

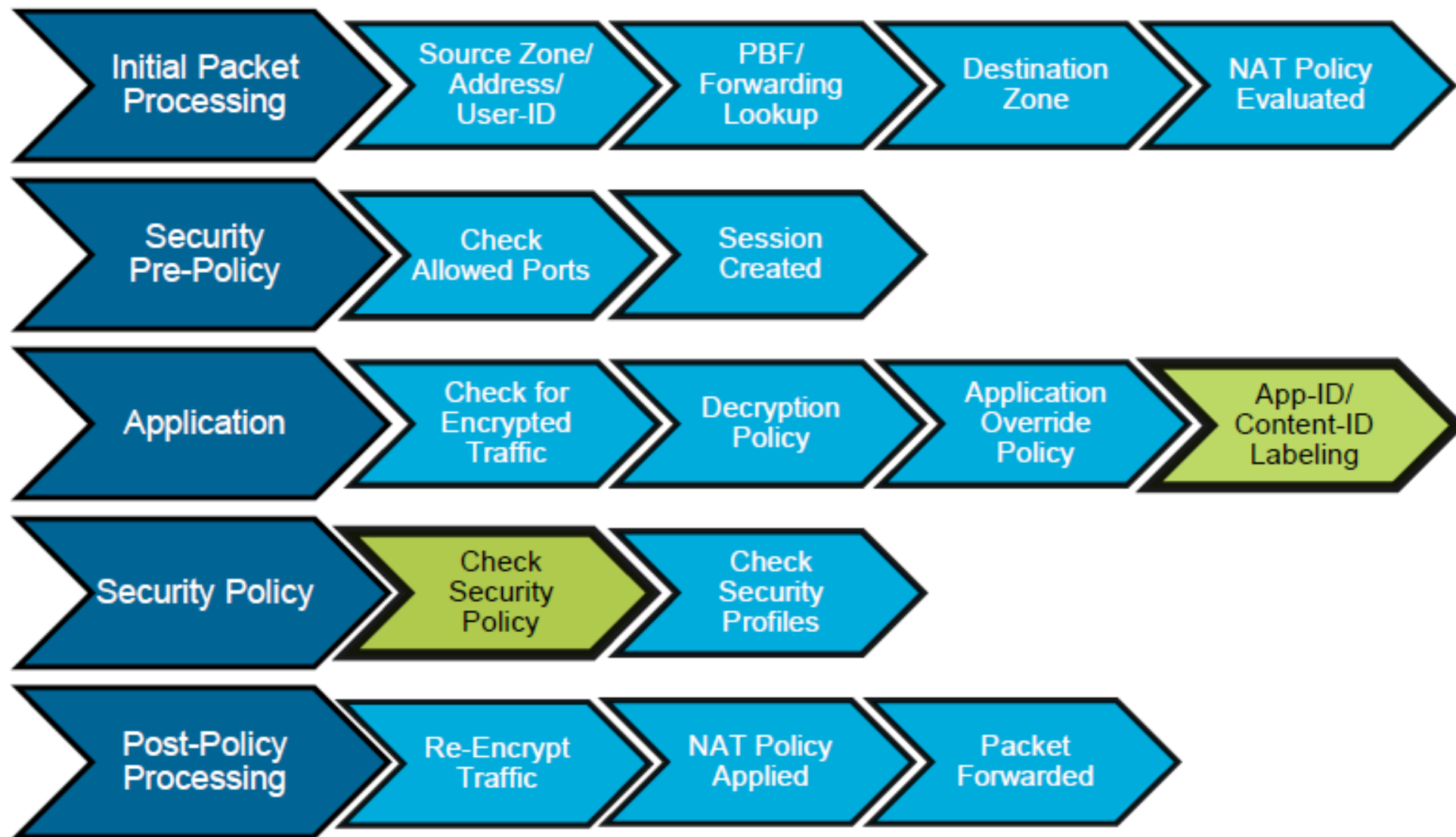
IP alapú kommunikáció

11. Előadás Cybersecurity II. NGFW

Kovács Ákos

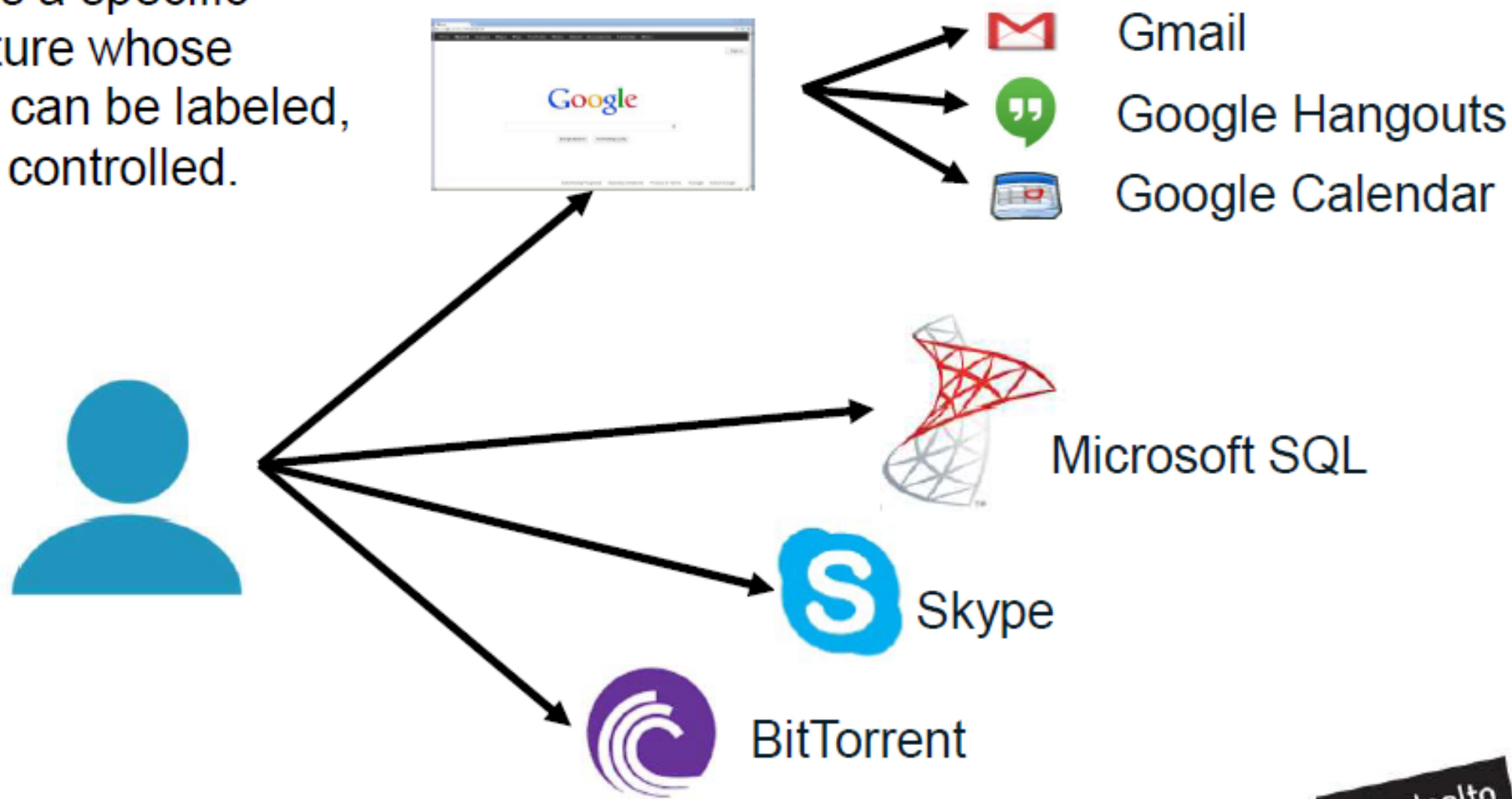
- APP-ID alapú
- Content-ID alapú
- URL alapú

Flow Logic of the Next-Generation Firewall



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	Type	Source			Destination		Application	Service	Action
			Zone	Address	User	Zone	Address			
1	FTP	universal	inside	any	any	outside	any	service-ftp	Allow	

