tilb
Távközlés-
Informatika
Laboratórium

IP alapú kommunikáció

11. Előadás Cybersecurity II. NGFW

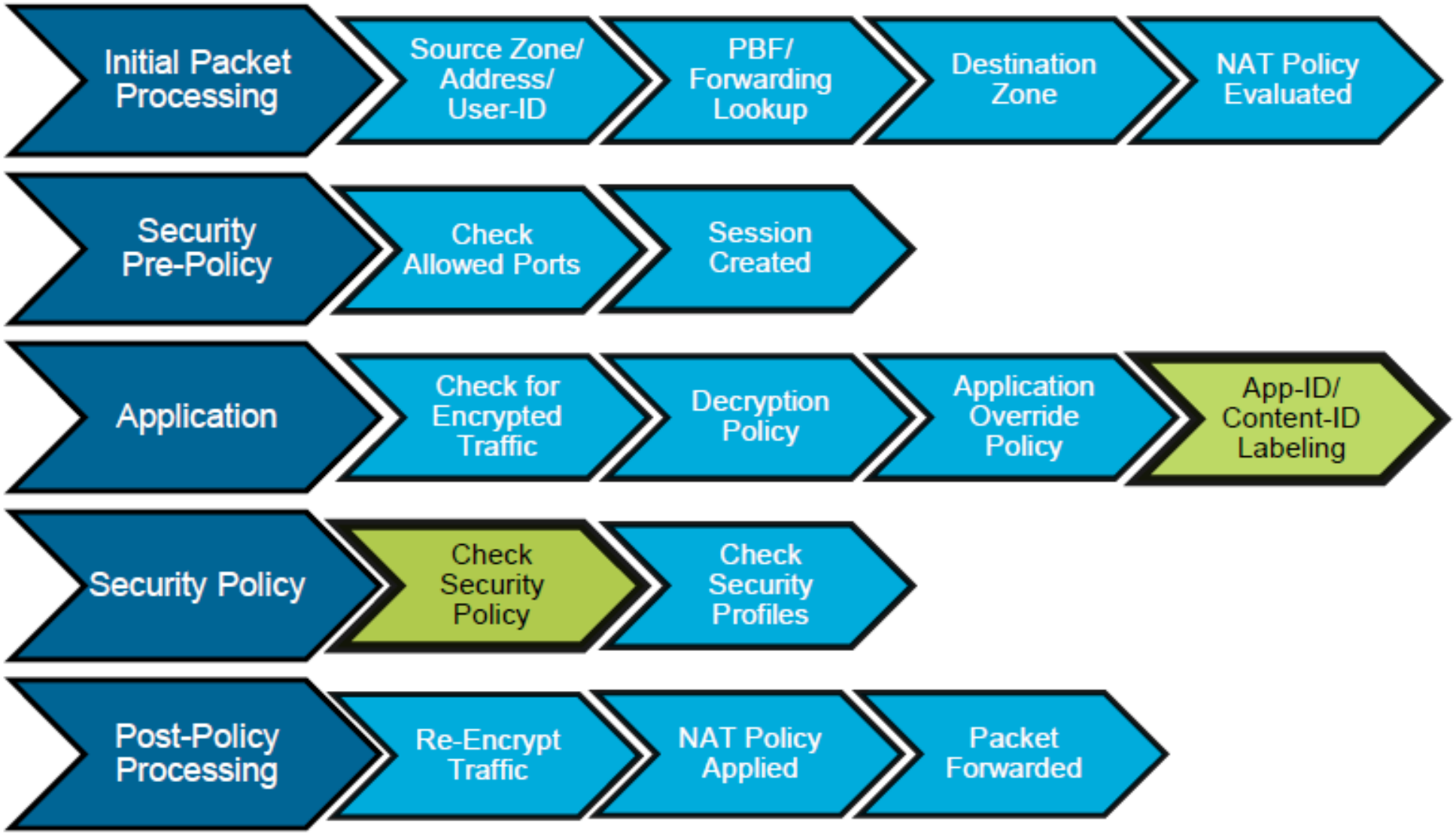
Kovács Ákos

paloalto NETWORKS
CYBERSECURITY ACADEMY

Szűrési metódusok

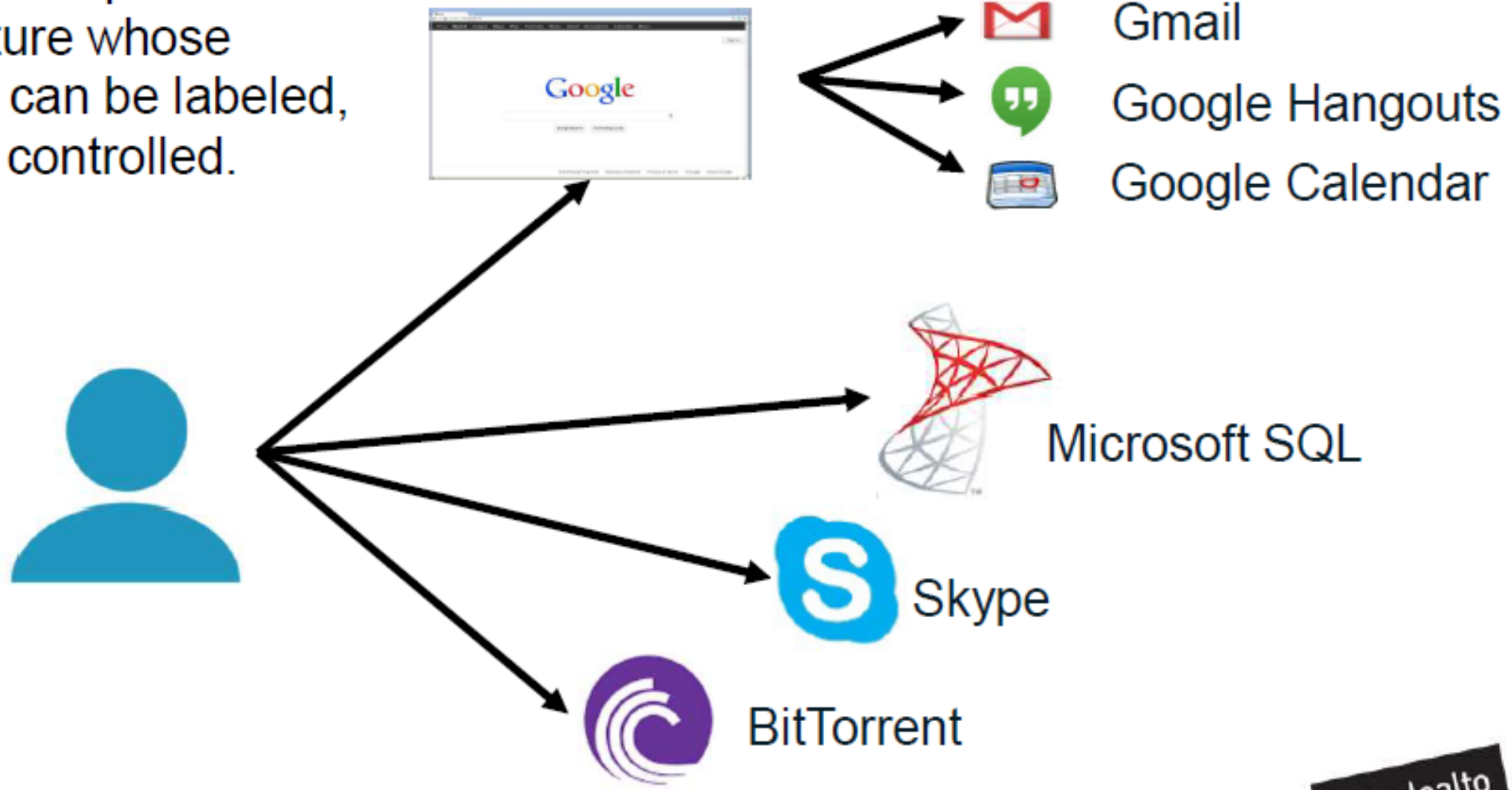
- APP-ID alapú
- Content-ID alapú
- URL alapú

