User: [1 - 20000]

Enable IPSec

Enable X-Auth Support

Group Name:

Group Password:

Confirm Group Password:

Skip Auth on IKE Rekey

Timeout Configuration

Login Lifetime: Days 30

Inactivity Logout: Hours 3

Default: SSL-VPN

OK Cancel

The screenshot shows the 'Tunnel Settings' tab selected in the GlobalProtect Gateway configuration. Under 'Tunnel Mode', the 'Enable IPSec' checkbox is checked. A callout bubble with the text 'Default: SSL-VPN' points to this checkbox. Other settings shown include a tunnel interface of 'tunnel.2', a max user limit of '1 - 20000', and timeout configurations for login lifetime (30 days) and inactivity logout (3 hours). Buttons for 'OK' and 'Cancel' are at the bottom.

GP-Gateway | Network Settings

Network > GlobalProtect > Gateways

The screenshot shows the 'Tunnel Settings' tab of the GlobalProtect Gateway configuration. On the left, there's a sidebar with 'General', 'Client Configuration', and 'Satellite Configuration' tabs. The main area has tabs for 'Tunnel Settings' (selected), 'Network Settings', and 'HIP Notification'. Under 'Tunnel Settings', the 'Inheritance Source' is set to 'ethernet1/4'. Below it, 'Primary DNS' is set to 'inherited'. There are also fields for 'Secondary DNS', 'Primary WINS', 'Secondary WINS', and 'DNS Suffix'. A red arrow points from the 'Inheritance Source' dropdown to the 'Check inheritance source status' link. Another red arrow points from the 'Primary DNS' dropdown to its value. At the bottom, there are two sections: 'IP Pool' containing '10.253.15.99-10.253.15.106' and 'Access Route' containing '0.0.0.0/0'. Green arrows point from these sections to blue callout boxes. The left callout box says 'IP addresses distributed to Clients' and the right one says 'Routes installed on Clients' VPN connection'. A note at the bottom left says 'These IPs will be added to the firewall's routing table'. A note at the bottom right says 'These routes will be added to the client's routing table'. At the bottom right are 'OK' and 'Cancel' buttons.

GlobalProtect Gateway

General Client Configuration Satellite Configuration

Tunnel Settings Network Settings HIP Notification

Inheritance Source: ethernet1/4

Primary DNS: inherited

Secondary DNS: 10.253.15.254

Primary WINS: None

Secondary WINS: None

DNS Suffix: Enter comma-separated DNS suffix for client (e.g. hr.mycompany.com, mycompany.com)

Inherit DNS Suffixes

IP Pool: 10.253.15.99-10.253.15.106

Access Route: 0.0.0.0/0

These IPs will be added to the firewall's routing table

These routes will be added to the client's routing table

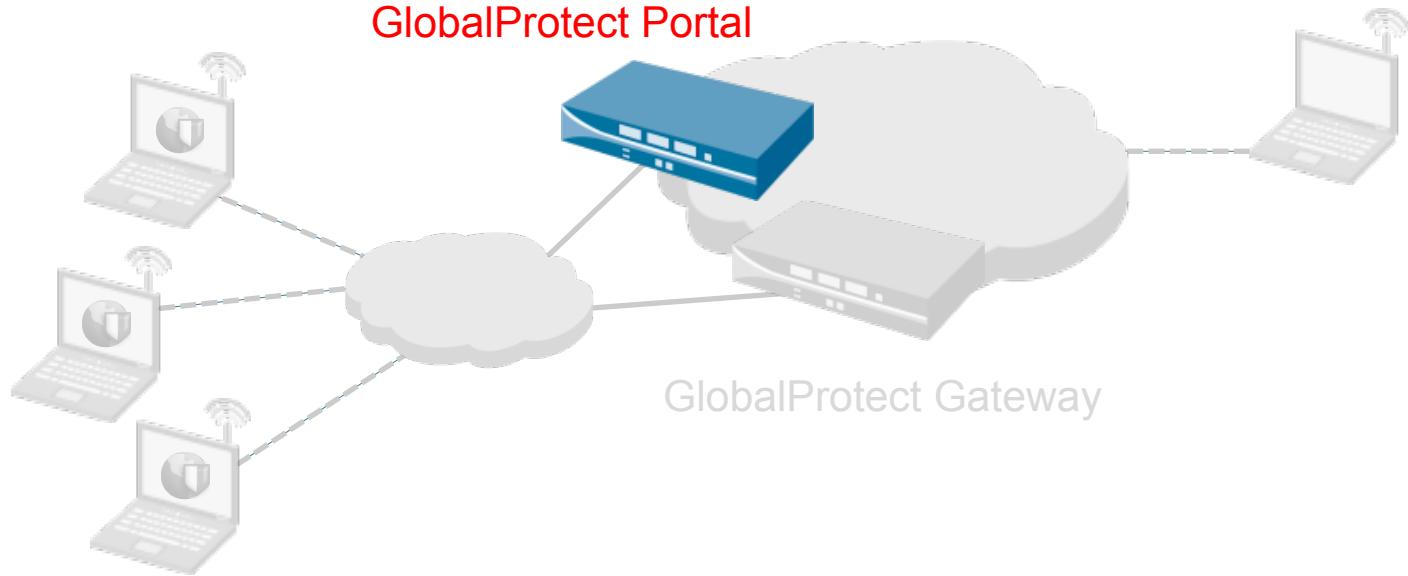
OK Cancel

IP addresses distributed to Clients

Routes installed on Clients' VPN connection

Configuration: GlobalProtect Portal

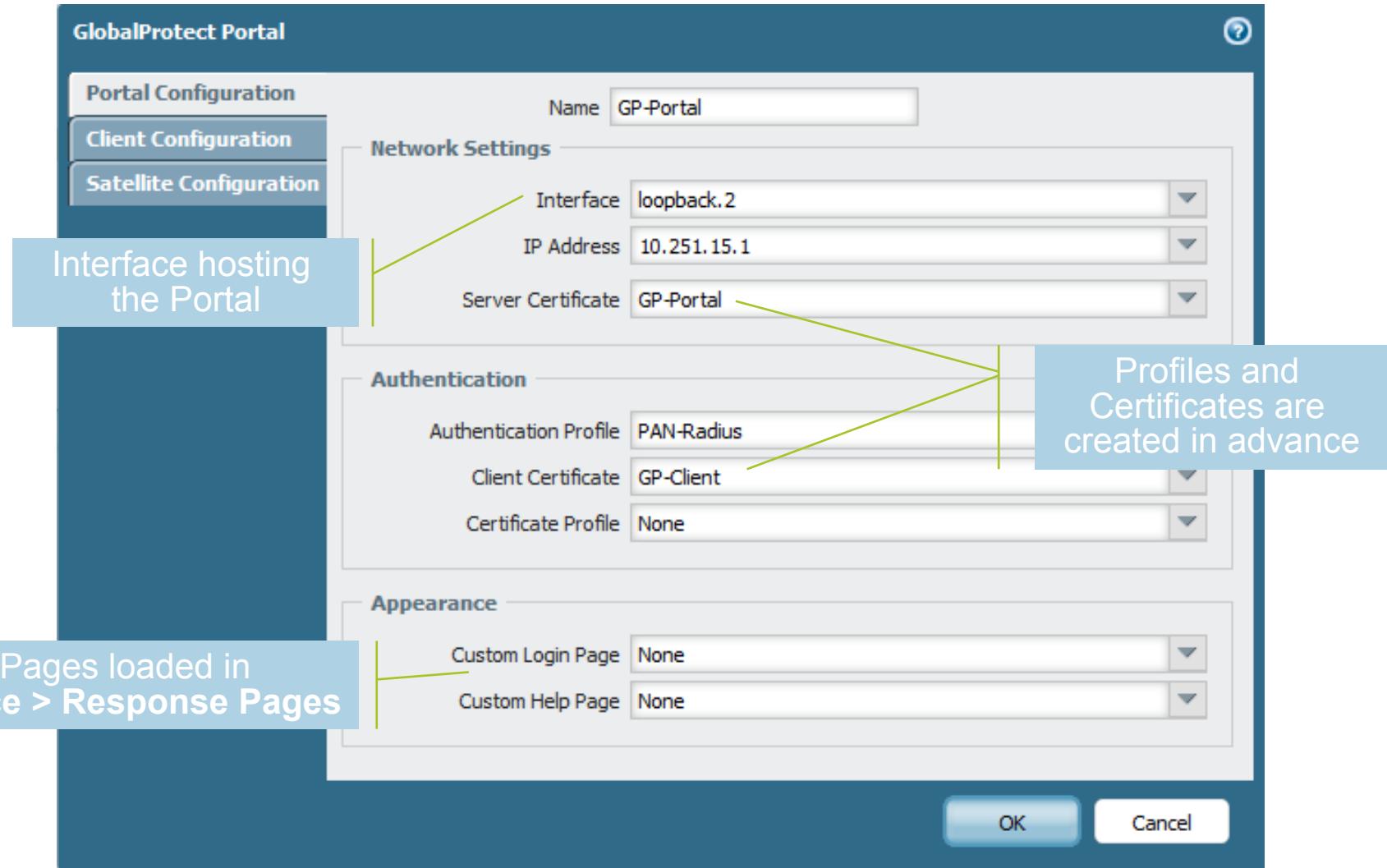
GlobalProtect Portal



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

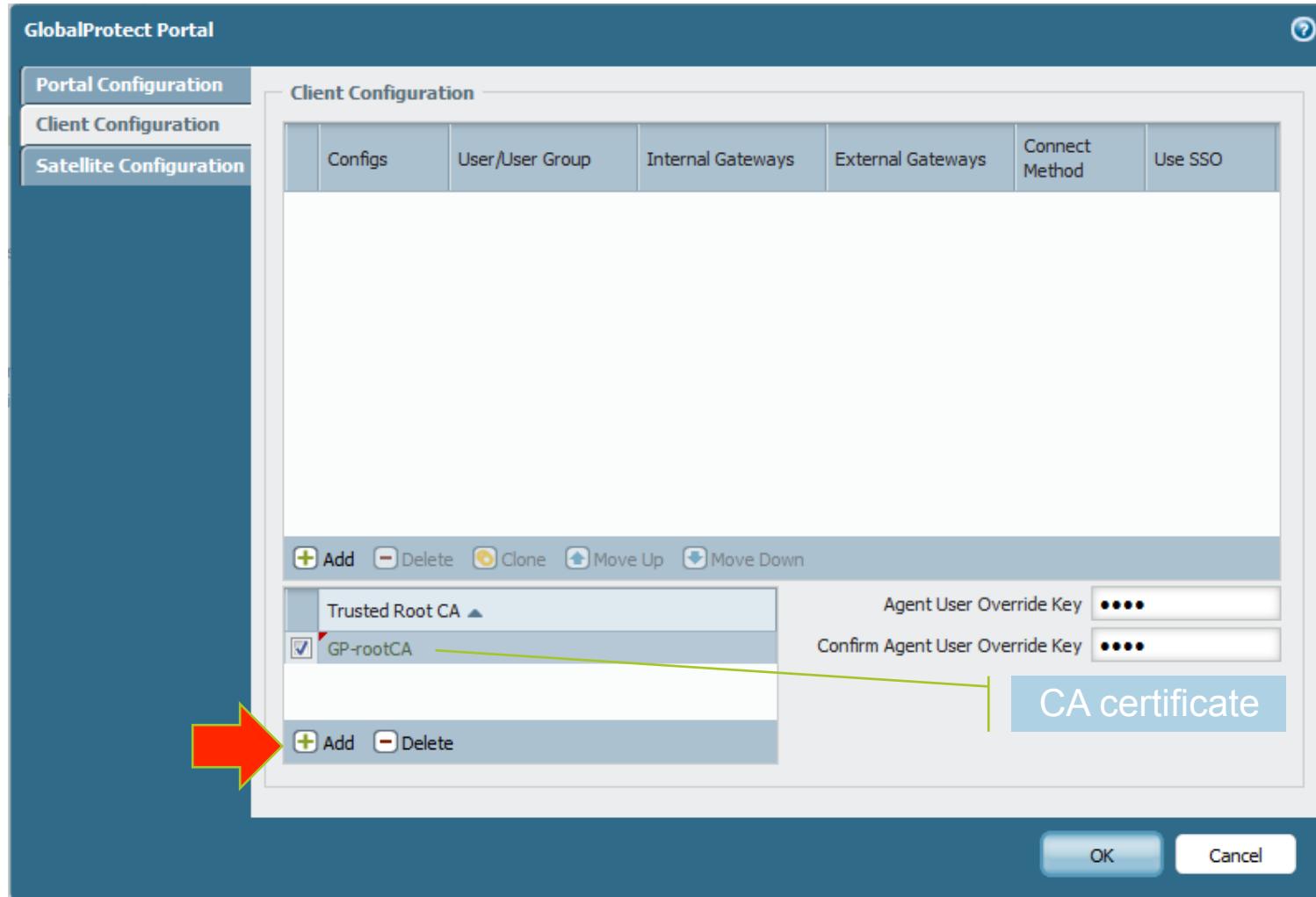
GP-Portal | Portal Configuration tab

Network > GlobalProtect > Portals



GP-Portal | Client Configuration - Certificates

Network > GlobalProtect > Portals



GP-Portal | Client Configurations – General tab

If Hostname resolves to IP Address, then Internal Gateway is used

Client VPN interfaces that take precedence over the GlobalProtect interface

GlobalProtect Portal

Portal Configuration

Client Configuration

Satellite Configuration

Client Configuration

Configs

General User/User Group Gateways Agent Data Collection

Name []

