



# PCNSE Bootcamp v10.1

Exam Domain #4  
Manage & Operate



## 4.1 Manage and Configure Log Forwarding

# Review - Where to apply Log Forwarding Profiles

The screenshot shows the 'Actions' tab of a 'Security Policy Rule' configuration. The 'Log Setting' section is expanded, displaying the following configuration:

- Action Setting: Action set to 'Allow', with the 'Send ICMP Unreachable' checkbox unchecked.
- Profile Setting: Profile Type set to 'Group', with the Group Profile set to 'Alert\_All'.
- Log Setting:
  - Log at Session Start: Unchecked
  - Log at Session End: Checked
  - Log Forwarding: Set to 'Add\_tag'
- Other Settings:
  - Schedule: Set to 'None'
  - QoS Marking: Set to 'None'
  - Disable Server Re: Unchecked

A red arrow points from the 'Log Forwarding' field in the main configuration to the same field in a detailed view of the 'Log Setting' section on the right, which is also highlighted with a red border. This indicates that the 'Log Forwarding' setting is being applied at the rule level.

# Log Forwarding Profile

Log Forwarding Profile

Name  ?

Shared  
 Enable enhanced application logging to Cortex Data Lake (including traffic and url logs)  
 Disable override

Description

<input type="checkbox"/>	NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS
<input type="checkbox"/>	Send_some_logs-threat-info	threat	(severity eq informational)		
<input type="checkbox"/>	Send_some_logs-threat-low	threat	(severity eq low)	<ul style="list-style-type: none"><li>• Panorama/Cortex Data Lake</li></ul>	
<input type="checkbox"/>	Send_some_logs-threat-med	threat	(severity eq medium)	<ul style="list-style-type: none"><li>• Panorama/Cortex Data Lake</li></ul>	
<input type="checkbox"/>	Send_some_logs-url-med	url	(severity eq medium)	<ul style="list-style-type: none"><li>• Panorama/Cortex Data Lake</li></ul>	
<input type="checkbox"/>	Send_some_logs-data-med	data	(severity eq medium)		
<input type="checkbox"/>	Send_some_logs-threat-hi	threat	(severity eq high)	<ul style="list-style-type: none"><li>• Panorama/Cortex Data Lake</li></ul>	
<input type="checkbox"/>	Send_some_logs-url-hi	url	(severity eq high)	<ul style="list-style-type: none"><li>• Panorama/Cortex Data Lake</li></ul>	
<input type="checkbox"/>	Send_some_logs-data-hi	data	(severity eq high)		

+ Add - Delete Clone

OK Cancel

## 4.1.1 Identify log types and criticalities

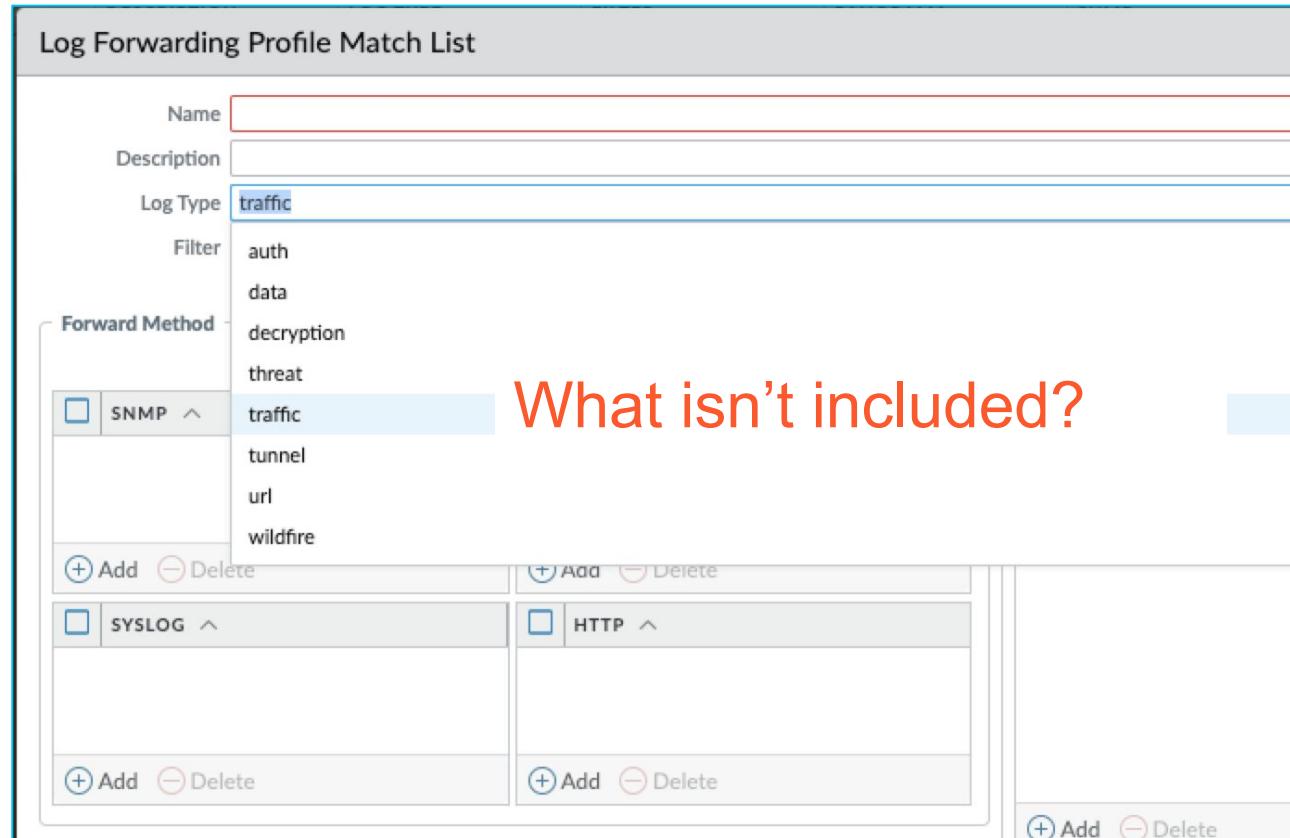
Log forwarding is covered heavily on the test. Understand the different types of logs from which you can forward.

- Authentication
- Data Filtering
- Decryption
- Traffic
- Threat
- Tunnel
- URL Filtering
- WildFire Submissions

Log Forwarding Profile Match List

Name: [redacted]  
Description: [redacted]  
Log Type: traffic  
Filter: auth, data, decryption, threat, tunnel, url, wildfire  
Forward Method: SNMP (selected), SYSLOG, HTTP  
Actions: + Add, - Delete

What isn't included?

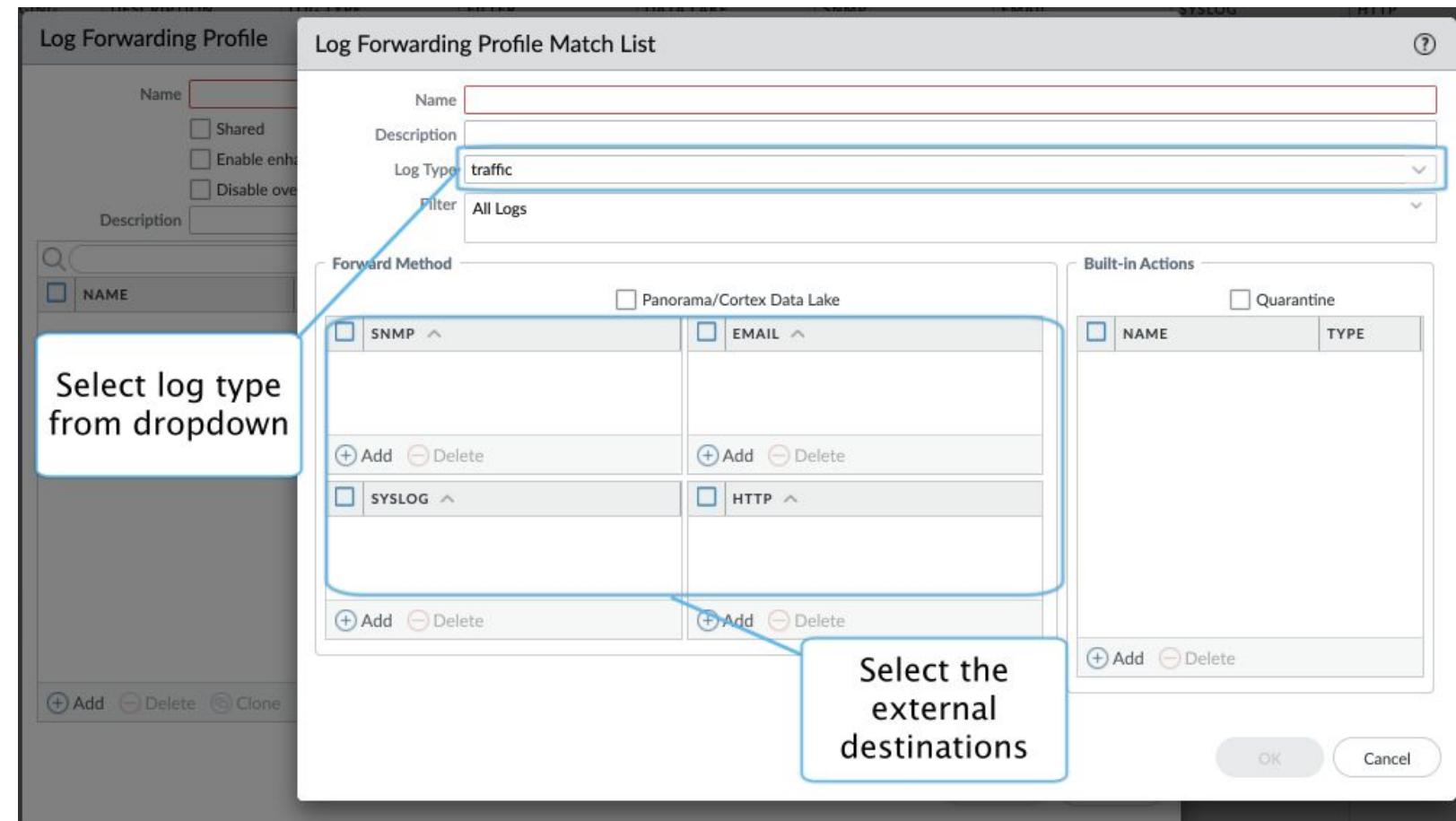


The screenshot shows a configuration interface for a log forwarding profile. At the top, there are fields for 'Name' and 'Description'. Below that is a 'Log Type' dropdown set to 'traffic', with other options like 'auth', 'data', 'decryption', 'threat', 'tunnel', 'url', and 'wildfire' listed. A 'Forward Method' section is open, showing 'SNMP' as the selected method, with 'SYSLOG' and 'HTTP' also available. There are '+ Add' and '- Delete' buttons for each method. A red annotation 'What isn't included?' is placed next to the list of log types.

# Methods Used to Forward Logs

## Method 1 - Log Forwarding Profile

Objects > Log Forwarding



# Methods Used to Forward Logs

Two Methods used to forward log events depending on the type

## Method 2

### Device > Log Settings

- System
- Config
- User-ID
- HIP Match
- IP-Tag
- GlobalProtect

The screenshot shows the PA-850 device configuration interface under the 'DEVICE' tab. On the left, a navigation tree includes 'Data Requisition', 'Device Quarantine', 'VM Information Sources', 'Troubleshooting', 'Certificate Management' (selected), 'Certificates', 'Certificate Profile', 'OCSP Responder', 'SSL/TLS Service Profile', 'SCEP', 'SSL Decryption Exclusion', 'SSH Service Profile', 'Response Pages', 'Log Settings' (highlighted with a red arrow), 'Server Profiles', 'SNMP Trap', 'Syslog', 'Email', 'HTTP', 'Netflow', and 'RADIUS'. The main area displays two tables: 'System' and 'Configuration'. The 'System' table lists log entries with columns for NAME, DESCRIPTION, FILTER, and PANORAMA. The 'Configuration' table lists log entries with columns for NAME, DESCRIPTION, FILTER, and PANORAMA. A red arrow points from the 'Log Settings' item in the navigation tree to the 'Log Settings' section in the main content area.

NAME	DESCRIPTION	FILTER	PANORAMA
system_logs		All Logs	<input checked="" type="checkbox"/>
auth_logs		(subtype eq auth)	<input type="checkbox"/>
Email for power failure		(eventid eq ps-failure)	<input type="checkbox"/>
power_off		(description contains 'Chassis Master Alarm: Power Supply')	<input type="checkbox"/>

NAME	DESCRIPTION	FILTER	PANORAMA
Config_files		All Logs	<input checked="" type="checkbox"/>

PANORAMA	SNMP TRAP	EMAIL	SYSLOG	HTTP
----------	-----------	-------	--------	------

# Log Message Format Customization

The screenshots demonstrate the process of customizing log message formats in a network management system. The top-left view shows the navigation structure where 'Server Profiles' is selected, and 'Syslog' is highlighted. The bottom-left view shows the configuration for a 'Syslog Server Profile' named 'synology'. The right view is a detailed 'Edit Log Format' dialog box where users can define their own log format by selecting fields from a list.