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	any	service-ftp	Allow

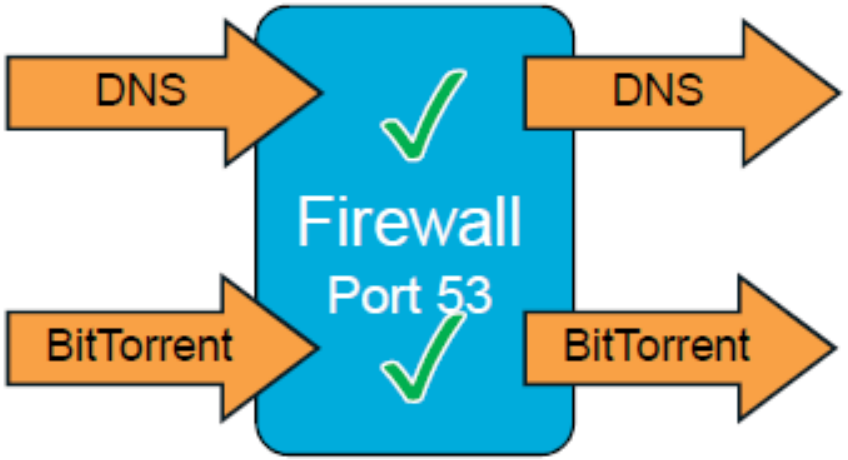
Application-based security rule

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

Port-Based Versus Next-Generation Firewalls

Traditional Firewalls

Firewall Rule: ALLOW Port 53



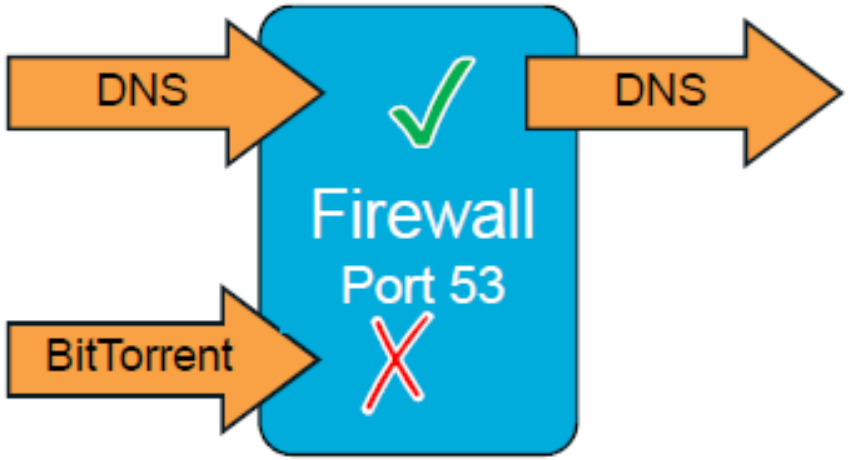
Packet on port 53: Allow

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

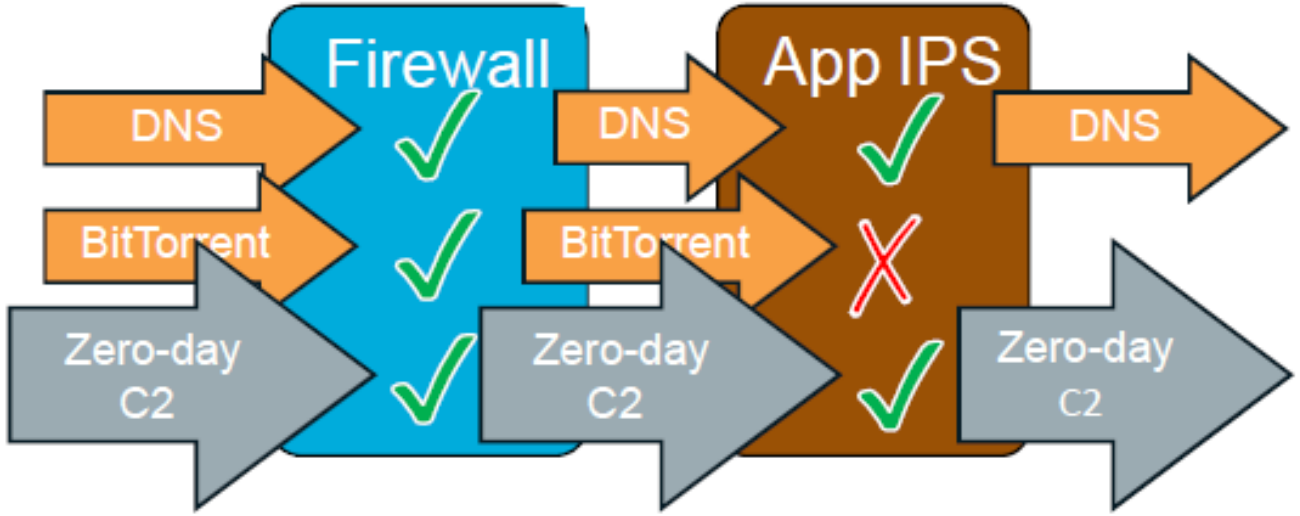
Visibility: BitTorrent detected and blocked

