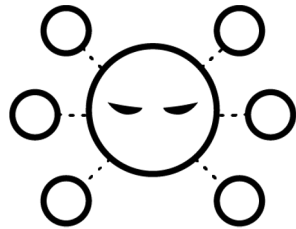


## BLOCK THREATS FROM KNOWN-BAD SOURCES



## *AVOID DANGEROUS NETWORK NEIGHBORHOODS*

---

- Block access to or from known-bad IP addresses
- Block access to or from known-bad domains
- Block access to or from known-bad URLs
- Other URL filtering features

## Learning Objectives

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

- Configure the firewall to block traffic from known-malicious IP addresses
- Configure the firewall to block traffic from known-malicious domains
- Configure the firewall to block traffic from known-malicious URLs
- Describe other URL filtering operations and options





**Block access to or from known-bad IP addresses**

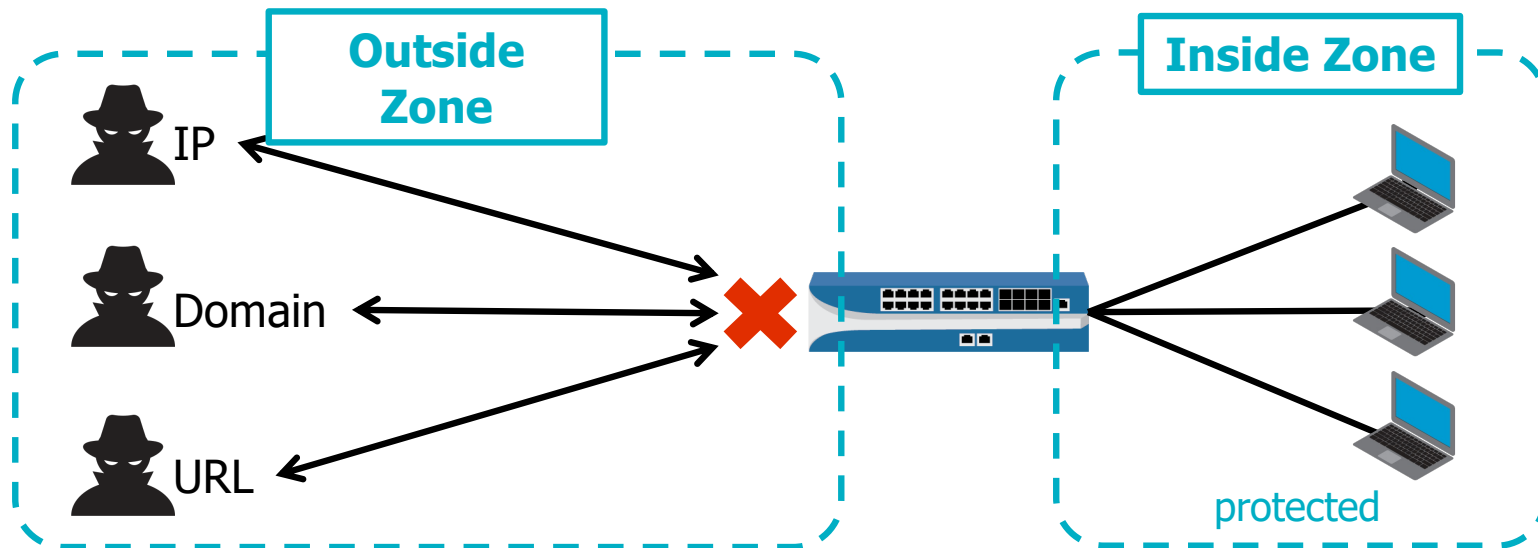
Block access to or from known-bad domains

Block access to or from known-bad URLs

Other URL filtering features



## Block Threats from Known-Bad Sources



- The firewall can block connections to known-bad sources.
- Useful for blocking the Delivery or Command-and-Control stage of the cyberattack lifecycle

# Block Known-Bad IP Addresses

## Policies > Security

	NAME	TAGS	TYPE	Source			Destination			APPLICATION	SERVICE	ACTION
				ZONE	ADDRESS	USER	ZONE	ADDRESS				
1	Block-Known-Bad-IPs	Users_Net	universal	Users_Net	any	any	Internet	194.87.95.16	IP address (or range)			
								A1	Address object			
								A2				
								Bureau-121				
								KP	Geographic region			
								Malicious-IP-Group				
								Palo Alto Networks - Known malicious IP addre...				

- Use the Security policy **Address** fields.
- Destination IP address: Block connections *to* a malicious IP address.
- Source IP address: Block connections *from* a malicious IP address.

# Create an Address Object

Objects > Addresses > Add

The screenshot shows the 'Add Address' dialog in the Palo Alto Networks management interface. The 'Name' field is set to 'Bureau-121' and the 'Description' is 'Address object for Bureau-121'. The 'Type' dropdown is currently set to 'IP Netmask' and is open, showing other options: 'IP Range', 'IP Wildcard Mask', and 'FQDN'. The 'Address' field contains '212.0.34.0/24' and has a 'Resolve' button next to it. The dialog also includes 'OK' and 'Cancel' buttons at the bottom right.

- Add malicious IP addresses to an address object:
  - The list of known-bad IP addresses can change quickly.
- Address objects can be used in Security policy rules:
  - In source or destination address fields
- Address objects can represent:
  - A single IP address
  - An IP netmask
  - An IP address range
  - A specific set of addresses
  - An FQDN

# Create a Static Address Group

**Objects > Address Groups > Add**

Address Group

Name: Malicious-IP-Group

Description: Contains malicious IP address objects.