**Syslog Server Profile**

Name: synology

Servers | Custom Log Format ←

NAME	SYSLOG SERVER	TRANSPORT	PORT	FORMAT	FACILITY
syslog	10.168.12.45	UDP	514	BSD	LOG_LOCAL

+ Add - Delete

Enter the IP address or FQDN of the Syslog server

**Edit Log Format**

**Traffic Log Format**

```
$bytes_received $cef-formatted-receive_time $bytes_sent  
$action_source $action $dg_hier_level_3 $container_of_app  
$device_name $is_saas_of_app
```

Fields

- 
- dst\_uuid
- dst\_vendor
- dstloc
- dstuser
- dynusergroup\_name
- elapsed
- flags
- from
- high\_res\_timestamp
- hostid
- http2\_connection
- inbound\_if
- is\_saas\_of\_app
- link\_change\_count
- link\_switches
- logset
- monitortag
- natdport
- natdst
- natsport
- natsrc
- ndpmatches
- nftrans
- nssai\_sd
- necai ect

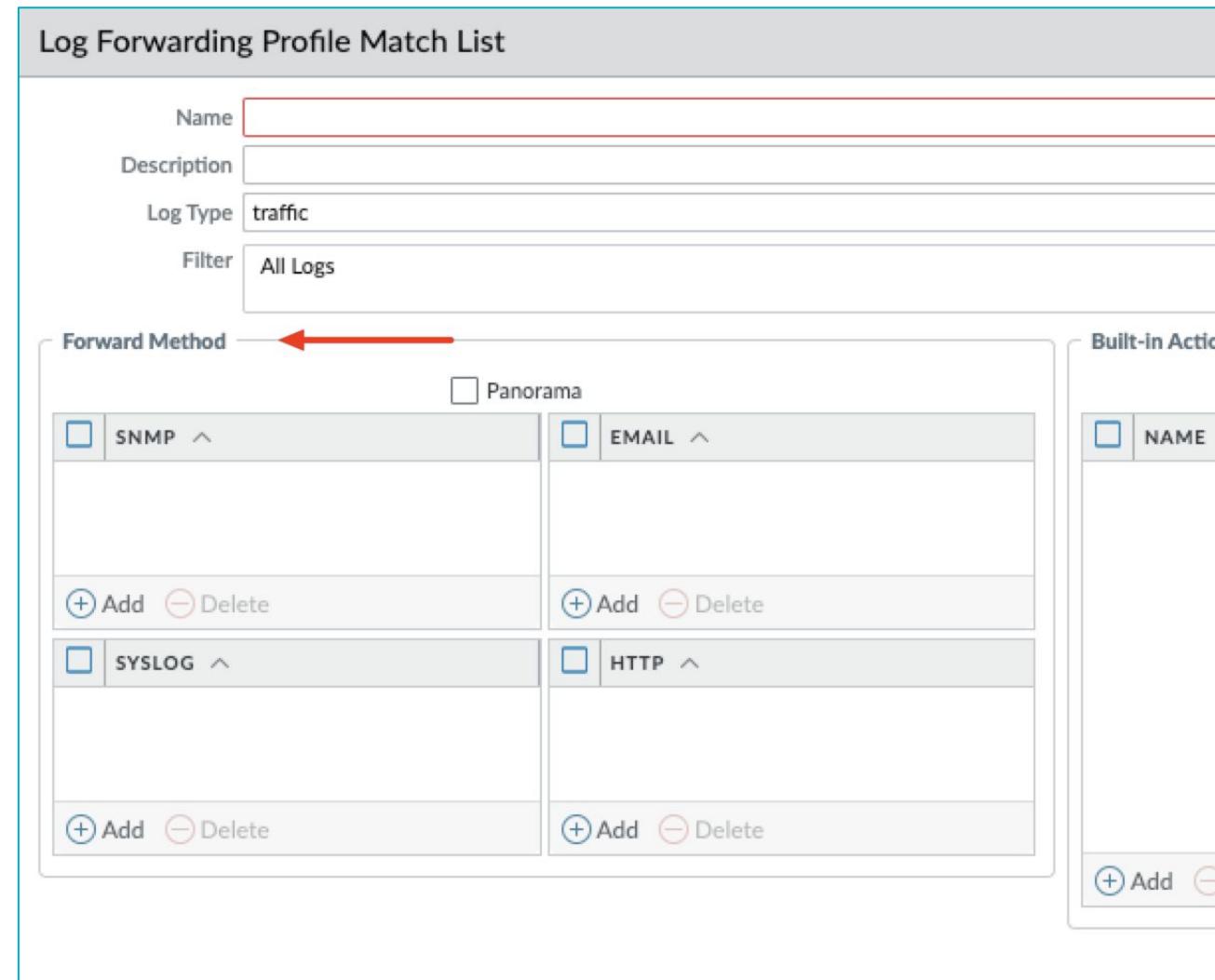
Enter the log format above. Click on the field names in the left panel to include them in the log format.

Restore default

OK Cancel

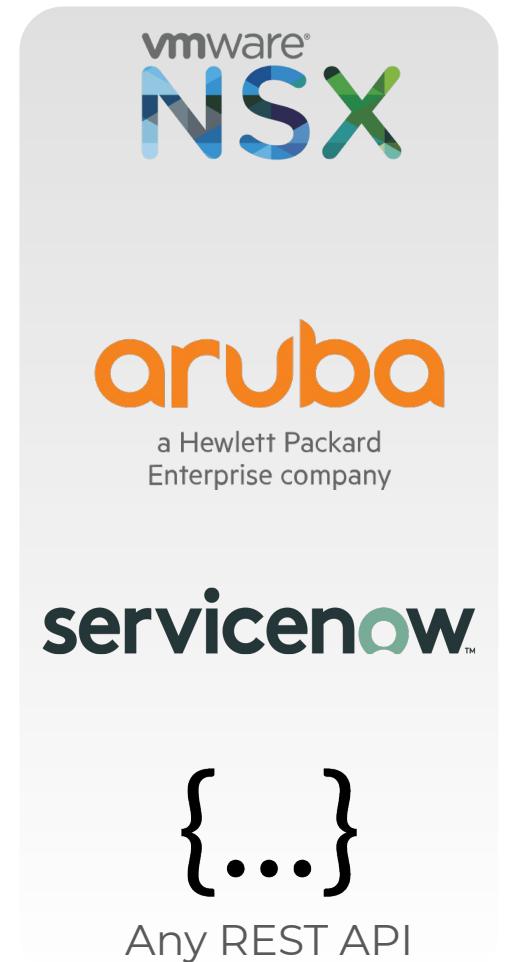
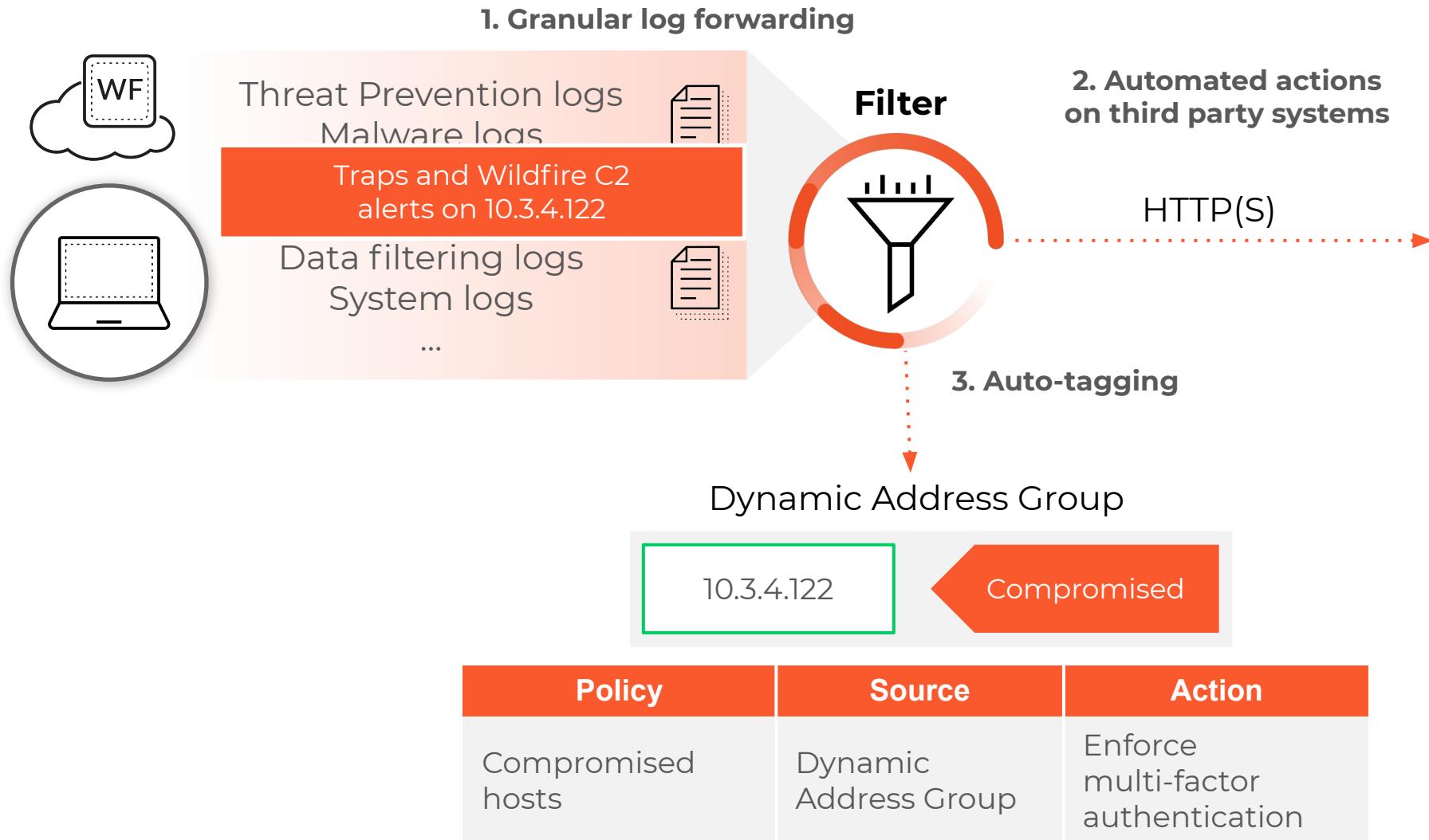
## 4.1.2 - More Logging Forwarding - Managing External Services

- SNMP traps
- Syslog
- HTTP server
- Email
- Panorama/Cortex Data Lake



## 4.1.3 Tags and Log Forwarding

Log Forwarding Profiles also provide a mechanism to collect the source or destination IP address of the event and tag it. The tag then can be used to assign the address to a Dynamic Address Group that is used in a Security policy rule.



# Automated Actions and Tagging with Log Forwarding

Log Forwarding Profiles also provide a mechanism to collect the source or destination IP address of the event and tag it. The tag then can be used to assign the address to a Dynamic Address Group that is used in a Security policy rule.

The screenshot shows the 'Log Forwarding Profile Match List' interface. At the top, there are two question mark icons. Below them, a 'Create Filter' button is highlighted in blue. The main area displays a filter condition: '(rule eq 'LogSinkHoleTraffic')'. A table below shows the detailed configuration of this filter:

Connector	Attribute	Operator	Value
and	Action	equal	From Policy
or	Action Source	not equal	From Application
Use with multiple match conditions			
<input type="checkbox"/> Negate	Address		
	App Characteristic		
	App Container		
	App Flap Count		
	App SaaS		
	App Sanctioned State		
	App Technology		
	Application		
	Application Characteristic		

At the bottom right are 'OK' and 'Cancel' buttons. A blue box highlights the 'Connector' column, and another blue box highlights the 'Operator' column. A blue callout box labeled 'Use with multiple match conditions' points to the 'Connector' column. A blue '+' icon with the text 'Add' is located in the top right corner of the table area.

# Going through adding Tagging Actions

- You can take an action for all log types that include a source or destination IP address in the log entry. You can tag the source IP address only, in Correlation logs and HIP Match logs; you cannot configure an action for System logs and Configuration logs because the log type does not include an IP address in the log entry.

Action

Name [redacted]

Tagging

Target: Source Address

Action:  Add Tag  Remove Tag

Registration: Local User-ID

Timeout (min): 0

Tags: [redacted]

Action

Name [redacted]

Tagging

Target: Source Address

Action: Destination Address

Registration: Source Address

Timeout (min): User

Tags: X-Forwarded-For Address

Action

Name [redacted]

Tagging

Target: Source Address

Action:  Add Tag  Remove Tag

Registration: Local User-ID

Timeout (min): 0

Tags: Local User-ID, Panorama User-ID, Remote User-ID

# Steps

1. Create Tag

Tag

Name: No\_decrypt\_tag  
 Shared  
Color: Magenta  
Comments: Don't decrypt destination

OK Cancel

2. Associate Tag with Dynamic Address Group

Address Group

Name: destinations\_not\_decrypted  
 Shared  
 Disable override  
Description:  
Type: Dynamic  
Match: 'No\_decrypt\_tag'

3. Create log forwarding profile to utilize a built in action to reference the tag

Action

Name: add\_dest\_to\_no\_decrypt  
Type:  Integration  Tagging

Tagging

Target: Destination Address  
Action:  Add Tag  Remove Tag  
Registration: Local User-ID  
Timeout (min): 1  
Tags: No\_decrypt\_tag

4. Create a Security Rule that takes uses tag

# CSV Log Export



The screenshot shows a log export interface with a large table of session logs and a modal dialog for exporting data to CSV.

**Table Headers:**

- Receive Time
- Type
- From Zone
- To Zone
- Source
- Source User
- Destination
- To Port
- Application
- Action
- Rule
- Session End Reason
- Bytes
- HTTP/2 Connection Session ID

**Table Data:**

The table contains approximately 20 rows of session logs. Key columns include:

- Type:** All entries are "end".
- From Zone:** L3-TAP.
- Source:** Various IP addresses (e.g., 115.218.106.148, 119.57.91.22, 95.191.44.211, 10.154.216.36).
- Source User:** pancademo\mar...
- Destination:** Various IP addresses (e.g., 10.154.173.98, 10.154.134.133, 10.154.173.238, 198.31.193.211).
- To Port:** Various ports (e.g., 3389, 56383, 8443, 29940, 110, 135, 25874, 80, 443, 80, 80, 80, 80, 80, 80, 80, 80, 80, 80, 80, 80, 80, 80).
- Action:** All entries are "allow".
- Rule:** Various rules (e.g., Allowed Personal Apps, IT Sanctioned SaaS Apps, Required Infrastructure, General Web Infrastructure).
- Session End Reason:** aged-out.
- Bytes:** Values range from 62 to 66k.
- HTTP/2 Connection Session ID:** All values are 0.

**Modal Dialog (Export to CSV):**

- Buttons:** Commit, Manual, All, SESSION END, APP, Export to CSV.
- Fields:** A dropdown menu is set to "All".
- Icons:** Includes icons for commit, manual, search, refresh, and export.

## New Admin features in 10.1

Uncommitted changes now survive a reboot or a power outage.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-new-features/management-features/persistent-uncommitted-changes-on-pan-os.html#id301d640f-10ce-46cf-99d6-900cac2a7e81>

Full admin audit tracking - CLI and GUI

<https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/set-up-panorama/set-up-administrative-access-to-panorama/configure-tracking-of-administrator-activity.html>

Scheduled Commits - The ability to schedule commits to take place at certain times. -  
*This is a Panorama feature.*

# Schedule Commits

Config Push Scheduler

Name  ?

