

App-ID



EDU-210 Version A  
PAN-OS® 9.0

## *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

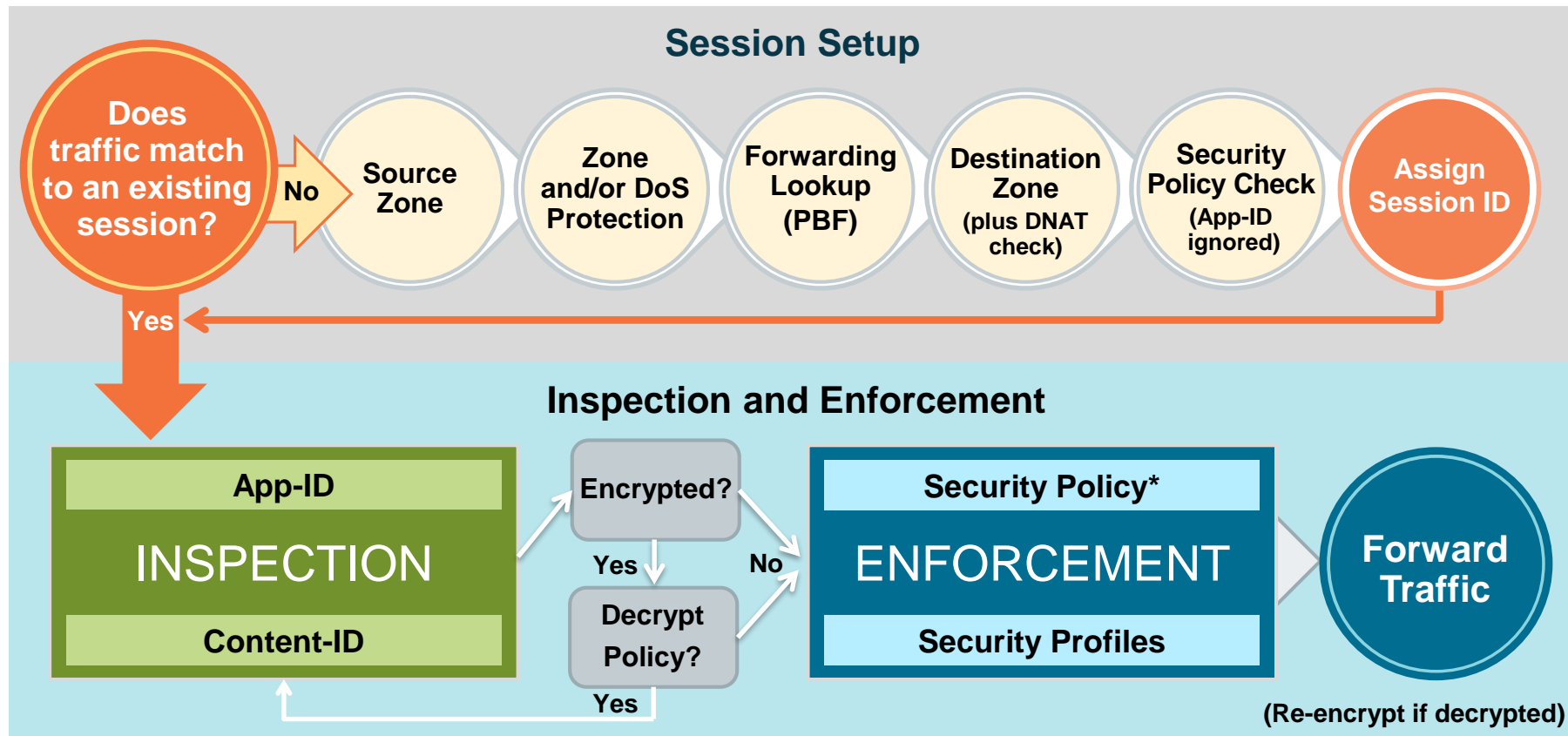
# Agenda

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

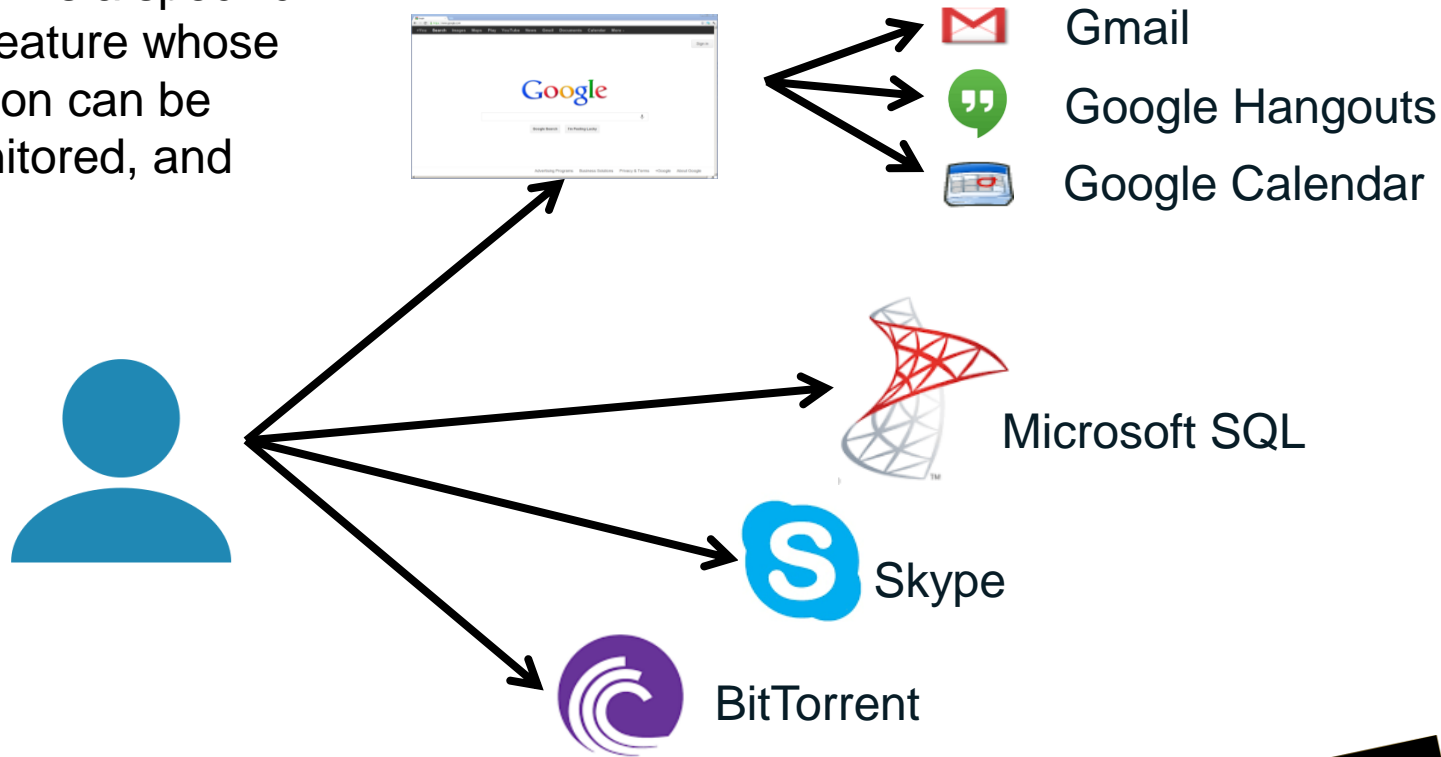
Identifying unknown application traffic

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

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

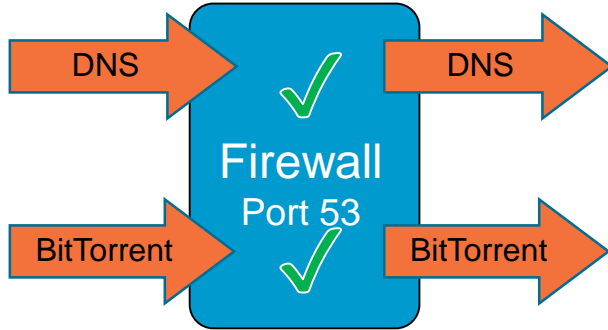
## Application-based security rule

	Name	Tags	Type	Source				Destination		Application	Service	Action
				Zone	Address	User	HIP Profile	Zone	Address			
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



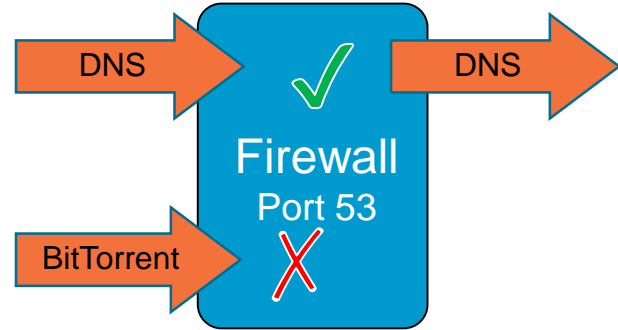
Packet on port 53: Allow

