URL FILTERING

MAKE THE WEB SAFE AGAIN

- URL Filtering Security Profiles
- Attaching URL Filtering Profiles

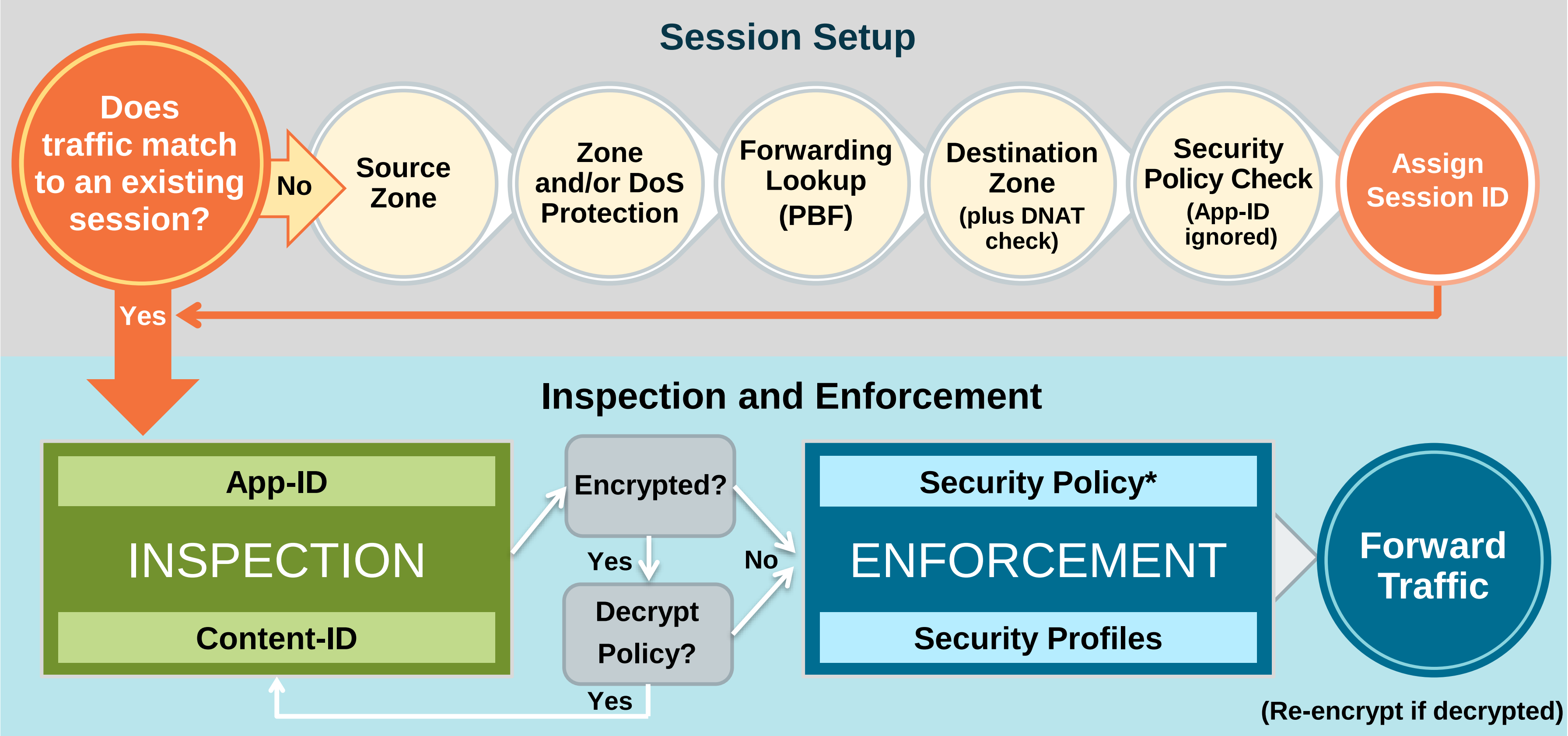
EDU-210 Version A
PAN-OS® 9.0

Agenda

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

- Describe how the firewall uses the PAN-DB database to filter user access to websites
- Configure a custom URL Filtering Profile to minimize the number of blocked websites between trusted zones
- Configure safe search and logging options
- Configure access to only enterprise versions of SaaS applications

Flow Logic of the Next-Generation Firewall



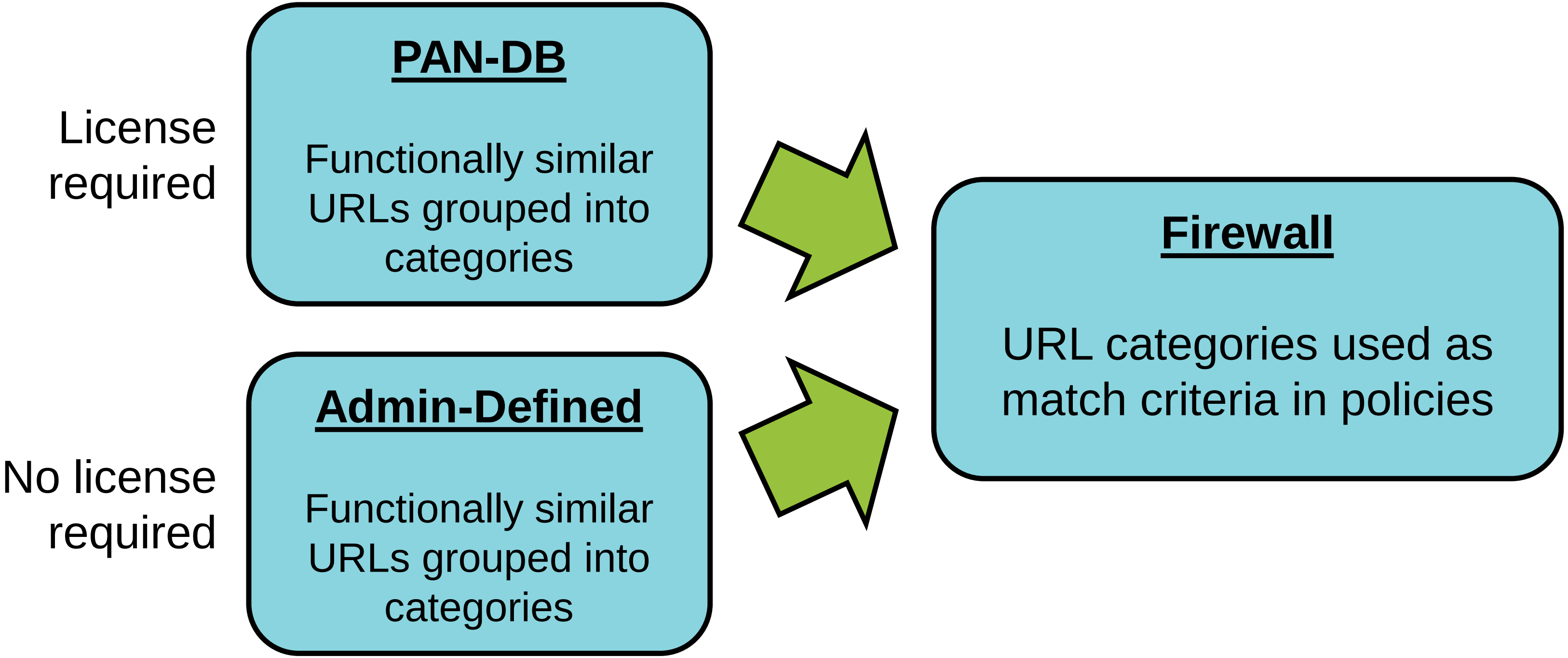
Session Setup
Does traffic match to an existing session?
No
Source Zone
Zone and/or DoS Protection
Forwarding Lookup (PBF)
Destination Zone (plus DNAT check)
Security Policy Check (App-ID ignored)
Assign Session ID
Yes
Inspection and Enforcement
App-ID
INSPECTION
Content-ID
Encrypted?
Yes
No
Decrypt Policy?
Yes
Security Policy*
ENFORCEMENT
Security Profiles
Forward Traffic
(Re-encrypt if decrypted)

