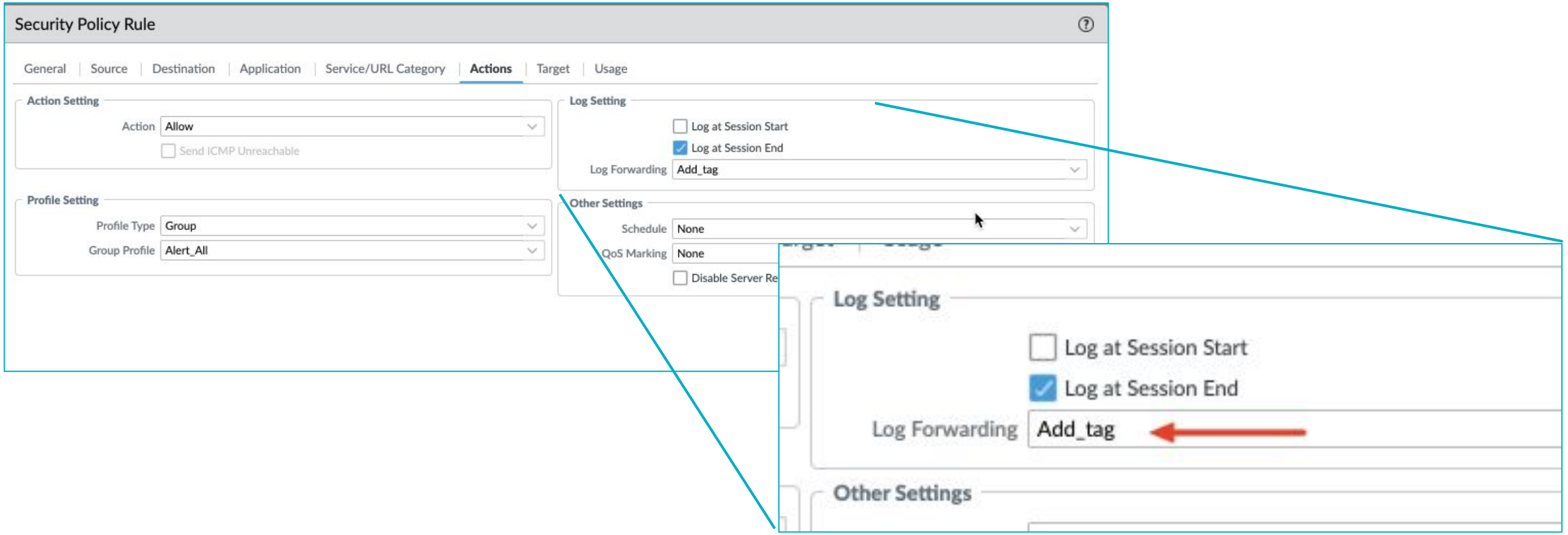
PCNSE Bootcamp v10.1

Exam Domain #4
Manage & Operate

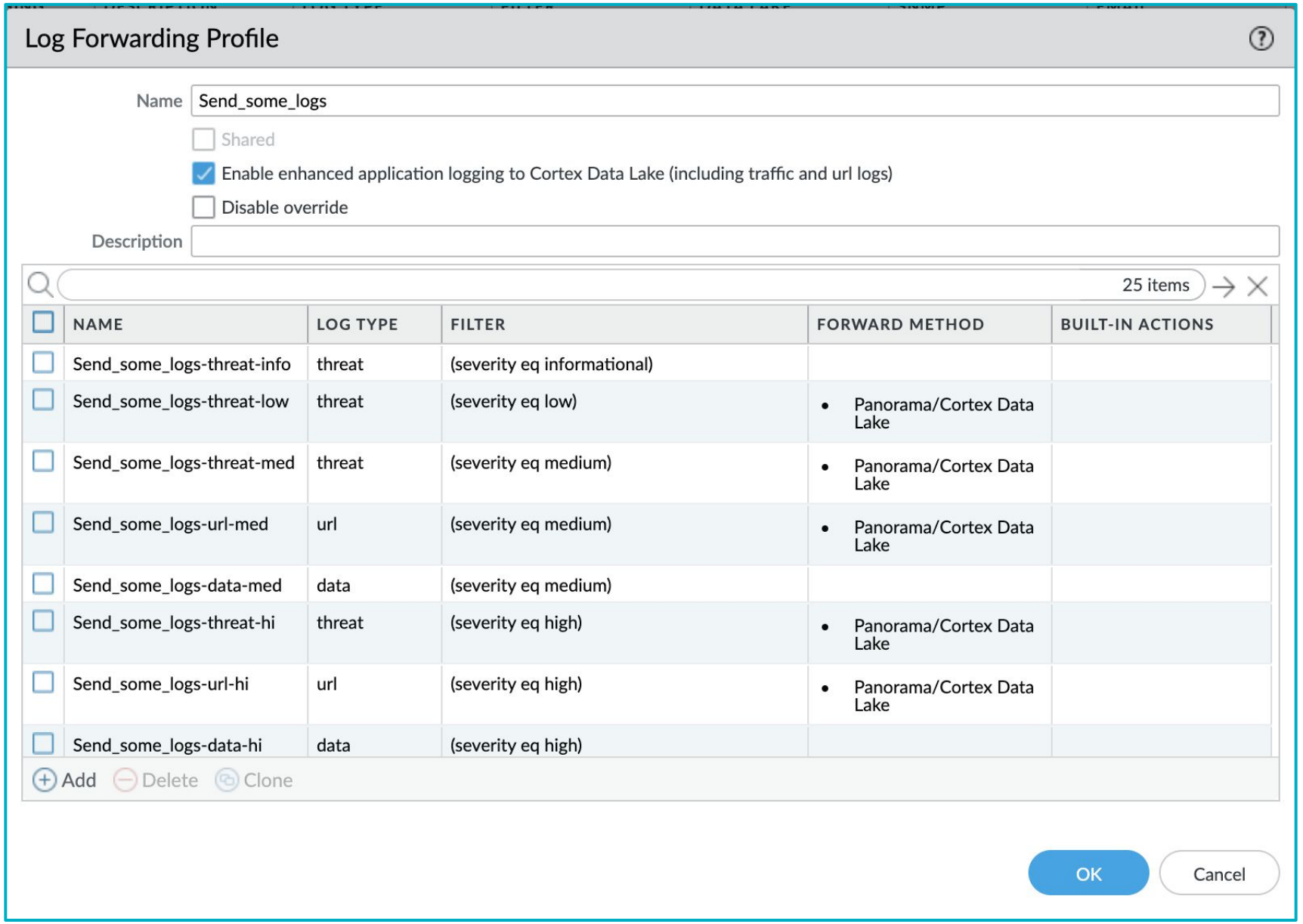
David Scrivens SE WEUR

4.1 Manage and Configure Log Forwarding

Review - Where to apply Log Forwarding Profiles



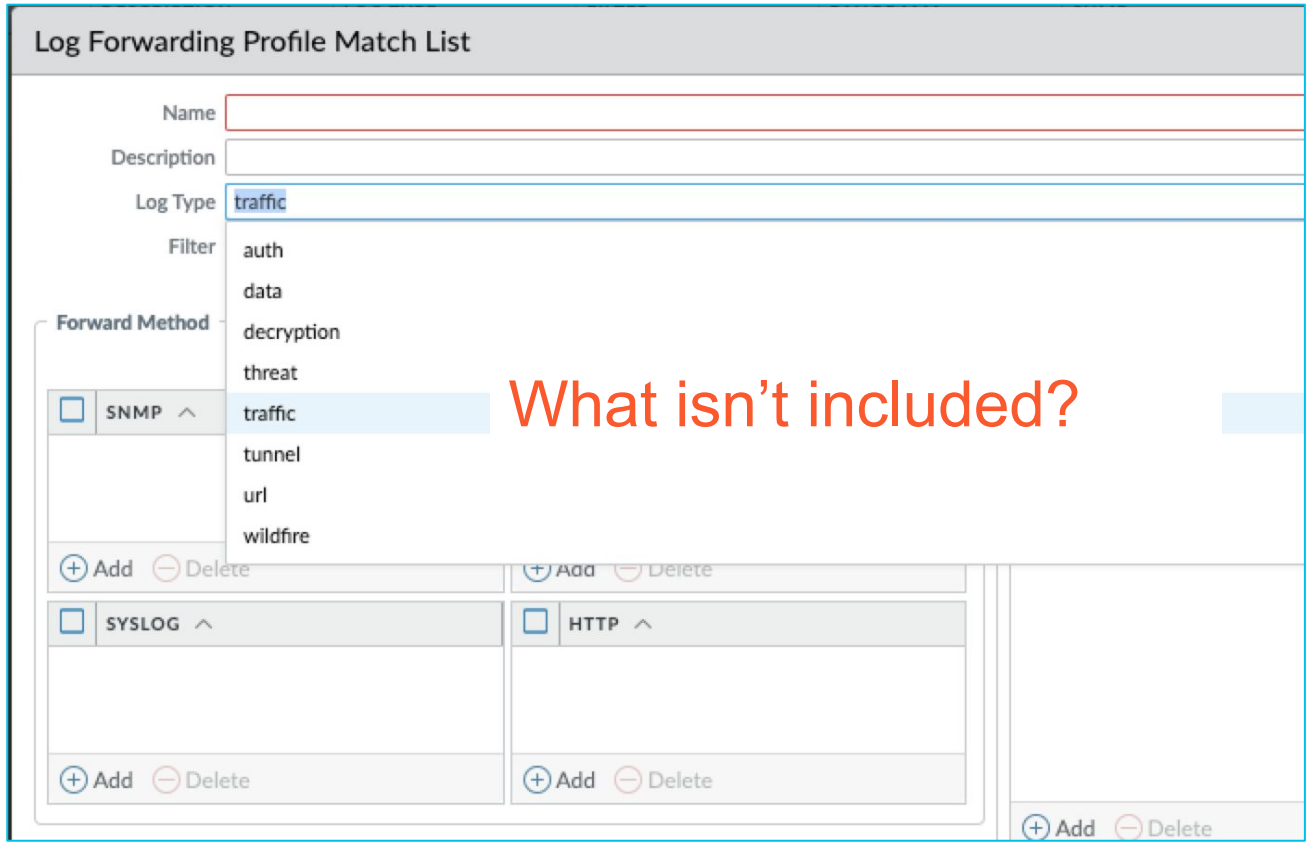
Log Forwarding Profile



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.

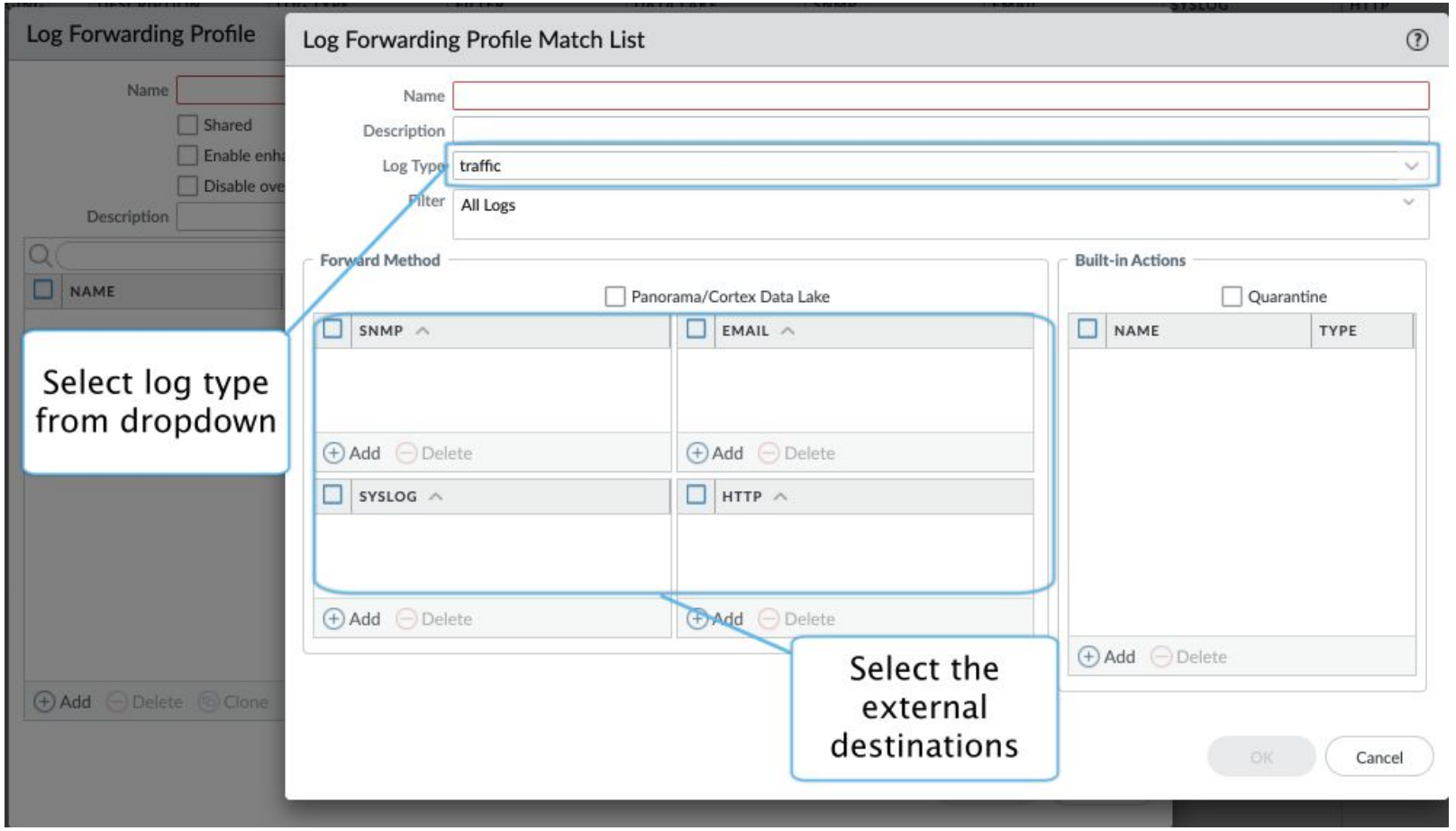
- Authentication
- Data Filtering
- Decryption
- Traffic
- Threat
- Tunnel
- URL Filtering
- WildFire Submissions



