App-ID

IDENTIFY AND CONTROL APPLICATIONS

- Application identification (App-ID) overview
- Using App-ID in a Security policy
- Identifying unknown application traffic
- Migrating to an App-ID-based Security policy
- Updating App-ID

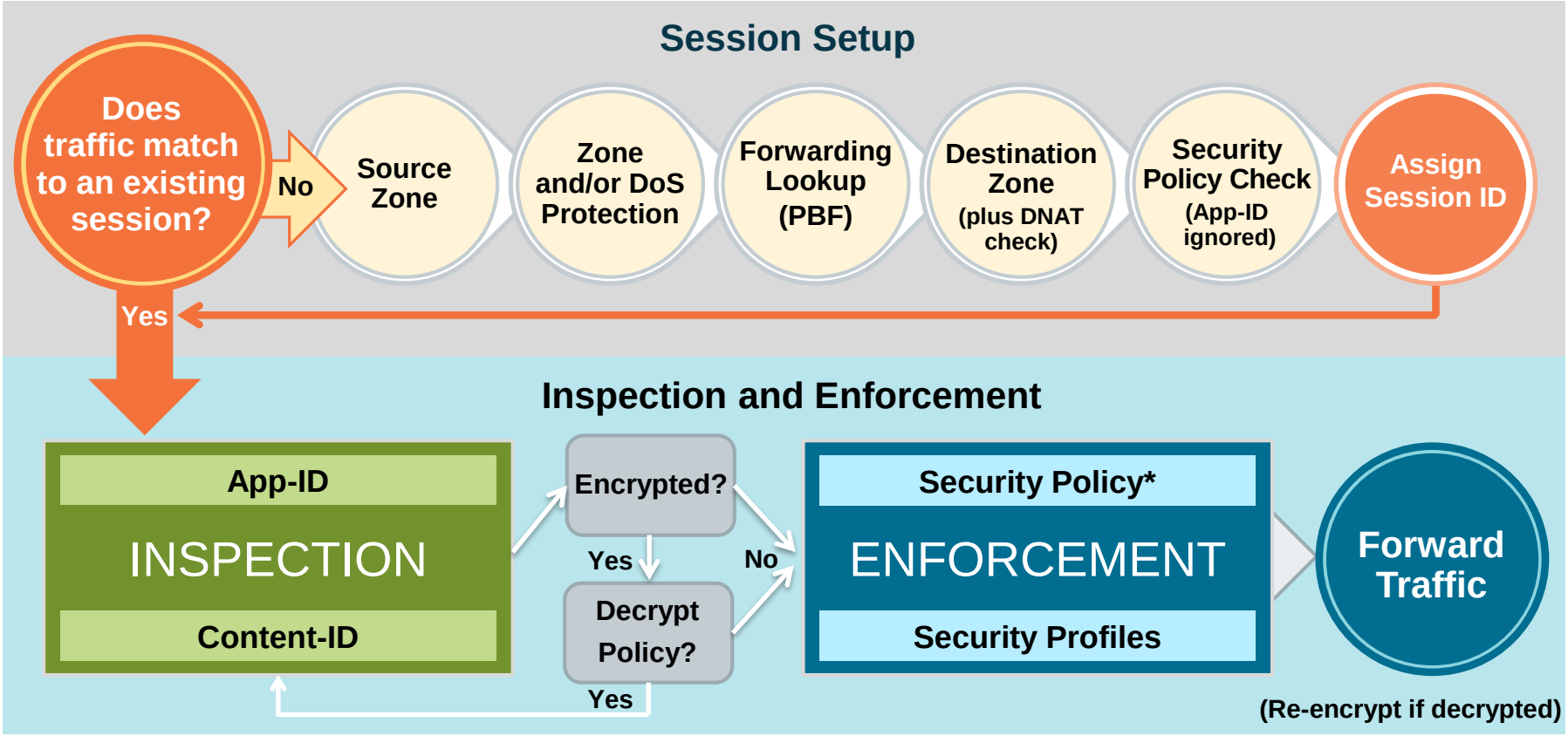
EDU-210 Version A
PAN-OS® 9.0

Agenda

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

- Define application identification
- Describe the four major technologies to help identify applications
- Configure application filters and application groups
- Detect unidentified applications traversing the firewall
- Migrate a port-based rule to an App-ID based rule
- Configure scheduling of updates to App-ID

Flow Logic of the Next-Generation Firewall



* Policy check relies on pre-NAT IP addresses

Application identification (App-ID) overview

Using App-ID in a Security policy

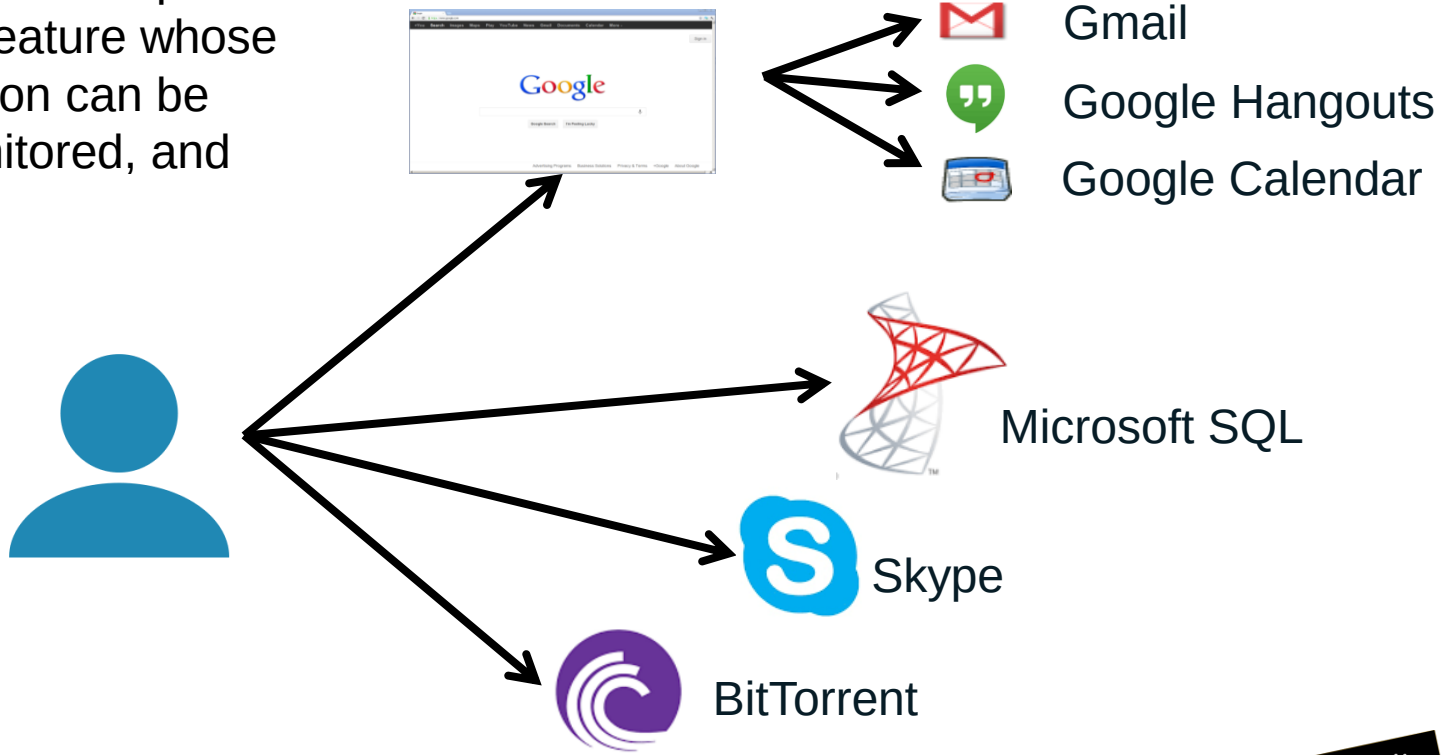
Identifying unknown application traffic

Migrating to an App-ID-based Security policy

Updating App-ID

What Is an Application?

- An *application* is a specific program or feature whose communication can be labeled, monitored, and controlled.



What Is App-ID?

- Multiple techniques to label traffic by application rather than just port

Port-based security rule

				Source				Destination				
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	FTP	egress	universal	inside	any	any	any	outside	any	any	service-ftp	Allow

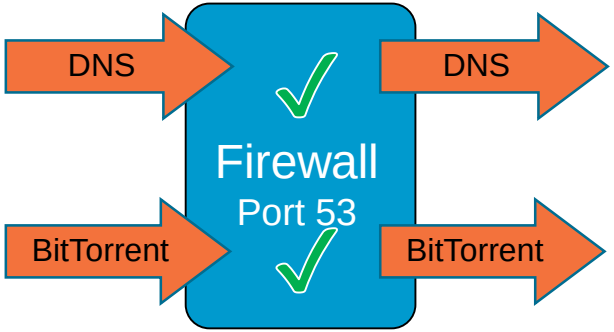
Application-based security rule

				Source				Destination				
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	FTP	egress	universal	inside	any	any	any	outside	any	ftp	application-default	Allow

Port-Based Versus Next-Generation Firewalls

Traditional Firewalls

Firewall Rule: ALLOW Port 53



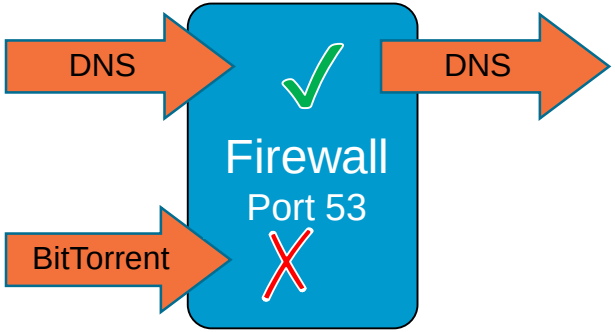
Packet on port 53: Allow

Packet on port 53: Allow

Visibility: Port 53 allowed

Palo Alto Networks Firewalls with App-ID

Firewall Rule: ALLOW DNS



DNS = DNS: Allow

BitTorrent ≠ DNS: Deny

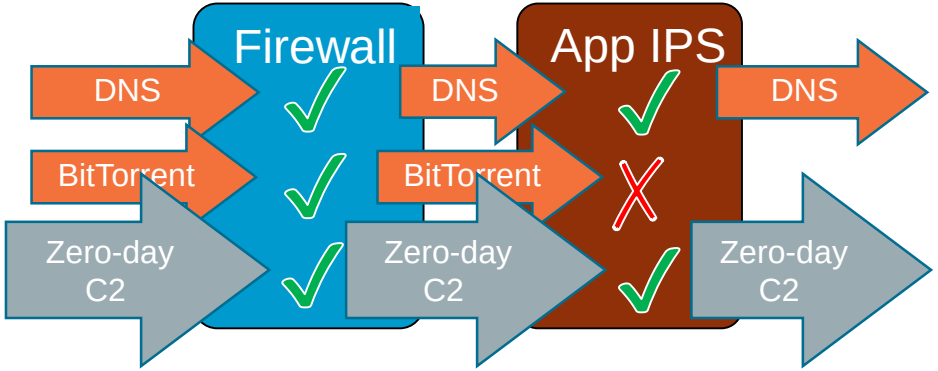
Visibility: BitTorrent detected and blocked