* Policy check relies on pre-NAT IP addresses

URL Filtering Security Profiles

Attaching URL Filtering Profiles

URL Filtering Feature



License required

PAN-DB

Functionally similar URLs grouped into categories

No license required

Admin-Defined

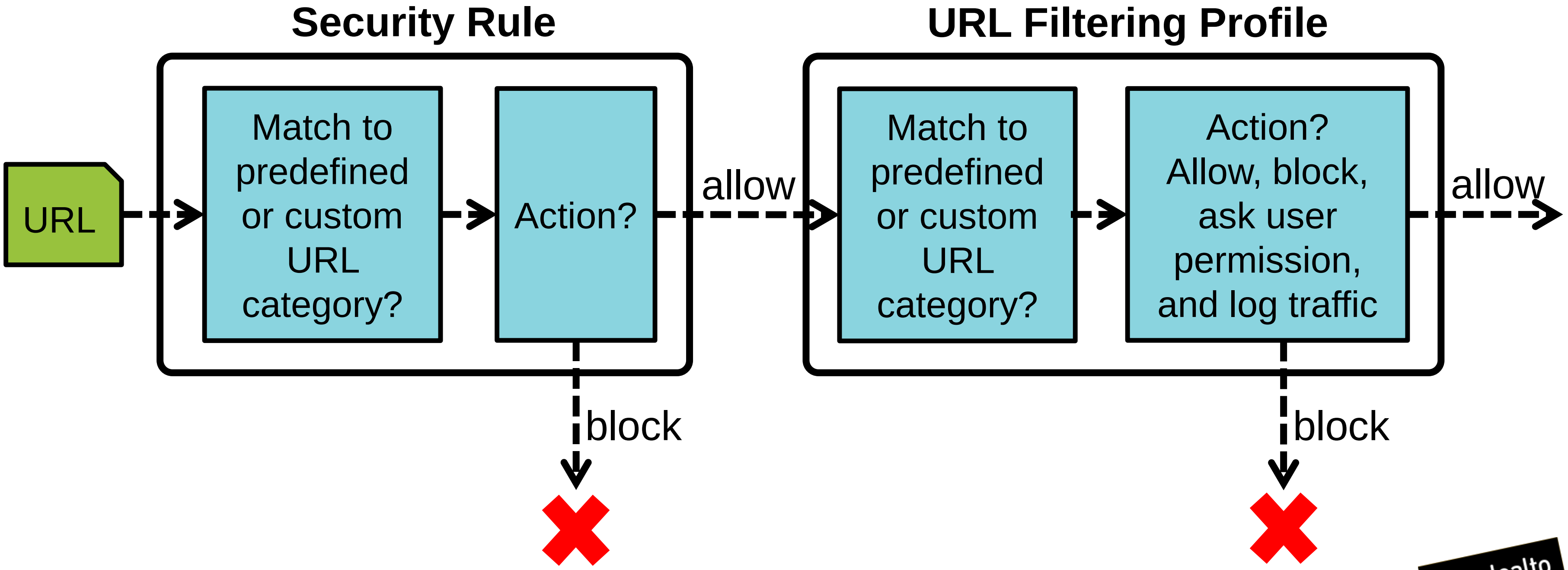
Functionally similar URLs grouped into categories

Firewall

URL categories used as match criteria in policies

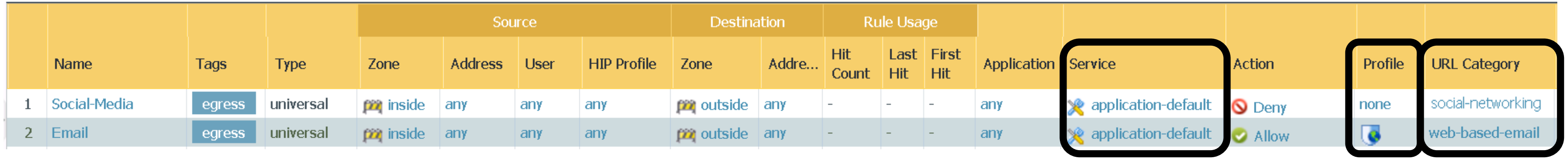
URL Filtering Profiles

- URL Filtering Profiles implement additional security checks on allowed traffic.


Security Rule
URL Filtering Profile
URL
Match to predefined or custom URL category?
Action?
allow
block
Match to predefined or custom URL category?
Action? Allow, block, ask user permission, and log traffic
allow
block

URL Category: Policy Versus Profile

Policies > Security



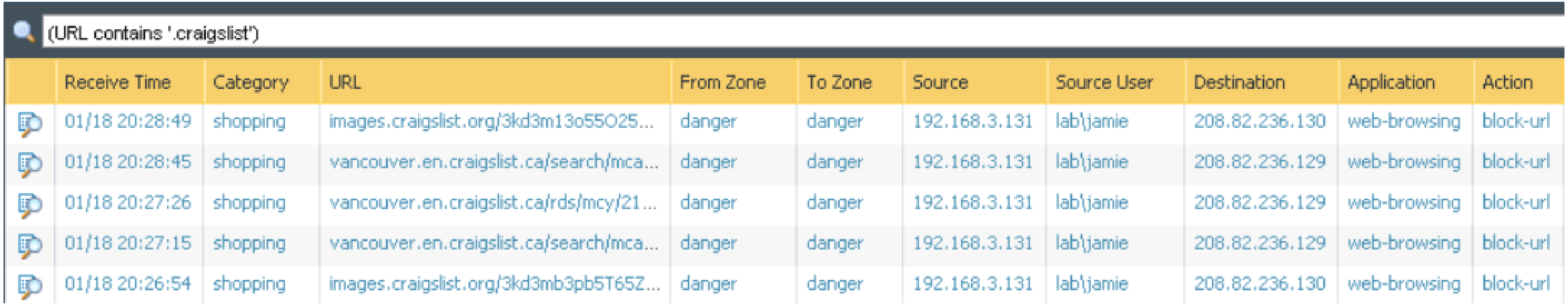
				Source				Destination		Rule Usage							
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Addre...	Hit Count	Last Hit	First Hit	Application	Service	Action	Profile	URL Category
1	Social-Media	egress	universal	inside	any	any	any	outside	any	-	-	-	any	application-default	Deny	none	social-networking
2	Email	egress	universal	inside	any	any	any	outside	any	-	-	-	any	application-default	Allow		web-based-email

URL Category in a Policy	URL Filtering Security Profile
Used as a match condition	Applied to traffic allowed by Security policy
URLs matched to predefined or custom URL categories	URLs matched to “block” or “allow” lists and predefined or custom URL categories
Action determined in the policy rule	Action more granularly configured for individual URLs or URL categories
URL category name logged in the URL Filtering log	URL details logged in the URL Filtering log

URL Filtering Log

- Attachment of a URL Filtering Profile to a Security rule generates log entries:
  - “alert,” “block,” “continue,” and “override” actions trigger log entries.

Monitor > Logs > URL Filtering

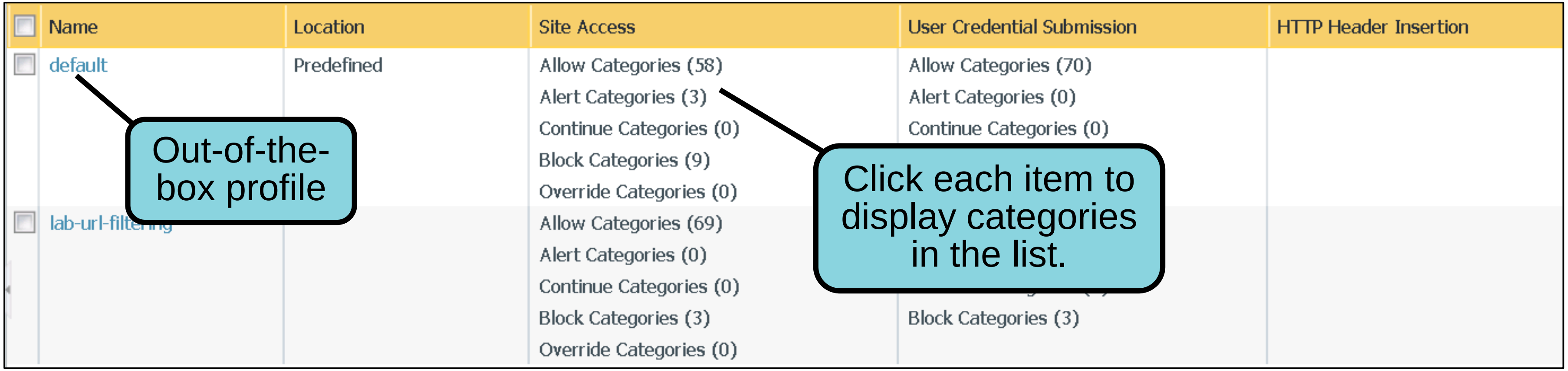


(URL contains '.craigslist')