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

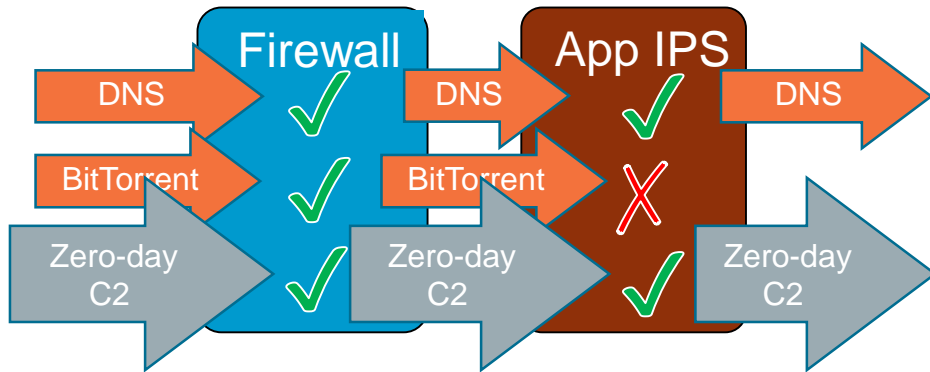
Visibility: BitTorrent detected and blocked

# Zero-Day Malware: IPS Versus App-ID

## Legacy Firewalls

Firewall Rule: ALLOW Port 53

Application IPS Rule: Block BitTorrent



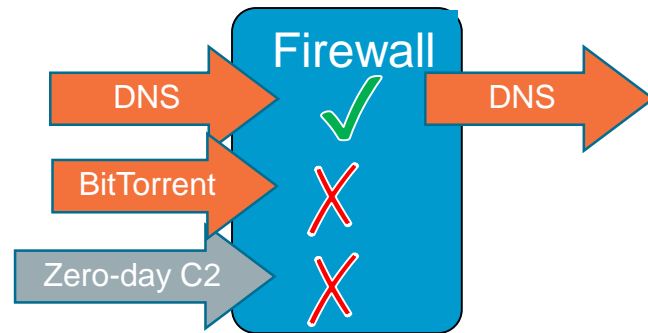
Packet on port 53: Allow

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

```
▶ Ethernet II, Src: 3ComCorp_c7:87:49 (00:04:75:c7:87:49), Dst: 3ComCorp_dd:bb:3a (00:07:09:00:00:00)
▶ 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... ..
```

```
▶ 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... ..
```

```
▶ 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... ..
```