Methods Used to Forward Logs

Method 1 - Log Forwarding Profile

Objects > Log Forwarding



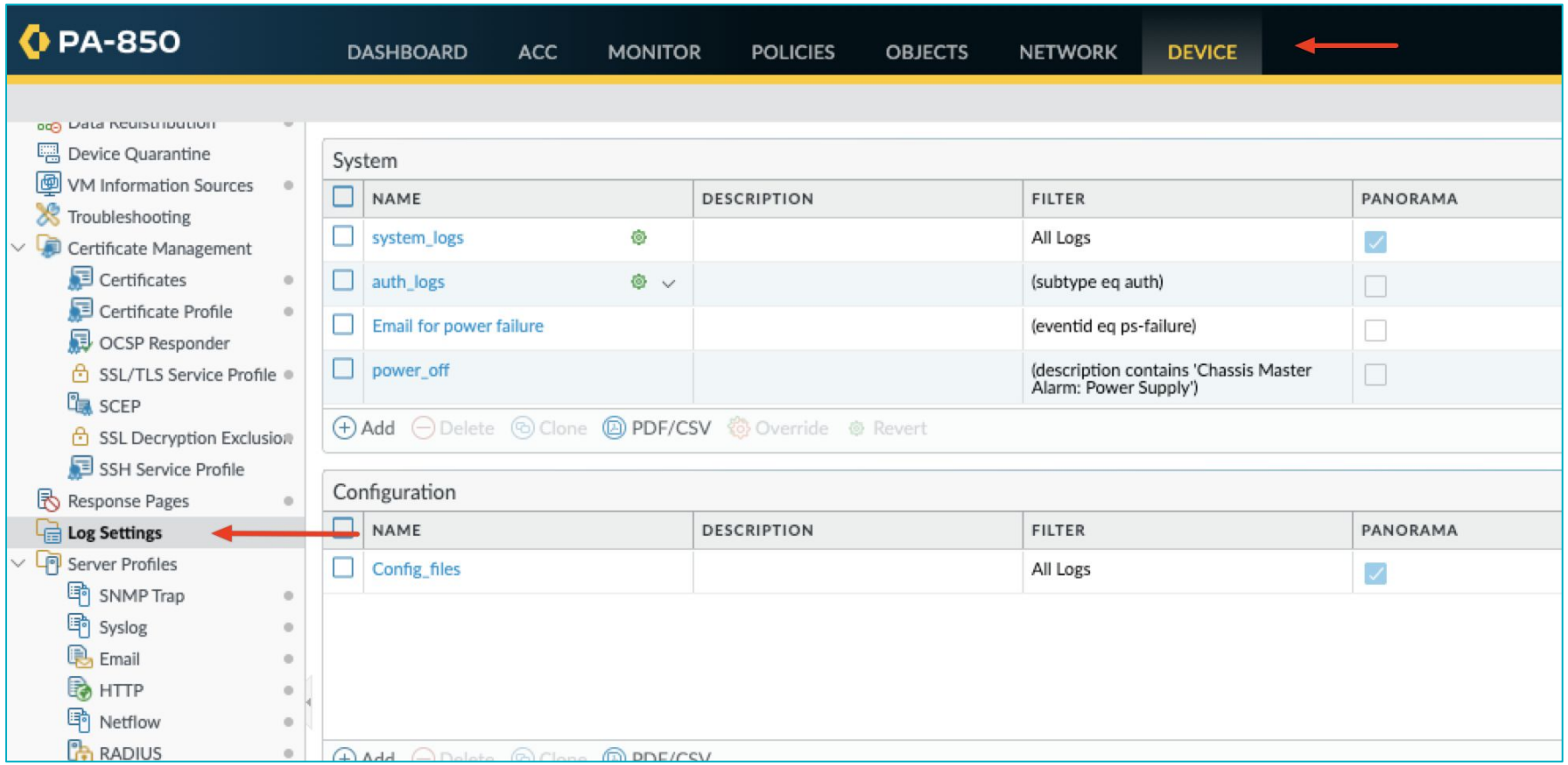
Methods Used to Forward Logs

Two Methods used to forward log events depending on the type

Method 2

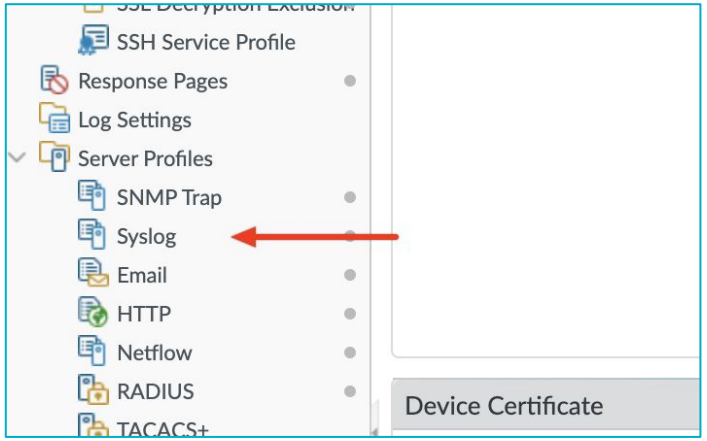
Device > Log Settings

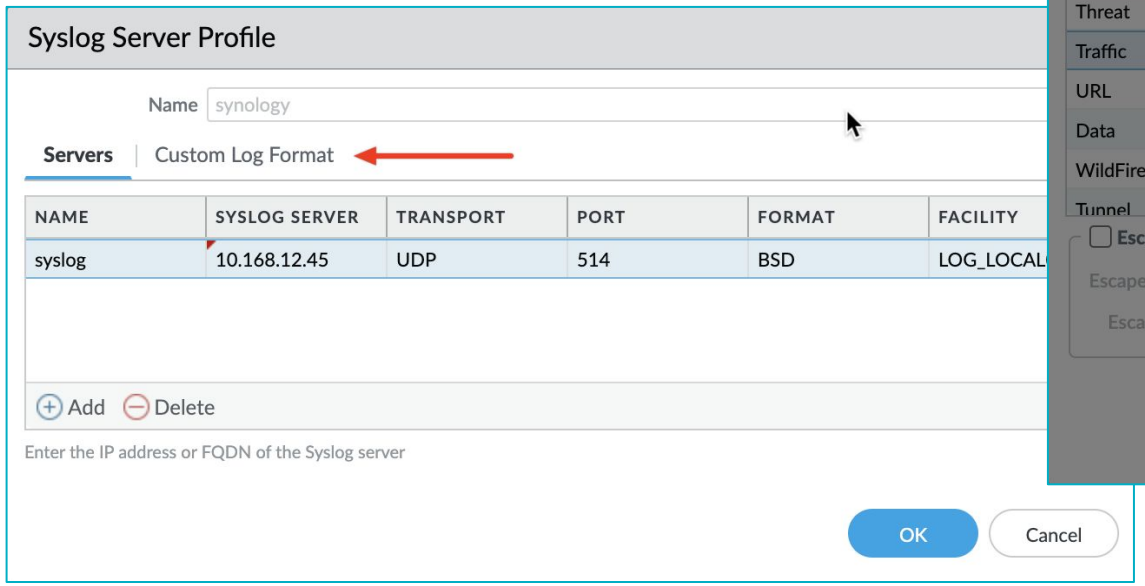
- System
- Config
- User-ID
- HIP Match
- IP-Tag
- GlobalProtect

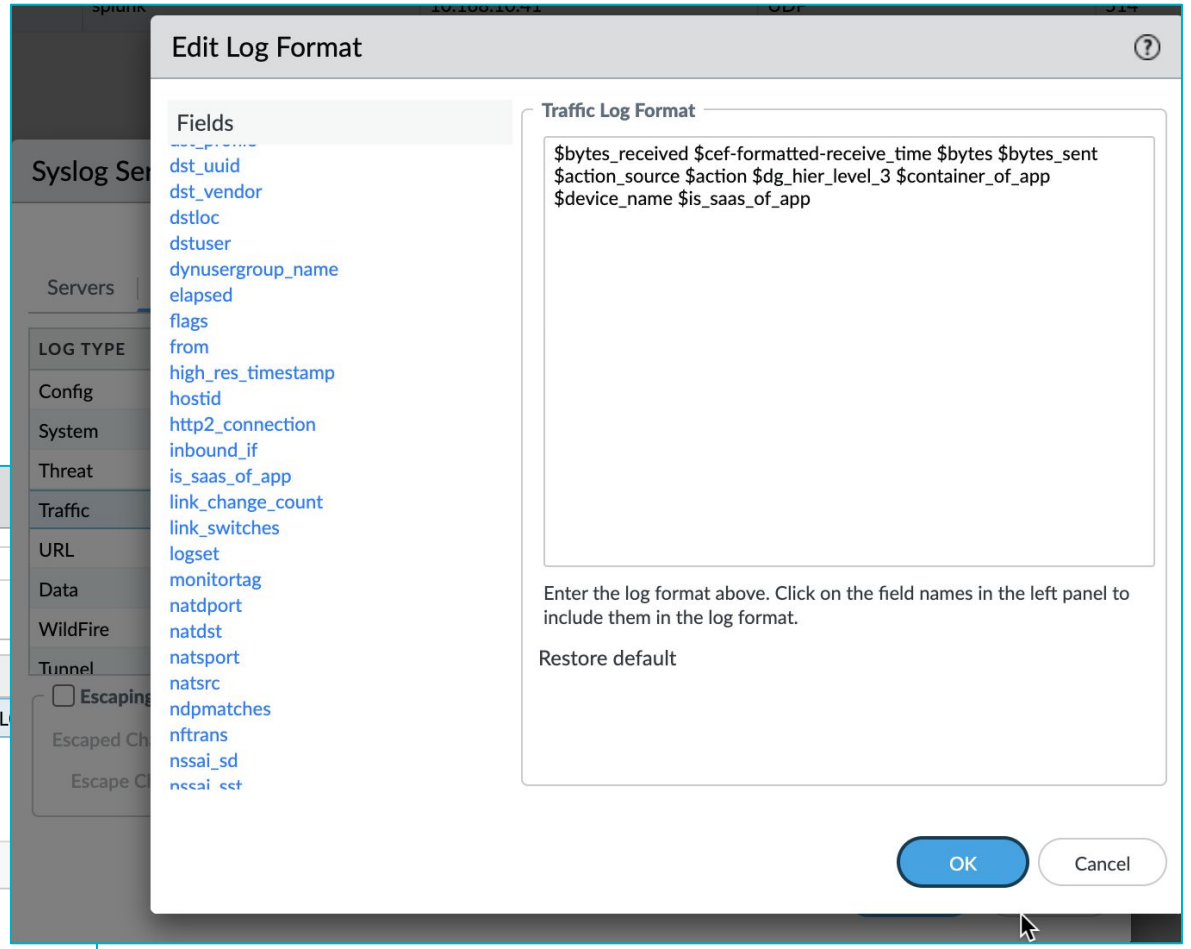


PANORAMA	SNMP TRAP	EMAIL	SYSLOG	HTTP

Log Message Format Customization

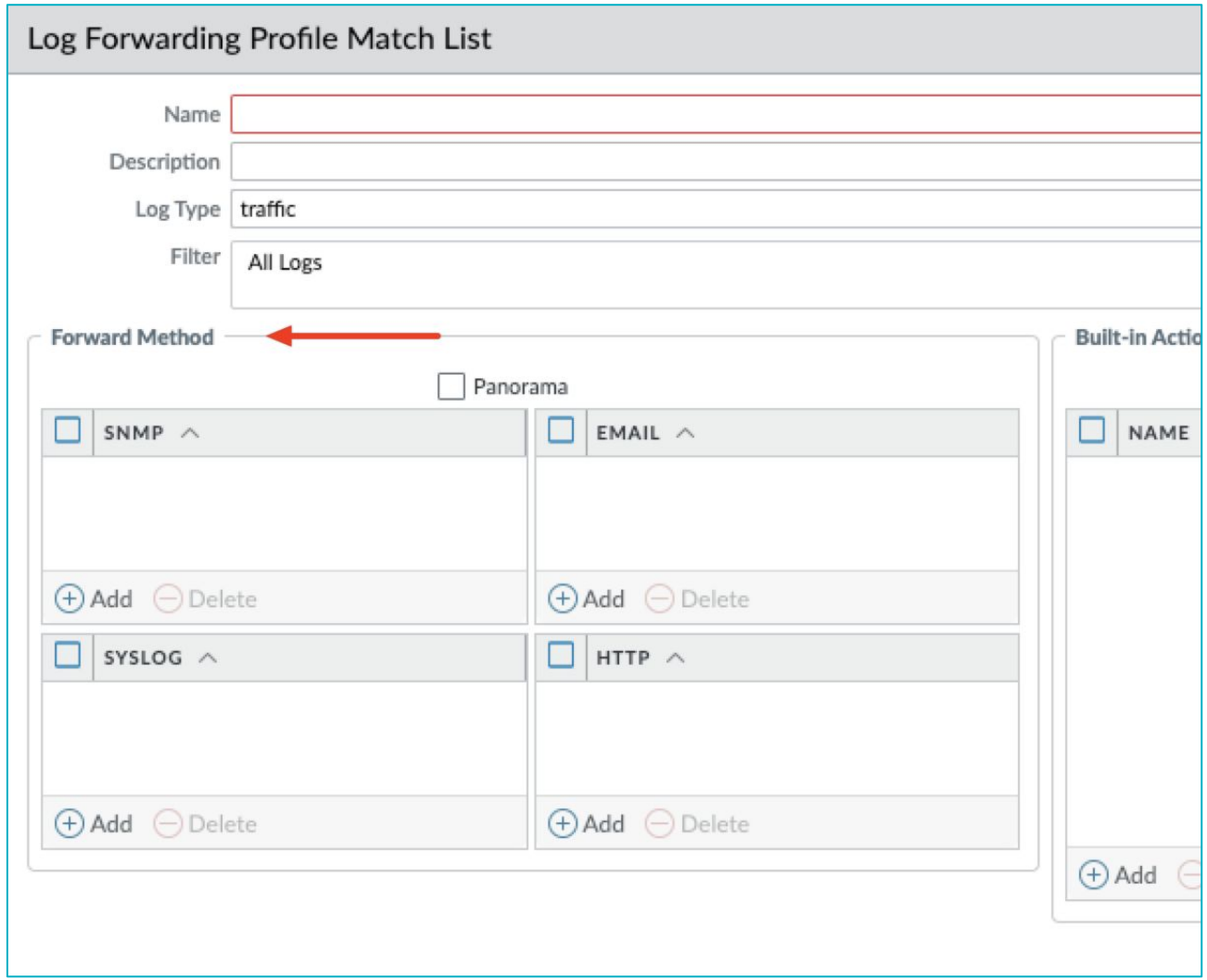






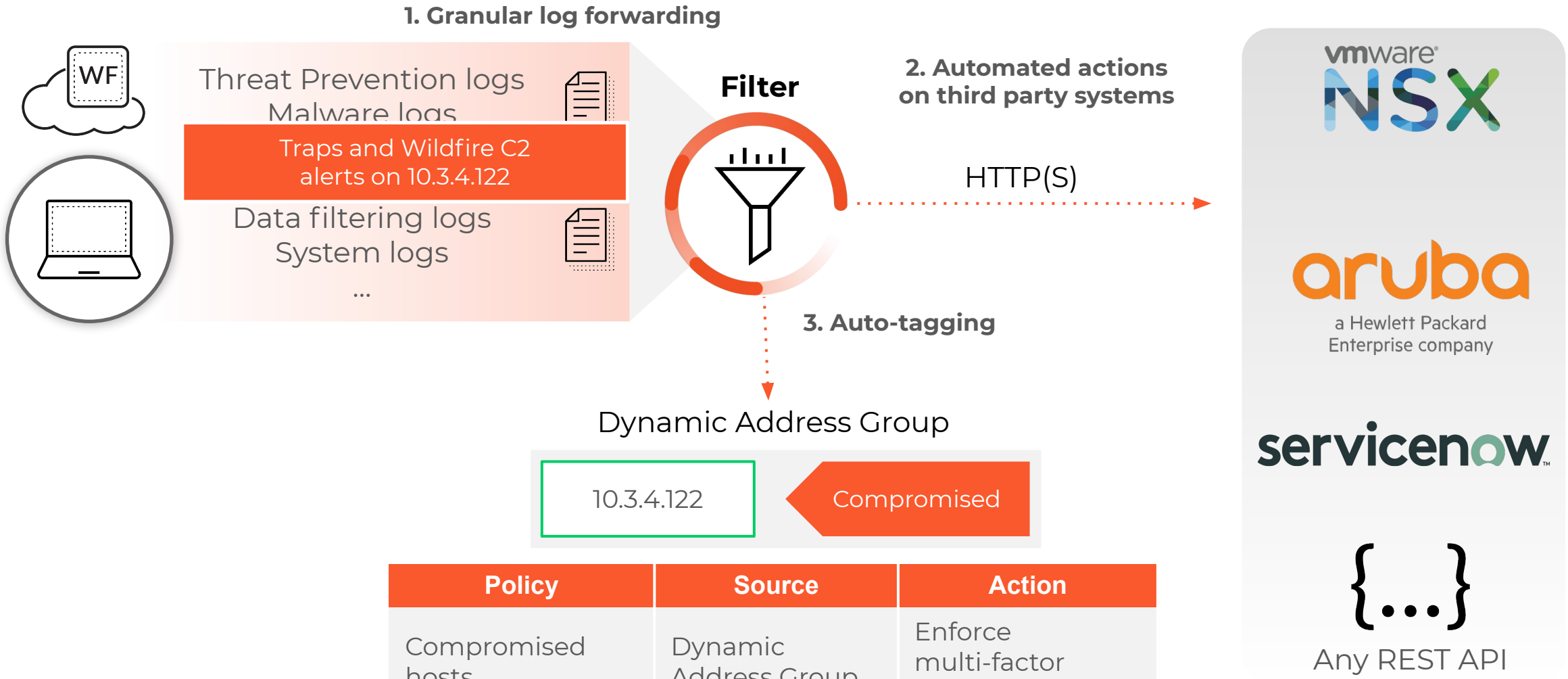
4.1.2 - More Logging Forwarding - Managing External Services

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



4.1.3 Tags and Log Forwarding

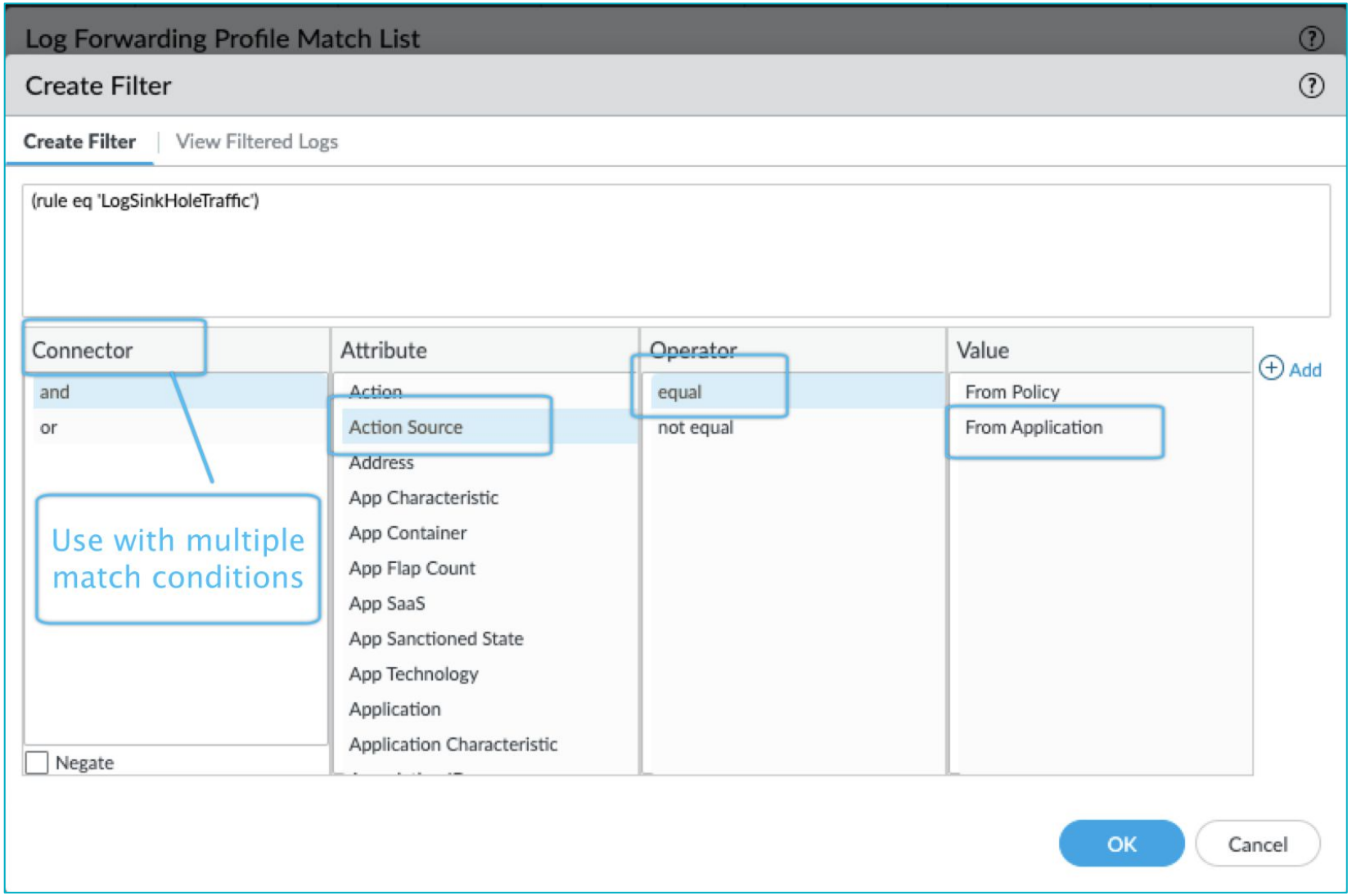
Log Forwarding Profiles also provide a mechanism to collect the source or destination IP address of the event and tag it. The tag then can be used to assign the address to a Dynamic Address Group that is used in a Security policy rule.



