

## 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

## 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





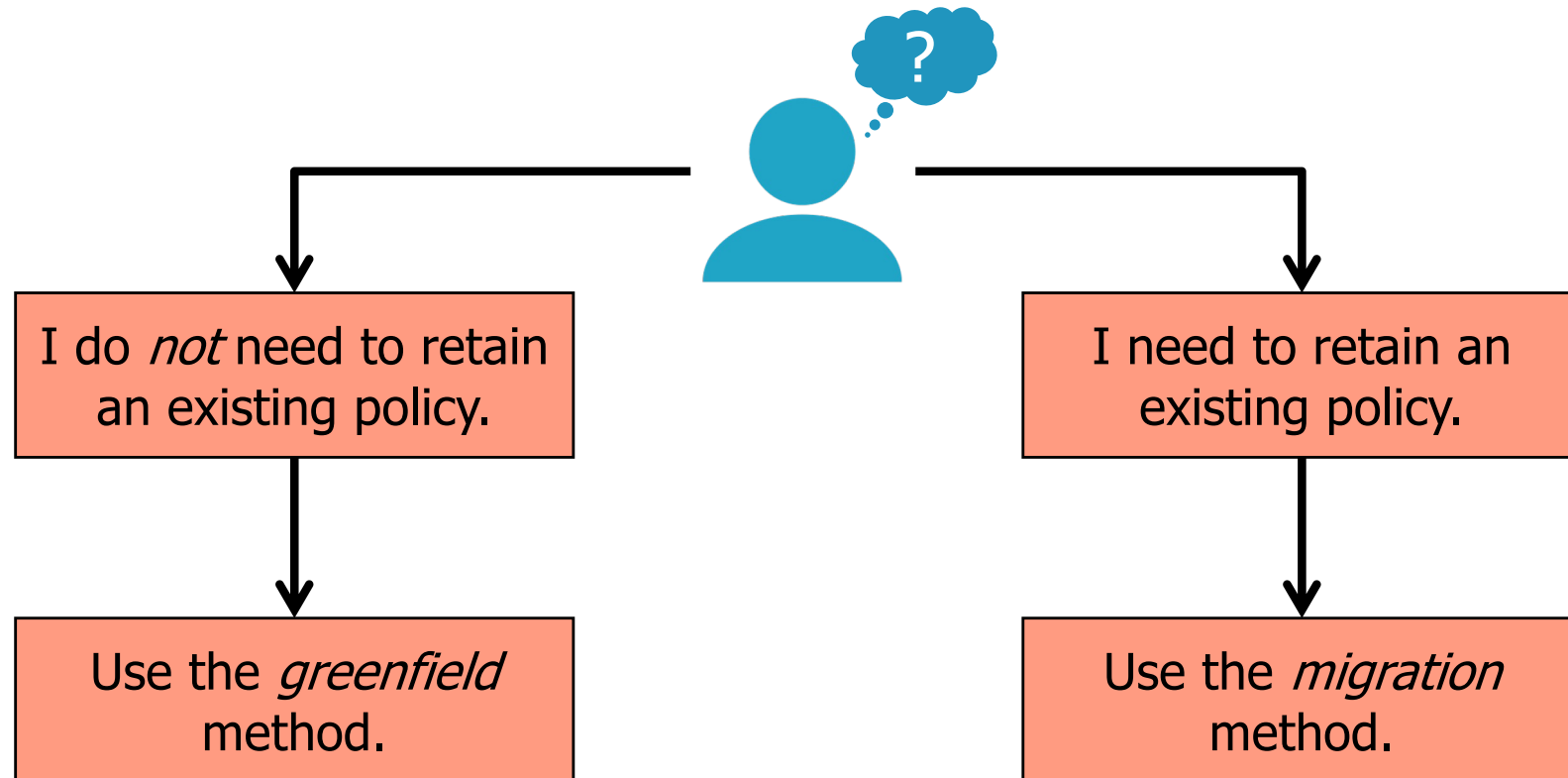
**Migrate to an App-ID-based Security policy**