	Receive Time	Category	URL	From Zone	To Zone	Source	Source User	Destination	Application	Action
	01/18 20:28:49	shopping	images.craigslist.org/3kd3m13o55O25...	danger	danger	192.168.3.131	lab\jamie	208.82.236.130	web-browsing	block-url
	01/18 20:28:45	shopping	vancouver.en.craigslist.ca/search/mca...	danger	danger	192.168.3.131	lab\jamie	208.82.236.129	web-browsing	block-url
	01/18 20:27:26	shopping	vancouver.en.craigslist.ca/rds/mcy/21...	danger	danger	192.168.3.131	lab\jamie	208.82.236.129	web-browsing	block-url
	01/18 20:27:15	shopping	vancouver.en.craigslist.ca/search/mca...	danger	danger	192.168.3.131	lab\jamie	208.82.236.129	web-browsing	block-url
	01/18 20:26:54	shopping	images.craigslist.org/3kd3mb3pb5T65Z...	danger	danger	192.168.3.131	lab\jamie	208.82.236.130	web-browsing	block-url

URL Filtering Security Profile

Objects > Security Profiles > URL Filtering



□	Name	Location	Site Access	User Credential Submission	HTTP Header Insertion
□	default	Predefined	Allow Categories (58) Alert Categories (3) Continue Categories (0) Block Categories (9) Override Categories (0)	Allow Categories (70) Alert Categories (0) Continue Categories (0)	
□	lab-url-filtering		Allow Categories (69) Alert Categories (0) Continue Categories (0) Block Categories (3) Override Categories (0)	Block Categories (3)	

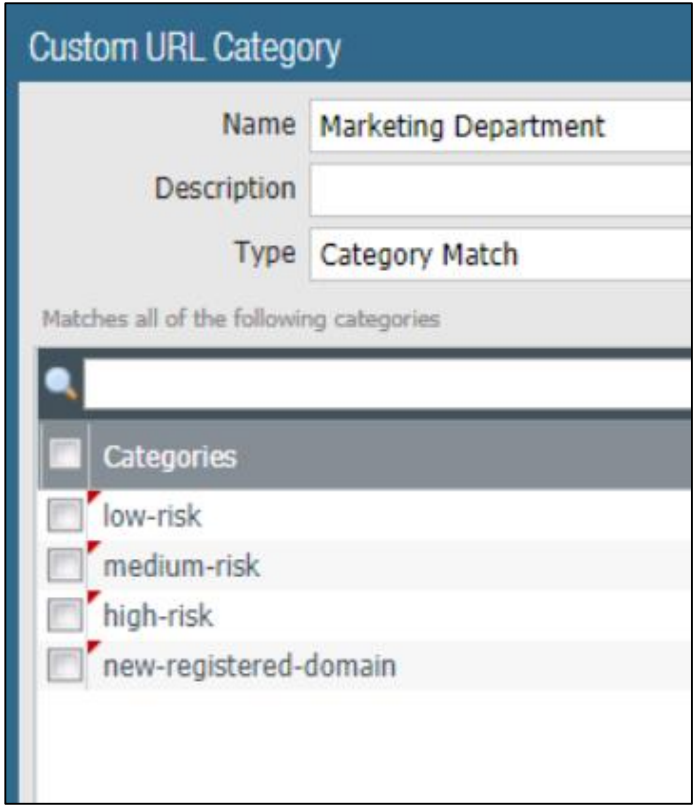
Out-of-the-box profile

Click each item to display categories in the list.

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

Multi-Category and Risk-Based URL Filtering

Device > Setup > Content-ID > URL Filtering



Custom URL Category

Name: Marketing Department

Description:

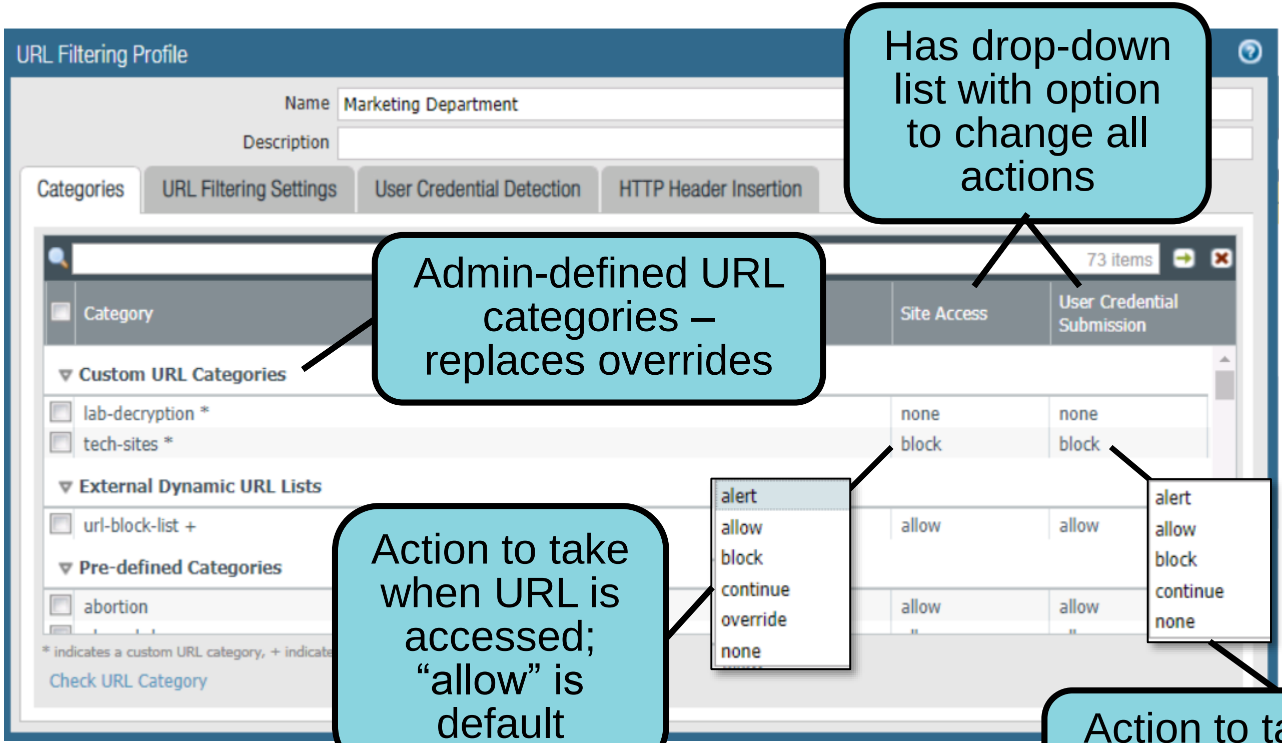
Type: Category Match

Matches all of the following categories

□	Categories
□	low-risk
□	medium-risk
□	high-risk
□	new-registered-domain

- PAN-DB URL Filtering cloud assigns websites to multiple categories.
- Categories indicate how risky the site is, the website’s content, and the website’s purpose or function.
- The security-related risk categories demonstrate levels of suspicious activity.
- Websites that have been registered for fewer than 32 days are considered new-registered-domains.

Configure Per-URL Category Actions



URL Filtering Profile

Name: Marketing Department

Description:

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

73 items

□ Category	Site Access	User Credential Submission
▽ Custom URL Categories		
□ lab-decryption *	none	none
□ tech-sites *	block	block
▽ External Dynamic URL Lists		
□ url-block-list +	allow	allow
▽ Pre-defined Categories		
□ abortion	allow	allow