Options

Use single sign-on

Config Refresh Interval (hours) 24

Connect Method user-logon

on-demand

user-logon

pre-logon

Third Party VPN

Cisco Systems VPN Adapter

Add Delete

Internal Host Detection

IP Address 10.253.15.254

Hostname int-dns1.mycompany.com

OK Cancel

GP-Portal | Client Configuration – Gateways Tab

Configs

General User/User Group Gateways Agent Data Collection

Cutoff Time 0

Internal Gateways

Name	Address
Int-GW-1	10.15.1.1

Add Delete

External Gateways

Name	Address	Priority	Manual
Ext-GW-1	10.252.15.1	Highest	<input type="checkbox"/>
Ext-GW-2	10.252.15.2	Highest	<input type="checkbox"/>

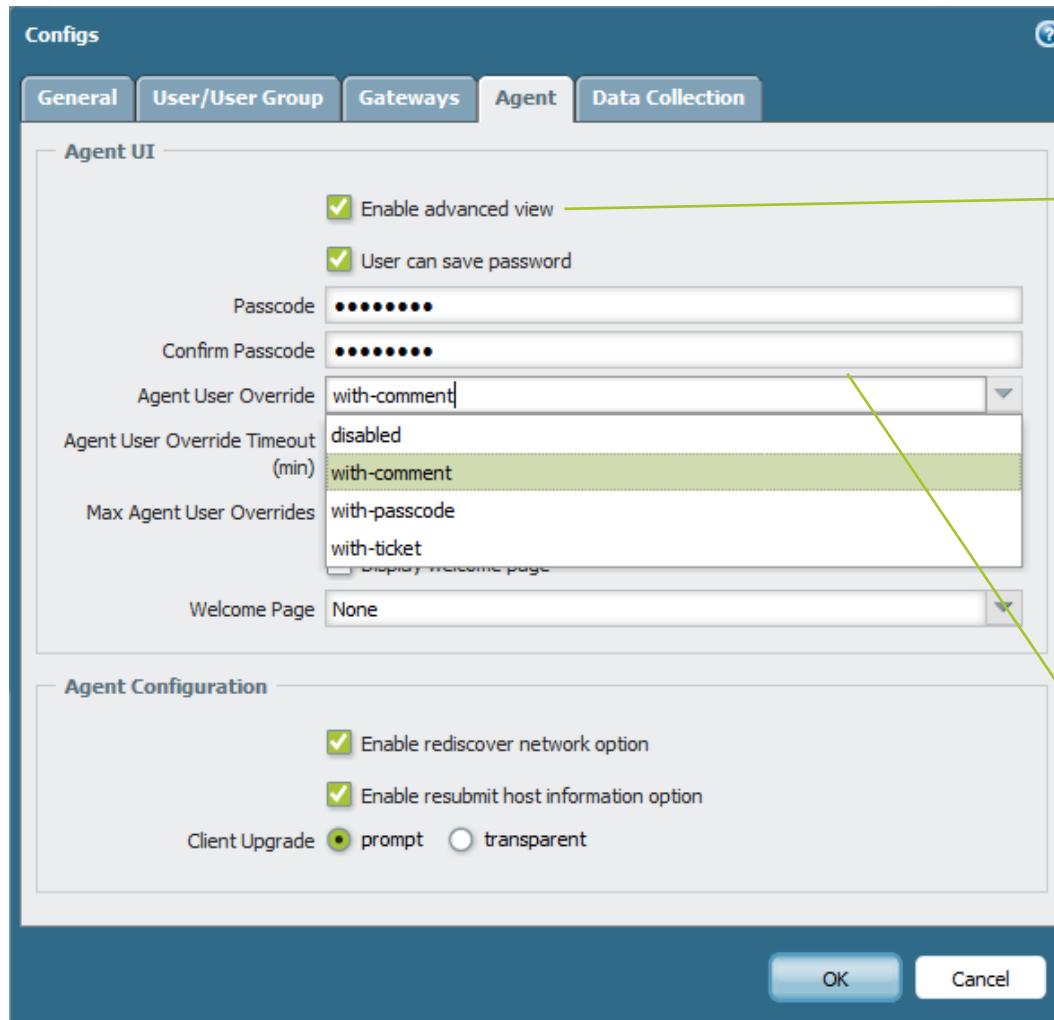
Manual only
Highest
High
Medium
Low
Lowest

Add Delete

OK Cancel

The screenshot shows the 'Gateways' tab of the GP-Portal Client Configuration dialog. The 'External Gateways' section has a dropdown menu open for the priority of 'Ext-GW-2'. The options in the menu are: Manual only, Highest (highlighted in green), High, Medium, Low, and Lowest.

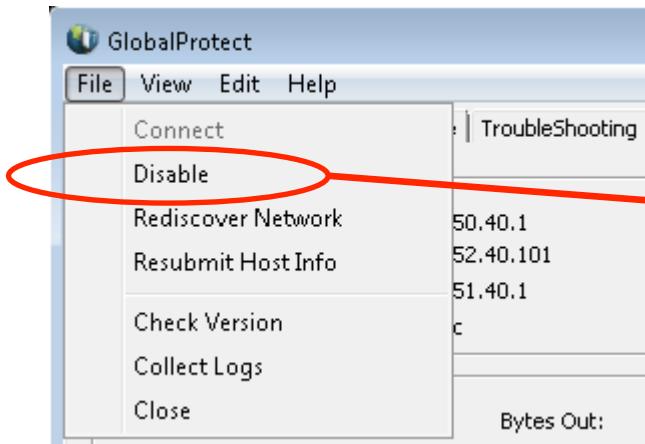
Client Configuration – Agent Tab



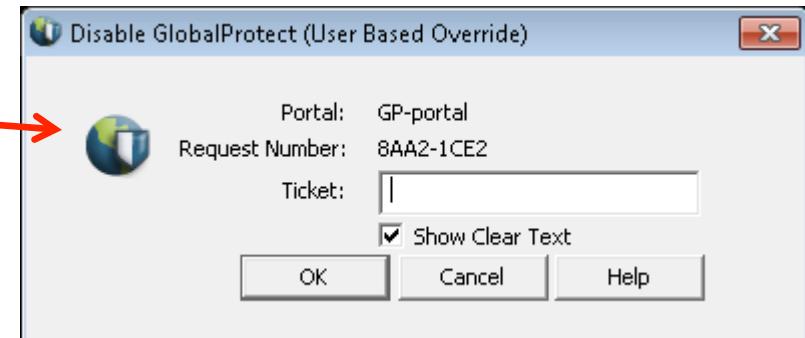
Can view the Troubleshooting tab in the Agent

End-user can disable the installed Agent

Disabling the GlobalProtect Agent - Ticket



On the Client system

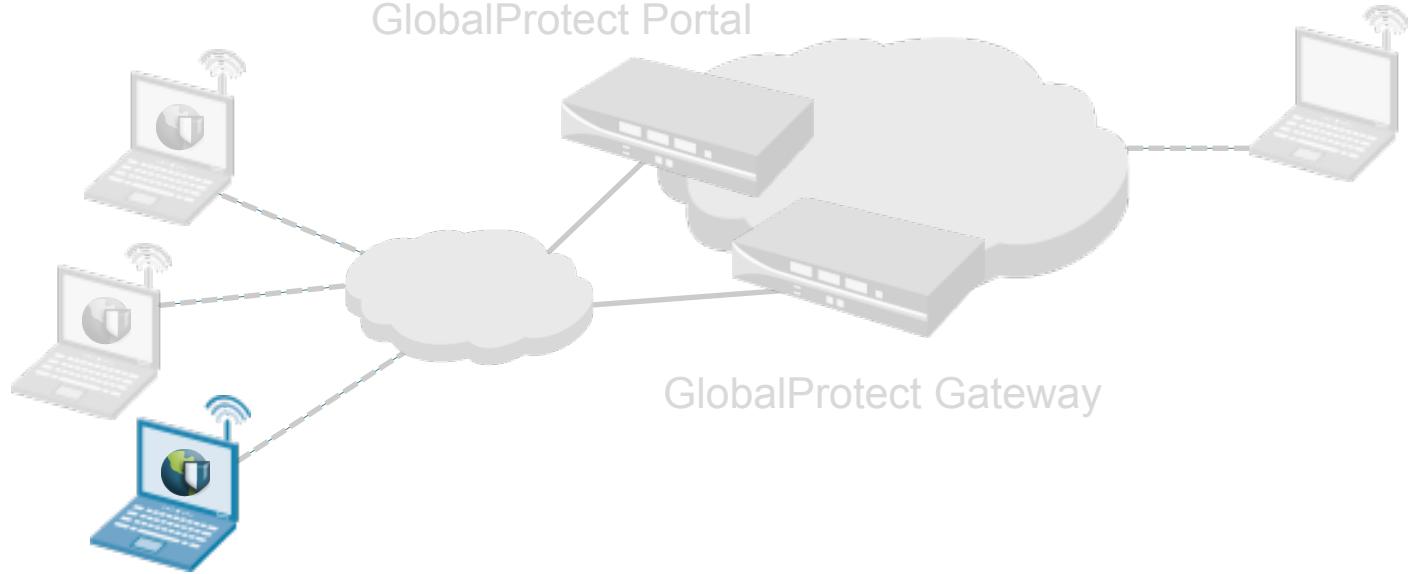


On the portal firewall



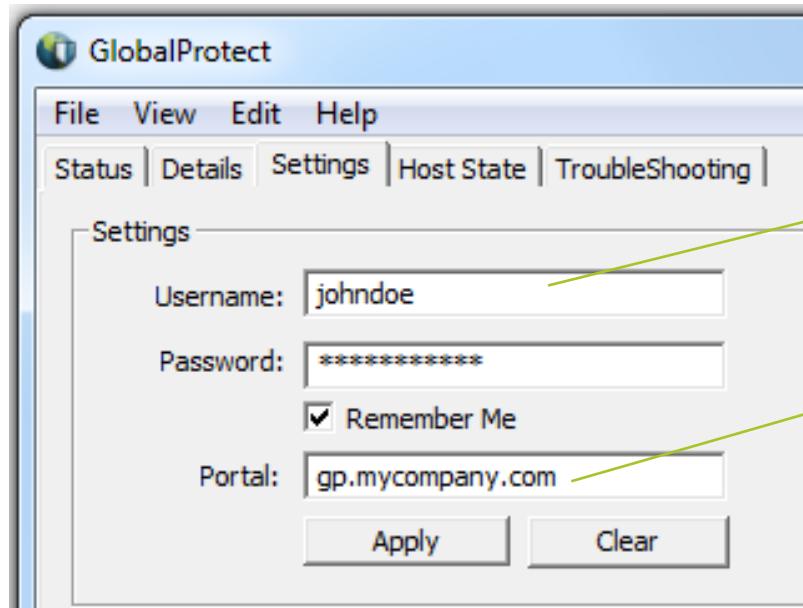
Configuration: GlobalProtect Agent

GlobalProtect Agent



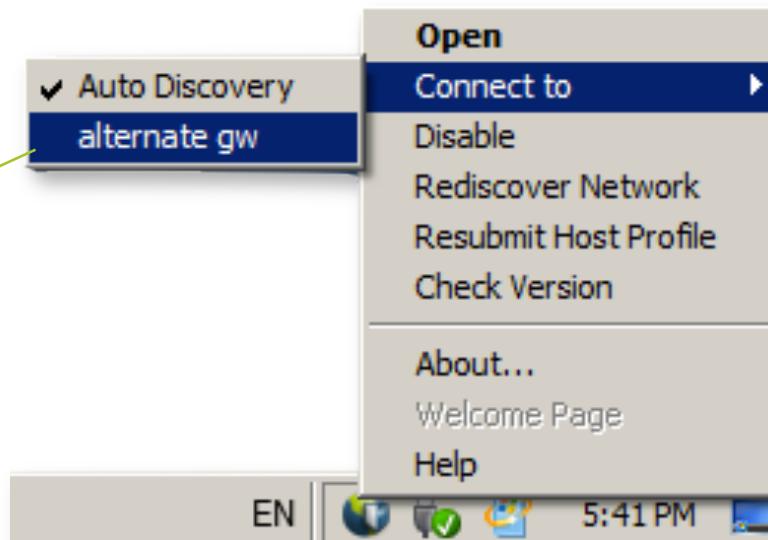
- Authenticates connection against the portal
- Establishes connection with gateways
- Sends HIP reports
- Allows users varying levels of control over the connections

