MAINTAIN APPLICATION-BASED POLICIES

THE BEST WAY TO PROTECT THE FUTURE IS TO PREPARE FOR IT

- Migrate to an App-ID-based Security policy
- Maintain an App-ID Security policy
- Maintain App-ID

paloalto NETWORKS

Learning Objectives

After you complete this module,
you should be able to:

- Convert to an application-based Security policy
- Maintain an application-based Security policy
- Maintain an optimal App-ID configuration on your firewall

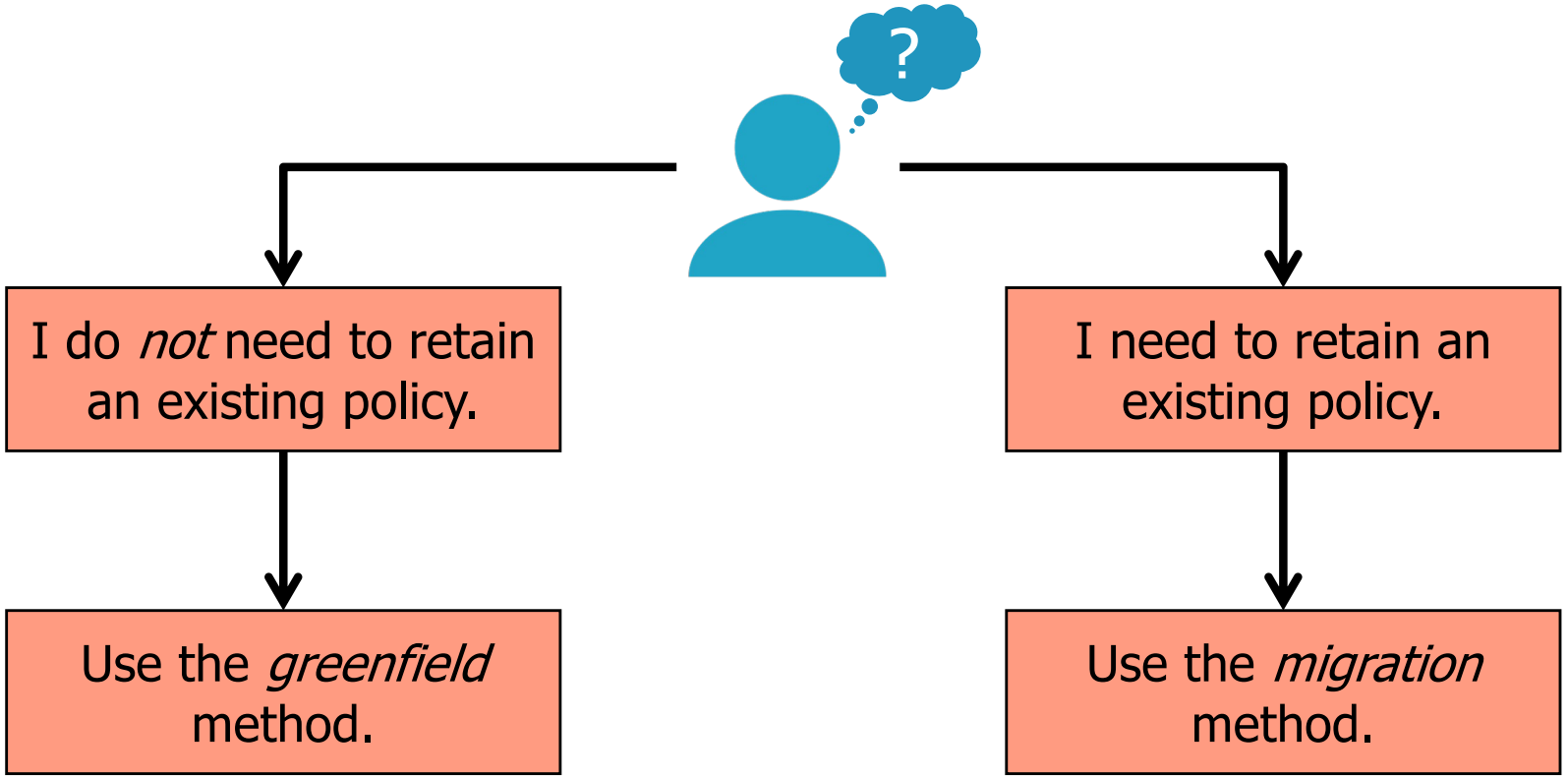
Migrate to an App-ID-based Security policy