The first UDP packet

Src address and Dst address

Src port and Dst port

Application data

# App-ID and TCP



## Client

## Example of an HTTP web request

Application Data  
000101010001111011  
101011000110011101

## SYN

SYN, ACK

ACK

GET

## Server

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

```

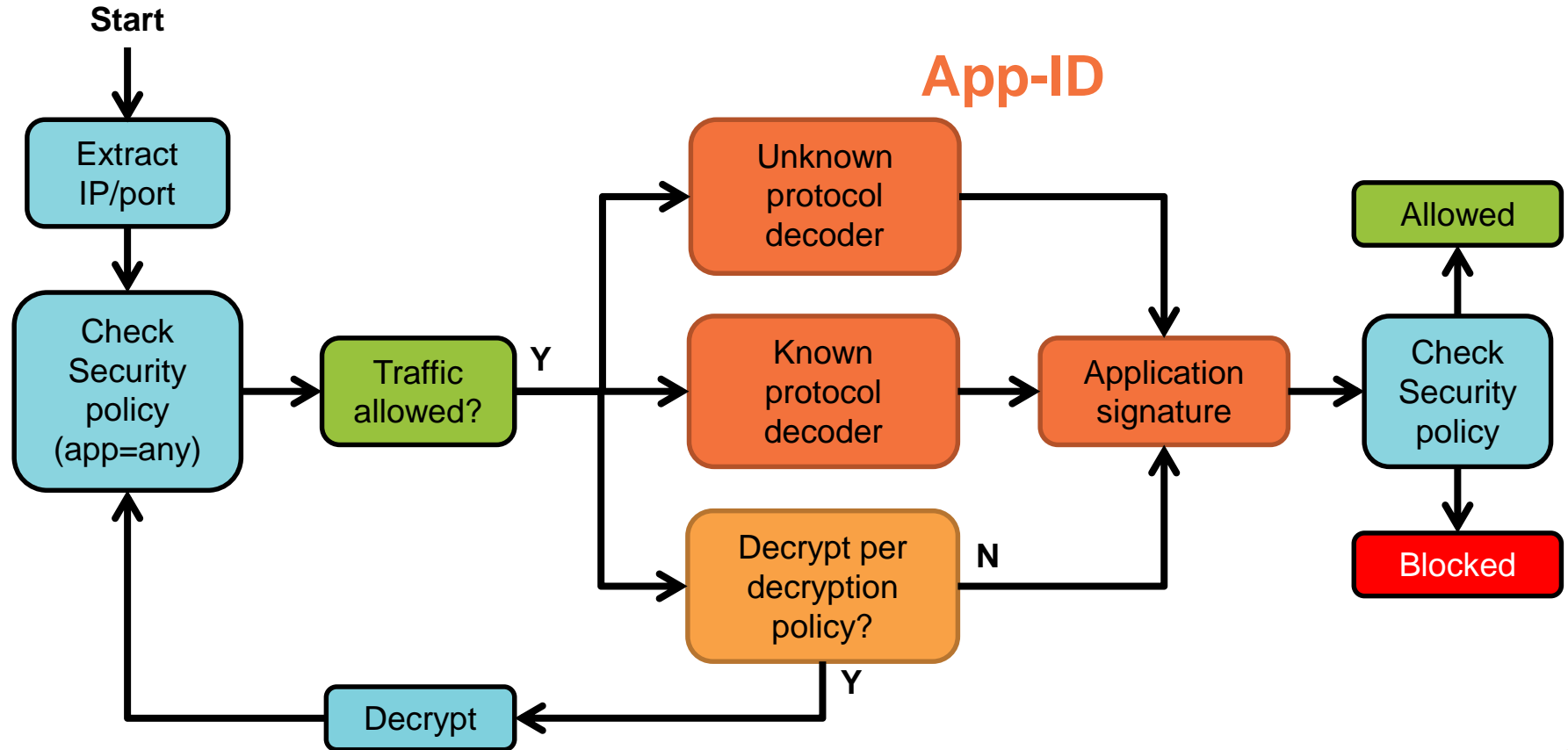
3 4.000000      fe80::200:ff:fe0b:1 f0d2:12          ICMPv6     58 Router Solicitation from 00:00:00:00:00:01
4 4.030002      fe80::200:ff:fe0b:2 f0d2:12          ICMPv6     58 Router Solicitation from 00:00:00:00:00:02
5 5.000000      10.1.0.1           10.2.0.1        MPTCP      74 5001 -> 5001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1250 TSecr=0 W
6 5.060248      10.1.0.1           10.2.0.1        MPTCP      74 5001 -> 5001 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1460 SACK_PERM=1 TSval=1250
7 5.060248      10.1.0.1           10.2.0.1        MPTCP      82 5001 -> 5001 [ACK] Seq=1 Ack=1 Win=29200 Len=0 TSval=1265 TSecr=1257
8 5.060379      10.1.0.1           10.2.0.1        MPTCP      70 [TCP Dup ACK 7#1] 5001 -> 5001 [ACK] Seq=1 Ack=1 Win=29200 Len=0 TSval=1265 TSecr=
9 5.060491      10.1.0.1           10.2.0.1        MPTCP      96 5001 -> 5001 [PSH, ACK] Seq=1 Ack=1 Win=29200 Len=24 TSval=1265 TSecr=1257
10 5.060508      10.1.0.1           10.2.0.1        MPTCP      1502 5001 -> 5001 [PSH, ACK] Seq=25 Ack=1 Win=29200 Len=1428 TSval=1265 TSecr=1257
11 5.063051      10.1.0.1           10.2.0.1        MPTCP      1502 5001 -> 5001 [PSH, ACK] Seq=1453 Ack=1 Win=29200 Len=1428 TSval=1265 TSecr=1257
12 5.065455      10.1.0.1           10.2.0.1        MPTCP      1502 5001 -> 5001 [PSH, ACK] Seq=2881 Ack=1 Win=29200 Len=1428 TSval=1265 TSecr=1257
13 5.067858      10.1.0.1           10.2.0.1        MPTCP      1502 5001 -> 5001 [PSH, ACK] Seq=4309 Ack=1 Win=29200 Len=1428 TSval=1265 TSecr=1257
14 5.070261      10.1.0.1           10.2.0.1        MPTCP      1502 5001 -> 5001 [PSH, ACK] Seq=5737 Ack=1 Win=29200 Len=1428 TSval=1265 TSecr=1257
15 5.072664      10.1.0.1           10.2.0.1        MPTCP      1502 5001 -> 5001 [PSH, ACK] Seq=7165 Ack=1 Win=29200 Len=1428 TSval=1265 TSecr=1257

Frame 10: 1502 bytes on wire (12016 bits), 1502 bytes captured (12016 bits)
Point-to-Point Protocol
Internet Protocol Version 4, Src: 10.1.0.1, Dst: 10.2.0.1
Transmission Control Protocol, Src Port: 5001 (5001), Dst Port: 5001 (5001) Seq: 25, Ack: 1, Len: 1428
Data (1428 bytes)
```