Type: Static

Addresses:

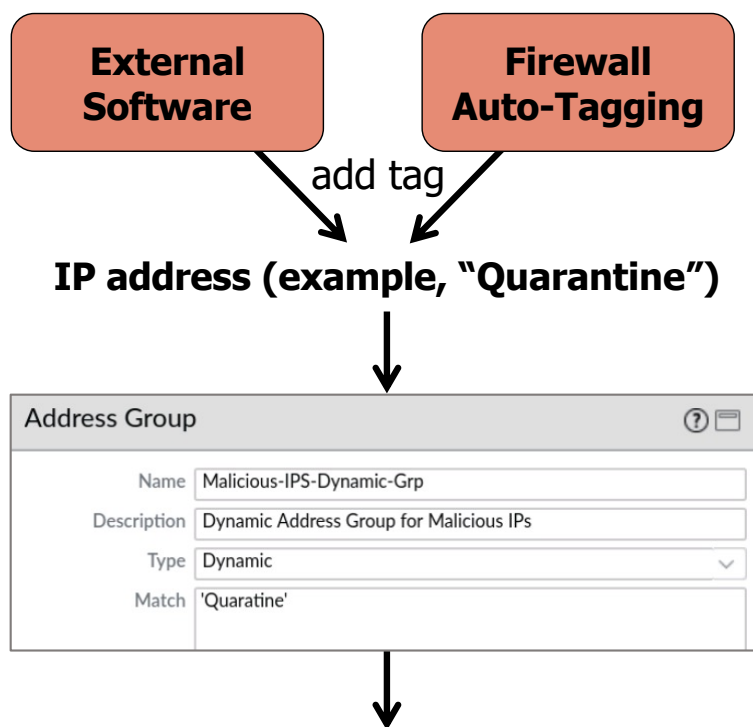
- ☐ ADDRESS ^
- ☐ malicious-fqdn-addr-object
- ☐ malicious-ip-address-1

Browse Add Delete

Tags: Users\_Net

- Use to shorten and simplify a policy rule
- Membership must be manually updated
- Updates require a commit operation
- Can contain:
  - Address objects
  - Other address groups

## Create a Dynamic Address Group

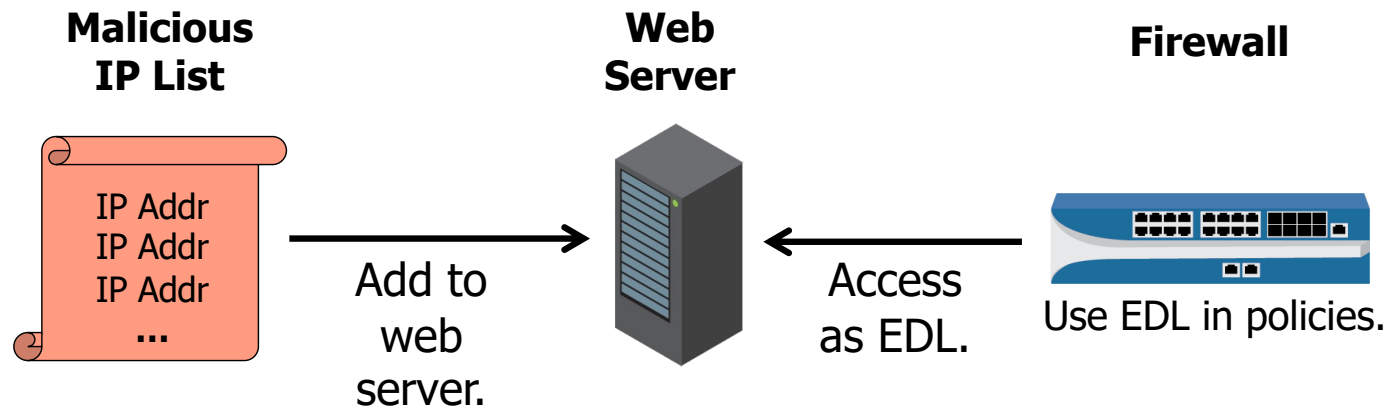


- Tagged IP addresses automatically added to group
- No commit necessary
- IP addresses in group used as match condition in rules

	NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	ACTION
				ZONE	ADDRESS	USER	ZONE	ADDRESS			
1	Block-Known-Bad-IPs	Users_Net	universal	Users_Net	any	any	Internet	Malicious-IPS-Dynamic-Grp	any	any	Deny



# Use External Malicious IP Lists



- All firewall models:
  - Support up to 30 EDLs
  - Feature different list capacities

## Objects > External Dynamic Lists > List Capacities

Capacities		
LIST TYPE	CURRENTLY USED IN POLICY	TOTAL CAPACITY
IPs	0	50000
Predefined IPs	3697	50000
Domains	4	50000
URLs	10	50000

# Use the Predefined Malicious IP Lists

## Objects > External Dynamic Lists > Add

<input type="checkbox"/>	NAME	LOCATION	DESCRIPTION	SOURCE
Dynamic IP Lists				
<input type="checkbox"/>	Palo Alto Networks - Bulletproof IP addresses	Predefined	IP addresses that are provided by bulletproof hosting providers. Because bulletproof hosting providers place few, if any, restrictions on content, attackers can use these services to host and distribute malicious, illegal, and unethical material.	Palo Alto Networks - Bulletproof IP addresses
<input type="checkbox"/>	Palo Alto Networks - High risk IP addresses	Predefined	IP addresses that have recently been featured in threat activity advisories distributed by high-trust organizations. However, Palo Alto Networks does not have direct evidence of maliciousness for these IP addresses.	Palo Alto Networks - High risk IP addresses
<input type="checkbox"/>	Palo Alto Networks - Known malicious IP addresses	Predefined	IP addresses that are currently used almost exclusively by malicious actors for malware distribution, command-and-control, and for launching various attacks.	Palo Alto Networks - Known malicious IP addresses

- Palo Alto Networks maintains three malicious IP address lists.
- They can be used in Security policy rules.

To display the IP list, click the name.

External Dynamic Lists (Read Only)

Name

Create List **List Entries And Exceptions**

List Entries

2531 items → ×

	LIST ENTRIES
<input type="checkbox"/>	176.103.55.73
<input type="checkbox"/>	123.195.7.136
<input type="checkbox"/>	200.35.56.81

# Configure Other Malicious IP Lists

Objects > External Dynamic Lists > Add

External Dynamic Lists

Name Malicious-IP-Address-Feed

Create List | List Entries And Exceptions

Type IP List

Description

Source http://mywebserver.mycompany.com/edlip.txt

Server Authentication

Certificate Profile None

Check for updates Five Minute

Five Minute  
Hourly  
Daily  
Weekly  
Monthly

Add to Security policy rule.

