URL FILTERING

EDU-210 Version A
PAN-OS® 9.0

MAKE THE WEB SAFE AGAIN

- URL Filtering Security Profiles
- Attaching URL Filtering Profiles

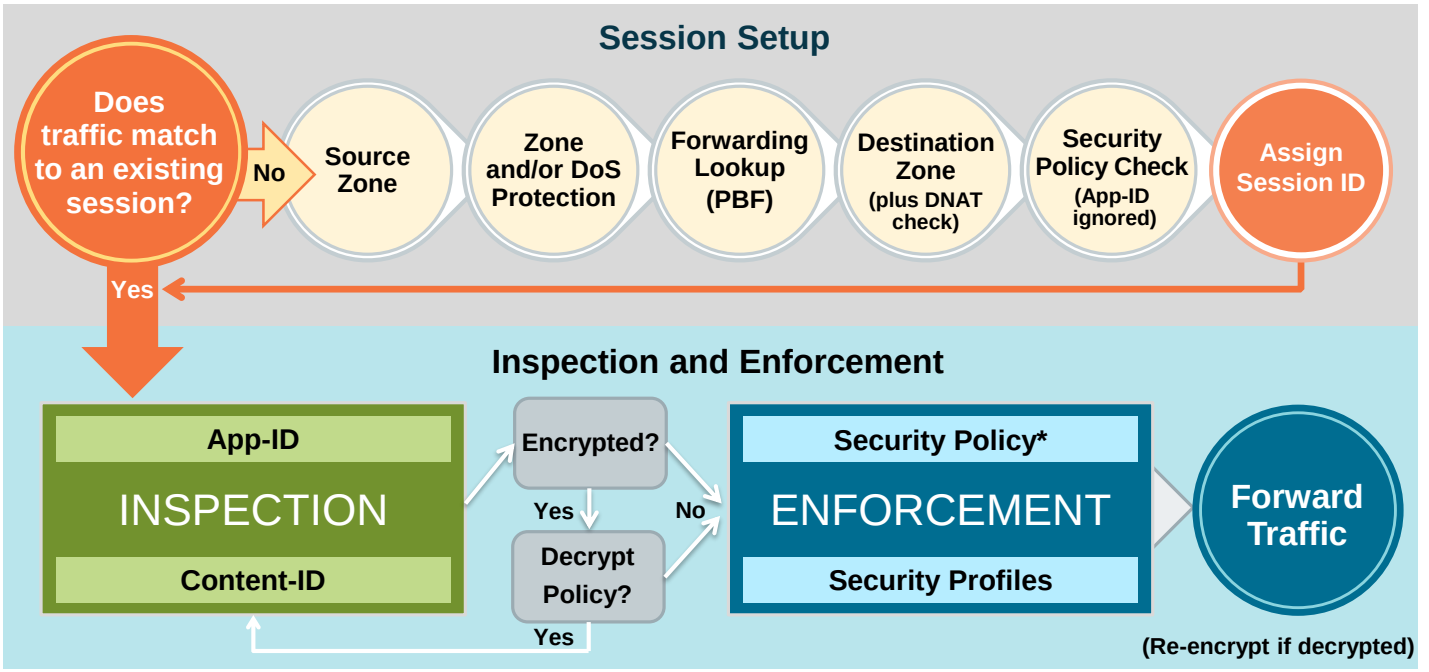
Agenda

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

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



* Policy check relies on pre-NAT IP addresses

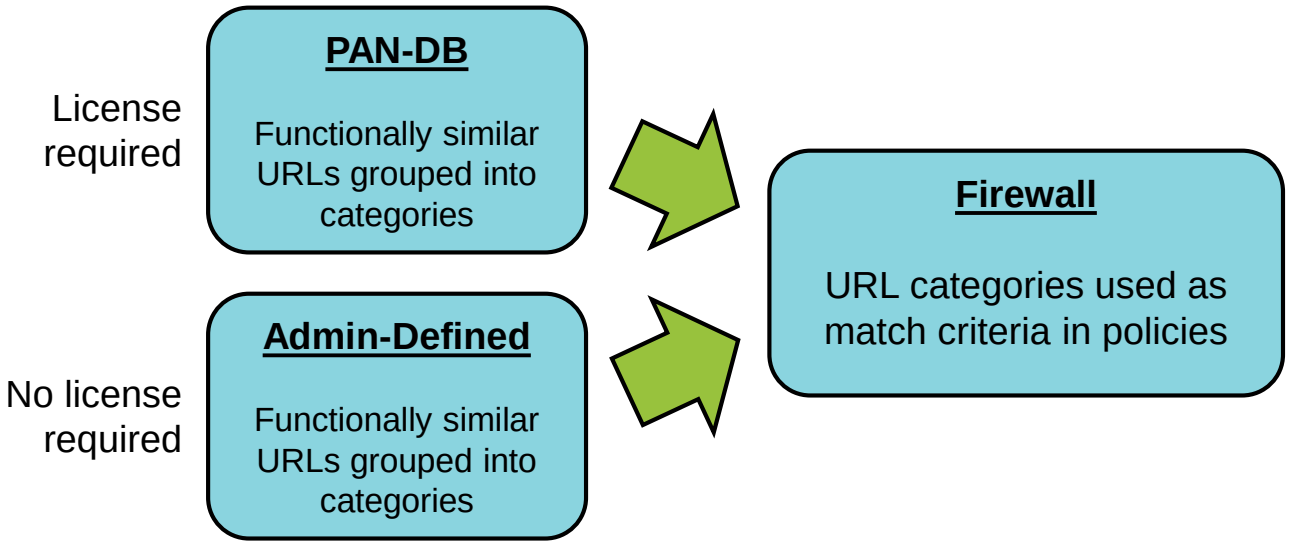
This diagram is a simplified version of the flow logic of a packet traveling through a Palo Alto Networks firewall. The course will reference this diagram to address where specific concepts fit into the packet processing sequence.