Zero-Day Malware – IPS Versus App-ID

Legacy Firewalls

Firewall Rule: ALLOW Port 53

Application IPS Rule: Block BitTorrent



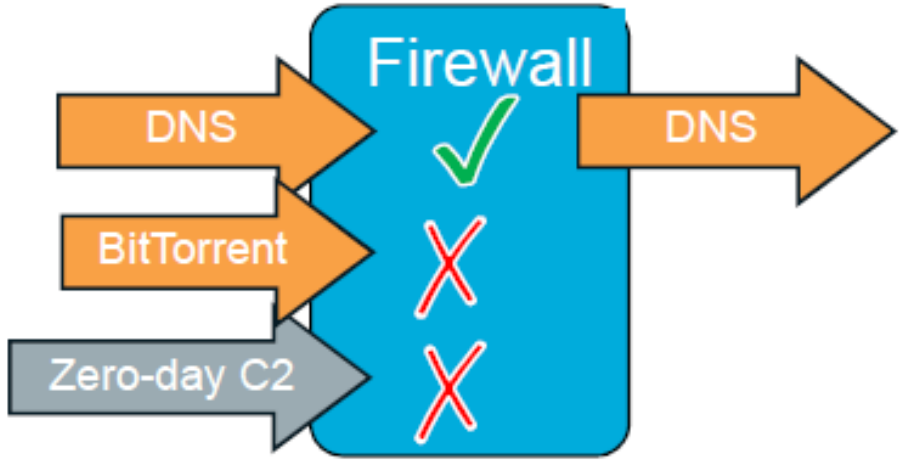
Packet on port 53: Allow

C2 ≠ BitTorrent: Allow

Visibility: Packet on port 53 allowed

Palo Alto Networks Firewall with App-ID

Firewall Rule: ALLOW DNS



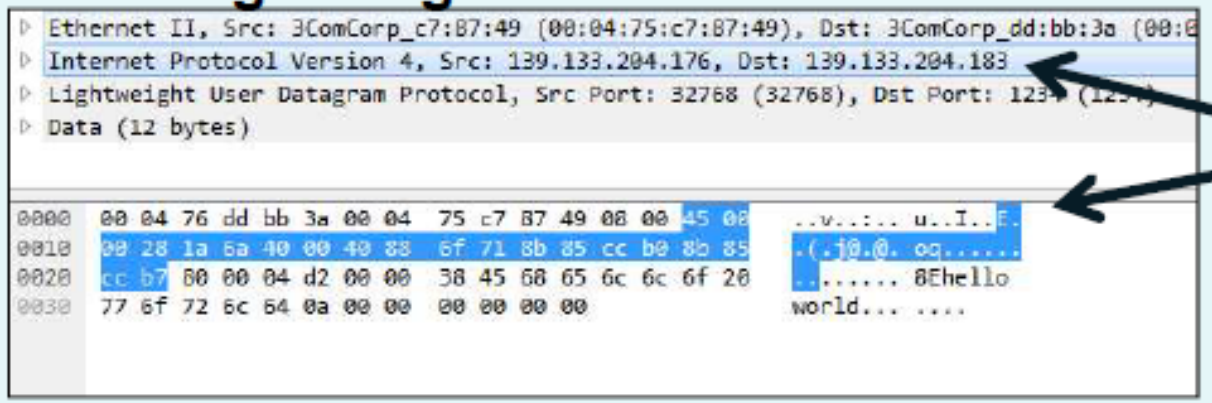
DNS = DNS: Allow

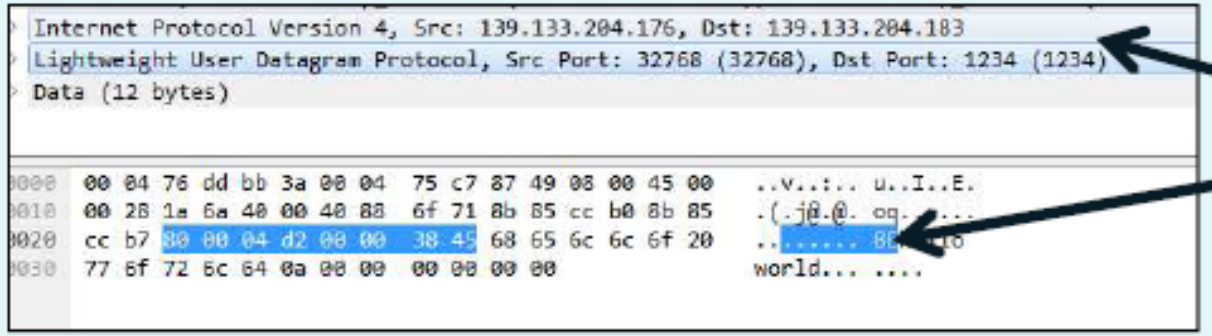
C2 ≠ DNS: Deny

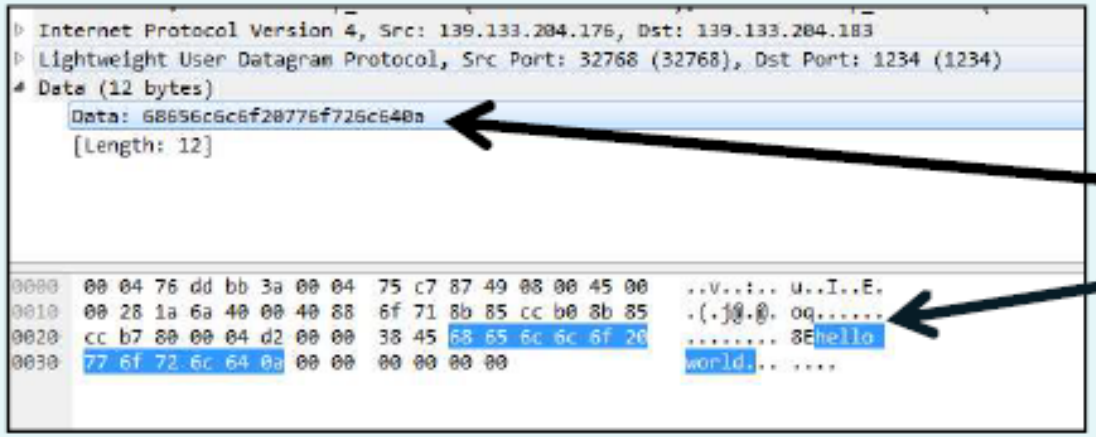
Visibility: Unknown traffic detected and blocked