Policy	Source	Action
Compromised hosts	Dynamic Address Group	Enforce multi-factor authentication

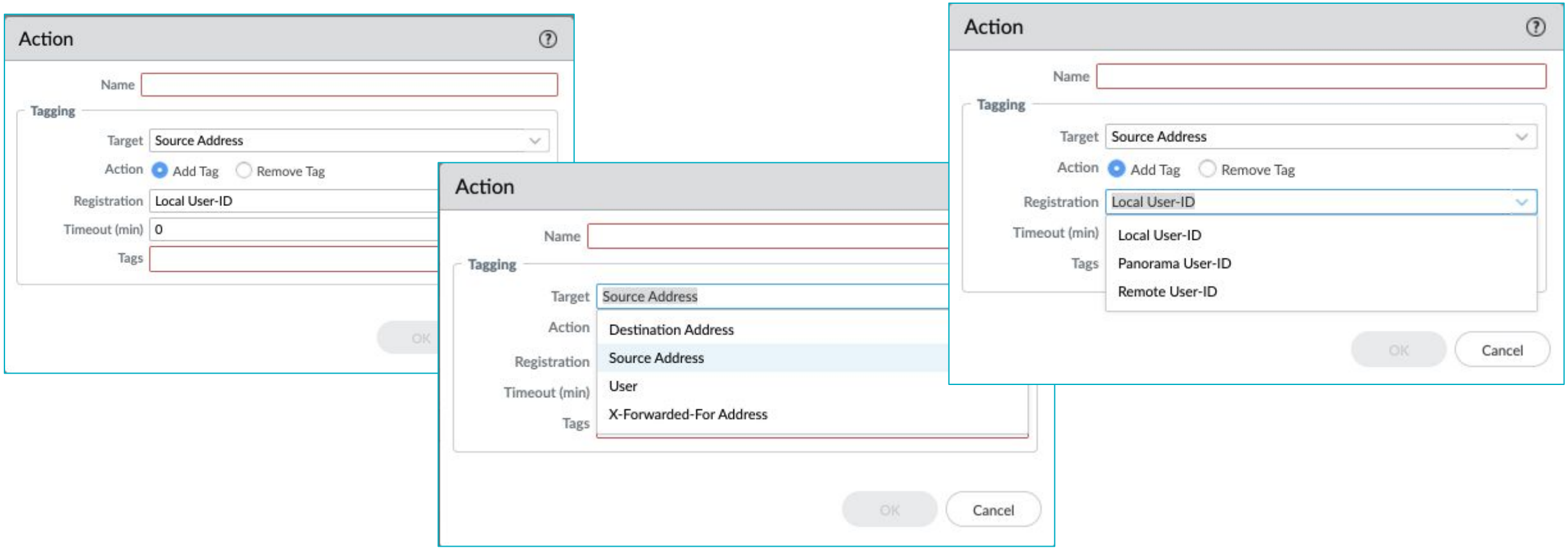
Automated Actions and Tagging with Log Forwarding

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.



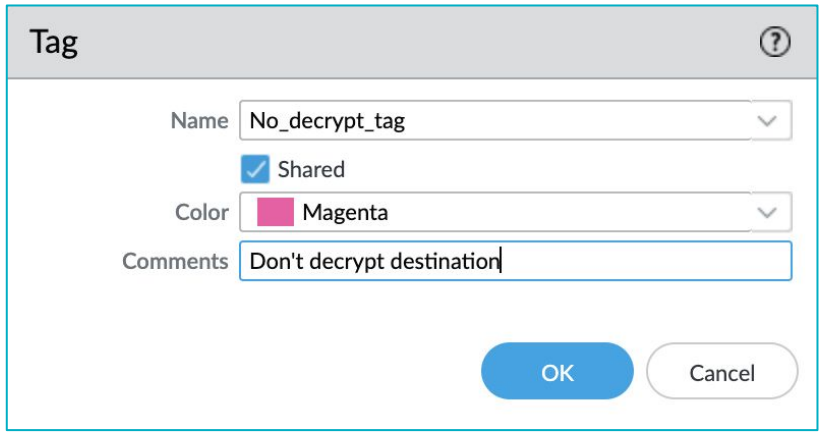
Going through adding Tagging Actions

- 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.

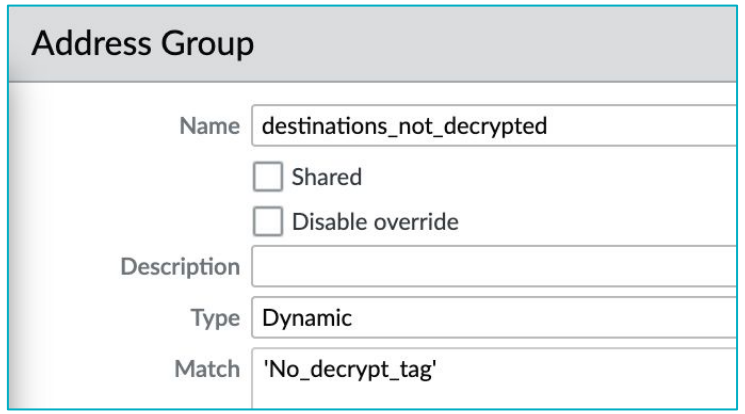


Steps

1. Create Tag

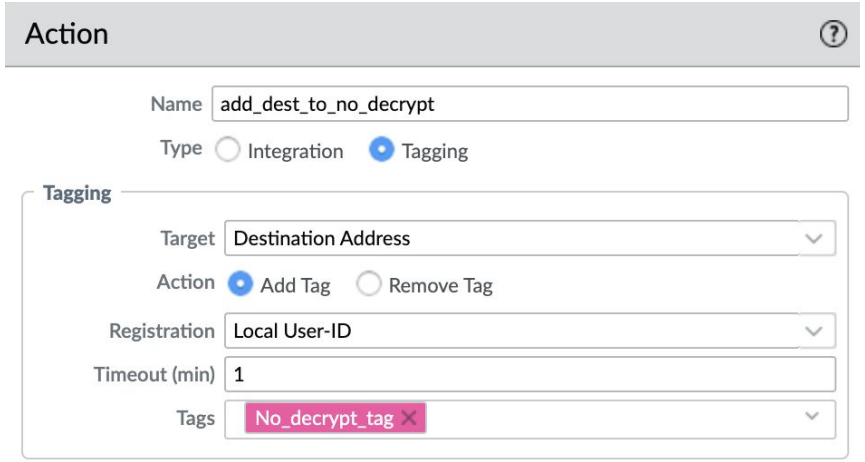


2. Associate Tag with Dynamic Address Group



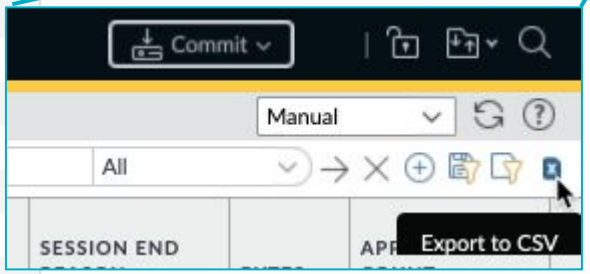
3. Create log forwarding profile to utilize a built in action to reference the tag

4. Create a Security Rule that takes uses tag



CSV Log Export

Receive Time	Type	From Zo	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	HTTP/2 Connection Session ID
08/08 11:01:28	end	L3-TAP	L3-TAP	115.218.106.148		10.154.173.98	3389	incomplete	allow	Allowed Personal Apps	aged-out	66	0
08/08 11:01:28	end	L3-TAP	L3-TAP	119.57.91.22		10.154.134.133	3389	incomplete	allow	Allowed Personal Apps	aged-out	66	0
08/08 11:01:28	end	L3-TAP	L3-TAP	95.191.44.211		10.154.173.238	56383	incomplete	allow	Allowed Personal Apps	aged-out	62	0
08/08 11:01:28	end	L3-TAP	L3-TAP	10.154.216.36	pancademo\mar...	198.31.193.211	8443	incomplete	allow	IT Sanctioned SaaS Apps	aged-out	78	0
08/08 11:01:28	end	L3-TAP	L3-TAP	89.23.248.246		10.154.59.142	29940	incomplete	allow	Allowed Personal Apps	aged-out	74	0
08/08 11:01:28	end	L3-TAP	L3-TAP	198.228.208.230		10.154.183.31	110	incomplete	allow	Allowed Personal Apps	aged-out	62	0
08/08 11:01:28	end	L3-TAP	L3-TAP	64.124.57.5		10.154.1.5	135	incomplete	allow	Allowed Personal Apps	aged-out	62	0
08/08 11:01:28	end	L3-TAP	L3-TAP	171.101.126.124		10.154.59.142	29940	incomplete	allow	Allowed Personal Apps	aged-out	62	0
08/08 11:01:28	end	L3-TAP	L3-TAP	10.154.173.238	pancademo\kra...	123.243.208.188	25874	incomplete	allow	IT Sanctioned SaaS Apps	aged-out	282	0
08/08 11:01:28	end	L3-TAP	L3-TAP	10.154.174.172	pancademo\eric....	67.215.253.139	80	incomplete	allow	IT Sanctioned SaaS Apps	aged-out	3.1k	0
08/08 11:01:28	end	L3-TAP	L3-TAP	10.154.228.4	pancademo\ben...	98.137.53.23	443	incomplete	allow	IT Sanctioned SaaS Apps	aged-out	3.0k	0
08/08 11:01:28	end	L3-TAP	L3-TAP	10.154.229.185	pancademo\bria...	198.189.255.201	80	incomplete	allow	IT Sanctioned SaaS Apps	aged-out	224	0
08/08 11:01:28	end	L3-TAP	L3-TAP	10.154.229.189	pancademo\fabi...	198.189.255.217	80	incomplete	allow	IT Sanctioned SaaS Apps	aged-out	228	0
08/08 11:01:28	end	L3-TAP	L3-TAP	10.154.229.189	pancademo\fabi...	198.189.255.207	80	incomplete	allow	IT Sanctioned SaaS Apps	aged-out	282	0
08/08 11:01:28	end	L3-TAP	L3-TAP	130.212.224.241		10.154.193.46	80	incomplete	allow	Required Infrastructure	aged-out	174	0
08/08 11:01:28	end	L3-TAP	L3-TAP	24.6.111.236		10.154.186.37	443	incomplete	allow	Required Infrastructure	aged-out	4.8k	0
08/08 11:01:28	end	L3-TAP	L3-TAP	10.154.230.62	pancademo\davi...	184.75.160.3	443	zynga-games	allow	IT Sanctioned SaaS Apps-443	aged-out	5.1k	0
08/08 11:01:28	end	L3-TAP	L3-TAP	10.154.198.104	pancademo\ross...	74.121.136.89	443	ssl	allow	IT Sanctioned SaaS Apps-443	aged-out	478	0
08/08 11:01:28	end	L3-TAP	L3-TAP	10.154.213.17	pancademo\bru...	50.16.211.20	80	web-browsing	allow	General Web Infrastructure	aged-out	2.0k	0
08/08 11:01:28	end	L3-TAP	L3-TAP	10.154.228.54	pancademo\joe....	98.139.43.115	80	incomplete	allow	IT Sanctioned SaaS Apps	aged-out	2.0k	0



New Admin features in 10.1

Uncommitted changes now survive a reboot or a power outage.

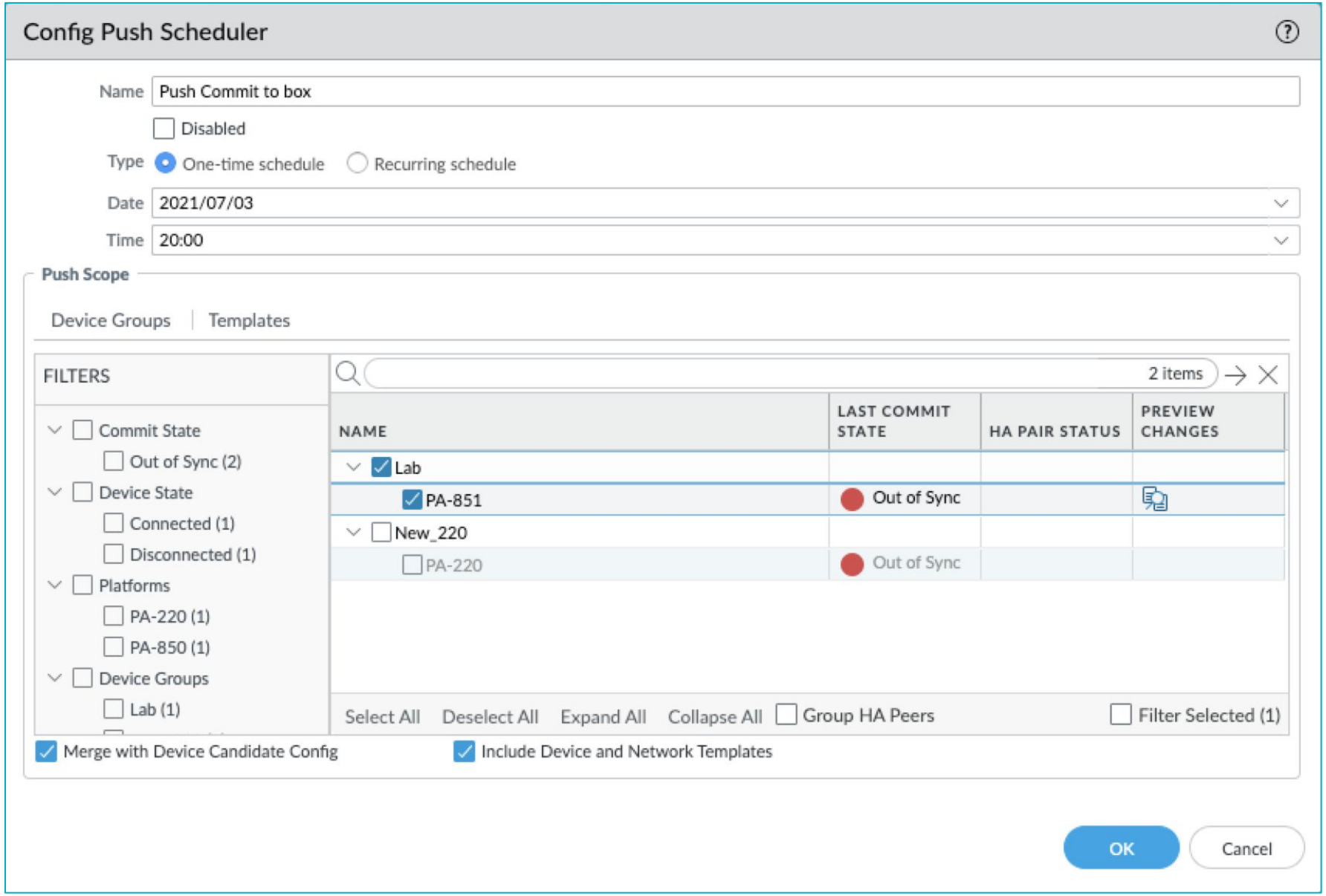
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-new-features/management-features/persistent-uncommitted-changes-on-pan-os.html#id301d640f-10ce-46cf-99d6-900cac2a7e81

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*.