Zero-Day Malware: IPS Versus App-ID

Legacy Firewalls

Firewall Rule: ALLOW Port 53

Application IPS Rule: Block BitTorrent



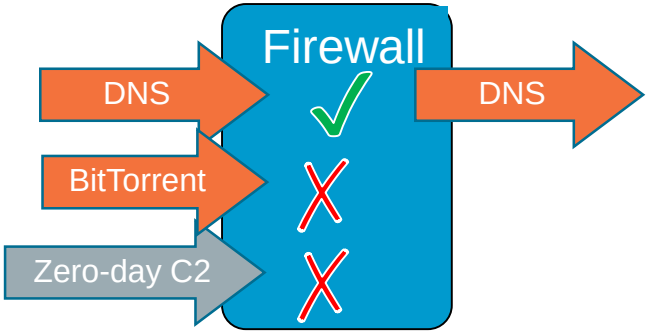
Packet on port 53: Allow

C2 ≠ BitTorrent: Allow

Visibility: Packet on port 53 allowed

Palo Alto Networks Firewall with App-ID

Firewall Rule: ALLOW DNS



DNS = DNS: Allow

C2 ≠ DNS: Deny

Visibility: Unknown traffic detected and blocked

App-ID and UDP

Lightweight UDP Packet

The first UDP packet

```
▷ Ethernet II, Src: 3ComCorp_c7:87:49 (00:04:75:c7:87:49), Dst: 3ComCorp_dd:bb:3a (00:0
▷ Internet Protocol Version 4, Src: 139.133.204.176, Dst: 139.133.204.183
▷ Lightweight User Datagram Protocol, Src Port: 32768 (32768), Dst Port: 1234 (1234)
▷ Data (12 bytes)

0000  00 04 76 dd bb 3a 00 04  75 c7 87 49 08 00 45 00   ..v..:.. u..I..E.
0010  00 28 1a 6a 40 00 40 88  6f 71 8b 85 cc b0 8b 85   .(.j@.@. oq......
0020  cc b7 80 00 04 d2 00 00  38 45 68 65 6c 6c 6f 20   ........ 8Ehello
0030  77 6f 72 6c 64 0a 00 00  00 00 00 00               world... ....
```

Src address and Dst address

```
▷ Internet Protocol Version 4, Src: 139.133.204.176, Dst: 139.133.204.183
▷ Lightweight User Datagram Protocol, Src Port: 32768 (32768), Dst Port: 1234 (1234)
▷ Data (12 bytes)

0000  00 04 76 dd bb 3a 00 04  75 c7 87 49 08 00 45 00   ..v..:.. u..I..E.
0010  00 28 1a 6a 40 00 40 88  6f 71 8b 85 cc b0 8b 85   .(.j@.@. oq......
0020  cc b7 80 00 04 d2 00 00  38 45 68 65 6c 6c 6f 20   ........ 8Ehello
0030  77 6f 72 6c 64 0a 00 00  00 00 00 00               world... ....
```

Src port and Dst port

```
▷ Internet Protocol Version 4, Src: 139.133.204.176, Dst: 139.133.204.183
▷ Lightweight User Datagram Protocol, Src Port: 32768 (32768), Dst Port: 1234 (1234)
◢ Data (12 bytes)
    Data: 68656c6c6f20776f726c640a
    [Length: 12]

0000  00 04 76 dd bb 3a 00 04  75 c7 87 49 08 00 45 00   ..v..:.. u..I..E.
0010  00 28 1a 6a 40 00 40 88  6f 71 8b 85 cc b0 8b 85   .(.j@.@. oq......
0020  cc b7 80 00 04 d2 00 00  38 45 68 65 6c 6c 6f 20   ........ 8Ehello
0030  77 6f 72 6c 64 0a 00 00  00 00 00 00               world... ....
```

Application data

App-ID and TCP

Client

Server

Example of an HTTP web request

SYN

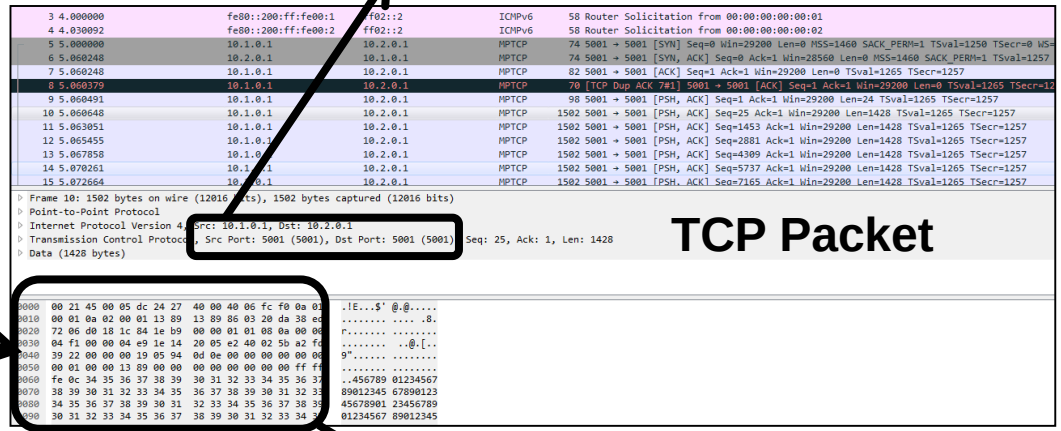
SYN, ACK

ACK

GET

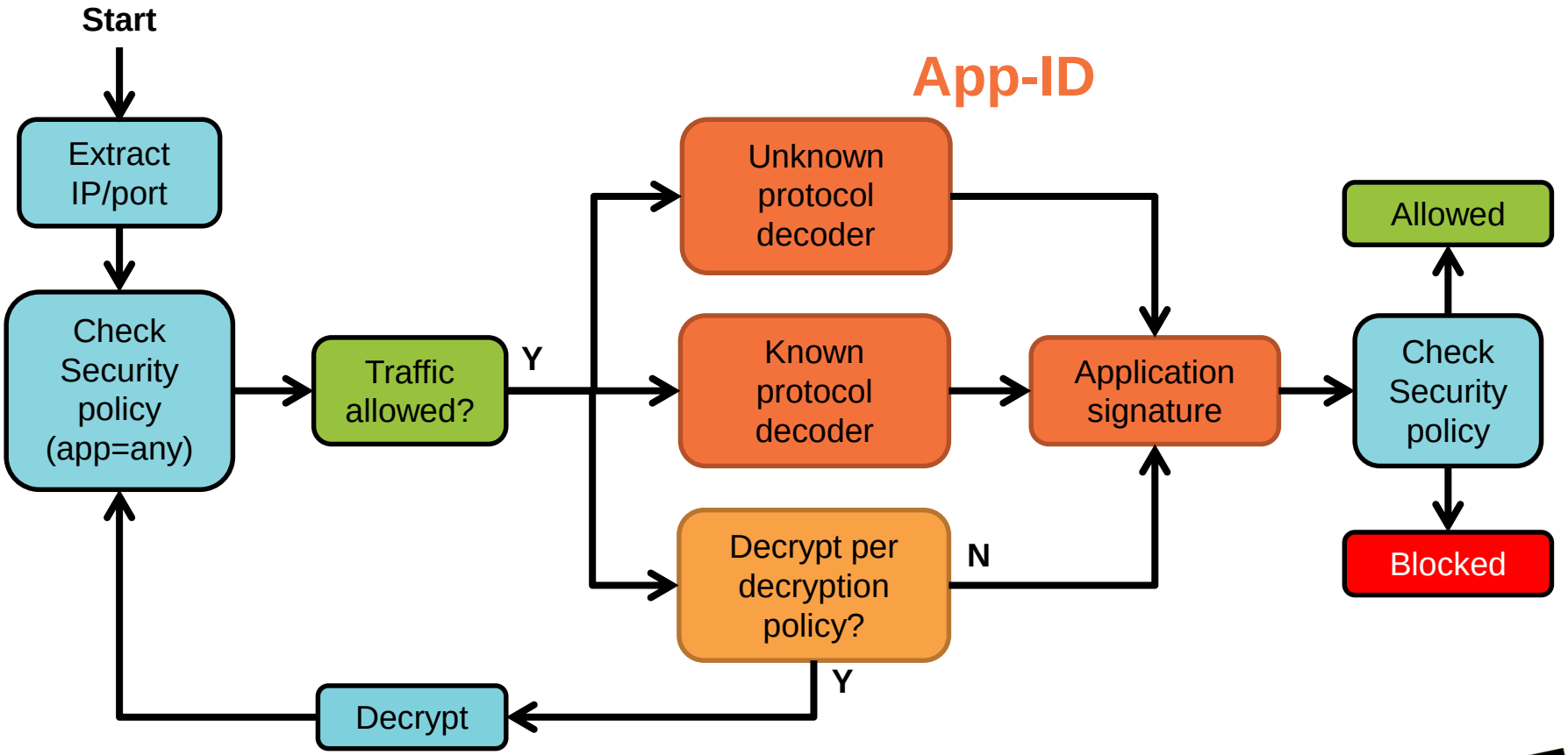
Application Data
0001010100011111011
1010110001100111101