App-ID and UDP

Lightweight UDP Packet







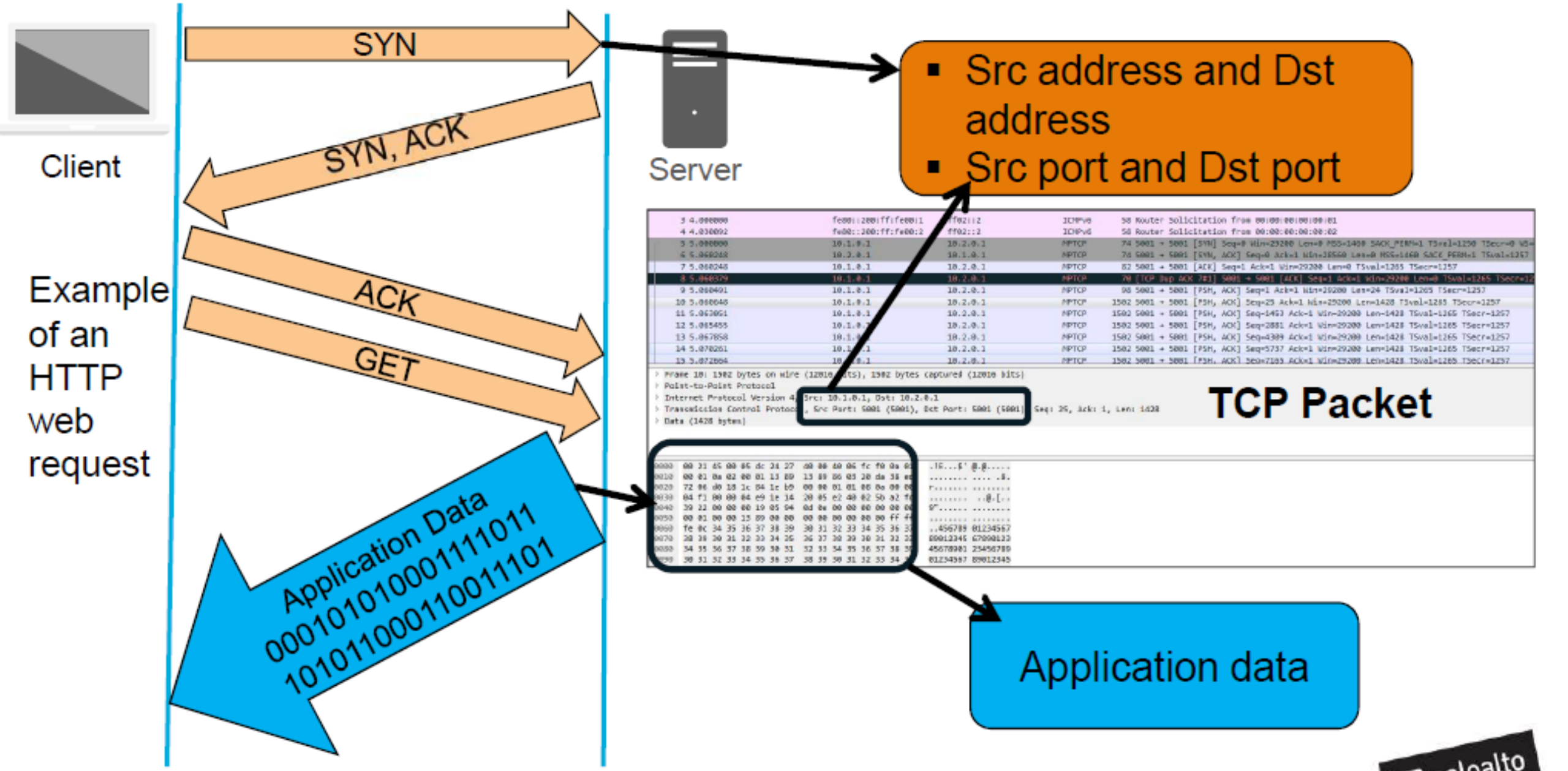
The first UDP packet

Src address and Dst address

Src port and Dst port

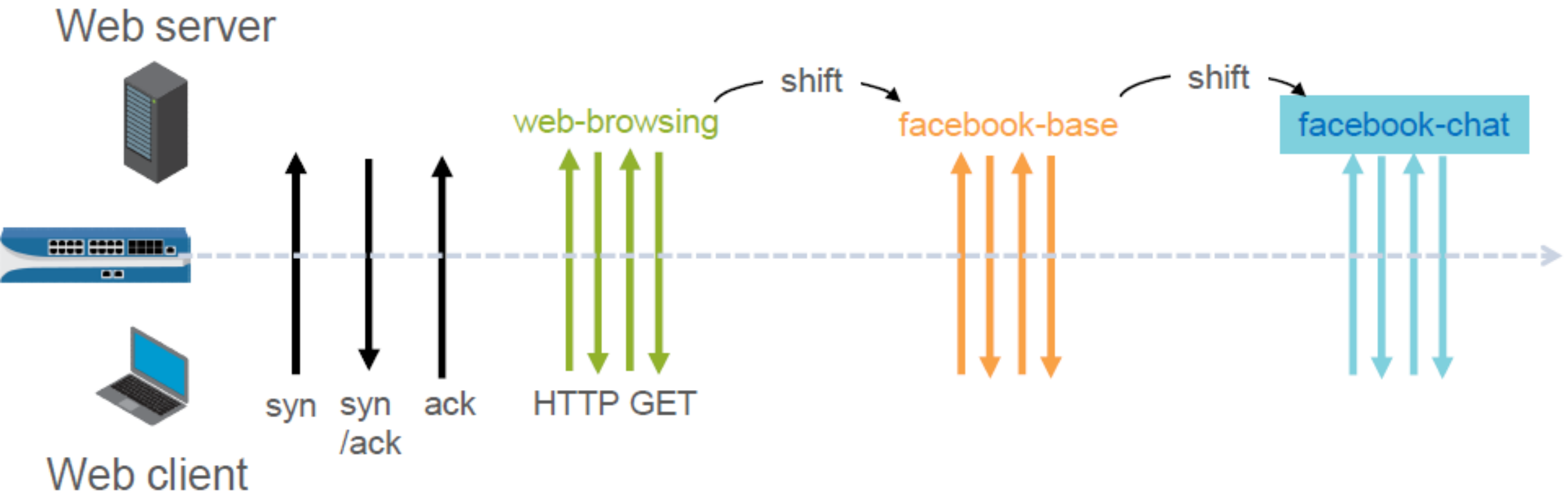
Application data

App-ID and TCP



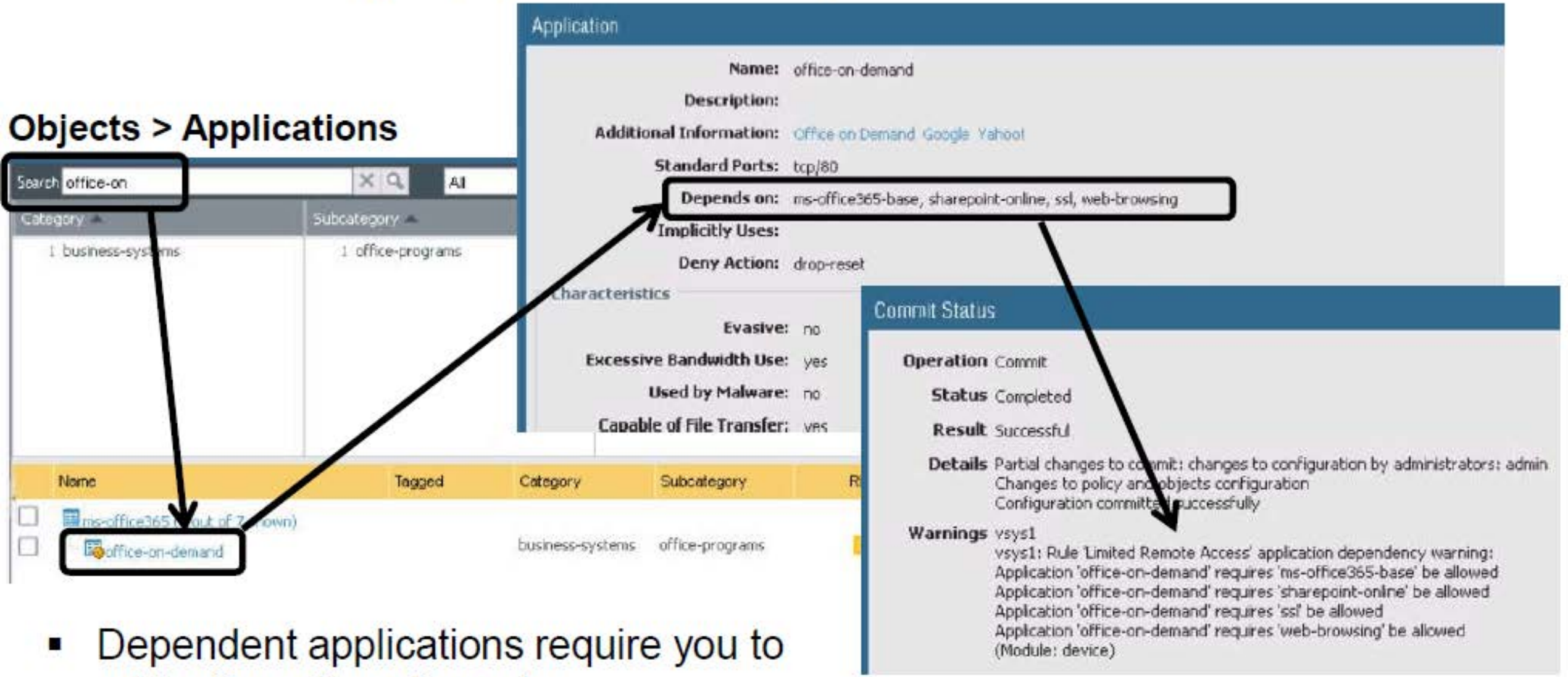
Application Shifts

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



Determining Application Dependencies

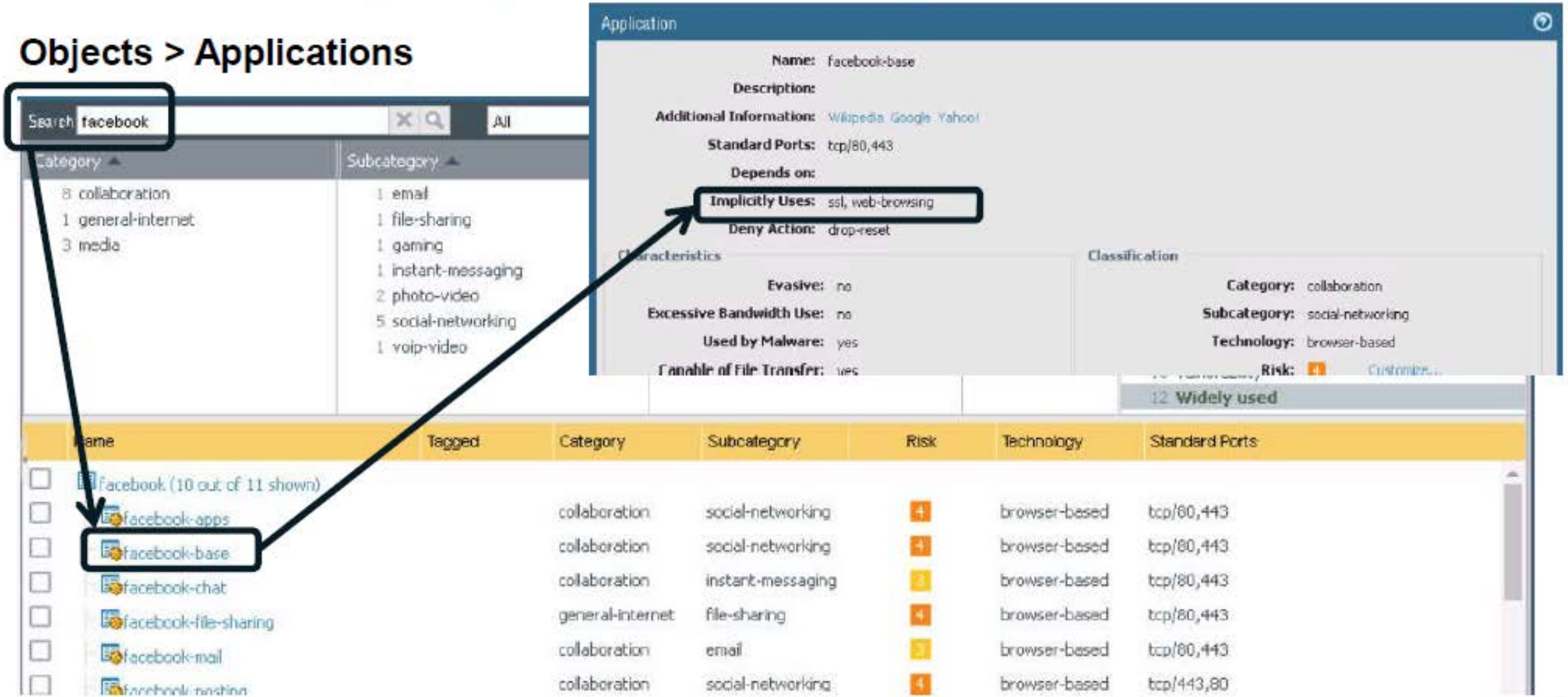
Objects > Applications



- Dependent applications require you to add a Security policy rule