## TCP Packet

# Application data

# App-ID Operation





Application identification (App-ID) overview

**Using App-ID in a Security policy**

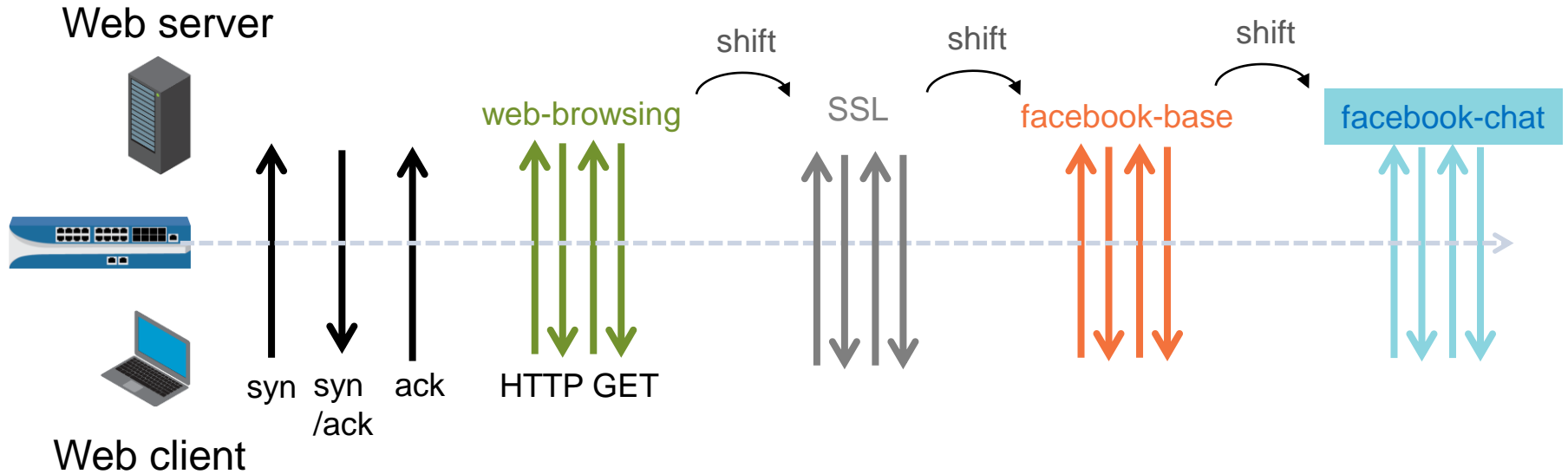
Identifying unknown application traffic

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	Req...						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

The screenshot displays the Palo Alto Networks management interface. On the left, the 'Objects > Applications' view shows a search bar with 'office-on' and a table listing applications. The 'office-on-demand' application is highlighted. On the right, the 'Application' details panel for 'office-on-demand' is shown, with a box around the 'Depends on' field. A second box highlights the 'Commit Status' panel, which shows a successful commit with warnings about application dependencies.

**Application Details:**

- Name:** office-on-demand
- Description:** Office on Demand allows subscribers of Microsoft Office 365 to stream Office (full versions of Word, Excel, PowerPoint, Access, and Publisher) to any Internet-connected Windows 7 or Windows 8 PC where it isn't installed. You can use Office on Demand to create documents or to keep working on documents you've saved to SkyDrive.
- Standard Ports:** tcp/80
- Depends on:** ms-office365-base, sharepoint-online, ssl, web-browsing
- Implicitly Uses:**
- Deny Action:** drop-reset
- Additional Information:** [Office on Demand](#) [Google](#) [Yahoo!](#)

**Commit Status:**

- Operation:** Commit
- Status:** Completed
- Result:** Successful
- Details:** Partial changes to commit: changes to configuration by administrators: admin  
Changes to policy and objects configuration  
Configuration committed successfully
- Warnings:** vsys1  
vsys1: Rule 'Limited Remote Access' application dependency warning:  
Application 'office-on-demand' requires 'ms-office365-base' be allowed  
Application 'office-on-demand' requires 'sharepoint-online' be allowed  
Application 'office-on-demand' requires 'ssl' be allowed  
Application 'office-on-demand' requires 'web-browsing' be allowed  
(Module: device)

- 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.

	Name	Tags	Type	Source				Destination		Application	Service	Action	Profile
				Zone	Address	User	HIP Profile	Zone	Address				
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

The screenshot displays the Palo Alto Networks configuration interface for Applications and Objects. On the left, the 'Objects' pane shows a search for 'facebook' and a list of objects. The 'facebook-base' object is selected. On the right, the 'Application' configuration pane for 'facebook-base' is shown.

**Search:** facebook

**Category:** collaboration, general-internet, media

**Object List:**

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

**Application Configuration:**

**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 facebook depicting members of a campus community that some American colleges and preparatory schools give to incoming students. Faculty and staff members are not to know other people.

**Characteristics:**

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

**Options:**

Option	Value	Action
TCP Timeout (seconds)	3600	<a href="#">Customize...</a>
TCP Half Closed (seconds)	120	<a href="#">Customize...</a>
TCP Time Wait (seconds)	15	<a href="#">Customize...</a>
App-ID Enabled	yes	

**Classification:**

**Category:** collaboration

**Subcategory:** social-networking

**Tags:** collaboration, social-networking, browser-based, tcp/443,80

# Application Filter

## Objects > Application Filter > Add

Application Filter

Name:  ☐ Apply to New App-IDs only  69 matching applications

Category	Subcategory	Technology	Risk	Characteristic
69 business-systems	22 auth-service	42 browser-based	24 1	9 Data Breaches
	38 database	26 client-server	27 2	10 Evasive
	45 erp-crm	1 peer-to-peer	13 3	3 Excessive Bandwidth
	178 general-business		5 4	18 FEDRAMP
	356 management			18 HIPAA
	11 marketing			24 No Certifications
	69 office-programs			9 PCI
	15 software-development			1 Poor Financial Viability
	33 software-update			14 Poor Terms Of Service

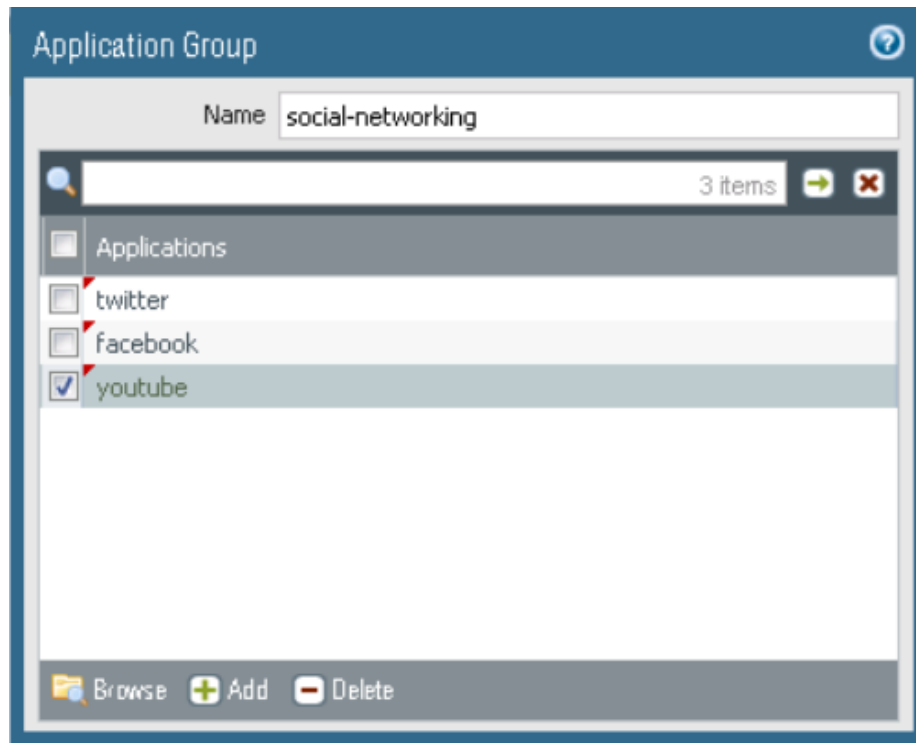
Name	Tagged	Category	Subcategory	Risk	Technology	Standard Ports
adobe-online-office		business-systems	office-programs	3	browser-based	443,80,tcp
ariel		business-systems	office-programs	2	client-server	25,80,tcp
babylon		business-systems	office-programs	1	client-server	80,tcp
benchmark		business-systems	office-programs	2	browser-based	443,80,tcp
cloudon		business-systems	office-programs	2	client-server	443,80,dynamic,tcp,udp
docuSign						