Disabled

Type  One-time schedule  Recurring schedule

Date  ▼

Time  ▼

**Push Scope**

[Device Groups](#) | [Templates](#)

FILTERS		NAME	LAST COMMIT STATE	HA PAIR STATUS	PREVIEW CHANGES
<input type="checkbox"/> Commit State <input type="checkbox"/> Out of Sync (2)		<input checked="" type="checkbox"/> Lab			
<input type="checkbox"/> Device State <input type="checkbox"/> Connected (1) <input type="checkbox"/> Disconnected (1)		<input checked="" type="checkbox"/> PA-851	Out of Sync		
<input type="checkbox"/> Platforms <input type="checkbox"/> PA-220 (1) <input type="checkbox"/> PA-850 (1)		<input type="checkbox"/> New_220			
<input type="checkbox"/> Device Groups <input type="checkbox"/> Lab (1)		<input type="checkbox"/> PA-220	Out of Sync		
<a href="#">Select All</a> <a href="#">Deselect All</a> <a href="#">Expand All</a> <a href="#">Collapse All</a> <input type="checkbox"/> <a href="#">Group HA Peers</a> <input type="checkbox"/> <a href="#">Filter Selected (1)</a>					
<input checked="" type="checkbox"/> <a href="#">Merge with Device Candidate Config</a>		<input checked="" type="checkbox"/> <a href="#">Include Device and Network Templates</a>			

OK Cancel

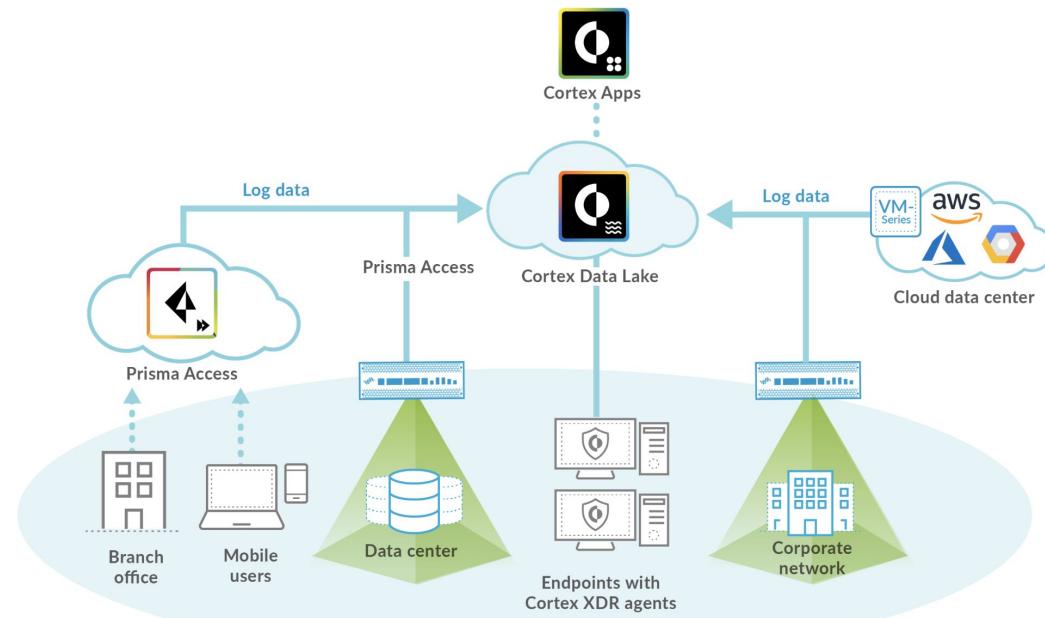
# Cortex Data Lake

All forwarded events are sent to their destination as they are generated on the firewall. A complete discussion of log forwarding configuration is here:

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/configure-log-forwarding.html>

Further information about Cortex Data Lake:

<https://docs.paloaltonetworks.com/cortex/cortex-data-lake/cortex-data-lake-getting-started>



Covered in Session #1.  
-Plan (should be review)

**Interpret log files, reports, and graphs to determine traffic and threat trends**

**Actionable Security Intelligence (read me – I'm important):**

[https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en\\_US/resources/whitepapers/actionable-threat-intelligence](https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/actionable-threat-intelligence)

**Storing Log Filters:**

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-and-manage-reports.html>

**PDF Reports:**

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-and-manage-reports/generate-custom-reports.html>

**User/Group Activity Report**

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-and-manage-reports/generate-usergroup-activity-reports.html>

**PDF Summary Report**

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-and-manage-reports/manage-pdf-summary-reports.html>

**App Scope**

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/use-the-app-scope-reports.html>

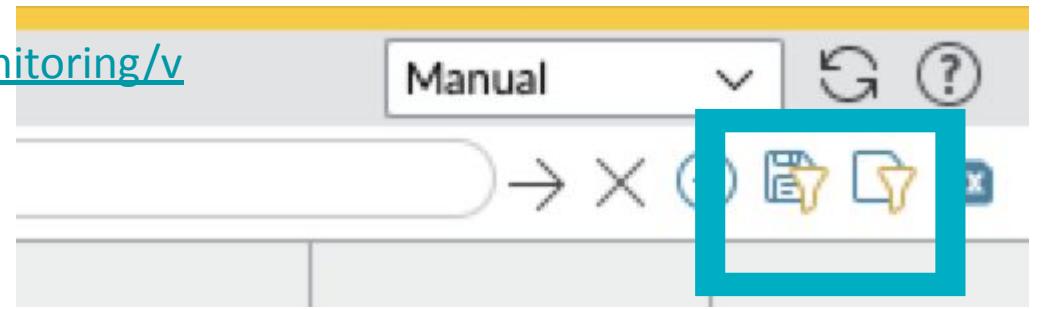
# Select Logging Columns to Display

Logs													
	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE DEVICE OS FAMILY	SOURCE DEVICE HOST	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	Columns >			
<input checked="" type="checkbox"/> Logs	07/13 17:35:49	drop	Public	Clientless	89.248.165.201					<input checked="" type="checkbox"/> Columns >			
<input checked="" type="checkbox"/> Traffic	07/13 17:35:49	end	Amazon	Amazon	169.254.68.186					<input checked="" type="checkbox"/> Adjust Columns			
<input checked="" type="checkbox"/> Threat	07/13 17:35:49	end	Server	Public	10.168.12.181	Windows	00:0c:29:09:93:01	00:0c:29:09:93:...		<input checked="" type="checkbox"/> From Zone			
<input checked="" type="checkbox"/> URL Filtering	07/13 17:35:47	drop	Public	Clientless	89.248.165.201					<input checked="" type="checkbox"/> To Zone			
<input checked="" type="checkbox"/> WildFire Submissions	07/13 17:35:47	end	Public	Public	89.248.165.201					<input checked="" type="checkbox"/> Source			
<input checked="" type="checkbox"/> Data Filtering	07/13 17:35:47	drop	Public	Public	89.248.165.201					<input checked="" type="checkbox"/> Source Device OS Family			
<input checked="" type="checkbox"/> HIP Match	07/13 17:35:47	end	Server	Public	10.168.12.181	Windows	00:0c:29:09:93:01	00:0c:29:09:93:...		<input type="checkbox"/> Source Device Model			
<input checked="" type="checkbox"/> GlobalProtect	07/13 17:35:47	drop	Public	Clientless	89.248.165.201					<input checked="" type="checkbox"/> Source Device Host			
<input checked="" type="checkbox"/> IP-Tag	07/13 17:35:47	end	Public	Public	162.142.125.67					<input checked="" type="checkbox"/> Source User			
<input checked="" type="checkbox"/> User-ID	07/13 17:35:47	drop	Public	Public	10.168.10.45	MacOS	M-C02DP3J8MD6M	14:7d:da:7e:22:... m-c02dp3j8md6m		<input checked="" type="checkbox"/> Source Dynamic Address Group			
<input checked="" type="checkbox"/> Decryption	07/13 17:35:47	end	Home	Public	128.14.209.149					<input checked="" type="checkbox"/> Destination			
<input checked="" type="checkbox"/> Tunnel Inspection	07/13 17:35:47	end	Public	Public	89.248.165.110					<input checked="" type="checkbox"/> Destination Dynamic Address Group			
<input checked="" type="checkbox"/> Configuration	07/13 17:35:47	drop	Public	Public	3.137.139.56					<input checked="" type="checkbox"/> Dynamic User Group			
<input checked="" type="checkbox"/> System	07/13 17:35:47	end	Public	Public	89.248.165.201					<input checked="" type="checkbox"/> To Port			
<input checked="" type="checkbox"/> Alarms	07/13 17:35:47	drop	Public	Public	10.168.12.3	PAN-OS	00:0c:29:0c:3d:49	00:0c:29:0c:3d:4...		<input checked="" type="checkbox"/> Application			
<input checked="" type="checkbox"/> Authentication	07/13 17:35:47	end	Server	Public	18.119.99.152					<input checked="" type="checkbox"/> Action			
<input checked="" type="checkbox"/> Unified	07/13 17:35:47	drop	Public	Public	10.168.12.3	PAN-OS	00:0c:29:0c:3d:49	00:0c:29:0c:3d:4...		<input checked="" type="checkbox"/> Rule			
<input checked="" type="checkbox"/> Packet Capture	07/13 17:35:47	end	Public	Public	10.168.12.3	PAN-OS	00:0c:29:0c:3d:49	00:0c:29:0c:3d:4...		<input checked="" type="checkbox"/> Session End Reason			
<input checked="" type="checkbox"/> App Scope	07/13 17:35:45	drop	Public	Public	10.168.12.3	PAN-OS	00:0c:29:0c:3d:49	00:0c:29:0c:3d:4...		<input checked="" type="checkbox"/> Bytes			
<input checked="" type="checkbox"/> Summary	07/13 17:35:45	end	Server	Public	10.168.12.3	PAN-OS	00:0c:29:0c:3d:49	00:0c:29:0c:3d:4...		<input checked="" type="checkbox"/> HTTP/2 Connection Session ID			
<input checked="" type="checkbox"/> Change Monitor	07/13 17:35:45	end	Public	Public	10.168.12.3	PAN-OS	00:0c:29:0c:3d:49	00:0c:29:0c:3d:4...		<input checked="" type="checkbox"/> SDWAN Site Name			
<input checked="" type="checkbox"/> Threat Monitor	07/13 17:35:45	drop	Public	Public	10.168.12.3	PAN-OS	00:0c:29:0c:3d:49	00:0c:29:0c:3d:4...		<input checked="" type="checkbox"/> App Flap Count			
<input checked="" type="checkbox"/> Threat Map	07/13 17:35:44	end	Server	Public	10.168.12.3	PAN-OS	00:0c:29:0c:3d:49	00:0c:29:0c:3d:4...		<input checked="" type="checkbox"/> SDWAN Policy Name			
<input checked="" type="checkbox"/> Network Monitor	07/13 17:35:44	end	Public	Public	10.168.12.3	PAN-OS	00:0c:29:0c:3d:49	00:0c:29:0c:3d:4...		<input type="checkbox"/> Action Source			
<input checked="" type="checkbox"/> Traffic Map	07/13 17:35:44	end	Server	Public	10.168.12.3	PAN-OS	00:0c:29:0c:3d:49	00:0c:29:0c:3d:4...		<input type="checkbox"/> App Category			
<input checked="" type="checkbox"/> Session Browser	07/13 17:35:44	end	Server	Public	10.168.12.3	PAN-OS	00:0c:29:0c:3d:49	00:0c:29:0c:3d:4...		<input type="checkbox"/> App Characteristic			
<input checked="" type="checkbox"/> Botnet	07/13 17:35:44	end	Server	Public	10.168.12.3	PAN-OS	00:0c:29:0c:3d:49	00:0c:29:0c:3d:4...		<input checked="" type="checkbox"/> App Container			
<input checked="" type="checkbox"/> PDF Reports	07/13 17:35:43	end	Server	Public	10.168.12.181	Windows	00:0c:29:09:93:01	00:0c:29:09:93:...		<input type="checkbox"/> App Risk			
<input checked="" type="checkbox"/> Manage PDF Summary	07/13 17:35:43	drop	Public	Public	89.248.165.201					<input type="checkbox"/> App SaaS			
<input checked="" type="checkbox"/> User Activity Report	07/13 17:35:43	drop	Public	Clientless	89.248.165.201					<input type="checkbox"/> App Sanctioned State			
<input checked="" type="checkbox"/> SaaS Application Usage	07/13 17:35:43	drop	Public	Public	45.134.26.45					<input type="checkbox"/> App Subcategory			
<input checked="" type="checkbox"/> Report Groups	07/13 17:35:43	drop	Public	Public						<input type="checkbox"/> App Technology			

# Log Filtering

Filters can be built and even stored for future use.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-and-manage-logs.html>



The screenshot shows a list of logs under the 'Traffic' tab. A search bar at the top of the table has the same filter as the search bar above: '(addr.src in 10.168.10.59) and (port.dst eq 443)'. The table has columns: RECEIVE TIME, TYPE, ZONE, TO ZONE, SOURCE, OS FAMILY, HOST, SOURCE USER, SOURCE DYNAMIC ADDRESS GROUP, DESTINATION, DESTINATION DYNAMIC ADDRESS GROUP, DYNAMIC USER GROUP, TO PORT, and APPLICATION. There are 10 rows of log entries, all showing traffic from source 10.168.10.59 to destination 10.168.12.2 via server 'ubuntu\_server' on port 443, with source user '00:0c:29:d8:ce:af-ubuntu\_server'. The 'Save Filter' and 'Load Filter' buttons are located to the right of the table.

	RECEIVE TIME	TYPE	ZONE	TO ZONE	SOURCE	OS FAMILY	HOST	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION
URL Filtering	07/13 17:47:21	end	Home	Server	10.168.10.59		ubuntu_server	00:0c:29:d8:ce:af-ubuntu_server		10.168.12.2			443	ssl
WildFire Submissions	07/13 17:47:21	end	Home	Server	10.168.10.59		ubuntu_server	00:0c:29:d8:ce:af-ubuntu_server		10.168.12.2			443	ssl
Data Filtering	07/13 17:47:16	end	Home	Server	10.168.10.59		ubuntu_server	00:0c:29:d8:ce:af-ubuntu_server		10.168.12.2			443	ssl
HIP Match	07/13 17:46:21	end	Home	Server	10.168.10.59		ubuntu_server	00:0c:29:d8:ce:af-ubuntu_server		10.168.12.2			443	ssl
GlobalProtect	07/13 17:46:21	end	Home	Server	10.168.10.59		ubuntu_server	00:0c:29:d8:ce:af-ubuntu_server		10.168.12.2			443	ssl
IP-Tag	07/13 17:46:21	end	Home	Server	10.168.10.59		ubuntu_server	00:0c:29:d8:ce:af-ubuntu_server		10.168.12.2			443	ssl
User-ID	07/13 17:45:21	end	Home	Server	10.168.10.59		ubuntu_server	00:0c:29:d8:ce:af-ubuntu_server		10.168.12.2			443	ssl
Decryption	07/13 17:45:21	end	Home	Server	10.168.10.59		ubuntu_server	00:0c:29:d8:ce:af-ubuntu_server		10.168.12.2			443	ssl
Tunnel Inspection	07/13 17:45:21	end	Home	Server	10.168.10.59		ubuntu_server	00:0c:29:d8:ce:af-ubuntu_server		10.168.12.2			443	ssl
Configuration	07/13 17:45:21	end	Home	Server	10.168.10.59		ubuntu_server	00:0c:29:d8:ce:af-ubuntu_server		10.168.12.2			443	ssl
System	07/13 17:45:21	end	Home	Server	10.168.10.59		ubuntu_server	00:0c:29:d8:ce:af-ubuntu_server		10.168.12.2			443	ssl
Alarms	07/13 17:45:21	end	Home	Server	10.168.10.59		ubuntu_server	00:0c:29:d8:ce:af-ubuntu_server		10.168.12.2			443	ssl
Authentication	07/13 17:45:21	end	Home	Server	10.168.10.59		ubuntu_server	00:0c:29:d8:ce:af-ubuntu_server		10.168.12.2			443	ssl
Unified	07/13 17:45:21	end	Home	Server	10.168.10.59		ubuntu_server	00:0c:29:d8:ce:af-ubuntu_server		10.168.12.2			443	ssl
Packet Capture	07/13 17:45:21	end	Home	Server	10.168.10.59		ubuntu_server	00:0c:29:d8:ce:af-ubuntu_server		10.168.12.2			443	ssl
App Scope	07/13 17:45:21	end	Home	Server	10.168.10.59		ubuntu_server	00:0c:29:d8:ce:af-ubuntu_server		10.168.12.2			443	ssl
Summary	07/13 17:45:21	end	Home	Server	10.168.10.59		ubuntu_server	00:0c:29:d8:ce:af-ubuntu_server		10.168.12.2			443	ssl
Change Monitor	07/13 17:44:20	end	Home	Server	10.168.10.59		ubuntu_server	00:0c:29:d8:ce:af-ubuntu_server		10.168.12.2			443	ssl
Threat Monitor														