Determining Implicitly Used Applications

Objects > Applications



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

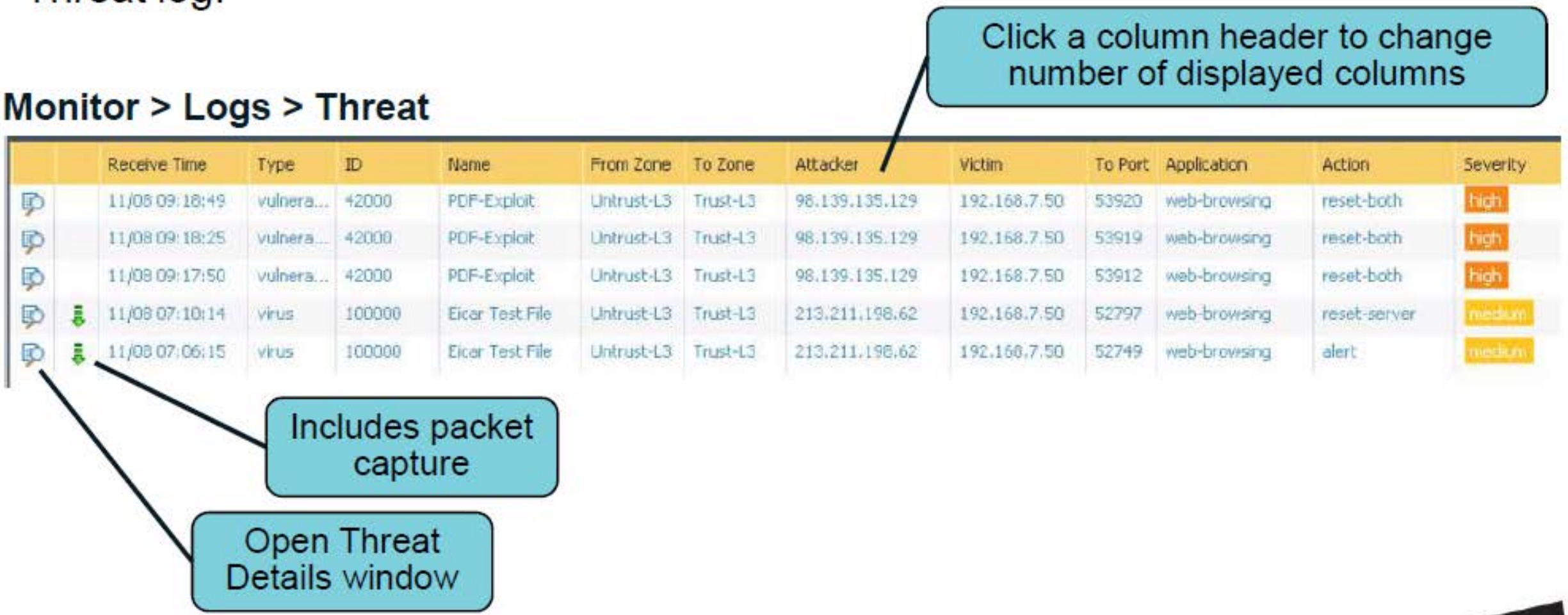
WildFire Analysis

Security Profile Group

Threat Log

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

Monitor > Logs > Threat



Default Vulnerability Protection Security Profiles

Objects > Security Profiles > Vulnerability Protection

Name	Location	Count	Rule Name	Threat Name	Host Type	Severity	Action	Packet Capture
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...					