Maintain an App-ID Security policy

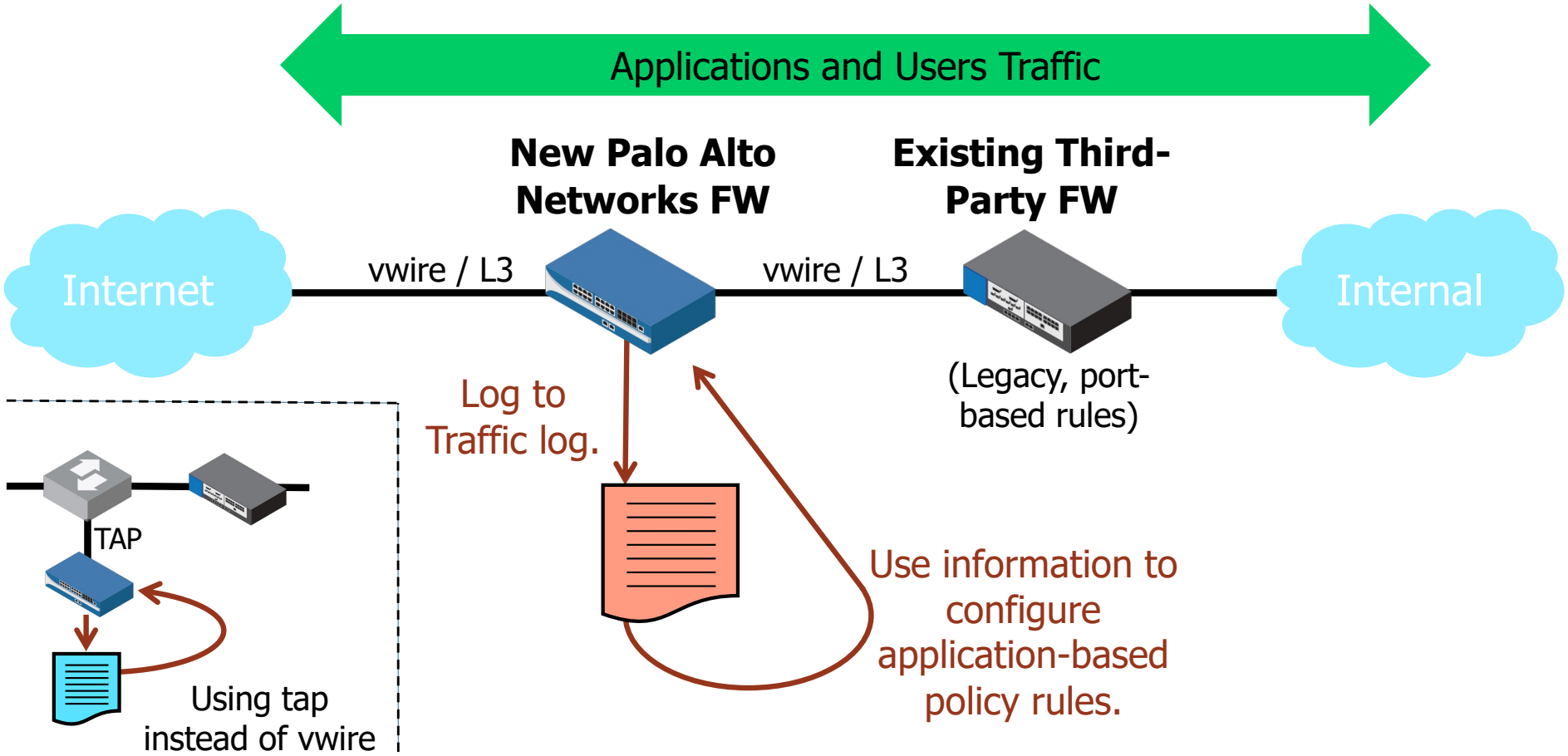
Maintain App-ID

paloalto NETWORKS

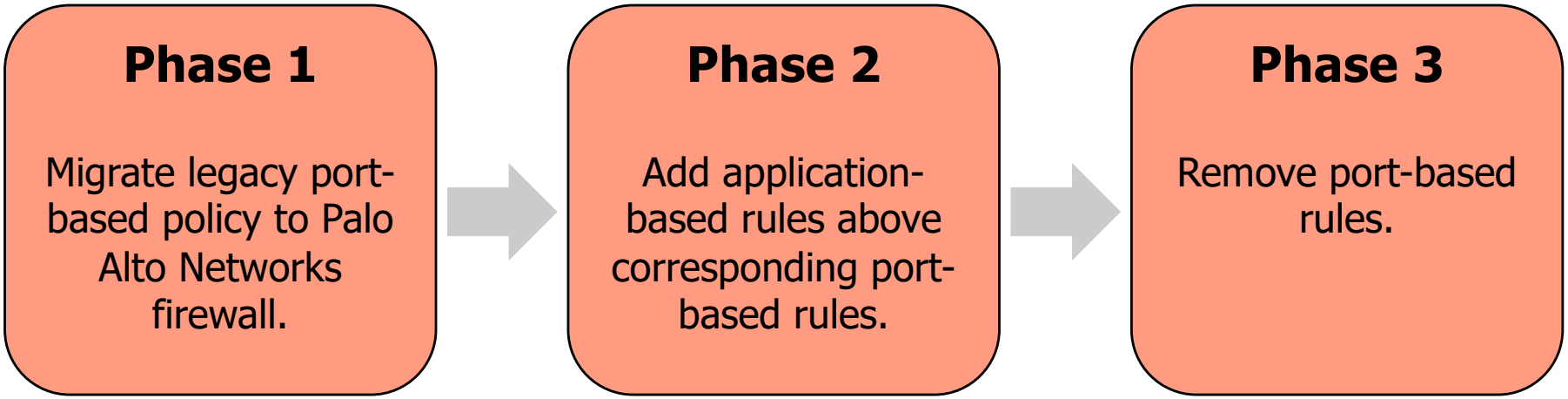
Moving to Application-Based Policies



Greenfield Example



Example Migration Method: Overview



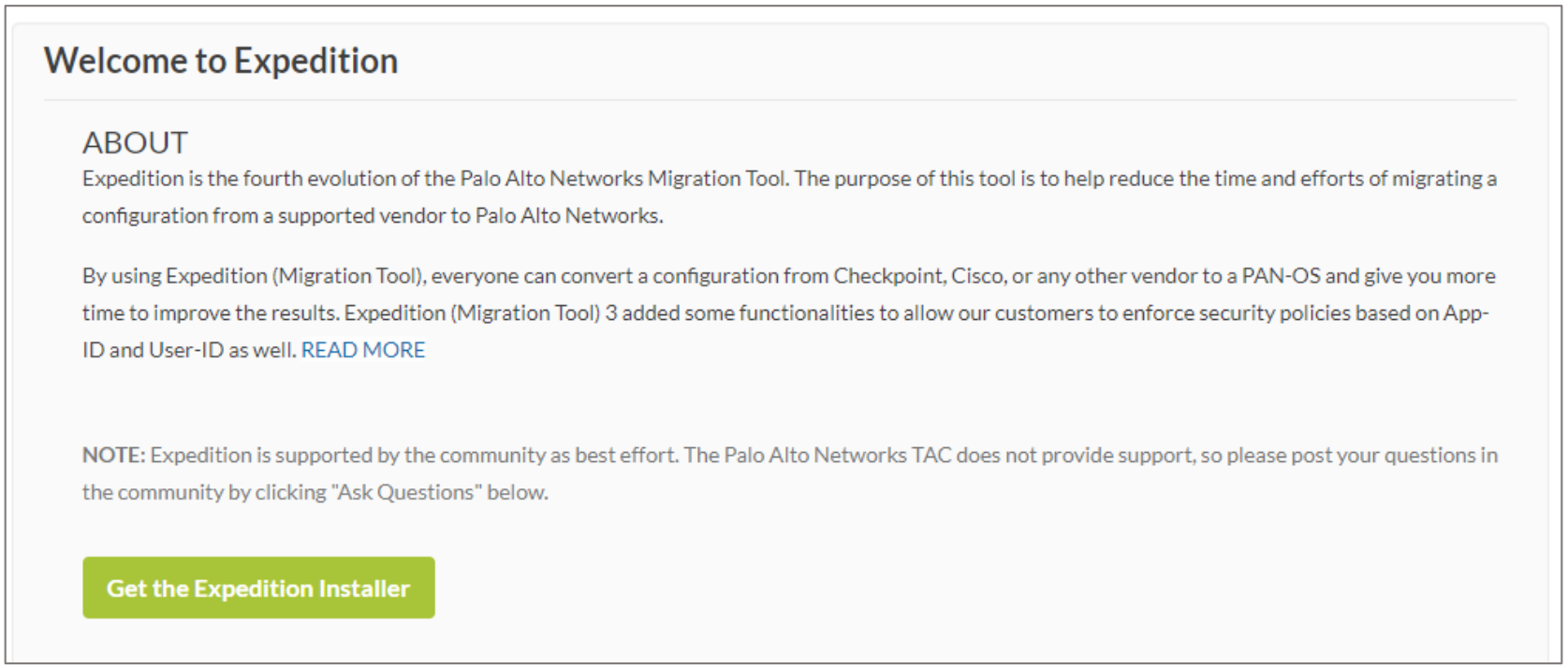
Goals:
- Successful cutover.
- Minimize user issues.
- Capture application traffic.

Goals:
- Reduce the attack surface.
- Remove *unknown* applications as soon as possible.

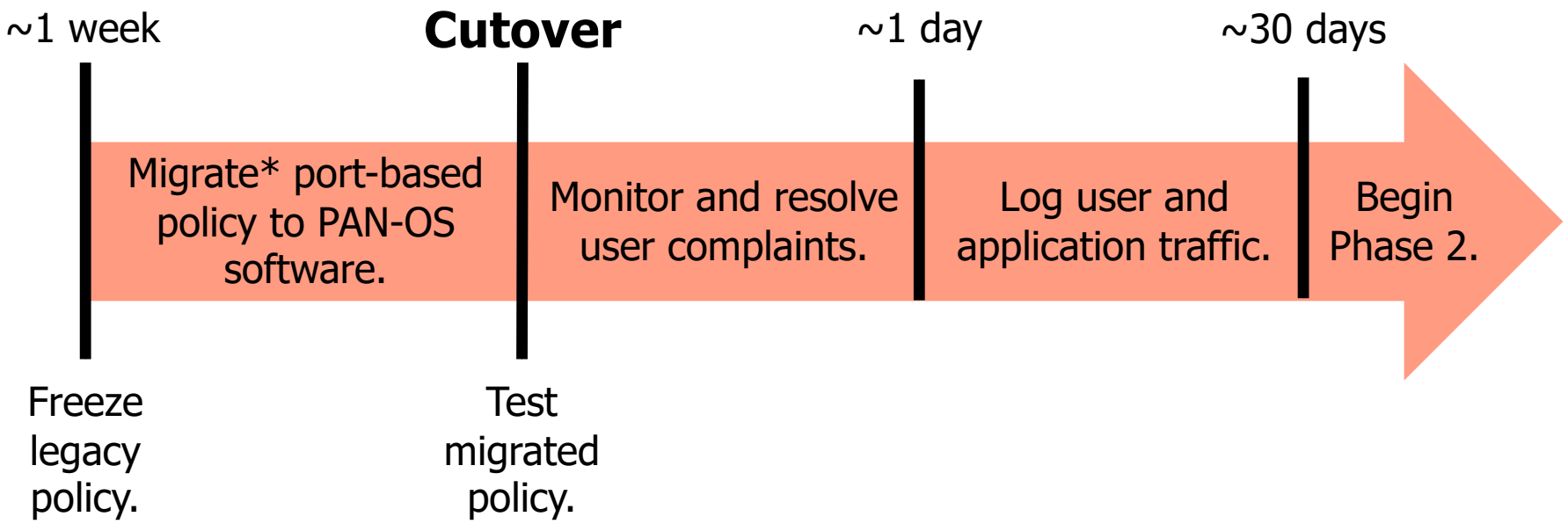
Goals:
- Complete policy migration.

Expedition (Migration Tool)

- Migrate policy from a pre-existing firewall.
- https://live.paloaltonetworks.com/t5/expedition-migration-tool/ct-p/migration_tool



Phase 1: Migrate Port-Based Rules



*Expedition tool provides some automation.

Phase 2: View Data of Port-Based Rules

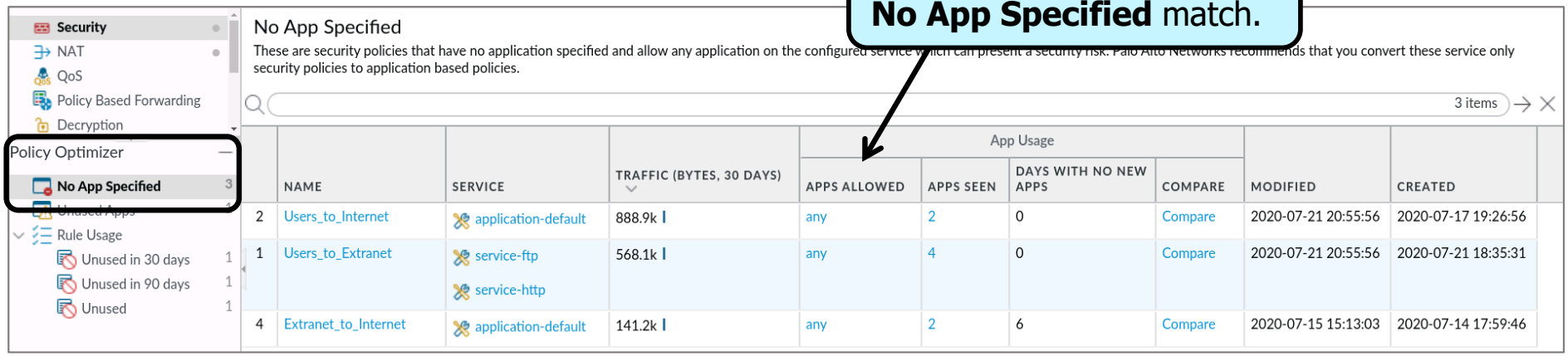
Use **No App Specified** to discover port-based rules.

Policies > Security

	NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION
				ZONE	ADDRESS	USER	ZONE	ADDRESS				
1	Users_to_Internet	Users_Net	universal	Users_Net	any	any	Extranet	any	any	service-ftp service-http	any	Allow

Policies > Security > Policy Optimizer > No App Specified

Application "any" triggers **No App Specified** match.

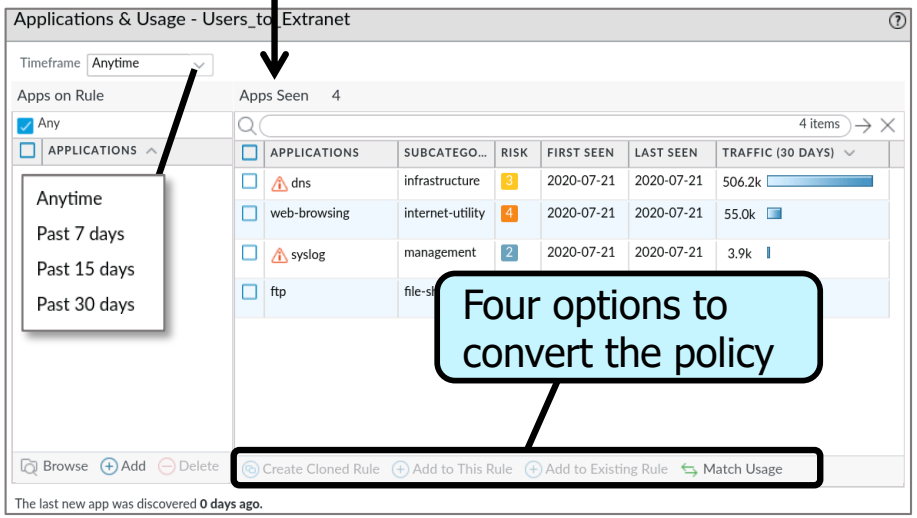


Phase 2: Discover Applications Matching a Port-Based Rule

Policies > Security > Policy Optimizer > No App Specified

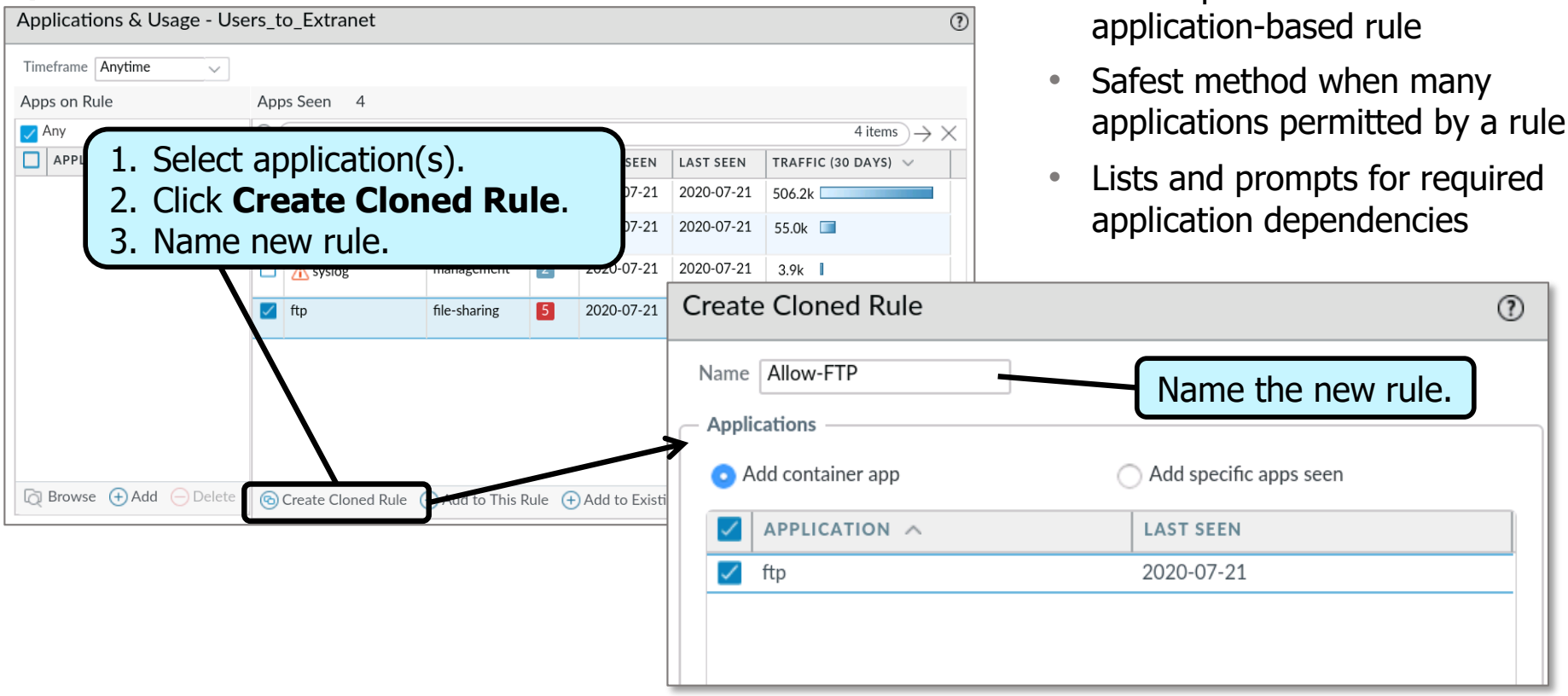
	NAME	SERVICE	TRAFFIC (BYTES, 30 DAYS)	App Usage				MODIFIED	CREATED
				APPS ALLOWED	APPS SEEN	DAYS WITH NO NEW APPS	COMPARE		
2	Users_to_Internet	application-default	888.9k	any	2	0	Compare	2020-07-21 20:55:56	2020-07-17 19:26:56
1	Users_to_Extranet	service-ftp service-http	568.1k	any	4	0	Compare	2020-07-21 20:55:56	2020-07-21 18:35:31
4	Extranet_to_Internet	application-default	141.2k	any	2	6	Compare	2020-07-15 15:13:03	2020-07-14 17:59:46