- An EDL:
  - Is maintained on a web server
  - Is periodically read by a firewall
- Use EDLs of type **IP List** in Security policy rules:
  - In source or destination address fields

## External Dynamic List Monitoring

- Identify traffic that matches an EDL.
- New log fields identify which EDL is associated with each rule.
- Monitor only IP address, URL, or domain EDLs.

External Dynamic List Type	Firewall Log	Log Fields
IP address	<ul style="list-style-type: none"><li>• Traffic</li><li>• Threat</li><li>• Decryption</li><li>• Tunnel Inspection</li><li>• Unified</li></ul>	<ul style="list-style-type: none"><li>• SOURCE EDL</li><li>• DESTINATION EDL</li></ul>
URL	<ul style="list-style-type: none"><li>• Traffic</li><li>• URL Category</li><li>• Tunnel Inspection</li></ul>	<ul style="list-style-type: none"><li>• URL CATEGORY</li><li>• URL CATEGORY LIST</li></ul>
Domain	<ul style="list-style-type: none"><li>• Threat</li></ul>	<ul style="list-style-type: none"><li>• NAME</li></ul>

Block access to or from known-bad IP addresses



**Block access to or from known-bad domains**

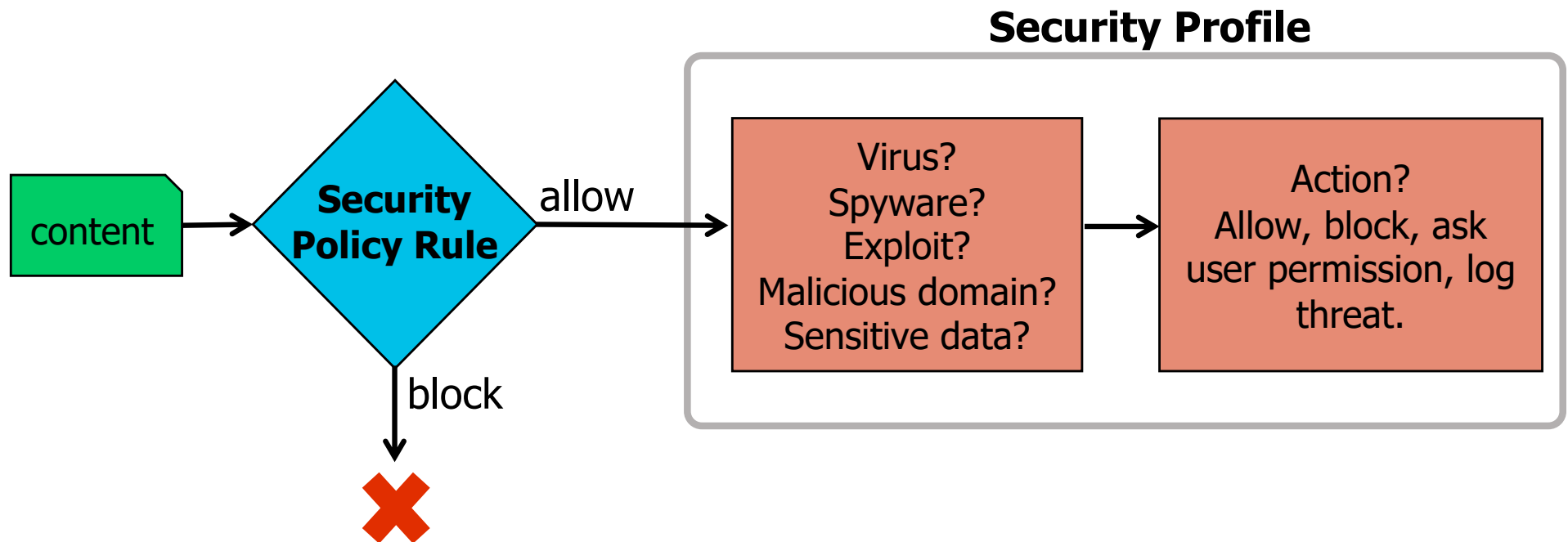
Block access to or from known-bad URLs

Other URL filtering features



## Security Policy with Security Profiles

- Security Profiles are attached to Security policy allow rules.
- Security Profiles implement additional security checks on allowed traffic.



# Security Profile Types

## Policies > Security

NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	ACTION	PROFILE
			ZONE	ADDRESS	USER	ZONE	ADDRESS				
1 Users_to_Extranet	Users_Net	universal	Users_Net	any	any	Extranet	any	any	application-default	Allow	
2 Users_to_Internet	Users_Net	universal	Users_Net	any	any	Internet	any	any	application-default	Allow	
3 Extranet_to_Internet	Extranet	universal	Extranet	any	any	Internet	any	any	application-default	Allow	



Antivirus



Anti-Spyware



Vulnerability Protection



URL Filtering

Can block access to  
malicious domains



File Blocking



Data Filtering



WildFire Analysis



Security Profile Group

## Anti-Spyware Security Profiles

- Palo Alto Networks distributes malicious domain signatures.
- Malicious domain signatures are detected using Anti-Spyware Profiles.
- A profile contains a ruleset to detect and process threats.

### Objects > Security Profiles > Anti-Spyware

<input type="checkbox"/>	Outbound-AS	Policies: 2	Block-Critical-High-Medium	any	critical,high,medium	reset-both	single-packet
			Default-Low-Info	any	informational,low	default	disable

- Attach an Anti-Spyware Profile to a Security policy rule.