Maintain an App-ID Security policy

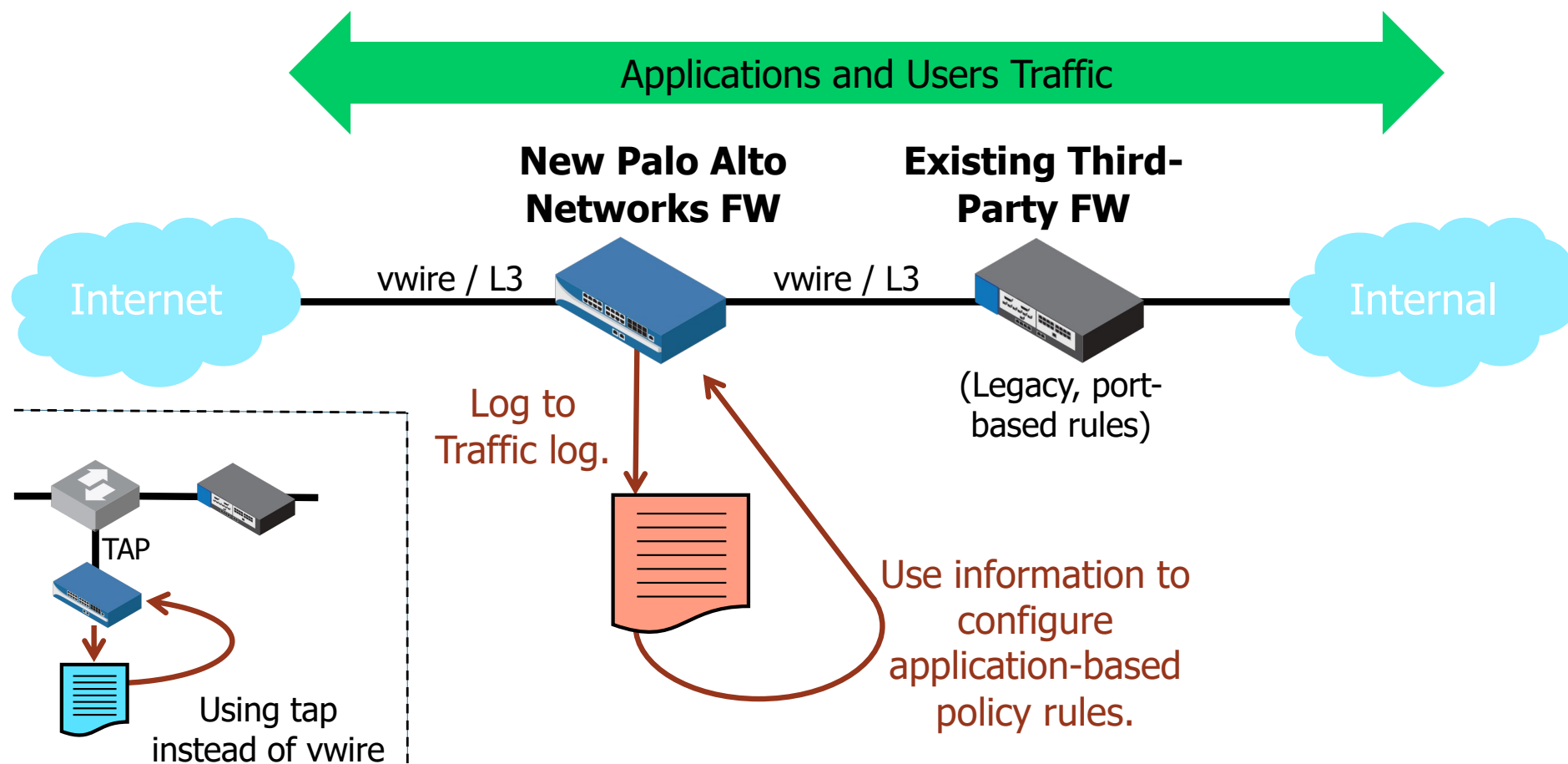
Maintain App-ID



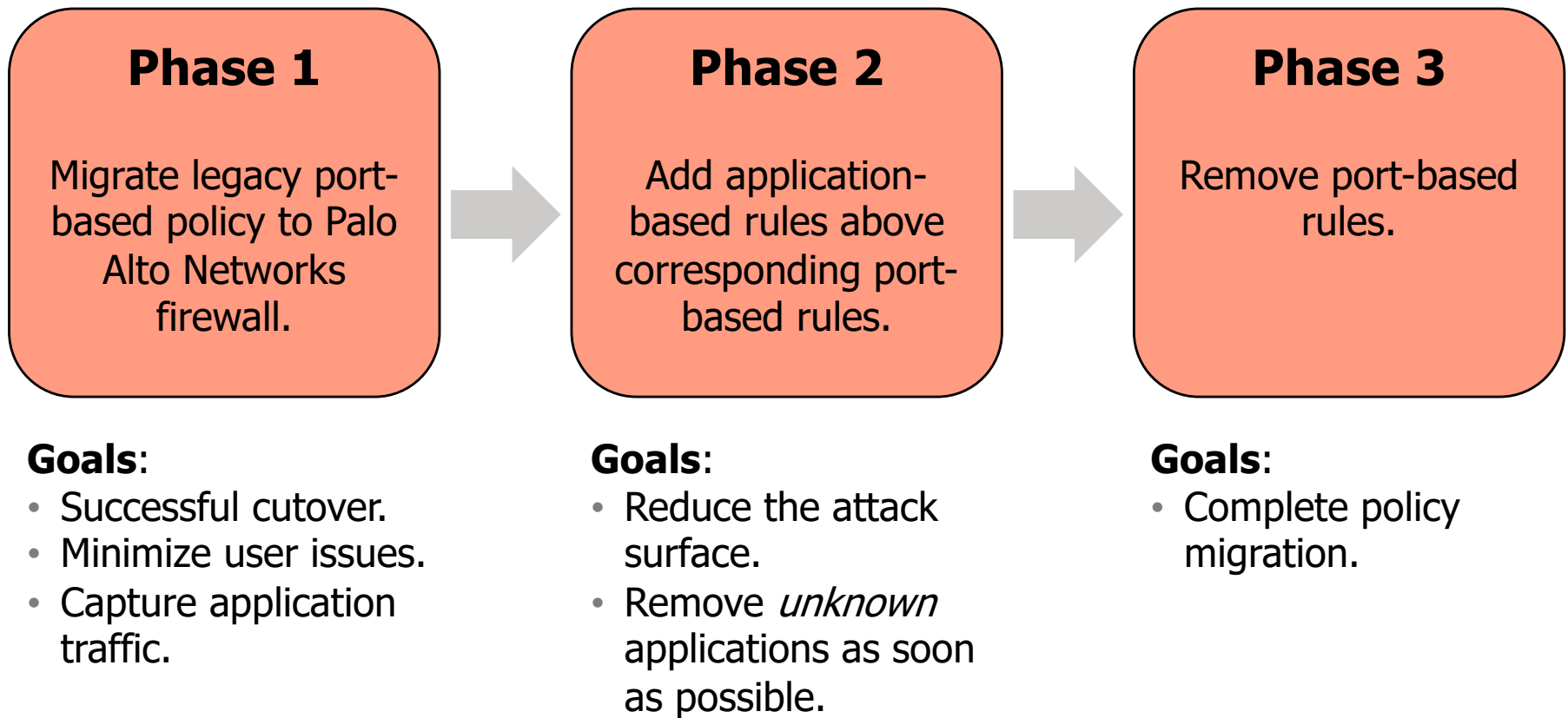
## Moving to Application-Based Policies



## Greenfield Example



## Example Migration Method: Overview



## Expedition (Migration Tool)

- Migrate policy from a pre-existing firewall.
- [https://live.paloaltonetworks.com/t5/expedition-migration-tool/ct-p/migration\\_tool](https://live.paloaltonetworks.com/t5/expedition-migration-tool/ct-p/migration_tool)