default	Predefined	Rules: 6	simple-client-critical	any	client	critical	default	disable
						high	de	
						medium	de	
						critical	de	
						high	default	disable
						medium	default	disable
			medium					

Add Delete Clone

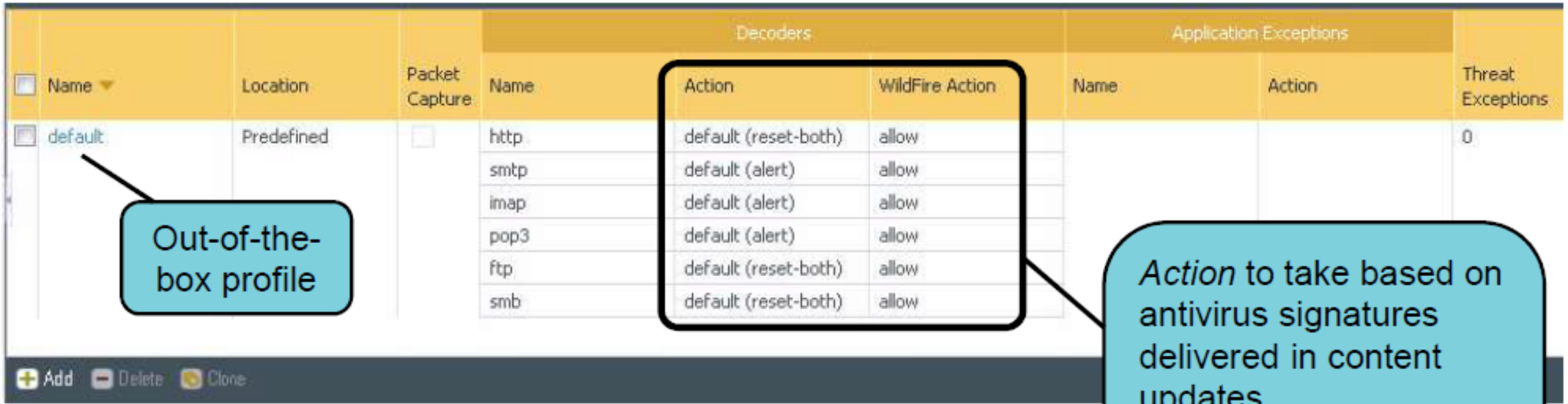
Default (read-only) profiles

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



Out-of-the-box profile

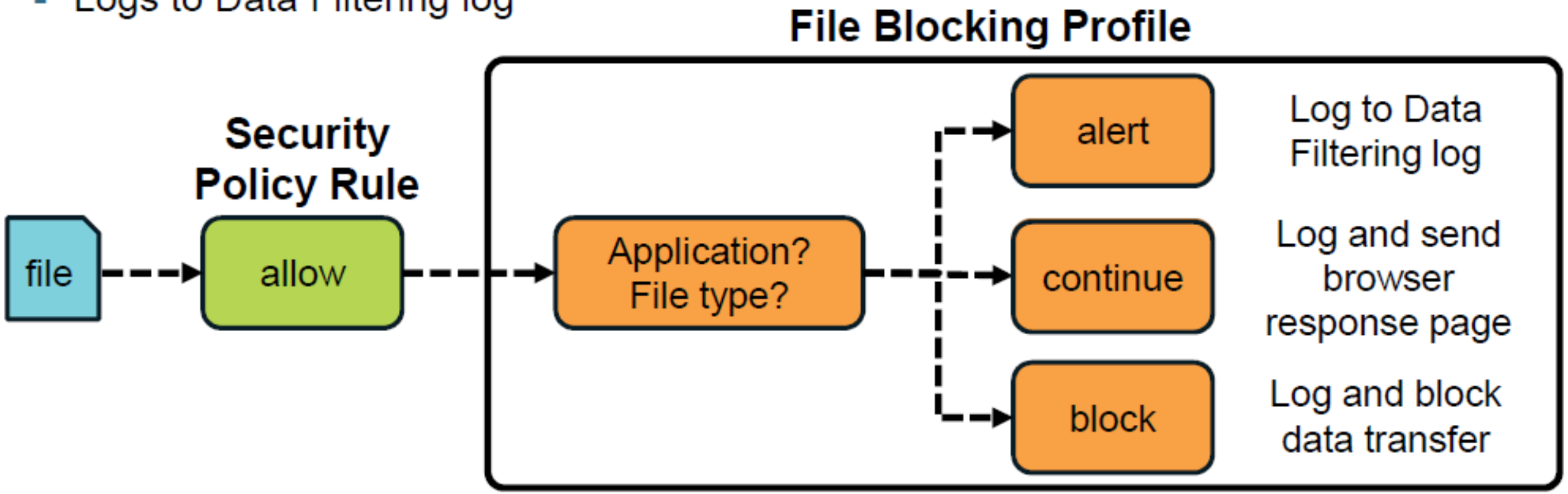
Action to take based on antivirus signatures delivered in content updates