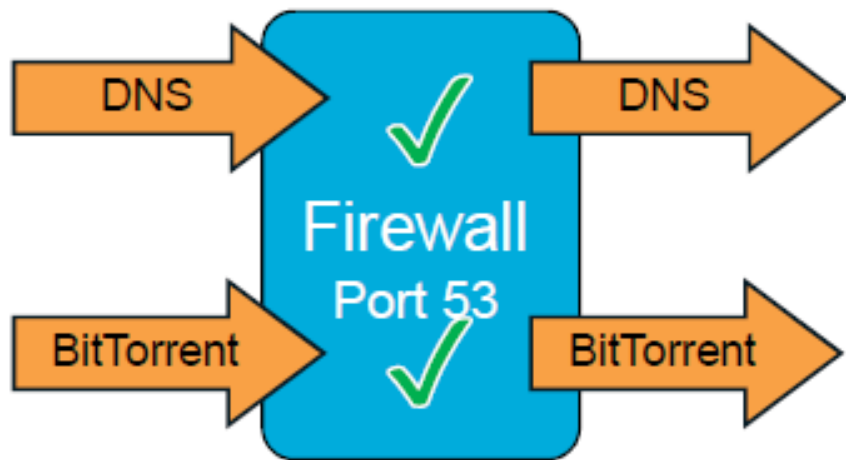
Application-based security rule

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

Port-Based Versus Next-Generation Firewalls

Traditional Firewalls

Firewall Rule: ALLOW Port 53



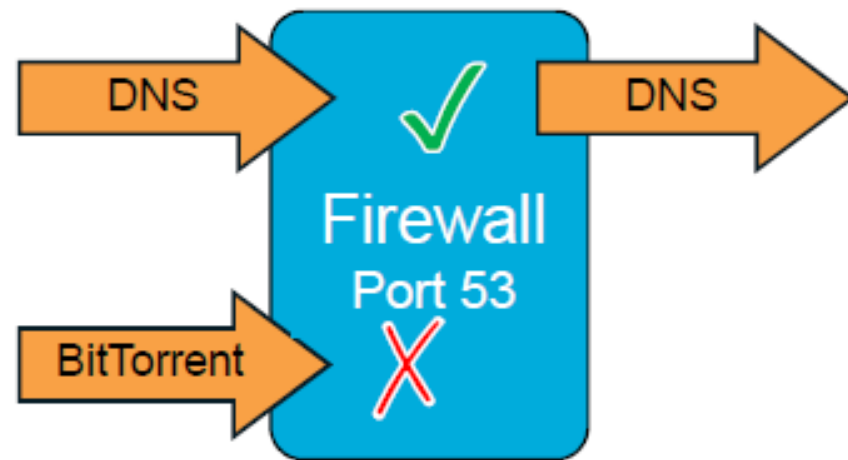
Packet on port 53: Allow

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

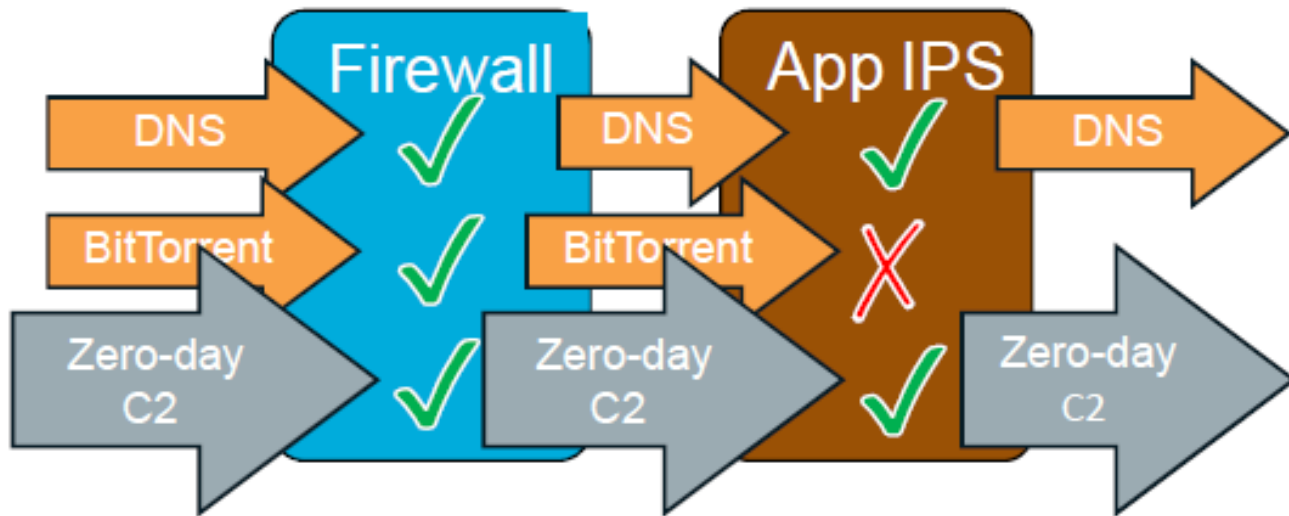
Visibility: BitTorrent detected and blocked

Zero-Day Malware – IPS Versus App-ID

Legacy Firewalls

Firewall Rule: ALLOW Port 53

Application IPS Rule: Block BitTorrent



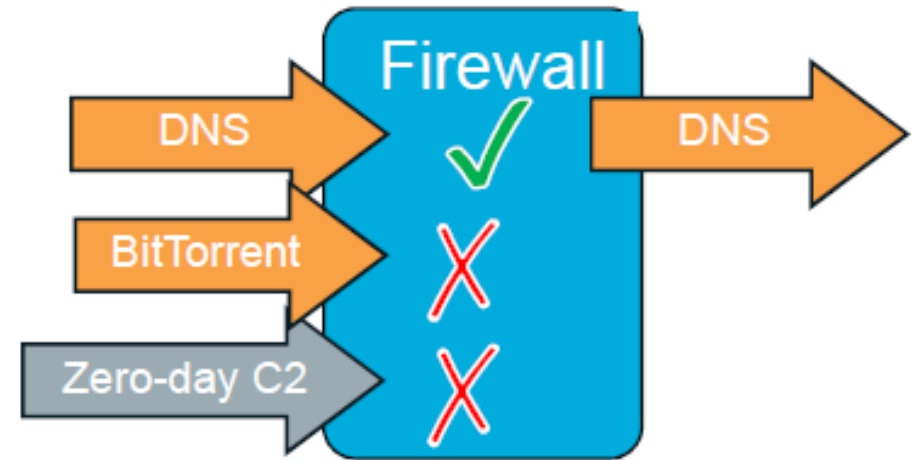
Packet on port 53: Allow

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 (00:0c:29:dd:bb:3a)
▶ 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... .....
```

The first UDP packet

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... .....
```