### Welcome to Expedition

#### ABOUT

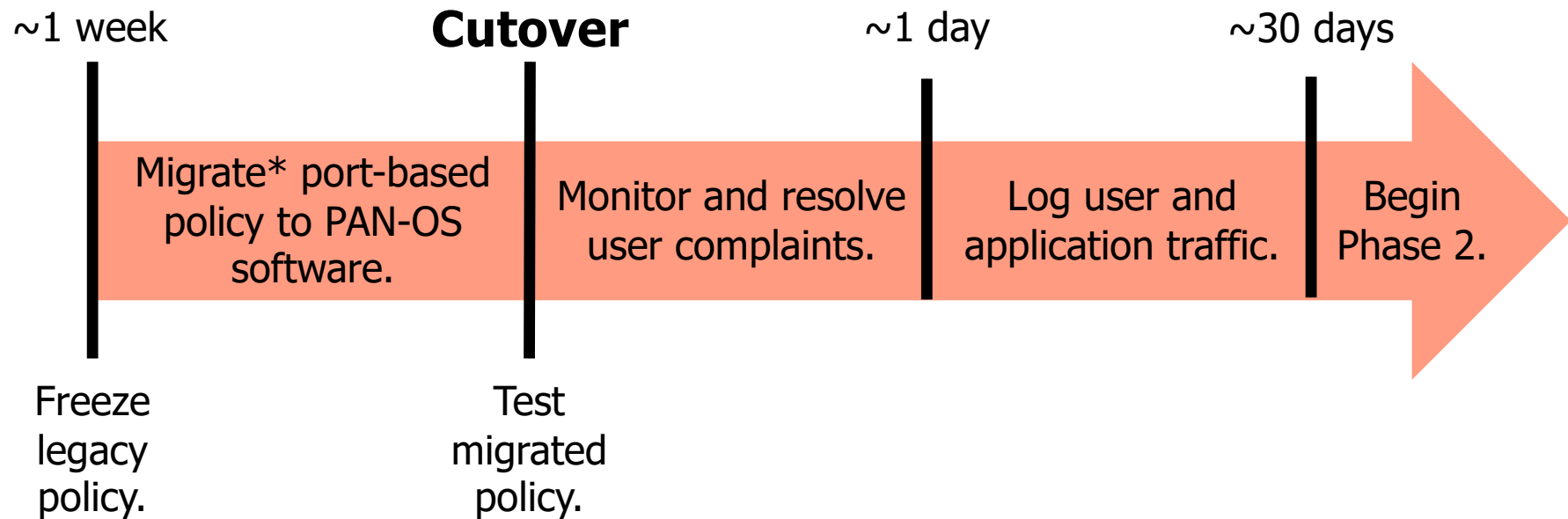
Expedition is the fourth evolution of the Palo Alto Networks Migration Tool. The purpose of this tool is to help reduce the time and efforts of migrating a configuration from a supported vendor to Palo Alto Networks.

By using Expedition (Migration Tool), everyone can convert a configuration from Checkpoint, Cisco, or any other vendor to a PAN-OS and give you more time to improve the results. Expedition (Migration Tool) 3 added some functionalities to allow our customers to enforce security policies based on App-ID and User-ID as well. [READ MORE](#)

**NOTE:** Expedition is supported by the community as best effort. The Palo Alto Networks TAC does not provide support, so please post your questions in the community by clicking "Ask Questions" below.

[Get the Expedition Installer](#)

## 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

<b>No App Specified</b> These are security policies that have no application specified and allow any application on the configured service which can present a security risk. Palo Alto Networks recommends that you convert these service only security policies to application based policies.										
3 items → ×										
	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 I	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 I	any	4	0	Compare	2020-07-21 20:55:56	2020-07-21 18:35:31	
4	Extranet_to_Internet	application-default	141.2k I	any	2	6	Compare	2020-07-15 15:13:03	2020-07-14 17:59:46	

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	<a href="#">Users_to_Internet</a>	application-default	888.9k	any	2	0	<a href="#">Compare</a>	2020-07-21 20:55:56	2020-07-17 19:26:56
1	<a href="#">Users_to_Extranet</a>	service-ftp service-http	568.1k	any	4	0	<a href="#">Compare</a>	2020-07-21 20:55:56	2020-07-21 18:35:31
4	<a href="#">Extranet_to_Internet</a>	application-default	141.2k	any	2	6	<a href="#">Compare</a>	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).

Applications & Usage - Users\_to\_Extranet

Timeframe: Anytime

Apps on Rule: Any

Apps Seen: 4

4 items

APPLICATIONS	SUBCATEGO...	RISK	FIRST SEEN	LAST SEEN	TRAFFIC (30 DAYS)
<input type="checkbox"/> dns	infrastructure	3	2020-07-21	2020-07-21	506.2k
<input type="checkbox"/> web-browsing	internet-utility	4	2020-07-21	2020-07-21	55.0k
<input type="checkbox"/> syslog	management	2	2020-07-21	2020-07-21	3.9k
<input type="checkbox"/> ftp	file-s				

Anytime  
Past 7 days  
Past 15 days  
Past 30 days

Four options to convert the policy

Browse Add Delete Create Cloned Rule Add to This Rule Add to Existing Rule Match Usage

The last new app was discovered 0 days ago.

## Phase 2: Clone a Port-Based Rule Using “Create Cloned Rule”

### Option 1 of 4:

1. Select application(s).  
2. Click **Create Cloned Rule**.  
3. Name new rule.

Applications & Usage - Users\_to\_Extranet

Timeframe: Anytime

Apps on Rule: 4 items

APP	NAME	LAST SEEN	TRAFFIC (30 DAYS)
<input checked="" type="checkbox"/>	Any	2020-07-21	506.2k
<input type="checkbox"/>	syslog	2020-07-21	55.0k
<input type="checkbox"/>	management	2020-07-21	3.9k
<input checked="" type="checkbox"/>	ftp	2020-07-21	

Buttons: Browse, Add, Delete, **Create Cloned Rule**, Add to This Rule, Add to Existing Rule

- 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

Create Cloned Rule

Name: Allow-FTP

Applications

☒ Add container app ☐ Add specific apps seen

APPLICATION	LAST SEEN
<input checked="" type="checkbox"/> ftp	2020-07-21

## Result of “Create Cloned Rule”

Applications & Usage - Users\_to\_Extranet

Timeframe: Anytime

Apps on Rule: ☒ Any

Apps Seen: 3

APPLICATIONS	SUBCATEGO...	RISK	FIRST SEEN	LAST SEEN	TRAFFIC (30 DAYS)
<input type="checkbox"/> dns	infrastructure	3	2020-07-21	2020-07-21	506.2k
<input type="checkbox"/> web-browsing	internet-utility	4	2020-07-21	2020-07-21	55.0k
<input type="checkbox"/> syslog	management	2	2020-07-21	2020-07-21	3.9k

3 items → ×

The last new app was discovered 0 days ago.