# How Data Populates the ACC

**Logging and Reporting Settings**

Log Storage | **Log Export and Reporting** | Pre-Defined Reports | Log Collector Status

Number of Versions for Config Audit	100
Max Rows in CSV Export	65535
Max Rows in User Activity Report	5000
Average Browse Time (sec)	60
Page Load Threshold (sec)	20
Syslog HOSTNAME Format	FQDN
Report Runtime	02:00
Report Expiration Period (days)	[1 - 2000]

Warning: Deletion of logs based on time period may take a long time and during this time the max sustainable log rate will be degraded

**OK**    **Cancel**

**Logging and Reporting Settings**

Storage | Log Export and Reporting | Pre-Defined Reports | Log Collector Status

**Storage Quota**

	Quota(%)	Quota(GB/MB)	Max Days
Traffic	25.395	42.35 GB	[1 - 2000]
Threat	12	20.01 GB	[1 - 2000]
Config	4	6.67 GB	[1 - 2000]
System	4	6.67 GB	[1 - 2000]
Alarm	3	5.00 GB	[1 - 2000]
App Stats	4	6.67 GB	[1 - 2000]
HIP Match	3	5.00 GB	[1 - 2000]
GlobalProtect	1	1.67 GB	[1 - 2000]
App Pcaps	1.5	2.50 GB	[1 - 2000]
Deleted Threat Pcaps	1	1.67 GB	[1 - 2000]
Decompression Filter Pcaps	1.5	2.50 GB	[1 - 2000]
IP-Tag	1	1.67 GB	[1 - 2000]
User-ID	1	1.67 GB	[1 - 2000]
HIP Reports	1.5	2.50 GB	[1 - 2000]
Data Filtering Captures	1.5	2.50 GB	[1 - 2000]
GTP and Tunnel	2	3.34 GB	[1 - 2000]
Authentication	1	1.67 GB	[1 - 2000]
Decryption	1	1.67 GB	[1 - 2000]

Total Allocated: 92.39% (154.08 GB)  
 Unallocated: 7.61% (12.68 GB)  
 Max: 166.76 GB  
 Core Files: 0 MB

Restore Defaults

Warning: Deletion of logs based on time period may take a long time and during this time the max sustainable log rate will be degraded

**OK**    **Cancel**

# PDF Reports

APPLICATION NAME	BYTES	SESSIONS
1 dns	14.7M	52.5k
2 web-browsing	2.2G	18.7k
3 ssl	5.5G	18.6k
4 ping	1.5M	7.5k
5 ntp	616.2k	3.4k
6 google-base	110.3M	2.7k
7 insufficient-data	3.2M	2.7k
8 syslog	2.6M	2.2k
9 icloud-base	203.2M	2.1k
10 ocsp	6.9M	1.8k
11 icloud-mail	72.4M	1.1k
12 paloalto-iot-security	108.4M	802
13 paloalto-shared-services	310.1M	767
14 paloalto-updates	453.9M	761
15 paloalto-wildfire-cloud	13.0M	728
16 zoom-base	19.9M	546
17 itunes-base	17.9M	526
18 apple-maps	17.7M	429
19 gmail-base	22.3M	298
20 unknown-tcp	2.6M	262
21 sip	100.8k	223
22 youtube-base	400.1M	190

Know the Main Categories

- Application
- Traffic
- Threat
- URL Filtering
- PDF Summary

## Custom Reports:

## User/Group Activity Report

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-and-manage-reports/generate-custom-reports.html>

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-and-manage-reports/generate-usergroup-activity-reports.html>

# PDF Summary Report

## PDF Summary Report

Name



Threat Reports Application Reports Trend Reports Traffic Reports URL Filtering Reports

Top users X

Top attackers by destination countries X

Top vulnerabilities X

Top attacker sources X

Top victims by source countries X

High risk user - Top applications X

Top attacker destinations X

Top victims by destination countries X

High risk user - Top threats X

Top victim sources X

Top threats X

High risk user - Top URL categories X

Top victim destinations X

Top spyware threats X

Top application categories (Pie Chart) X

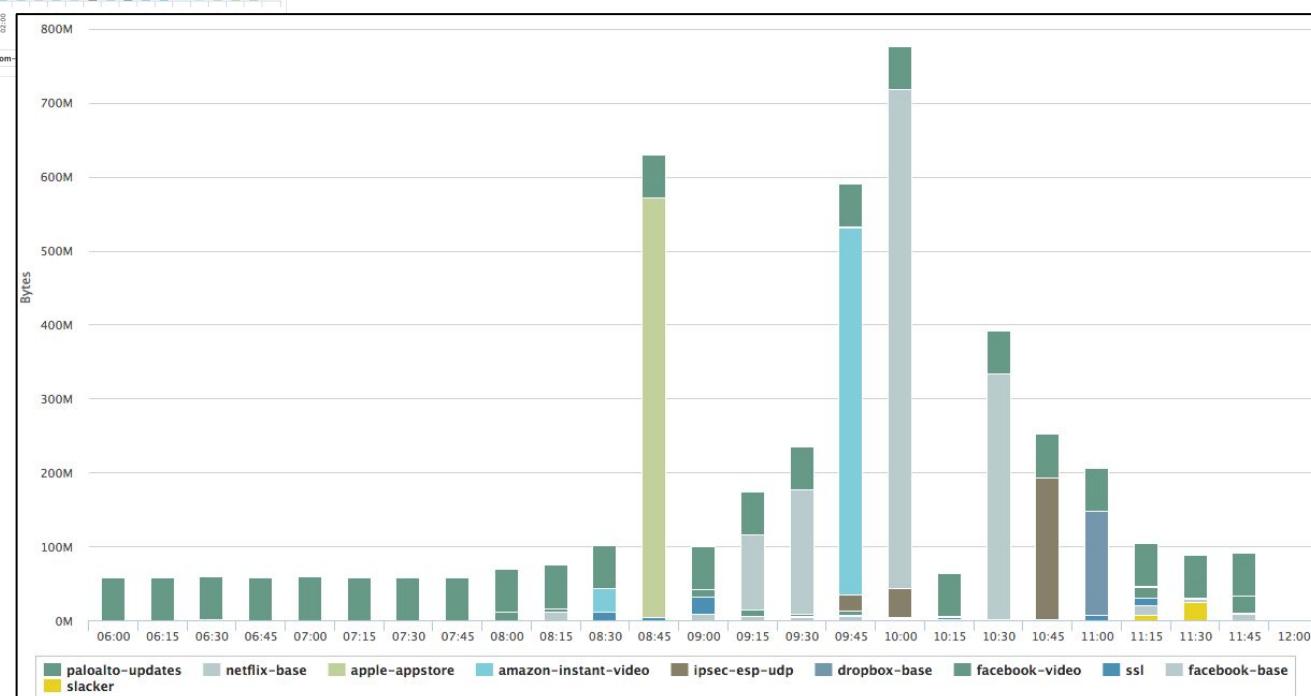
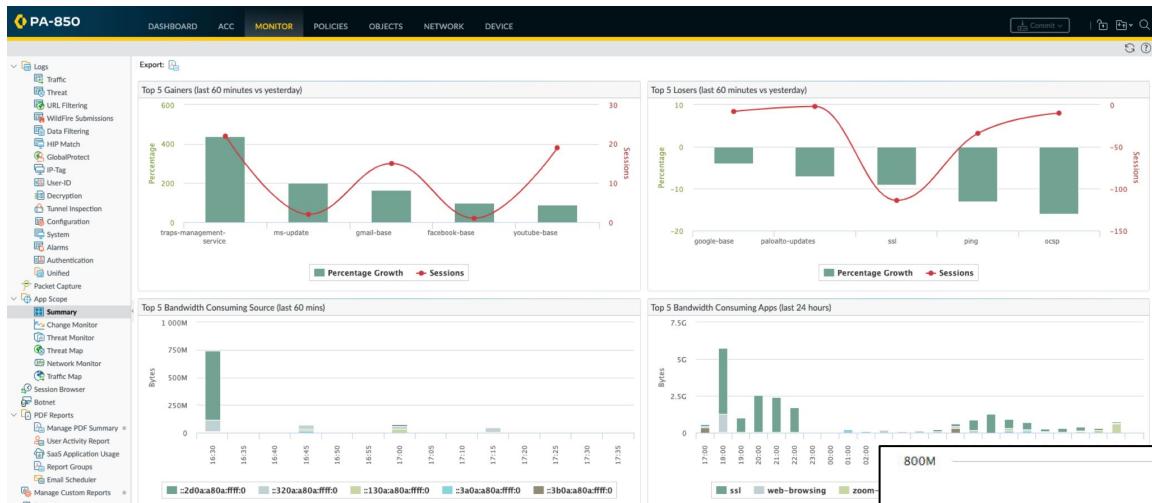
OK

Cancel

## PDF Summary Report :

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-and-manage-reports/manage-pdf-summary-reports.html>

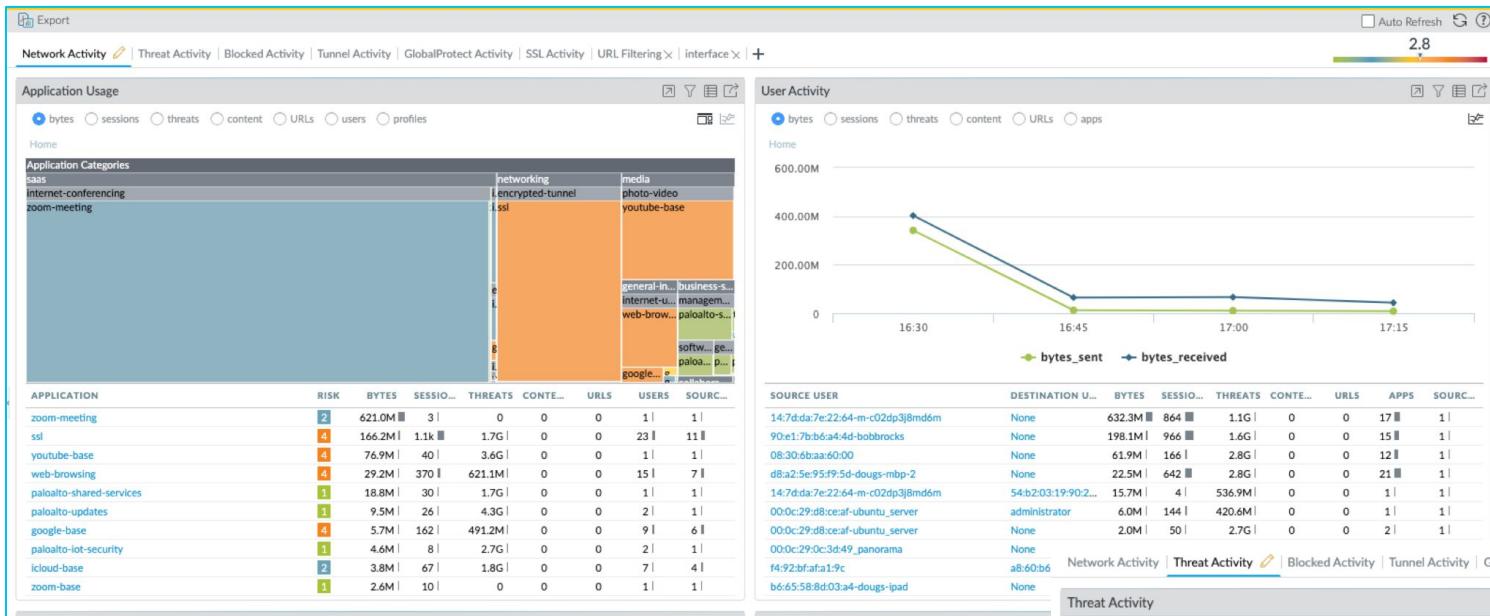
# App Scope



## App Scope Reports:

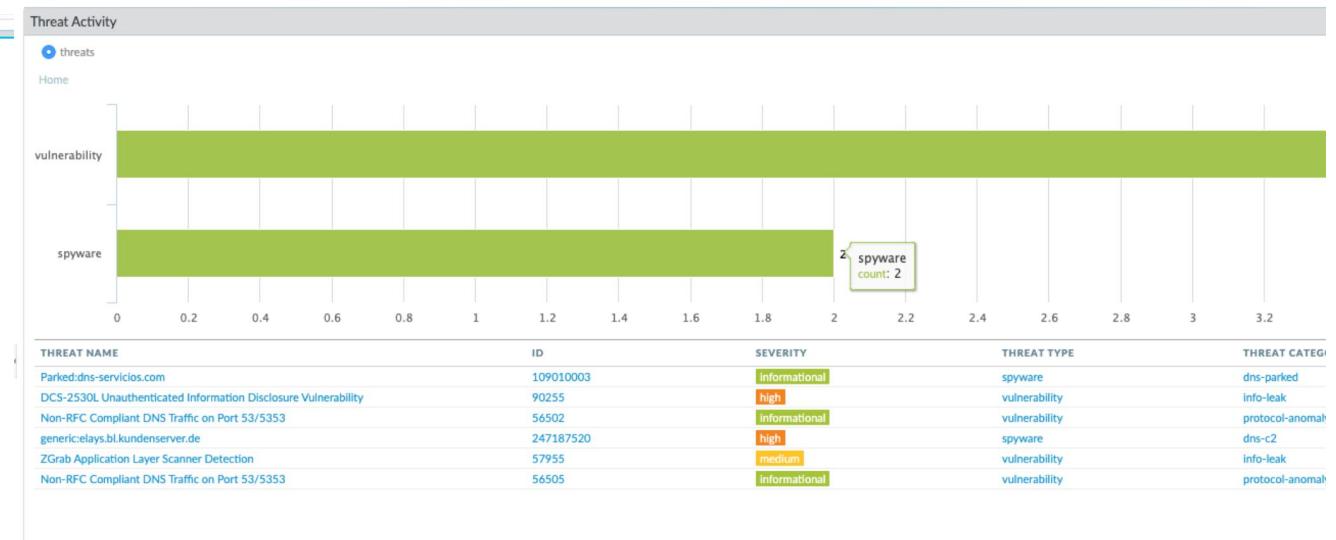
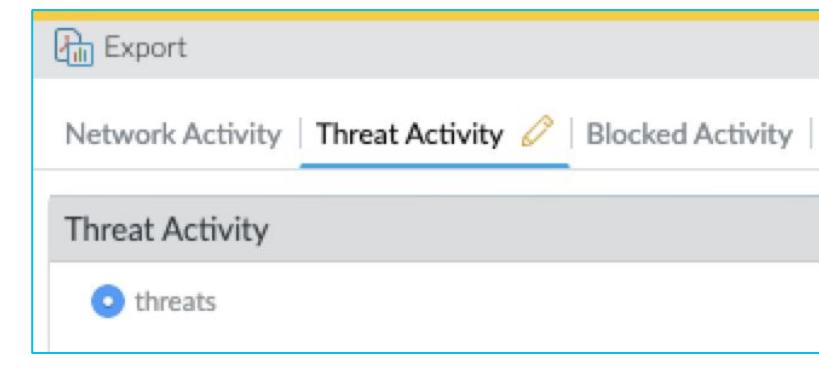
<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/use-the-app-scope-reports.html>

# Application Command Center (ACC)



## Application Command Center:

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/use-the-application-command-center.html>



# Automated Correlation Engine - Panorama Only!

Monitor -> Automated Correlation Engine -> Correlation Objects

Screenshot of the Palo Alto Networks PANORAMA interface showing the 'Correlation Objects' section under 'Automated Correlation Engine'.