### Policies > Security

	NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	ACTION	PROFILE
				ZONE	ADDRESS	USER	ZONE	ADDRESS				
1	Allow_Trusted_Apps ▾	Users_Net	universal	Users_Net	any	any	Internet	any	Trusted-Apps	application-default	Allow	



# Configure Other Malicious Domain Lists

Objects > External Dynamic Lists > Add

The screenshot shows the 'External Dynamic Lists' configuration window. The 'Name' field is set to 'Malicious\_Domains\_Feeds'. A callout box points to this field with the text 'Add to Anti-Spyware Profile.' The 'Type' dropdown is set to 'Domain List'. The 'Source' field contains the URL 'https://mywebserver.mycompany.com/domain.txt'. The 'Check for updates' dropdown is set to 'Hourly', and a callout box shows the available options: 'Five Minute', 'Hourly', 'Daily', 'Weekly', and 'Monthly'. The 'Server Authentication' section shows 'Certificate Profile' set to 'None'.

External Dynamic Lists

Name: Malicious\_Domains\_Feeds

Create List | List Entries And Exceptions

Type: Domain List

Description:

Source: https://mywebserver.mycompany.com/domain.txt

☐ Automatically expand to include subdomains

Server Authentication

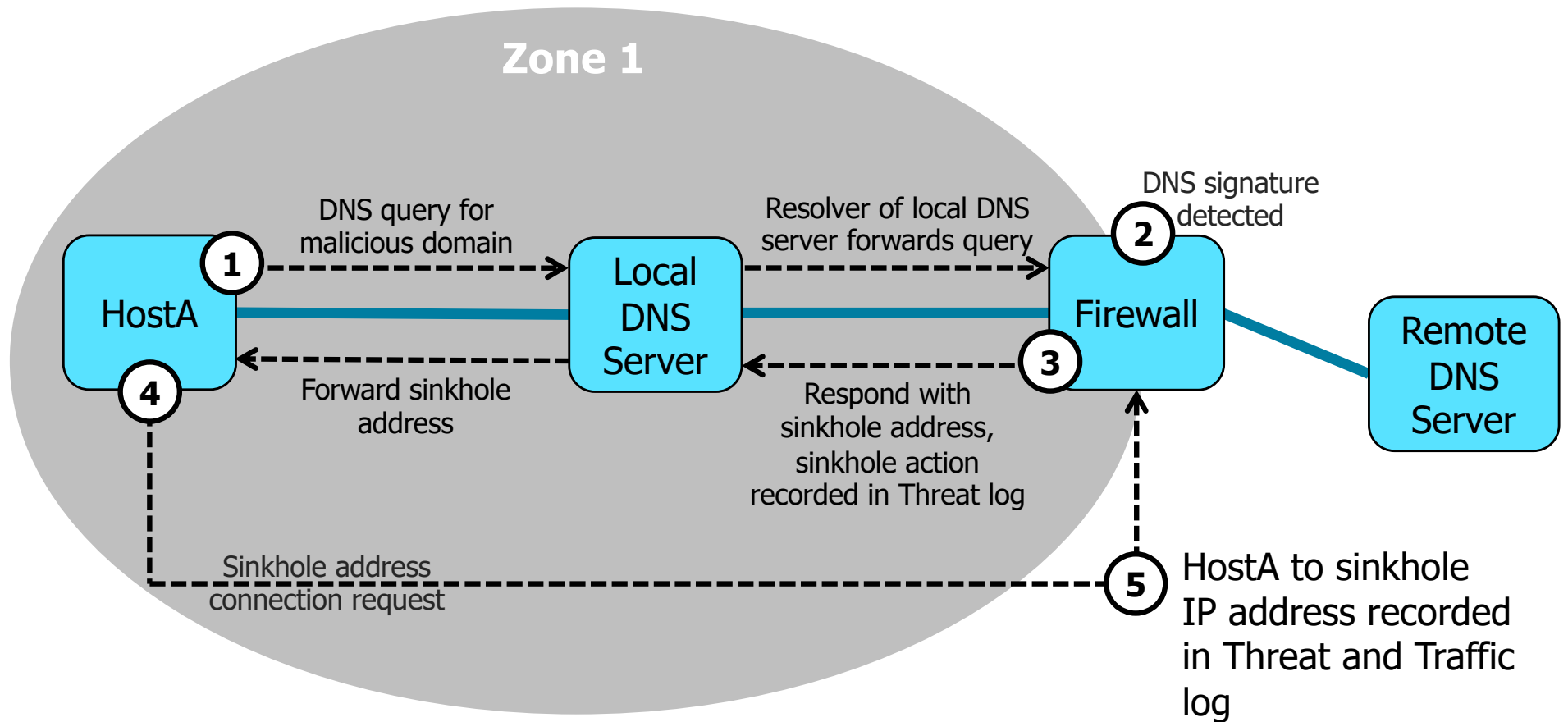
Certificate Profile: None

Check for updates: Hourly

Five Minute  
Hourly  
Daily  
Weekly  
Monthly

- Malicious domain lists are available from many sources.
- Malicious domain lists are accessed as EDLs.
- EDL must be of type **Domain List**.

# DNS Sinkhole Operation



# Configure DNS Signature Match Protection

- Third-party malicious domain lists are made available as EDLs.
- Best practice is to enable sinkhole.
- Can use the Palo Alto Networks IP address or, optionally, your own internal address.

## Objects > Security Profiles > Anti-Spyware > Add

Anti-Spyware Profile

Name: Outbound-AS  
Description: Anti-Spyware Profile for Outbound Traffic

Signature Policies | Signature Exceptions | **DNS Policies** | DNS Ex

DNS Policies

9 items

<input type="checkbox"/>	SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
External Dynamic Lists				
<input type="checkbox"/>	Malicious-Domains-EDL		sinkhole	disable
<input type="checkbox"/>	Malicious_Domains_Feeds		sinkhole	disable
Palo Alto Networks Content				
<input type="checkbox"/>	default-paloalto-dns		sinkhole	disable

DNS Sinkhole Settings





Sinkhole IPv4: Palo Alto Networks Sinkhole IP (sinkhole.paloaltonetworks.com)  
Sinkhole IPv6: IPv6 Loopback IP (::1)

Custom EDL with malicious domains with policy action configured as sinkhole.