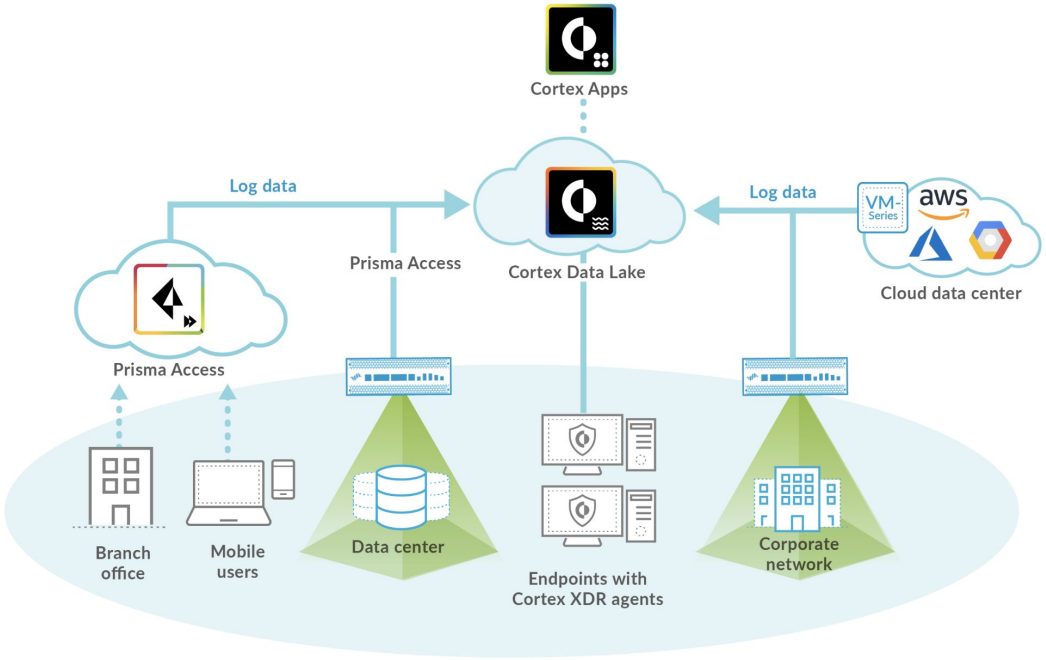
Schedule Commits



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)

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

Storing Log Filters:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-and-manage-reports.html

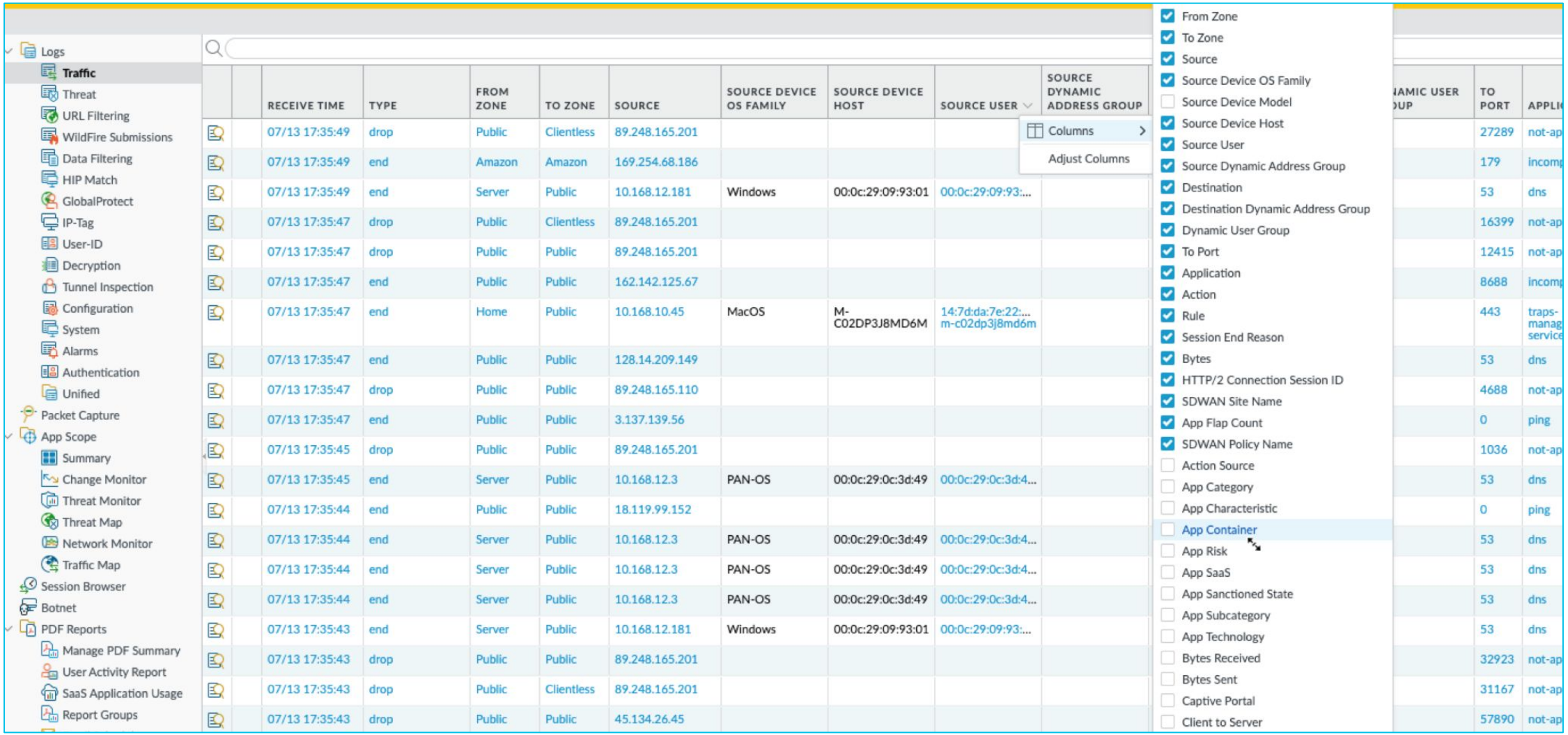
PDF Reports:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-and-manage-reports/generate-custom-reports.html

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

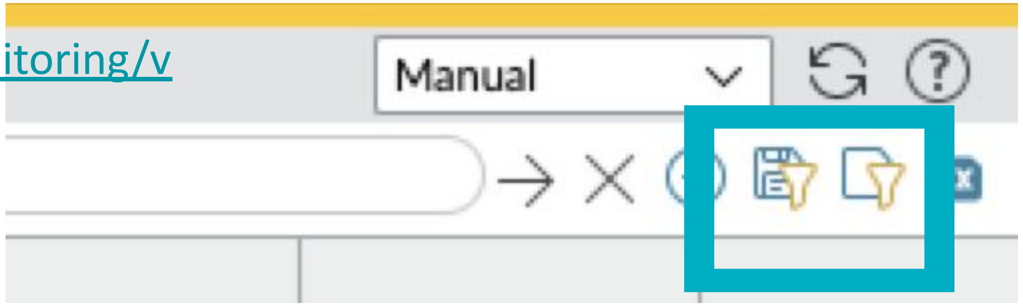
App Scope
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/use-the-app-scope-reports.html

Select Logging Columns to Display

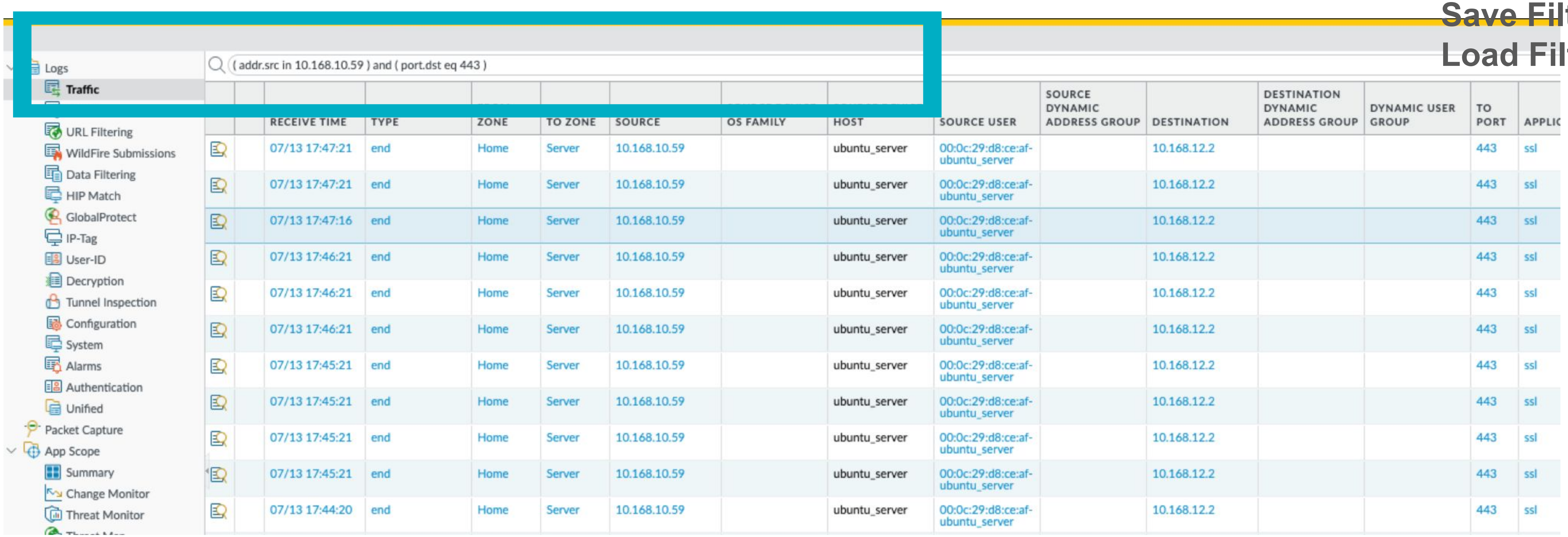


Log Filtering

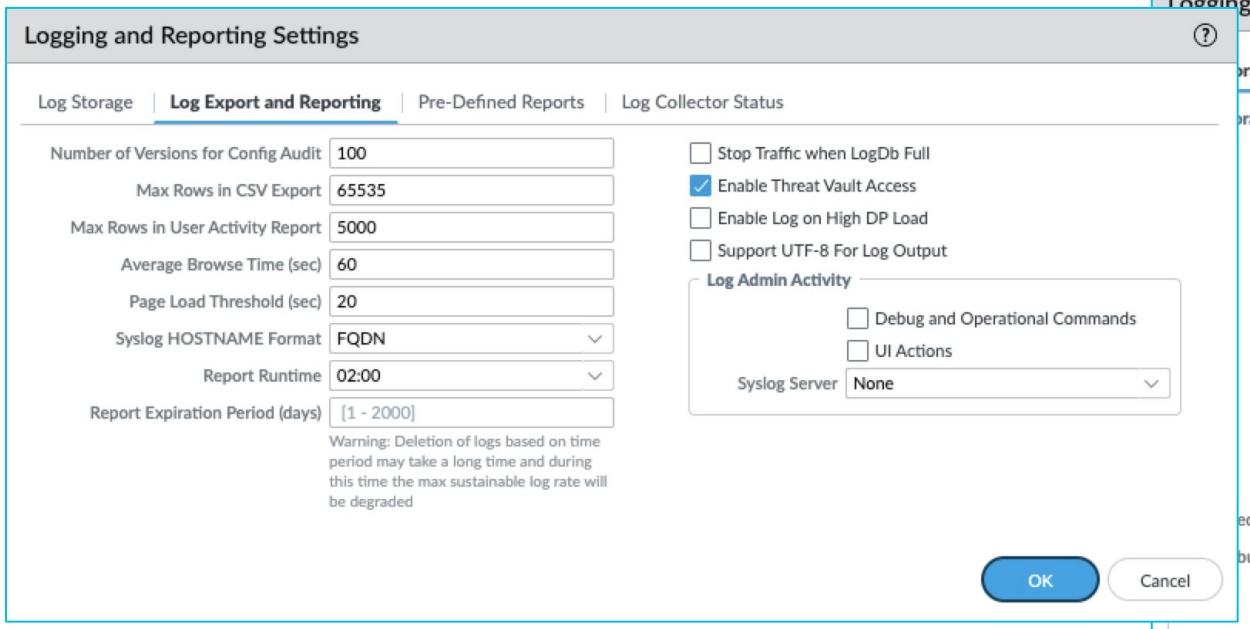
Filters can be built and even stored for future use.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-and-manage-logs.html