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

### Policies > Security

	NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION
				ZONE	ADDRESS	USER	ZONE	ADDRESS				
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

Must manually configure as **application-default**

## Phase 2: Replace a Port-Based Rule Using “Add to This Rule”

### Option 2 of 4:

Applications & Usage - Users\_to\_Extranet

Timeframe: Anytime

Apps on Rule: Apps Seen: 4

4 items → ×

SK	FIRST SEEN	LAST SEEN	TRAFFIC (30 DAYS)
1	2020-07-21	2020-07-21	506.2k
2	2020-07-21	2020-07-21	55.0k
3	2020-07-21	2020-07-21	3.9k
4	2020-07-21	2020-07-21	2.1k

1. Select application(s).  
2. Click **Add to This Rule**.

Buttons: Browse, Add, Delete, Create Cloned Rule, Add to This Rule, Add to Existing Rule

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

Add to This Rule

Applications

☒ Add container app ☐ Add specific apps seen

APPLICATION	LAST SEEN
ftp	2020-07-21

## 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:

The screenshot shows the Palo Alto Networks GUI. The main window is titled "Applications & Usage - Users\_to\_Extranet". It has a "Timeframe" dropdown set to "Anytime". Below this is a table titled "Apps on Rule" with columns "APPLICATIONS", "SUBCATEGORY", "RISK", and "FIRST SEEN". The table contains four rows: "Any" (checked), "syslog" (unchecked), "ftp" (checked), and "file-sharing" (checked). A callout box with a blue background and black text contains the instructions: "1. Select application(s). 2. Click **Add to Existing Rule**." An arrow points from the "Add to Existing Rule" button in the bottom toolbar to the "Add Apps to Existing Rule" dialog box. The dialog box has a "Name" dropdown and a list of applications. The list includes "1 - Users\_to\_Extranet", "2 - Users\_Net-Apps", "3 - Users\_to\_Internet", "4 - Extranet\_to\_Internet", and "5 - Allow-PANW-Apps". The "2 - Users\_Net-Apps" option is selected. To the right of the list is a radio button labeled "Add specific apps seen". Below the list is a table with the header "LAST SEEN" and one row with the date "2020-07-21". The bottom toolbar of the main window includes buttons for "Browse", "Add", "Delete", "Create Cloned Rule", "Add to This Rule", "Add to Existing Rule", and "Match Usage".

Applications & Usage - Users\_to\_Extranet

Timeframe: Anytime

Apps on Rule: Apps Seen: 4

☒ Any

APPLICATIONS	SUBCATEGORY	RISK	FIRST SEEN
<input type="checkbox"/> syslog	management	2	2020-07-21
<input checked="" type="checkbox"/> ftp	file-sharing	5	2020-07-21

1. Select application(s).  
2. Click **Add to Existing Rule**.

**Add Apps to Existing Rule**

Name: [dropdown]

Applic: 1 - Users\_to\_Extranet  
2 - Users\_Net-Apps  
3 - Users\_to\_Internet  
4 - Extranet\_to\_Internet  
5 - Allow-PANW-Apps

☐ Add specific apps seen

LAST SEEN
2020-07-21

Toolbar: Browse, Add, Delete, Create Cloned Rule, Add to This Rule, **Add to Existing Rule**, Match Usage

## Result of “Add to Existing 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	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:

Applications & Usage - Users\_to\_Extranet

Timeframe: Anytime

Apps on Rule: Apps Seen 4

4 items

APPLICATIONS	SUBCATEGO...	RISK	FIRST SEEN	LAST SEEN	TRAFFIC (30 DAYS)
<input type="checkbox"/> dns	infrastructure	3	2020-07-21	2020-07-21	506.2k
<input type="checkbox"/> web-browsing			2020-07-21	2020-07-21	55.0k
<input type="checkbox"/> syslog			2020-07-21	2020-07-21	3.9k
<input type="checkbox"/> ftp			2020-07-21	2020-07-21	3.1k

All applications are added to the left-side **Apps on Rule** column.

Click **Match Usage**.

Match Usage

The last new app was discovered 0 days ago.

- 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”

### 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	<div>dns</div> <div>ftp</div> <div>syslog</div> <div>web-browsing</div>	<div>service-ftp</div> <div>service-http</div>	any	Allow

Must manually configure as **application-default**

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

# Prioritize Port-Based Rules to Convert

**No App Specified** 3

These are security policies that have no application specified. They are not prioritized by application risk. Palo Alto Networks recommends that you specify an application for these rules to help you identify rules that should be removed to reduce your attack surface.

**Prioritize rules passing more data.**

**Prioritize rules with more applications.**

**Prioritize rules that are more stable.**

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

**Prioritize rules that match more sessions.**

Expected, and can help identify rules that should be removed to reduce your attack surface.

☐ Exclude rules reset during the last 90 days

1 item →

	NAME	Rule Usage				MODIFIED	CREATED
		HIT COUNT	LAST HIT	FIRST HIT	RESET DATE		
4	Extranet_to_Internet	0	-	-	2020-07-21 21:53:57	2020-07-15 15:13:03	2020-07-14 17:59:46

## 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

	NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS	HIT COUNT
				ZONE	ADDRESS	USER	ZONE	ADDRESS							
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			none		0

All rules

Selected rules

Reset

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

## Phase 3: Disable Port-Based Rules

### Policies > Security

	NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS	HIT COUNT
				ZONE	ADDRESS	USER	ZONE	ADDRESS							
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

	NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS	HIT COUNT
				ZONE	ADDRESS	USER	ZONE	ADDRESS							
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

	NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS	HIT COUNT
				ZONE	ADDRESS	USER	ZONE	ADDRESS							
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_Internet	Users_Net	universal	Users_Net	any	any	Extranet	any	any	application-default	any	Allow	none		896291
3	Extranet_to_Internet	none	universal	Extranet	any	any	Internet	any	any	application-default	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

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

Security

NAT

QoS

Policy Based Forwarding

Decryption

Policy Optimizer

No App Specified

Unused Apps

Rule Usage

Unused in 30 days

Unused Applications

These are application based security policies where the number of applications allowed on the policy is greater than the number of applications seen on that policy. For example, if a security policy allows 400 applications using an application filter but only 30 applications are seen on this security policy then you may want to convert this policy to allow only the specific applications you see on this security policy.