Can use Palo Alto Networks IP or internal IP address

# View Malicious Domains in the Threat Log

Monitor > Logs > Threat

	RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	TO PORT	APPLICATI...	ACTION	SEVERITY	URL
	07/20 22:01:59	spyware	malicious-domains-edl	Users_Net	Internet	192.168.1.20	4.2.2.2	53	dns	sinkhole	medium	quora.com
	07/20 22:01:44	spyware	malicious-domains-edl	Users_Net	Internet	192.168.1.20	4.2.2.2	53	dns	sinkhole	medium	quora.com
	07/20 22:01:28	spyware	malicious-domains-edl	Users_Net	Internet	192.168.1.20	4.2.2.2	53	dns	sinkhole	medium	producthunt.com
	07/20 22:00:49	spyware	malicious-domains-edl	Users_Net	Internet	192.168.1.20	4.2.2.2	53	dns	sinkhole	medium	quora.com

Internal DNS server or infected host

Typically an external DNS server

- If you see a sinkhole in the Threat log:
  - Filter the Traffic log to see who is attempting to connect to the sinkhole IP address.
  - Hosts attempting to connect to the sinkhole address could be infected.
- Check logs daily or run a daily report.

Block access to or from known-bad IP addresses

Block access to or from known-bad domains

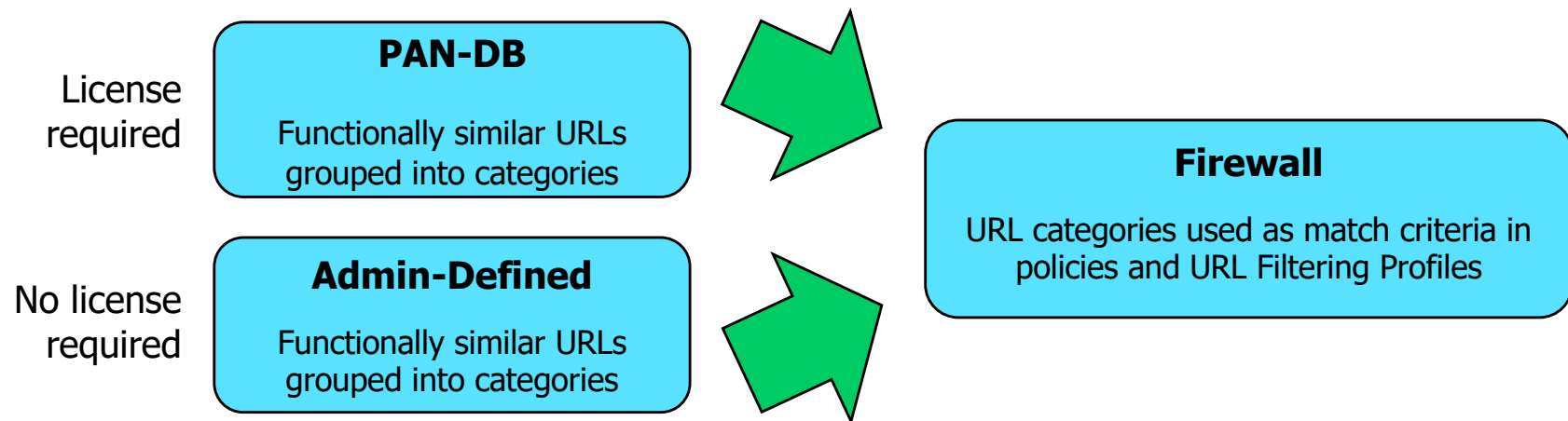


**Block access to or from known-bad URLs**

Other URL filtering features



## URL Filtering Features



- Use URL filtering to reduce the attack surface:
  - Disrupts the Delivery or Command-and-Control stage of the cyberattack lifecycle
- Two methods:
  - Use URL categories as a match condition in a Security policy deny rule.
  - Block access to a URL category in a URL Filtering Profile.

# Use a Security Policy Deny Rule

## Policies > Security

	NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION
				ZONE	ADDRESS	USER	ZONE	ADDRESS				
1	Block-Risky-URLs	Users_Net	universal	Users_Net	any	any	Internet	any	any	application-default	command-and-control dynamic-dns hacking high-risk malware phishing unknown	Deny

- Block access for most employees to risky URL categories:
  - Recommend blocking command-and-control, dynamic-dns, hacking, high-risk, malware, phishing, unknown
  - Other categories to consider blocking include adult, extremism, new-registered-domain, parked, proxy-avoidance-and-anonymizers, questionable
- Deny rules typically are added to the top portion of a Security policy.

# Block Access to Specific URLs

- Cannot add specific URLs to a policy rule
- To block specific URLs:
  1. Add specific URLs to a custom URL category.
  2. Add a custom URL category to a policy rule.

## Objects > Custom Objects > URL Category

Custom URL Category

Name: URLs-Block-Per-Company-Policy

Description: URLs that are blocked by company policy.

Type: URL List

Matches any of the following URLs, domains or host names

4 items

- ☐ SITES
- ☐ danger.org
- ☐ \*.danger.org
- ☐ malware.net
- ☐ \*.malware.net

## Policies > Security

	NAME	TAGS	TYPE	Source			Destination		APPLICATI...	SERVICE	URL CATEGORY	ACTION
				ZONE	ADDRESS	USER	ZONE	ADDRESS				
1	Block-Per-Company-Policy	Users_Net	universal	Users_Net	any	any	Internet	any	any	application-default	URLs-Block-Per-Company-Policy	Deny



# Multi-Category and Risk-Based URL Filtering

## Objects > Custom Objects > URL Category

Custom URL Category

Name: Marketing-Department

Description: Custom URL Filter for the Marketing Department

Type: Category Match

Matches all of the following categories

SEARCH

<input type="checkbox"/>	CATEGORIES
<input type="checkbox"/>	low-risk
<input type="checkbox"/>	medium-risk
<input type="checkbox"/>	high-risk
<input type="checkbox"/>	newly-registered-domain

+ Add - Delete

- PAN-DB URL filtering assigns websites to multiple categories.
- Categories indicate:
  - The site's risk
  - The site's content
  - The site's purpose or function
- The security-related risk categories demonstrate levels of suspicious activity.
- Websites registered for fewer than 32 days are assigned to *newly-registered-domain*.