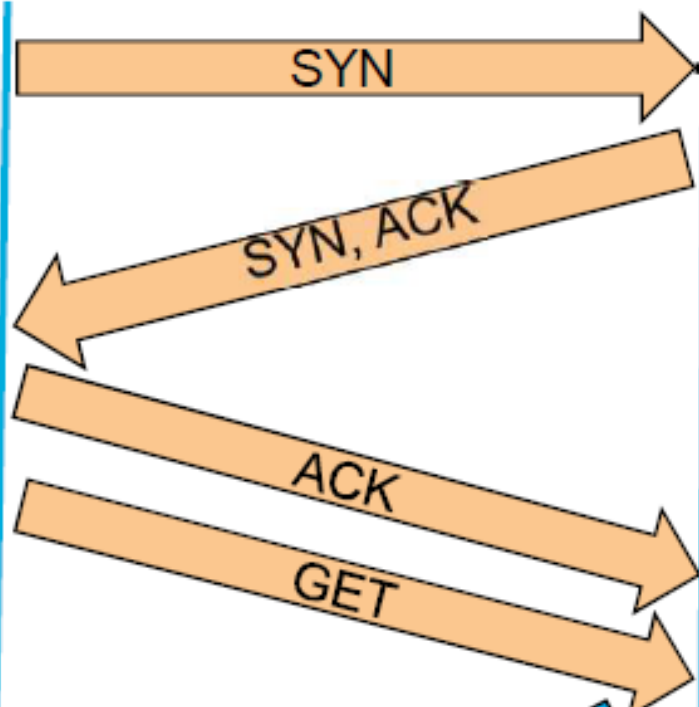
Application data



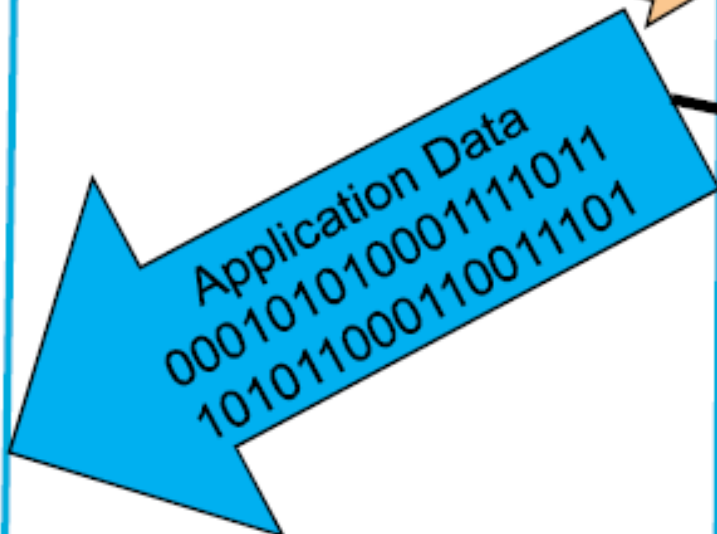
App-ID and TCP



Client



Example of an HTTP web request



Server

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

3 4.000000	fe00::200::ff:fe00:1	ff02::2	ICMPv6	58	Router Solicitation from 00:00:00:00:00:00
4 4.010002	fe00::200::ff:fe00:2	ff02::2	ICMPv6	58	Router Solicitation from 00:00:00:00:00:00
5 5.000000	10.1.0.1	10.2.0.1	HTTP	74	5001 → 5001 [SYN] Seq=9 Win=29200 Len=0 MSS=1460 SAQ_PERM=1 TSval=1250 TSecr=0 W=0
6 5.000048	10.2.0.1	10.1.0.1	HTTP	76	5001 → 5001 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SAQ_PERM=1 TSval=1257 TSecr=1257
7 5.000248	10.1.0.1	10.2.0.1	HTTP	82	5001 → 5001 [ACK] Seq=1 Ack=1 Win=29200 Len=0 TSval=1255 TSecr=1257
8 5.000579	10.1.0.1	10.2.0.1	HTTP	78	TCP RST Seq=5001 Len=0
9 5.000401	10.1.0.1	10.2.0.1	HTTP	98	5001 → 5001 [PSH, ACK] Seq=1 Ack=1 Win=29200 Len=24 TSval=1263 TSecr=1257
10 5.000648	10.1.0.1	10.2.0.1	HTTP	1502	5001 → 5001 [PSH, ACK] Seq=23 Ack=1 Win=29200 Len=1428 TSval=1285 TSecr=1257
11 5.003051	10.1.0.1	10.2.0.1	HTTP	1502	5001 → 5001 [PSH, ACK] Seq=1453 Ack=1 Win=29200 Len=1428 TSval=1265 TSecr=1257
12 5.005455	10.1.0.1	10.2.0.1	HTTP	1502	5001 → 5001 [PSH, ACK] Seq=2881 Ack=1 Win=29200 Len=1428 TSval=1265 TSecr=1257
13 5.007858	10.1.0.1	10.2.0.1	HTTP	1502	5001 → 5001 [PSH, ACK] Seq=4309 Ack=1 Win=29200 Len=1428 TSval=1265 TSecr=1257
14 5.010261	10.1.0.1	10.2.0.1	HTTP	1502	5001 → 5001 [PSH, ACK] Seq=5737 Ack=1 Win=29200 Len=1428 TSval=1265 TSecr=1257
15 5.012664	10.1.0.1	10.2.0.1	HTTP	1502	5001 → 5001 [PSH, ACK] Seq=7165 Ack=1 Win=29200 Len=1428 TSval=1265 TSecr=1257

Frame 10: 1382 bytes on wire (12816 bits), 1382 bytes captured (12816 bits) on interface 0
Ethernet II, Src: Palo Alto (08:00:27:00:00:00), Dst: 10.2.0.1 (08:00:27:00:00:00)
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=26, Ack=1, Len=1428
Data (1428 bytes)