For more information about the packet handling sequence inside of a PAN-OS® device, see the *Packet Flow Sequence in PAN-OS* document available on the Palo Alto Networks Support website at https://live.paloaltonetworks.com/docs/DOC-1628.

URL Filtering Security Profiles

Attaching URL Filtering Profiles

URL Filtering Feature



Palo Alto Networks maintains the PAN-DB URL filtering database that groups websites into categories. A firewall with a valid URL Filtering license can use the PAN-DB database to filter user access to websites. For example, the www.yahoo.com website is assigned to the internet-portal category. You can block user access to www.yahoo.com through the firewall by denying access to the internet-portal category. An administrator can create their own custom URL categories and use them as match criteria in firewall policies even if the firewall does not have a URL Filtering license. URL categories can be used in Authentication, Decryption, QoS, and Security policies.

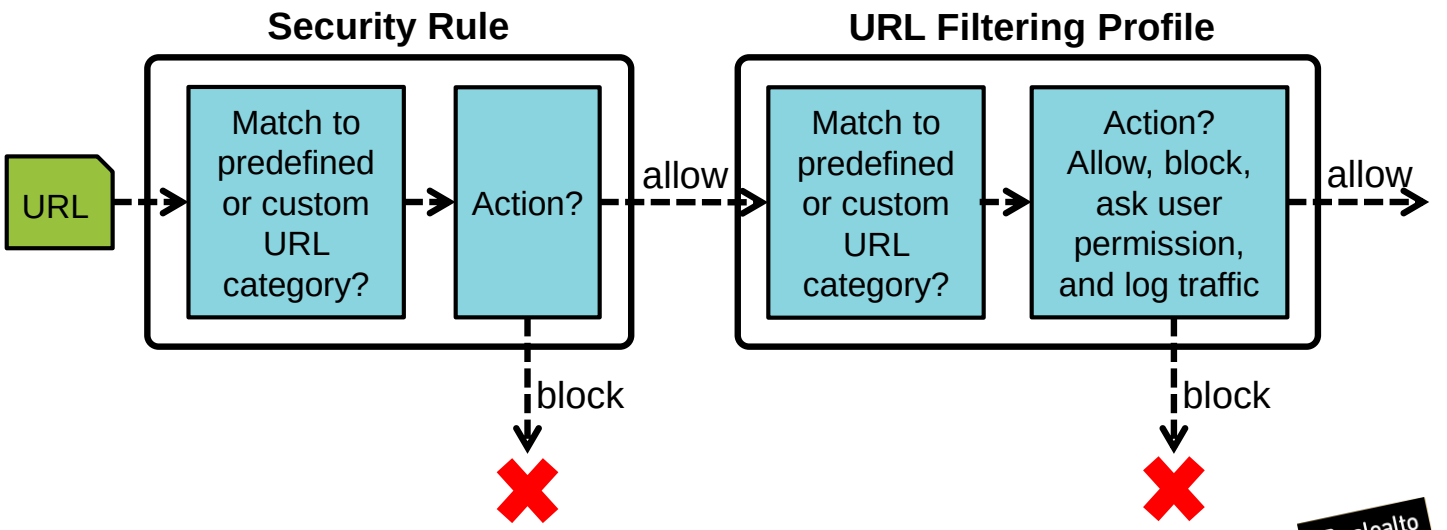
The firewall's initial cache of URLs is created from a seed database file downloaded from the PAN-DB cloud server. The size of the cache depends on the firewall model and ranges from a few hundred thousand to a few million URLs. The firewall backs up the cache to disk every eight hours and after a firewall is rebooted by an administrator. Cached entries expire based on timeouts included in the database for each URL. These timeouts are not configurable.