1 item

				App Usage					
NAME	SERVICE	TRAFFIC (BYTES, 30 DAYS)	APPS ALLOWED	APPS SEEN	DAYS WITH NO NEW APPS	COMPARE	MODIFIED	CREATED	
6	Allow-PANW-Apps	application-default	189.3M	5	3	0	Compare	2020-07-20 22:38:04	2020-07-20 22:38:04



# View Unused Applications Allowed by a Security Policy Rule

## Policies > Security > Policy Optimizer > Unused Apps

**Unused Applications**

These are application based security policies where the number of applications allowed on the policy is greater than the number of applications seen on that policy. For example, if a security policy allows 400 applications using an application filter but only 30 applications are seen on this security policy then you may want to convert this policy to allow only the specific applications you see on this security policy.

1 item → ×

	NAME	SERVICE	TRAFFIC (BYTES, 30 DAYS)	App Usage				MODIFIED	CREATED
				APPS ALLOWED	APPS SEEN	DAYS WITH NO NEW APPS	COMPARE		
6	Allow-PANW-Apps	application-default	189.3M	5	3	0	Compare	2020-07-20 22:38:04	2020-07-20 22:38:04

**Application** ?

☐ Any

☒ APPLICATIONS ^

☐ paloalto-apps

NAME	MEMBERS	APPLICATIONS
paloalto-apps	5	paloalto-dns-security paloalto-updates paloalto-userid-agent paloalto-wildfire-cloud pan-db-cloud

paloalto-apps is application group.

**Applications & Usage - Allow-PANW-Apps** ?

Timeframe: Anytime

Apps on Rule: 5    Apps Seen: 3

☐ Any

☒ APPLICATIONS ^

☐ paloalto-apps

APPLICATIONS	SUBCATEGO...	RISK	FIRST SEEN	LAST SEEN	TRAFFIC (30 DAYS)
paloalto-updates	software-update	1	2020-07-20	2020-07-21	172.4M
pan-db-cloud	general-business	1	2020-07-21	2020-07-21	15.8M
paloalto-dns-security	general-business	1	2020-07-20	2020-07-21	1.1M

Applications actually used

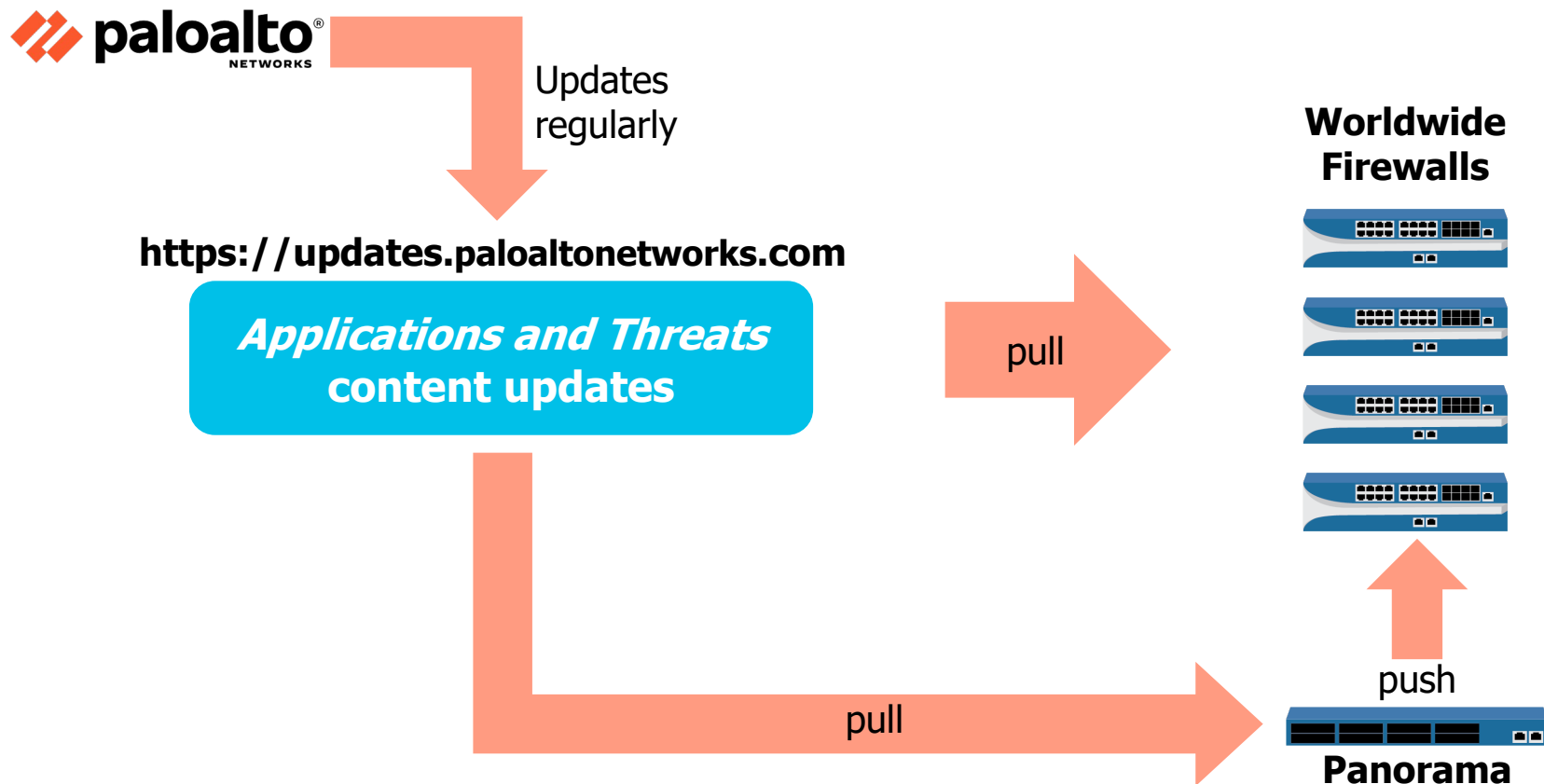
Migrate to an App-ID-based Security policy