The left sidebar shows navigation categories: Logs, External Logs, Automated Correlation Engine (selected), and App Scope.

The main table lists correlation objects:

TITLE	CATEGORY	STATE	DESCRIPTION
Multiple User from One Endpoint MFA Credential Theft	credential-theft-abuse	active	This correlation object detects multiple account abuse from a possibly compromised endpoint
WildFire C2	compromised-host	active	This correlation object detects hosts that have exhibited command-and-control (C2) network behavior corresponding to malware detected by WildFire elsewhere on your network.
WildFire and Traps ESM Correlated C2	compromised-host	active	This correlation object detects hosts that have received malware detected by WildFire or executed malware as seen by Traps, and have also exhibited command- and control (C2) network behavior corresponding to the detected malware.
Single Account and Endpoint MFA Credential Theft	credential-theft-abuse	active	This correlation object detects activity from a possibly compromised user account from a single endpoint
Compromise Activity Sequence	compromised-host	active	This correlation object detects a host involved in a sequence of activity indicating remote compromise, starting with scanning or probing activity, progressing exploitation, and concluding with network contact to a known malicious domain.
Exploit Kit Activity	compromised-host	active	This object detects probable exploit kit activity targeted at a host on the network. Exploit kits are identified by a vulnerability exploit or exploit kit landing page signature, combined with either a malware download signature or a known command-and-control signature.
Single Account 1 FA Multiple Endpoints Credential Timeouts	credential-theft-abuse	active	This correlation object detects timed out attempts of first factor authentications from multiple endpoints using a single user account
Beacon Detection	compromised-host	active	This correlation object detects likely compromised hosts based on activity that resembles command-and-control (C2) beaconing, such as repeated visits to recently registered domains or dynamic DNS domains, repeated file downloads from the same location, generation of unknown traffic, etc.
Single Account and Endpoint MFA Credential Timeout	credential-theft-abuse	active	This correlation object detects timeout MFA authentication attempts from a single endpoint using single account
Multiple Endpoint MFA Credential Timeout Abuse	credential-theft-abuse	active	This correlation object detects timed out second factor authentications from multiple endpoints using a single user account
Multiple Endpoint MFA Credential Abuse	credential-theft-abuse	active	This correlation object detects activity from multiple endpoints using a single user account
Exploit Kit Delivering XOR obfuscated malware	compromised-host	active	This correlation object detects exclusive-or (XOR) obfuscated malware downloaded to a host. XOR obfuscation is a technique to evade detection by encrypting portions of a file in order to hide malicious code. This correlation object specifically identifies XOR obfuscated malware that is delivered to the host by an exploit kit. While the Exploit Kit Activity object detects exploit kits combined with either a malware download signature or a known command-and-control signature, this object is provided to specifically detect an event where XOR obfuscation malware inserted on a host by an exploit kit and to distinguish such an event from other exploit kit activities.
Single Account 1 FA Credential Abuse	credential-theft-abuse	active	This correlation object detects timed out first factor authentications from an endpoint using a single user account

## Automated Correlation Engine:

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/use-the-automated-correlation-engine.html>



## 4.1.4 Identify system and traffic issues using the web interface and CLI tools.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-cli-quick-start>

show system info

show session info

show session id <session-id>

request license info

request system restart

show routing route

ping src X host X (good if you use service routes and vsys)

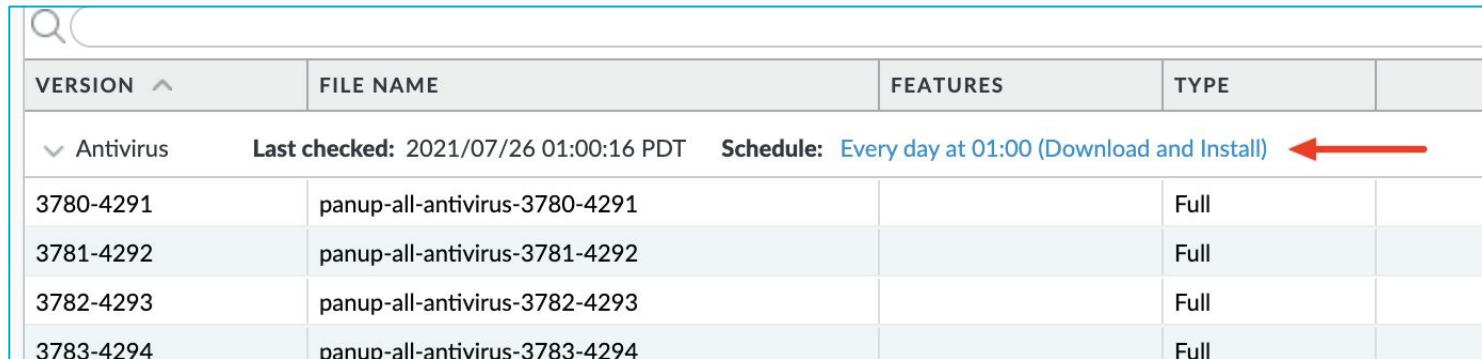
admin@PA-851> request content upgrade info						
Version	Size	Released on	Downloaded	Installed		
8425-6795	63MB	2021/07/02 11:10:33 PDT		no		no
8434-6840	63MB	2021/07/22 23:18:20 PDT		yes	current	
8432-6829	63MB	2021/07/19 21:42:04 PDT		no		no
8427-6806	63MB	2021/07/07 19:13:47 PDT		no		no
8429-6810	63MB	2021/07/12 16:00:17 PDT		no		no
8430-6813	63MB	2021/07/13 10:01:41 PDT		no		no
8423-6789	63MB	2021/06/29 16:05:46 PDT		no		no
8428-6809	63MB	2021/07/09 16:49:07 PDT		no		no
8422-6787	63MB	2021/06/28 17:11:31 PDT		no		no
8426-6800	63MB	2021/07/06 21:54:37 PDT		no		no
8424-6793	63MB	2021/07/01 10:24:06 PDT		no		no
8433-6838	63MB	2021/07/22 15:36:06 PDT		yes	previous	
8431-6821	63MB	2021/07/16 17:25:01 PDT		no		no

## **4.2 Plan & Execute the Process to Update a Palo Alto Networks System**

## 4.2.1 Update a Single Firewall

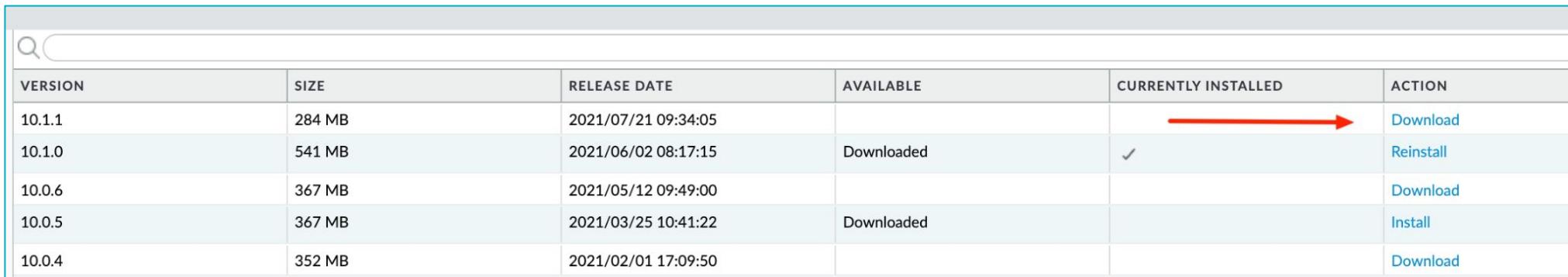
- Focuses on Dynamic Updates and Software Updates

- Dynamic Updates



VERSION	FILE NAME	FEATURES	TYPE
▼ Antivirus	Last checked: 2021/07/26 01:00:16 PDT   Schedule: Every day at 01:00 (Download and Install)		
3780-4291	panup-all-antivirus-3780-4291		Full
3781-4292	panup-all-antivirus-3781-4292		Full
3782-4293	panup-all-antivirus-3782-4293		Full
3783-4294	panup-all-antivirus-3783-4294		Full

- Software Updates



VERSION	SIZE	RELEASE DATE	AVAILABLE	CURRENTLY INSTALLED	ACTION
10.1.1	284 MB	2021/07/21 09:34:05			→ Download
10.1.0	541 MB	2021/06/02 08:17:15	Downloaded	✓	→ Reinstall
10.0.6	367 MB	2021/05/12 09:49:00			→ Download
10.0.5	367 MB	2021/03/25 10:41:22	Downloaded		→ Install
10.0.4	352 MB	2021/02/01 17:09:50			→ Download

## 4.2.1 Updating Palo Alto Firewalls - Preupgrade checklist

- Review release notes.
- Do not schedule Panorama and firewall upgrades at the same time.
- Upgrade Panorama first, wait at least 24 hours and then upgrade the firewall.
- Upgrade should be carried out during non-business hours or a scheduled maintenance window to minimize impact.
- Allocate sufficient time in the change window for upgrade, troubleshooting and possible downgrade procedures. It may take up to 2-3 hours to upgrade a slower or older system, depending on config. Multiply if upgrading across multiple versions.
- Have a robust pre and post test plan
- Backup configuration and device state before upgrade.

# Steps for Upgrading Single Firewall

Step 1: Backup Configuration

Step 2: Look at User-ID since the reboot will repopulate the User-ID

- For IP address-to-username mappings:

```
show user user-id-agent state all
```

```
show user server-monitor state all
```

- For group mappings: show user group-mapping statistics

Step 3: Ensure the latest content release (or min for version upgrading to)

Step 4: Determine Upgrade Path

Step 5: Upgrade (Download and Install the version)

## 4.2.2 Update HA pairs.

- Dynamic Updates
  - This task can be difficult if dynamic updates have no network path to the Palo Alto Networks update servers.
  - Dynamic updates in HA clusters include an option to “Sync-to-peer” for use when the secondary firewall has no network route to the update
- HA Upgrades
  - Firewalls in HA pairs or clusters must upgrade PAN-OS software individually.
  - In active/passive HA pairs, a firewall typically is put into suspend mode and then upgraded.
  - After the upgrade is complete, the firewall is made active, and the partner enters suspend mode and is upgraded.



Know the Steps

# Upgrading Versions

For instance - if you are running version 9.0.10 and want to upgrade to 10.1.1, how would you do it?

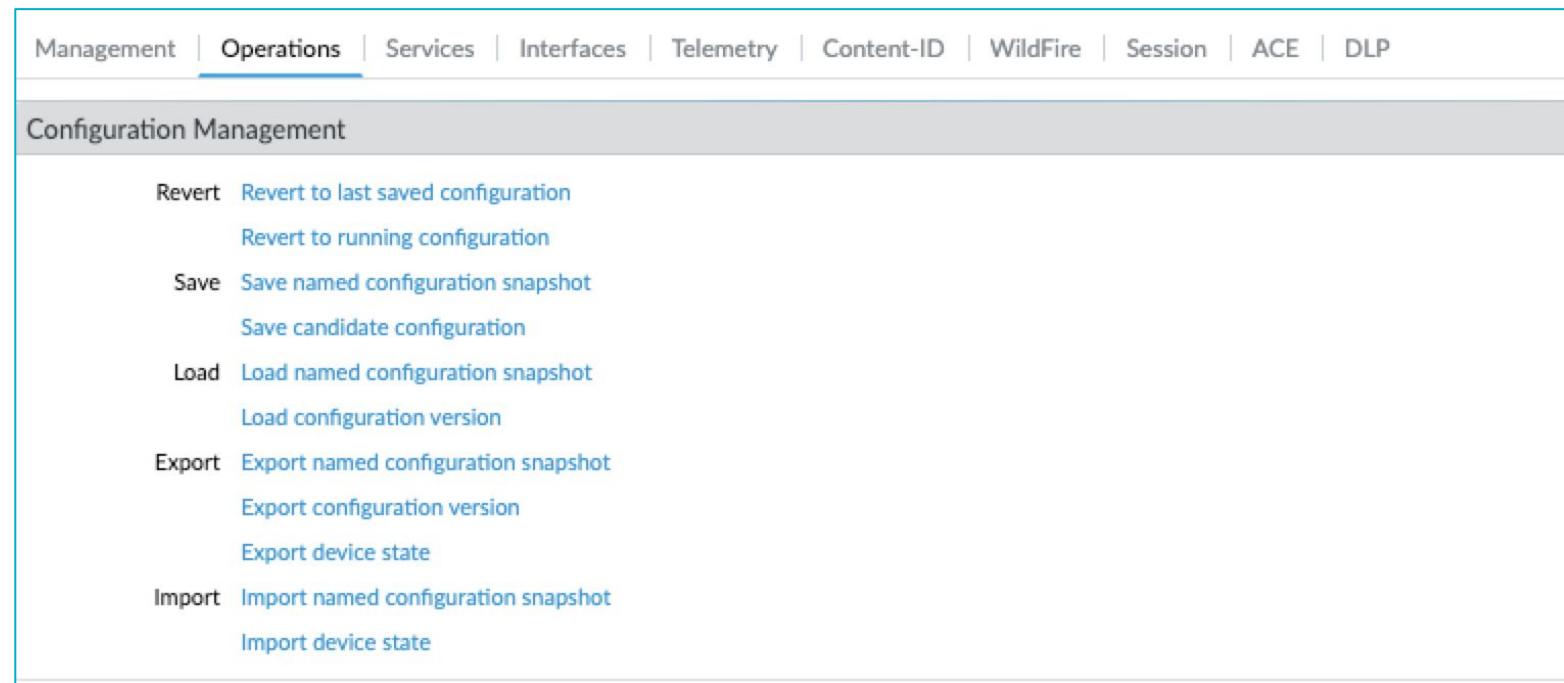
- Download 9.1.0
- Download and install the *preferred* release of 9.1.x
- Reboot
- Download 10.0
- Download and install the *preferred* release of 10.0.x
- Reboot
- Download 10.1.0
- Download and install the *preferred* release of 10.1.x