- Src address and Dst address
- Src port and Dst port



Application data

App-ID Operation



Application identification (App-ID) overview

Using App-ID in a Security policy

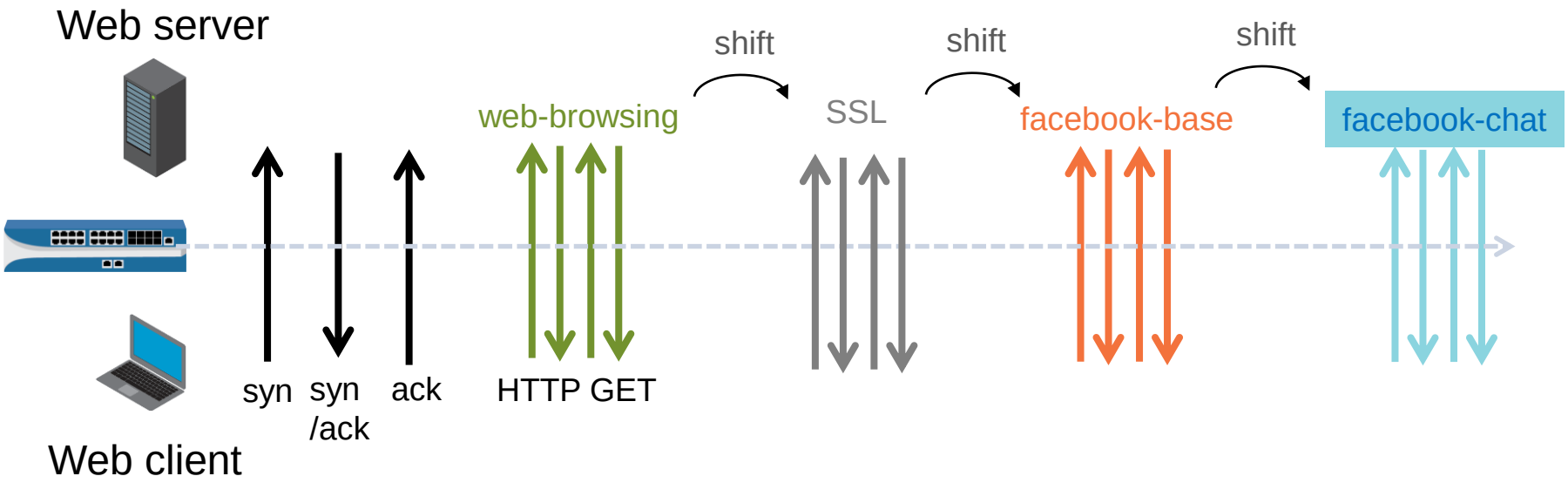
Identifying unknown application traffic

Migrating to an App-ID-based Security policy

Updating App-ID

Application Shifts

- Network traffic can shift from one application to another during a session.



Dependent Applications

Joe

192.168.15.22

Zone: Inside

http://login.microsoftonline.com
Destination Port: TCP 80

1. HTTP GET = web-browsing

2. Request specifically Office on Demand

Office on Demand

74.125.224.64

Zone: Outside

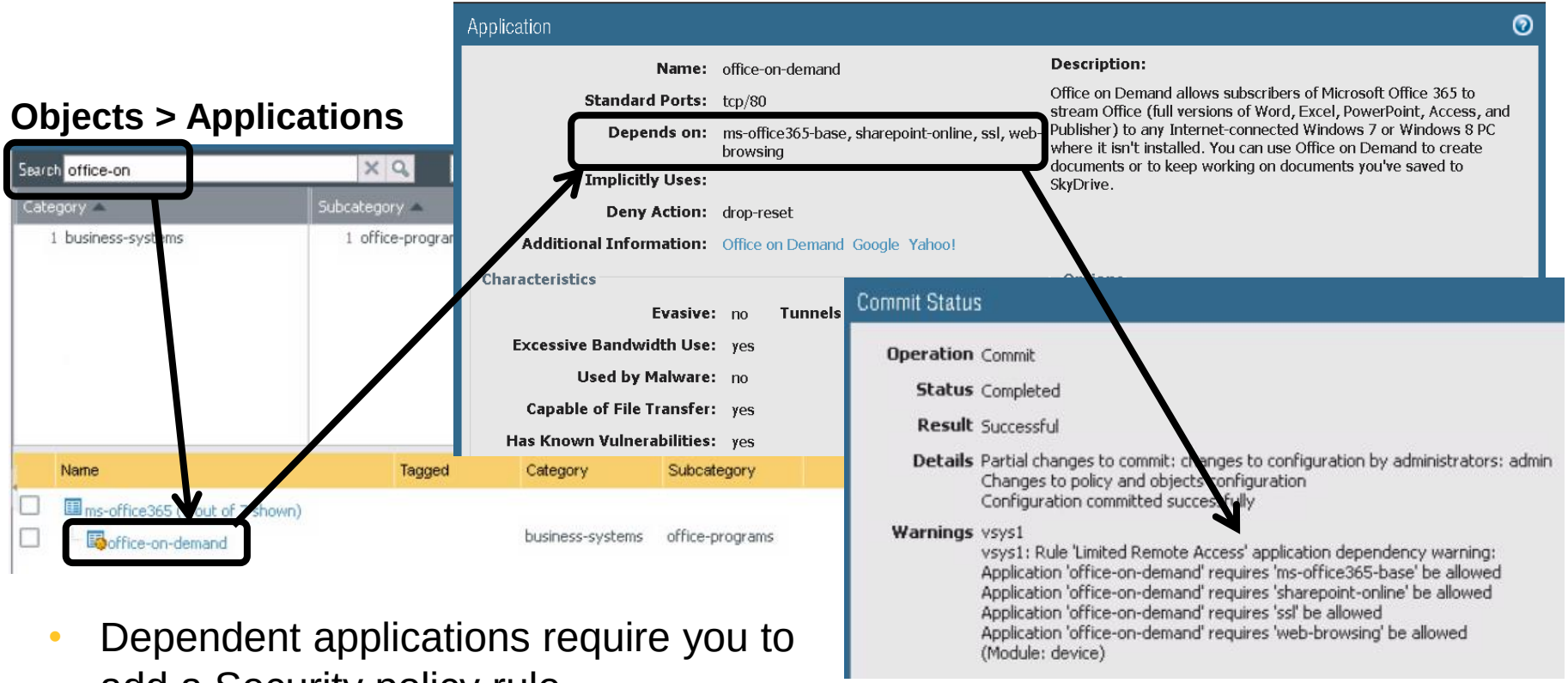
	Name	Tags	Type	Source				Destination		Rule Usage			Application	Service
				Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit		
1	Requi						any						ssl web-browsing	application-default
2	Office						any	outside	any	-	-	-	ms-office365-base office-on-demand sharepoint-online	application-default

office-on-demand dependent on ms-office365-base and sharepoint-online

Application shift

Determining Application Dependencies

Objects > Applications



- Dependent applications require you to add a Security policy rule.

Implicit Applications

- Many common applications implicitly allow parent applications.
- No explicit Security policy rule is required for a parent application.

				Source				Destination					
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
1	App Specific	internal	universal	inside	any	any	any	dmz	any	flash ping ssl web-browsing	application-default	Allow	
2	Allow Facebook	egress	universal	inside	any	any	any	outside	any	facebook-base facebook-chat facebook-mail	application-default	Allow	

facebook-base implicitly allows web-browsing and SSL

Determining Implicitly Used Applications

Objects > Applications

Search facebook

Category	Subcat
8 collaboration	1 e
1 general-internet	1 F
3 media	1 g
	1 i
	2 p
	5 s
	1 v

Name

- facebook (10 out of 11 shown)
- facebook-apps
- facebook-base
- facebook-chat
- facebook-file-sharing
- facebook-mail
- facebook-posting

Application

Name: facebook-base

Standard Ports: tcp/80,443

Depends on:

Implicitly Uses: ssl, web-browsing

Deny Action: drop-reset

Additional Information: Wikipedia Google Yahoo!

Description:

Facebook (branded as "facebook") is a social networking website launched on February 4, 2004. The free-access website is privately owned and operated by Facebook, Inc. Users can join networks organized by city, workplace, school, and region to connect and interact with other people. People can also add friends and send them messages, and update their personal profile to notify friends about themselves. The website's name refers to the paper facebooks depicting members of a campus community that some American colleges and prepatory schools give to incoming

Characteristics

Evasive:	no	Tunnels Other Applications:	yes
Excessive Bandwidth Use:	no	Prone to Misuse:	no
Used by Malware:	yes	Widely Used:	yes
Capable of File Transfer:	yes		
Has Known Vulnerabilities:	yes		

Options

TCP Timeout (seconds):	3600	Customize...
TCP Half Closed (seconds):	120	Customize...
TCP Time Wait (seconds):	15	Customize...
App-ID Enabled:	yes	