- Click **App Seen** number or **Compare** to view any applications that matched the port-based rule.
- The firewall displays a list of applications seen and identified by a rule.
- Use applications listed to create application-based rule(s).



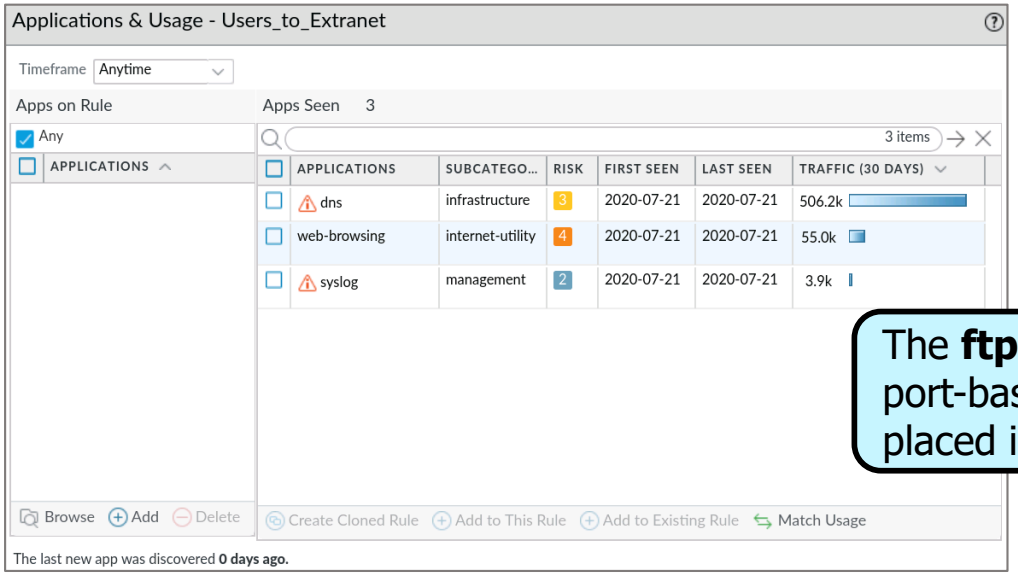
Phase 2: Clone a Port-Based Rule Using "Create Cloned Rule"

Option 1 of 4:



- *Clones* port-based rule to new application-based rule
- Safest method when many applications permitted by a rule
- Lists and prompts for required application dependencies

Result of "Create Cloned Rule"



The **ftp** application is removed from the port-based rule **Apps Seen** list and placed in a new rule.

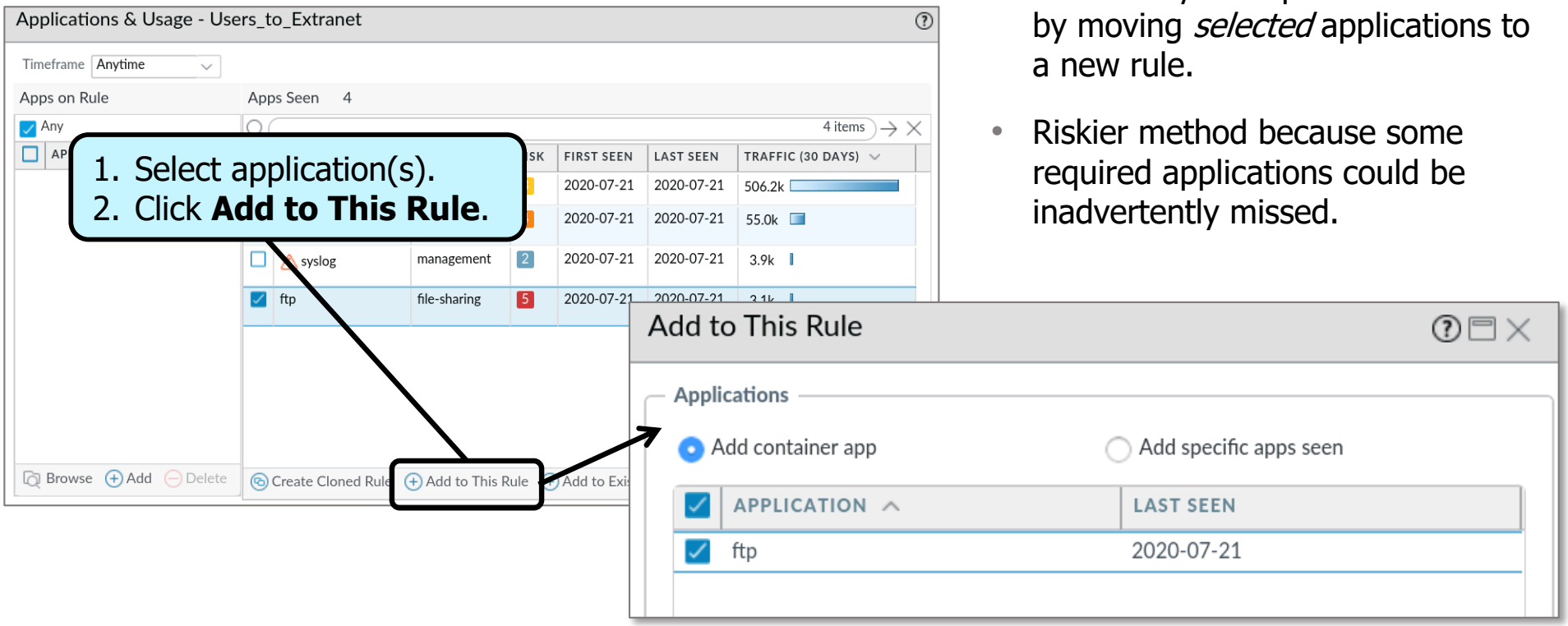
Must manually configure as **application-default**

Policies > Security

	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION
1	Allow-FTP	Users_Net	universal	Users_Net	any	any	Extranet	any	ftp	service-ftp	any	Allow
2	Users_to_Extranet	Users_Net	universal	Users_Net	any	any	Extranet	any	any	service-ftp service-http	any	Allow

Phase 2: Replace a Port-Based Rule Using "Add to This Rule"

Option 2 of 4:



- Firewall *replaces* port-based rule by moving *selected* applications to a new rule.
- Riskier method because some required applications could be inadvertently missed.

Result of "Add to This Rule"

Policies > Security

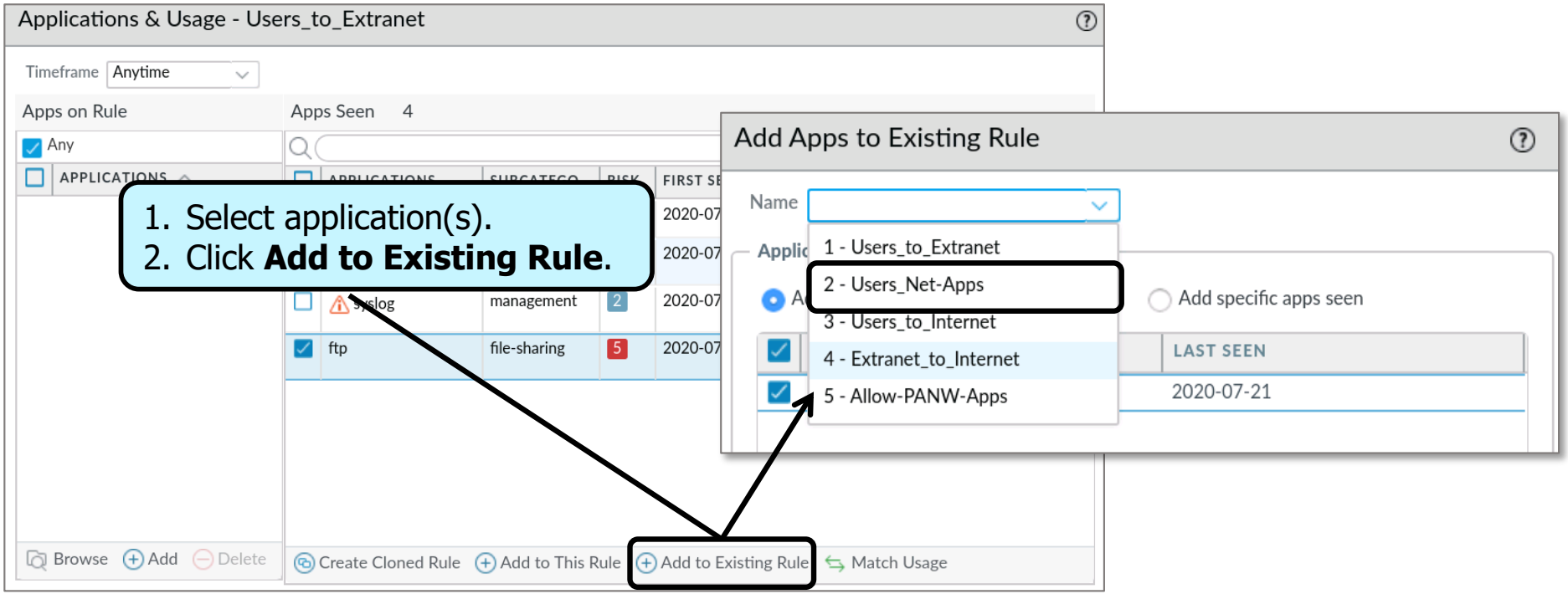
	NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION
				ZONE	ADDRESS	USER	ZONE	ADDRESS				
1	Users_to_Extranet	Users_Net	universal	Users_Net	any	any	Extranet	any	ftp	service-ftp service-http	any	Allow

Must manually configure as **application-default**

New application-based rule *replaces* port-based rule.