If a URL is not found in the cache, the firewall contacts the PAN-DB cloud servers for the lookup. The firewall will cache these URL lookups to expedite future lookups. The firewall does not require a nightly download of a URL Filtering file because all updates are downloaded dynamically from the cloud as needed.

The firewall can apply URL filtering to SSL encrypted traffic even if the traffic is not decrypted. The URL category can be matched to a Security policy rule even with SSL encrypted traffic because the URL information is seen in cleartext. App-ID would identify the application as SSL.

URL Filtering Profiles

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



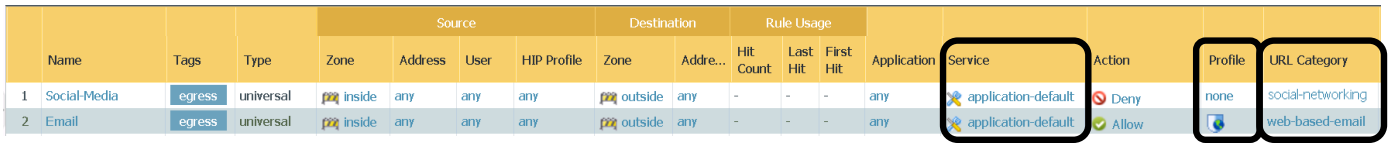
6 | © 2019 Palo Alto Networks, Inc.

Security Profiles are objects that are added to Security policy rules that are configured with an action of "allow." Security Profiles are not necessary for Security policy rules configured with the "deny" action because no further processing is needed if the network traffic will be blocked. As with Security policy rules, Security Profiles are applied to all packets over the life of a session.

The URL Filtering Profiles represent additional security checks to be performed on allowed network traffic. URL Filtering Profiles enable you to have more granular control over which URLs can be accessed through the firewall. For example, you could use a URL Filtering Profile to allow access to banking websites but block access to known malware websites. URL Filtering Profiles log detected threats to the log found at **Monitor > Logs > URL Filtering**.

URL Category: Policy Versus Profile

Policies > Security



	Name	Tags	Type	Source Zone	Source Address	Source User	Source HIP Profile	Destination Zone	Destination Addre...	Rule Usage Hit Count	Rule Usage Last Hit	Rule Usage 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

The **URL Category** column can be used as a match condition in Captive Portal, Decryption, QoS, and Security policy rules. The **URL Category** column can contain one or more URL categories defined by Palo Alto Networks or custom user-defined URL categories. The **Action** column in the Captive Portal, Decryption, and Security policy rules determines the action taken on the items listed in the **URL Category** column.

A URL Filtering Security Profile provides more granular control for traffic allowed by a Security policy rule. Like the other Security Profiles, a URL Filtering Security Profile is applied only if the Security policy allows the traffic. You can use a profile to assign different actions to specific URLs and URL categories for more focused control of web access. For example, you can create a Security policy rule to allow access to all web-based email websites but attach a profile that blocks access to specific email websites.

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

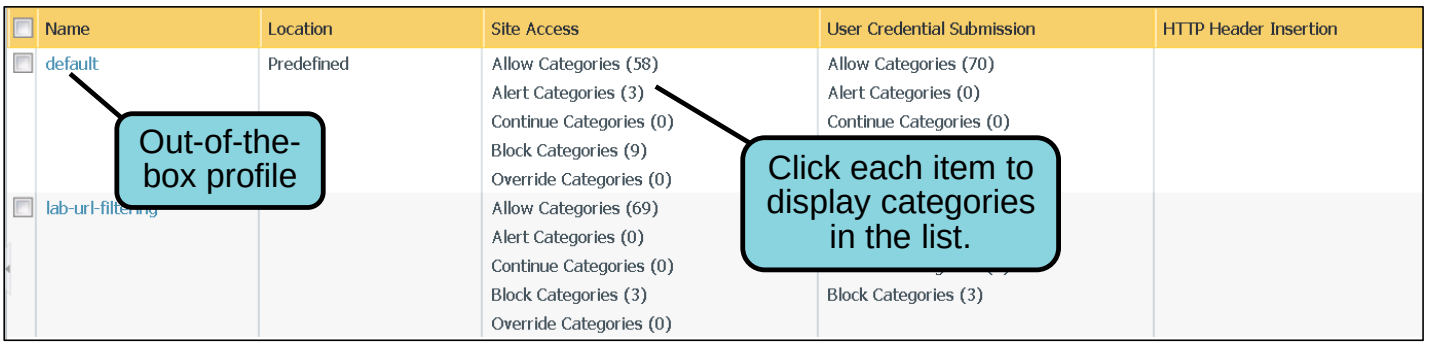
Receive Time	Category	URL	From Zone	To Zone	Source	Source User	Destination	Application	Action
01/18 20:28:49	shopping	images.craigslist.org/3kd3m13o55O25...	danger	danger	192.168.3.131	lab\jamie	208.82.236.130	web-browsing	block-url
01/18 20:28:45	shopping	vancouver.en.craigslist.ca/search/mca...	danger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

Access of a URL that matches a URL or URL category configured with an “alert,” “block,” “continue,” or “override” action results in a log entry in the URL Filtering log. In the example URL Filtering log, the user has applied the (URL contains ‘craigslist’) filter to display only those webpages that have attempted to connect to Craigslist.