VERSION	SIZE	RELEASE DATE
10.1.1	297 MB	2021/07/21 09:33:46
10.1.0	917 MB	2021/06/02 08:16:22
10.0.6	441 MB	2021/05/12 09:48:56
10.0.5	440 MB	2021/03/25 10:41:47
10.0.4	431 MB	2021/02/01 17:09:54
10.0.3	431 MB	2020/12/09 18:53:33
10.0.3-c45	431 MB	2020/11/10 08:27:14
10.0.3-c31	430 MB	2020/10/23 14:02:44
10.0.2-c46	382 MB	2020/10/05 10:13:51
10.0.1	332 MB	2020/09/03 09:32:34
10.0.0	806 MB	2020/07/16 20:15:10
9.1.10	398 MB	2021/06/10 11:28:23
9.1.9	397 MB	2021/04/08 15:09:20

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-upgrade/upgrade-pan-os/upgrade-the-firewall-pan-os/determine-the-upgrade-path.html>

# Config Files to grab

- Device > Setup > Operations > Save Named Configuration Snapshot
- Device > Setup > Operations > Export Named Configuration Snapshot
- Device > Setup > Operations > Export Device State
- Device > Support > Generate Tech Support File



<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRcCAK>

**Identify the relationship between Panorama and devices as it pertains to dynamic updates versions and policy implementation and/or HA peers.**

The screenshot shows the Panorama dashboard with the 'PANORAMA' tab selected. On the left, a sidebar lists various cloud services, AWS components, SD-WAN, DLP, Google Cloud Platform, and security tools like IPS Signature Converter and Zero Touch Provisioning. The main pane displays two sections of device updates:

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE
Antivirus Last checked: 2021/07/13 17:18:03 PDT						
3768-4279	panup-all-antivirus-3768-4279		Full	98 MB	a9bf032938143e...	2021/07/05 06:17:00 PDT
3769-4280	panup-all-antivirus-3769-4280		Full	98 MB	c592d2d7ac7b07...	2021/07/06 06:30:37 PDT
3770-4281	panup-all-antivirus-3770-4281		Full	99 MB	69af5c11b19506a...	2021/07/07 07:06:27 PDT
3771-4282	panup-all-antivirus-3771-4282		Full	100 MB	6edfdb56583882...	2021/07/08 08:03:24 PDT
3772-4283	panup-all-antivirus-3772-4283		Full	100 MB	9e0c74595ac157...	2021/07/09 07:30:53 PDT
3773-4284	panup-all-antivirus-3773-4284		Full	100 MB	66c47cee27df8fc...	2021/07/10 08:16:15 PDT
3774-4285	panup-all-antivirus-3774-4285		Full	100 MB	a99ad95a728676...	2021/07/12 12:51:33 PDT
3775-4286	panup-all-antivirus-3775-4286		Full	99 MB	20e943298073b0...	2021/07/12 12:02:12 PDT
3776-4287	panup-all-antivirus-3776-4287		Full	99 MB	571b0fc4cdc4583...	2021/07/13 09:47:10 PDT
Applications and Threats Last checked: 2021/07/13 17:05:05 PDT						
8417-6756	panupv2-all-contents-8417-6756	Contents	Full	63 MB	4e82e11d45cb81...	2021/06/14 18:36:04 PDT
8417-6756	panupv2-all-apps-8417-6756	Apps	Full	53 MB	b8d1e13c546fea4...	2021/06/14 18:35:44 PDT
8418-6771	panupv2-all-contents-8418-6771	Contents	Full	63 MB	fc86e676290390...	2021/06/16 17:48:51 PDT
8418-6771	panupv2-all-apps-8418-6771	Apps	Full	54 MB	4bff548c095fec5b...	2021/06/16 17:49:28 PDT
8419-6773	panupv2-all-contents-8419-6773	Contents	Full	63 MB	ad24a3acd53adc4...	2021/06/18 20:47:32 PDT
8419-6773	panupv2-all-apps-8419-6773	Apps	Full	54 MB	6d6b930b104920...	2021/06/18 20:47:15 PDT
8420-6777	panupv2-all-contents-8420-6777	Contents	Full	63 MB	631ee9dd5f6ddb...	2021/06/22 18:51:08 PDT
8420-6777	panupv2-all-apps-8420-6777	Apps	Full	54 MB	7d1a57f60c01d29...	2021/06/22 18:51:26 PDT
R421-A7R1	panupv2-all-contents-R421-A7R1	Contents	Full	63 MB	d5a19frfrff935he...	2021/06/24 18:52:42 PDT

See previous sections

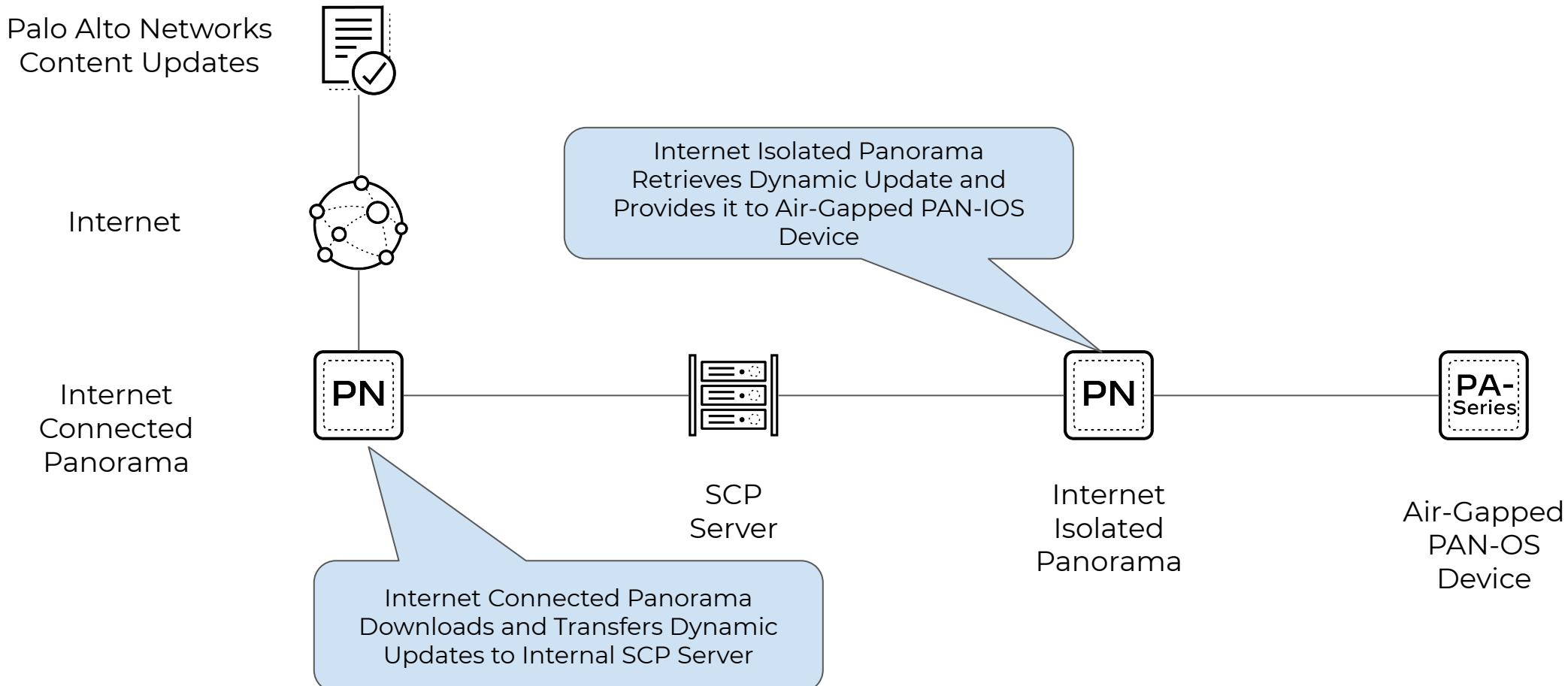
## Deploy Upgrades to Firewalls, Log Collectors, and WildFire Appliances Using Panorama

<https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-licenses-and-updates/deploy-updates-to-firewalls-log-collectors-and-wildfire-appliances-using-panorama.html>

## 4.2.3 Perform Panorama (Content) Push

### Automatic Content Updates Through Offline Panorama

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/panorama-features/automatic-content-updates-through-offline-panorama.html>



## 4.2.4 Schedule & Manage Dynamic Updates

PANORAMA

DASHBOARD ACC MONITOR POLICIES Device Groups OBJECTS NETWORK DEVICE PANORAMA

Commit ▾ | ↗ Tasks | Language | **paloalto**  
Panorama

User Identification Data Redistribution Scheduled Config Push Device Quarantine Managed Devices Summary Health Troubleshooting Templates Device Groups Managed Collectors Collector Groups Certificate Management Certificates Certificate Profile SSL/TLS Service Profile SCEP SSH Service Profile Log Ingestion Profile Log Settings Server Profiles SNMP Trap Syslog Email HTTP RADIUS SCP TACACS+ LDAP Kerberos SAML Identity Provider Scheduled Config Export Software Dynamic Updates Plugins SD-WAN

Check Now Upload Install From File Revert Content Schedules

VERSION ▾ FILE NAME FEATURES TYPE SIZE SHA256 RELEASE DATE DOWNLOADED ACTION DOCUMENTATION

Last checked: 2021/09/15 00:45:30 PDT

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOADED	ACTION	DOCUMENTATION
3831-4342	panup-all-antivirus-3831-4342		Full	88 MB	c22e22273aab83...	2021/09/06 04:04:25 PDT		Download	Release Notes
3832-4343	panup-all-antivirus-3832-4343		Full	88 MB	6e15e4a676e204...	2021/09/07 04:04:09 PDT		Download	Release Notes
3833-4344	panup-all-antivirus-3833-4344		Full	88 MB	6e15e4a676e204...	2021/09/07 04:04:09 PDT		Download	Release Notes
3835-4346	panup-all-antivirus-3835-4346		Full	88 MB	6e15e4a676e204...	2021/09/07 04:04:09 PDT		Install	Release Notes
3836-4347	panup-all-antivirus-3836-4347		Full	88 MB	6e15e4a676e204...	2021/09/07 04:04:09 PDT		Install	Release Notes
3837-4348	panup-all-antivirus-3837-4348		Full	88 MB	6e15e4a676e204...	2021/09/07 04:04:09 PDT		Install	Release Notes
3838-4349	panup-all-antivirus-3838-4349		Full	88 MB	6e15e4a676e204...	2021/09/07 04:04:09 PDT		Install	Release Notes
3839-4350	panup-all-antivirus-3839-4350		Full	88 MB	6e15e4a676e204...	2021/09/07 04:04:09 PDT		Install	Release Notes
Applications and Threats									
8446-6886	panupv2-all-apps-8446-6886		Download and Install	PA-220 vm-300-edge		Daily 00:00		Download	Release Notes
8446-6886	panupv2-all-apps-8446-6886		Download and Install	PA-220 vm-300-edge		Every-min		Download	Release Notes
8447-6897	panupv2-all-apps-8447-6897		Download and Install	PA-220 vm-300-edge		Daily 00:45		Download	Release Notes
8447-6897	panupv2-all-apps-8447-6897		Download and Install	PA-220 vm-300-edge		Daily 00:45		Download	Release Notes
8448-6902	panupv2-all-apps-8448-6902		Download and Install	PA-220 vm-300-edge		Daily 00:45		Download	Release Notes
8448-6902	panupv2-all-apps-8448-6902		Download and Install	PA-220 vm-300-edge		Daily 00:45		Download	Release Notes
8449-6906	panupv2-all-apps-8449-6906		Download and Install	PA-220 vm-300-edge		Daily 00:45		Download	Release Notes
8449-6906	panupv2-all-apps-8449-6906		Download and Install	PA-220 vm-300-edge		Daily 00:45		Download	Release Notes
8450-6909	panupv2-all-apps-8450-6909	Apps	Full	43 MB	400233f0d01bb...	2021/08/26 19:45:39 PDT		Download	Release Notes
8451-6911	panupv2-all-contents-8451-6911	Contents	Full	46 MB	e1a506c5aa6d10...	2021/08/30 17:55:46 PDT		Download	Release Notes
8451-6911	panupv2-all-apps-8451-6911	Apps	Full	43 MB	0dbc1a5583321...	2021/08/30 17:56:00 PDT		Download	Release Notes
8452-6913	panupv2-all-apps-8452-6913	Apps	Full	43 MB	32e3692e1e227...	2021/08/31 18:53:43 PDT		Download	Release Notes
8453-6919	panupv2-all-contents-8453-6919	Contents	Full	46 MB	56280ffaadacbb1...	2021/09/02 19:02:37 PDT	✓	Install	Release Notes
8453-6919	panupv2-all-apps-8453-6919	Apps	Full	43 MB	bb4b347b60ad0...	2021/09/02 19:02:22 PDT		Download	Release Notes
8454-6927	panupv2-all-contents-8454-6927	Contents	Full	46 MB	3bc305d47608bf...	2021/09/08 22:41:46 PDT	✓	Install	Release Notes

Schedules

NAME TYPE ENABLED ACTION DEVICES LOG COLLECTORS RECURRENCE START TIME

- App and threat app-and-threat Enabled Download and Install PA-220  
vm-300-edge Daily 00:00
- Wildfire wildfire Enabled Download and Install PA-220  
vm-300-edge Every-min
- Anti Virus anti-virus Enabled Download and Install PA-220  
vm-300-edge Daily 00:45

+ Add - Delete Close

## 4.2.5 Schedule & Manage Dynamic Software Updates

The screenshot shows the PANORAMA software interface. On the left, there is a navigation sidebar with various options like Data Redistribution, Device Quarantine, Managed Devices, Templates, Device Groups, Managed Collectors, Collector Groups, Certificate Management, Log Ingestion Profile, Log Settings, Server Profiles, Software, Dynamic Updates, Plugins, SD-WAN, Cisco ACL, DLP, Zero Touch Provisioning, IPS Signature Converter, Cloud Services, Google Cloud Platform, AWS, VMware, VMware vCenter, Interconnect, Azure, Licenses, Support, Device Deployment, Master Key and Diagnostics, and Policy Recommendation. The 'Dynamic Updates' option is highlighted with a red box. The main pane displays a table of software updates with columns: VERSION, FILE NAME, FEATURES, TYPE, SIZE, SHA256, RELEASE DATE, DOWNLOADED, CURRENTLY INSTALLED, ACTION, and DOCUMENTATION. A modal window titled 'Applications and Threats Update Schedule' is open over the table, showing settings for a weekly schedule on Wednesday at 01:02. It includes fields for Recurrence (Weekly), Day (Wednesday), Time (01:02), Action (download-and-install), Threshold (hours) [1 - 336], and Allow Extra Time to Review New App-IDs (New App-ID Threshold [1 - 336]). Buttons for Delete Schedule, OK, and Cancel are at the bottom of the modal.