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

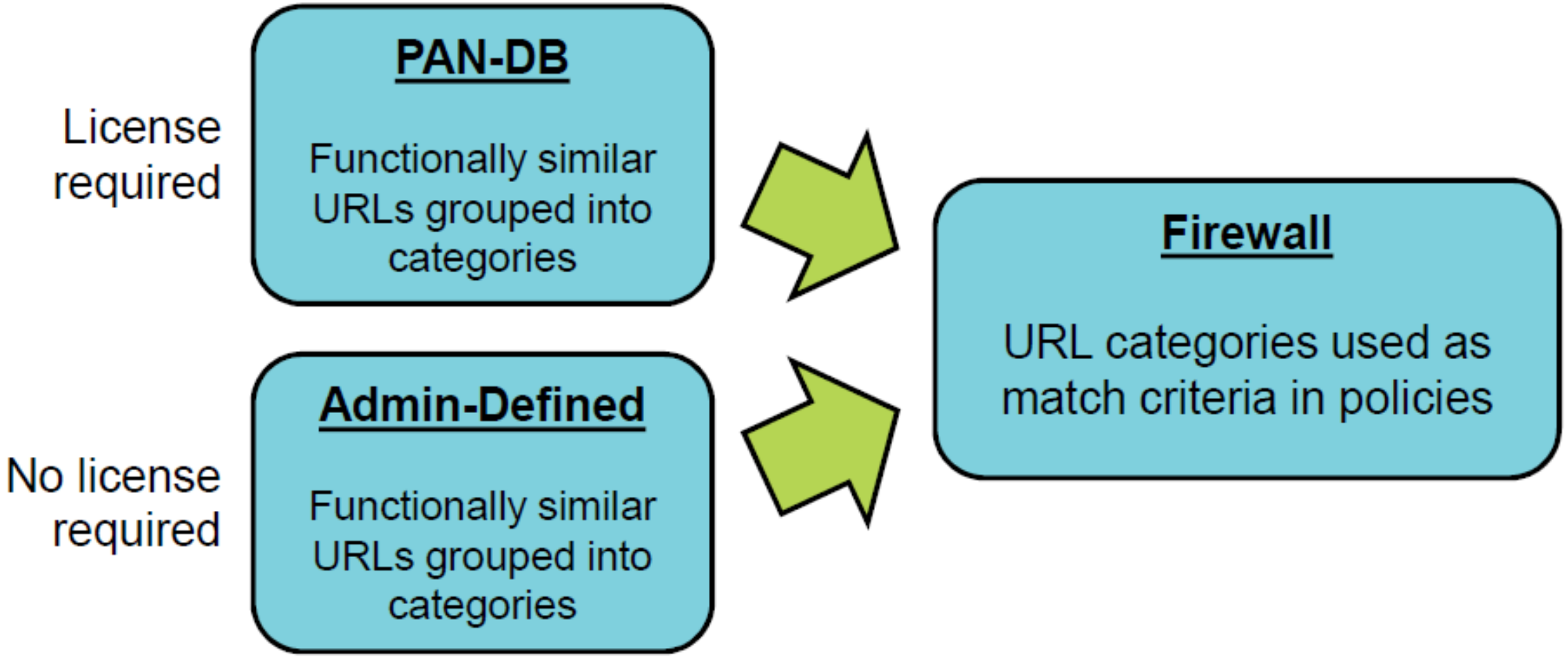


Security Profile Groups

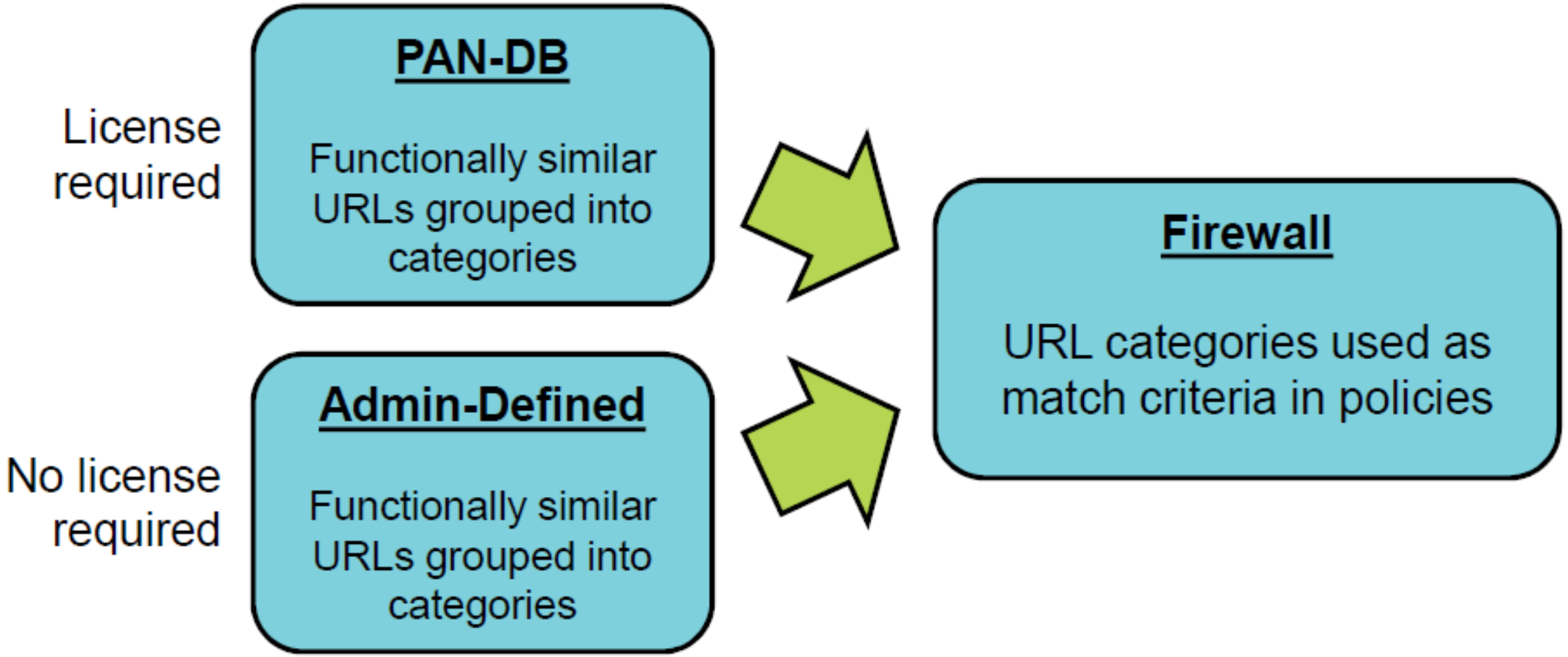
Objects > Security Profile Groups > Add

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

URL Filtering Feature