Classification

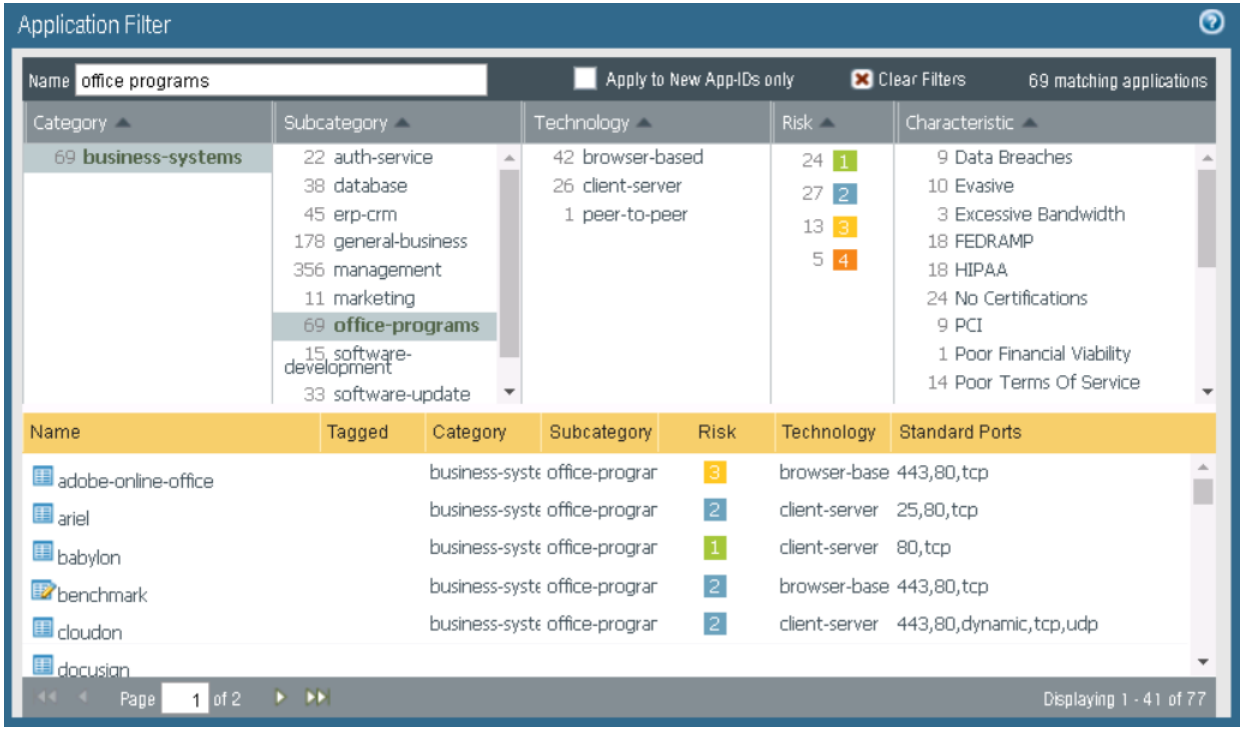
Category: collaboration

Subcategory: social-networking

collaboration	social-networking	4	browser-based	tcp/443,80

Application Filter

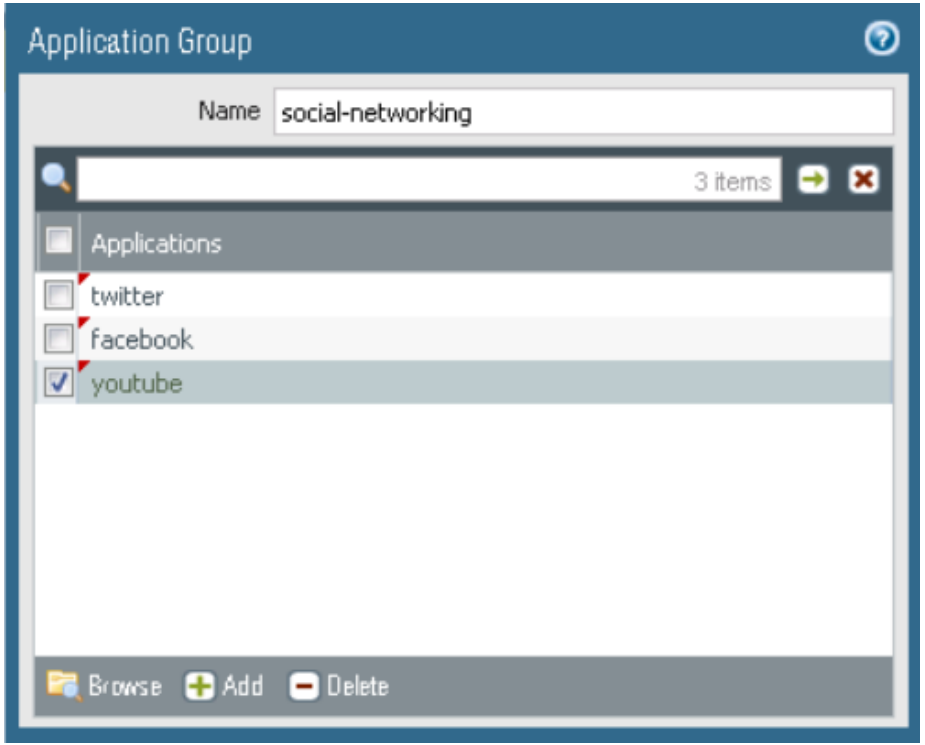
Objects > Application Filter > Add



- Dynamic grouping of applications
- Created by selecting filters in the App-ID database
- Used to simplify Security, QoS, and PBF policy rulebases

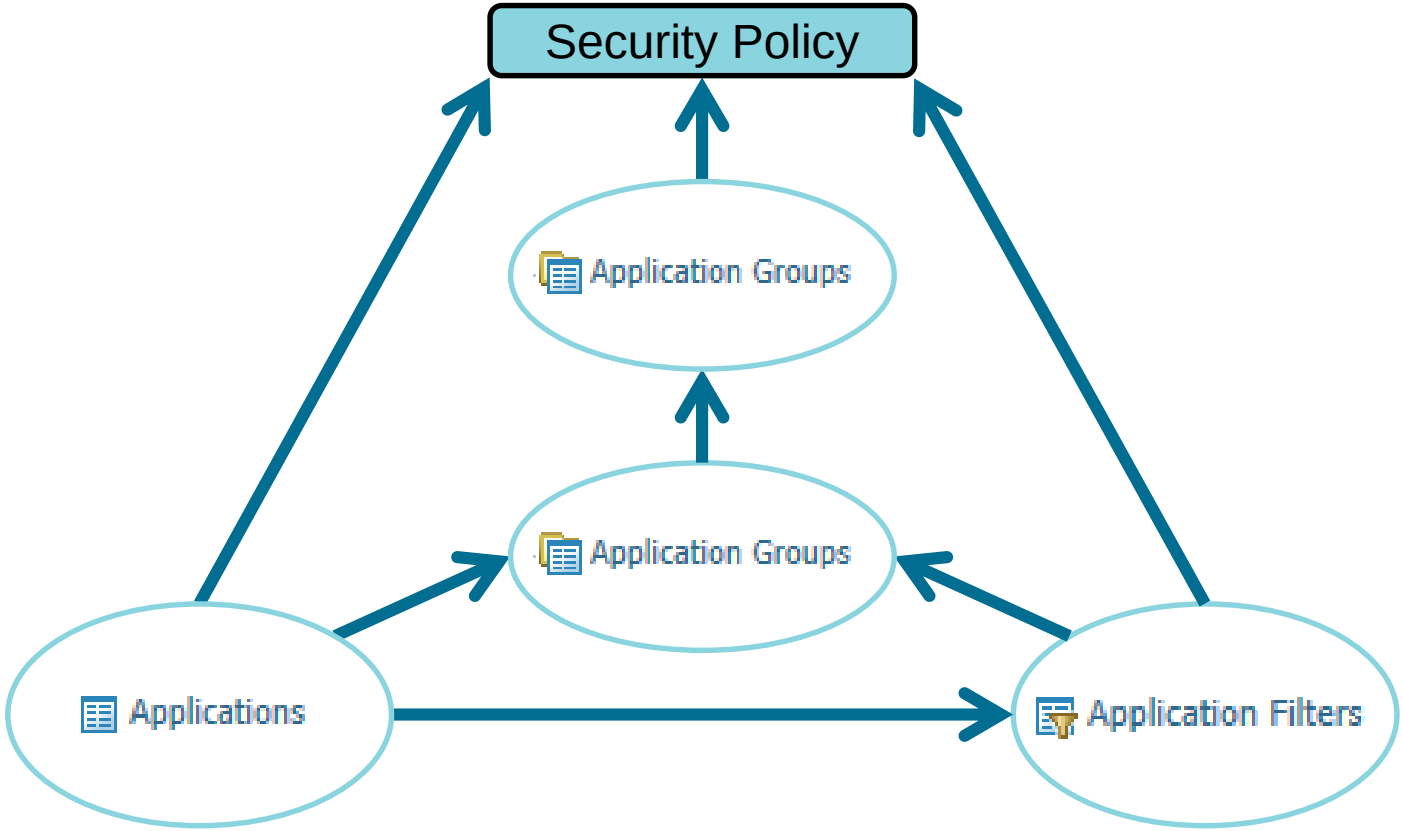
Application Groups

Objects > Application Groups > Add



- Static, administrator-defined sets of applications
- Used to simplify Security and QoS policy rulebases

Nesting Application Groups and Filters



Applications and Security Policy Rules

Policies > Security

Application Filter

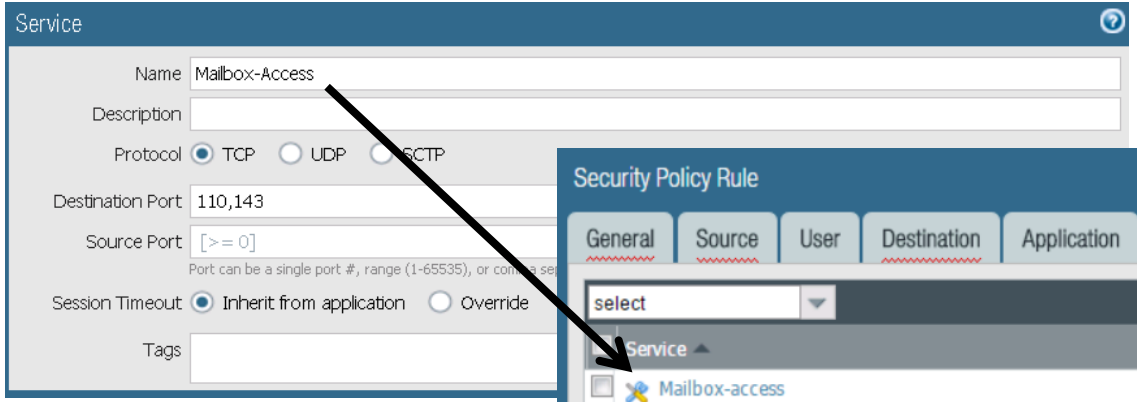
Application Group

				Source				Destination					
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
1	Social Networking	egress	universal	inside	any	any	any	outside	any	social-networking	application-default	Allow	
2	Office Programs	egress	universal	inside	any	any	any	outside	any	office programs	application-default	Allow	
3	FTP Server	egress	universal	inside	any	any	any	outside	any	ftp	application-default	Allow	