The screenshot shows the PANORAMA software interface with a sidebar on the right. The sidebar has a tree view with categories: Managed Collectors, Collector Groups, Certificate Management, Log Ingestion Profile, Log Settings, Server Profiles, Software, Dynamic Updates, Plugins, SD-WAN, Cisco ACL, DLP, Zero Touch Provisioning, IPS Signature Converter, Cloud Services, Google Cloud Platform, AWS, VMware, VMware vCenter, Interconnect, Azure, Licenses, Support, Device Deployment, GlobalProtect Client, Dynamic Updates, Plugins, Licenses, Master Key and Diagnostics, and Policy Recommendation. The 'Dynamic Updates' option is highlighted with a red box.

## 4.2.6 References

**Software and Content Updates:**

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/software-and-content-updates.html>

**Determine the Upgrade Path to PAN-OS 10.1:**

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/upgrade-pan-os/upgrade-the-firewall-pan-os/determine-the-upgrade-path.html>

**Downgrade PAN-OS:**

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/upgrade-pan-os/downgrade-pan-os.html>

**Downgrade PAN-OS:**

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases.html>

**Scheduled Dynamic Updates in an Ha Environment:**

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClrnCAC>

**Upgrade an HA Firewall Pair:**

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/upgrade-pan-os/upgrade-the-firewall-pan-os/upgrade-an-ha-firewall-pair.html>

**Manage Software and Content Updates:**

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-web-interface-help/panorama-web-interface/panorama-device-deployment/manage-software-and-content-updates.html>

**Upgrade Firewalls Using Panorama:**

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/upgrade-pan-os/upgrade-the-firewall-pan-os/upgrade-firewalls-using-panorama.html>

**Automatic Content Updates Through Offline Panorama:**

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/panorama-features/automatic-content-updates-through-offline-panorama.html>

## 4.3 Manage HA Functions

## 4.3.1 & 4.3.2 Configure Link and Path Monitoring

- Why monitor links?
  - Can configure any or all as part of a group.
  - Can have multiple groups
- Path Monitoring
  - Similar to link monitoring but “pinging” IP addresses to determine failover
  - Can define VLAN, Virtual Router and VWIRE
    - VLAN and VWire need **source IP**

Link Monitoring

Enabled

Failure Condition  Any  All

HA Path Group Virtual Wire

Name

Source IP

Enabled

Failure Condition  Any  All

Ping Interval

Ping Count

DESTINATION IP GROUP	DESTINATION IP	ENABLED	FAILURE CONDITION

### 4.3.3 Choosing an HA Pair Type

Active/passive mode has simplicity of design

Both active/active and active/passive mode support a virtual wire deployment.

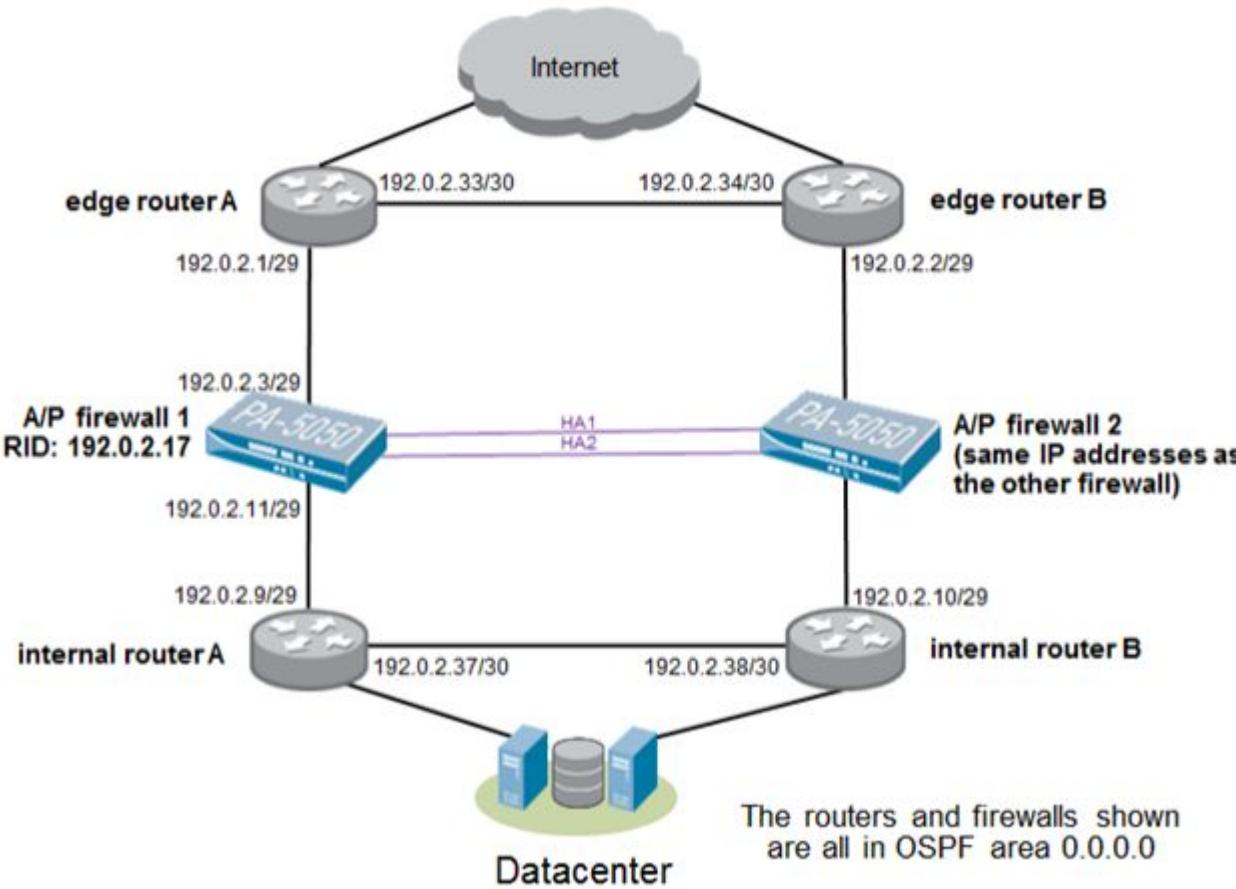
Active/active mode requires advanced design concepts replicating NAT pools, and deploying floating IP addresses to provide proper failover.

Active/active mode is recommended if each firewall needs its own routing instances and you require full, real-time redundancy out of both firewalls all the time. Active/active mode has faster failover and can handle peak traffic flows better than active/passive mode because both firewalls are actively processing traffic.

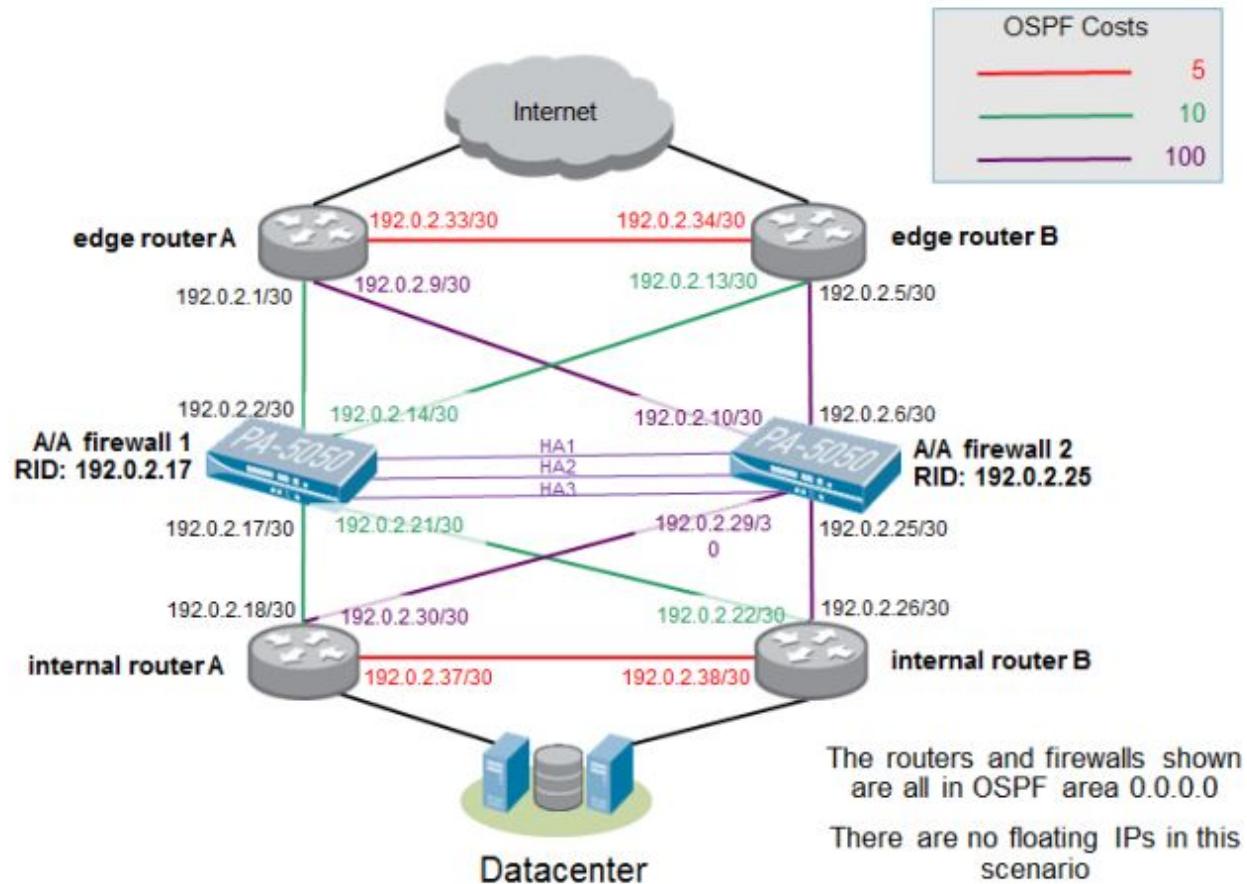
In active/active mode, the HA pair can be used to temporarily process more traffic than what one firewall normally can handle.

In cases of virtual firewall deployments, the cloud architecture might limit your deployment choices. Consult the design and deployment documentation specific to your chosen cloud vendor.

### 4.3.3 Identify When to Use HA Links (HA1 + HA2 Cluster >= NGFW A/P)

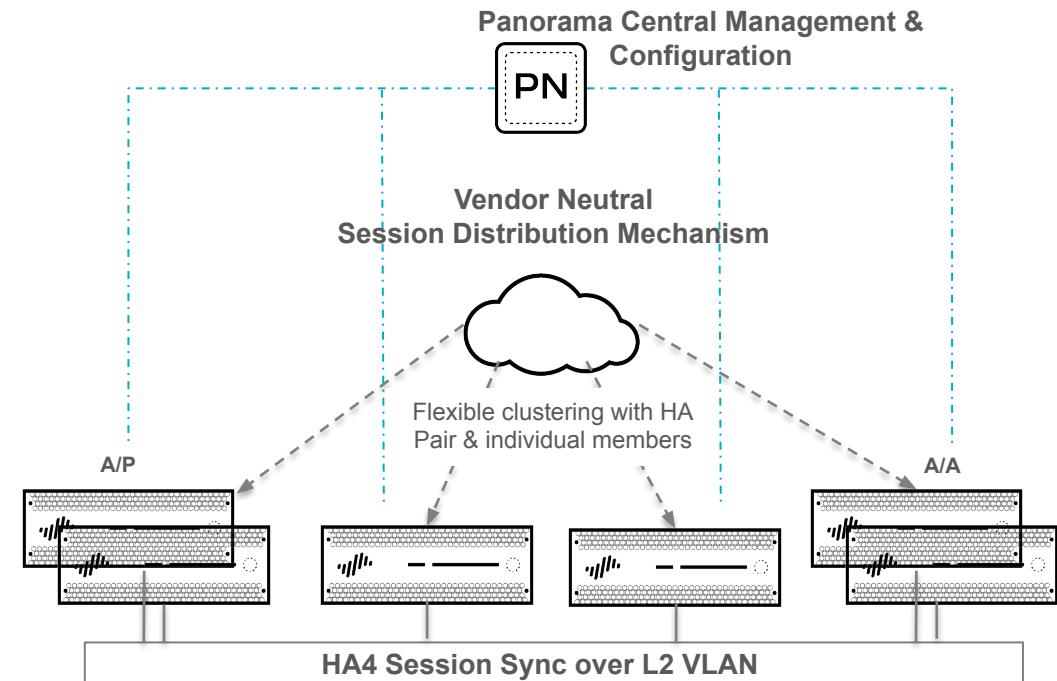


### 4.3.3 Identify When to Use HA Links (HA1 + HA2 + HA3 Cluster >= NGFW A/A)



## 4.3.3 Identify When to Use HA Links (HA4 Cluster >= 3 NGFW)

- HA Clustering support from PAN-OS 10.0
- HA1, HA2 & HA3 not supported
- Up to 16 members in a cluster
- **Session state synchronization via HA4**
- Common Use Cases
  - Multiple DCs
  - Active/Passive DCs
  - Horizontal scaling of DCs
- IPv6 is supported and a key use case
- Education and Financial Services are other key use cases



### 4.3.3 Identify When to Use HA Links (HA4 Cluster >= 3 NGFW)

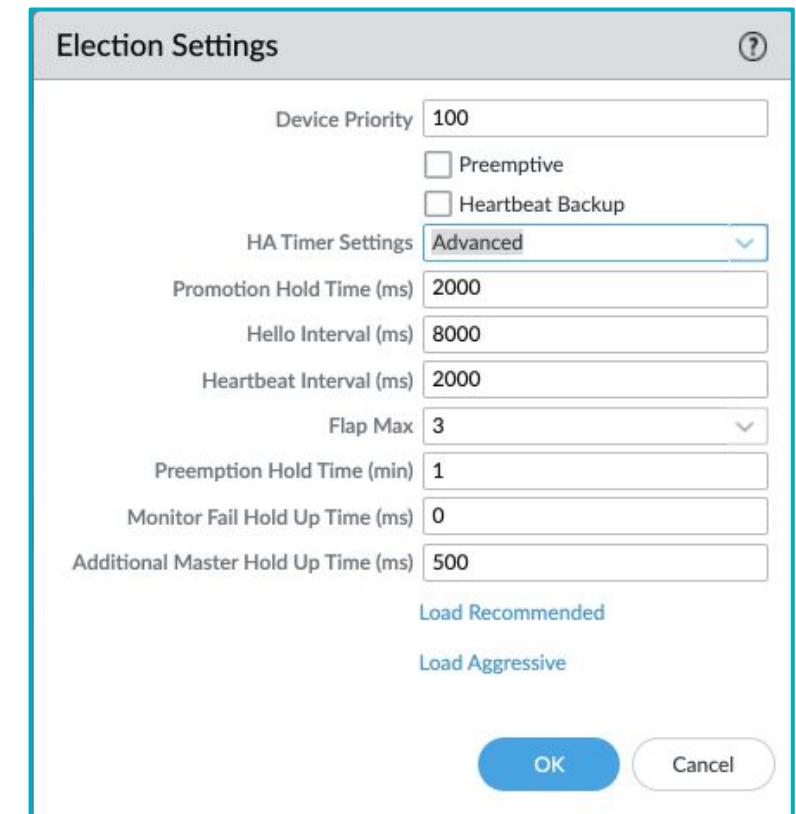
- Support Layer 3 or Vwire
- All firewalls need to be the same model
- Can be a combination of a standalone and an HA pair
- HA-4 performs session sync and will take place over a data interface