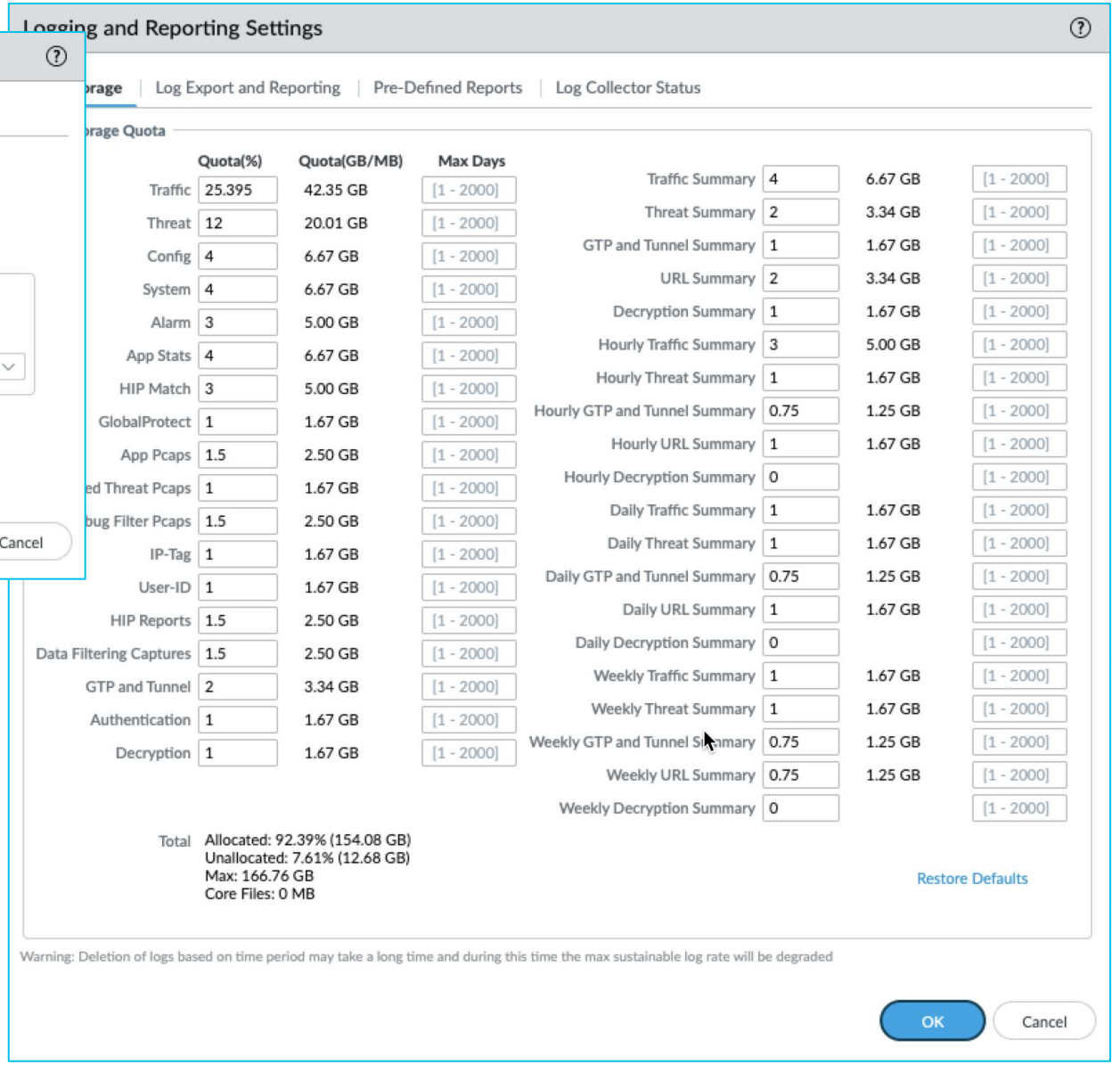


Save Filter
Load Filter

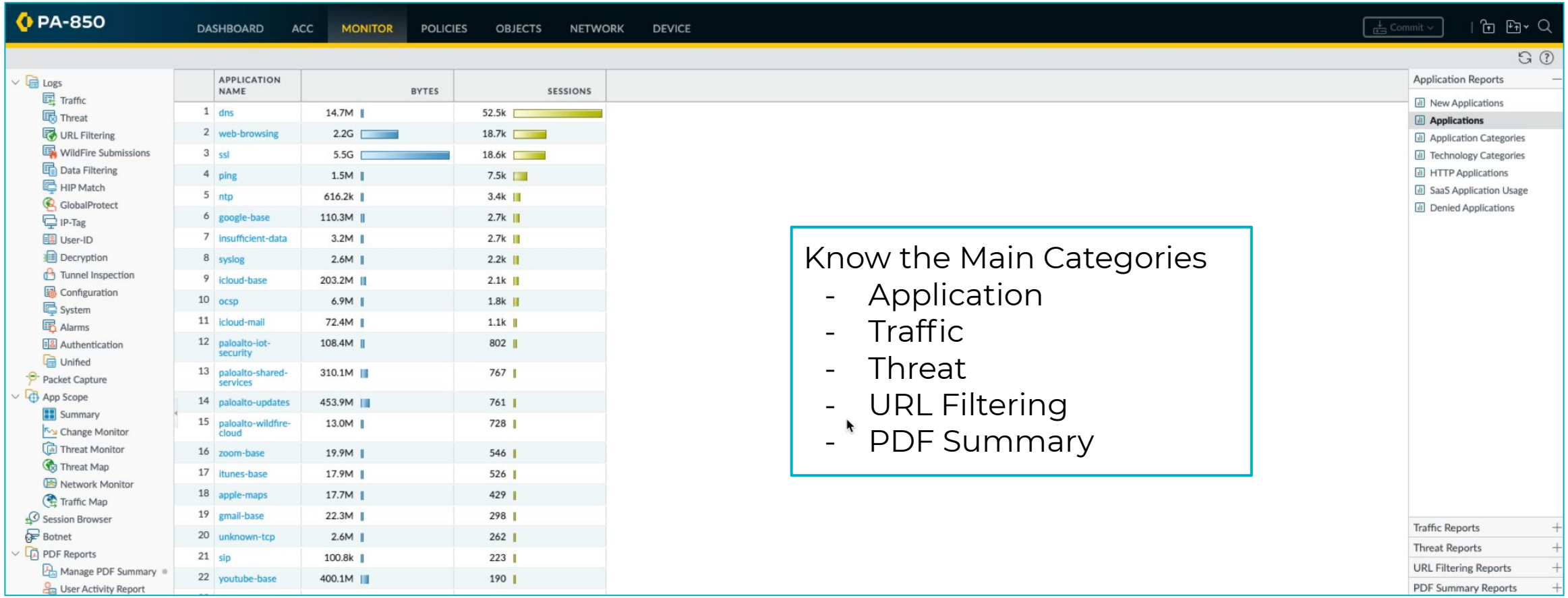


How Data Populates the ACC





PDF Reports



Know the Main Categories
- Application
- Traffic
- Threat
- URL Filtering
- PDF Summary

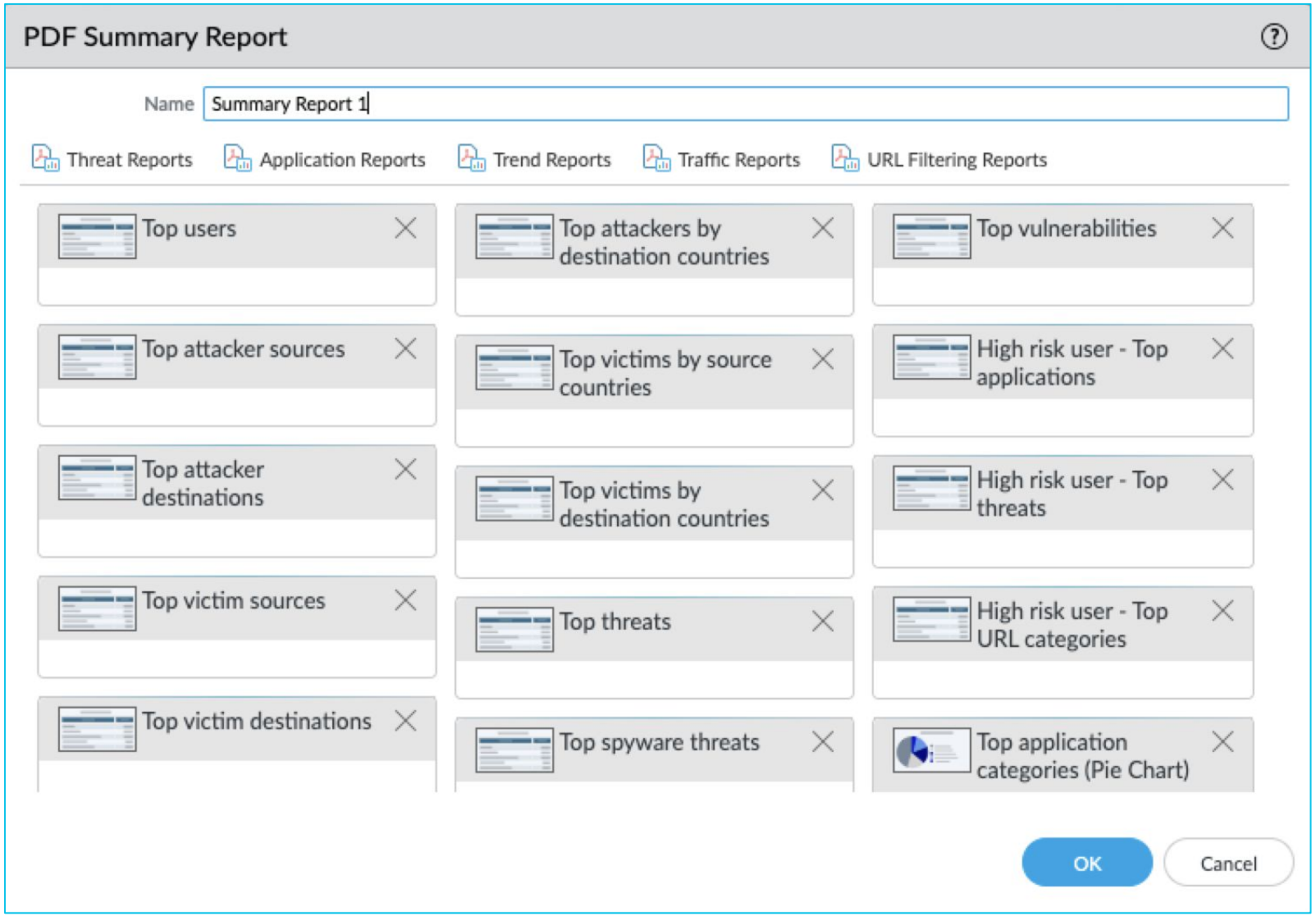
Custom Reports:

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

User/Group Activity Report

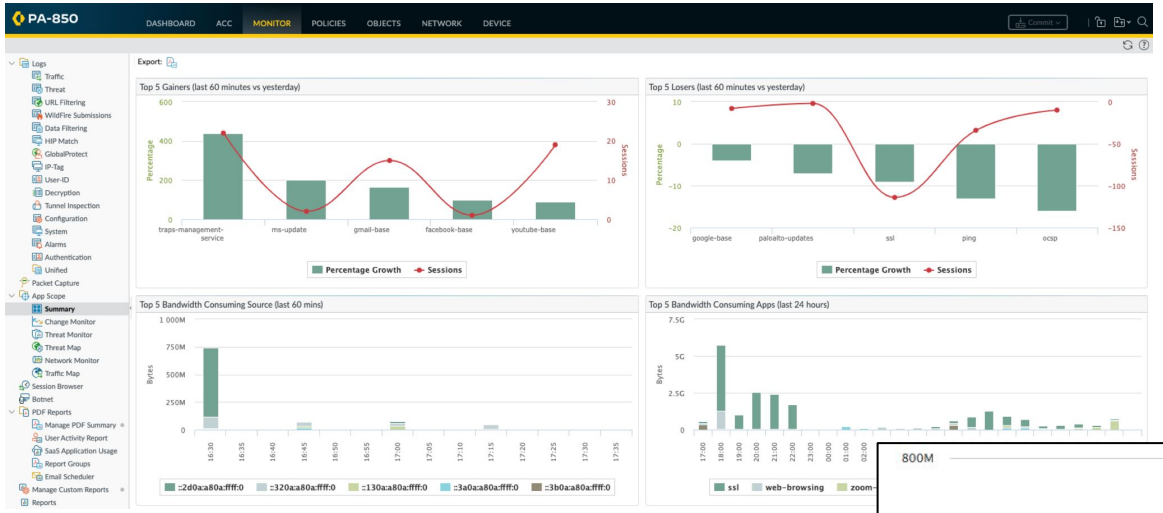
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-and-manage-reports/generate-usergroup-activity-reports.html

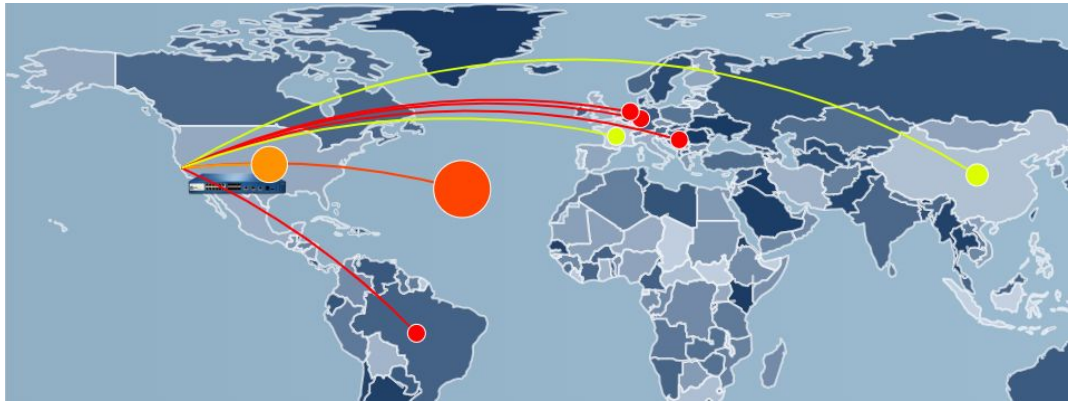
PDF Summary Report

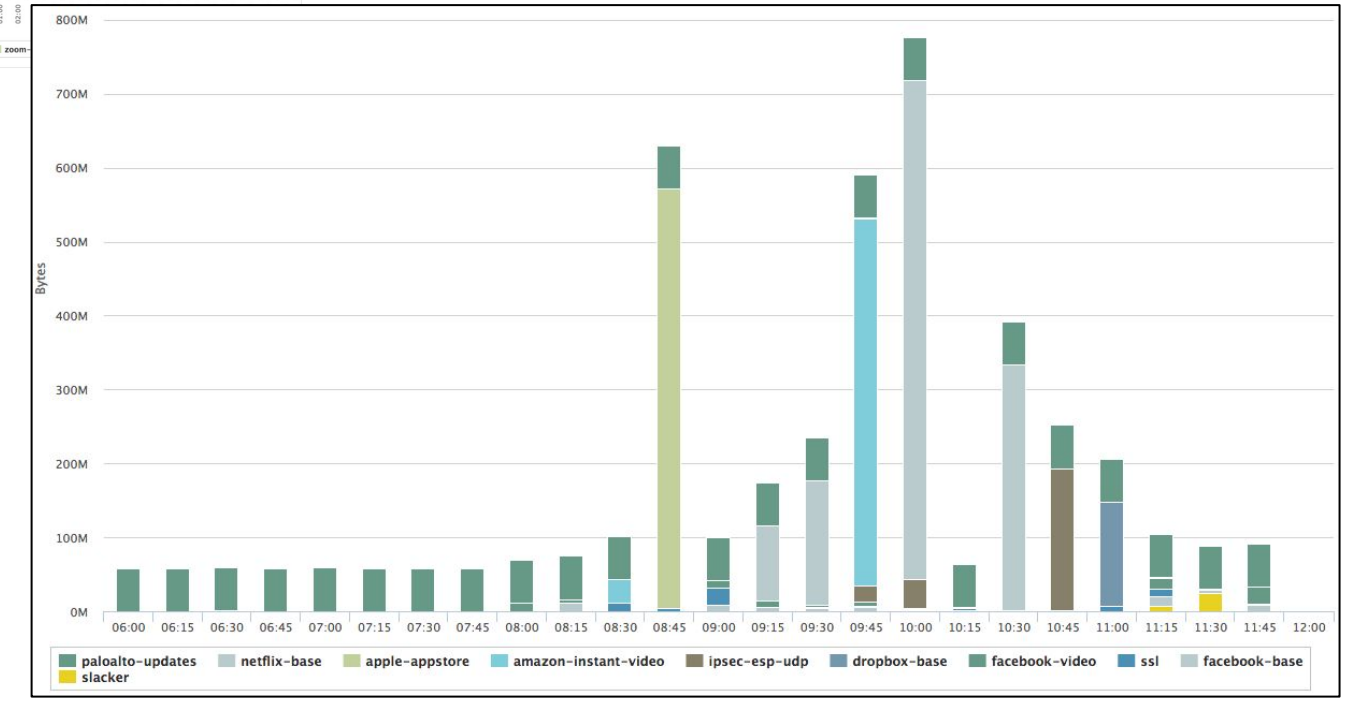


PDF Summary Report :
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-and-manage-reports/manage-pdf-summary-reports.html