Maintain an App-ID Security policy

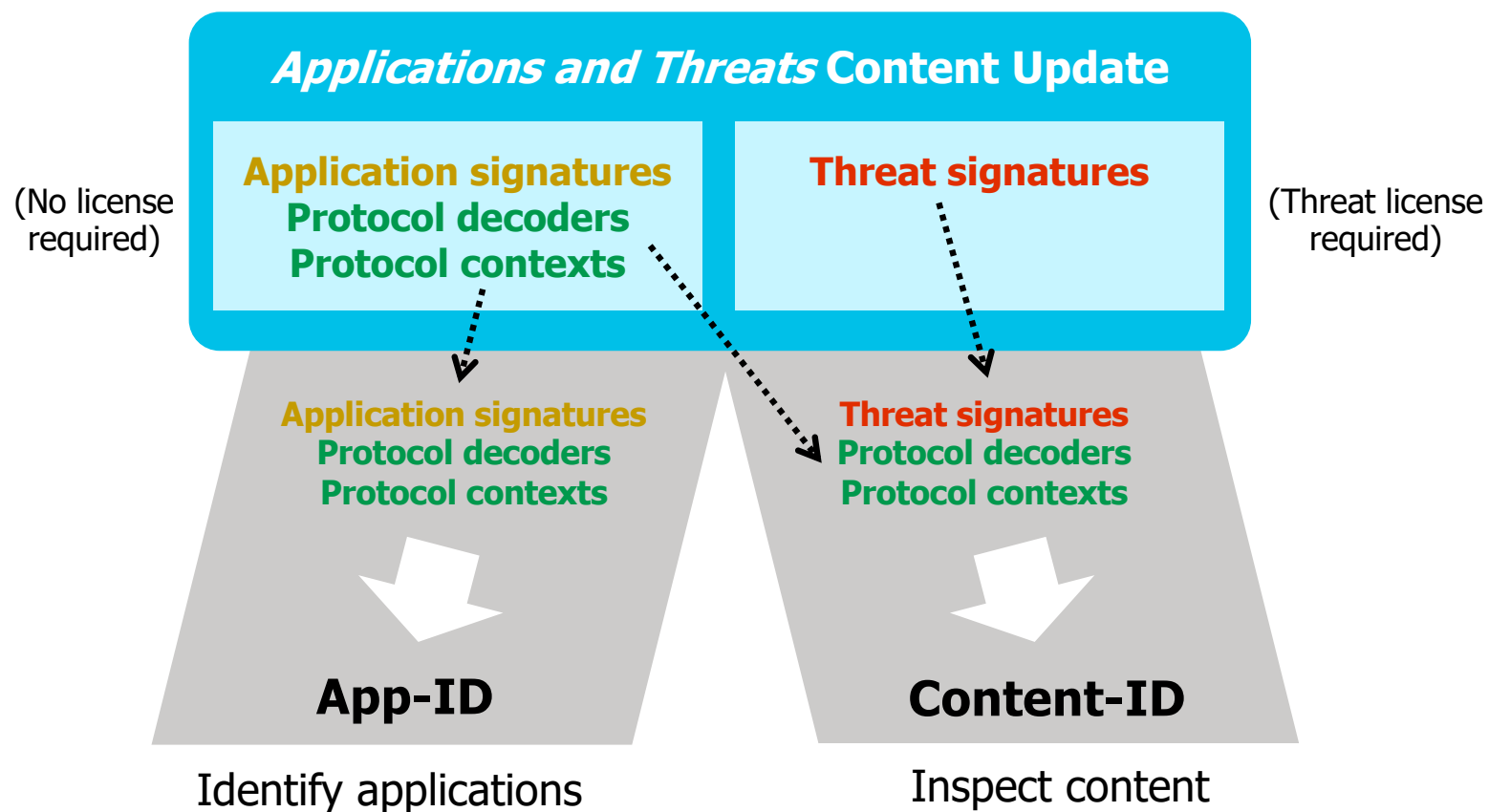


**Maintain App-ID**

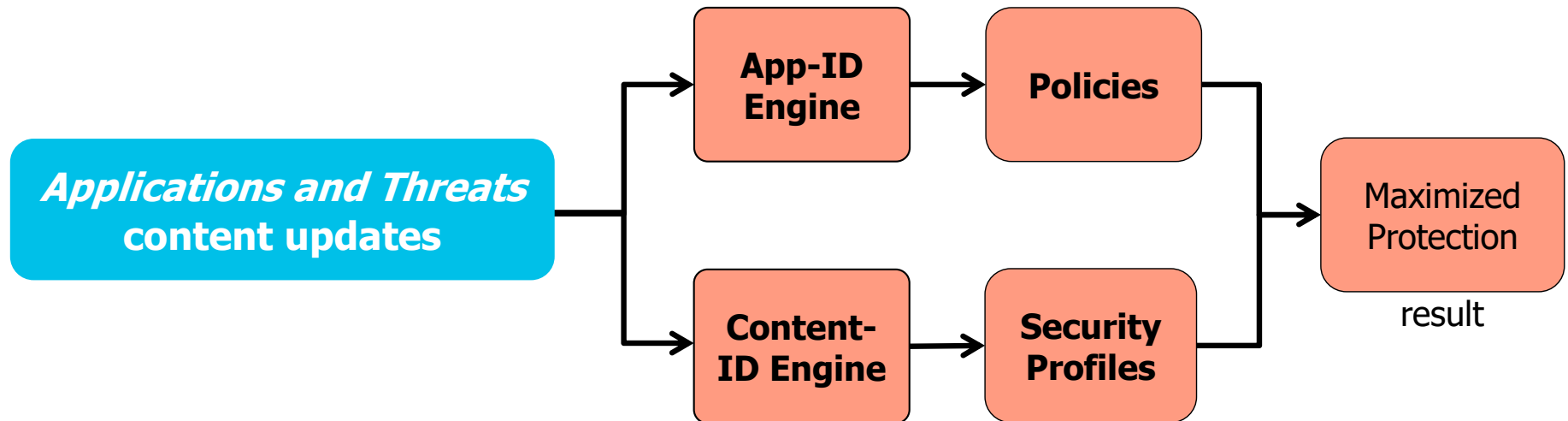
# Applications and Threats Content Updates