Client Configuration



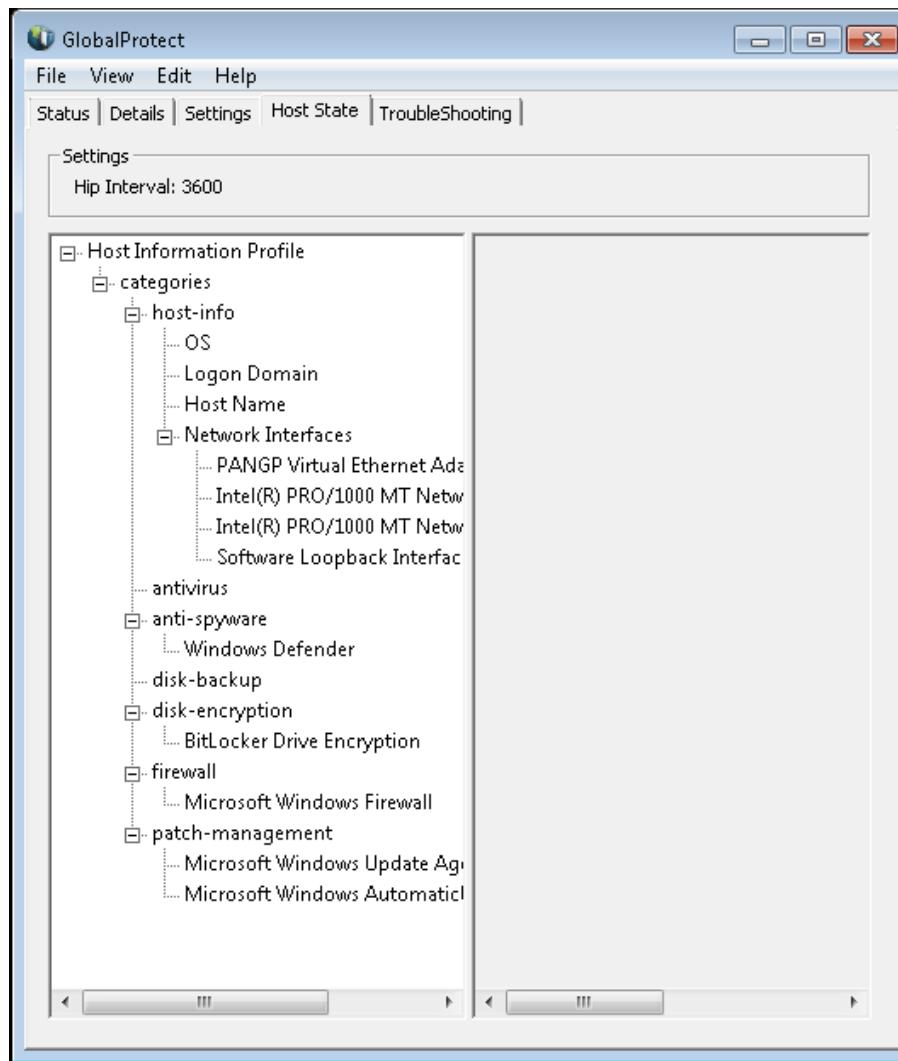
Can be left blank
if using single
sign-on

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



Manual gateway selection

Advanced View



Troubleshooting GlobalProtect Agent

The screenshot shows the GlobalProtect Agent application window. At the top, there's a toolbar with File, View, Edit, Help, and tabs for Status, Details, Settings, Host State, and TroubleShooting. Below this is a 'Connection' section with the following details:

Portal:	10.250.40.1
Assigned Local IP:	10.252.40.101
GlobalProtect Gateway IP:	10.251.40.1
Protocol:	IPSec

Under 'Statistics', the following metrics are displayed:

Bytes In:	3215284	Bytes Out:	331252
Packet In:	2831	Packet Out:	1853
Packet I/Error:	0	Packet O/Error:	0

At the bottom, there's a table for 'Gateway' information:

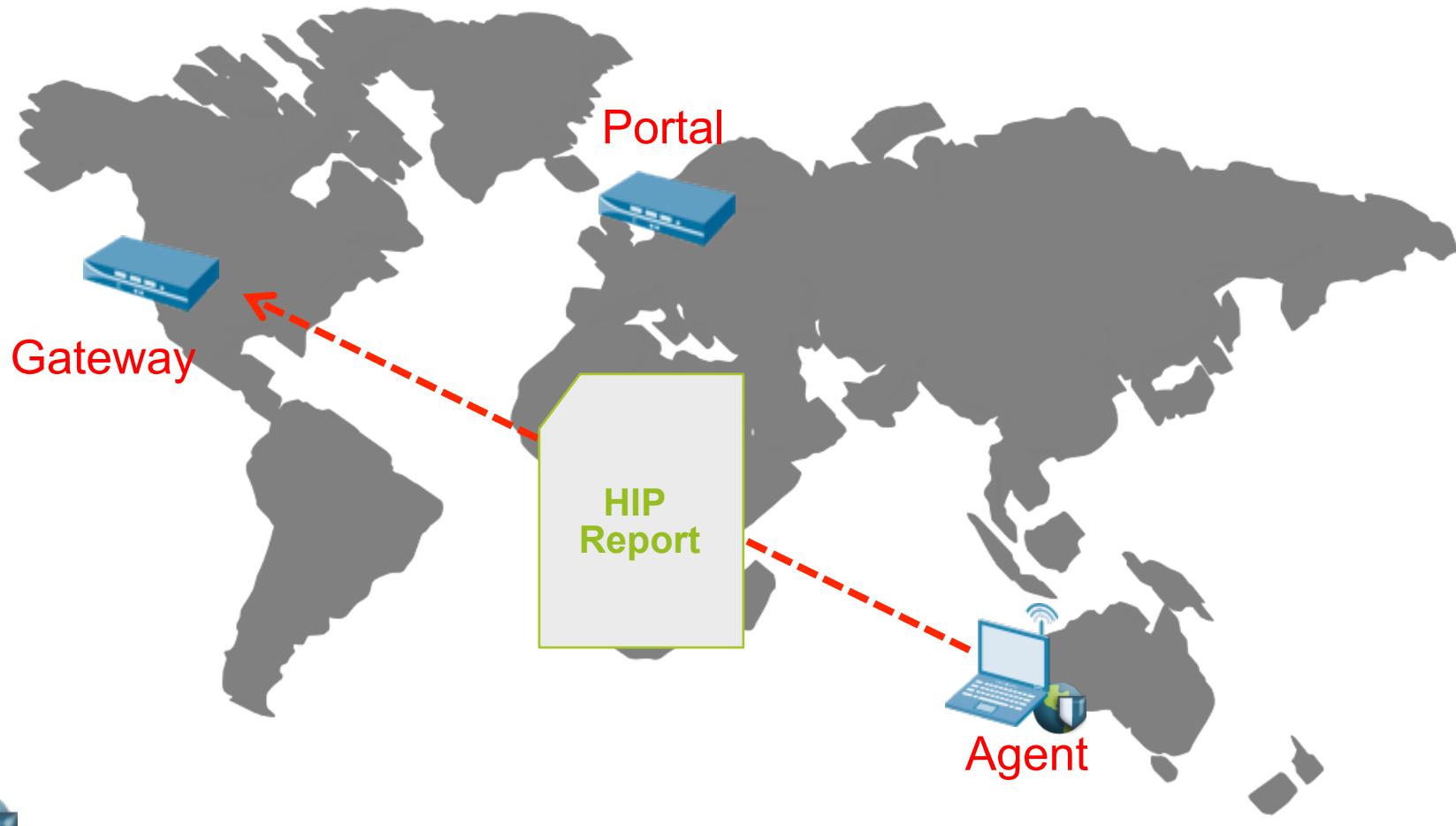
Gateway	Type	Tunnel	Status	Authenticated	Uptime	PasswdExprDays
10.251.40.1	External	Yes	Success	Yes	00:03:38	N/A

The screenshot shows the GlobalProtect Troubleshooting interface. The 'Type' dropdown is set to 'Logs'. The log area displays several debug messages from the PanGP Service:

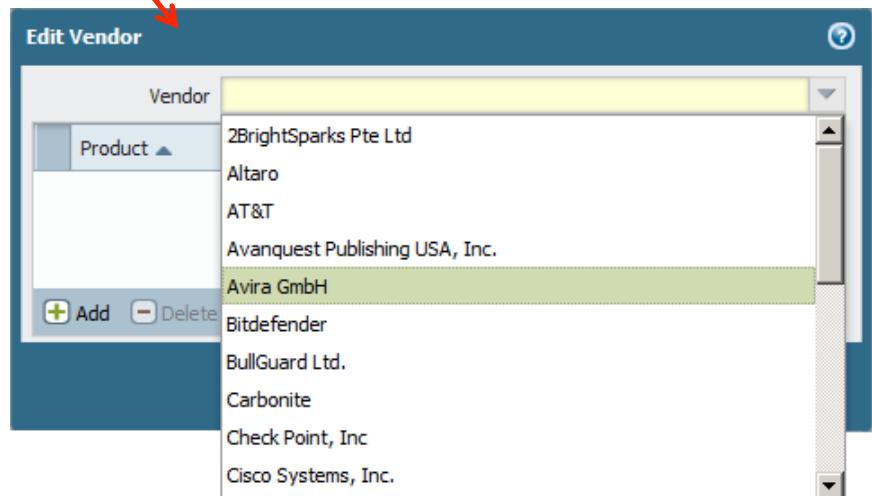
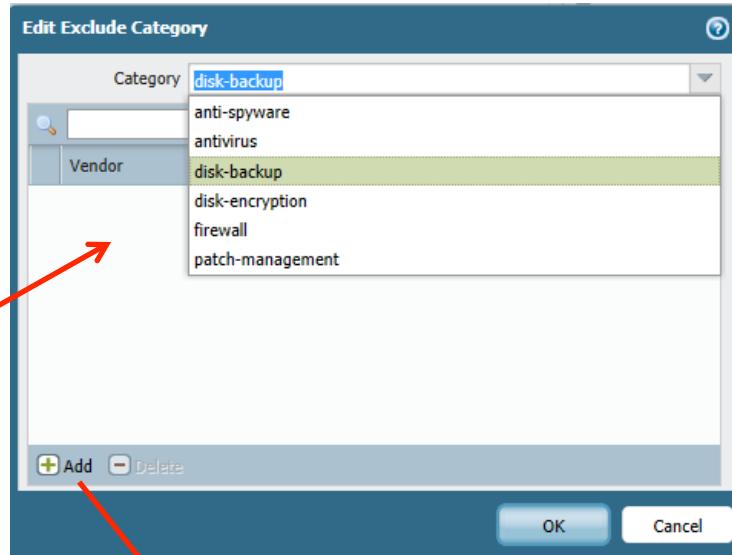
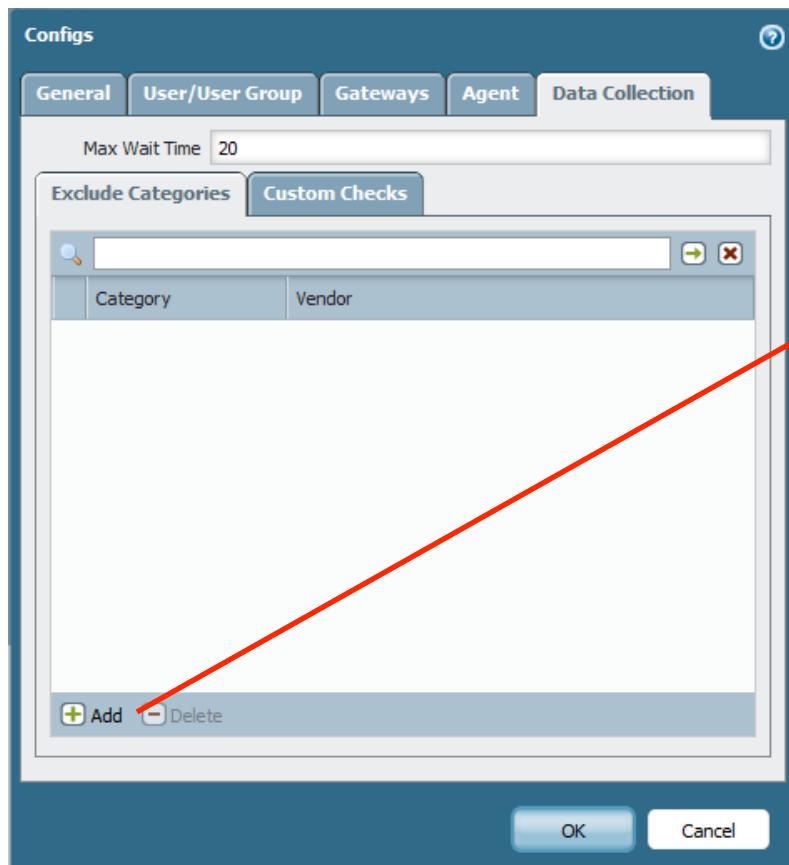
```
(T316) 11/19/12 17:21:23:756 Debug( 404): pan_get_full_path(): full path in multibyte char is C:\Pr  
(T316) 11/19/12 17:21:23:756 Debug( 720): File C:\Program Files\Palo Alto Networks\GlobalProtect\  
(T316) 11/19/12 17:21:23:756 Debug( 325): set trusted root ca file C:\Program Files\Palo Alto Netw  
(T316) 11/19/12 17:21:23:778 Debug( 828): CPanMSService::SendNReceive(): SSL is connected.  
(T316) 11/19/12 17:21:23:778 Debug( 834): Msg length is 52016. Sending POST /sslvpn/hipreport.
```