Page 1 of 2 Displaying 1 - 41 of 77

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

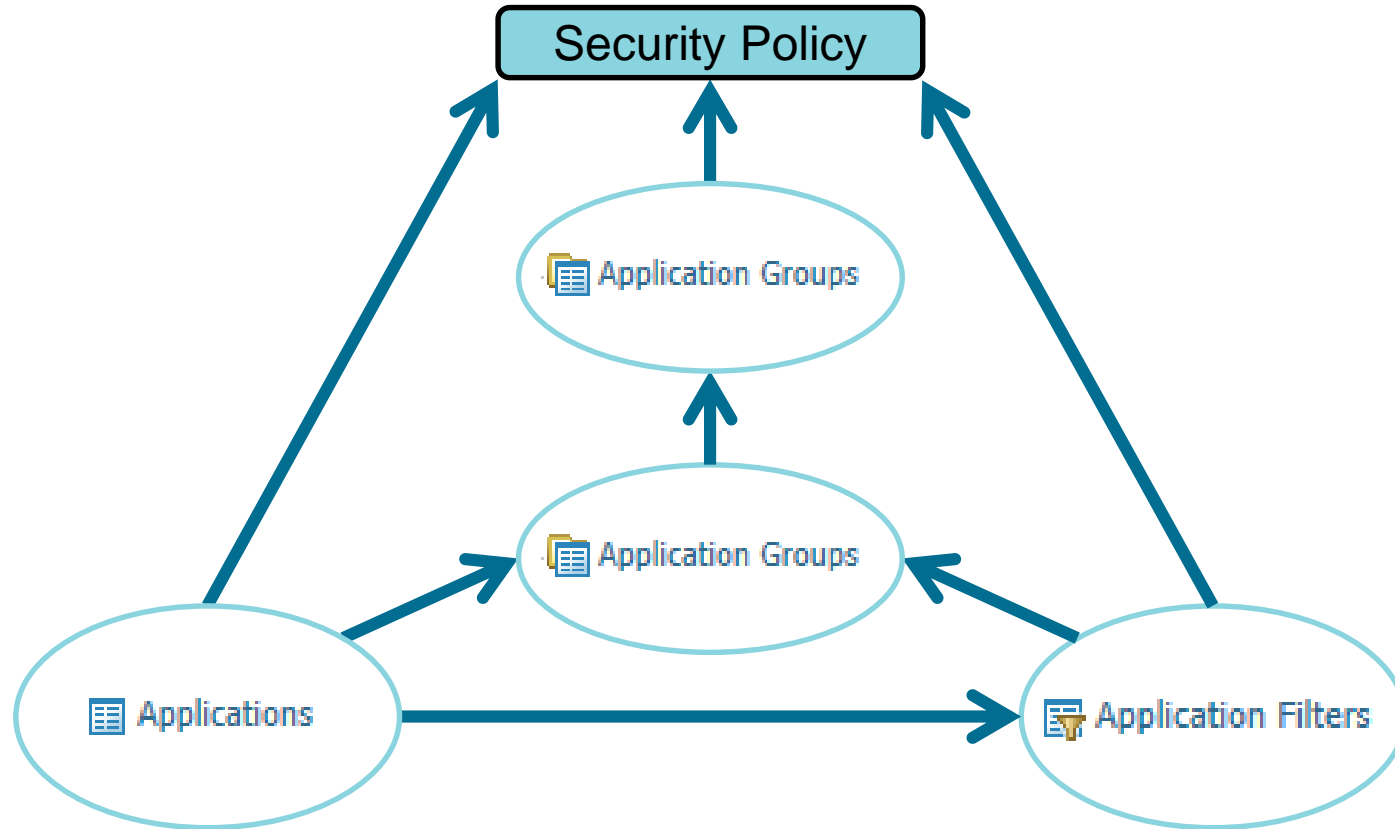
# Application Groups

## 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

				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 Filter

Application Group

Application

# Creating and Using Custom Services

## Objects > Services

Service

Name Mailbox-Access

Description

Protocol ☒ TCP ☐ UDP ☐ SCTP

Destination Port 110,143

Source Port [ $\geq 0$ ]

Port can be a single port #, range (1-65535), or comma separated list

Session Timeout ☒ Inherit from application ☐ Override

Tags

## Policies > Security

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

select

Service

Mailbox-access

Any

URL Category

+ Add - Delete

# 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 Block Page** ⓘ

☒ Enable Application Block Page

OK Cancel

**Application Blocked**

Access to the application you were trying to use has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: 192.168.1.20