* indicates a custom URL category, + indicate

Check URL Category

Has drop-down list with option to change all actions

Admin-defined URL categories – replaces overrides

Action to take when URL is accessed; “allow” is default

Action to take if user submits credentials to allowed URL

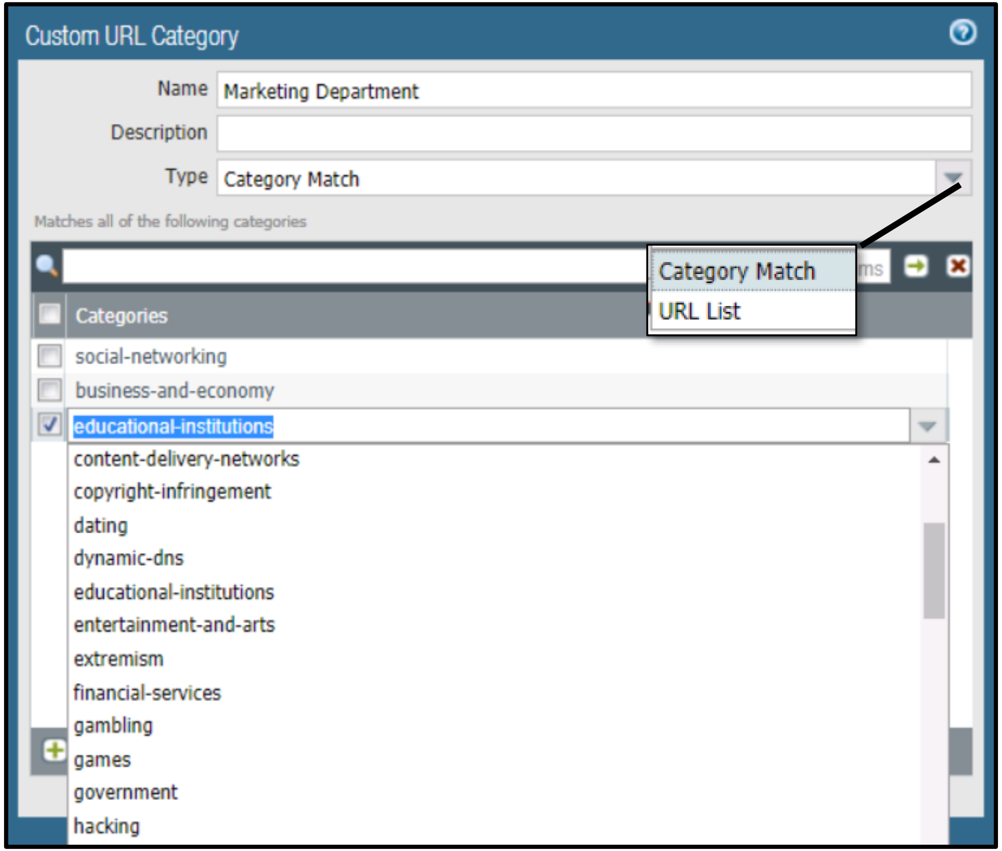
URL matching order:

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

Configure a Custom URL Category

Objects > Custom Objects > URL Category > Add



Custom URL Category

Name: Marketing Department

Description:

Type: Category Match

- Category Match
- URL List

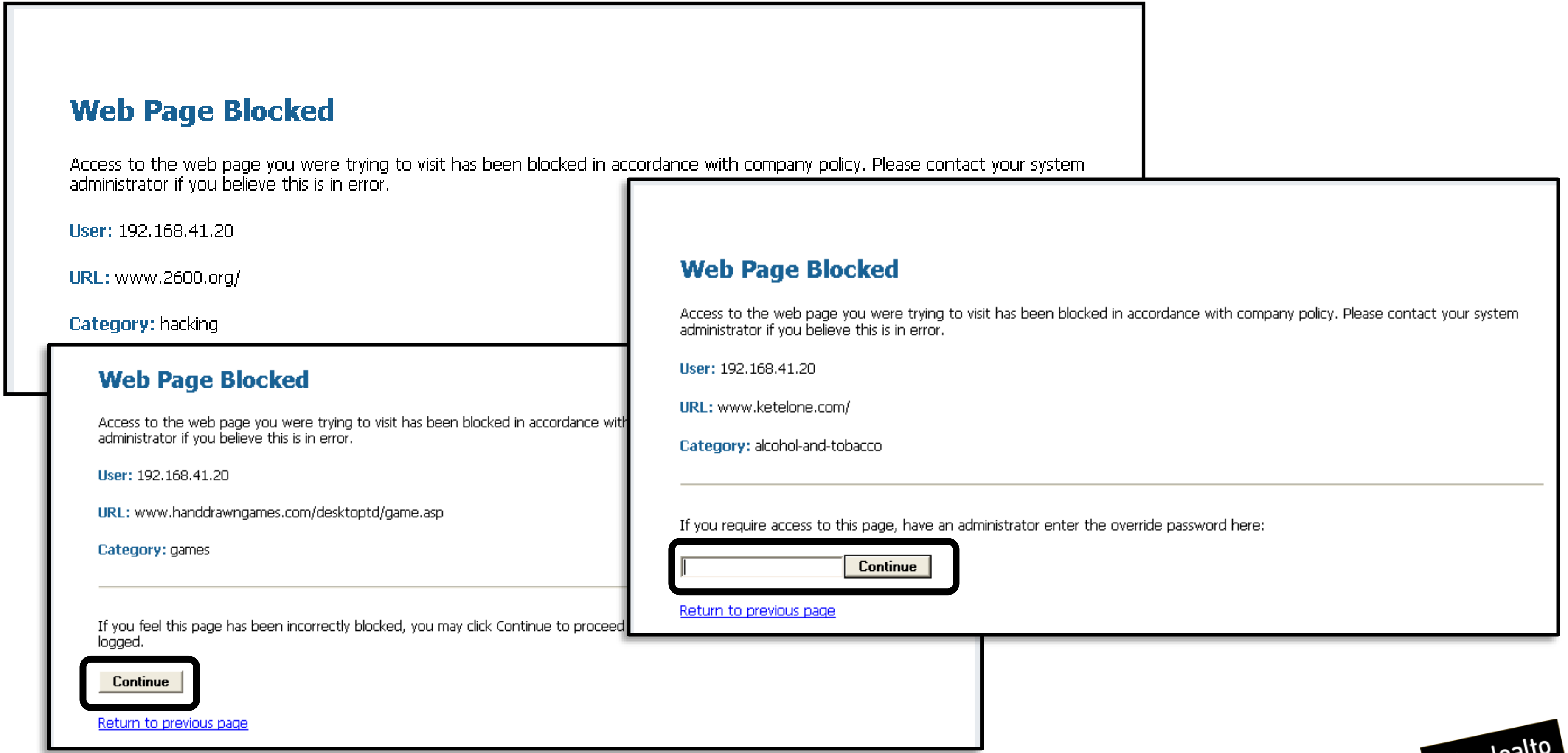
Matches all of the following categories

	Categories
□	social-networking
□	business-and-economy
☑	educational-institutions

- content-delivery-networks
- copyright-infringement
- dating
- dynamic-dns
- educational-institutions
- entertainment-and-arts
- extremism
- financial-services
- gambling
- games
- government
- hacking

- Define URL categories enforcement separate from category defaults
- Create URL filtering based on URL or category
- Replaces URL filtering overrides

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.handdrawngames.com/desktoptd/game.asp

Category: games

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

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

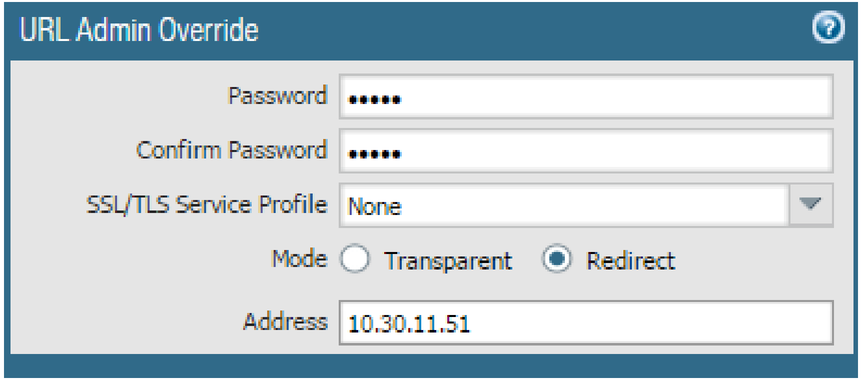
URL: www.ketelone.com/

Category: alcohol-and-tobacco

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

URL Admin Settings

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

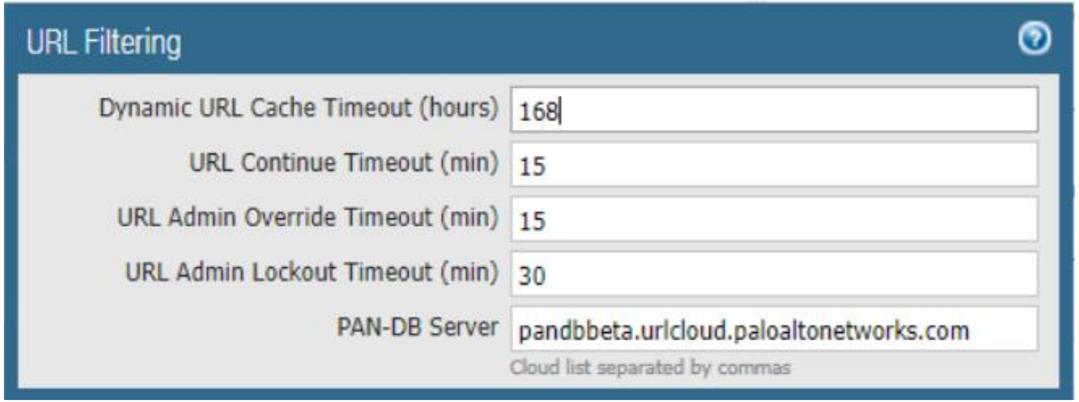


URL Admin Override

Password	•••••
Confirm Password	•••••
SSL/TLS Service Profile	None
Mode	○ Transparent ● Redirect
Address	10.30.11.51

Configure a URL Admin Override password that a user must enter to access a URL configured with an "override" action.