App Scope

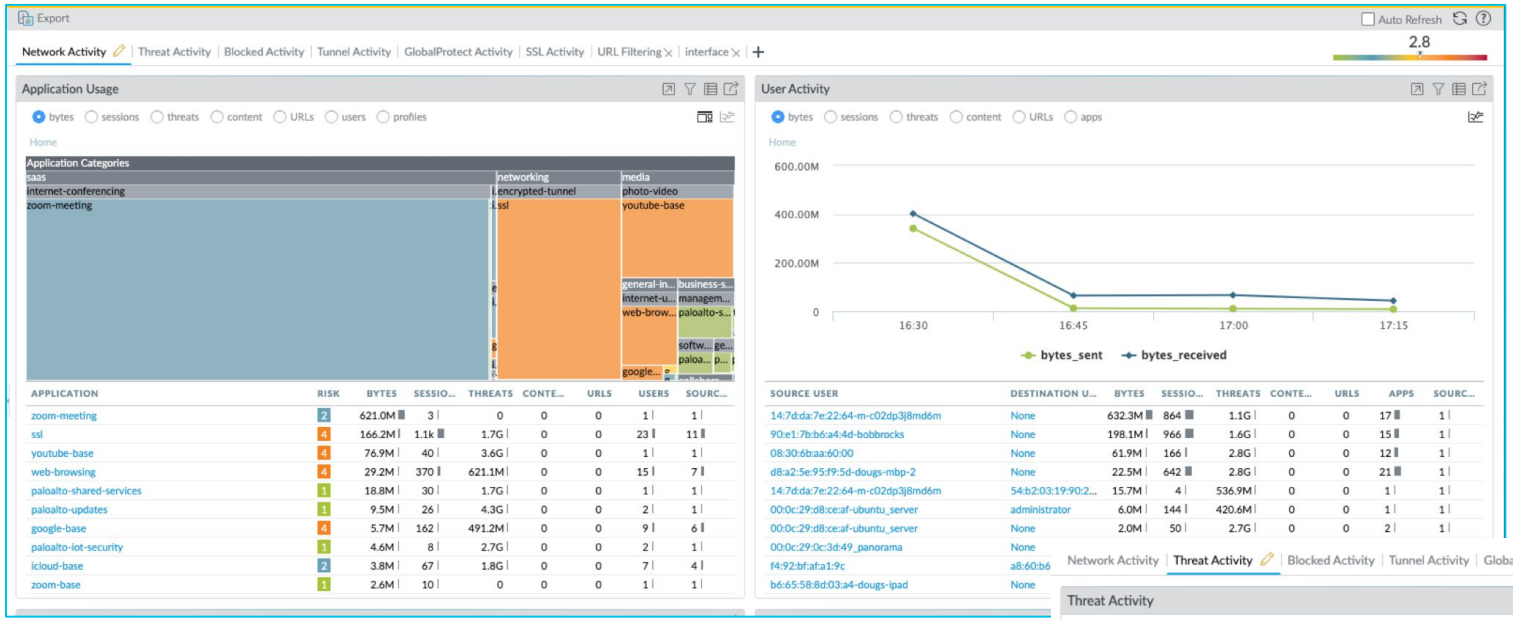


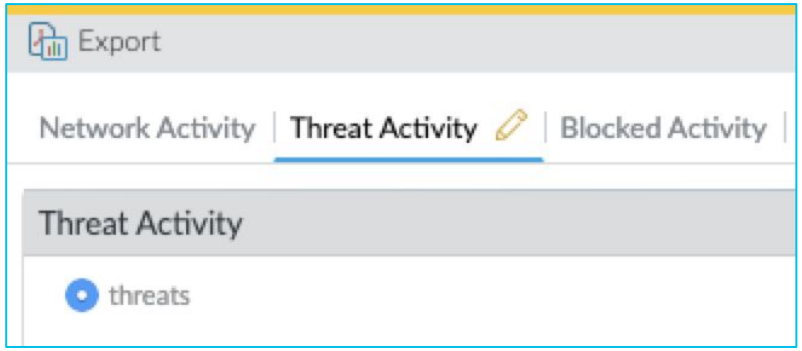


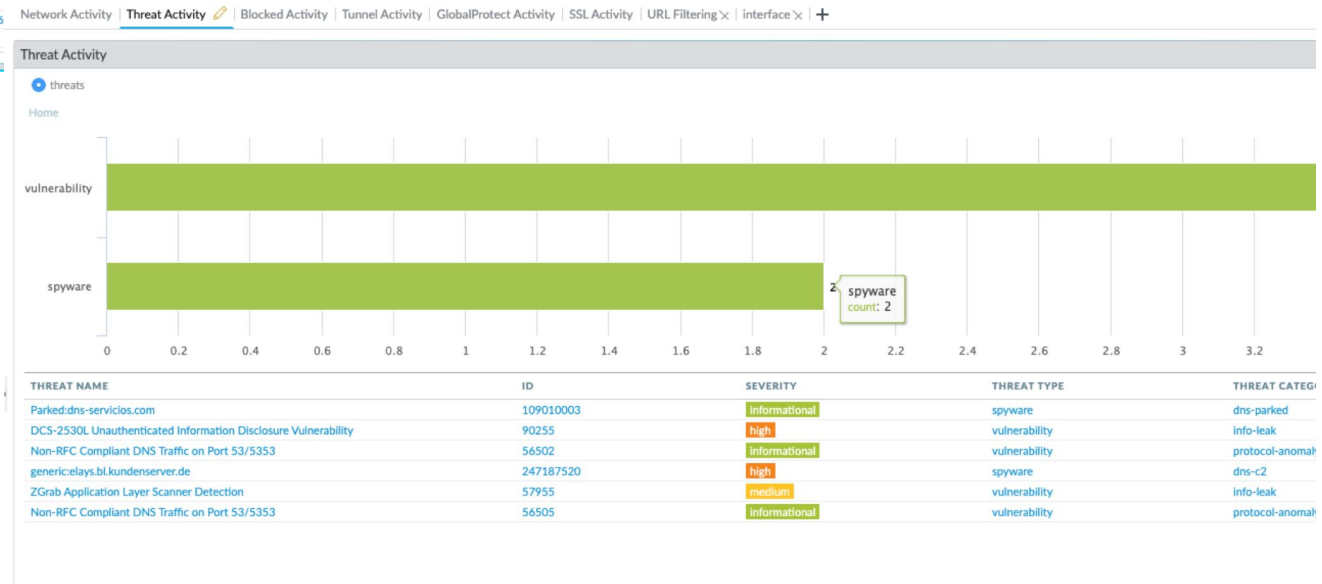


App Scope Reports:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/use-the-app-scope-reports.html

Application Command Center (ACC)



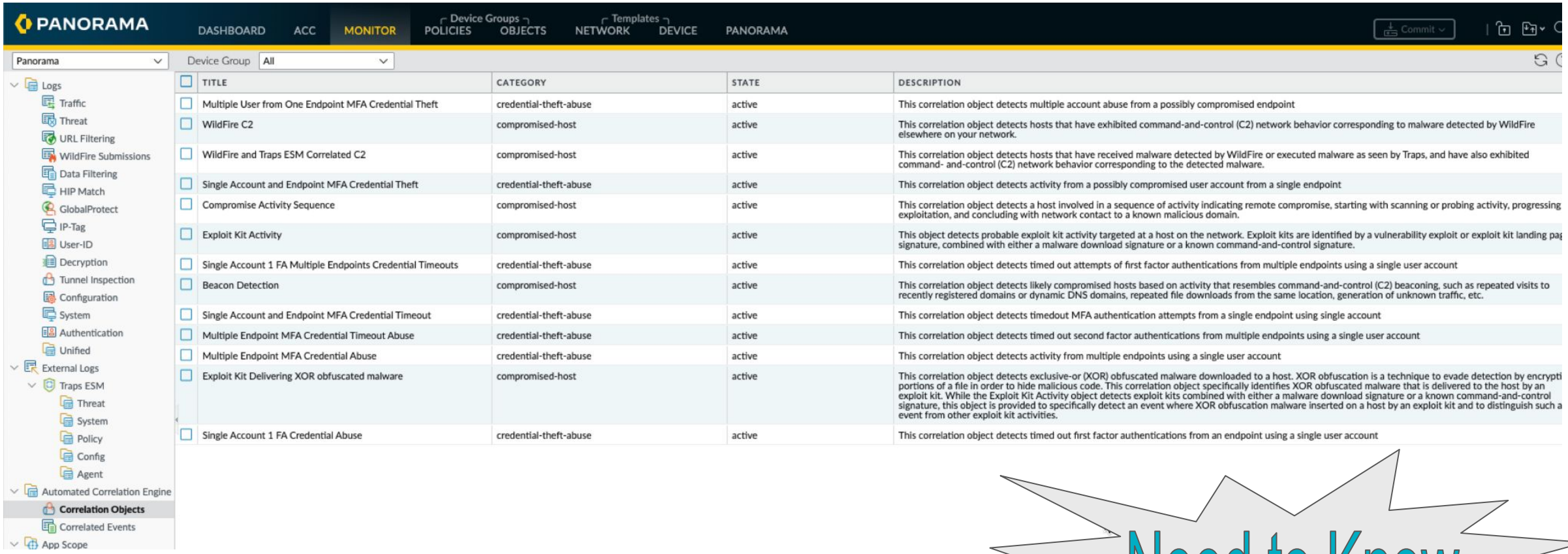




Application Command Center:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/use-the-application-command-center.html

Automated Correlation Engine - *Panorama Only!*

Monitor -> Automated Correlation Engine -> Correlation Objects



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 pag 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 timedout 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 encrypti 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 a 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
```

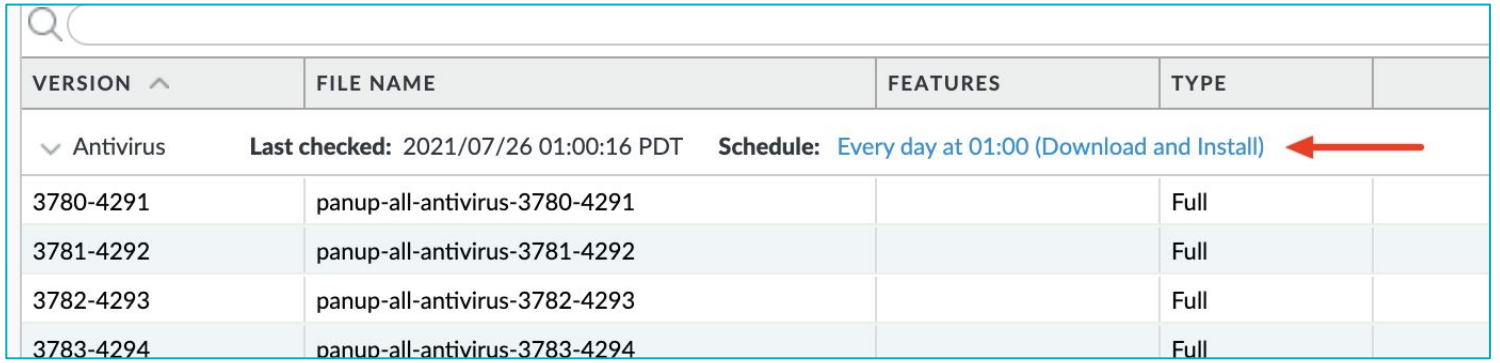
```
admin@PA-851> request content upgrade info