Actions that require user interaction—“continue” or “override”—log the initial blocking action *and* the successful user action. For example, if a user is presented with a continue response page and clicks the **Continue** button, the firewall adds block-continue and continue log entries.

URL Filtering Security Profile

Objects > Security Profiles > URL Filtering



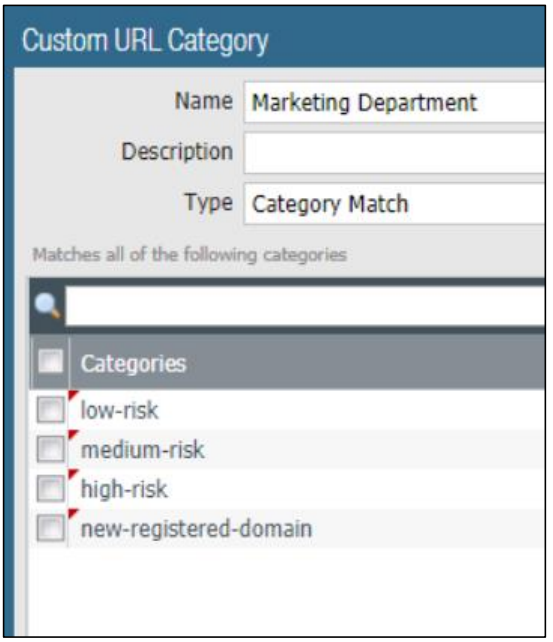
- To create customized profiles:
  - Clone the default read-only profile and edit the clone, or
  - Add a brand new profile

The Palo Alto Networks firewall includes a predefined, read-only default URL Filtering Profile. URL Filtering Profiles enable you to monitor and control how users access the web over HTTP and HTTPS.

The default profile is configured to block websites such as known malware sites, phishing sites, and adult content sites. The default profile cannot be deleted or modified. To create a customized URL Filtering Profile, clone the default profile and edit the clone. Or you can create a new URL Filtering Profile. By default, all categories are allowed in a new URL Filtering Profile. Use customized URL Filtering Profiles to minimize the number of blocked websites between more trusted zones or to maximize the number of blocked websites between less trusted zones. In a Zero Trust configuration, no zone is completely trusted.

Multi-Category and Risk-Based URL Filtering

Device > Setup > Content-ID > URL Filtering



- 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.

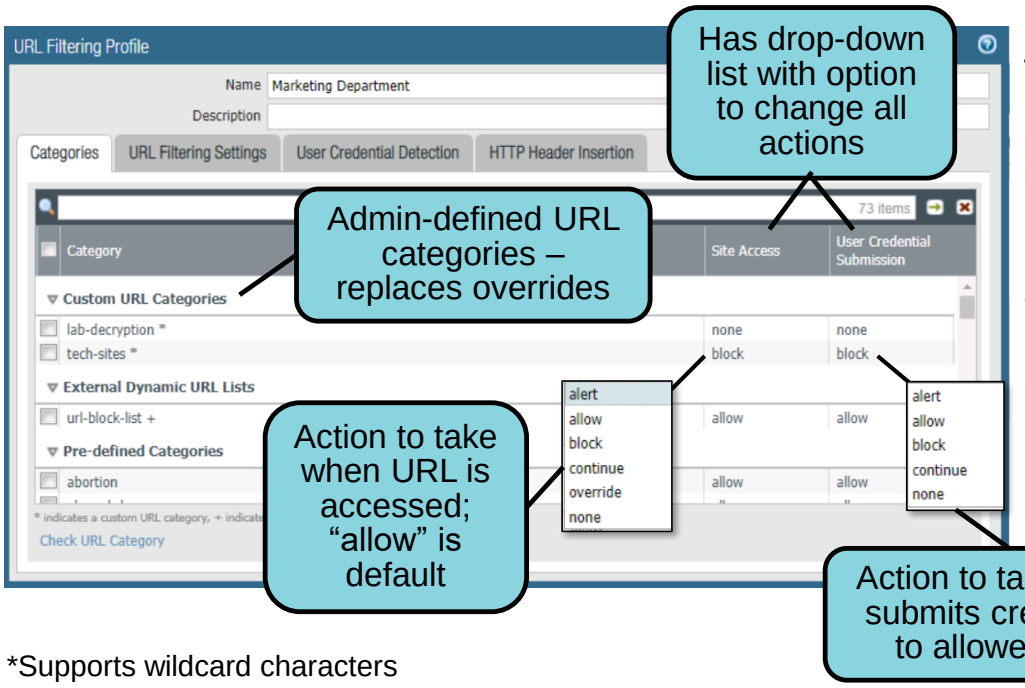
The PAN-DB URL Filtering cloud assigns multiple categories to websites to indicate recently registered domains, how risky a website is, the website's content, and the website's purpose or function.
The security-related categories are:

- Low-risk
- Medium-risk
- High-risk
- New-registered-domain

The three risk categories indicate whether the website is demonstrating varying levels of suspicious activity and that the website has not been confirmed as a malware or phishing site. The new-registered-domain category is for websites that have been registered within the last 32 days. A website can be classified with a security-related category until it no longer meets the criteria for that category. An example of changing criteria would be a website that has been registered for more than 32 days and no longer meets the criteria of a new-registered-domain.

If you want to enable multicategory and risk-based URL filtering, you must enable the firewall to connect to the beta PAN-DB server.

Configure Per-URL Category Actions



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

You can configure each URL Filtering Profile with specific actions to take for individual URL category matches. URL matches to a block or allow list always take precedence over a match to a URL category. You also can configure the action to take if a user submits credentials to an allowed URL. Choose the credential submission detection method on the **User Credential Detection** tab. If user credential detection is enabled, credentials submission events are logged to the URL Filtering log.

You can augment the predefined URL category list by creating your own custom URL category, which would be marked in the list by an asterisk. To create a custom URL category list, browse to **Objects** > **Custom Objects** > **URL Category** and click **Add**. Create a list of URLs and assign the list to a custom URL category. For example, My Custom URLs is a custom URL category list. You can build custom URL categories even if a firewall does not have a URL Filtering license. Custom URL category lists accept wildcard characters as do block and allow lists. The web interface includes the capability to import a custom URL category list from a text file or to export a custom category URL list to a text file.

You also can augment the predefined URL category list by using External Dynamic Lists, or EDLs, of URLs that are maintained on a web server and are made available to a firewall by HTTP(S). EDLs are marked in the list by a plus character (+). To configure access to an EDL, browse to **Objects** > **External Dynamic Lists** and click **Add**. After you have configured a firewall with an EDL and performed a commit, future URL changes on an EDL do not require that you perform a commit.

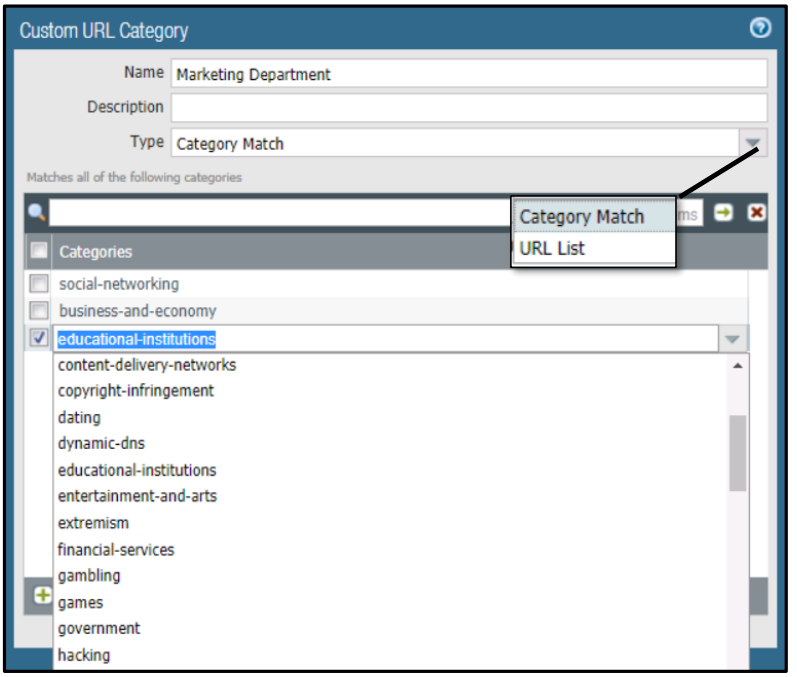
You define the actions the firewall takes for the URL categories, custom URL category lists, and EDLs. You also define the actions the firewall takes when users submit their credentials to URLs. The available actions are:

- alert: Allows the user to access the website but adds an alert to the URL Filtering log
- allow: Allows the user to access the website; no log or user message is generated
- block: Traffic is blocked, a block log entry is added to the URL Filtering log, and a response page is sent to the user's browser.