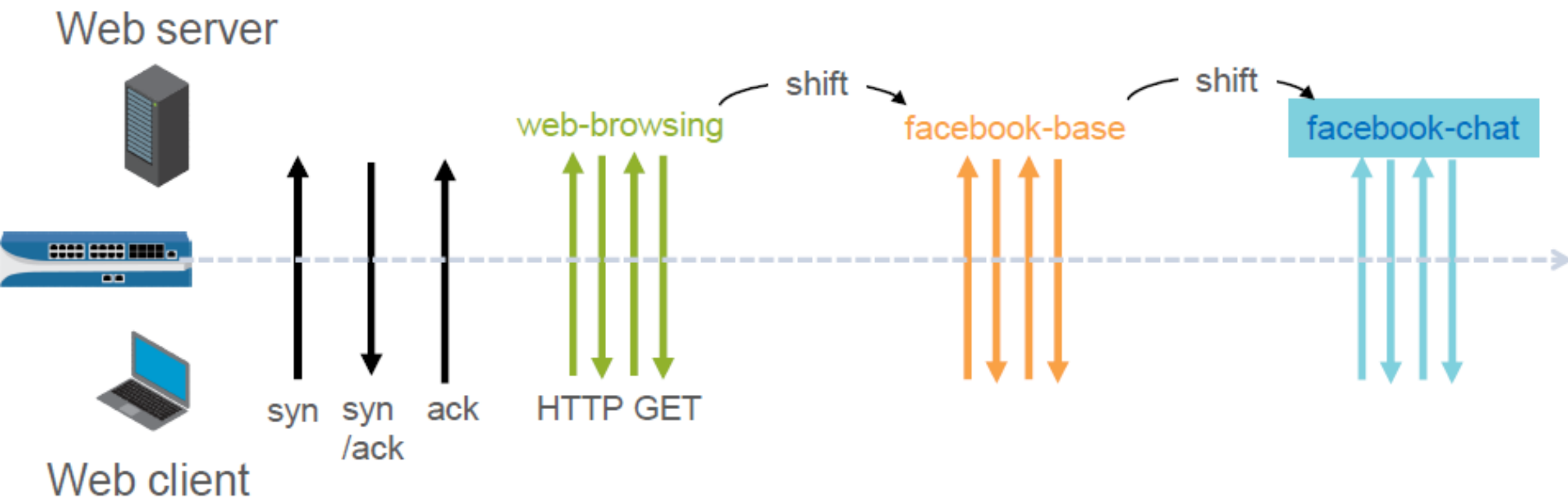
TCP Packet

Application data



Application Shifts

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



Determining Application Dependencies

Objects > Applications

The screenshot displays the Palo Alto Networks management console interface. On the left, the 'Objects > Applications' view shows a search bar with 'office-on' and a table of applications. The 'office-on-demand' application is selected and highlighted. On the right, the application details for 'office-on-demand' are shown, including its name, description, additional information, standard ports, and dependencies. The 'Depends on' field is highlighted with a red box and contains the text 'ms-office365-base, sharepoint-online, ssl, web-browsing'. Below the application details, the 'Commit Status' section shows the operation completed successfully, with a warning message indicating that the application depends on other applications that are not yet allowed.

Search: office-on

Category: 1 business-systems

Subcategory: 1 office-programs

Application Details:

- Name:** office-on-demand
- Description:**
- Additional Information:** Office on Demand Google Yahoo!
- Standard Ports:** tcp/80
- Depends on:** ms-office365-base, sharepoint-online, ssl, web-browsing
- Implicitly Uses:**
- Deny Action:** drop-reset
- Characteristics:**
- Evasive:** no
- Excessive Bandwidth Use:** yes
- Used by Malware:** no
- Capable of File Transfer:** yes

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

Determining Implicitly Used Applications

Objects > Applications

Search All

Category **▲** Subcategory **▲**

- 8 collaboration
 - 1 general-internet
 - 3 media
- 1 email
- 1 file-sharing
- 1 gaming
- 1 instant-messaging
- 2 photo-video
- 5 social-networking
- 1 voip-video

Application

Name: facebook-base
Description:
Additional Information: [Wikipedia](#) [Google](#) [Yahoo!](#)
Standard Ports: tcp/80,443
Depends on:
Implicitly Uses: ssl, web-browsing
Deny Action: drop-reset

Classification

Evasive: no
Excessive Bandwidth Use: no
Used by Malware: yes
Capable of File Transfer: yes

Category: collaboration
Subcategory: social-networking
Technology: browser-based
Risk: 4 Customizable

12 Widely used



Name	Tagged	Category	Subcategory	Risk	Technology	Standard Ports
<input type="checkbox"/> Facebook (10 out of 11 shown)						
<input type="checkbox"/> facebook-apps		collaboration	social-networking	4	browser-based	tcp/80,443
<input type="checkbox"/> facebook-base		collaboration	social-networking	4	browser-based	tcp/80,443
<input type="checkbox"/> facebook-chat		collaboration	instant-messaging	3	browser-based	tcp/80,443
<input type="checkbox"/> facebook-file-sharing		general-internet	file-sharing	4	browser-based	tcp/80,443
<input type="checkbox"/> facebook-mail		collaboration	email	3	browser-based	tcp/80,443
<input type="checkbox"/> facebook-messaging		collaboration	social-networking	4	browser-based	tcp/443,80