Host Checks

Host Information Profile (HIP)

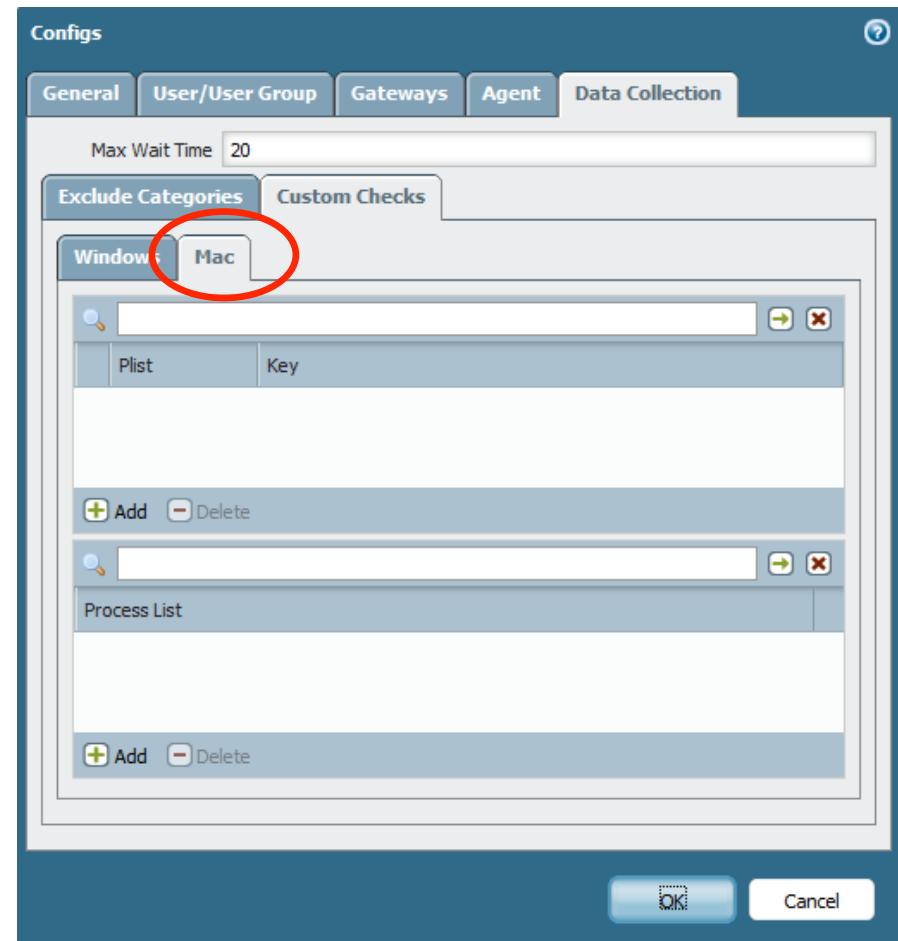
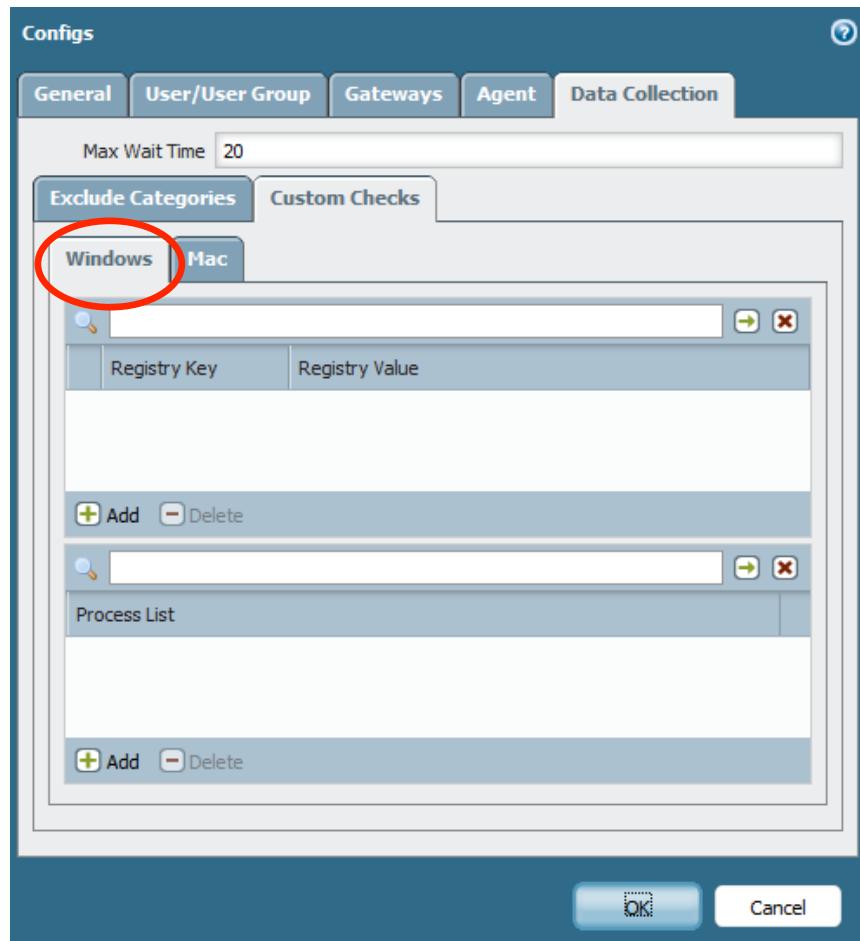


Portal: Client Configuration – Data Collection



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

Portal: Client Configuration – Custom Checks



HIP Objects

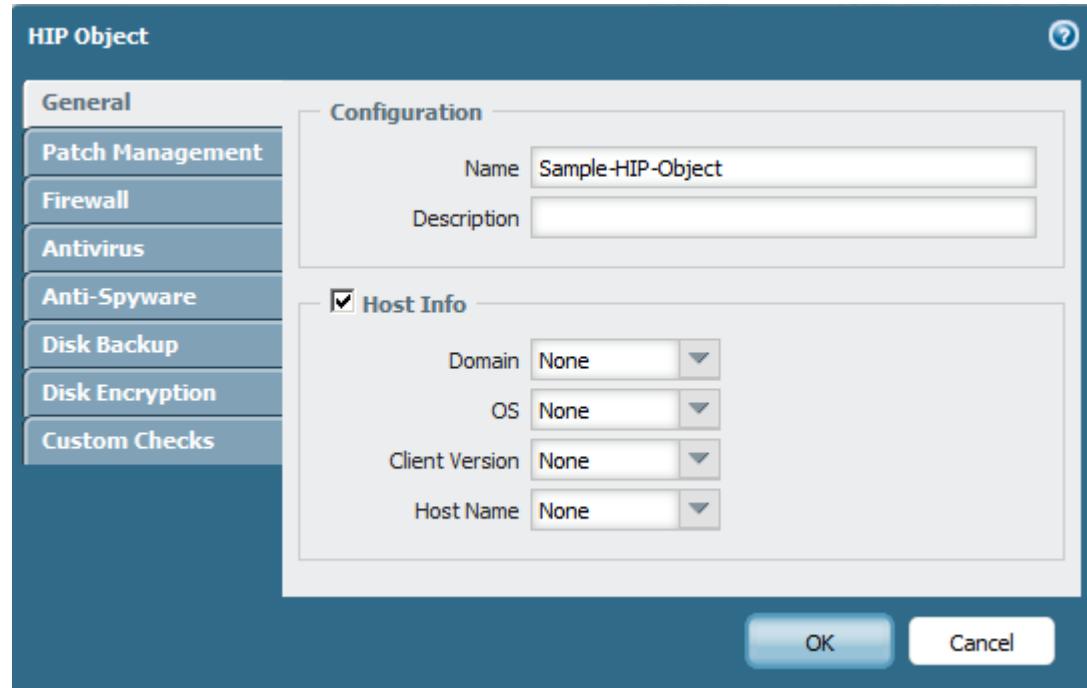
The screenshot shows the Palo Alto Networks GlobalProtect Objects interface. The left sidebar contains a navigation menu with items like Addresses, Address Groups, Regions, Applications, Application Groups, Application Filters, Services, Service Groups, GlobalProtect, HIP Objects (which is selected and highlighted in green), HIP Profiles, Custom URL Category, Dynamic Block Lists, Custom Signatures, Security Profiles, and Antivirus. The main pane displays a table of HIP Objects. The table has columns for Name, Location, Category, Criteria, and Vendor. There are two entries listed:

Name	Location	Category	Criteria	Vendor
HIP-Object-Win7-Standard-SW		host-info	os contains Microsoft Windows 7	
HIP-Object-Disk-Standards		patch-management	missing-patches check has-all is-installed yes is-enabled yes	Microsoft Corp.: Microsoft Windows AutomaticUpdate
		antivirus	virdef-version within 30 days last-scan-time within 3 days is-installed yes real-time-protection yes	Symantec Corp.: Symantec Endpoint Protection
		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

HIP Objects are used to define match criteria for GlobalProtect Clients

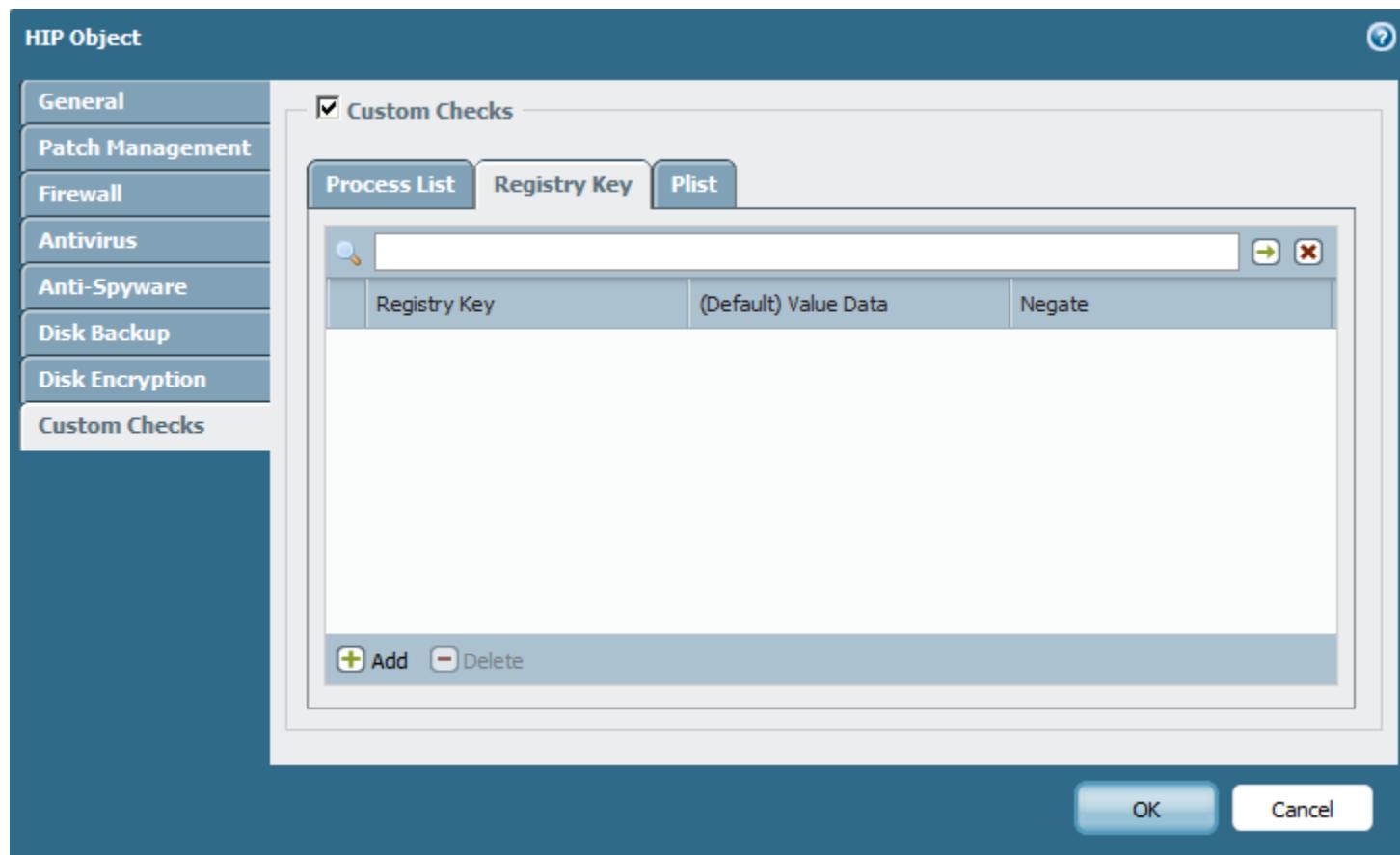
Configuring HIP Objects

Objects > GlobalProtect > HIP Objects



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

Custom Checks



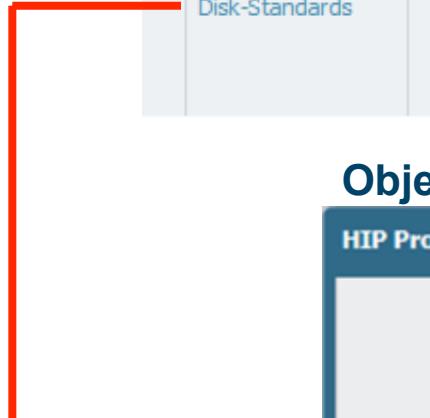
HIP objects can check for specific Registry Keys (Windows)
or Plist values (Mac)