# Applications and Threats Package Contents

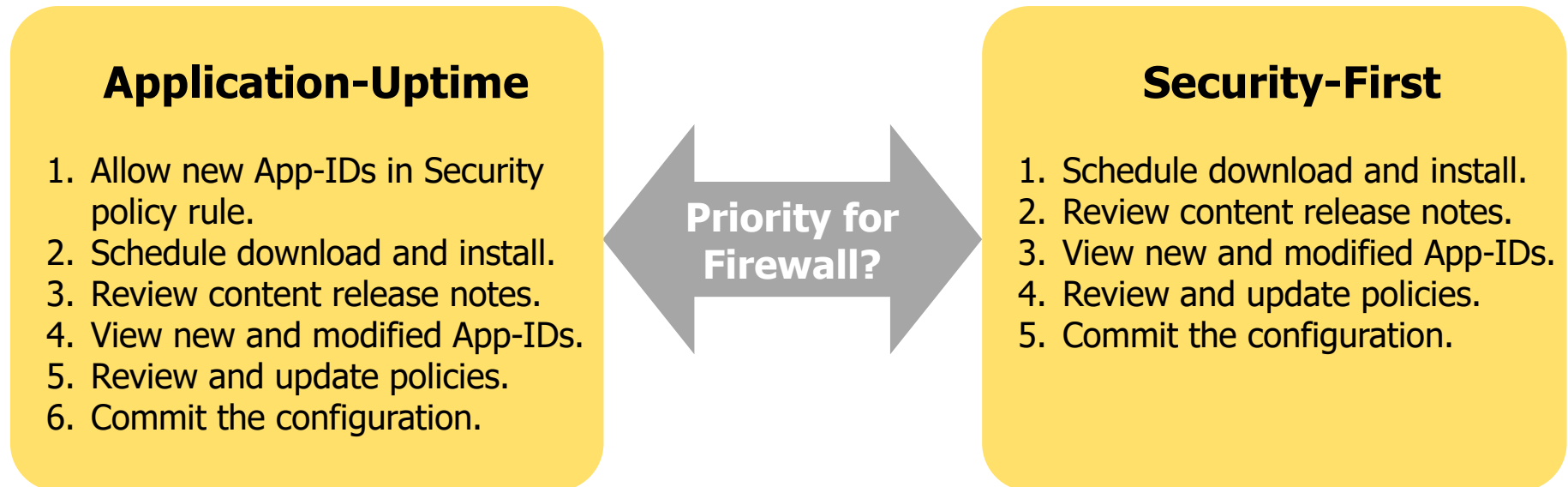


## App-ID and Content-ID Depend on Content Updates



- 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

Application Filter

NAME  ☐ Apply to New App-IDs only  80 matching applications

CATEGORY ^	SUBCATEGORY ^	RISK ^	TAGS ^	CHARACTERISTIC ^
80 business-systems	277 management			1 Data Breaches
	11 marketing			10 Evasive
	20 medical			3 Excessive Bandwidth
	80 office-programs	15 3	0 Palo Alto Networks	7 FEDRAMP
	201 photo-video	5 4	75 Web App	10 HIPAA
	50 proxy		0 empty	11 IP Based Restrictions
	101 remote-access			34 No Certifications
	24 routing			8 PCI

Policies > Security > Add

	NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION
				ZONE	ADDRESS	USER	ZONE	ADDRESS				
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
<div> <div>Applications and Threats</div> <div>Last checked: 2020/07/21 20:14:24 UTC</div> <div>Schedule: <a href="#">Every Wednesday at 01:05 (Download only)</a></div> </div>									
8285-6146	panupv2-all-contents-8285-6146	Apps, Threats	Full	56 MB	22776b5...	2020/06/23 22:53:57 UTC			<a href="#">Download</a>

### Applications and Threats Update Schedule

Recurrence:

Minutes Past Half-Hour:

Action:

☐ Disable new apps in content update

Threshold (hours):

A content update must be at least this many hours old for the action to be taken.

**Allow Extra Time to Review New App-IDs**

Set the amount of time the firewall waits before installing content updates that contain new App-IDs. You can use this wait period to assess and adjust your security policy based on the new App-IDs.

New App-ID Threshold (hours):

## Application-Uptime

### Applications and Threats Update Schedule

Recurrence:

Minutes Past Half-Hour:

Action:

☐ Disable new apps in content update

Threshold (hours):

A content update must be at least this many hours old for the action to be taken.

**Allow Extra Time to Review New App-IDs**

Set the amount of time the firewall waits before installing content updates that contain new App-IDs. You can use this wait period to assess and adjust your security policy based on the new App-IDs.

New App-ID Threshold (hours):