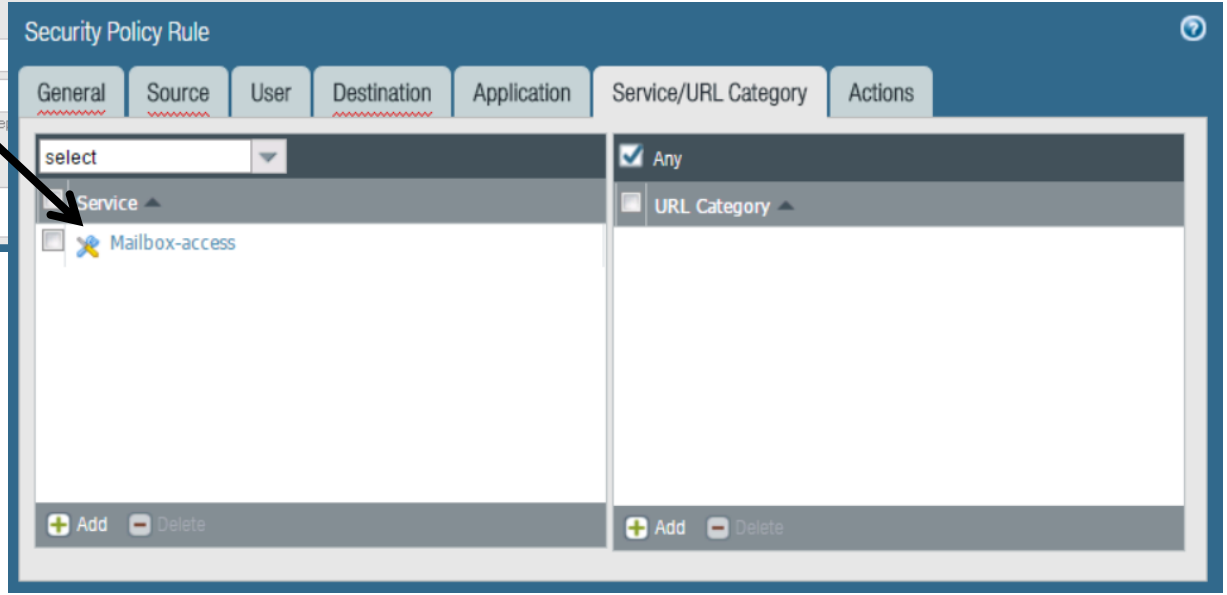
Application

Creating and Using Custom Services

Objects > Services



Policies > Security

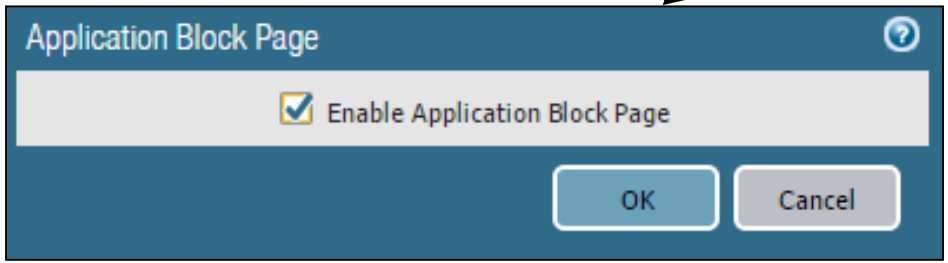


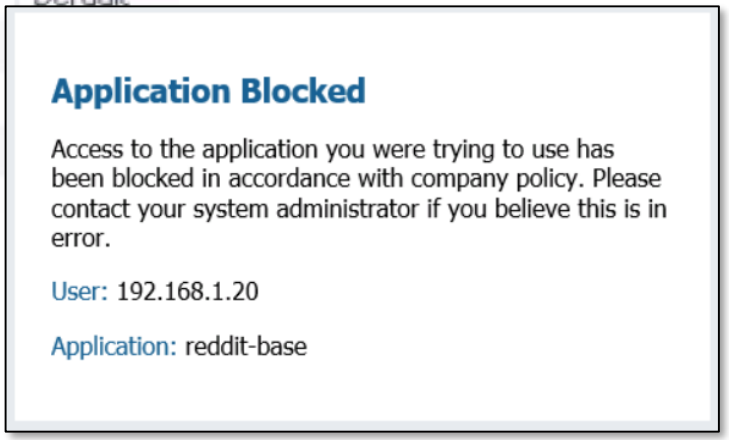
Application Block Page

- For blocked web-based applications, a response page can be displayed in the user's browser.

Device > Response Pages

Type	Action	Location
Antivirus / Anti-spyware Block Page		Default
Application Block Page	Enabled	
Captive Portal Comfort Page		
Data Filtering Block Page		
File Blocking Continue Page		





Application identification (App-ID) overview

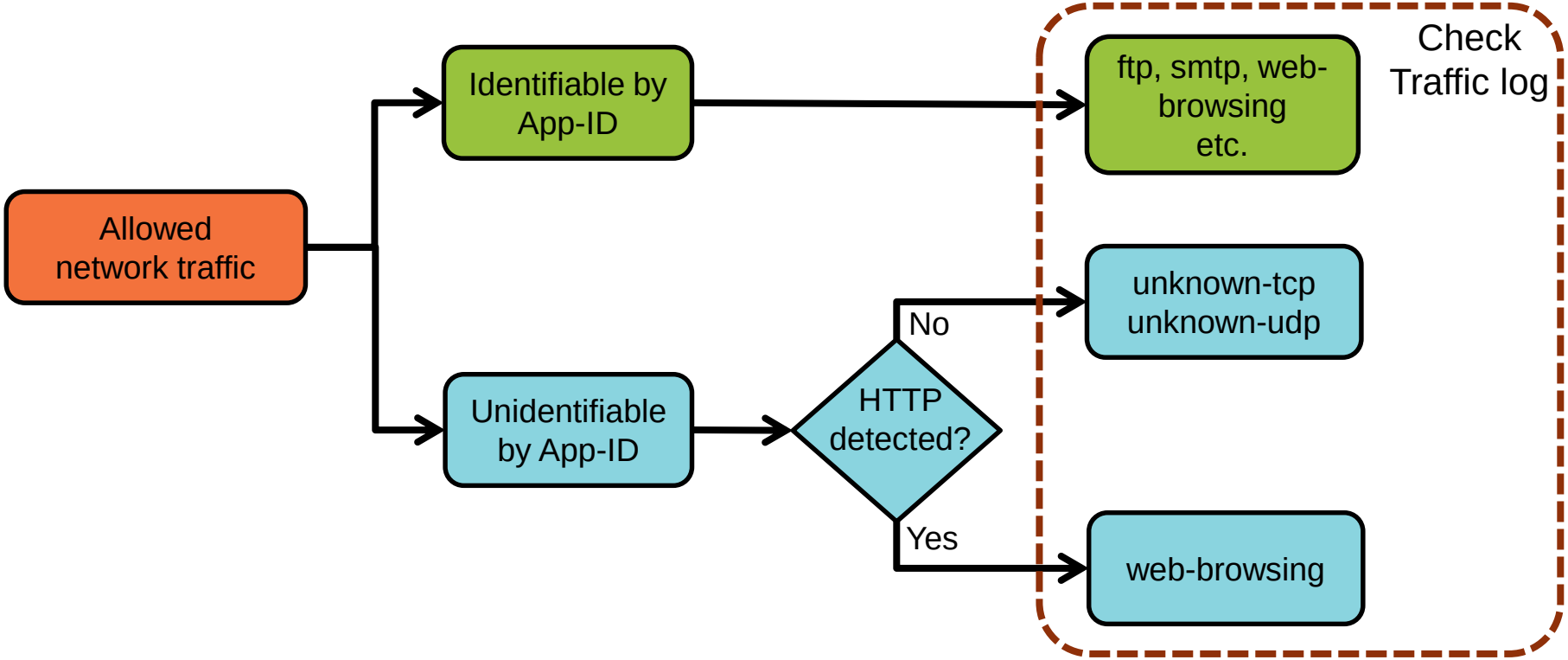
Using App-ID in a Security policy

Identifying unknown application traffic

Migrating to an App-ID-based Security policy

Updating App-ID

Unknown Network Traffic



Identify Unknown Application Traffic

Iterative process:

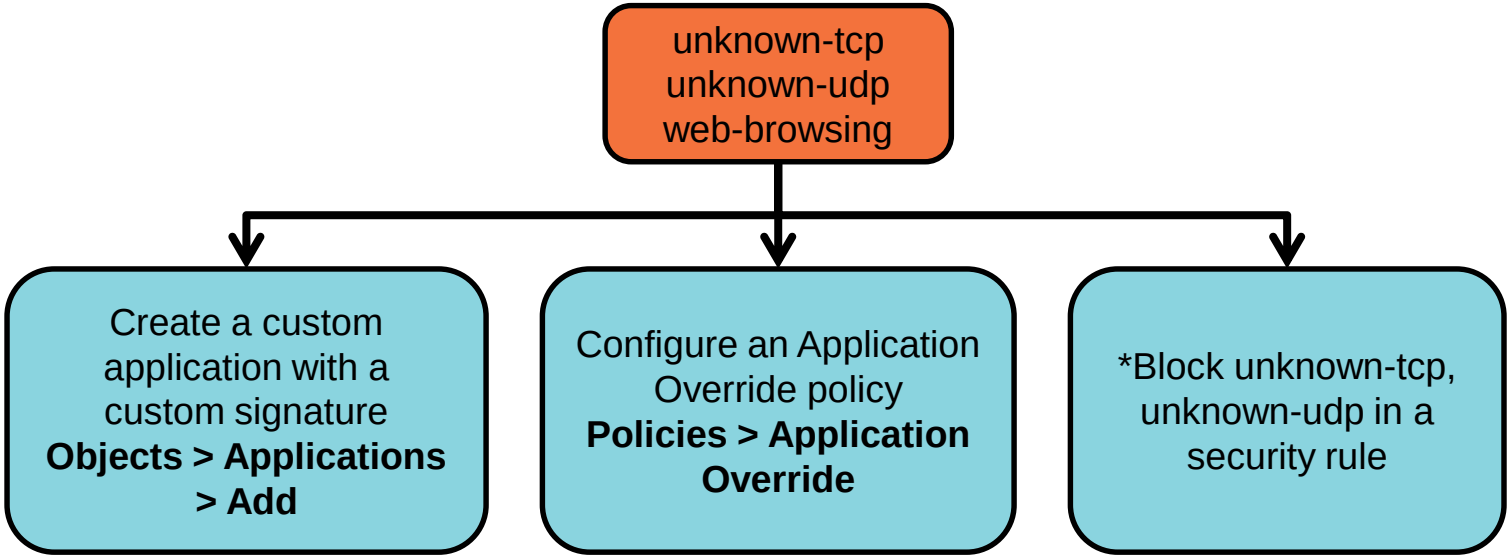
- Create rules to allow or block applications known to be traversing the firewall
- Create a *temporary* rule to detect unidentified applications traversing the firewall
- As applications are identified, create specific rules to allow or block them

Policies > Security

				Source				Destination				
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	Known Good	egress	universal	any	any	any	any	any	any	known good	application-default	Allow
2	Known Bad	egress	universal	any	any	any	any	any	any	known bad apps	application-default	Deny
3	Unclassified Apps	egress	universal	any	any	any	any	any	any	any	any	Allow