## Control URL Access for Specific Users

- Enable User-ID on source zone.
- Add users or groups to policy rules controlling URL access.

	NAME	TAGS	TYPE	Source			Destination		APPLICATI...	SERVICE	URL CATEGORY	ACTION
				ZONE	ADDRESS	USER	ZONE	ADDRESS				
1	Allow-Pentesters	Users_Net	universal	Users_Net	any	Pentesters-Grp	Internet	any	any	application-default	Risky-URLs	Allow

- Enable logging on a policy rule:
  - Recommended if the URLs are risky.
  - Logging information also helps to improve or refine policy rules.

## Use a URL Filtering Profile

- Attach the URL Filtering Profile to a Security policy allow rule.

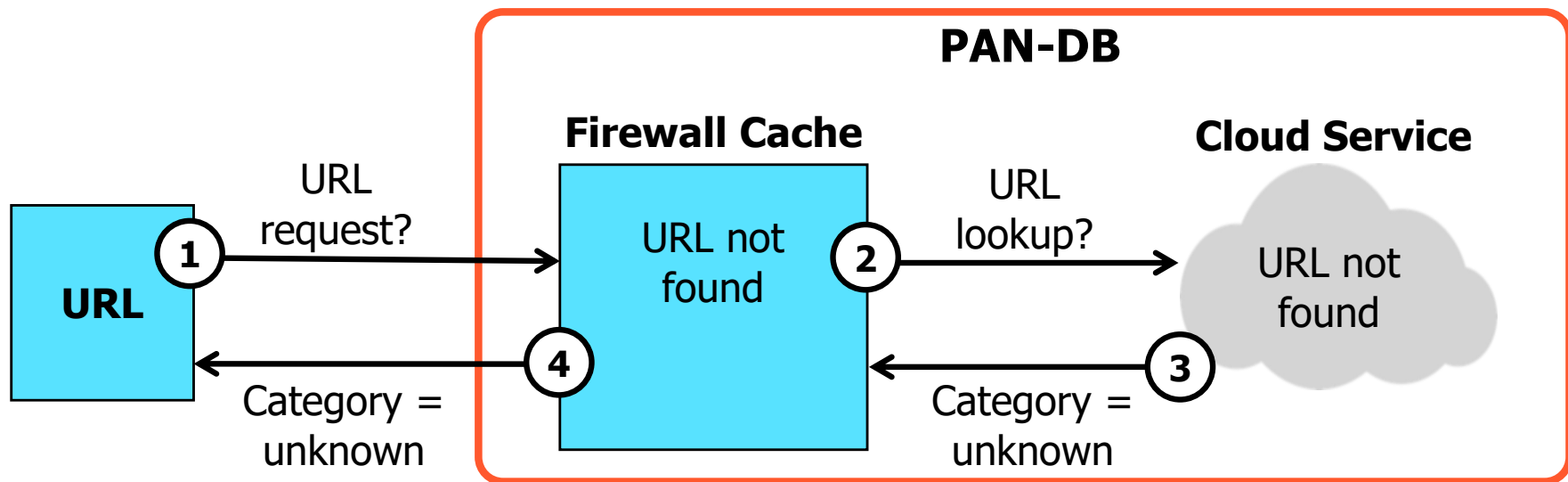
### Policies > Security

	NAME	TAGS	TYPE	Source			Destination		APPLICATI...	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
				ZONE	ADDRESS	US...	ZONE	ADDRESS						
1	<a href="#">Allow-Some-Web-Access</a>	Users_Net	universal	Users_Net	any	any	Internet	any	any	application-default	any	Allow		

- Profile can individually block, allow, or log access to URL categories:
  - Block: command-and-control, dynamic-dns, hacking, high-risk, malware, phishing, unknown.
  - Consider blocking: adult, extremism, new-registered-domain, parked, proxy-avoidance-and-anonymizers, questionable.
- Enable logging for better visibility in logs and reports.

## When Encountering Unknown URLs

Category column in URL Filtering log lists *unknown*.



Recommendation: Set unknown URL category action to support your security requirements.

# Real-Time Webpage Analysis

## Objects > Security Profiles > URL Filtering

URL Filtering Profile

Name: Corp-URL-Profile

Description: Company URL filtering profile for real-time web page analysis

Categories: URL Filtering Settings | User Credential Detection | HTTP Header Insertion | **Inline ML**

Available Models

MODEL	DESCRIPTION	ACTION
Phishing Detection	Machine Learning engine to dynamically identify credential phishing pages	block
Javascript Exploit Detection	Machine Learning engine to dynamically detect Javascript based exploitation attacks	block