Example - HIP Objects and Profiles

Objects > GlobalProtect > HIP Objects

Name	Location	Category	Criteria	Vendor
<input type="checkbox"/> 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
		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



HIP Profile

Name: Windows7-Disk-HIP

Description:

Match: "HIP-Object-Disk-Standards" and "HIP-Object-Win7-Standard-SW"

Add Match Criteria

OK Cancel

Security Policy with HIP Profile

Objects > GlobalProtect > HIP Profiles

HIP Profile

Name	Windows7-Disk-HIP
Description	
Match	"HIP-Object-Disk-Standards" and "HIP-Object-Win7-Standard-SW"
+ Add Match Criteria	
OK Cancel	

Policies > Security

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

Gateway: HIP Notification

Network > GlobalProtect > Gateways

The screenshot shows the GlobalProtect Gateway configuration interface. The main menu bar includes 'GlobalProtect Gateway', 'File', 'Edit', 'View', 'Help', and tabs for 'General', 'Client Configuration', 'Tunnel Settings', 'Network Settings', and 'HIP Notification'. A sub-menu 'Satellite Configuration' is also visible. The 'HIP Notification' tab is active, displaying a dialog box titled 'HIP Notification' with a 'Windows7-Disk-HIP' profile selected. The dialog has two tabs: 'Match Message' (selected) and 'Not Match Message'. Under 'Match Message', the 'Enable' checkbox is checked. The notification type is set to 'pop-up-message'. The 'Template' section shows a rich text editor with a 'Tahoma' font selected, and the message content reads: 'Your system is out of compliance with company policy and may experience reduced network performance. Contact support to bring your system back in compliance with standards.' A blue callout box labeled 'Link icon' points to the link icon in the rich text editor toolbar. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

HIP Match Log

Monitor > Logs > HIP Match

The screenshot shows the 'Monitor > Logs > HIP Match' interface. A modal window titled 'Log Details' is displayed over the log table.

Log Details:

Report Generated	07/02/2012 11:03:43
User Information	User: jparapurath
Host Information	Machine Name: PAN00317
OS	Microsoft Windows 7 Professional (build 7600), 32-bit
Client Version	1.0.0-79

Network Information:

Interface	MAC Address	IP Address
PANGP Virtual Ethernet Adapter	02-50-41-00-00-01	169.254.204.70
PAN Virtual Ethernet Adapter	02-50-41-00-00-01	169.254.16.130
Juniper Network Connect Virtual Adapter	00-FF-00-06-CF-87	169.254.160.237
Broadcom NetXtreme 57xx Gigabit Controller	A4-BA-DB-BA-3F-07	10.16.0.34
Dell Wireless 1397 WLAN Mini-Card	70-F1-A1-66-0C-4F	169.254.218.37
Software Loopback Interface 1	00-00-00-00-00-00	127.0.0.1

Antivirus:

Software	Vendor	Version	Engine Version	Definition Version	Date	Real Time Protection	Last scanned
Symantec Endpoint Protection	Symantec Corp.	11.0.5002.333	20101.3.0.103	7/1/2012 rev. 20	7/1/2012 ✓	n/a	

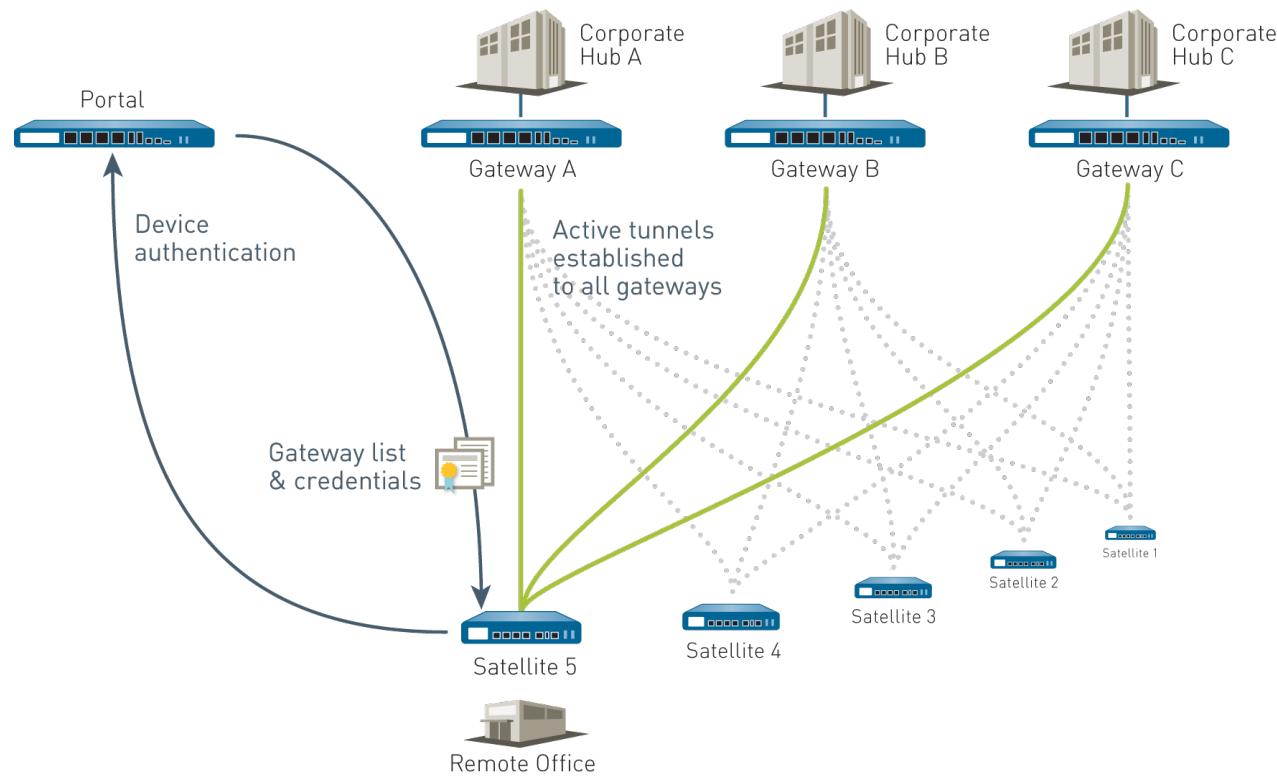
Anti-Spyware:

	F önüne	Definition	Real Time	Last

Buttons:

- Close

Large-Scale VPNs with GlobalProtect Satellites

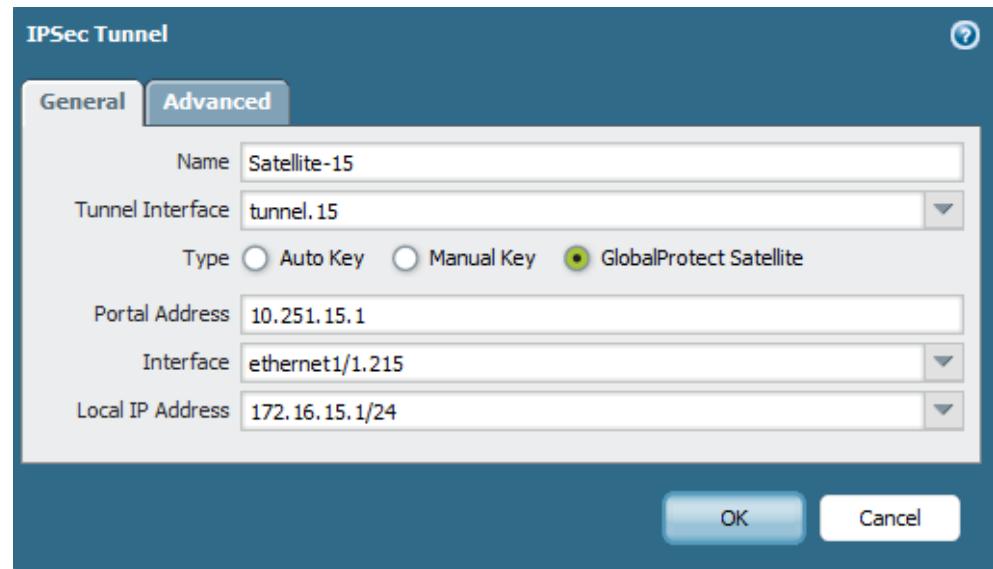


- GlobalProtect Satellites connect to existing Portal and Gateways
- Receive network and routing information from Portal like standard clients
- Minimal deployment tasks on Satellite device
- Satellites can be connected to multiple gateways simultaneously

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

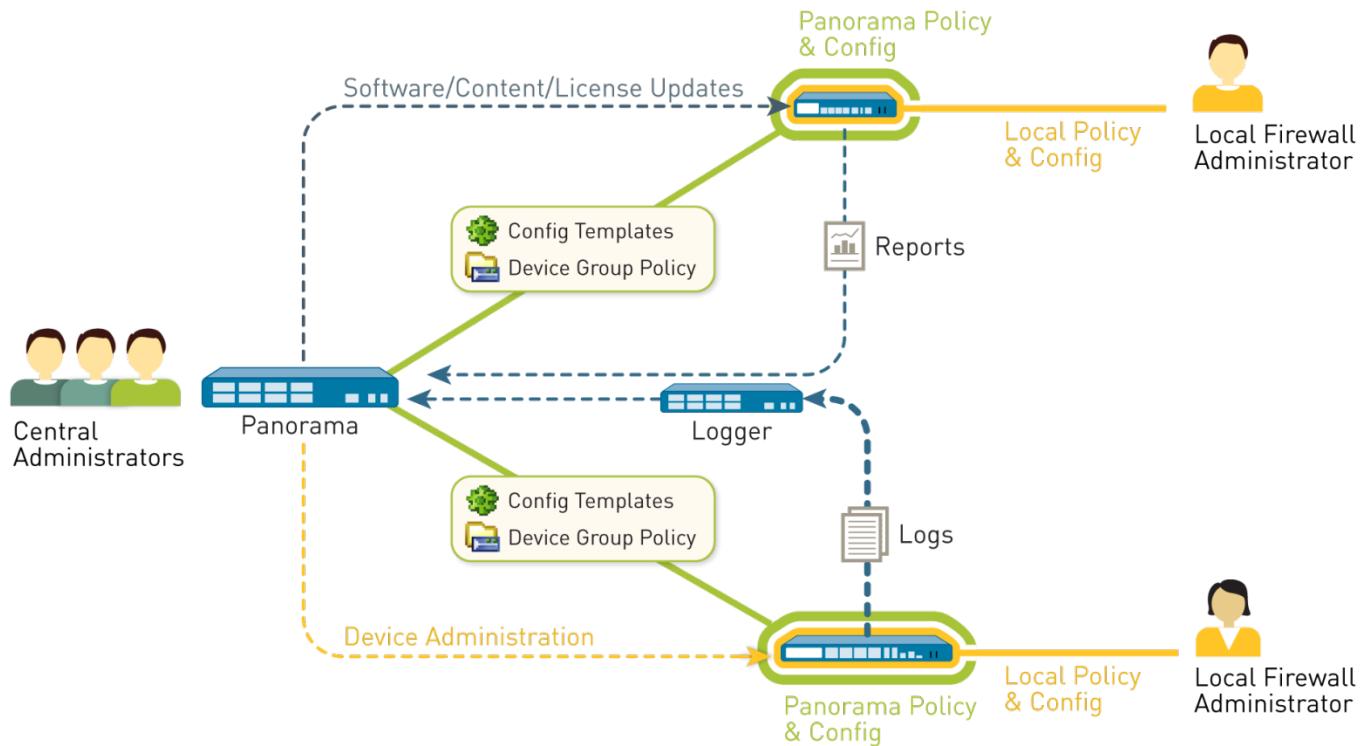


Panorama

CNSE Bootcamp

Panorama

Panorama Benefits



Panorama is designed to provide three benefits:

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

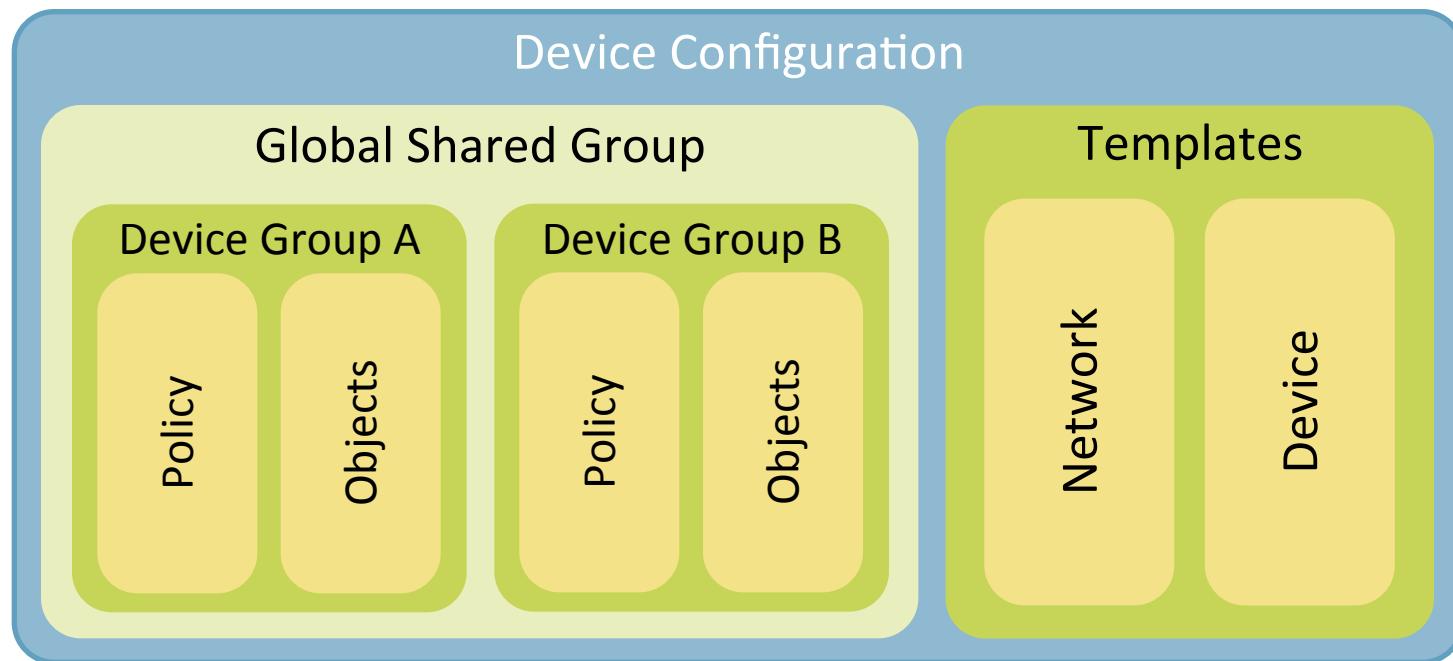
Deployment

- 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

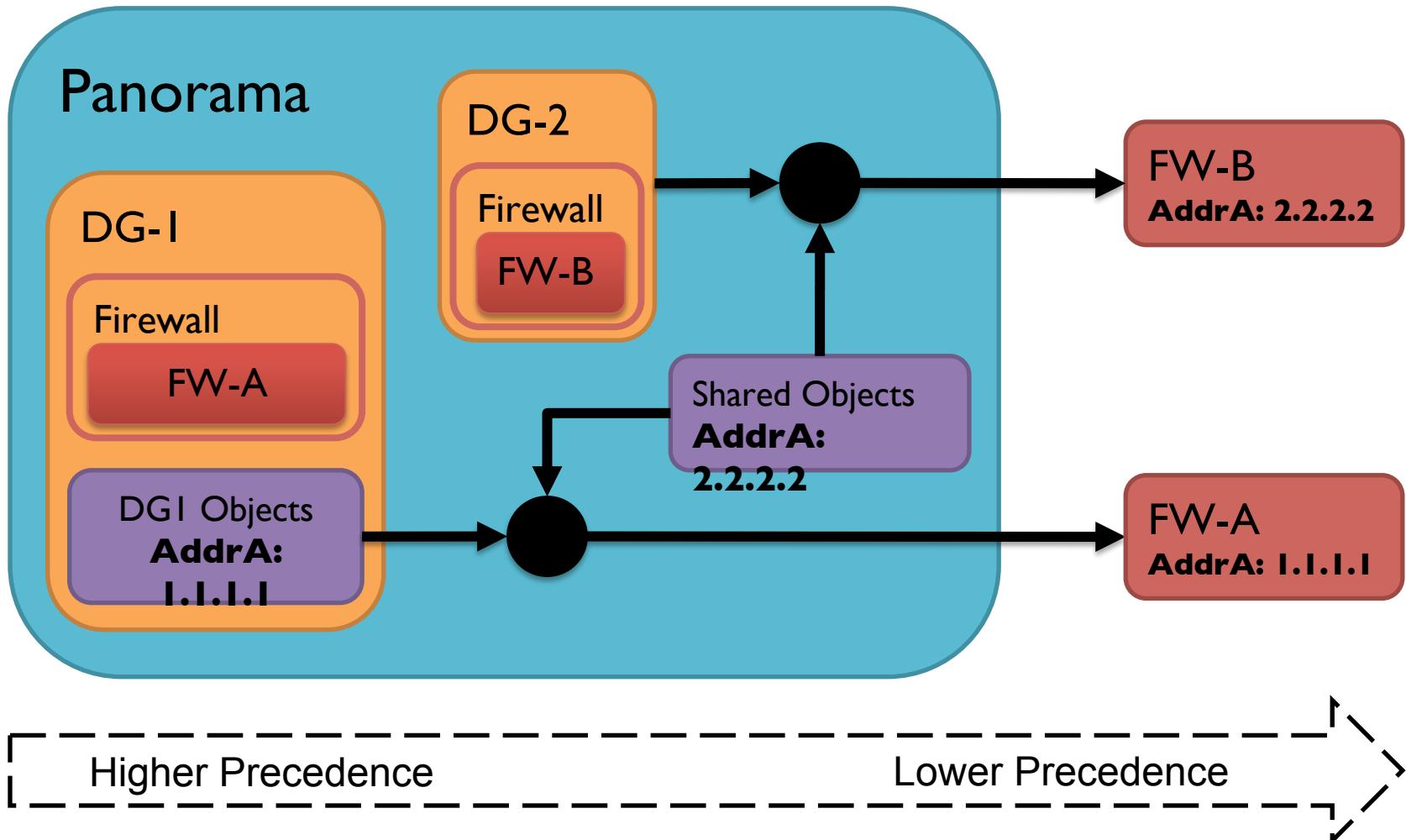
- Device Groups manage shared Policies and Objects
- Templates manage Network and Device configurations



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

The screenshot displays two windows from the Palo Alto Networks Panorama interface.

Left Window: Shows the "Device Group" list under the "Panorama" context. The selected group is "DG-01". The list includes DG-01 through DG-16. The left sidebar shows various policy categories like Security, NAT, QoS, etc., each with Pre Rules and Post Rules sub-options.

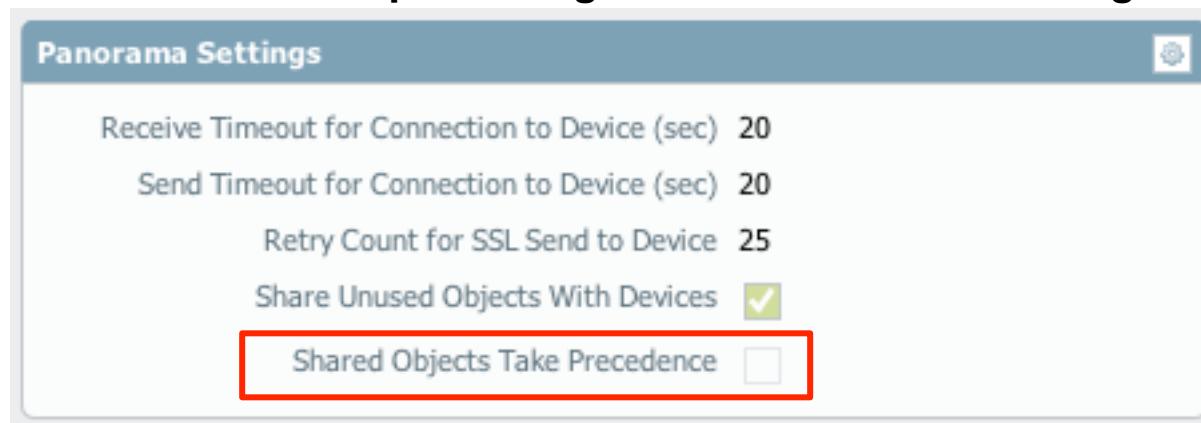
Right Window: Shows the "Combined Rules Preview" for the "ca3demo" device group. The rulesbase is set to "Security". The preview table lists numerous rules, including "Allow All Demo", "LogAll", "Read Only Facebook", "IT Allow Override", "Allow facebook posting", "Webmail file blocking", "Allow SSL and SSH", "Allow Web-browsing", "Block encrypted tunnel", "Block Peer to Peer", "Block Proxies and An...", "Mail server", and "Sharepoint". The columns include Name, Tag, Zone, Address, User, HIP Profile, Destination Zone, and Destination Address.

A red circle highlights the "Combined Rules Preview" button at the bottom of the right window's toolbar.

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

Name	Source			Destination		Application	Service	Action
	Zone	Address	User	Zone	Address			
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 Pre Rules