Phase 2: Replace a Port-Based Rule Using "Add to Existing Rule"

Option 3 of 4:



Result of "Add to Existing Rule"

Policies > Security

	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION
1	Users_to_Extranet	Users_Net	universal	Users_Net	any	any	Extranet	any	any	service-ftp service-http	any	Allow
2	Users_Net-Apps	Users_Net	universal	Users_Net	any	any	Extranet	any	dns ftp ssh ssl	application-default	any	Allow

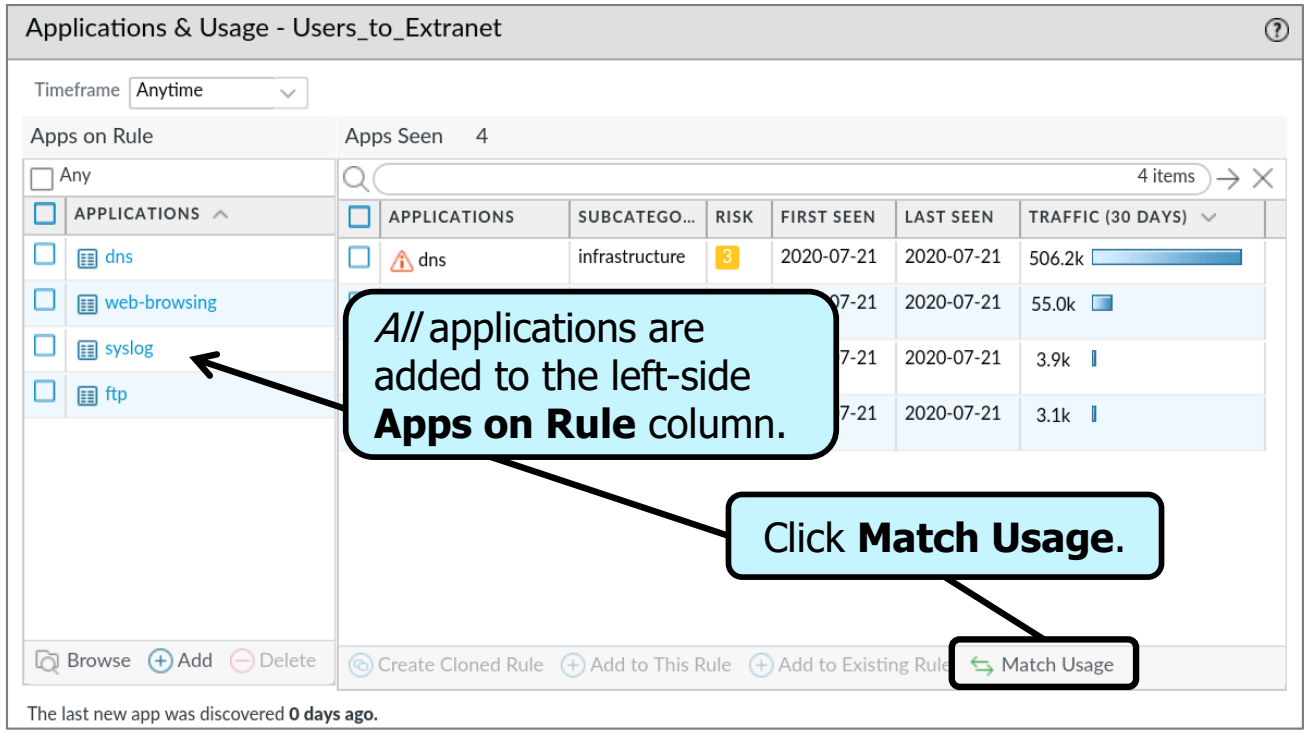
No change to port-based rule

Existing internal-apps rule *modified* to include ftp application

Existing rule was already configured for **application-default**.

Phase 2: Replace a Port-Based Rule Using "Match Usage"

Option 4 of 4:



- Use only when the rule matches a small number of legitimate applications.
- Copies *all* applications under **Apps Seen** to **Apps on Rule**.
- Firewall *replaces* port-based rule with application-based rule.

Result of "Match Usage"

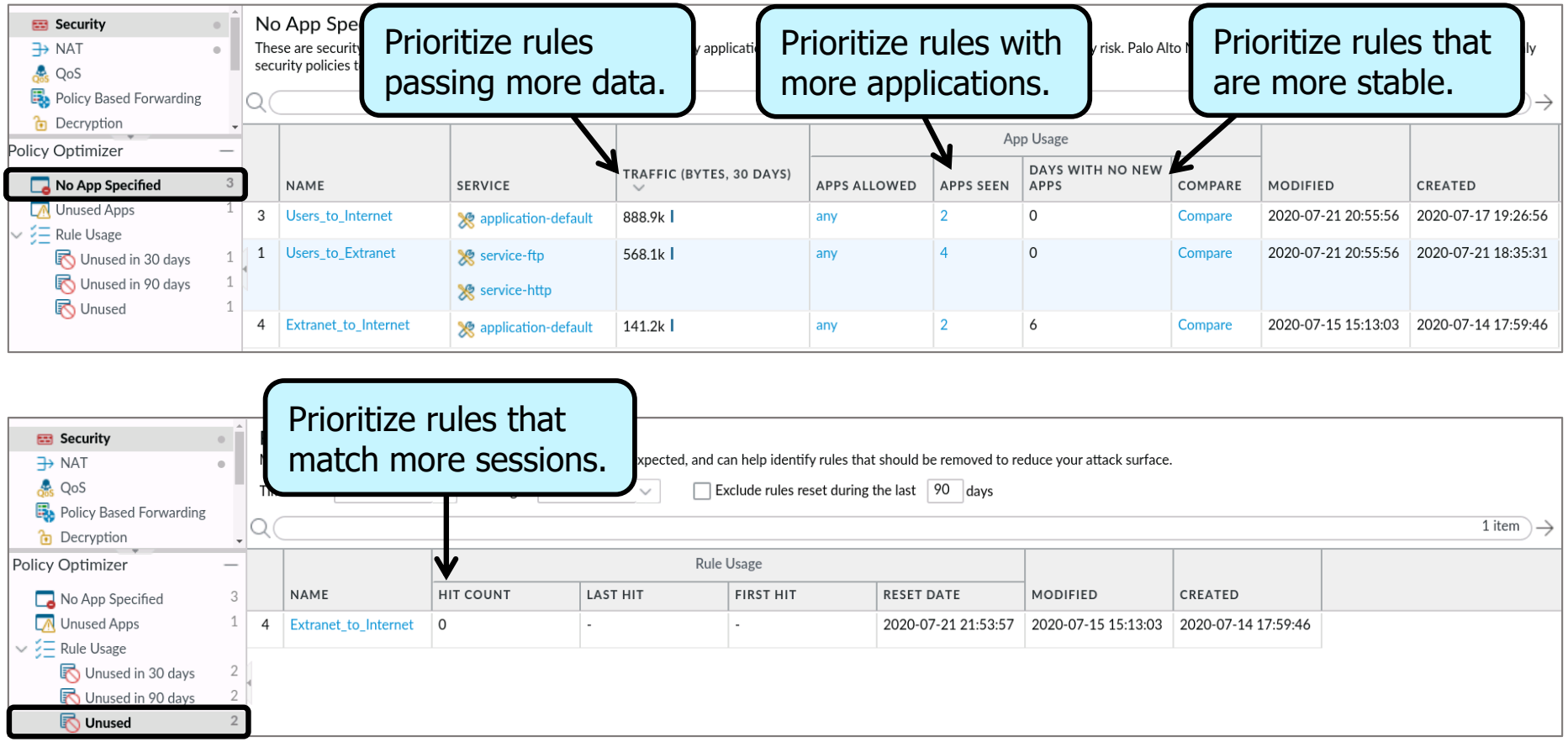
Must manually configure as **application-default**

Policies > Security

	NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION
				ZONE	ADDRESS	USER	ZONE	ADDRESS				
1	Users_to_Extranet	Users_Net	universal	Users_Net	any	any	Extranet	any	dns ftp syslog web-browsing	service-ftp service-http	any	Allow

New application-based rule *replaces* port-based rule.

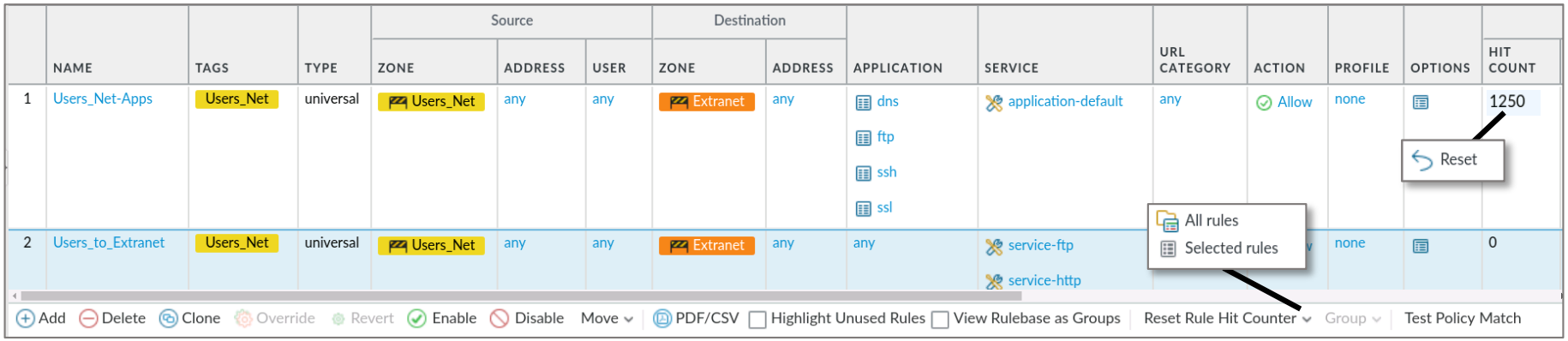
Prioritize Port-Based Rules to Convert



Phase 3: Review Port-Based Rules

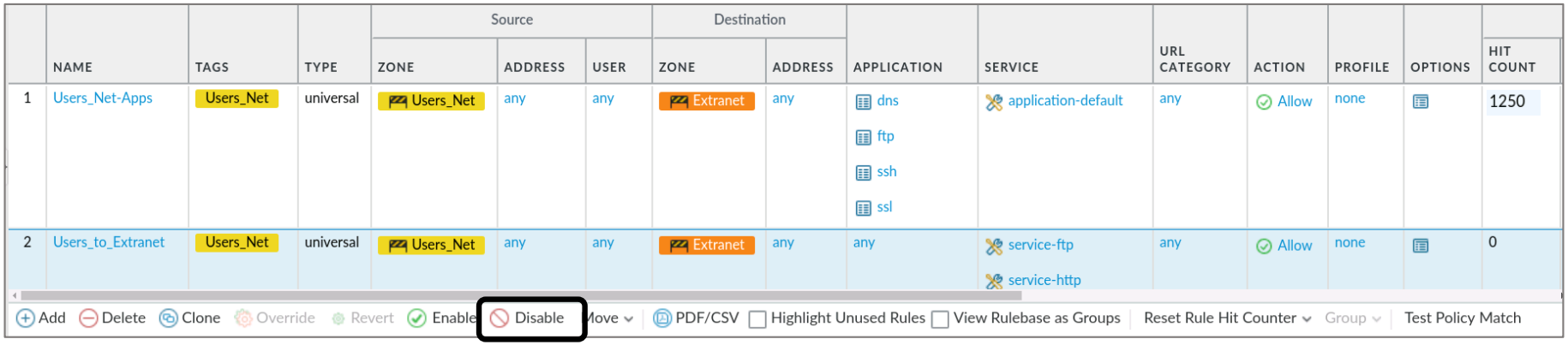
- After 60 days, review the **Hit Count** columns in the Security policy.
- Look for port-based rules with zero hits.