FIREWALL MODEL	NUMBER OF MEMBERS SUPPORTED PER CLUSTER
PA-3200 Series	6
PA-5200 Series	16
PA-7000 Series firewalls that have at least one of the following cards: PA-7000-100G-NPC, PA-7000-20GQXM-NPC, PA-7000-20GX-NPC	PA-7080: 4 PA-7050: 6
VM-300	6
VM-500	6
VM-700	16

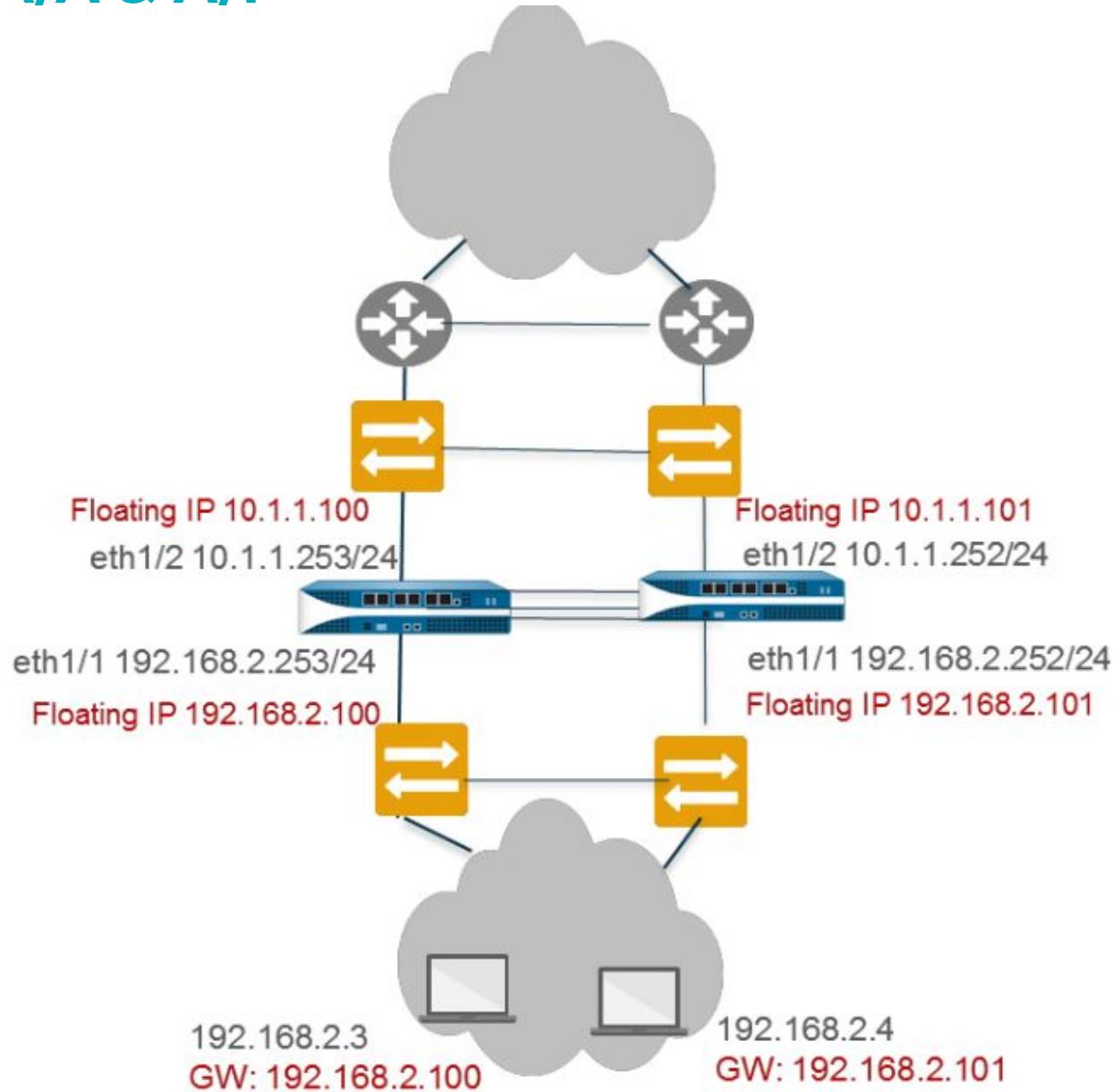
<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/high-availability/ha-clustering-best-practices-and-provisioning.html>

#### 4.3.4 Tune HA Failover

- HA interface Types (ha1, ha2, etc...)
- Different preferences for failover (recommended, aggressive, advanced)
- Link Monitoring and path monitoring
- What is clustering (HA4)
- Device Priority - which one wins?
  - answer: lower value
- Pre-emption



## 4.3.5 Configure A/A & A/P



## 4.3.6 Manage HA Interfaces

HA LINKS AND BACKUP LINKS	DESCRIPTION
Control Link	<p>The HA1 link is used to exchange hellos, heartbeats, and HA state information, and management plane sync for routing, and User-ID information. The firewalls also use this link to synchronize configuration changes with its peer. The HA1 link is a Layer 3 link and requires an IP address.</p> <p>ICMP is used to exchange heartbeats between HA peers.</p> <p>Ports used for HA1—TCP port 28769 and 28260 for clear text communication; port 28 for encrypted communication (SSH over TCP).</p> <p>If you enable encryption on the HA1 link, you can also <a href="#">Refresh HA1 SSH Keys</a> and <a href="#">Configure Key Options</a>.</p>
Data Link	<p>The HA2 link is used to synchronize sessions, forwarding tables, IPSec security associations and ARP tables between firewalls in an HA pair. Data flow on the HA2 link is always unidirectional (except for the HA2 keep-alive); it flows from the active or active-primary firewall to the passive or active-secondary firewall. The HA2 link is a Layer 2 link, and it uses ether type 0x7261 by default.</p> <p>Ports used for HA2—The HA data link can be configured to use either IP (protocol number 99) or UDP (port 29281) as the transport, and thereby allow the HA data link to span subnets.</p>
HA1 and HA2 Backup Links	<p>Provide redundancy for the HA1 and the HA2 links. In-band ports can be used for backup links for both HA1 and HA2 connections when dedicated backup links are not available. Consider the following guidelines when configuring backup HA links:</p> <ul style="list-style-type: none"><li>• The IP addresses of the primary and backup HA links must not overlap each other.</li><li>• HA backup links must be on a different subnet from the primary HA links.</li><li>• HA1-backup and HA2-backup ports must be configured on separate physical ports. The HA1-backup link uses port 28770 and 28260.</li><li>• PA-3200 Series firewalls don't support an IPv6 address for the HA1-backup link; use an IPv4 address.</li></ul> <p> Palo Alto Networks recommends enabling heartbeat backup (uses port 28771 on the MGT interface) if you use an in-band port for the HA1 or the HA1 backup links.</p>
Packet-Forwarding Link	<p>In addition to HA1 and HA2 links, an active/active deployment also requires a dedicated HA3 link. The firewalls use this link for forwarding packets to the peer during session setup and asymmetric traffic flow. The HA3 link is a Layer 2 link that uses MAC-in-MAC encapsulation. It does not support Layer 3 addressing or encryption. PA-7000 Series firewalls synchronize sessions across the NPCs one-for-one. On PA-800 Series, PA-3200 Series, and PA-5200 Series firewalls, you can configure aggregate interfaces as an HA3 link. The aggregate interfaces can also provide redundancy for the HA3 link; you cannot configure backup links for the HA3 link. On PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls, the dedicated HSCI ports support the HA3 link. The firewall adds a proprietary packet header to packets traversing the HA3 link, so the MTU over this link must be greater than the maximum packet length forwarded.</p>
HA4 Link and HA4 Backup Link	<p>The HA4 link and HA4 backup link perform session cache synchronization among all HA cluster members having the same cluster ID. The HA4 link between cluster members detects connectivity failures between cluster members by sending and receiving Layer 2 keepalive messages. View the status of the HA4 and HA4 backup links on the firewall dashboard.</p>

## 4.3.7 References

### HA Concepts

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/high-availability/ha-concepts.html>

### HA-Lite on Palo Alto Networks PA-200

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIUzCAK>

### Overview of HA Clustering

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/high-availability/ha-clustering-overview>

### HA Links and Backup Links

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/high-availability/ha-concepts/ha-links-and-backup-links.html>

### Set Up Active/Passive HA

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/high-availability/set-up-activepassive-ha.html>

### Set Up Active/Active HA

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/high-availability/set-up-activeactive-ha.html>

### Setting up HA clustering

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/high-availability/configure-ha-clustering.html>

### HA Clustering Provisioning Best Practices

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/high-availability/ha-clustering-best-practices-and-provisioning.html#id53986e31-4241-4297-9343-0d574a0bdf52>

### SNMP Support

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/snmp-monitoring-and-traps/snmp-support>

## 4.3.7 References

### Monitor Statistics Using SNMP

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/snmp-monitoring-and-traps/monitor-statistics-using-snmp>

### Supported MIBs

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/snmp-monitoring-and-traps/supported-mibs>

### Monitor Device Health

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/device-monitoring-on-panorama/monitor-device-health.html>

### A use case illustrating an active/active deployment can be found here:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/high-availability/set-up-activeactive-ha/determine-your-activeactive-use-case/use-case-configure-activeactive-ha-with-floating-ip-address-bound-to-active-primary-firewall.html>

### Information Synchronized Between HA Pairs

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000C1XGCA0>

### What Settings Don't Sync in Active/Passive HA?

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/high-availability/reference-ha-synchronization/what-settings-dont-sync-in-active-passive-ha.html>

## **4.4 Identify Benefits & Differences Between the Heatmap & BPA Reports**

## 4.4.1 Identify How to Use the Heatmap & BPA to Optimize FW Configurations

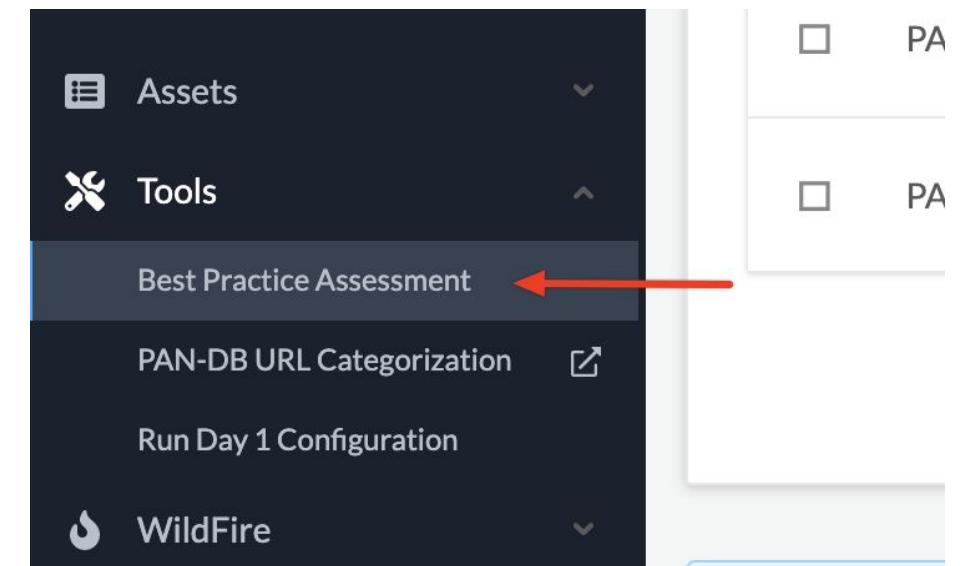
**Best Practice Assessment (BPA)** tool for Palo Alto Networks firewalls and Panorama evaluates a device's configuration by measuring the adoption rate of a firewall's capabilities, and by validating whether the policies adhere to best practices.

How do you generate a BPA? You go to the Support site

What do you need? A tech support file

**Device -> Support -> Tech Support File**

What else is needed? Mapping the Zones



## 4.4.1 Identify How to Use the Heatmap & BPA to Optimize FW Configurations

The **Heatmap** measures the adoption rate of the following Palo Alto Networks firewall features:

- WildFire
- Threat Prevention (IPS)
- Anti-Spyware
- DNS Sinkhole
- Antivirus
- Vulnerability Protection
- URL Filtering
- File Blocking
- Data Filtering
- User-ID
- App-ID
- Service/Port
- Logging

Metric	2017-06-07 02:28:10	2017-07-14 02:04:50	2017-10-26 03:19:32	2018-02-05 06:20:59	2018-02-05 06:52:14	2018-02-05 06:52:34	2018-05-29 06:06:59	2018-06-21 15:20:25
Total Rule Count	282	344	349	347	347	347	350	5
Allow Rule Count	274	338	342	339	339	339	341	2
Deny Rule Count	8	6	7	8	8	8	9	3
WildFire Adoption %	4.0	75.4	75.4	78.8	78.8	78.8	78.0	0.0
Anti-Spyware Adoption %	3.6	75.1	75.4	78.8	78.8	78.8	78.0	50.0
DNS Sinkhole Adoption %	0.0	0.0	0.6	78.8	78.8	78.8	78.0	50.0
Anti-Virus Adoption %	5.1	76.3	76.3	79.1	79.1	79.1	78.3	0.0
Vulnerability Protection Adoption %	6.9	77.8	78.1	79.6	79.6	79.6	78.9	50.0
URL-Filtering Adoption %	2.9	2.4	2.3	2.4	2.4	2.4	2.1	0.0
Credential Theft Adoption %	N/A	N/A	N/A	2.4	2.4	2.4	2.1	0.0
File-Blocking Adoption %	4.0	75.4	75.4	78.2	78.2	78.2	77.4	0.0
Data-Filtering Adoption %	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
User ID Adoption %	17.4	32.3	31.8	30.8	30.5	30.5	30.6	0.0
App ID Adoption %	9.6	7.3	7.7	7.2	7.2	7.2	7.4	60.0
Service / Port Adoption %	100.0	100.0	100.0	92.0	92.0	92.0	92.3	33.3
Logging Adoption %	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0

## 4.4.1 Identify How to Use the Heatmap & BPA to Optimize FW Configurations

The BPA tool enables you to create a firewall configuration that meets security best practices. The seven primary categories of the Best Practice Assessment tool are as follows:

- Security
- Policy Based Forwarding
- Decryption Rulebase
- Decryption
- Application Override
- Captive Portal
- DoS Protection

# Thank you!

## Exam Domain #4 Manage & Operate