Content-ID

- Threat prevention engine and policies to inspect and control content traversing the firewall
- Scans network traffic for:
 - Software vulnerability exploits
 - Viruses
 - Spyware
 - Malicious URLs
 - Restricted files and data

Security Profile Types

Policies > Security

	Name	Type	Source			Destination		Application	Service	Action	Profile
			Zone	Address	User	Zone	Address				
1	Limited Remote Access	universal	Trust-L3	192.168.1.3/24	any	Untrust-L3	any	dns ftp office-on-de...	application-default	Allow	
2	Unexpected Traffic	universal	Untrust-L3	any	any	Trust-L3	any	any	application-default	Allow	



Antivirus



Anti-Spyware



Vulnerability Protection



URL Filtering



File Blocking



Data Filtering



WildFire Analysis



Security Profile Group

Threat Log

- Vulnerability Protection, Antivirus, and Anti-spyware Profiles log events to the Threat log.

Monitor > Logs > Threat

Click a column header to change number of displayed columns

	Receive Time	Type	ID	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	Severity
	11/08 09:18:49	vulnera...	42000	PDF-Exploit	Untrust-L3	Trust-L3	98.139.135.129	192.168.7.50	53920	web-browsing	reset-both	high
	11/08 09:18:25	vulnera...	42000	PDF-Exploit	Untrust-L3	Trust-L3	98.139.135.129	192.168.7.50	53919	web-browsing	reset-both	high
	11/08 09:17:50	vulnera...	42000	PDF-Exploit	Untrust-L3	Trust-L3	98.139.135.129	192.168.7.50	53912	web-browsing	reset-both	high
	11/08 07:10:14	virus	100000	Eicar Test File	Untrust-L3	Trust-L3	213.211.198.62	192.168.7.50	52797	web-browsing	reset-server	medium
	11/08 07:06:15	virus	100000	Eicar Test File	Untrust-L3	Trust-L3	213.211.198.62	192.168.7.50	52749	web-browsing	alert	medium

Includes packet capture

Open Threat Details window

Default Vulnerability Protection Security Profiles

Objects > Security Profiles > Vulnerability Protection

Name	Location	Count	Rule Name	Threat Name	Host Type	Severity	Action	Packet Capture
<input type="checkbox"/> strict	Predefined	Rules: 10	simple-client-critical	any	client	critical	reset-both	disable
			simple-client-high	any	client	high	reset-both	disable
			simple-client-medium	any	client	medium	reset-both	disable
			simple-client-informational	any	client	informational	default	disable
			simple-client-low	any	client	low	default	disable
			simple-server-critical	any	server	critical	reset-both	disable
			simple-server-high	any	server	high	reset-both	disable
			more...					
<input type="checkbox"/> default	Predefined	Rules: 6	simple-client-critical	any	client	critical	default	disable
						high	de	de
						medium	de	de
						critical	de	de
						high	default	disable
						medium	default	disable
			medium					

Default (read-only) profiles

Rules specify actions on detected events

- To create customized profile actions:
 - **Clone** the default read-only profile and edit clone, or
 - **Add** a brand new profile

Default Antivirus Security Profile

Objects > Security Profiles > Antivirus

Name	Location	Packet Capture	Decoders		Application Exceptions		Threat Exceptions
			Name	Action	Name	Action	
default	Predefined	<input type="checkbox"/>	http	default (reset-both)	allow		0
			smtp	default (alert)	allow		
			imap	default (alert)	allow		
			pop3	default (alert)	allow		
			ftp	default (reset-both)	allow		
			smb	default (reset-both)	allow		

Out-of-the-box profile

Action to take based on antivirus signatures delivered in content updates

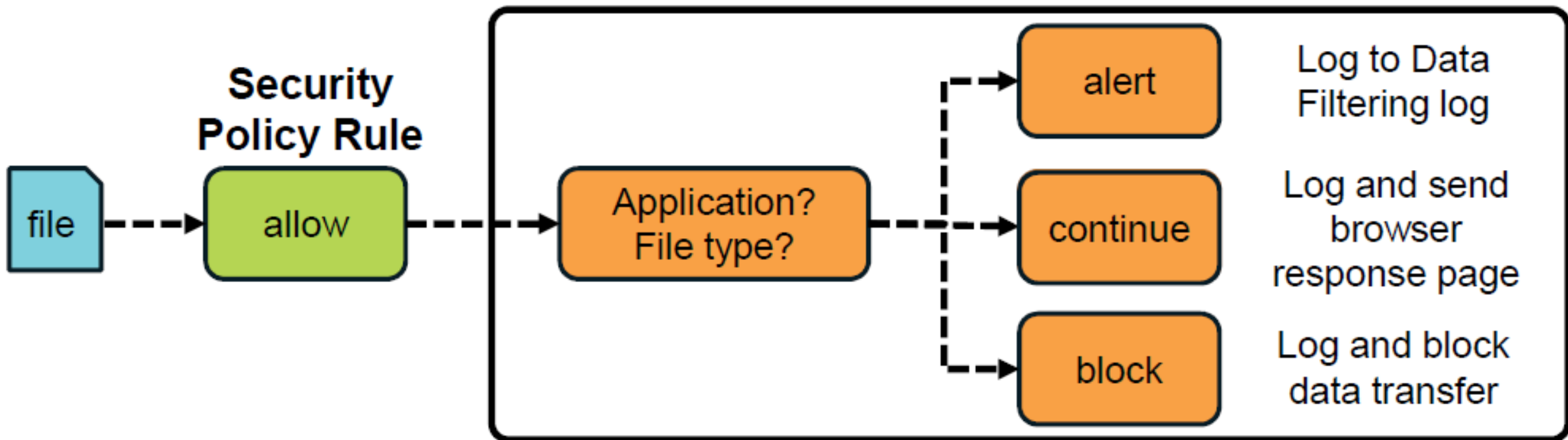
WildFire Action to take based on signatures delivered by WildFire