Device > Setup > Content-ID > URL Filtering

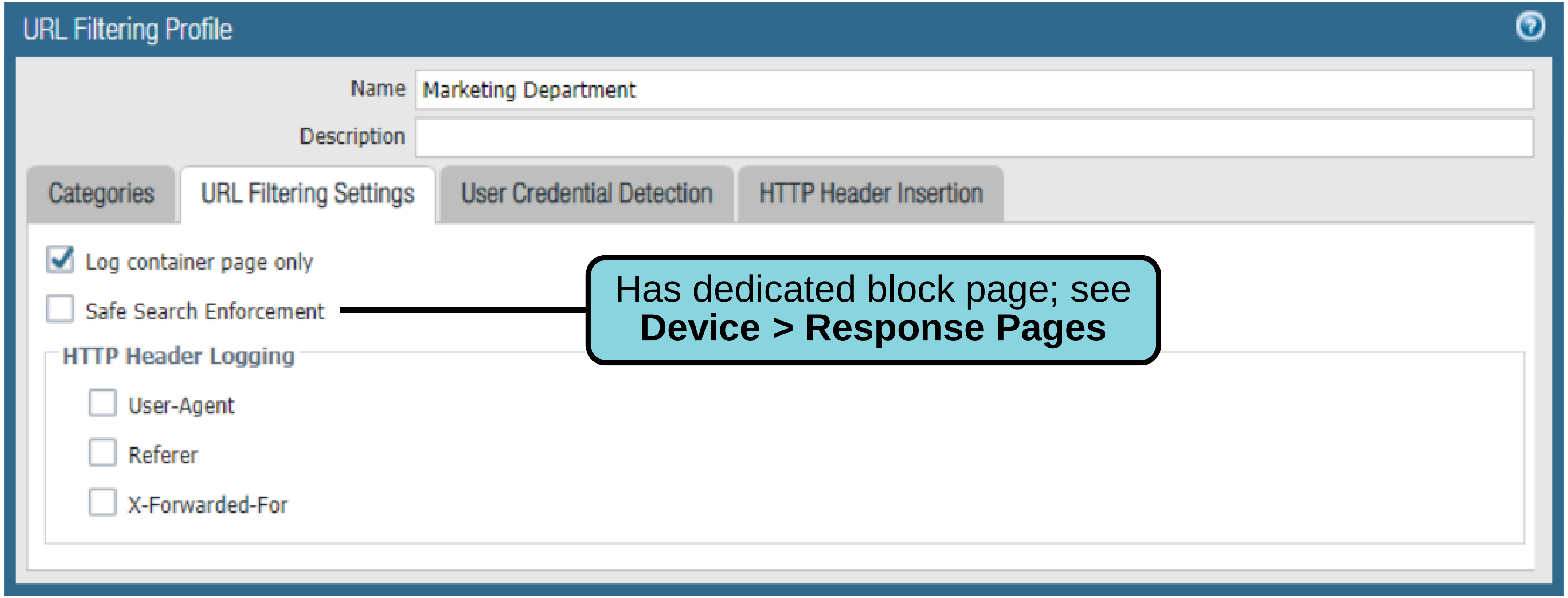


URL Filtering

Dynamic URL Cache Timeout (hours)	168
URL Continue Timeout (min)	15
URL Admin Override Timeout (min)	15
URL Admin Lockout Timeout (min)	30
PAN-DB Server	pandbbeta.urlcloud.paloaltonetworks.com Cloud list separated by commas

Configure Safe Search and Logging Options

Objects > Security Profiles > URL Filtering > Add



URL Filtering Profile

Name: Marketing Department

Description:

☑ Log container page only

□ Safe Search Enforcement

HTTP Header Logging

□ User-Agent

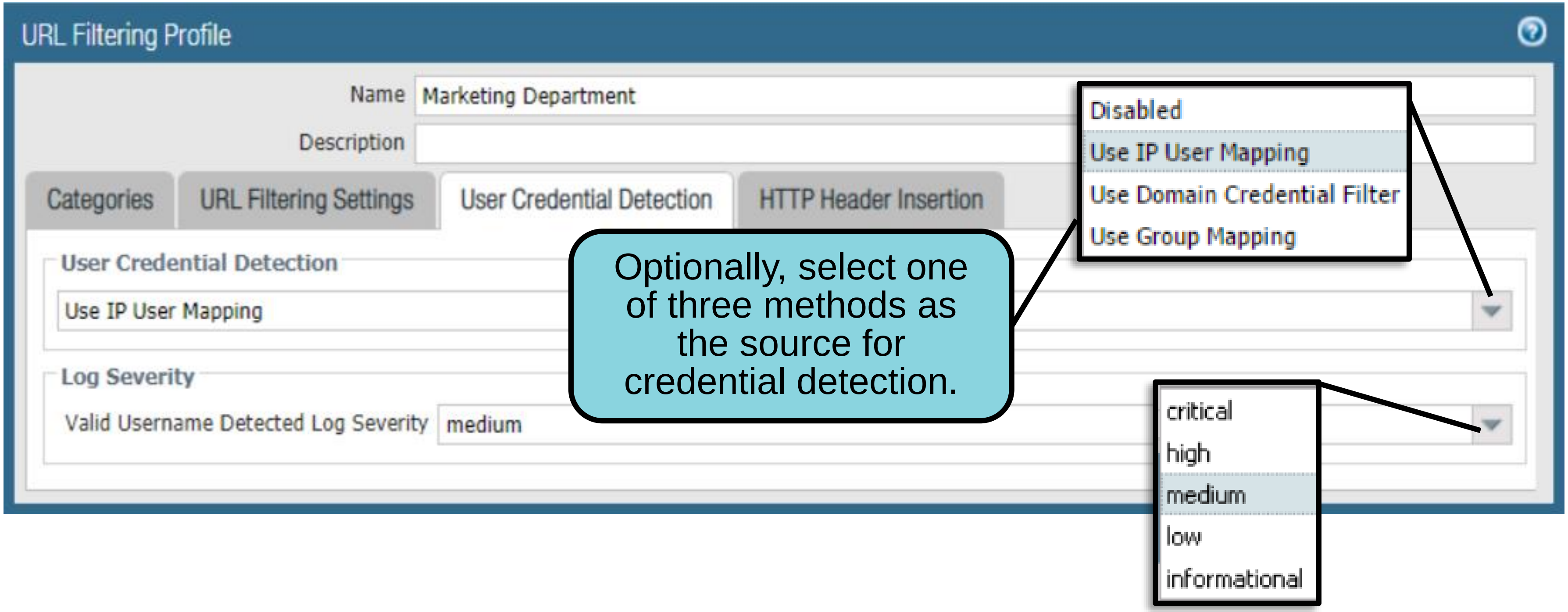
□ Referer

□ X-Forwarded-For

Has dedicated block page; see **Device > Response Pages**

Configure Credential Phishing Prevention Method

Objects > Security Profiles > URL Filtering > Add



URL Filtering Profile

Name: Marketing Department

Description:

User Credential Detection

Use IP User Mapping

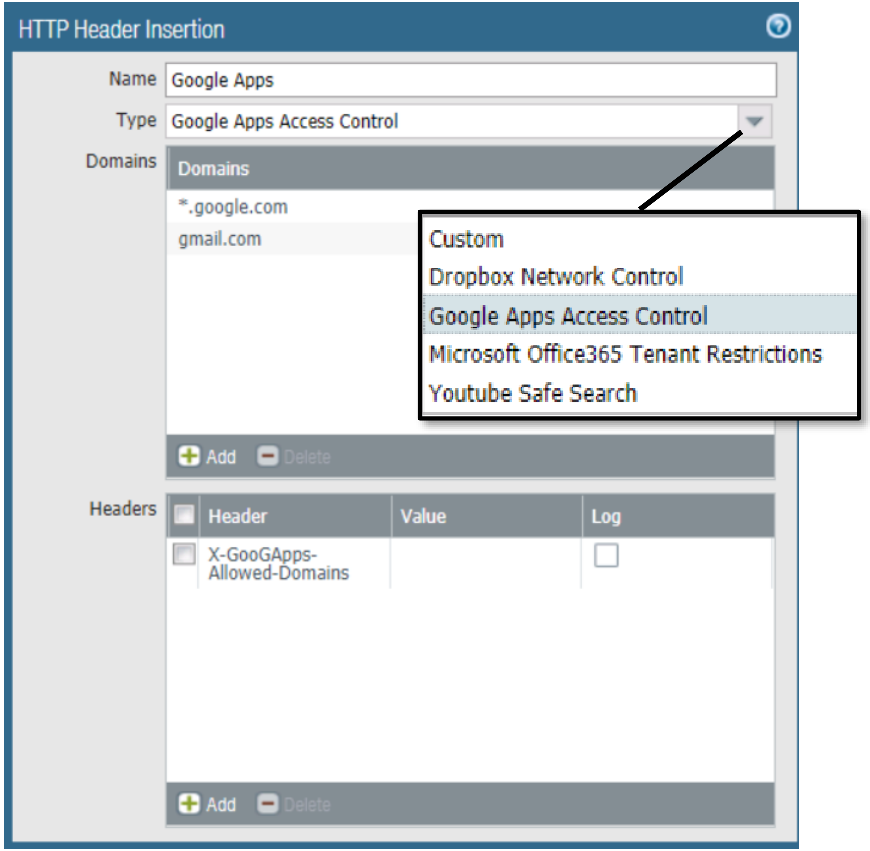
Log Severity

Valid Username Detected Log Severity: medium

Optionally, select one of three methods as the source for credential detection.

HTTP Header Insertion and Modification

- Enable access to only enterprise versions of SaaS applications
- Inserts header if missing or overwrites existing header
- Four predefined SaaS applications:
  - Dropbox
  - Google
  - Office 365
  - YouTube



HTTP Header Insertion

Name: Google Apps

Type: Google Apps Access Control

Domains:

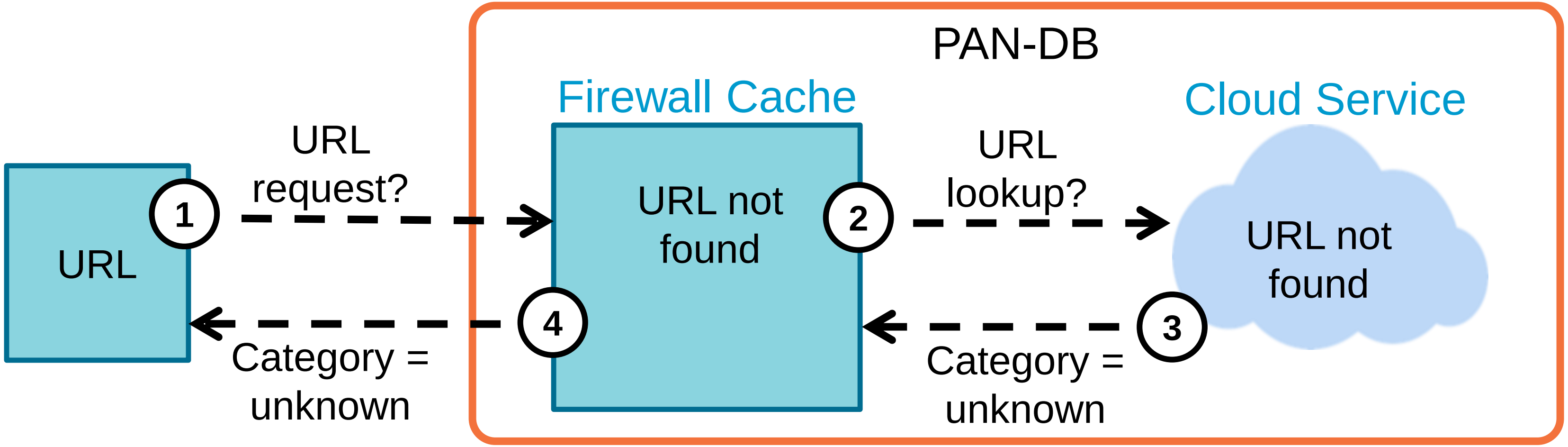
Domains
*.google.com
gmail.com

Headers:

☐	Header	Value	Log
☐	X-GooGApps-Allowed-Domains		☐

Handling Unknown URLs

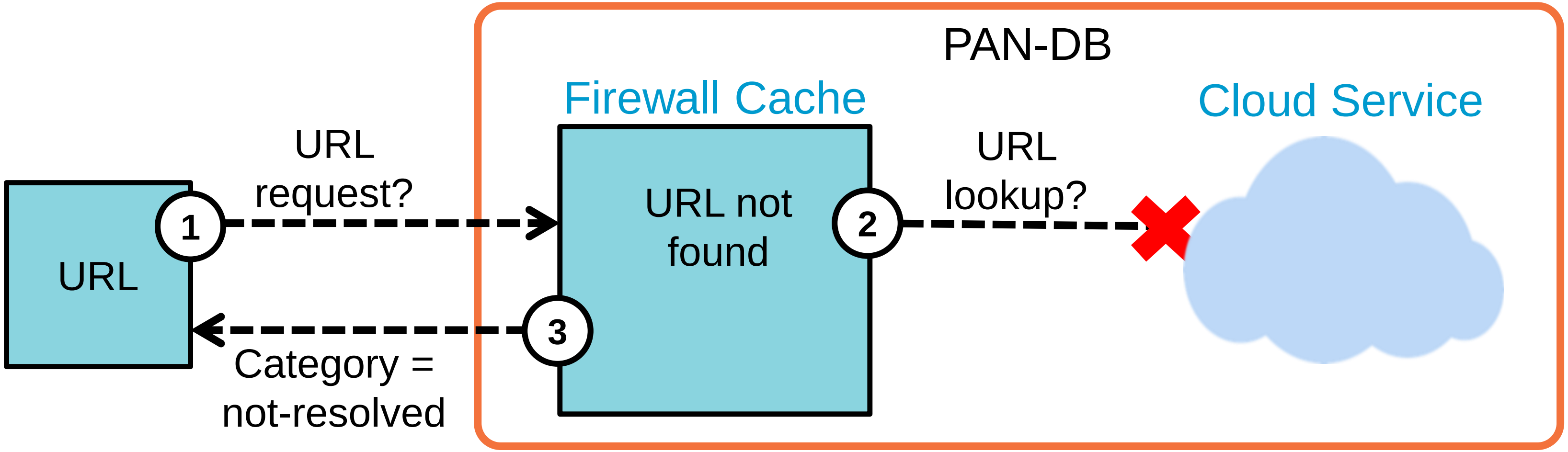
- Category column in URL Filtering log lists *unknown*.



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

Handling Not-Resolved URLs

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

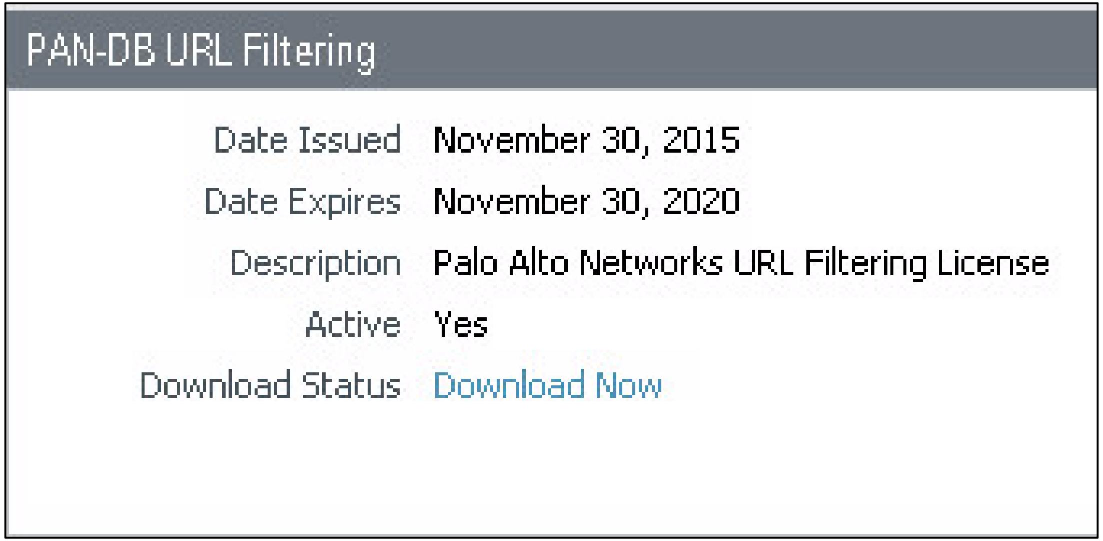


Recommendation: Set not-resolved URL category match action to “alert”