Exceptions

☐ CUSTOM URL CATEGORY/EDL

+ Add - Delete

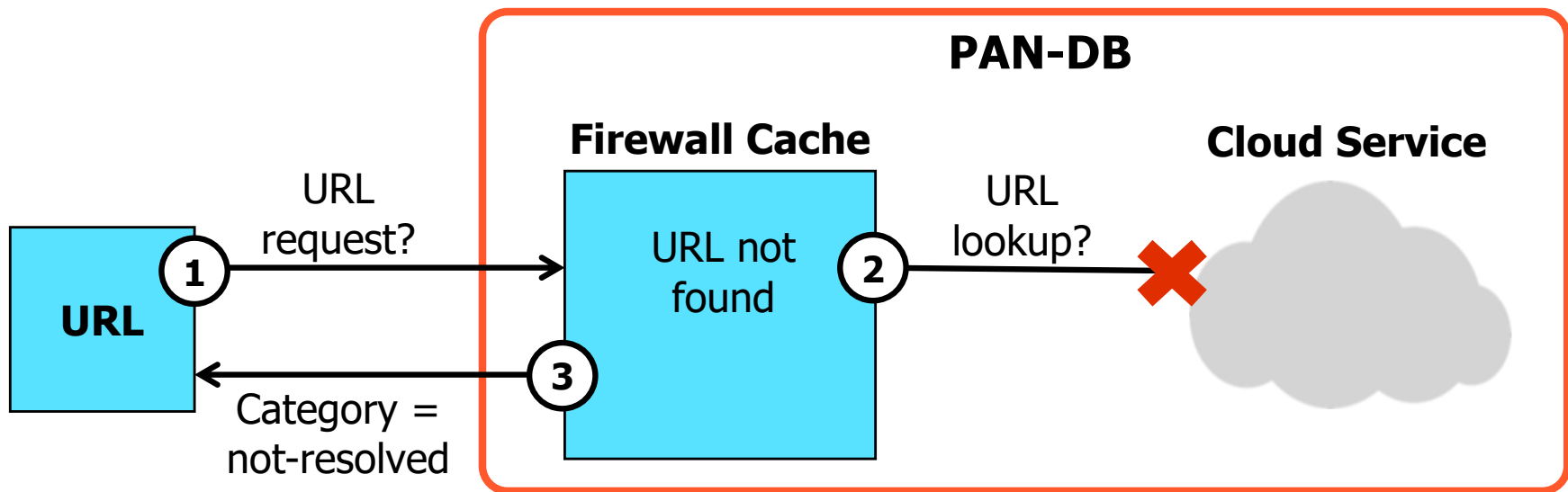
Classification engines for each type of malicious web content to apply to a policy.

Define policy action for each classification engine.

(Optionally) Add URL exceptions to exclude specific URLs.

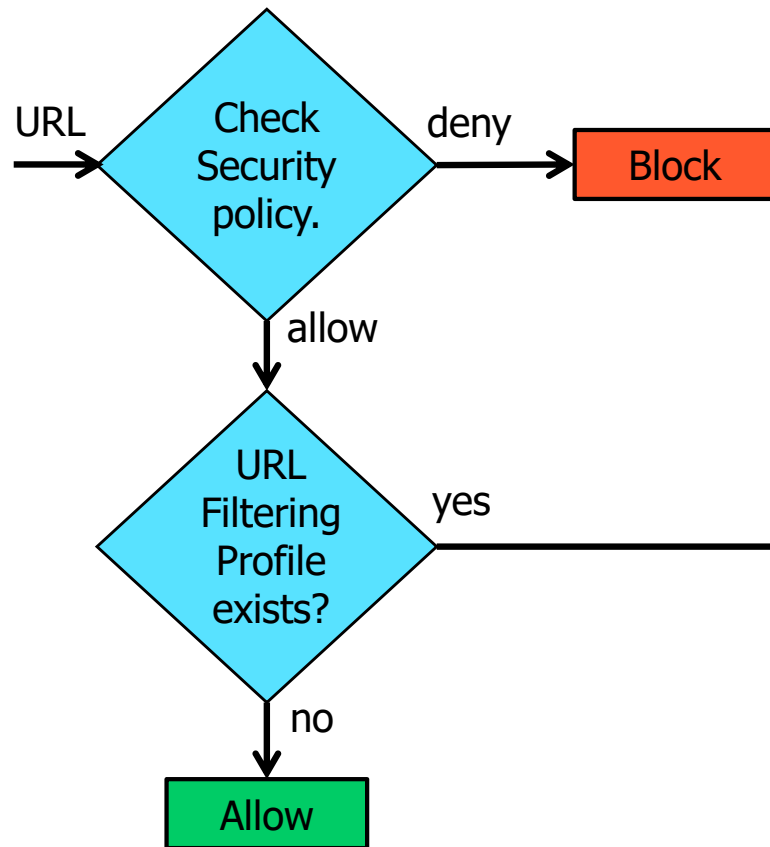
## When Encountering Not-Resolved URLs

Category column in URL Filtering log lists *not-resolved*.

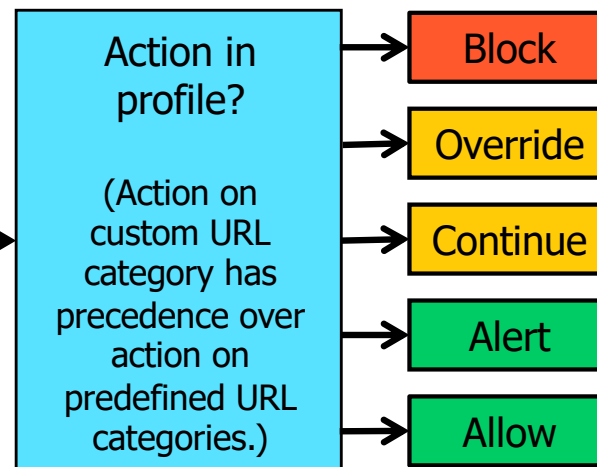


Recommendation: Set *not-resolved* URL category match action to "alert."

## URL Filtering Action Precedence



Knowledge of the URL filtering processing precedence helps you when you create or interpret a firewall configuration.



# URL Filtering Precedence Example

Allow **Pentesters-Grp** to access all **hacking** category URLs except **www.hackers9.com**.

## Policies > Security

	NAME	TAGS	TYPE	Source			Destination		APPLICATI...	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
				ZONE	ADDRESS	USER	ZONE	ADDRESS						
1	Allow-Pentesters	Users_Ne...	universal	Users_Net	any	Pentesters-Grp	Internet	any	any	application-default	any	Allow		

Outbound-URL-Filt  
profile

1

## Objects > Custom Objects > URL Category

Custom URL Category

Name: Denied-Hacking-URLs

Description: URL Category to Block Hacking URLs

Type: URL List

Matches any of the following URLs, domains or host names

1 item

SITES

www.hackers9.com

URL Filtering Profile

Name: Outbound-URL-Filt

Description: URL Filter for Outbound Traffic

Categories | URL Filtering Settings | User Credential Detection | HTTP Header Insertion | Inline ML

CATEGORY

Custom URL Categories

Denied-Hacking-URLs \*

Pre-defined Categories

hacking

Action taken

2 block

3 continue



# Configure Other Malicious URL Lists

Objects > External Dynamic Lists > Add

External Dynamic Lists

Name: Malicious\_URL\_Feeds

Create List | List Entries And Exceptions

Type: URL List

Description:

Source: http://mywebserver.mycompany.com/url.txt

Server Authentication

Certificate Profile: None

Check for updates: Five Minute

Five Minute  
Hourly  
Daily  
Weekly  
Monthly

- Malicious URL lists are available from third parties.
- Lists can be used in firewall policy rules and URL Filtering Profiles.
- Lists are accessed as EDLs.
- EDL must be of type **URL List**.