Monitor > Logs > Traffic to see application identification

Controlling Unknown Applications



*Could block more traffic than intended

Application identification (App-ID) overview

Using App-ID in a Security policy

Identifying unknown application traffic

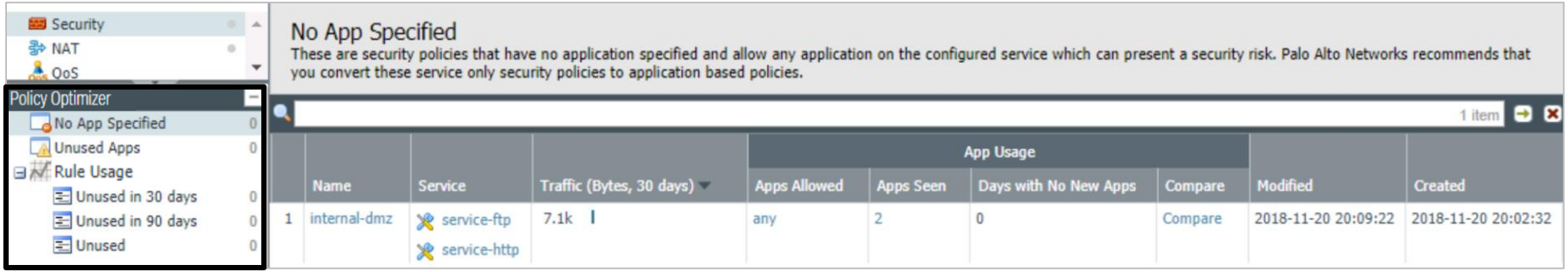
Migrating to an App-ID-based Security policy

Updating App-ID

Policy Optimizer

- Migrate port-based rules to App-ID-based rules
- Help reduce attack surface and provide information about application usage
- Prevent evasive applications from running on non-standard ports
- Identify over-provisioned application-based rules

Policies > Security > Policy Optimizer > No App Specified



Moving to Application-Based Policies

Phase 1

Identify legacy port-based policy rules

Phase 2

Add application-based rules above corresponding port-based rules

Phase 3

Remove port-based rules

Phase 1: Viewing Data of Port-Based Rules

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

Policies > Security

	Name	Source			Destination		Application	Service
		Zone	Address	User	Zone	Address		
1	internal-dmz	inside	any	any	dmz	any	any	service-ftp service-http

Application “any” triggers **No App Specified** match

Policies > Security > Policy Optimizer > No App Specified

Security
NAT
QoS
Policy Optimizer
No App Specified 0
Unused Apps 0
Rule Usage
Unused in 30 days 0
Unused in 90 days 0
Unused 0

No App Specified

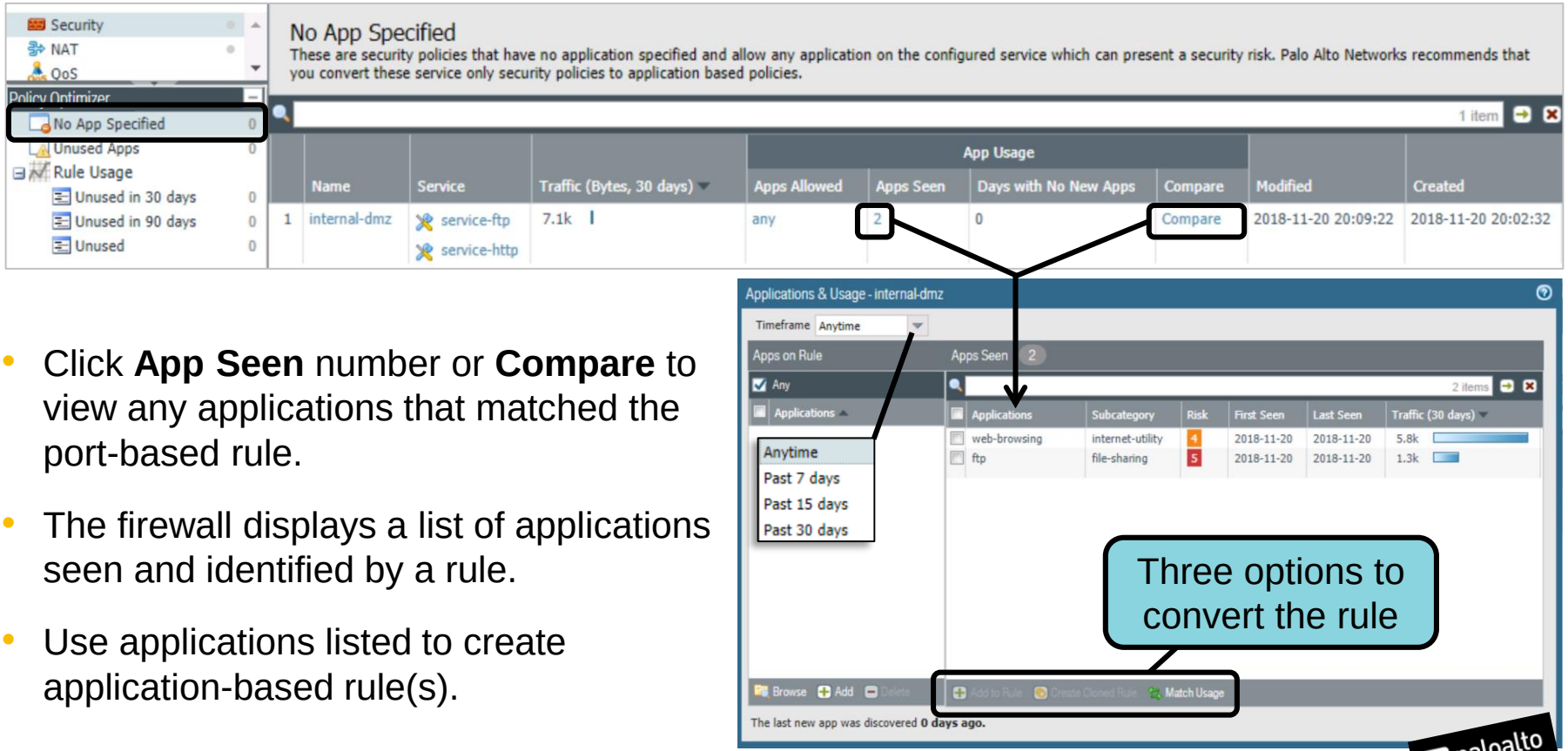
These are security policies that have no application specified and allow any application on the configured service which can present a security risk. Palo Alto Networks recommends that you convert these service only security policies to application based policies.

1 item

	Name	Service	Traffic (Bytes, 30 days)	App Usage				Modified	Created
				Apps Allowed	Apps Seen	Days with No New Apps	Compare		
1	internal-dmz	service-ftp service-http	7.1k	any	2	0	Compare	2018-11-20 20:09:22	2018-11-20 20:02:32

Discovering Applications Matching a Port-Based Rule

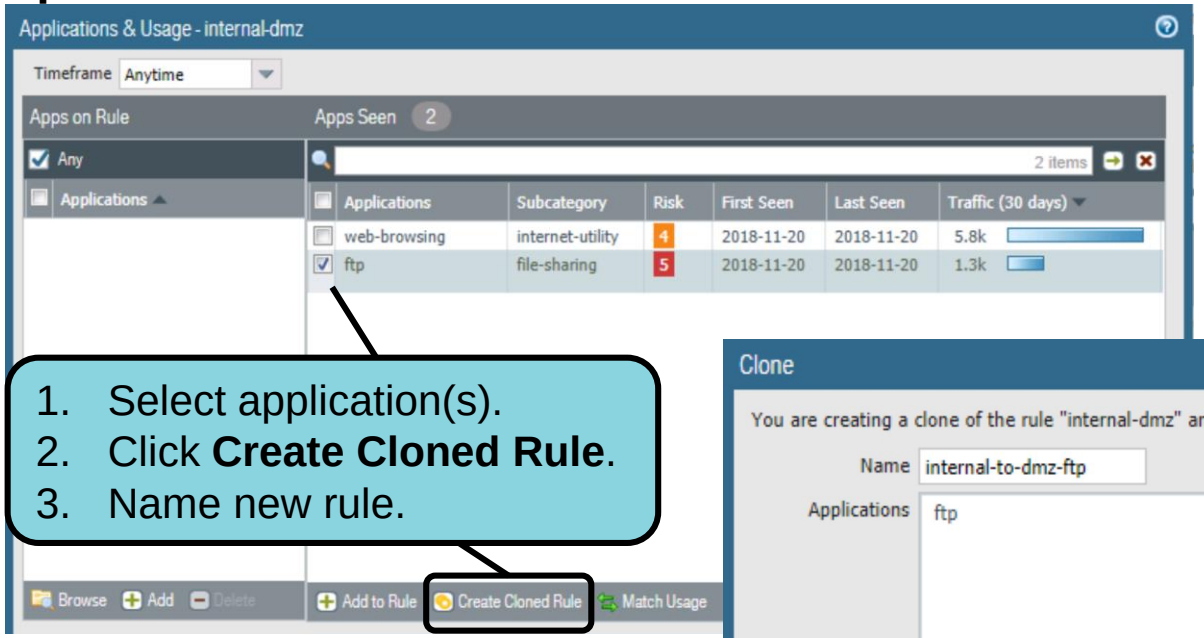
Policies > Security > Policy Optimizer > No App Specified



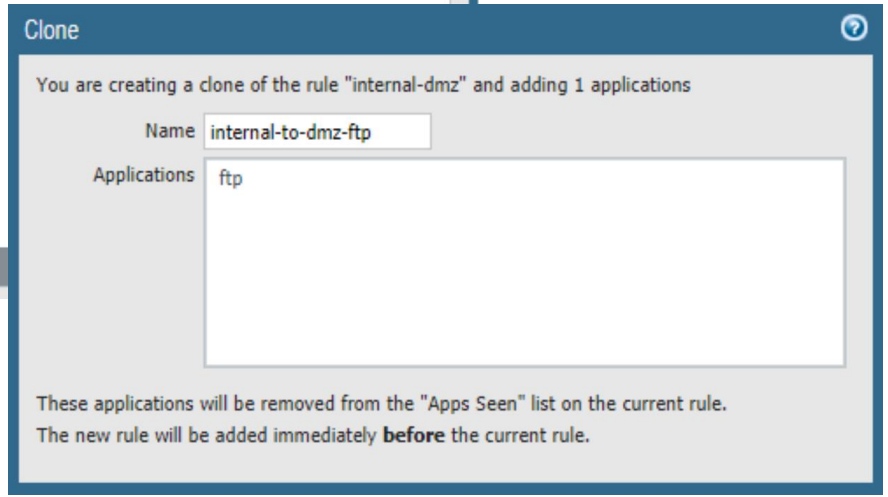
- Click **App Seen** number or **Compare** to view any applications that matched the port-based rule.
- The firewall displays a list of applications seen and identified by a rule.
- Use applications listed to create application-based rule(s).