Application: reddit-base



Application identification (App-ID) overview

Using App-ID in a Security policy

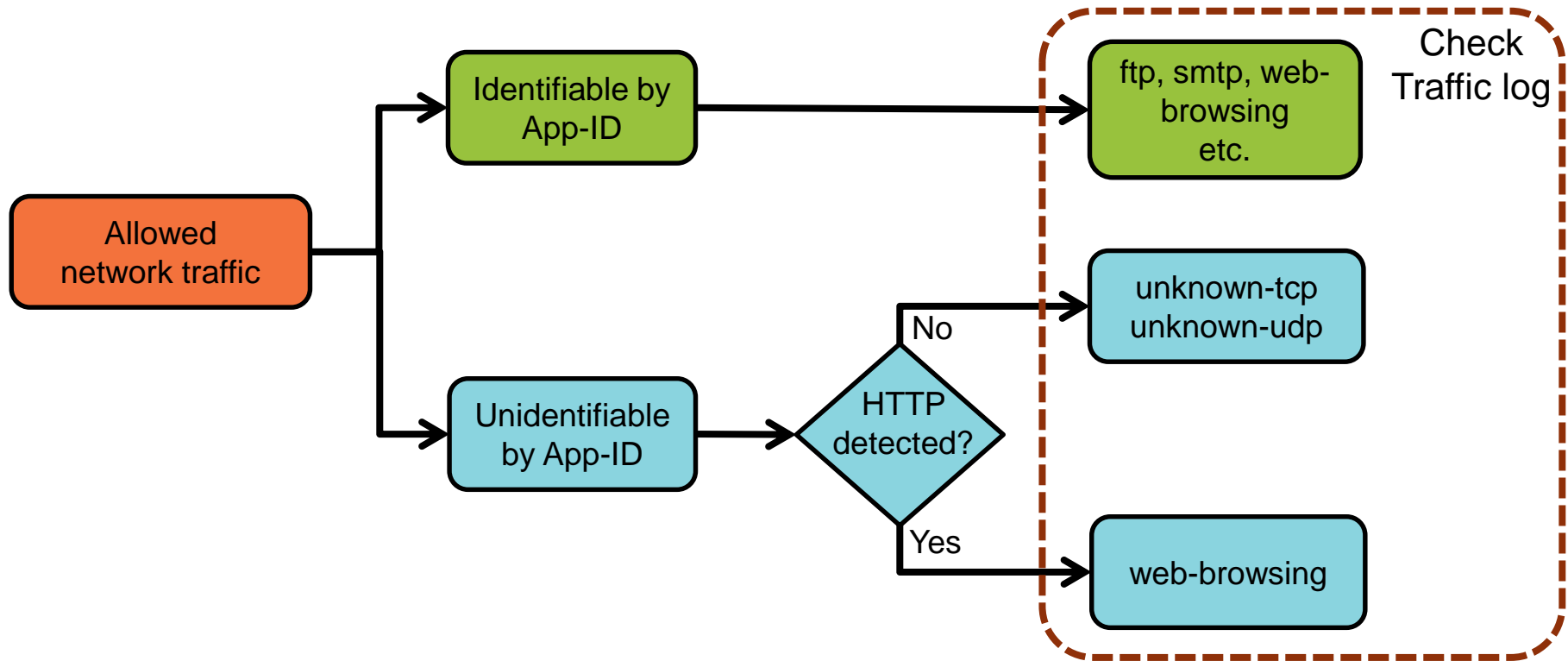
**Identifying unknown application traffic**

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

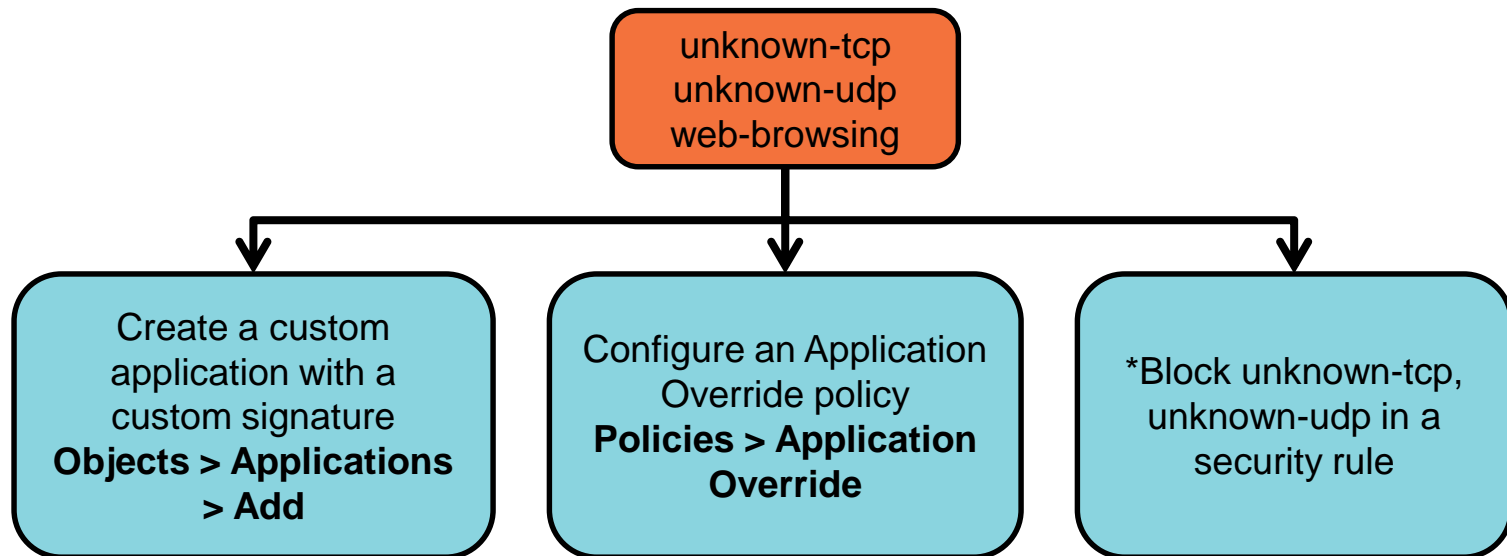
## Policies > Security

	Name	Tags	Type	Source				Destination		Application	Service	Action
				Zone	Address	User	HIP Profile	Zone	Address			
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