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
```

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

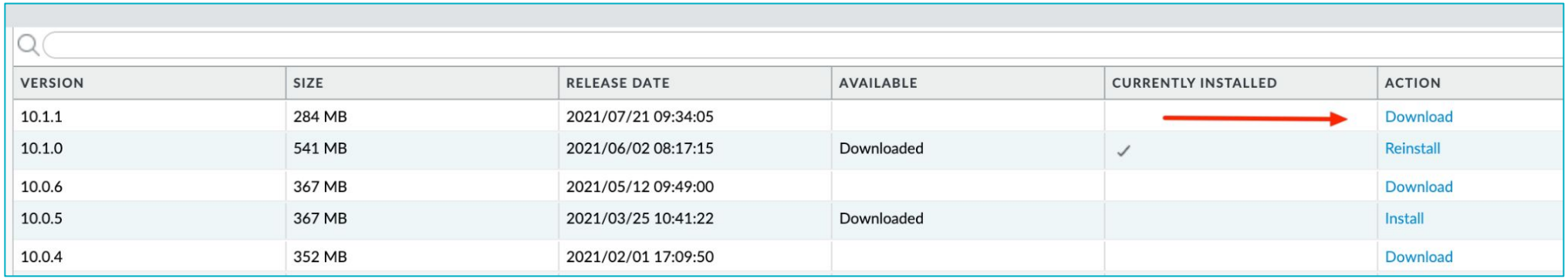
4.2 Plan & Execute the Process to Update a Palo Alto Networks System

4.2.1 Update a Single Firewall

- Focuses on Dynamic Updates and Software Updates
  - Dynamic Updates



  - Software Updates



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.

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?

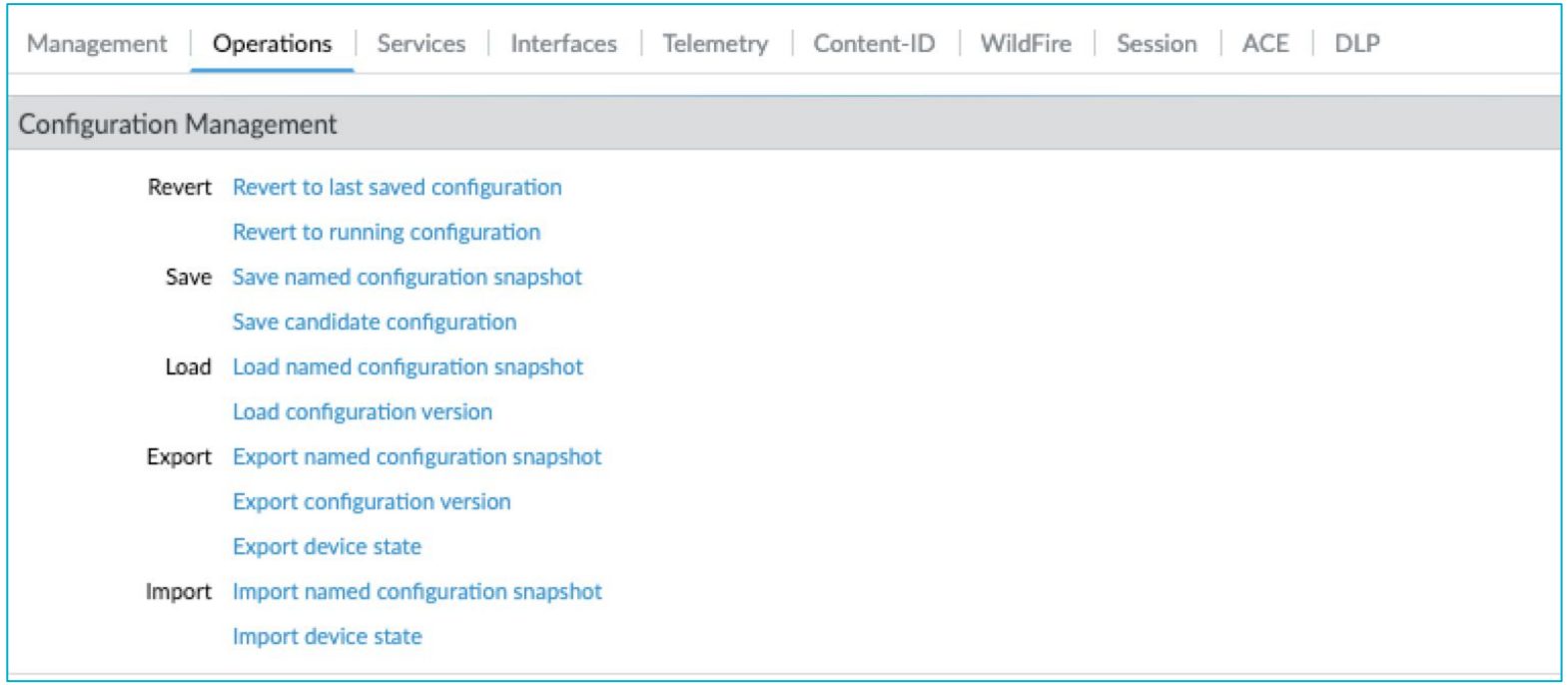
- Download 9.1.0
- Download and install the *preferred* release of 9.1.x
- Reboot
- Download 10.0
- Download and install the *preferred* release of 10.0.x
- Reboot
- Download 10.1.0
- Download and install the *preferred* release of 10.1.x

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

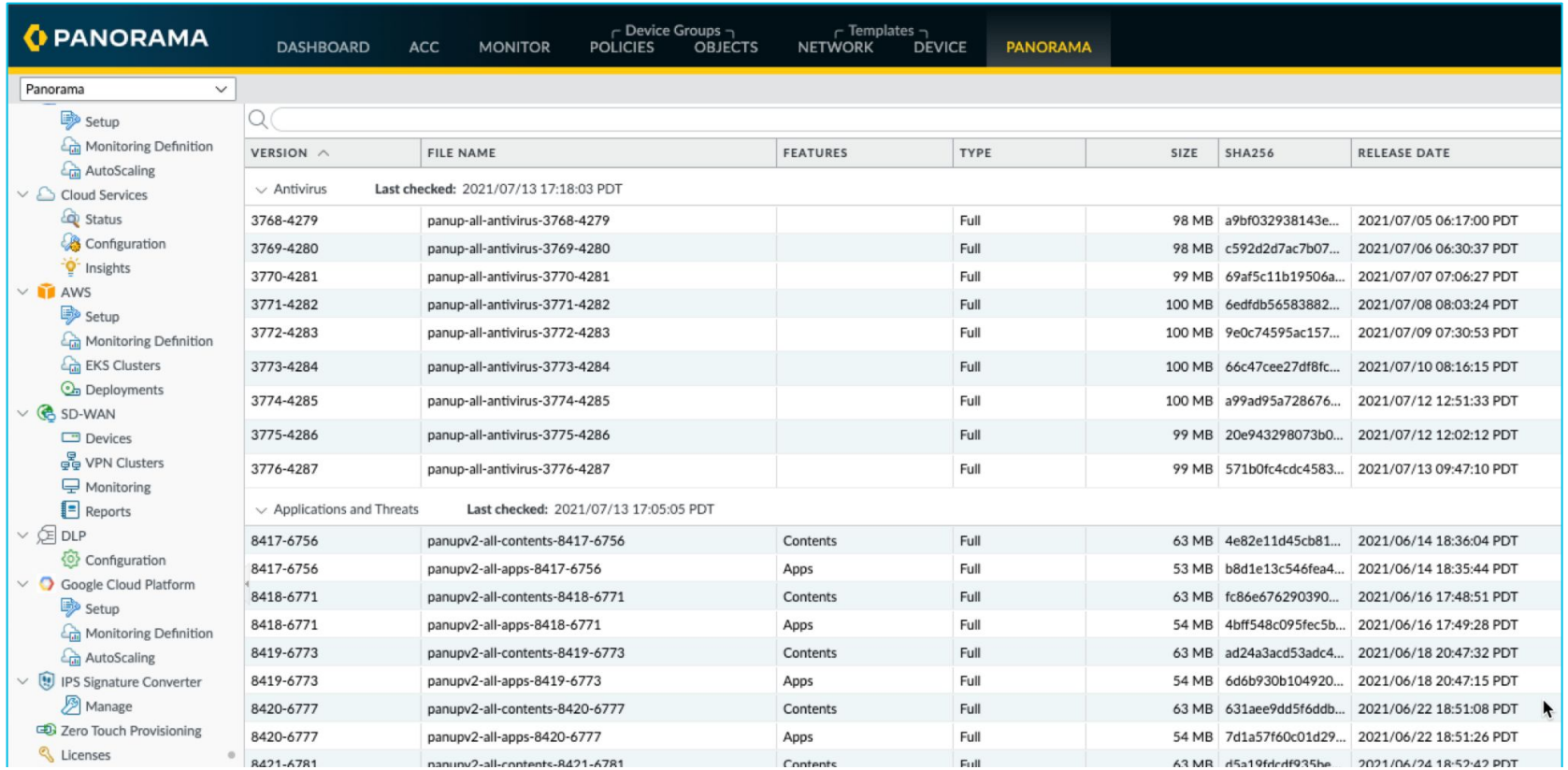
Config Files to grab

- 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=kA10g000000ClRcCAK

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



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	631aee9dd5f6ddb...	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

See previous sections

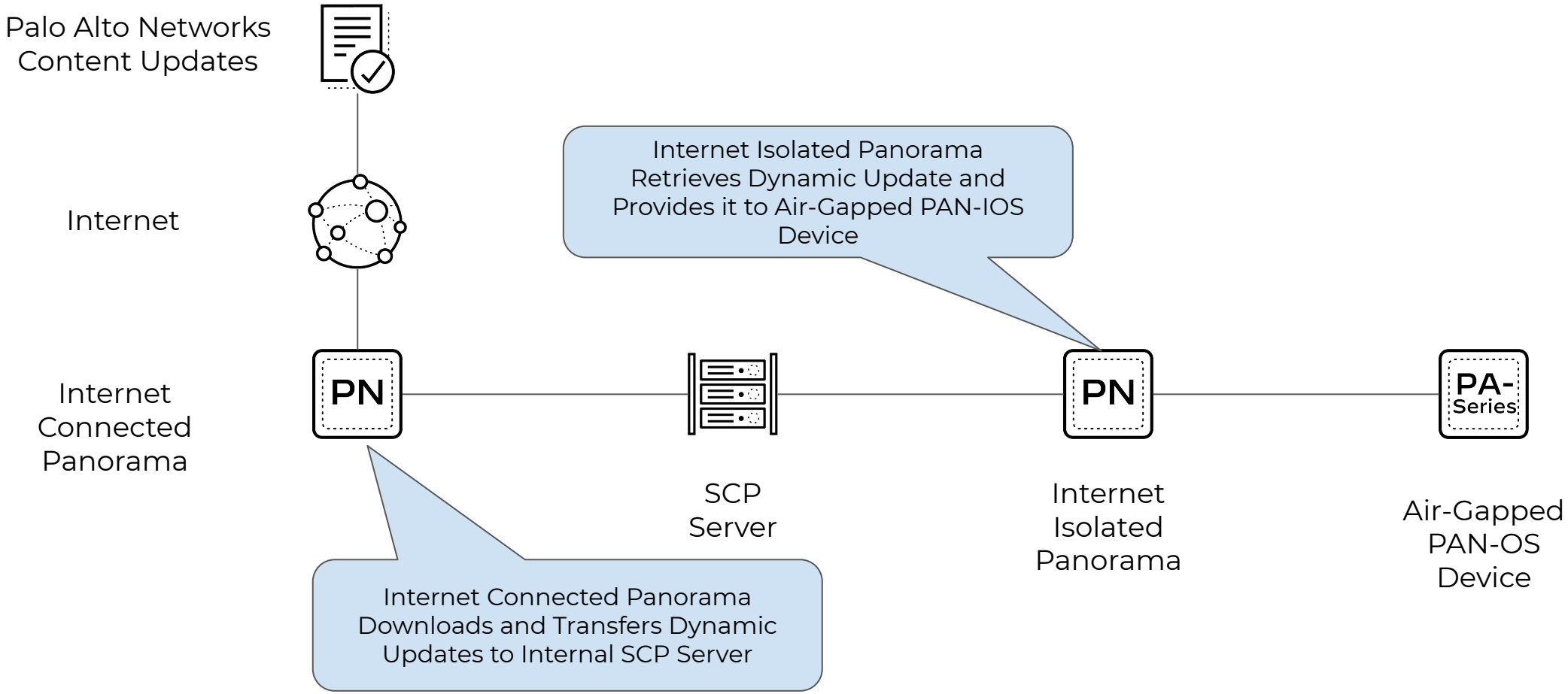
Deploy Upgrades to Firewalls, Log Collectors, and WildFire Appliances Using Panorama

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

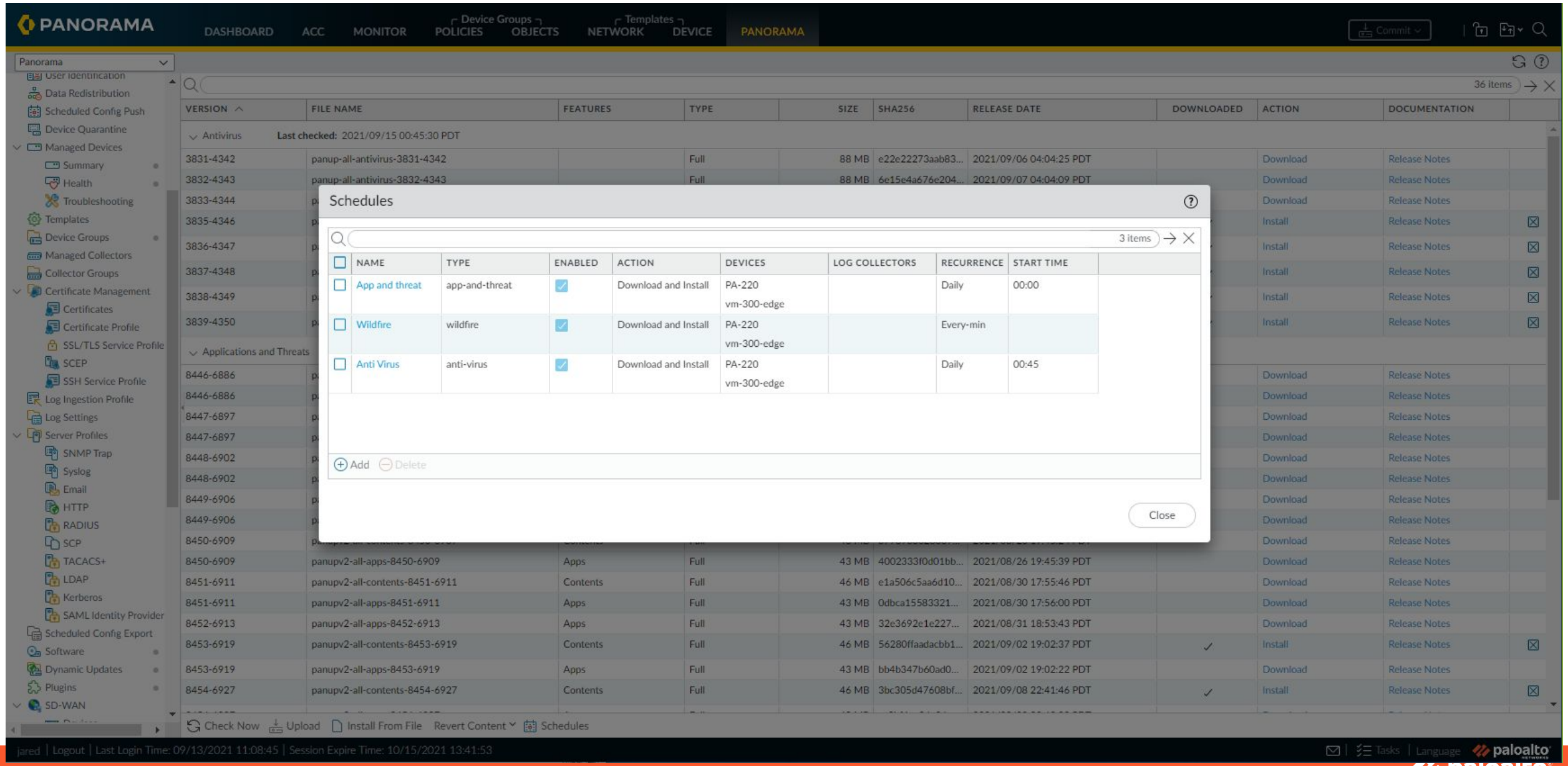
4.2.3 Perform Panorama (Content) Push

Automatic Content Updates Through Offline Panorama

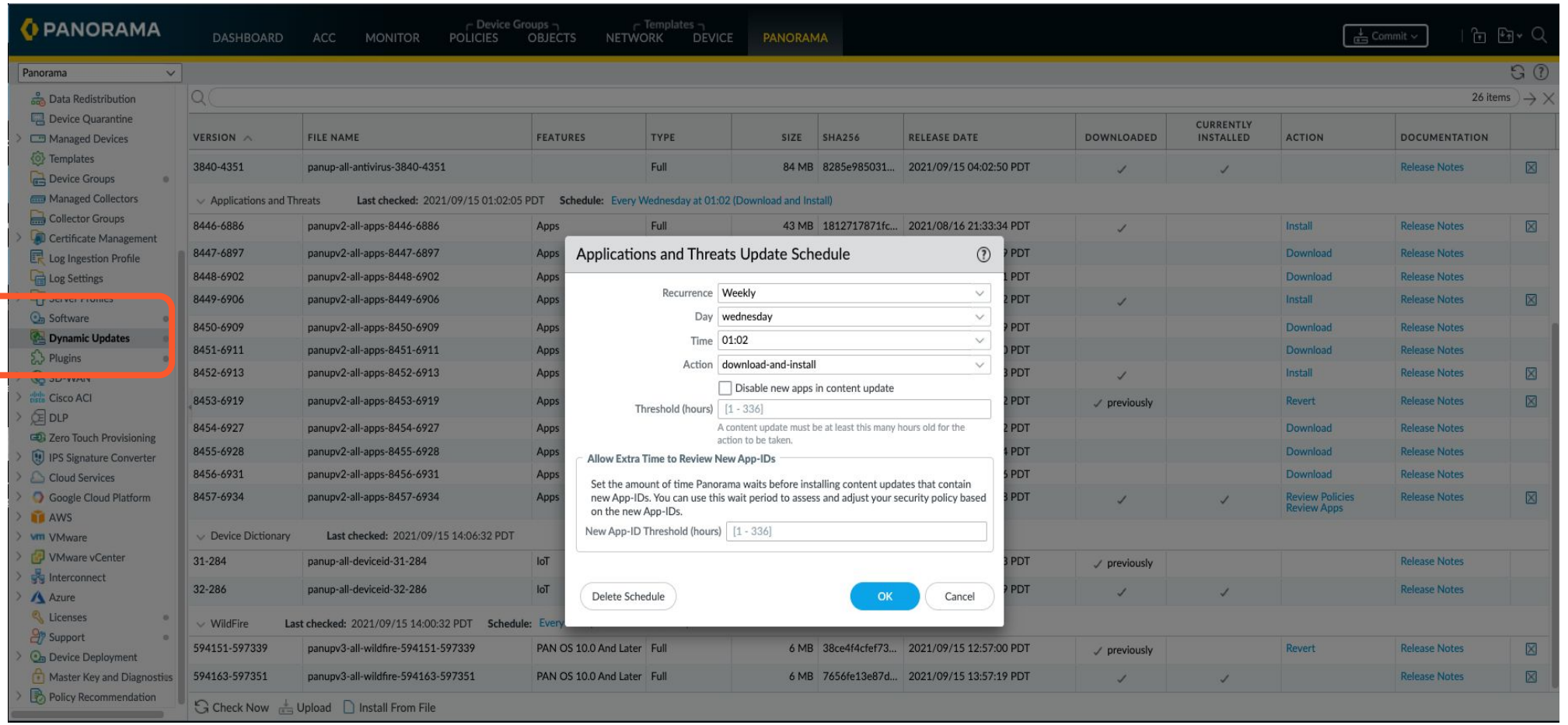
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/panorama-features/automatic-content-updates-through-offline-panorama.html

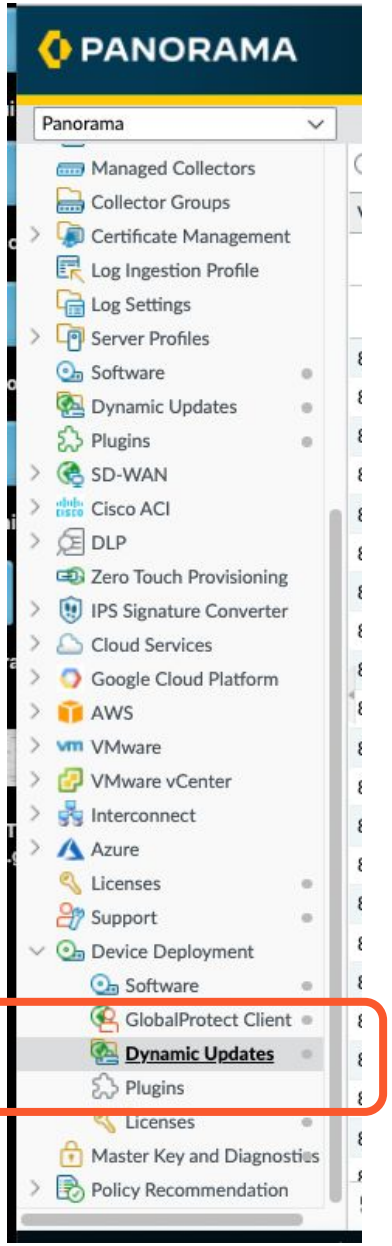


4.2.4 Schedule & Manage Dynamic Updates



4.2.5 Schedule & Manage Dynamic Software Updates





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

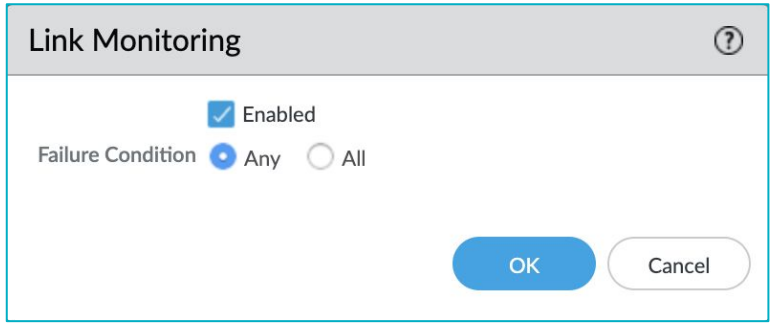
Upgrade Firewalls Using Panorama:
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/upgrade-pan-os/upgrade-the- firewall-pan-os/upgrade-firewalls-using-panorama.html

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

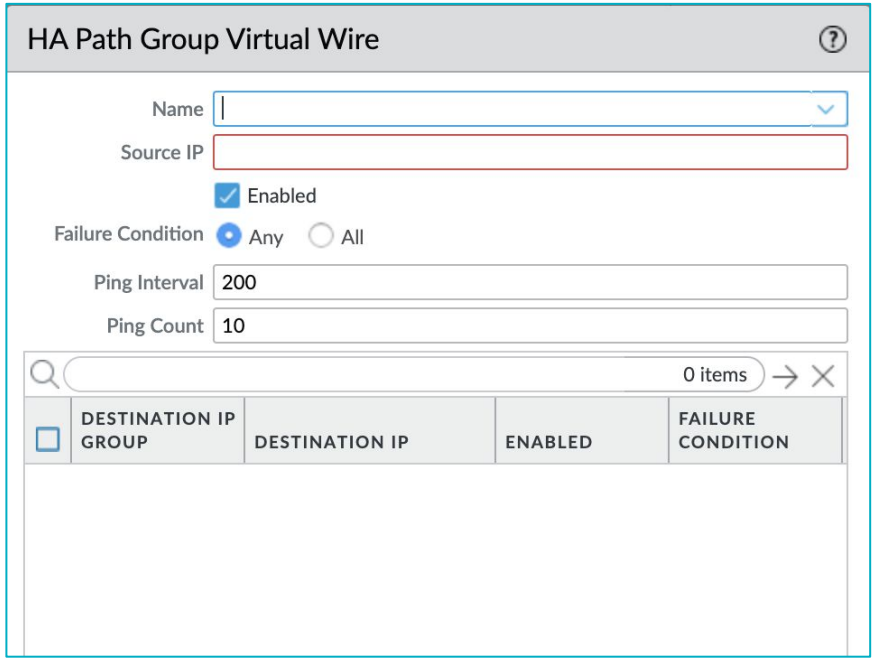
4.3 Manage HA Functions

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**



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.

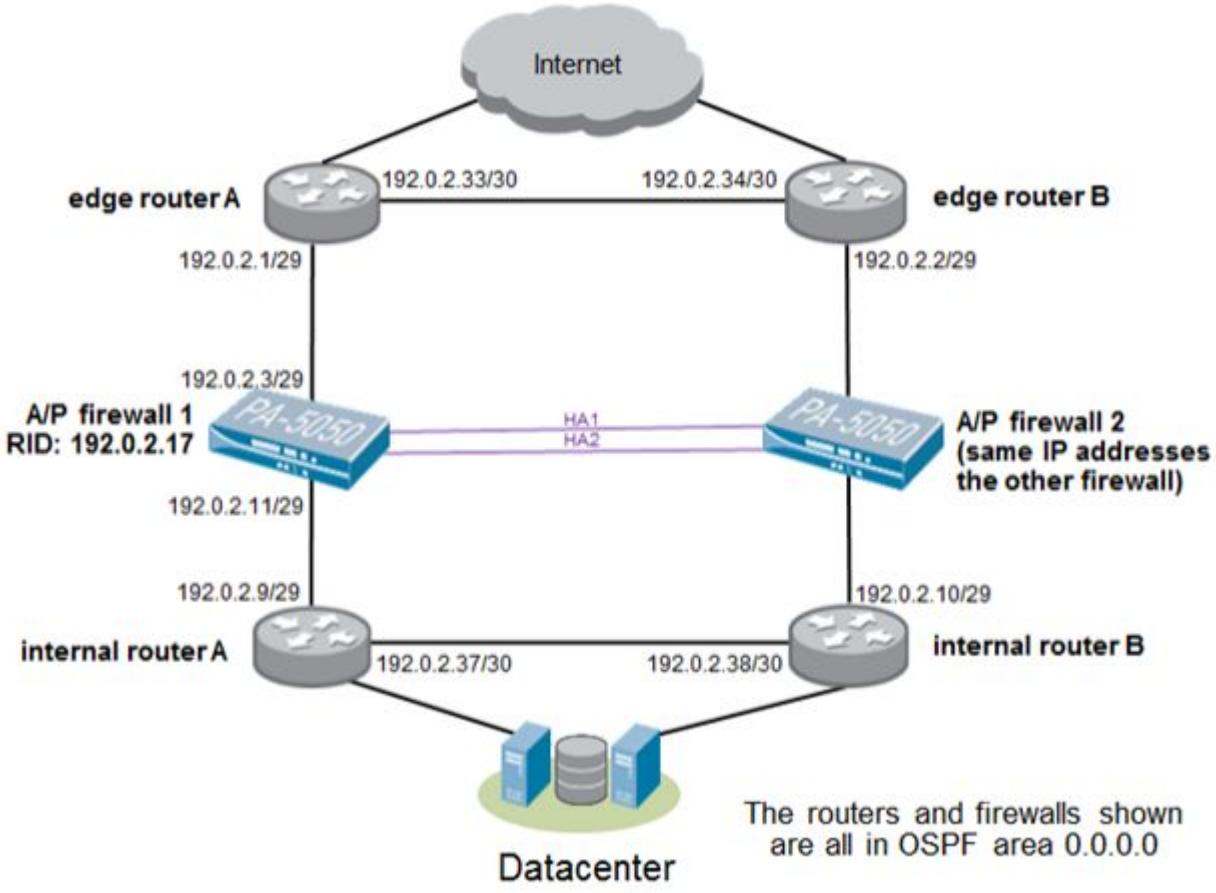
Active/active mode requires advanced design concepts replicating NAT pools, and deploying floating IP addresses to provide proper failover.

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.

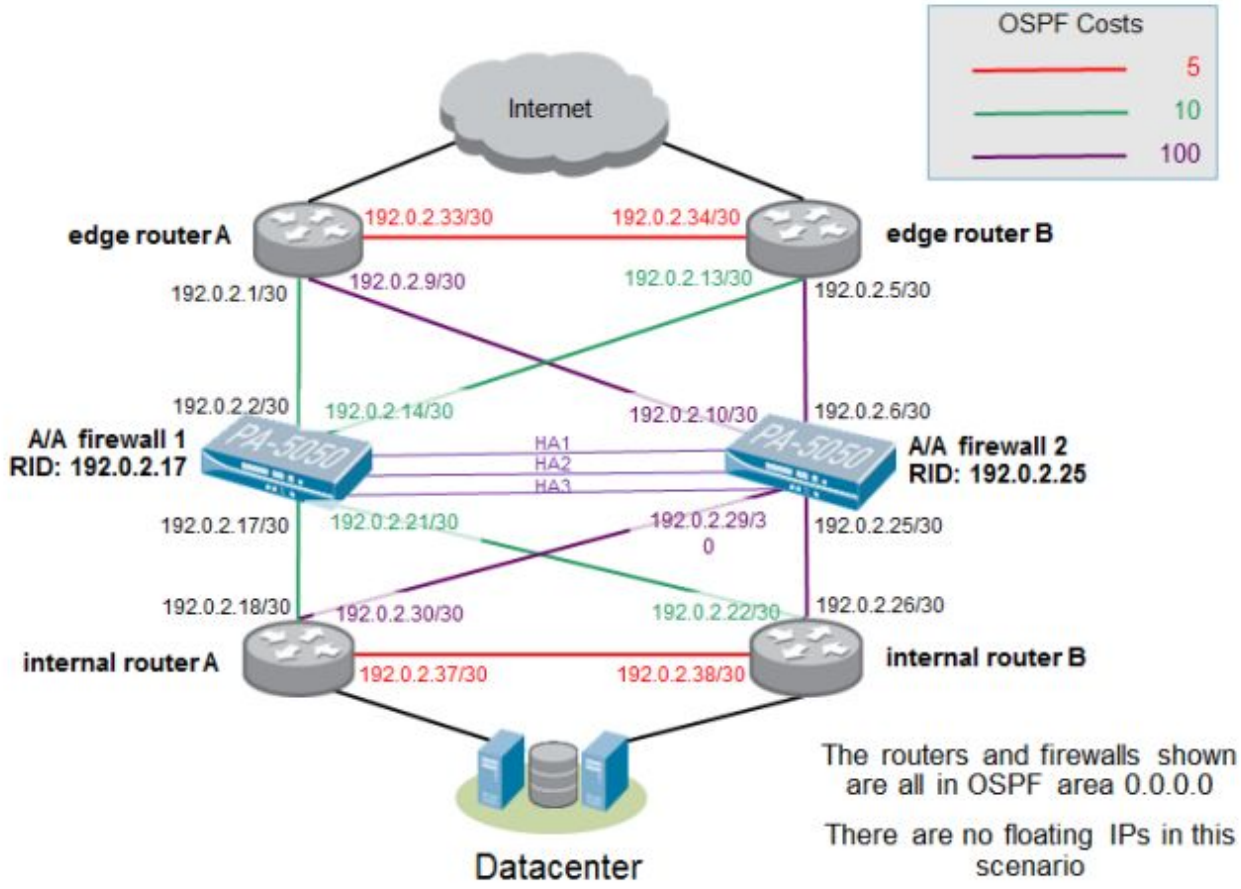
In active/active mode, the HA pair can be used to temporarily process more traffic than what one firewall normally can handle.