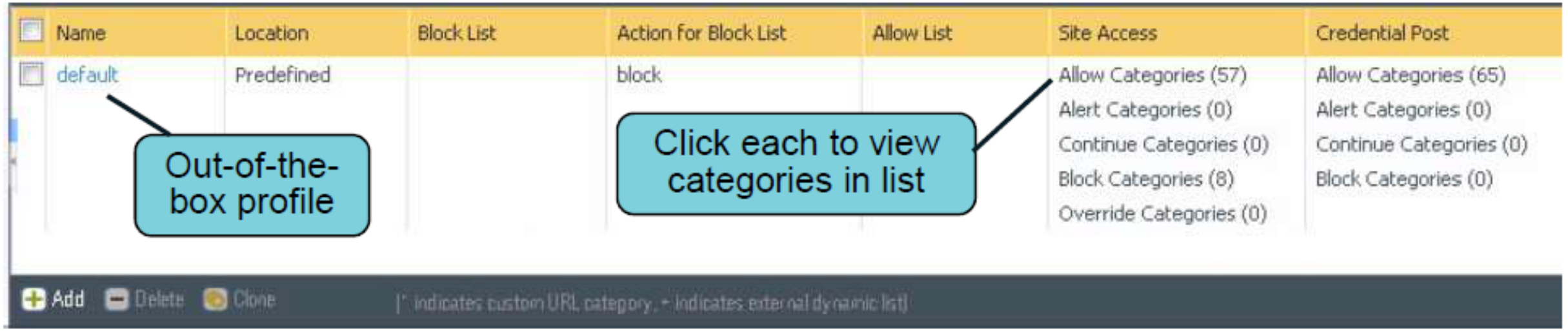


URL Filtering Feature



URL Filtering Security Profile

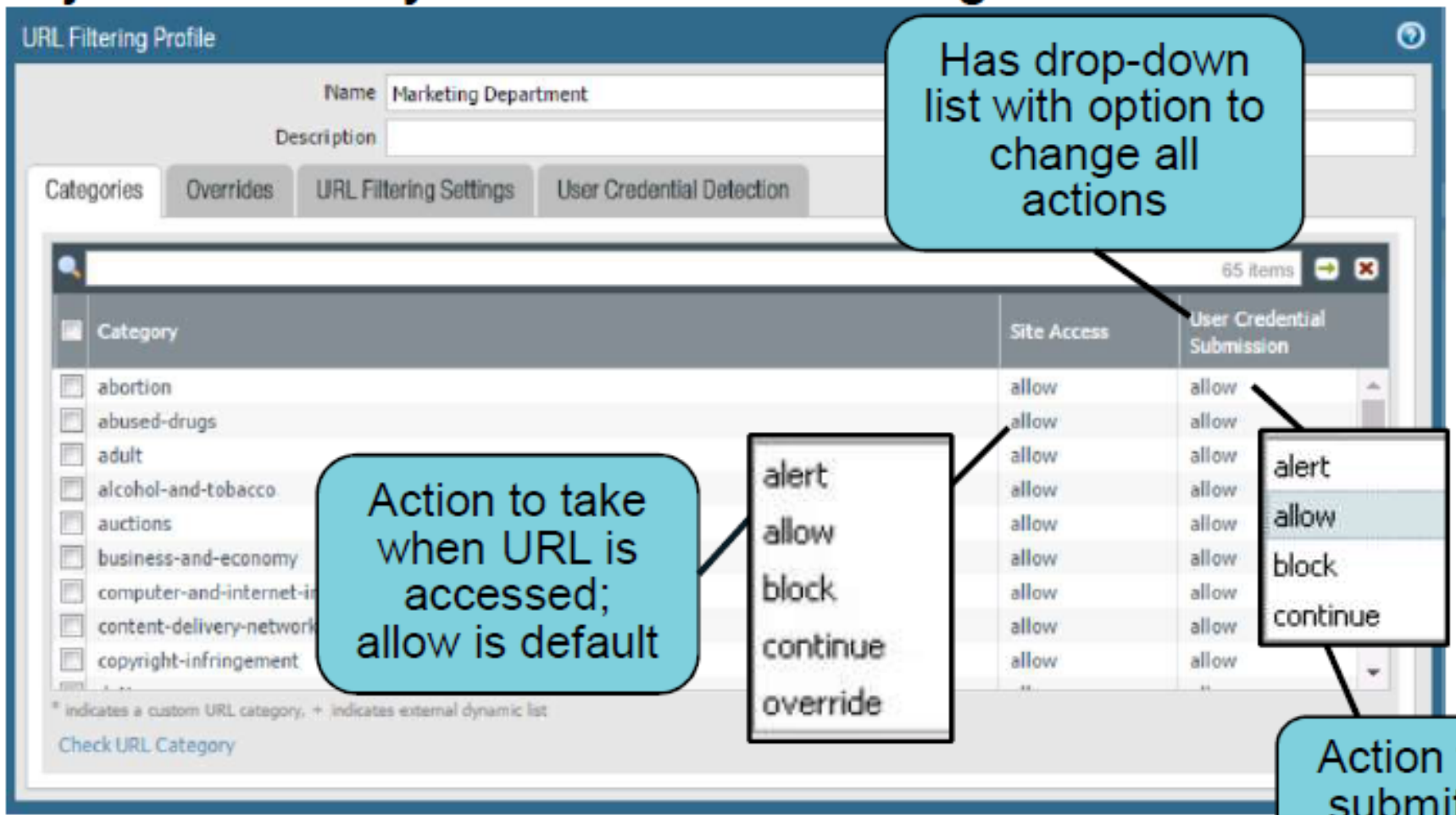
Objects > Security Profiles > URL Filtering



- 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 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