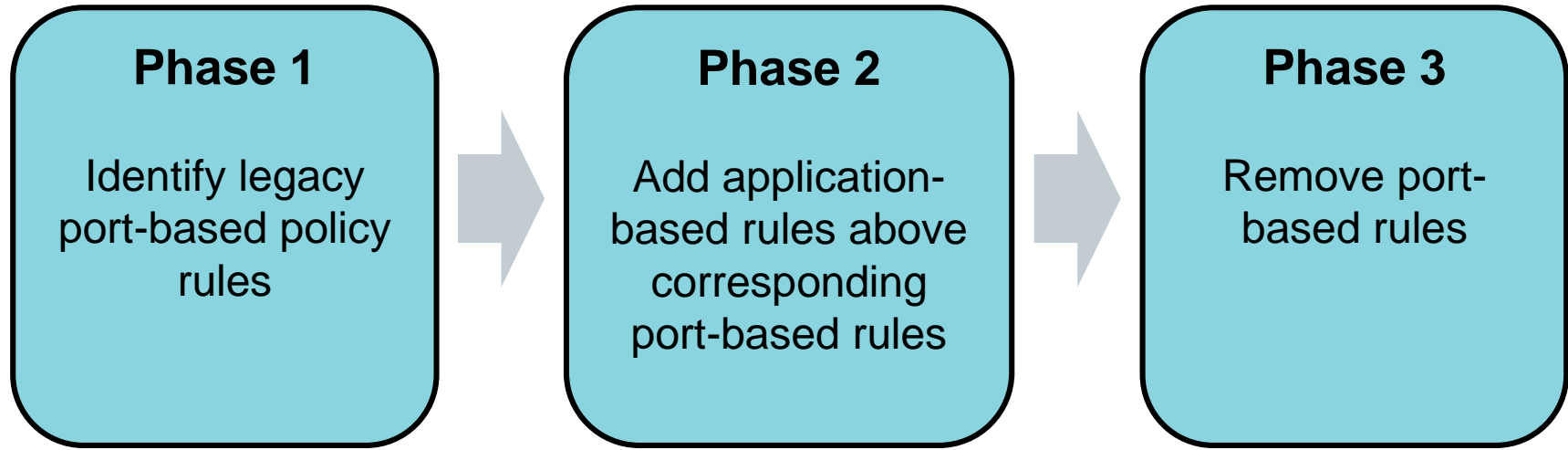
- Migrate port-based rules to App-ID-based rules
- Help reduce attack surface and provide information about application usage
- Prevent evasive applications from running on non-standard ports
- Identify over-provisioned application-based rules

## Policies > Security > Policy Optimizer > No App Specified

**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.

	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	<a href="#">Compare</a>	2018-11-20 20:09:22	2018-11-20 20:02:32

# Moving to Application-Based Policies



# 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

<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.									
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

The screenshot shows the Palo Alto Networks Policy Optimizer interface. On the left, a sidebar lists 'Security' > 'NAT' > 'QoS' > 'Policy Optimizer'. Under 'Policy Optimizer', 'No App Specified' is selected and highlighted with a black box. The main area displays a table of security policies. The first policy is 'internal-dmz' with service 'service-ftp' and 'service-http'. The 'App Usage' section for this policy shows 'Apps Allowed' as 'any' (highlighted with a black box), 'Apps Seen' as '0' (highlighted with a black box), and a 'Compare' button (highlighted with a black box). A callout line points from the 'Compare' button to the 'Applications & Usage' window below.

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

- 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).

The screenshot shows the 'Applications & Usage - internal-dmz' window. The 'Timeframe' is set to 'Anytime'. The 'Apps on Rule' section shows 'Any' selected. The 'Apps Seen' count is '2'. A list of applications is displayed with columns: Applications, Subcategory, Risk, First Seen, Last Seen, and Traffic (30 days). The applications listed are 'web-browsing' (internet-utility, Risk 4, 5.8k traffic) and 'ftp' (file-sharing, Risk 5, 1.3k traffic). A callout box points to the 'Anytime' dropdown menu, which lists 'Anytime', 'Past 7 days', 'Past 15 days', and 'Past 30 days'. Another callout box points to the 'Add to Rule', 'Create Cloned Rule', and 'Match Usage' buttons at the bottom. A third callout box points to the 'Compare' button in the top window. A text box at the bottom states 'The last new app was discovered 0 days ago.'

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



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

## Option 1 of 3:

Applications & Usage - internal-dmz

Timeframe: Anytime

Apps on Rule: Apps Seen 2

Applications	Subcategory	Risk	First Seen	Last Seen	Traffic (30 days)
<input type="checkbox"/> web-browsing	internet-utility	4	2018-11-20	2018-11-20	5.8k
<input checked="" type="checkbox"/> ftp	file-sharing	5	2018-11-20	2018-11-20	1.3k

1. Select application(s).

2. Click **Create Cloned Rule**.

3. Name new rule.

Buttons: Browse, Add, Delete, Add to Rule, **Create Cloned Rule**, Match Usage

- 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

Clone

You are creating a clone of the rule "internal-dmz" and adding 1 applications

Name: internal-to-dmz-ftp

Applications: ftp

These applications will be removed from the "Apps Seen" list on the current rule.  
The new rule will be added immediately **before** the current rule.

# Result of Using “Create Cloned Rule”

Applications & Usage - internal-dmz

Timeframe: Anytime

Apps on Rule: Apps Seen 1

☒ Any

☐ Applications

1 item

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

Must manually configure as **application-default**

	Name	Source			Destination		Application	Service	Action
		Zone	Address	User	Zone	Address			
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

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

## Option 2 of 3:

Applications & Usage - internal-dmz

Timeframe: Anytime

Apps on Rule: Apps Seen 2

Applications	Subcategory	Risk	First Seen	Last Seen	Traffic (30 days)
<input checked="" type="checkbox"/> web-browsing	internet-utility	4	2018-11-20	2018-11-20	5.8k
<input type="checkbox"/> ftp	file-sharing	5	2018-11-20	2018-11-20	1.3k

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

Buttons: Browse, Add, Delete, **Add to Rule**, Create Cloned Rule, Match Usage

The last new app was discovered 1 days ago.

- 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

Apps on Rule Apps Seen 2

Any

Applications

web-browsing

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

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

	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

Must manually configure as **application-default**

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

# Replacing a Port-Based Rule Using “Match Usage”

## Option 3 of 3:

Applications & Usage - internal-dmz

Timeframe: Anytime

Apps on Rule: Apps Seen 2

Any

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

Click Match Usage

Match Usage

The last new app was discovered 1 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 Using “Match Usage”

Applications & Usage - internal-dmz

Timeframe: Anytime

Apps on Rule: Apps Seen 2

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

Any	Applications	Subcategory	Risk	First Seen	Last Seen	Traffic (30 days)
<input type="checkbox"/> web-browsing	<input type="checkbox"/> web-browsing	internet-utility	4	2018-11-20	2018-11-21	11.5k
<input type="checkbox"/> ftp	<input type="checkbox"/> ftp	file-sharing	5	2018-11-20	2018-11-21	2.6k

## Policies > Security

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

Must manually configure as **application-default**

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

# Prioritizing Port-Based Rules to Convert

Security

- NAT
- QoS
- Policy Based Forwarding
- Decryption

Policy Optimizer

- No App Specified
- Unused Apps
- Rule Usage
  - Unused in 30 days
  - Unused in 90 days
  - Unused

No App Specified

Prioritize rules passing more data

Prioritize rules with more applications

Prioritize rules that are more stable

Name	Service	Traffic (Bytes, 30 days)	Apps Allowed	Apps Seen	Days with No New Apps	Compare	Modified	Created
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