- To create customized profile actions:
 - **Clone** the default read-only profile and edit clone, or
 - **Add** a brand new profile

File Blocking Overview

- Prevent introduction of malicious data
- Prevent exfiltration of sensitive data
- Logs to Data Filtering log

File Blocking Profile



Security Profile Groups

Objects > Security Profile Groups > Add

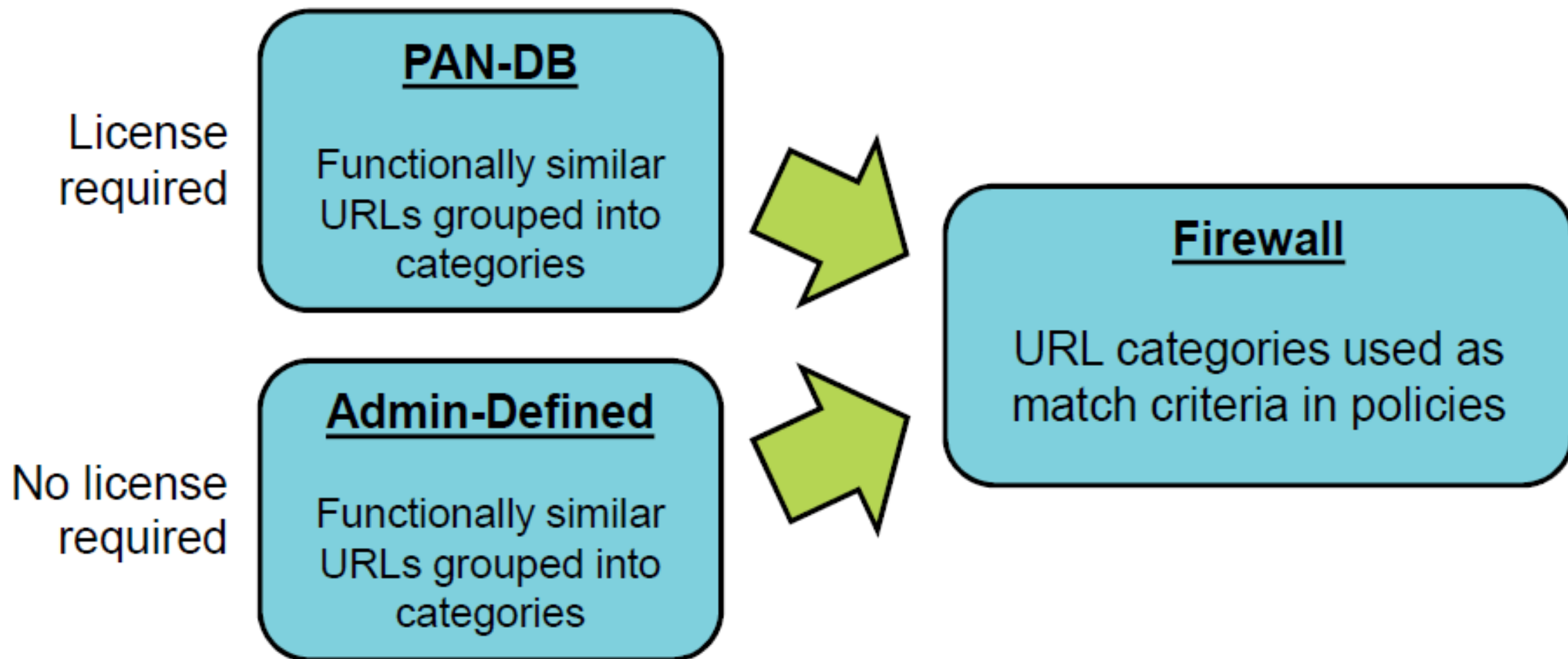
Security Profile Group ?

Name	Strict Profiles
Antivirus Profile	Strict Antivirus
Anti-Spyware Profile	Strict Anti-Spyware
Vulnerability Protection Profile	Strict Protection
URL Filtering Profile	Strict URL Filtering
File Blocking Profile	Strict File Transfer
Data Filtering Profile	None
WildFire Analysis Profile	None