Policies > Security



Phase 3: Disable Port-Based Rules

Policies > Security



	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS	HIT COUNT
1	Users_Net-Apps	Users_Net	universal	Users_Net	any	any	Extranet	any	dns ftp ssh ssl	application-default	any	Allow	none		1250
2	Users_to_Extranet	Users_Net	universal	Users_Net	any	any	Extranet	any	any	service-ftp service-http	any	Allow	none		0

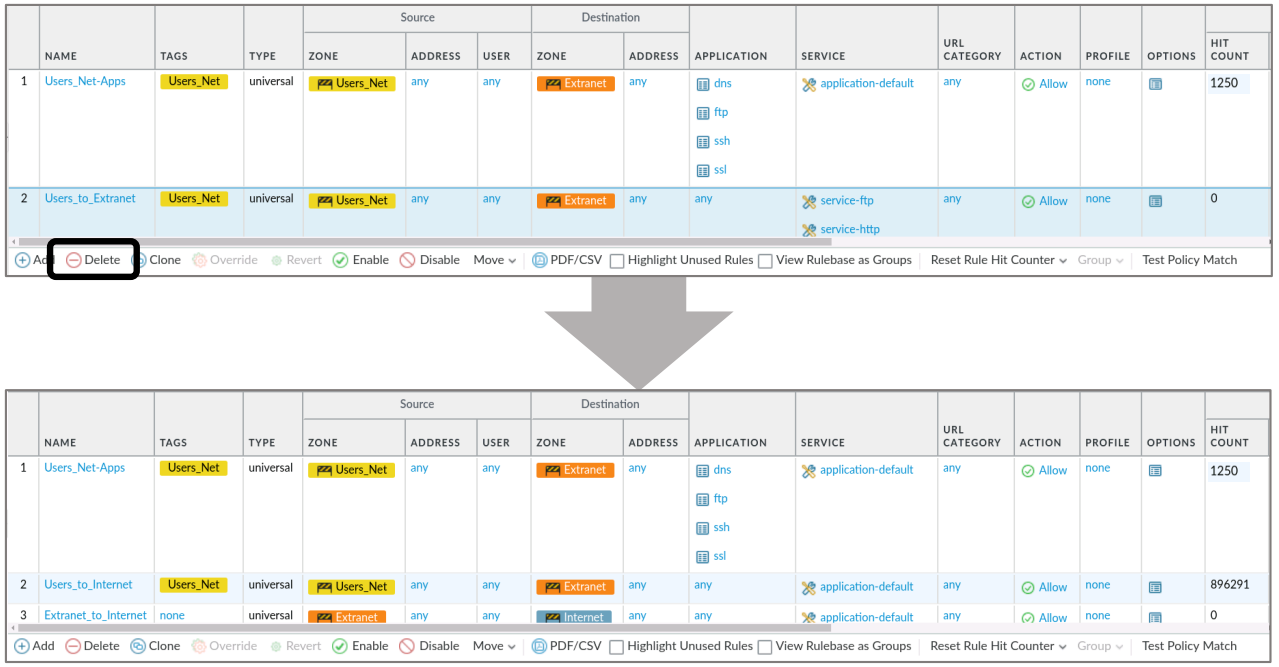
Add | Delete | Clone | Override | Revert | Enable | Disable | Move | PDF/CSV | Highlight Unused Rules | View Rulebase as Groups | Reset Rule Hit Counter | Group | Test Policy Match

- Disable port-based rules that have not matched to any new traffic.
- Disabled rules are rendered in gray italic font.
- Tag rules that must be removed later (optional).

Phase 3: Remove Port-Based Rules

- After 90 days, delete port-based rules that have not matched to any new traffic.
- The goals:
  - At least 80% application-based rules
  - No inbound or outbound *unknown* applications (internal is acceptable)

Policies > Security



Migrate to an App-ID-based Security policy

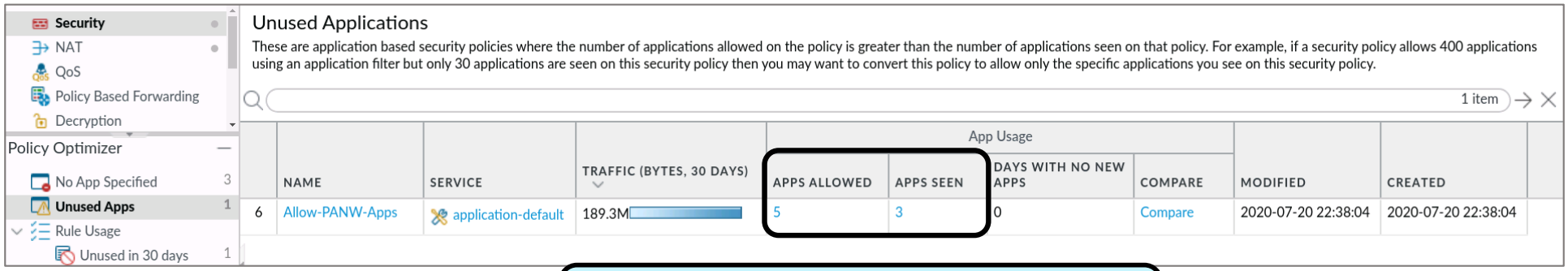
Maintain an App-ID Security policy

Maintain App-ID

Discover Security Policy Rules That Allow Unused Applications

- Applications in use change over time.
- Regularly identify and adjust allowed applications:
  - Maintains the smallest possible attack surface

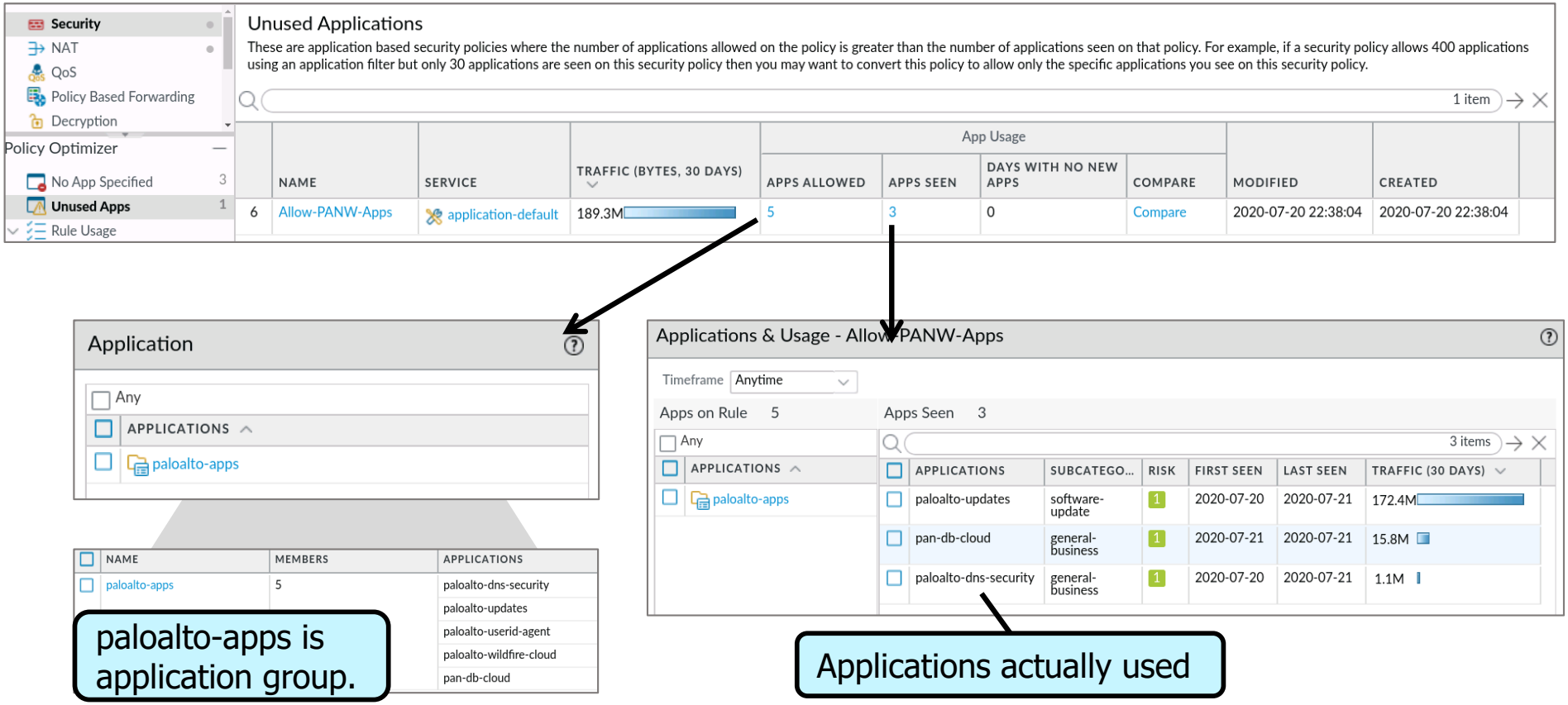
Policies > Security > Policy Optimizer > Unused Apps



Rule allows five applications, but only three applications are currently in use.