Security

- NAT
- QoS
- Policy Based Forwarding
- Decryption

Policy Optimizer

- No App Specified
- Unused Apps
- Rule Usage
  - Unused in 30 days
  - Unused in 90 days
  - Unused

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

Prioritize rules that match more sessions


Name	Hit Count	Last Hit	First Hit	Reset Date	Modified	Created
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

	Name	Source			Destination		Application	Service	Action	Rule Usage
		Zone	Address	HIP Profile	Zone	Address				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

 Reset










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














 All rules  
 Selected rules



# Disabling Port-Based Rules

## Policies > Security

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

	Name	Source			Destination		Application	Service	Action	Rule Usage
		Zone	Address	HIP Profile	Zone	Address				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



	Name	Source			Destination		Application	Service	Action	Rule Usage
		Zone	Address	HIP Profile	Zone	Address				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

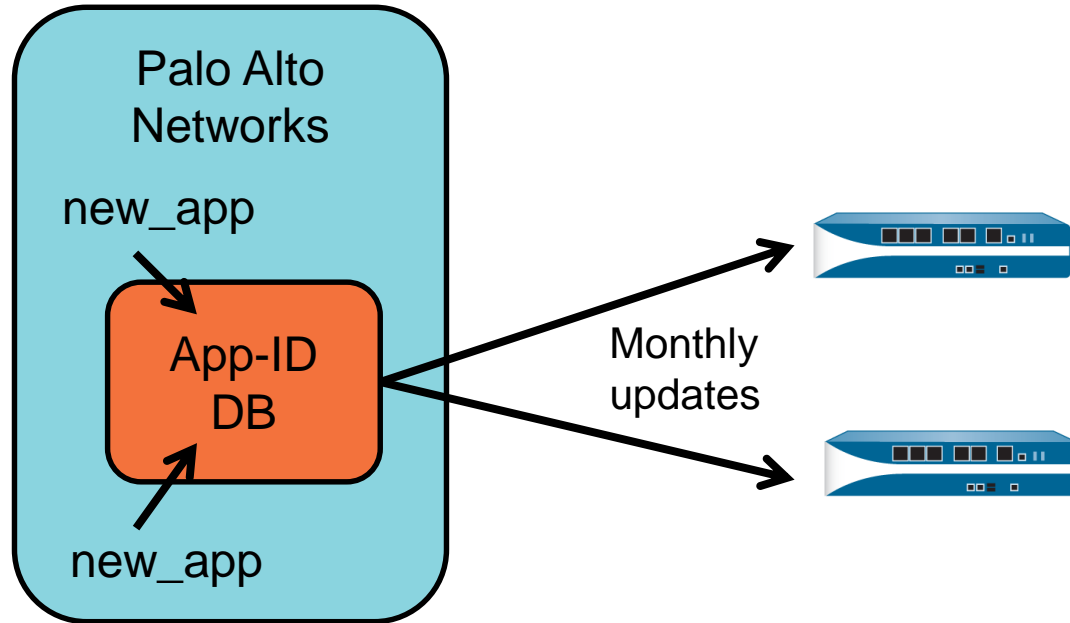
Identifying unknown application traffic

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			<a href="#">Download</a>
8109-5227	panupv2-all-contents-8109-5227	Apps, Threats	Full	44 MB	2018/12/28 00:48:12 UTC		✓	<a href="#">Review Policies</a> <a href="#">Review Apps</a>

Applications and Threats Update Schedule

Recurrence: Hourly

Minutes Past Hour: 5

Action: download-and-install

☐ Disable new apps in content update

Threshold (hours): [1 - 336]

None

download-only

download-and-install

Allow Extra Time to Review New App

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

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

If selected, new application signatures are disabled.

Click to schedule updates.

Every 30 Minutes

Hourly

Daily

Weekly

None

# 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

The screenshot shows the 'New and Modified Applications since last installed content' window. The left sidebar lists 'Modified Apps' including 'gmail-downloading', 'gmail-posting', 'gmail-uploading', 'infoblox-grid', and 'mongodb'. The main panel displays details for 'gmail-downloading'. Annotations highlight key areas:

- Used to determine risk:** Points to the 'Content Version: 787' field.
- Based on characteristics:** Points to the 'Risk: 2' field.
- If necessary, modify for your environment:** Points to the 'Options' section, specifically 'App-ID Enabled: yes'.
- New data for software as a service:** Points to the 'SaaS Characteristics' section.

**Application Details:**

- Name:** gmail-downloading
- Description:** This App-ID detects Gmail.
- Standard Ports:** tcp/443
- Depends on:** gmail-base, ssl, web-browsing
- Implicitly Uses:**
- Deny Action:** drop-reset
- Additional Information:** Wikipedia Google Yahoo!

**Characteristics:**

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

**Options:**

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

**SaaS Characteristics:**

- Certifications:** FEDRAMP, HIPAA, SOC I, SOC II, SSAE16
- Data Breaches:** no
- IP Based Restrictions:** no
- Poor Financial Viability:** no
- Poor Terms Of Service:** no

**Classification:**

- Category:**
- Subcategory:**
- Technology:** browser-based

**Buttons:** Policy Review Recommended, Review Policies, Close.

**Right Sidebar:** Download, Download, Download, Revert, Download, Download, Review Policies (checked), Review Apps, Install, Review Policies, Review Apps.

# Pre-Analyze New Application and Policy Interaction

## Objects > Applications

<input type="checkbox"/>	 24sevenoffice	business-systems	erp-crm
<input type="checkbox"/>	 2ch		
<input type="checkbox"/>	 2ch-base	collaboration	social-networking
<input type="checkbox"/>	 2ch-posting	collaboration	web-posting
<input type="checkbox"/>	 360-safeguard-update	business-systems	software-update
<input type="checkbox"/>	 3pc	networking	ip-protocol
<input type="checkbox"/>	 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

Policy review based on candidate configuration

Content Version: 743-4276 Rulebase: Security Virtual System: vsys1 Type: New Applications Application: Include rules with Application 'Any'

				Source				Destination					
Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	
Unclassified Apps	egress	universal	any	any	any	any	any	any	any	+ any	✓ Allow	none	
egress-outside	egress	universal	any inside	any	any	any	any outside	any	any	+ application-d...	✓ Allow	none	
danger-simulated-traf...		universal	any danger	any	any	any				+ application-d...	✓ Allow		

Security

QoS

Policy Based Forwarding

Enabled

cylance

diameter-over-sctp

directv

gitlab

gitlab-base

gitlab-uploading



# 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.