- continue: A response page is sent to the user's browser that prompts the user to click **Continue** to proceed and logs the action to the URL Filtering log. The "log" action is recorded as "block-continue" when the response page is generated and is changed to "continue" if the user clicks **Continue**.
- override: A response page is sent to the user's browser that prompts the user for the administrator-defined override password and logs the action to the URL Filtering log.
- none: (For a custom URL category only) Allows the firewall to inherit the URL Filtering category assignment from the URL database vendor

Configure a Custom URL Category

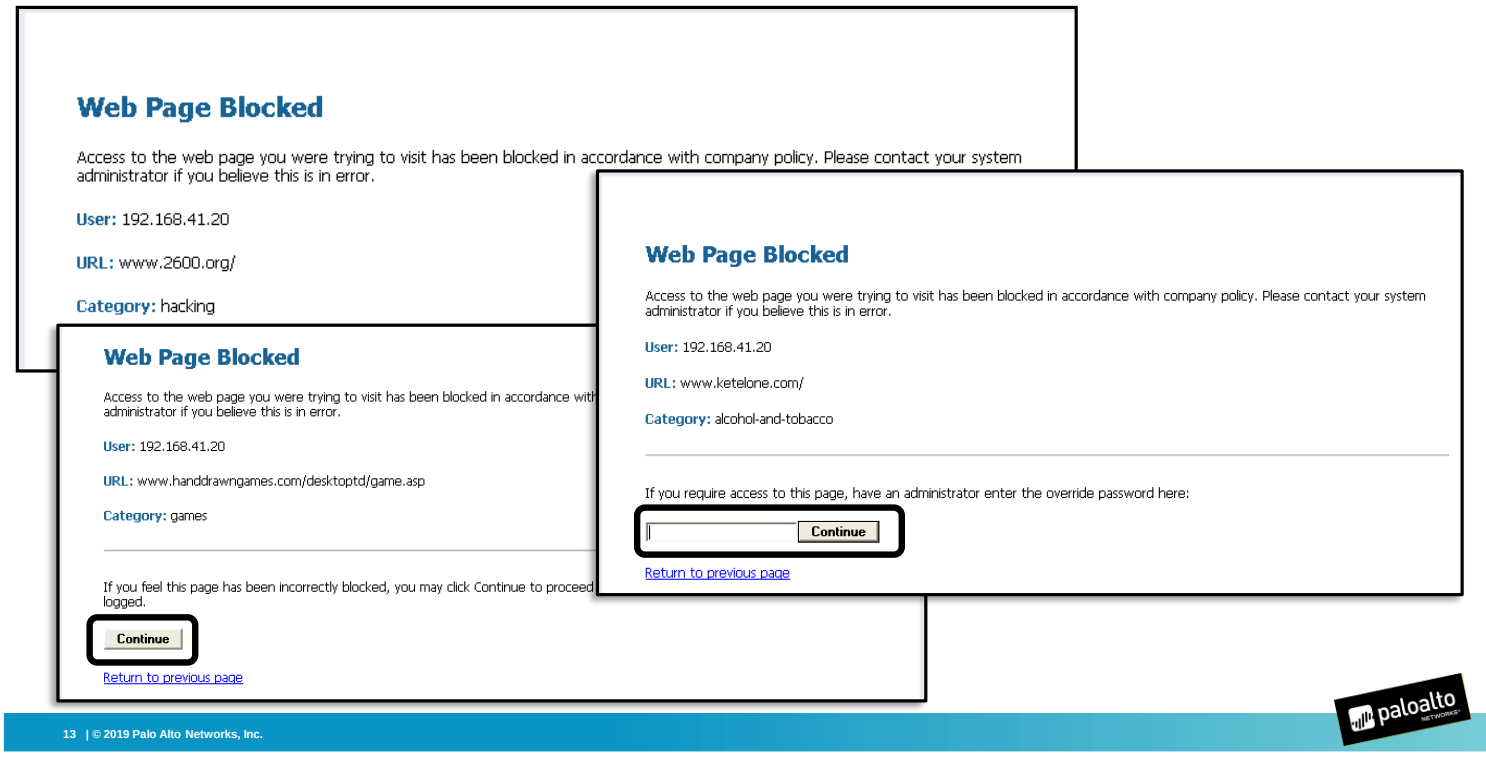
Objects > Custom Objects > URL Category > Add



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

With the release of PAN-OS 9.0, you can define a **Custom URL Category** based on specific websites or category matches that always should be blocked or allowed. A **Custom URL Category** is used to enforce a website separately from the URL category default settings. Custom categories can be defined on individual URLs, a list of URLs, or a list of PAN-DB URL categories. After a **Custom URL Category** is created, the category object will be managed in the **Custom URL Category** section of the URL Filtering Profile. **Custom URL Category** replaces URL filtering overrides that were available in previous versions of PAN-OS software.

URL Filtering Response Pages



HTML block pages—whose size limit is 16KB—are displayed in the user's browser when a user attempts to access a URL or URL category with a configured action of "block," "continue," or "override." Each page includes the user's IP address, the URL, and the URL category. The user's IP address is replaced with a username if User-ID technology is enabled.