Panorama Post Rule

Policy Evaluation Order



Panorama Admins



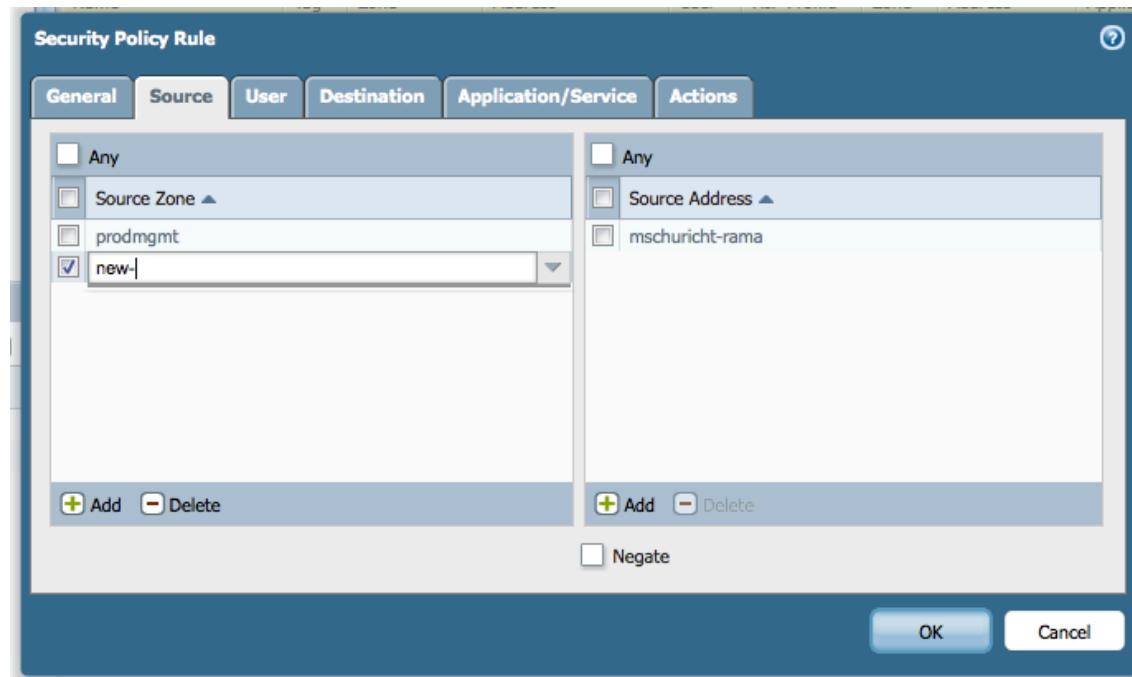
Local Admin



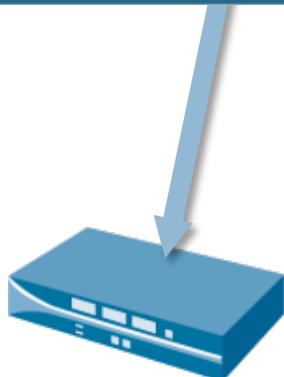
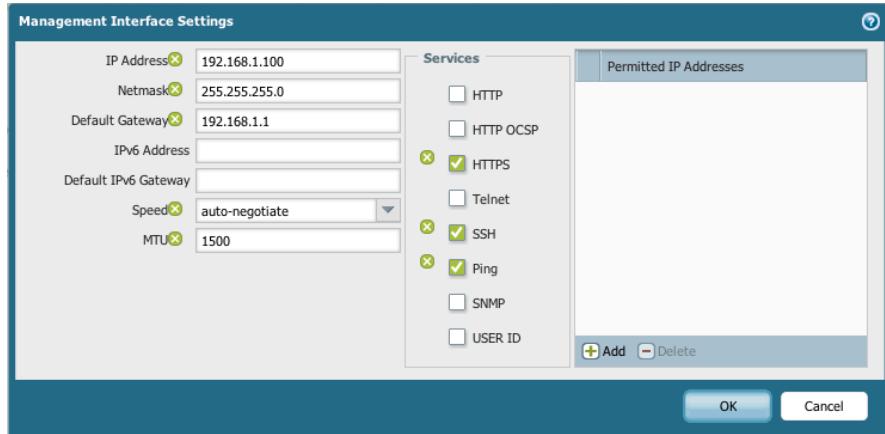
Evaluation order

Shared Policy | Zones

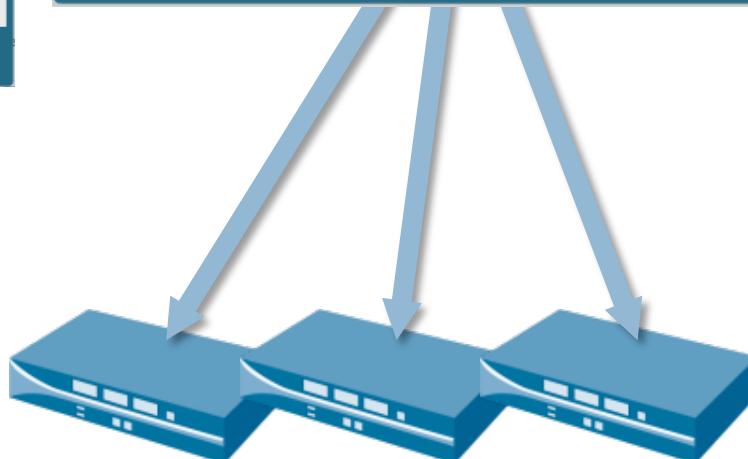
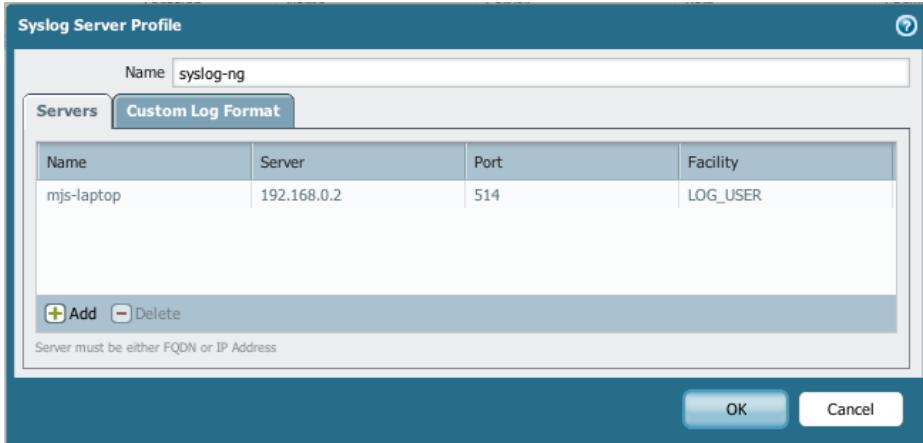
- Zones are required to be manually entered once
 - Commit All will fail if Zone does not exist on firewall
- Deletion occurs when no references or wrong reference (e.g. Missing, misspellings, case sensitivity) exists to a Zone string
 - No Zone management table like other “objects”



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

The screenshot shows the Palo Alto Networks Panorama web interface. At the top, there is a navigation bar with tabs: Dashboard, ACC, Monitor, Policies, Objects, Network, **Device**, and Panorama. Below the navigation bar is a context menu with 'Panorama' selected. On the left, there is a sidebar with various configuration options like Setup, Admin Roles, and Certificate Management. The main content area has a 'Template' dropdown set to 'tmpl720'. A red circle highlights the dropdown menu, which lists several templates: tmpl41, tmpl108 (selected), tmpl720, test1, newtmp31, tmpl1, tmpl4, test, tmpl2, test2, tmpl12, and tmpl3. To the right of the template list are three tabs: Content-ID, WildFire, and Session. Further right is a 'Panorama Settings' section with fields for Panorama Servers, Receive Timeout, Send Timeout, and Retry Count. At the bottom right is a 'Management Interface Settings' section.

Override Values on Managed Device

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

The screenshot shows the 'Management Interface Settings' dialog box. It includes fields for IP Address (192.168.1.1), Netmask (255.255.255.0), Default Gateway, IPv6 Address (200-template Value: "192.168.1.1"), Default IPv6 Gateway, Speed (auto-negotiate), and MTU (1500). To the right is a 'Services' section with checkboxes for HTTP, HTTP OCSP, HTTPS (checked), Telnet, SSH (checked), Ping (checked), SNMP, and USER ID. A 'Permitted IP Addresses' table is also present. Callouts with arrows point from text boxes on the left to specific fields or sections in the dialog:

- 'Indicates overridden value' points to the MTU field.
- 'Template name and value upon revert' points to the IPv6 Address field.
- 'Indicates templated value' points to the Services section.
- 'Templated value' points to the '200-template Value: "192.168.1.1"' text in the IPv6 Address field.

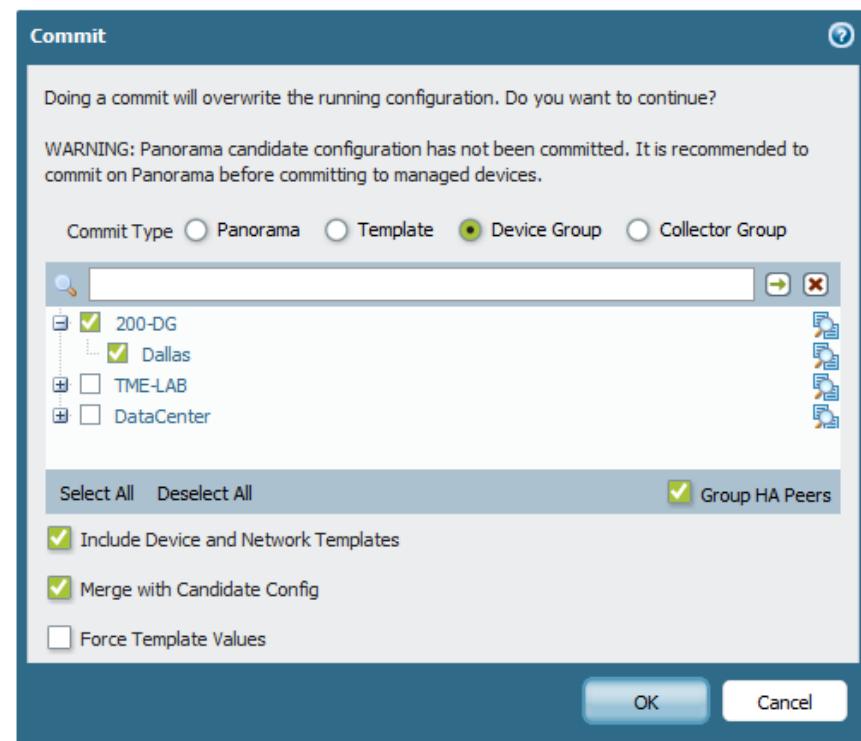
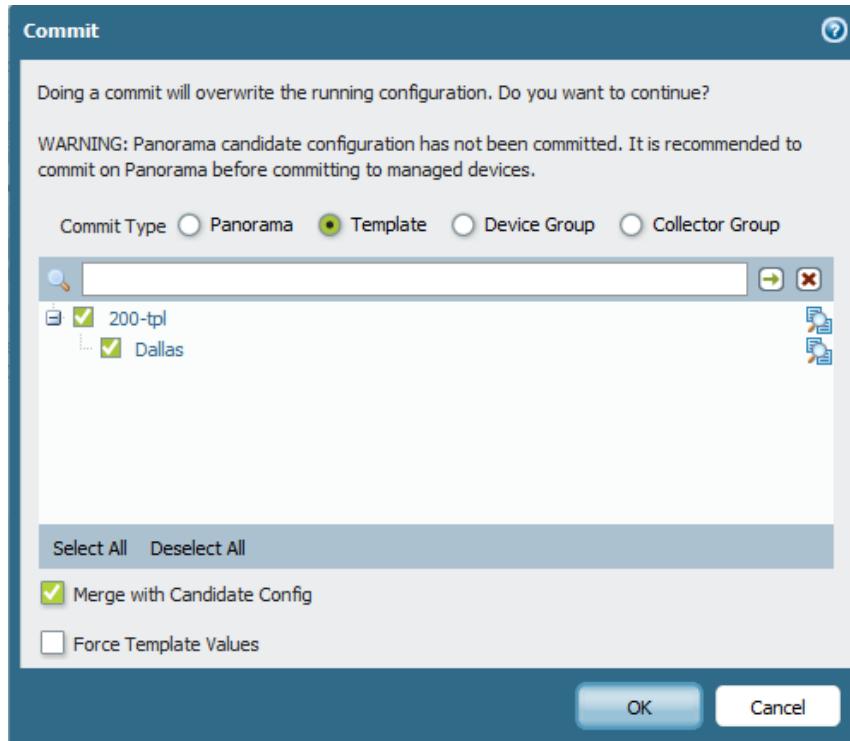
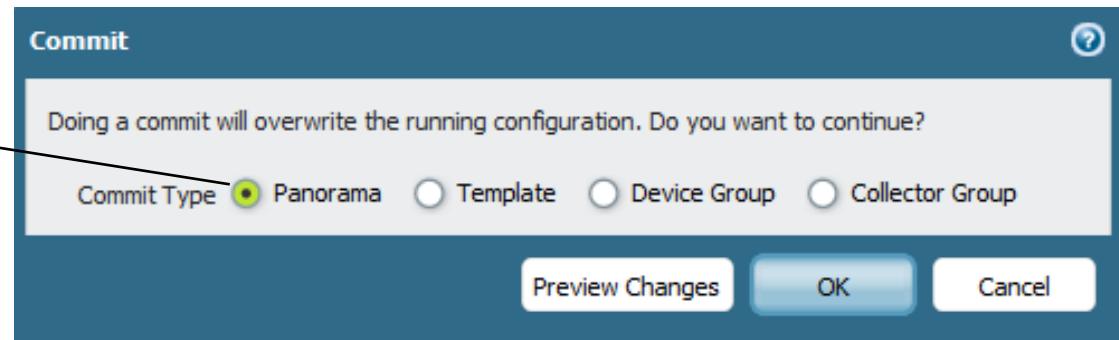
Context Switch

- 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]

The screenshot shows the Palo Alto Networks Panorama dashboard. At the top left is the Palo Alto Networks logo. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies, Objects, and Network. Below the navigation is a "DEVICE GROUPS" section. On the left, a "Context" dropdown menu is open, showing a list of devices: Panorama, ACME-GW-2, Dallas, PA-4020, PA-4060-1, PA-4060-2, PA-5060, and santadara-2. The item "PA-4060-2" is highlighted with a green background. To the right of the context menu, there are sections for "Logged In Admins" (listing admin accounts from 10.20.1.16 and 10.20.0.100), "Data Logs" (showing "No data available."), and "System Logs". A red oval highlights the "Context" dropdown menu.