Downloading the URL Seed Database

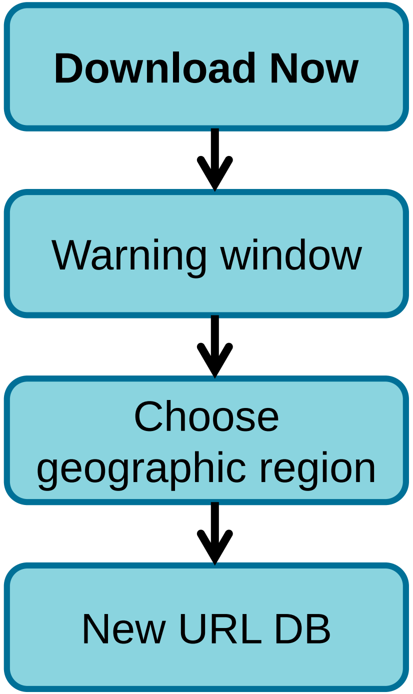
- Download an initial seed database to use the URL Filtering feature

Device > Licenses



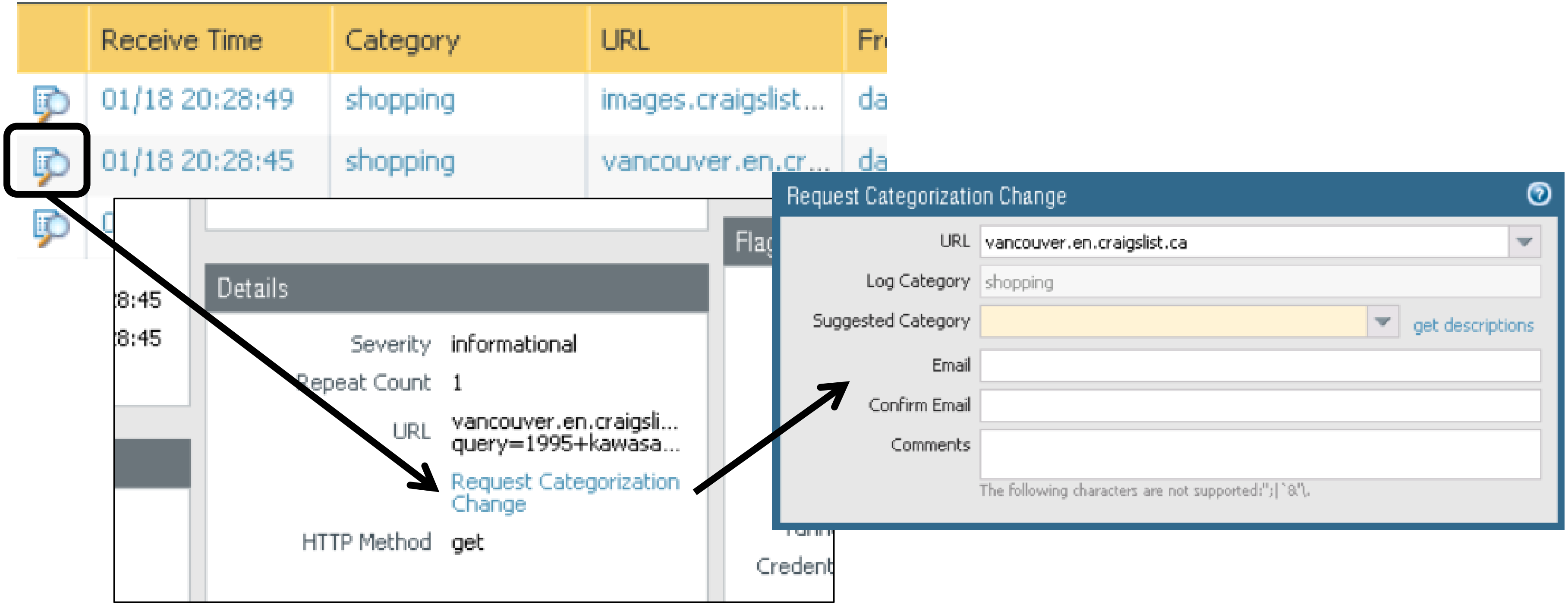
PAN-DB URL Filtering

Date Issued	November 30, 2015
Date Expires	November 30, 2020
Description	Palo Alto Networks URL Filtering License
Active	Yes
Download Status	Download Now



Recategorization Request: Via Log Entries

Monitor > Logs > URL Filtering



	Receive Time	Category	URL	Fr
	01/18 20:28:49	shopping	images.craigslist...	da
	01/18 20:28:45	shopping	vancouver.en.cr...	da
	0			

Details

Severity	informational
Repeat Count	1
URL	vancouver.en.craigsli... query=1995+kawasa...
	Request Categorization Change
HTTP Method	get

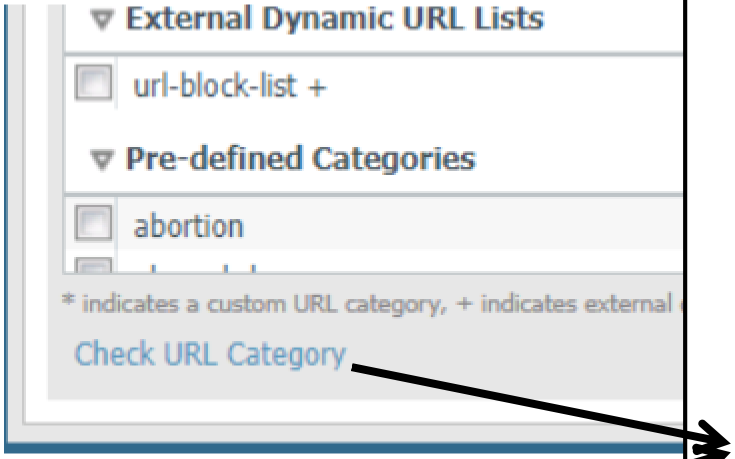
Request Categorization Change

URL	vancouver.en.craigslist.ca
Log Category	shopping
Suggested Category	get descriptions
Email	
Confirm Email	
Comments	

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

Recategorization Requests: Via Webpage

Objects > Security Profiles > URL Filtering > Add



▼ External Dynamic URL Lists

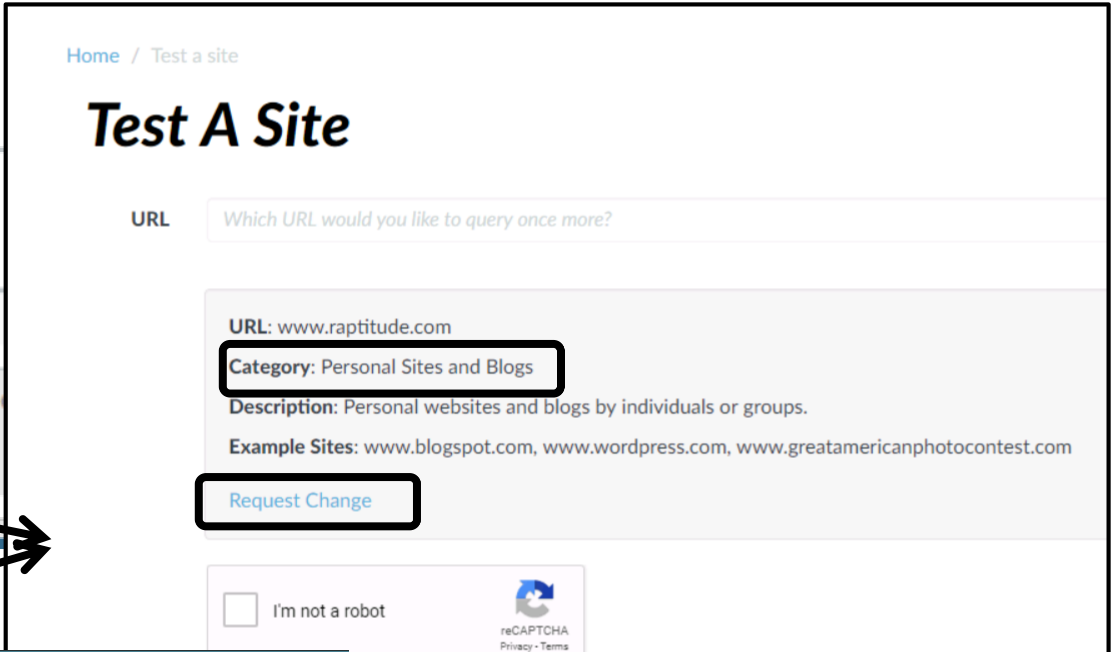
□ url-block-list +

▼ Pre-defined Categories

□ abortion

* indicates a custom URL category, + indicates external

Check URL Category



Home / Test a site

Test A Site

URL Which URL would you like to query once more?