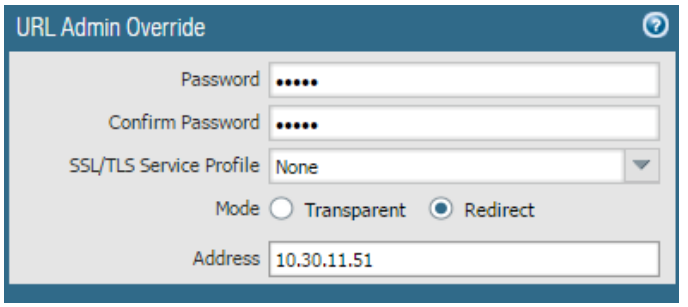
A user that successfully uses the continue or override response page has access for 15 minutes to the URL category associated with the URL that generated the event, and is not presented the response page again. This timeout time is configurable at **Device > Setup > Content-ID > URL Filtering**. The override password is set at **Device > Setup > Content ID > URL Admin Override**. A firewall can have only one URL Admin Override password.

URL Filtering response pages in a Layer 3 environment require the configuration of a Layer 3 interface on the firewall with an Interface Management Profile configured to allow response pages. Response pages also work in a Virtual Wire configuration.

To customize response pages, see the *Customizing Response Pages* Tech Note on the Palo Alto Networks Support website at https://live.paloaltonetworks.com/t5/Documentation-Articles/Customizing-Response-Pages/ta-p/57809.

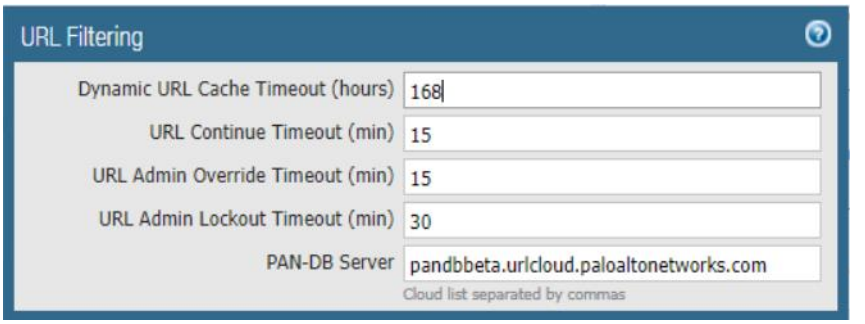
URL Admin Settings

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



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



A user must enter the URL Admin Override password to access a URL assigned to a URL category with the “override” action configured. A firewall can have only one URL Admin Override password at a time.

The SSL/TLS Service Profile can specify a certificate to use to secure the connection to the firewall when the **Mode** is set to **Redirect**.

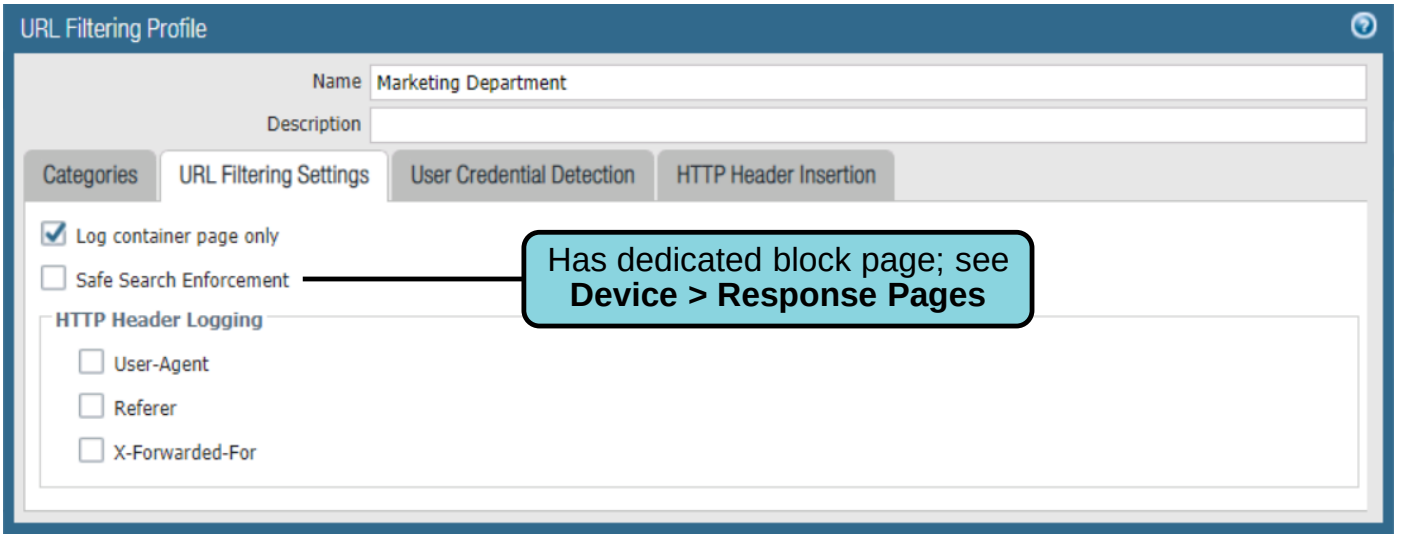
Transparent mode ensures that block pages appear to originate from the blocked website. The firewall impersonates the web server in the original request and prompts for a password. If it is an SSL connection and the browser does not trust the firewall’s certificate, the browser reports a certificate error. **Transparent** mode is required if no Layer 3 interfaces are configured on the firewall.