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

Option 1 of 3:



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

Result of Using “Create Cloned Rule”

Applications & Usage - internal-dmz

Timeframe Anytime

Apps on Rule | Apps Seen 1

Any | 1 item

Applications	Applications	Subcategory	Risk	First Seen	Last Seen	Traffic (30 days)
	web-browsing	internet-utility	4	2018-11-20	2018-11-20	5.8k

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

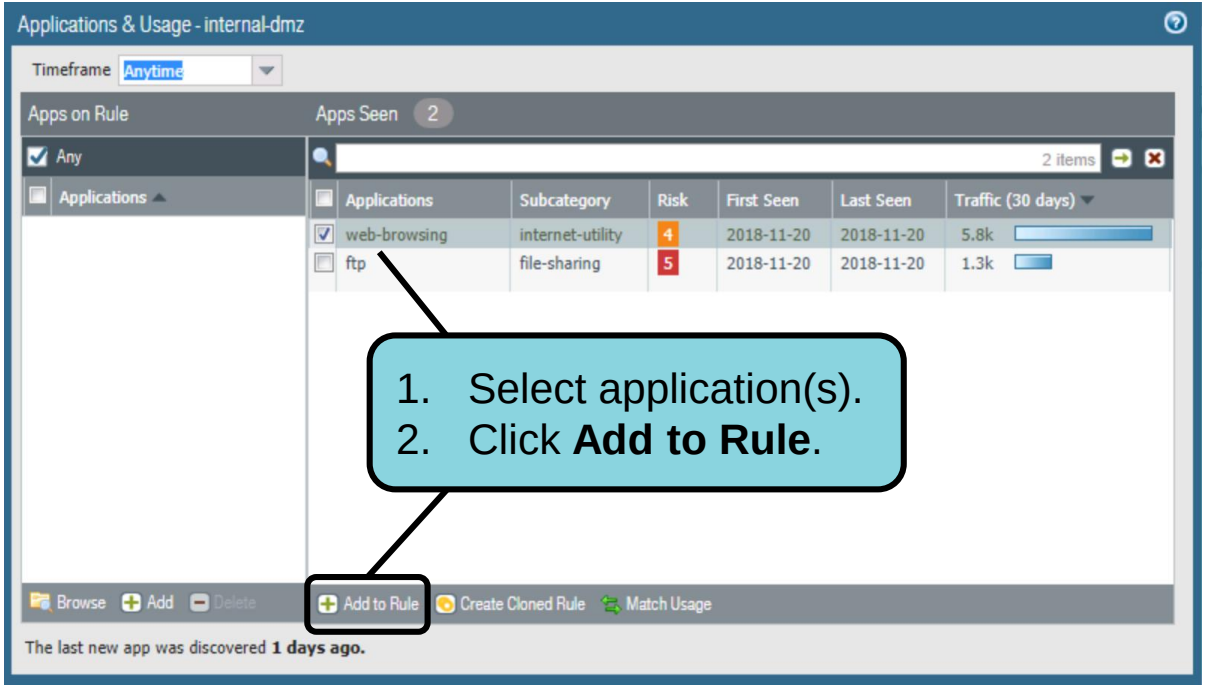
Policies > Security

		Source			Destination				
	Name	Zone	Address	User	Zone	Address	Application	Service	Action
1	internal-to-dmz-ftp	inside	any	any	dmz	any	ftp	service-ftp service-http	Allow
2	internal-dmz	inside	any	any	dmz	any	any	service-ftp service-http	Allow

Must manually configure as **application-default**

Replacing a Port-Based Rule Using “Add to Rule”

Option 2 of 3:



- Firewall *replaces* port-based rule with application-based rule.
- Moves *selected* applications to a new rule
- Lists and prompts for required application dependencies
- Riskier method because some required applications could be inadvertently missed.

Result of Using “Add to Rule”

Applications & Usage - internal-dmz

Timeframe Anytime

The **web-browsing** application is added to the left-side **Applications** column.

Apps on Rule | Apps Seen 2

Any | 2 items

Applications
web-browsing

Applications	Subcategory	Risk	First Seen	Last Seen	Traffic (30 days)
web-browsing	internet-utility	4	2018-11-20	2018-11-20	5.8k
ftp	file-sharing	5	2018-11-20	2018-11-20	1.3k

Policies > Security

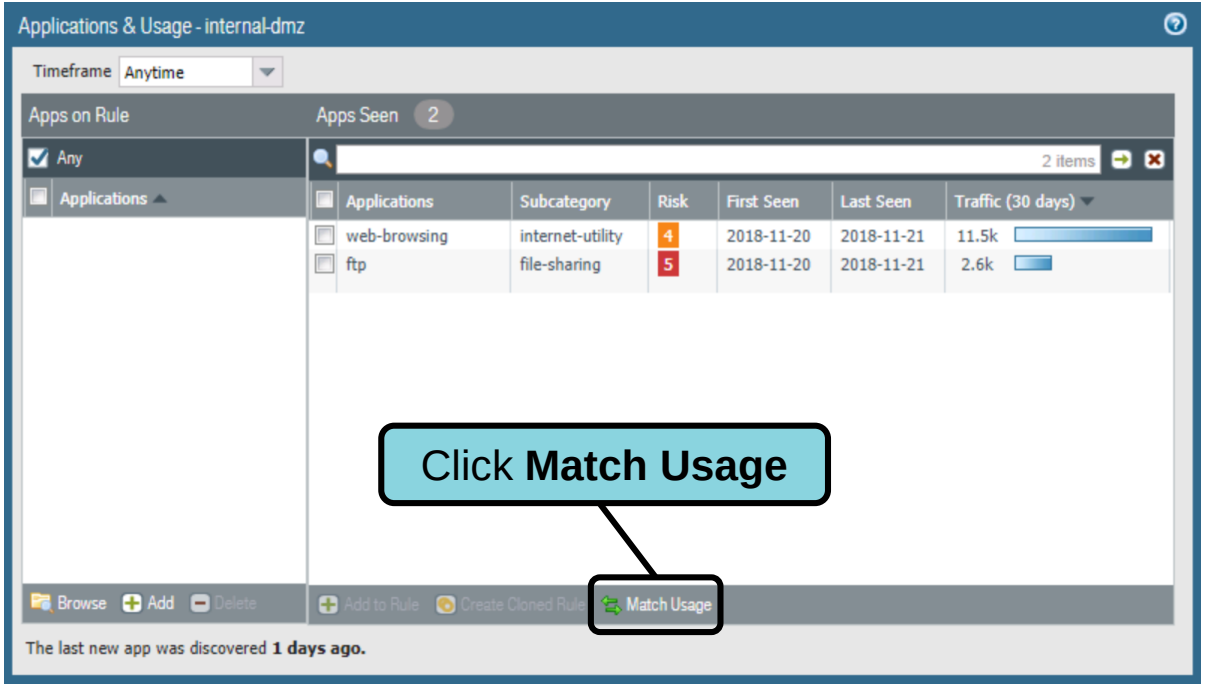
Must manually configure as **application-default**

	Name	Source			Destination		Application	Service	Action
		Zone	Address	User	Zone	Address			
1	internal-dmz	inside	any	any	dmz	any	web-browsing	service-ftp service-http	Allow

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

Replacing a Port-Based Rule Using “Match Usage”

Option 3 of 3:



- 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 Using “Match Usage”

Applications & Usage - internal-dmz

Timeframe Anytime

Apps on Rule | Apps Seen 2

Any | 2 items

Applications	Applications	Subcategory	Risk	First Seen	Last Seen	Traffic (30 days)
web-browsing	web-browsing	internet-utility	4	2018-11-20	2018-11-21	11.5k
ftp	ftp	file-sharing	5	2018-11-20	2018-11-21	2.6k

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

Must manually configure as **application-default**

Policies > Security

	Name	Source Zone	Source Address	Source User	Destination Zone	Destination Address	Application	Service	Action
1	internal-dmz	inside	any	any	dmz	any	ftp web-browsing	service-ftp service-http	Allow

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

Prioritizing Port-Based Rules to Convert

Prioritize rules passing more data

Prioritize rules with more applications

Prioritize rules that are more stable

Security
NAT
QoS
Policy Based Forwarding
Decryption

No App
These are
you conve
ecommends that

Policy Optimizer
- No App Specified 2
- Unused Apps 1
- Rule Usage
  - Unused in 30 days 2
  - Unused in 90 days 2
  - Unused 2

	Name	Service	Traffic (Bytes, 30 days)	App Usage			Compare	Modified	Created
				Apps Allowed	Apps Seen	Days with No New Apps			
5	inside-to-dmz	service-http	493.1k	any	1	0	Compare	2018-10-20 18:52:23	2018-10-03 16:48:47
2	allow-ftp-port	service-ftp	3.7k	any	1	0	Compare	2018-10-20 18:34:28	2018-10-20 18:34:28

Prioritize rules that match more sessions

Security
NAT
QoS
Policy Based Forwarding
Decryption

Hit Count

Monitoring rule usage can help ensure rules are performing as expected, and can help identify rules that should be removed to reduce your attack surface.

Timeframe All time Usage Unused Exclude rules reset during the last 90 days

Policy Optimizer
- No App Specified 2
- Unused Apps 1
- Rule Usage
  - Unused in 30 days 2
  - Unused in 90 days 2
  - Unused 2

	Name	Rule Usage				Modified	Created
		Hit Count	Last Hit	First Hit	Reset Date		
3	block-known-bad-ips	0	-	-	-	2018-10-20 00:53:00	2018-10-20 00:53:00
7	intrazone-default	0	-	-	-	2018-10-03 16:48:47	2018-10-03 16:48:47

Phase 3: Reviewing Port-Based Rules

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

Policies > Security

		Source			Destination					Rule Usage
	Name	Zone	Address	HIP Profile	Zone	Address	Application	Service	Action	Hit Count
5	app-based-inside-to-dmz	inside	any	any	dmz	any	web-browsing	application-default	Allow	58
6	inside-to-dmz	inside	any	any	dmz	any	any	service-http	Allow	0

Add | Delete | Clone | Override | Revert | Enable | Disable | Move | PDF/CSV | Highlight Unused Rules | Reset Rule Hit Counter | Group | View

Reset

All rules

Selected rules

Disabling Port-Based Rules

Policies > Security

		Source			Destination					Rule Usage
	Name	Zone	Address	HIP Profile	Zone	Address	Application	Service	Action	Hit Count
5	app-based-inside-to-dmz	inside	any	any	dmz	any	web-browsing	application-default	Allow	66
6	*inside-to-dmz*	*inside*	*any*	*any*	*dmz*	*any*	*any*	*service-http*	*Allow*	0

Add | Delete | Clone | Override | Revert | Enable | Disable | Move | PDF/CSV | Highlight Unused Rules | Reset Rule Hit Counter | Group | View

- 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).