Block access to or from known-bad IP addresses

Block access to or from known-bad domains

Block access to or from known-bad URLs



**Other URL filtering features**



# 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 company policy. Please contact your system administrator if you believe this is in error.

**User:** 192.168.41.20

**URL:** www.handdrawngames.com/desktopd/game.asp

**Category:** games

If you feel this page has been incorrectly blocked, you may click Continue to proceed to the page you were trying to visit. You will be logged out.

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:

[Return to previous page](#)

# URL Admin Settings

**Device > Setup > Content-ID > URL Admin Override > Add**

URL Admin Override ?

Password

Confirm Password

SSL/TLS Service Profile

Mode ☐ Transparent ☒ Redirect

Address

- Configure URL Admin Override password.


**Device > Setup > Content-ID > URL Filtering**

URL Filtering ?

URL Continue Timeout (min)

URL Admin Override Timeout (min)

URL Admin Lockout Timeout (min)

 ☐ Hold client request for category lookup

Category lookup timeout (sec)

PAN-DB Server

Cloud list separated by commas

- Configure URL Admin Override password timeout period.

# HTTP Header Insertion and Modification

- Limit access to only enterprise versions of SaaS applications.
- Four predefined SaaS applications:
  - Dropbox
  - Google
  - Office 365
  - YouTube
- Inserts HTTP header if missing or overwrites existing header.
- **Dynamic Fields** inserts *X-Authenticated-User* header to specify user's name and domain to secondary devices:
  - To enforce additional user-based policy controls

Objects > Security Profiles > URL Filtering > Add

HTTP Header Insertion

Name: Outbound-GoogleURL-HTTP-Header

Type: Google Apps Access Control

Domains: DOMAINS

- \*.google.com
- gmail.com

For traffic to google.com or gmail.com, add the header and user's domain name.

Custom

- Dropbox Network Control
- Dynamic Fields
- Google Apps Access Control
- Microsoft Office365 Tenant Restrictions
- Youtube Safe Search

HEADER	VALUE	LOG
X-GooGApps-Allowed-Domains		<input type="checkbox"/>

+ Add - Delete

# Configure Safe Search and Logging Options

**Objects > Security Profiles > URL Filtering > Add**

URL Filtering Profile

Name

Outbound-URL-Filt

Description

URL Filter for Outbound Traffic

Categories

URL Filtering Settings

User Credential Detection

HTTP Header Insertion

Inline ML

☒ Log container page only

☒ Safe Search Enforcement

HTTP Header Logging

☐ User-Agent




☐ Referer

☐ X-Forwarded-For

Has dedicated block page. See **Device > Response Pages.**

# Recategorization Request: Via Log Entries

## Monitor > Logs > URL Filtering

	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL
	07/17 19:45:27	News-Sites	News-Sites,news,low-risk	a57.foxnews.com/
	07/17 19:45:27	News-Sites	News-Sites,news,low-risk	static.foxnews.com/
	07/17 19:45:27			

### Details

Severity informational

Repeat Count 1

URL static.foxnews.com/

[Request Categorization Change](#)

HTTP Method

### Request Categorization Change

URL

Log Category

Current Category

Categorization on the server has been updated since this log entry was generated

Suggested Category [get descriptions](#)

Email

Confirm Email

Comments

The following characters are not supported: ";' & \.

# Recategorization Requests: Via Webpage

Objects > Security Profiles > URL Filtering > Add

Custom URL Categories

☐

Denied-Hacking-URLs \*

☐

Risky-URLs \*

☐

URLs-Block-Per-Company-Policy \*

Pre-defined Categories

☐

abortion

☐

abused-drugs

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

[Check URL Category](#)

## Test A Site

URL

Which URL would you like to query once more?

SEARCH

URL: www.raptitude.com

Category: Personal Sites and Blogs

Description: Personal websites and blogs by individuals or groups.

Example Sites: www.blogspot.com, www.wordpress.com, www.greatamericanphotocontest.com

Category: Low Risk

Description: Sites that are not medium or high risk are considered low risk. These sites have displayed benign activity for a minimum of 90 days. The low risk category includes both sites that have a history of only benign activity, and sites found to be malicious in the past, but that have displayed benign activity for at least 90 days.

Example Sites: www.google.com, www.schwab.com, www.amazon.com

[Request Change](#)





## Module Summary

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

- Configure the firewall to block traffic from known-malicious IP addresses
- Configure the firewall to block traffic from known-malicious domains
- Configure the firewall to block traffic from known-malicious URLs
- Describe other URL filtering operations and options



# Questions



## Lab 9: Blocking Threats from Known-Bad Sources

- Test Access to Known Malicious IP Addresses
- Block Access to Malicious IP Addresses Using Address Objects and Groups
- Block Access to Malicious IP Addresses by Geographic Region
- Block Access to Malicious IP Addresses Using an EDL
- Test Access to Malicious Domains
- Block Access to Malicious Domains Using an EDL in an Anti-Spyware Profile
- Add the Anti-Spyware Profile to a Security Policy Rule
- Block Access to Malicious URLs Using the Security Policy
- Create a Custom URL Category
- Use a Custom URL Category to Block Access to Malicious URLs
- Block Access to a Malicious URL Using a URL Filtering Profile



**Protecting our  
digital way  
of life.**