View Unused Applications Allowed by a Security Policy Rule

Policies > Security > Policy Optimizer > Unused Apps

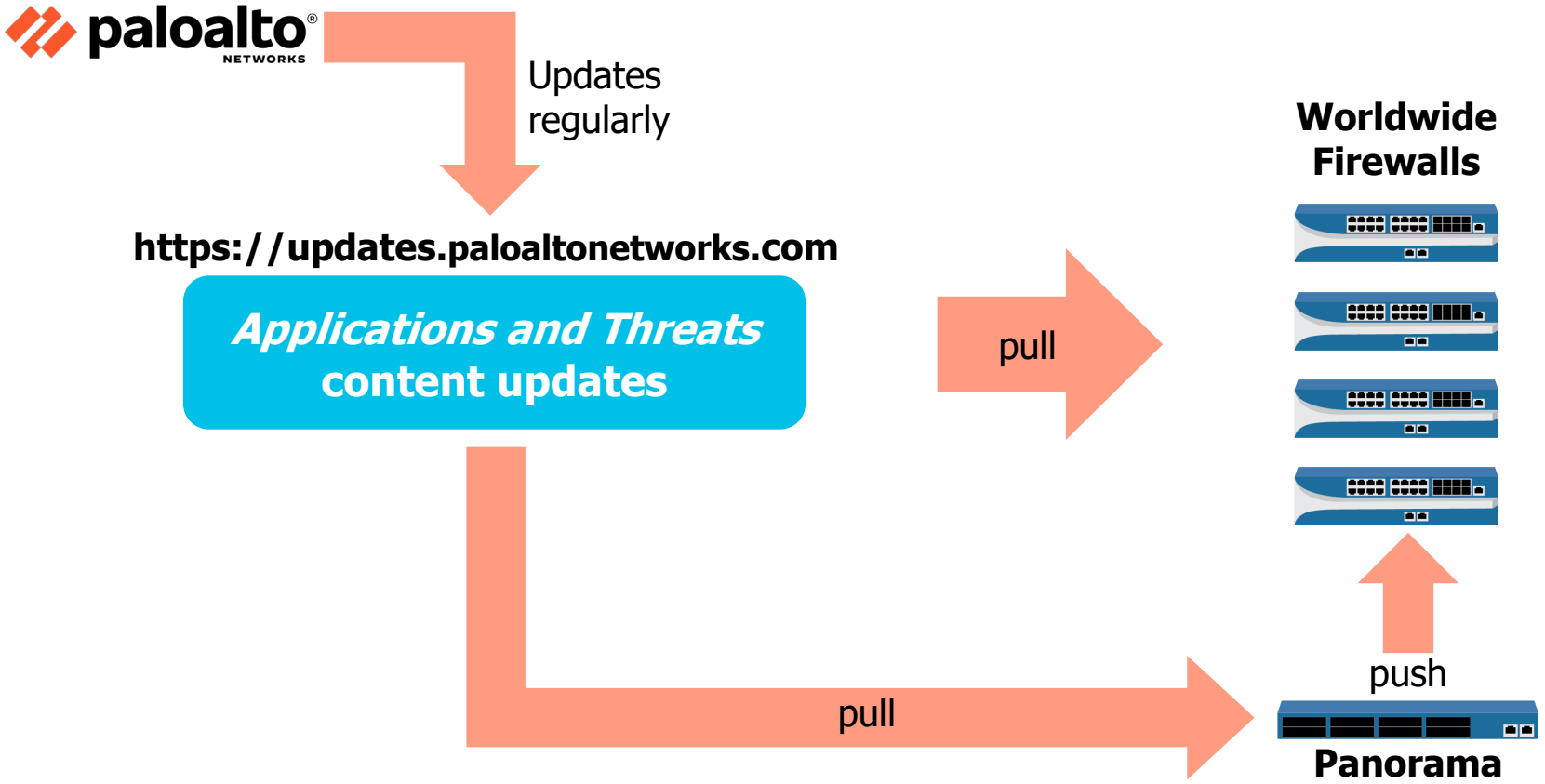


Migrate to an App-ID-based Security policy

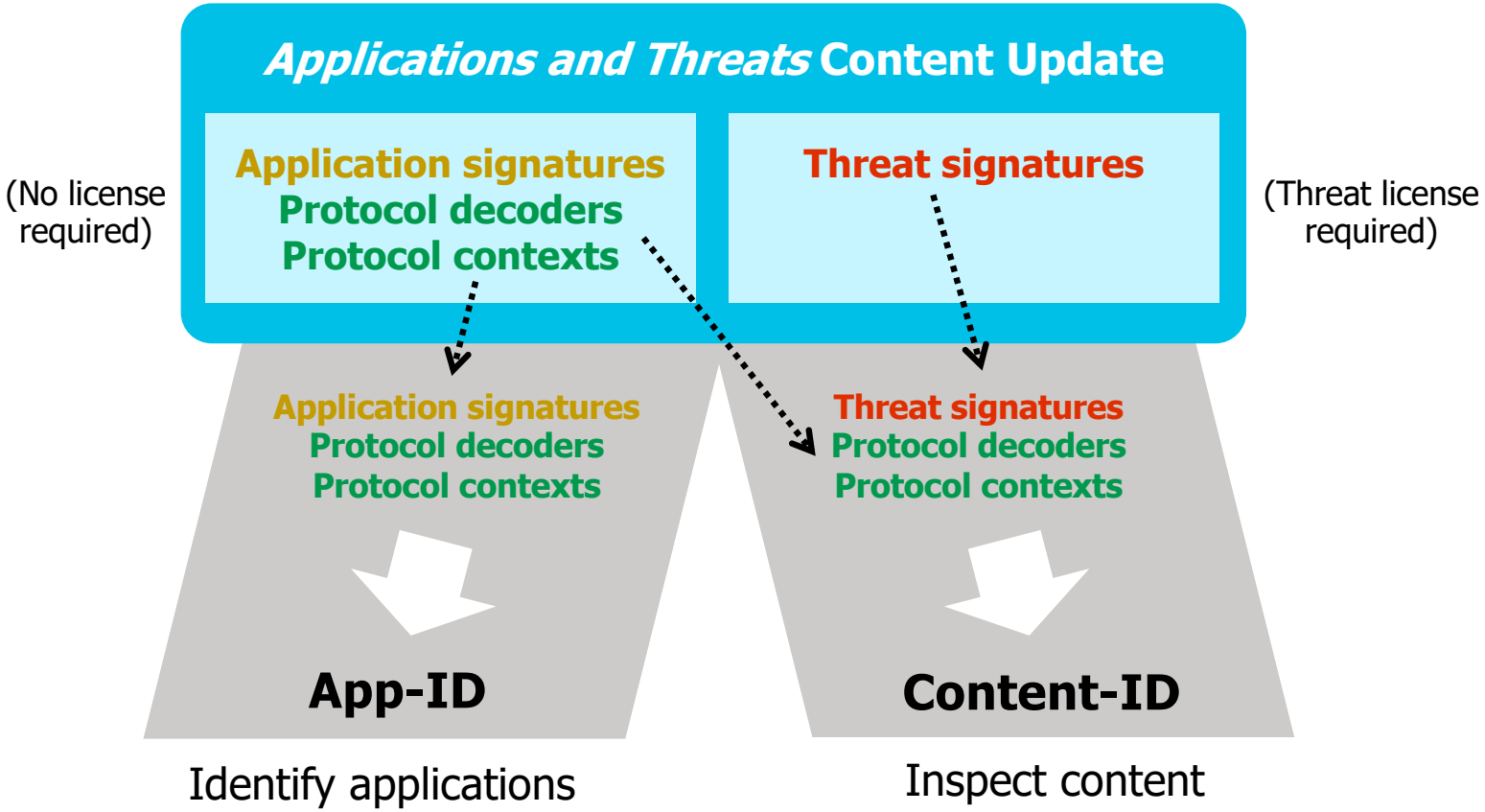
Maintain an App-ID Security policy

Maintain App-ID

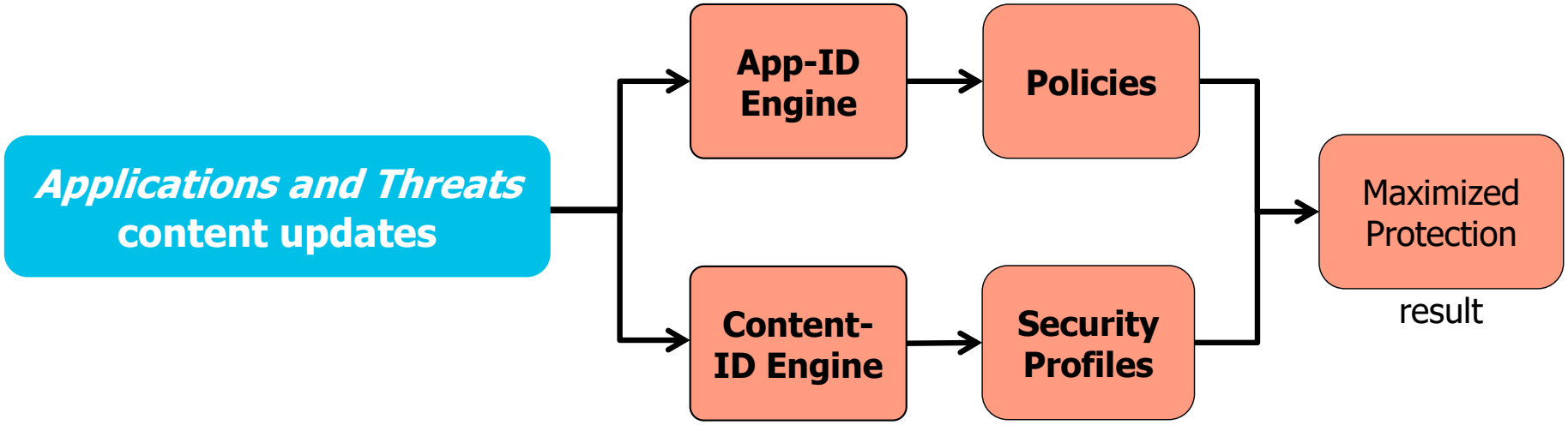
Applications and Threats Content Updates



Applications and Threats Package Contents

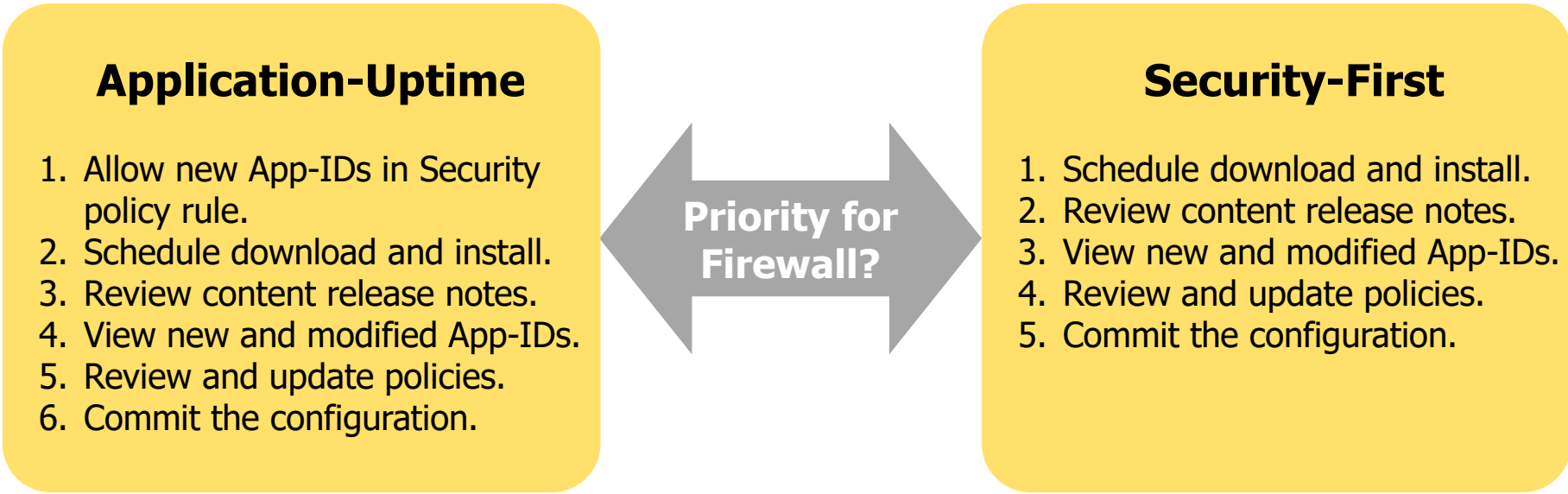


App-ID and Content-ID Depend on Content Updates



- To maintain optimal protection, schedule regular content updates.
- If App-ID cannot identify the traffic, then Content-ID cannot inspect the traffic.