Removing 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

		Source			Destination					Rule Usage
	Name	Zone	Address	HIP Profile	Zone	Address	Application	Service	Action	Hit Count
5	app-based-inside-to-dmz	inside	any	any	dmz	any	web-browsing	application-default	Allow	66
6	*inside-to-dmz*	*inside*	*any*	*any*	*dmz*	*any*	*any*	*service-http*	*Allow*	0

Add | Delete | Clone | Override | Revert | Enable | Disable | Move | PDF/CSV | Highlight Unused Rules | Reset Rule Hit Counter | Group | View

		Source			Destination					Rule Usage
	Name	Zone	Address	HIP Profile	Zone	Address	Application	Service	Action	Hit Count
5	app-based-inside-to-dmz	inside	any	any	dmz	any	web-browsing	application-default	Allow	66

Application identification (App-ID) overview

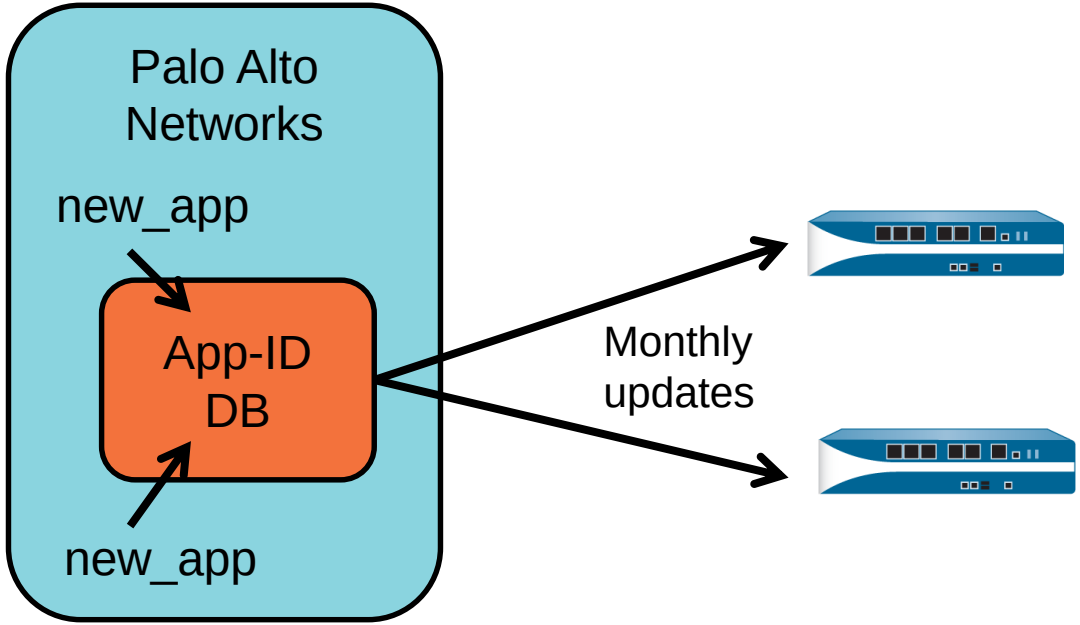
Using App-ID in a Security policy

Identifying unknown application traffic

Migrating to an App-ID-based Security policy

Updating App-ID

Dynamic Content Updates: App-ID



Choices:

- Scheduled download only
- Scheduled download and install
- Manual download and install

Scheduled App-ID Updates

Device > Dynamic Updates

Version	File Name	Features	Type	Size	Release Date	Download...	Currently Installed	Action
Applications and Threats	**Last checked:** 2019/02/20 01:05:11 UTC			**Schedule:**	**Every Wednesday at 01:05 (Download only)**			
748-4315	panupv2-all-contents-748-4315	Apps, Threats	Full	35 MB	2017/11/08 00:49:47 UTC			Download
8109-5227	panupv2-all-contents-8109-5227	Apps, Threats	Full	44 MB	2018/12/28 00:48:11 UTC		✔	Review Policies Review Apps

Click to schedule updates.

Applications and Threats Update Schedule

Recurrence: Hourly

Every 30 Minutes
Hourly
Daily
Weekly
None

utes Past Hour: 5

Action: download-and-install

None
download-only
download-and-install

Disable new apps in content update

If selected, new application signatures are disabled.

Threshold (hours): [1 - 336]

Allow Extra Time to Review New App

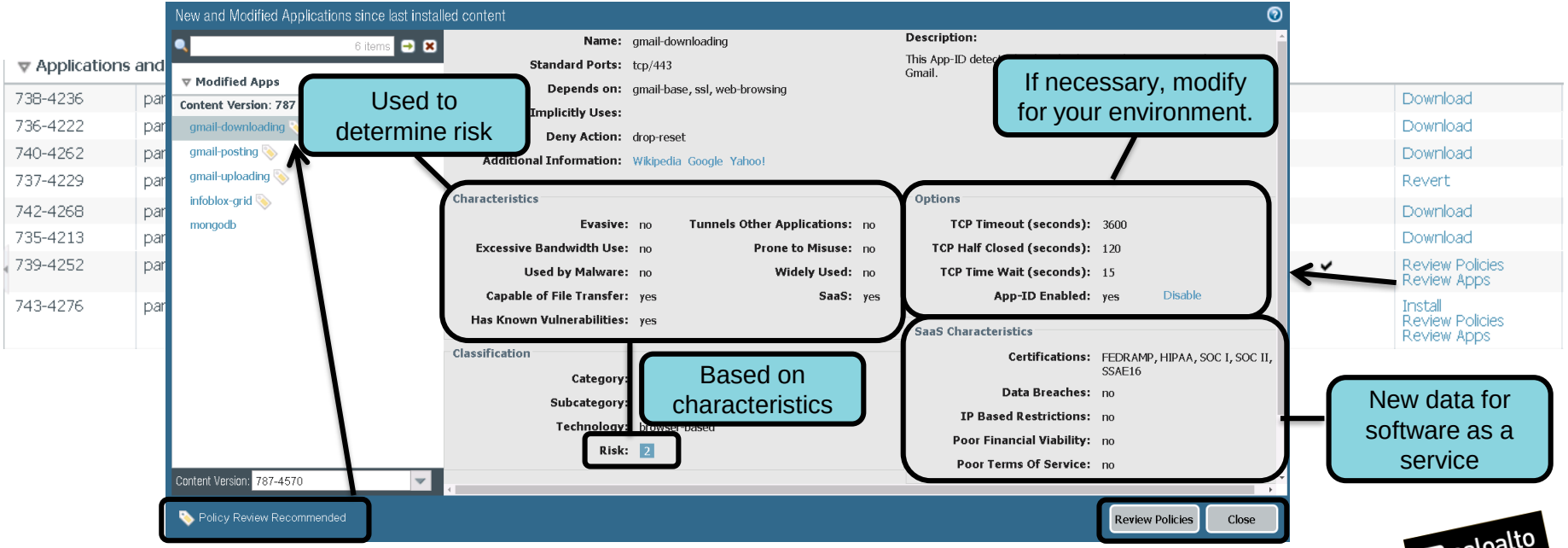
Set the amount of time the firewall waits
new App-IDs. You can use this wait peri
based on the new App-IDs.

New App-ID Threshold (hours): [1 - 336]

Content Update Absorption

- **Review Apps** for list of modified applications and details for each application
- **Review Policies** to see policy rules that may enforce traffic differently

Device > Dynamic Updates



Pre-Analyze New Application and Policy Interaction

Objects > Applications

24sevenoffice	business-systems	erp-crm
2ch		
2ch-base	collaboration	social-networking
2ch-posting	collaboration	web-posting
360-safeguard-update	business-systems	software-update
3pc	networking	ip-protocol
4shared	general-internet	file-sharing

Page 1 of 66

Add | Delete | Clone | Enable | Disable | Import | Export | PDF/CSV | Review Policies | Tag

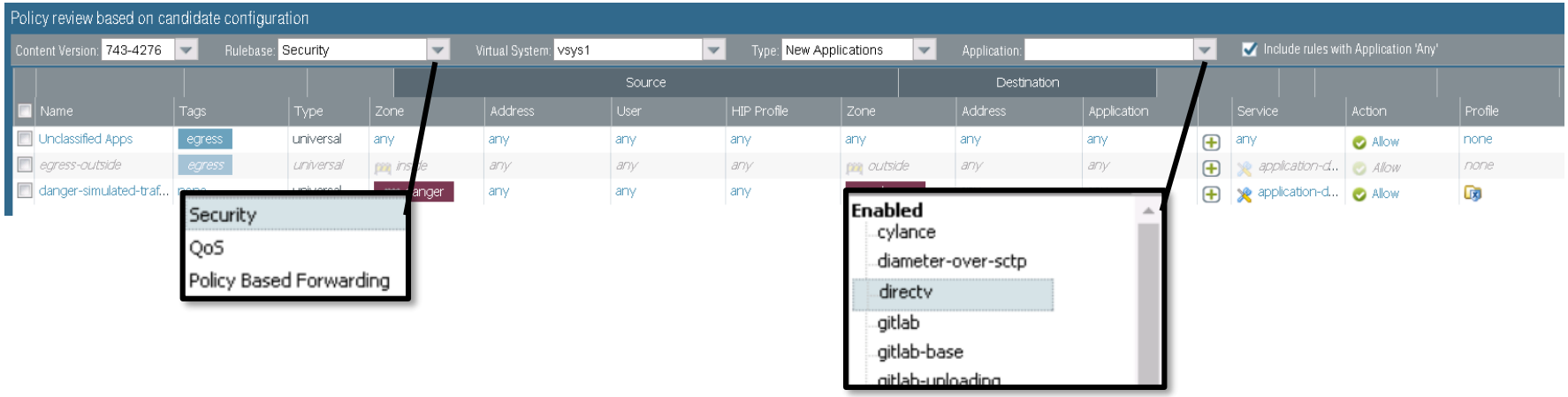
Select and enable or disabled application(s).

Click to preview new application signature and policy interaction.

Review Policies

- View which policy rules will match new applications

Objects > Applications > Review Policies



Module Summary

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

- Define application identification
- Describe the four major technologies to help identify applications
- Configure application filters and application groups
- Detect unidentified applications traversing the firewall
- Migrate a port-based rule to an App-ID based rule
- Configure scheduling of updates to App-ID

Questions?

App-ID Lab (Pages 65-89 in the Lab Guide)

- Load a firewall lab configuration
- Create an application-based firewall rule
- Enable the Application Block Page
- View the Traffic log for application information

PROTECTION. DELIVERED.

paloalto NETWORKS®