## Security-First



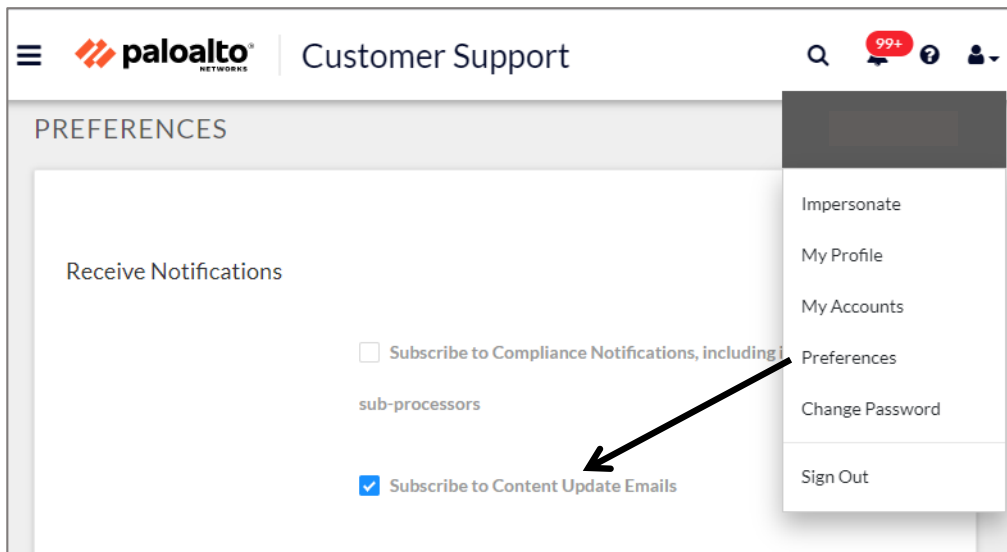
# Review Content Update Release Notes

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: <a href="#">Every Wednesday at 01:02 (Download only)</a>										
8296-6207	panupv2-all-contents-8296-6207	Apps, Threats	Full	56 MB	a643b97f...	2020/07/21 02:20:59 UTC	✓		<a href="#">Install</a> <a href="#">Review Policies</a> <a href="#">Review Apps</a>	<a href="#">Release Notes</a>

<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

## Device > Dynamic Updates

Application-Uptime  
and Security-First

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	✓		<a href="#">Install</a> <a href="#">Review Policies</a> <a href="#">Review Apps</a>	<a href="#">Release Notes</a>

### New and Modified Applications since last installed content

397 items → ×

▾ New Apps

Content Version: 8229

appletvplus

disneyplus

houseparty

overwatch

paloalto-zero-touch-provision

pkix-cmp

ring

traceroute6

universal-data-mover

ws-discovery

Content Version: 8235

http2-5gc

Content Version: 8240

crowdstrike

Content Version: 8291-6174

Name: appletvplus

Standard Ports: tcp/443,80

Depends on: itunes-base, ssl

Implicitly Uses: web-browsing

Previously Identified As: http-video, ssl, web-browsing

Deny Action: drop-reset

Additional Information: Wikipedia Google Yahoo!

Characteristics

Evasive: no

Excessive Bandwidth Use: yes

Used by Malware: no

Capable of File Transfer: no

Has Known Vulnerabilities: yes

Tunnels Other Applications: no

Prone to Misuse: no

Widely Used: yes

Options

Session Timeout (seconds): 30

TCP Timeout (seconds): 3600

TCP Half Closed (seconds): 120

TCP Time Wait (seconds): 15

App-ID Enabled: yes [Disable](#)

Classification

Category: media

Subcategory: photo-video

Risk: 2

Review Policies

Close

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: <a href="#">Every Wednesday at 01:02 (Download only)</a>										
8296-6207	panupv2-all-contents-8296-6207	Apps, Threats	Full	56 MB	a643b97f...	2020/07/21 02:20:59 UTC	✓		<a href="#">Install</a> <a href="#">Review Policies</a> <a href="#">Review Apps</a>	<a href="#">Release Notes</a>

Policy review based on candidate configuration

Content Version: 8296-6207    Rulebase: Security    Virtual System: vsys1    Type: New Applications    Application: crowdstrike    ☐ Include rules with

	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE
<input type="checkbox"/>	Users_Net-Apps	Users_Net	universal	Users_Net	any	any	any	Extranet	any	any	dns	application-default	Allow	none

Security  
 QoS  
 Policy Based Forwarding  
 SD-WAN

New Applications  
 Modified Applications

Enabled  
 abb-rp570  
 abbott-poca  
 amazon-prime-video  
 appletvplus  
 azure-govt-key-vault  
 beyond-trust-remote-suppo  
 cisco-viptela-ipsec-esp  
 classdojo  
 control-m  
 crowdstrike  
 disco

Add app to selected policies    Remove app from selected policies    Close

Review the policy  
impact of new or  
modified  
applications.

# Update Policies

Application-Uptime  
and Security-First

## Device > Dynamic Updates > Review Policies

Policy review based on candidate configuration

Content Version: 8296-6207 Rulebase: Security Virtual System: vsys1 Type: New Applications Application: crowdstrike ☐ Include rules w

	NAME	TAGS	Source					Destination			APPLICATION	SERVICE	ACTION	PROFIL
			TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
<input checked="" type="checkbox"/>	Users_Net-Apps	Users_Net	universal	Users_Net	any	any	any	Extranet	any	any	dns ftp ssh ssl web-browsing	application-default	Allow	none

Add app to selected policies Remove app from selected policies Close

Select policy and click **Add app to selected policies** button.

## Policies > Security

	NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
1	Users_Net-Apps	Users_Net	universal	Users_Net	any	any	any	Extranet	any	any	crowdstrike dns ftp ssh ssl web-browsing	application-default	Allow

Perform a commit after the policy update and before initiating an install.

# 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			<a href="#">Download</a>	<a href="#">Release Notes</a>

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

Download Application and Threats ?

Operation

Download

Status

Completed

Result

Successful

Details

File successfully downloaded

Warnings

## 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	✓		<a href="#">Install</a> <a href="#">Review Details</a> <a href="#">Review Apps</a>	<a href="#">Release Notes</a>

# 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

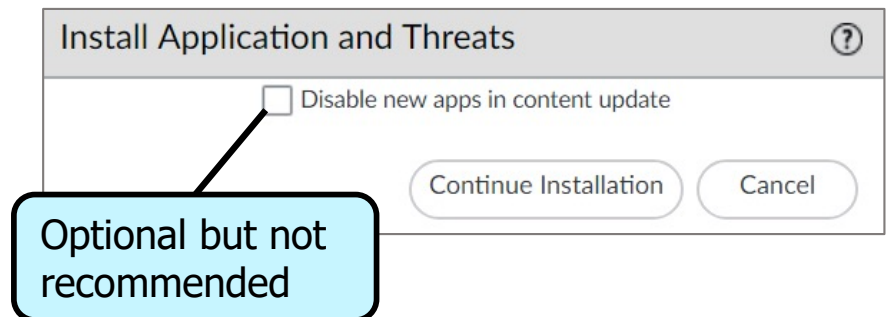
1. Click **Install** to install the content update.

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.**