Determine Your Content Update Workflow and Configuration

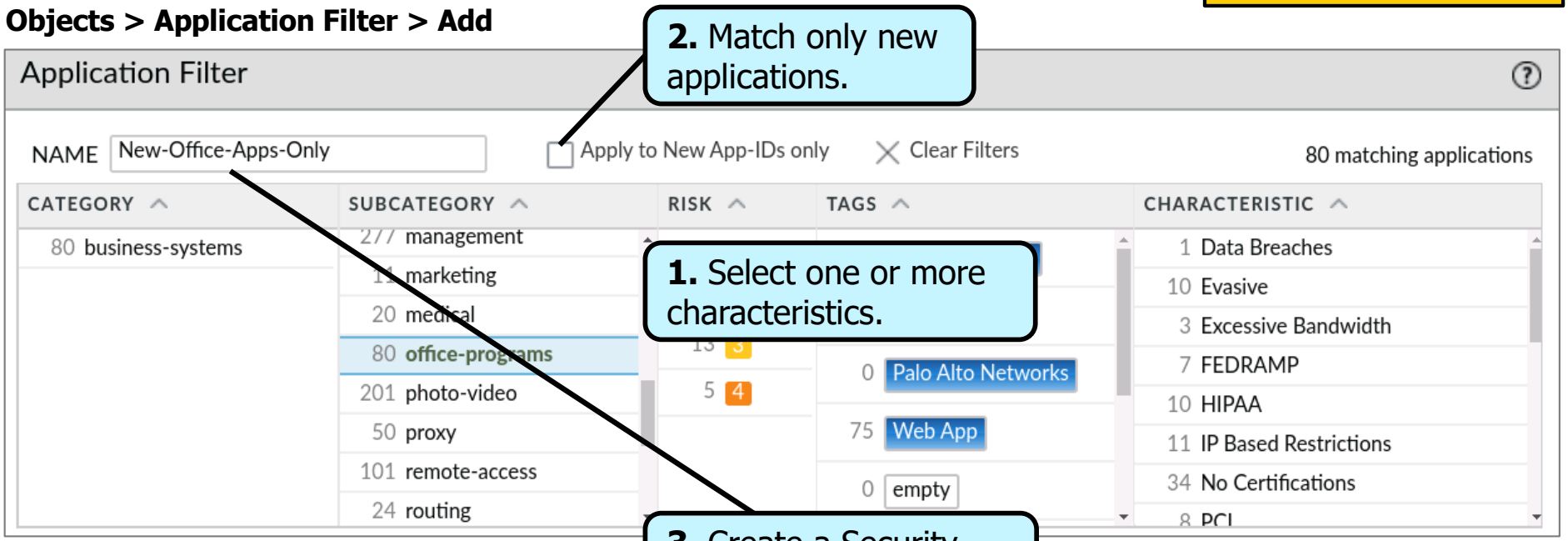


- Priorities can be different for different firewalls:
  - Perimeter firewalls, internal firewalls, remote offices, test-dev environments, etc.

Not Blocking New Applications

Application-Uptime Recommended

Objects > Application Filter > Add



2. Match only new applications.

1. Select one or more characteristics.

3. Create a Security policy allow rule.

Policies > Security > Add

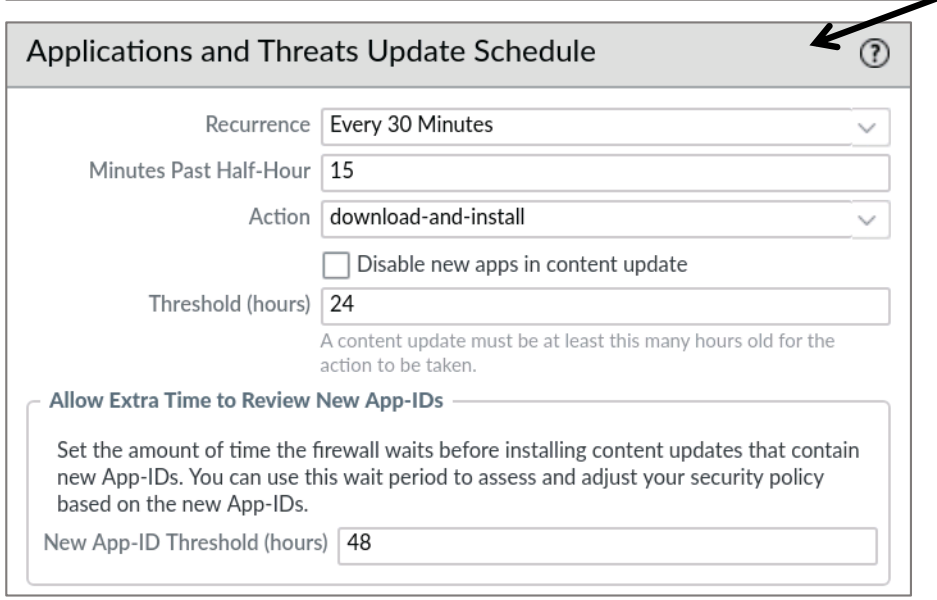
	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION
1	Allow-Only-New-Apps	Users_Net	universal	Users_Net	any	any	Extranet	any	New-Office-Apps-Only	application-default	any	Allow

Schedule Download and Install

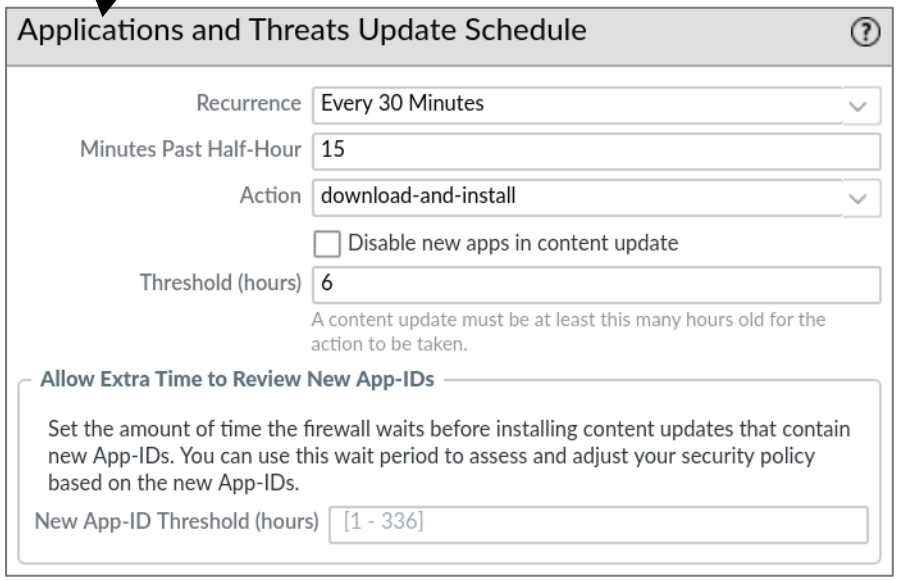
Application-Uptime and Security-First

Device > Dynamic Updates

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLO...	CURRENTLY INSTALLED	ACTION
Applications and Threats	**Last checked:** 2020/07/21 20:14:24 UTC			**Schedule:** Every Wednesday at 01:05 (Download only)					
8285-6146	panupv2-all-contents-8285-6146	Apps, Threats	Full	56 MB	2277b5...	2020/06/23 22:53:57 UTC			Download



Application-Uptime



Security-First

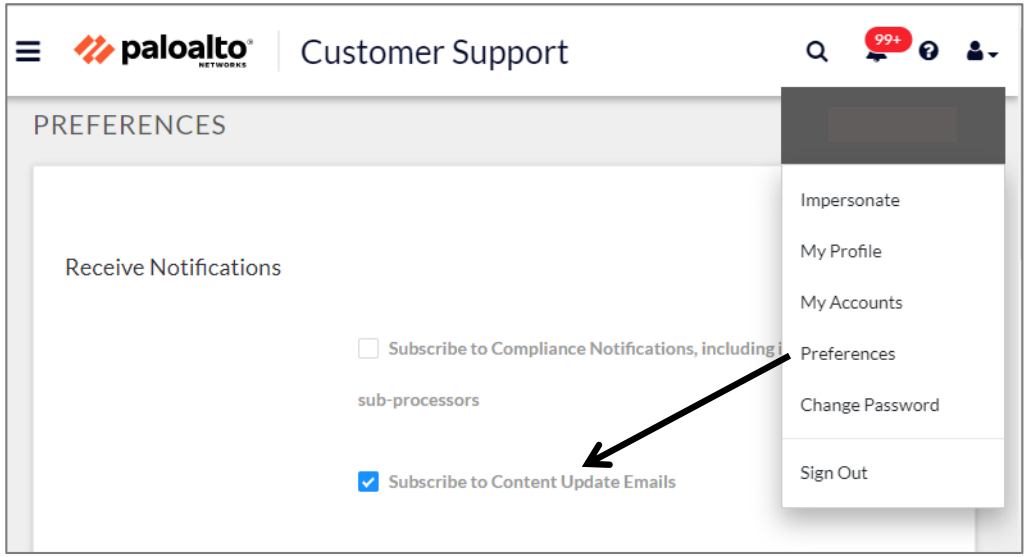
Review Content Update Release Notes

Application-Uptime and Security-First

Device > Dynamic Updates

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLO...	CURRENTLY INSTALLED	ACTION	DOCUMENTA...
Applications and Threats	**Last checked:** 2020/07/22 01:02:06 UTC	**Schedule:** Every Wednesday at 01:02 (Download only)								
8296-6207	panupv2-all-contents-8296-6207	Apps, Threats	Full	56 MB	a643b97f...	2020/07/21 02:20:59 UTC	✓		Install Review Policies Review Apps	Release Notes

https://support.paloaltonetworks.com



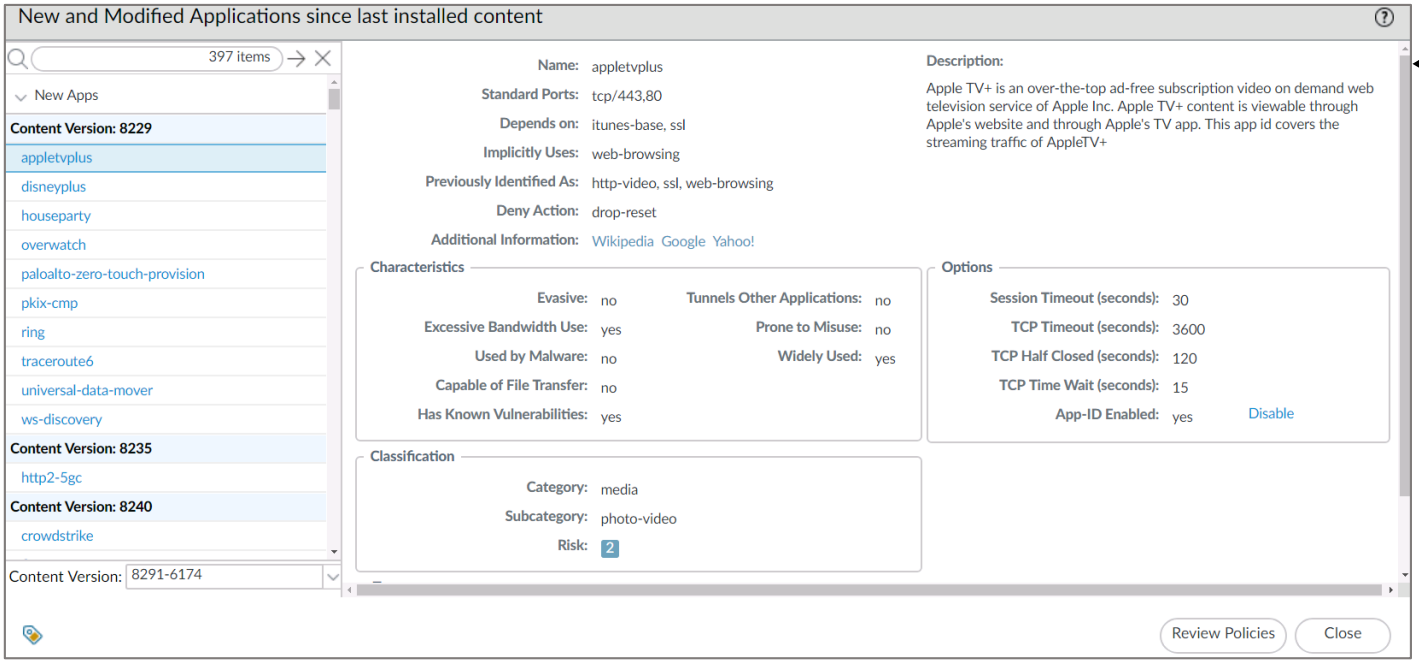
- Content Release Notes describe Security policy impacts.
- Get Content Release Notes from:
  - Firewall
  - Customer Support email