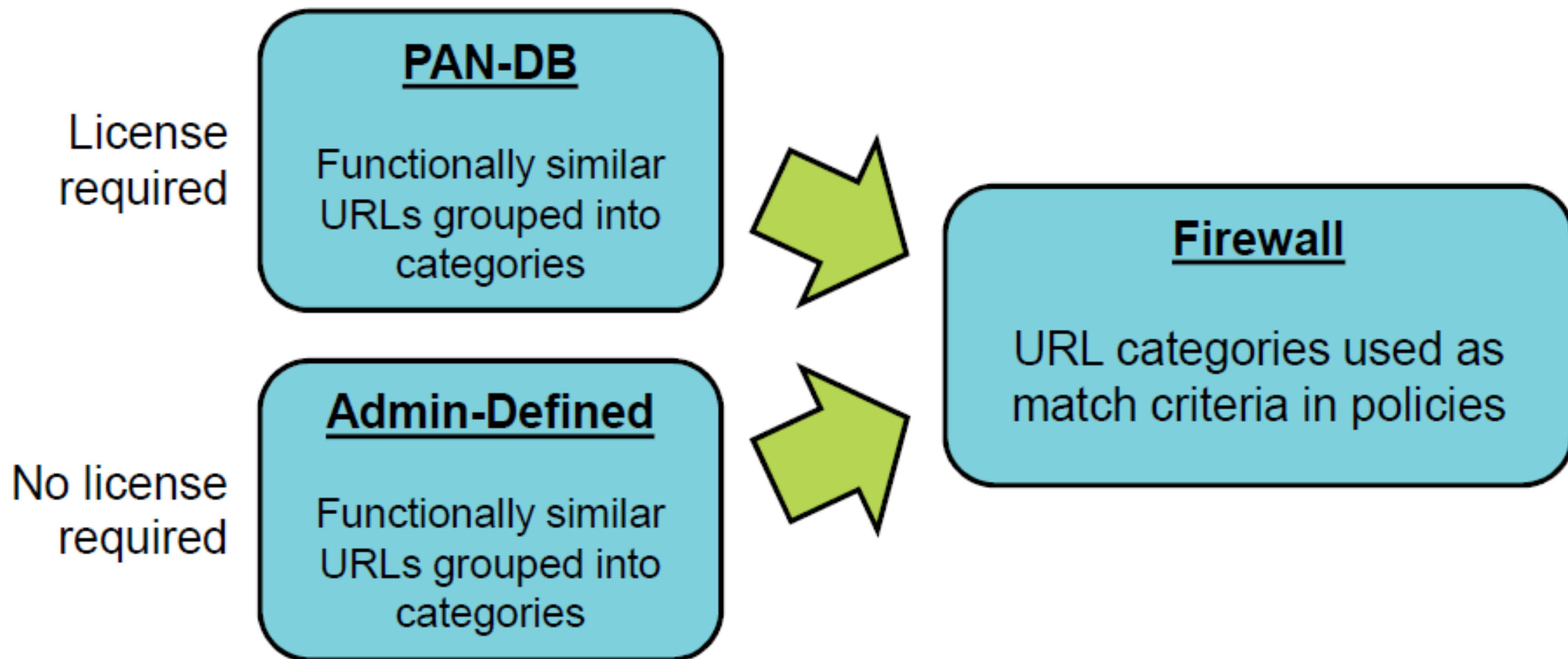
OK Cancel

- Add Security Profiles that are commonly used together
- Simplifies Security policy rule administration

URL Filtering Feature



URL Filtering Feature



URL Filtering Security Profile

Objects > Security Profiles > URL Filtering

Name	Location	Block List	Action for Block List	Allow List	Site Access	Credential Post
default	Predefined		block		Allow Categories (57) Alert Categories (0) Continue Categories (0) Block Categories (8) Override Categories (0)	Allow Categories (65) Alert Categories (0) Continue Categories (0) Block Categories (0)

Out-of-the-box profile

Click each to view categories in list

+ Add - Delete Clone | * indicates custom URL category, + indicates external dynamic list

- To create customized profiles:
 - **Clone** the default read-only profile and edit clone, or
 - **Add** a brand new profile

Configure Per-URL Category Actions

Objects > Security Profiles > URL Filtering > Add

URL Filtering Profile

Name: Marketing Department

Description:

Categories | Overrides | URL Filtering Settings | User Credential Detection

Category	Site Access	User Credential Submission
abortion	allow	allow
abused-drugs	allow	allow
adult	allow	allow
alcohol-and-tobacco	allow	allow
auctions	allow	allow
business-and-economy	allow	allow
computer-and-internet-in	allow	allow
content-delivery-network	allow	allow
copyright-infringement	allow	allow

* indicates a custom URL category, + indicates external dynamic list

Check URL Category

Has drop-down list with option to change all actions

Action to take when URL is accessed; allow is default

Alert, allow, block, continue, override

Alert, allow, block, continue

Action to take if user submits credentials to allowed URL

URL matching order:

1. Block list*
2. Allow list*
3. Custom URL categories*
4. External dynamic lists*
5. PAN-DB firewall cache
6. Downloaded PAN-DB file
7. PAN-DB cloud

*Supports wildcard characters

URL Filtering Response Pages

Web Page Blocked

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

User: 192.168.41.20

URL: www.2600.org/

Category: hacking

Web Page Blocked

Access to the web page you were trying to visit has been blocked in accordance with administrator if you believe this is in error.

User: 192.168.41.20

URL: www.handdrawinggames.com/desktopdf/game.asp

Category: games

If you feel this page has been incorrectly blocked, you may click Continue to proceed logged.

Continue

[Return to previous page](#)

Web Page Blocked

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

User: 192.168.41.20

URL: www.ketelone.com/

Category: alcohol-and-tobacco

If you require access to this page, have an administrator enter the override password here:

Continue

[Return to previous page](#)