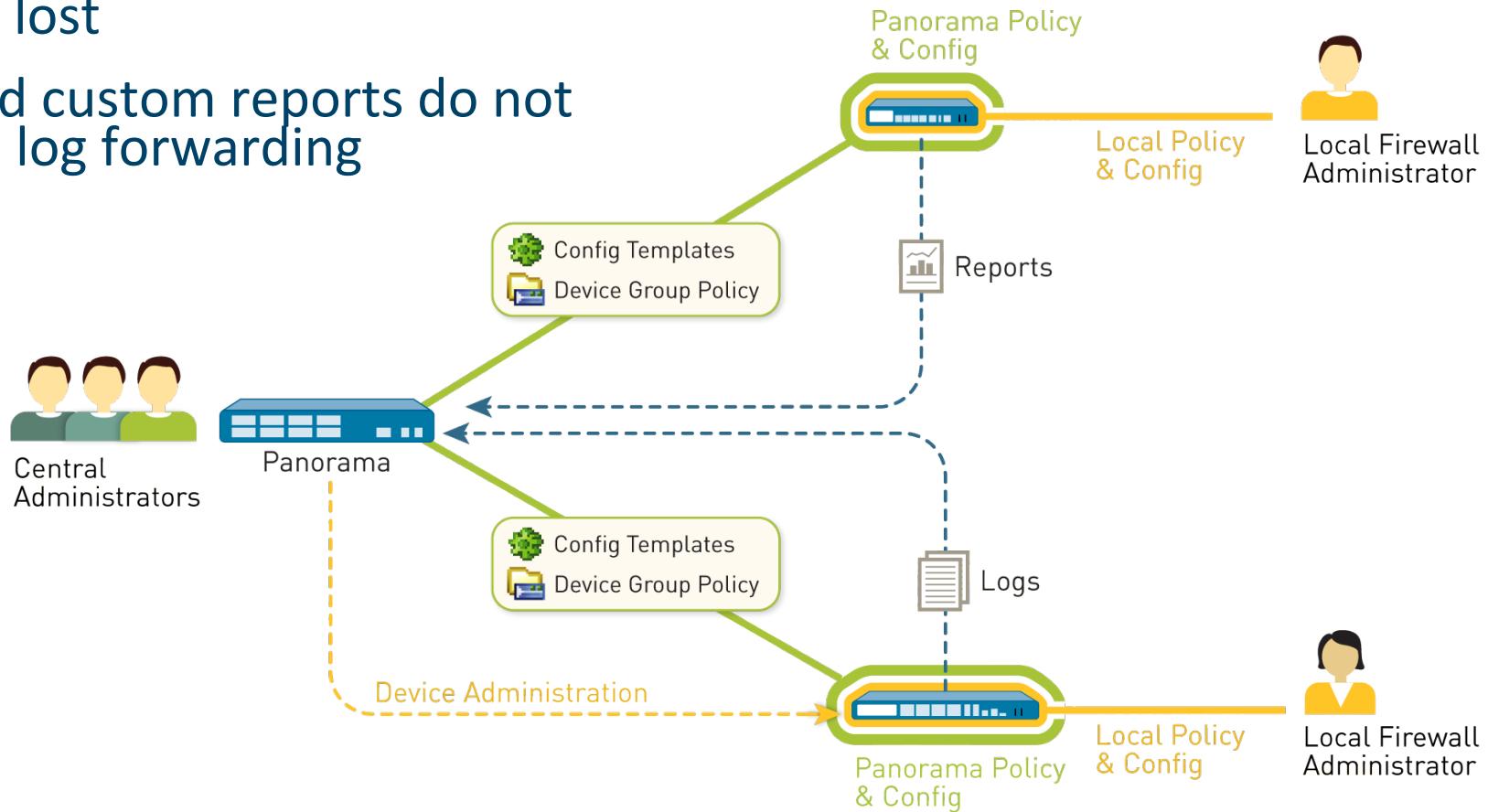
Commit Workflow

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



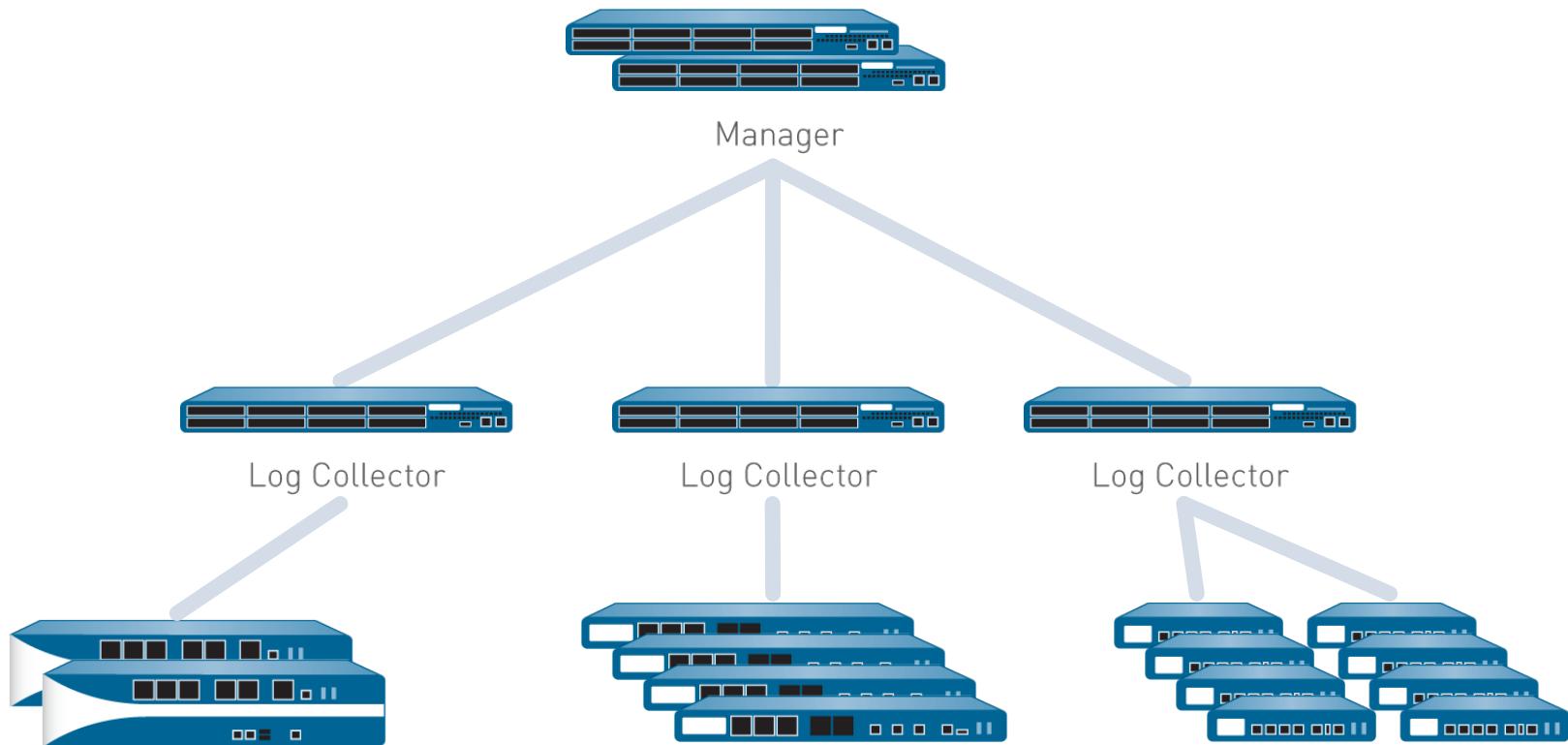
Logging and Reporting

- 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

Context: Panorama

Time Frame: Last 60 Minutes

Sort By: Sessions

Top N: 25

Go

Custom select ...

Panorama

Application Command Center

Top 25 Applications

Application	Sessions	Bytes	Threats
4 web-browsing	10,080	1,726,094,385	10,024

Context: training1

Time Frame: Last 60 Minutes

Sort By: Sessions

Top N: 25

Go

Custom select ...

Firewall 1

Application Command Center

Top 25 Applications

Application	Sessions	Bytes	Threats
4 web-browsing	10,004	1,725,436,986	10,024

Context: Training 4

Time Frame: Last 60 Minutes

Sort By: Sessions

Top N: 25

Go

Custom select ...

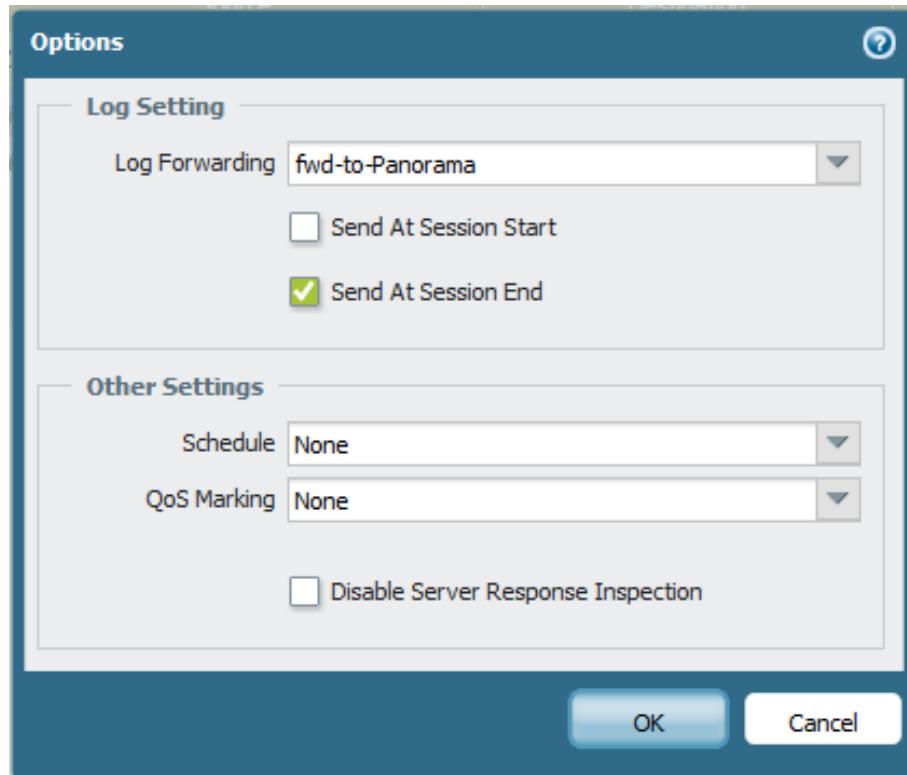
Firewall 2

Application Command Center

Top 25 Applications

Application	Sessions	Bytes	Threats
4 web-browsing	76	657,399	0

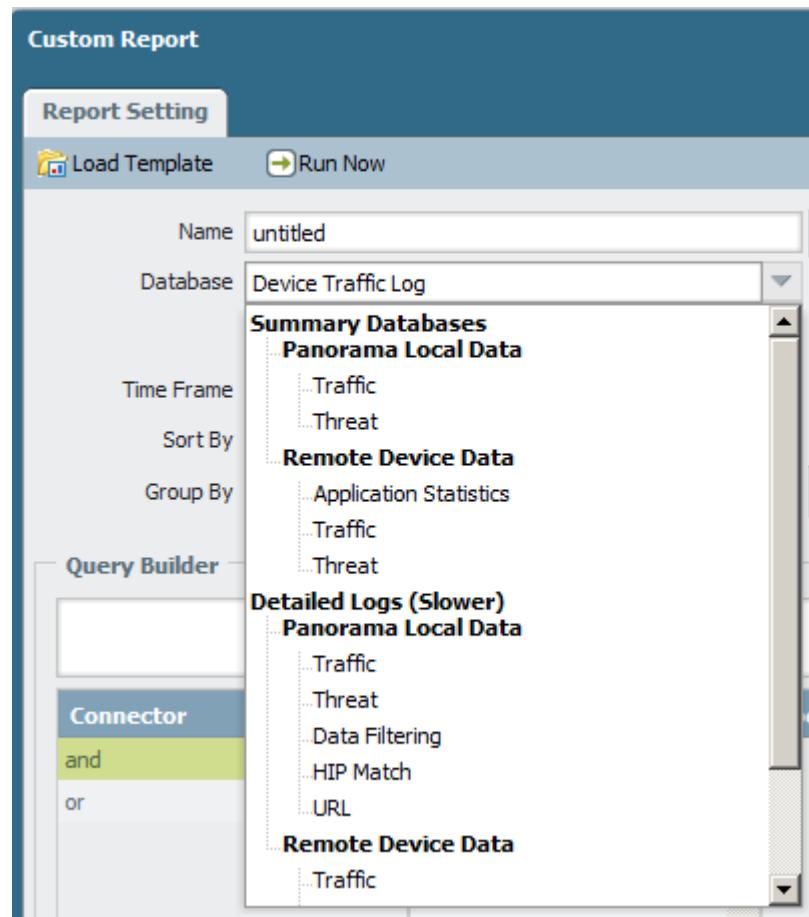
Logging and Reporting Configurations



- 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?