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)

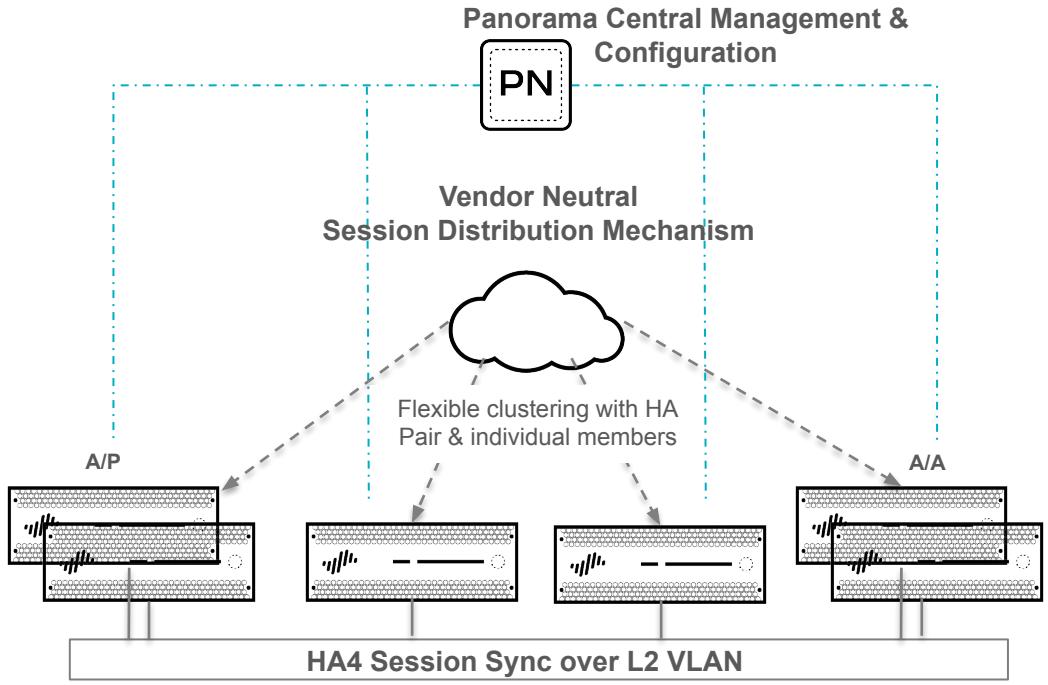


4.3.3 Identify When to Use HA Links (HA1 + HA2 + HA3 Cluster >= NGFW A/A)



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)

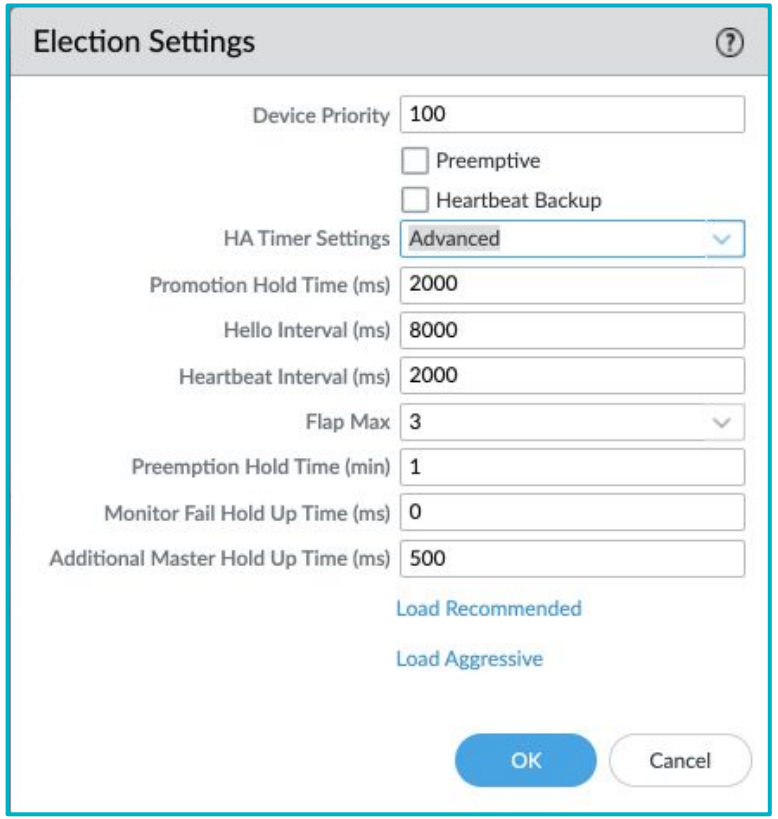
- Support Layer 3 or Vwire
- All firewalls need to be the same model
- Can be a combination of a standalone and an HA pair
- HA-4 performs session sync and will take place over a data interface

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-7000-20GXM-NPC	PA-7080: 4 PA-7050: 6
VM-300	6
VM-500	6
VM-700	16

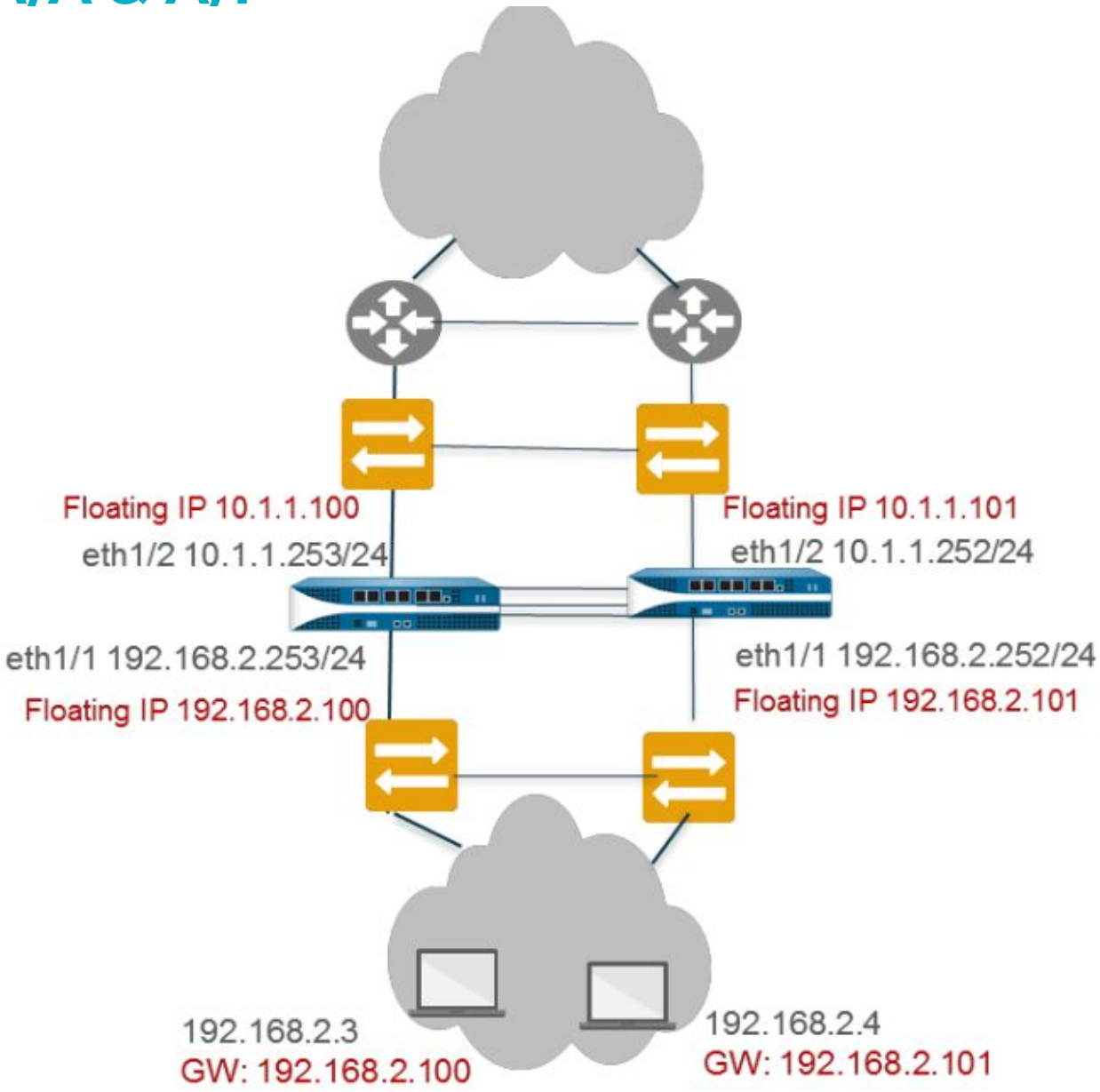
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/high-availability/ha-clustering-best-practices-and-provisioning.html

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	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. ICMP is used to exchange heartbeats between HA peers. Ports used for HA1—TCP port 28769 and 28260 for clear text communication; port 28 for encrypted communication (SSH over TCP). If you enable encryption on the HA1 link, you can also Refresh HA1 SSH Keys and Configure Key Options.
Data Link	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. 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.
HA1 and HA2 Backup Links	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: • The IP addresses of the primary and backup HA links must not overlap each other. • HA backup links must be on a different subnet from the primary HA links. • HA1-backup and HA2-backup ports must be configured on separate physical ports. The HA1-backup link uses port 28770 and 28260. • PA-3200 Series firewalls don't support an IPv6 address for the HA1-backup link; use an IPv4 address. 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.
Packet-Forwarding Link	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.
HA4 Link and HA4 Backup Link	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.

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=kA10g000000ClUzCAK

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=kA10g000000ClXGCA0

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

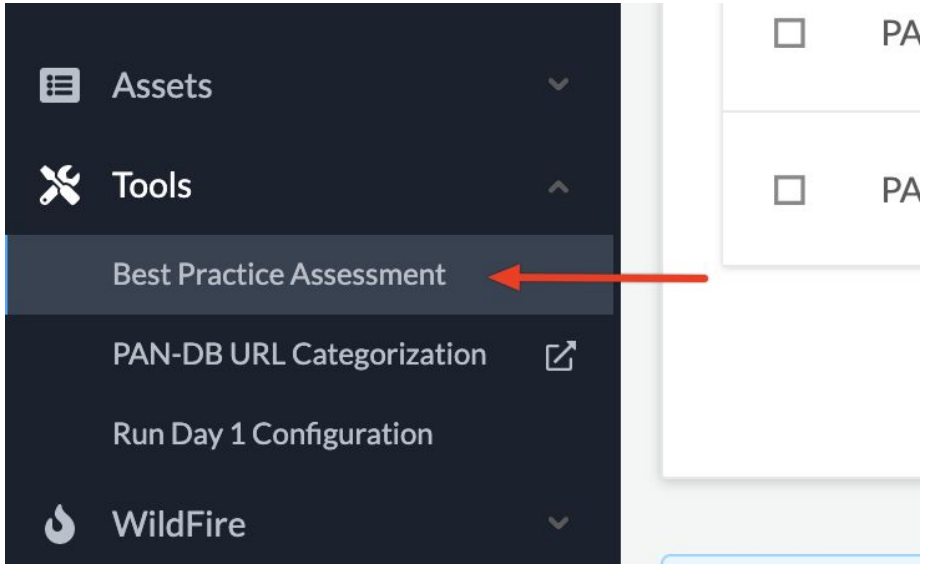
Best Practice Assessment (BPA) tool for Palo Alto Networks firewalls and Panorama evaluates a device's configuration by measuring the adoption rate of a firewall's capabilities, and by validating whether the policies adhere to best practices.

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 Kow 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

paloalto NETWORKS

PCNSE

Thank you!

Exam Domain #4
Manage & Operate