URL: www.raptitude.com

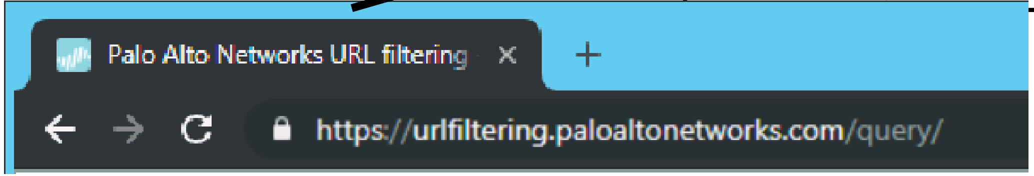
Category: Personal Sites and Blogs

Description: Personal websites and blogs by individuals or groups.

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

Request Change

□ I'm not a robot



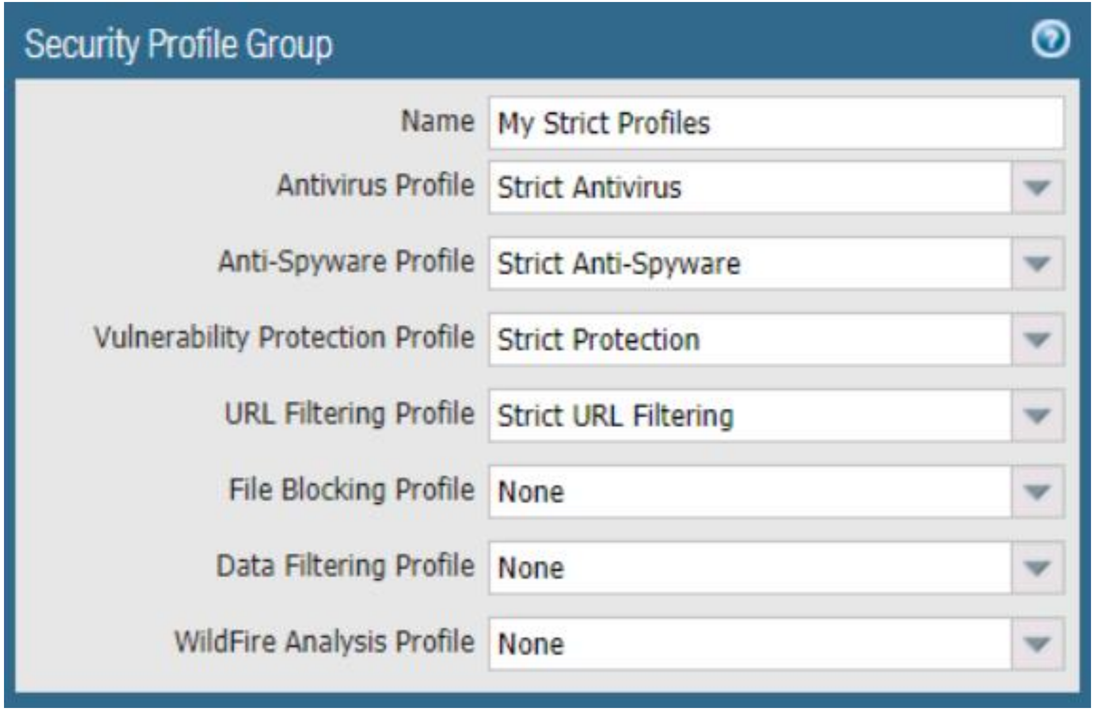
https://urlfiltering.paloaltonetworks.com/query/

URL Filtering Security Profiles

Attaching URL Filtering Profiles

Security Profile Groups

Objects > Security Profile Groups > Add



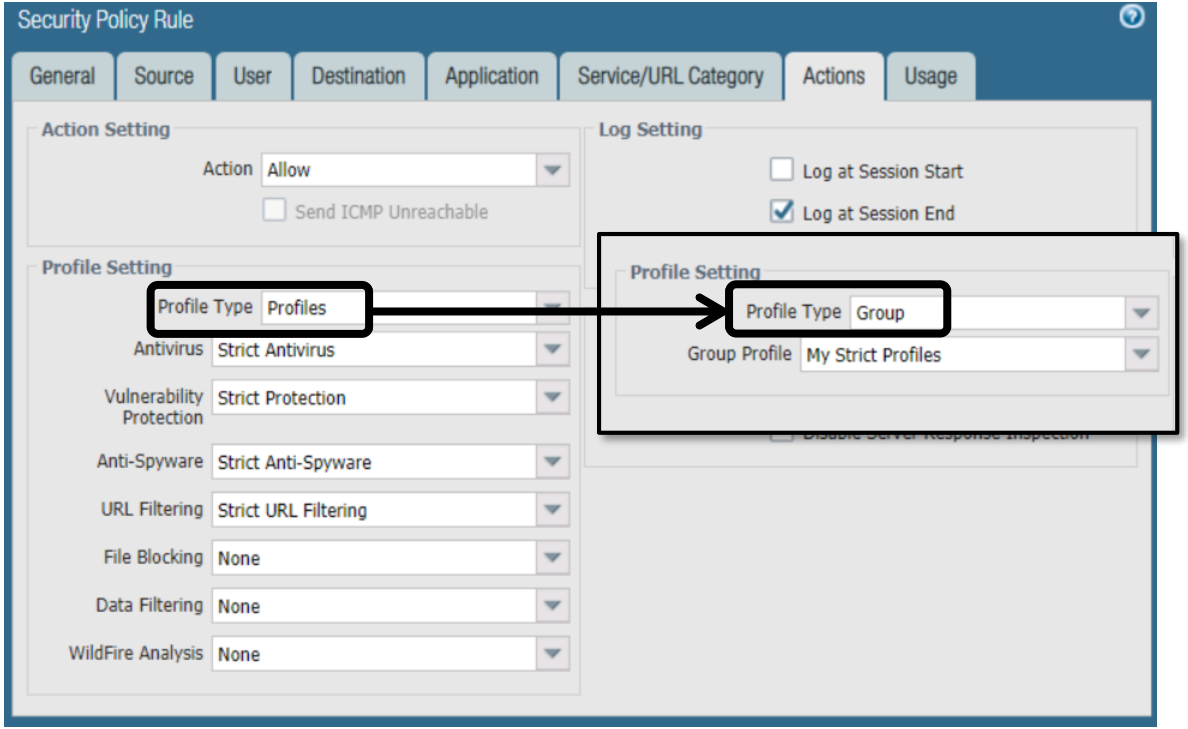
Security Profile Group

Name	My 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	None
Data Filtering Profile	None
WildFire Analysis Profile	None

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

Assigning Security Profiles to Security Rules

Policies > Security > Add



Security Policy Rule

Action Setting

Action: Allow

☐ Send ICMP Unreachable

Log Setting

☐ Log at Session Start

☑ Log at Session End

☐ Disable Server Response Inspection

Profile Setting

Profile Type: Profiles

Antivirus: Strict Antivirus

Vulnerability Protection: Strict Protection

Anti-Spyware: Strict Anti-Spyware

URL Filtering: Strict URL Filtering

File Blocking: None

Data Filtering: None

WildFire Analysis: None

Profile Setting

Profile Type: Group

Group Profile: My Strict Profiles

- Assign individual Security Profiles to a Security policy rule, or
- Assign a Security Profile Group to a Security policy rule

Module Summary

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

- Describe how the firewall uses the PAN-DB database to filter user access to websites
- Configure a custom URL Filtering Profile to minimize the number of blocked websites between trusted zones
- Configure safe search and logging options
- Configure access to only enterprise versions of SaaS applications

Questions?

URL Filtering Lab (Pages 129-142 in the Lab Guide)

- Load a firewall lab configuration
- Configure a custom URL category
- Configure an EDL
- Create and test a URL Filtering Profile

PROTECTION. DELIVERED.

paloalto NETWORKS®