Review New and Updated Application Details

Application-Uptime and Security-First

Device > Dynamic Updates

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLO...	CURRENTLY INSTALLED	ACTION	DOCUMENTA...
Applications and Threats	**Last checked:** 2020/07/22 01:02:06 UTC	**Schedule:** Every Wednesday at 01:02 (Download only)								
8296-6207	panupv2-all-contents-8296-6207	Apps, Threats	Full	56 MB	a643b97f...	2020/07/21 02:20:59 UTC	✓		Install Review Policies Review Apps	Release Notes



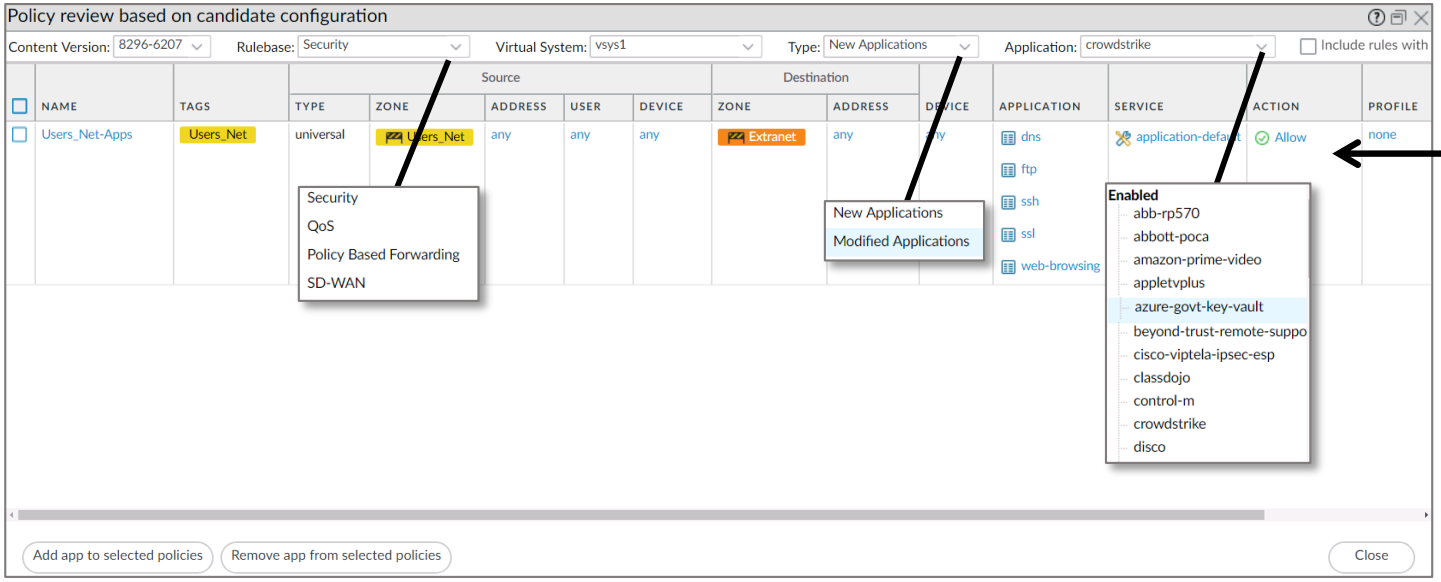
Review new and modified application information.

Review Policies

Application-Uptime and Security-First

Device > Dynamic Updates

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLO...	CURRENTLY INSTALLED	ACTION	DOCUMENTA...
Applications and Threats	**Last checked:** 2020/07/22 01:02:06 UTC	**Schedule:** Every Wednesday at 01:02 (Download only)								
8296-6207	panupv2-all-contents-8296-6207	Apps, Threats	Full	56 MB	a643b97f...	2020/07/21 02:20:59 UTC	✓		Install Review Policies Review Apps	Release Notes

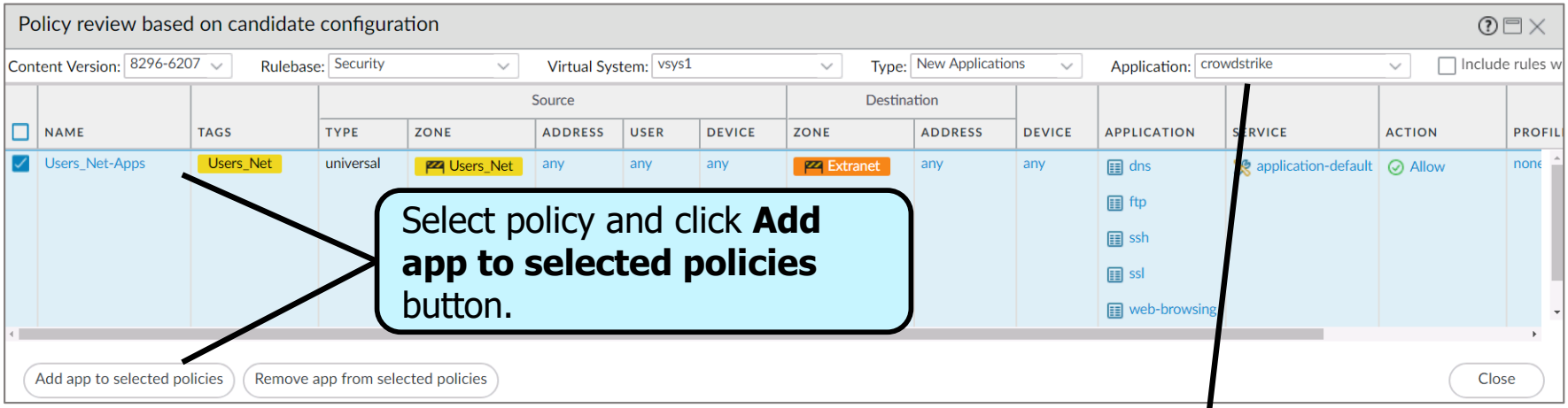


Review the policy impact of new or modified applications.

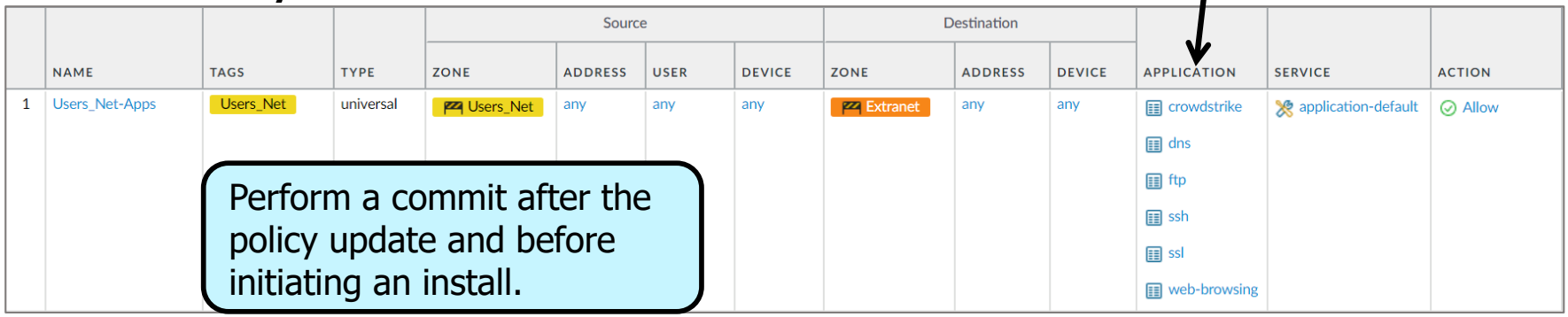
Update Policies

Application-Uptime and Security-First

Device > Dynamic Updates > Review Policies



Policies > Security

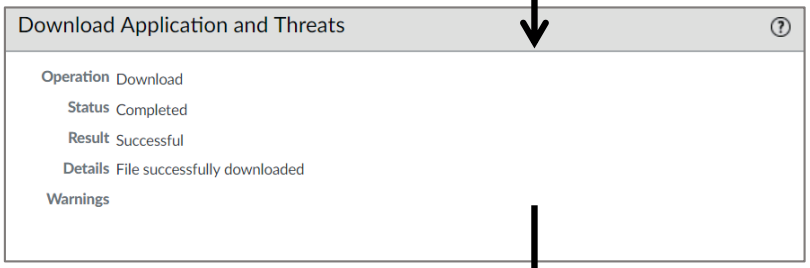


Manual Download Example

Device > Dynamic Updates

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLO...	CURRENTLY INSTALLED	ACTION	DOCUMENTA...
Applications and Threats	**Last checked:** 2020/07/22 19:34:49 UTC	**Schedule:** Every Wednesday at 01:05 (Download only)								
8297-6210	panupv2-all-contents-8297-6210	Apps, Threats	Full	56 MB	af1a9fb5a...	2020/07/22 02:37:19 UTC			Download	Release Notes

1. Click **Check Now** to see latest the updates.
2. Read the release notes.
3. Click **Download**.



Device > Dynamic Updates

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLO...	CURRENTLY INSTALLED	ACTION	DOCUMENTA...
Applications and Threats	**Last checked:** 2020/07/22 20:24:27 UTC	**Schedule:** Every Wednesday at 01:05 (Download only)								
8297-6210	panupv2-all-contents-8297-6210	Apps, Threats	Full	56 MB	af1a9fb5a...	2020/07/22 02:37:19 UTC	✓		Install Review Policies Review Apps	Release Notes

Manual Install Example

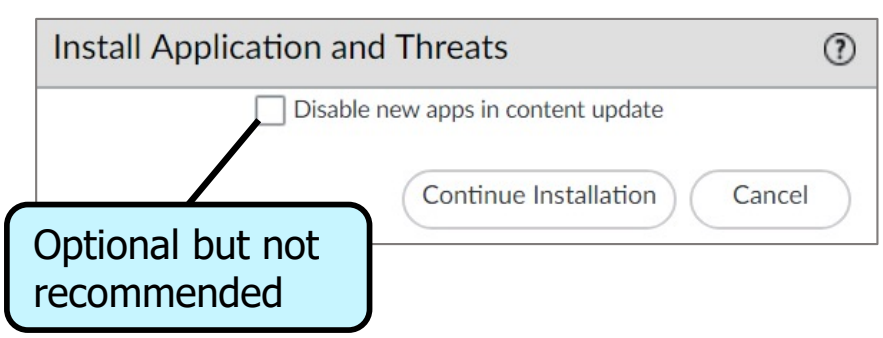
Device > Dynamic Updates

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLO...	CURRENTLY INSTALLED	ACTION	DOCUMENTA...
Applications and Threats	**Last checked:** 2020/07/22 20:24:27 UTC	**Schedule:** Every Wednesday at 01:05 (Download only)								
8297-6210	panupv2-all-contents-8297-6210	Apps, Threats	Full	56 MB	af1a9fb5a...	2020/07/22 02:37:19 UTC	✓		Install Review Policies Review Apps	Release Notes

1. Click **Install** to install the content update.
2. Click **Continue Installation**.

- Disabling of new application signatures enables you to review and update policies even after a commit operation:
  - Possibly time-consuming to re-enable

3. Commit your configuration.



Module Summary

Now that you have completed this module, you should be able to:

- Convert to an application-based Security policy
- Maintain an application-based Security policy
- Maintain an optimal App-ID configuration on your firewall

Questions

Lab 11: Maintaining Application Based Policies

- Create and Test a Custom Service Object for HTTP
- Create and Test an FTP Application-Based Security Policy Rule
- Schedule App-ID Updates

Protecting our digital way of life.