Redirect mode ensures that the block page originates from the configured IP address or DNS hostname on the firewall. The firewall intercepts the request and redirects it to the configured IP address. The IP address must correspond to a Layer 3 interface on the firewall with an Interface Management Profile configured to allow response pages. **Redirect** mode also supports session cookies and is the recommended mode.

The **URL Admin Override Timeout** field specifies the lifetime of the override before a user must re-enter the URL Admin Override password for URLs in the same category. The **URL Admin Lockout Timeout** field specifies the waiting period that a user must wait after three unsuccessful override attempts.

Configure Safe Search and Logging Options

Objects > Security Profiles > URL Filtering > Add



Safe search is a best-effort setting in web browsers that is used to prevent sexually explicit content from appearing within search results. The search provider and not Palo Alto Networks determines what is considered explicit. The capability of the firewall to detect a browser's safe search setting is provided with the weekly Applications and Threats content updates.

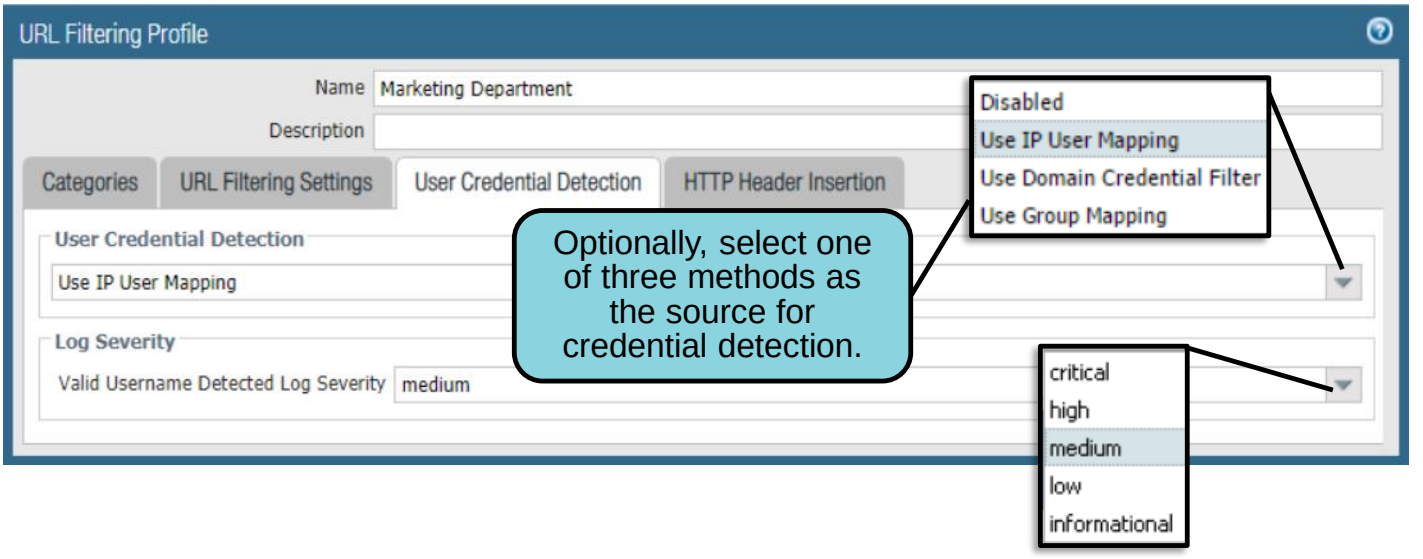
Safe Search Enforcement, if enabled, prevents users who use the Google, Yahoo, Bing, Yandex, or YouTube search engines from viewing search results unless their browser is configured with the strict safe search option. Users see a URL Filtering block page in their browsers if you enable this feature. If SSL is used, you must enable decryption for **Safe Search Enforcement** to function. To help enforce safe searching, you can add a Security policy rule to prevent access to other search providers.

If the **Log container page only** option is enabled in a URL Filtering Profile, only the URL of the main container page is logged, not the URLs of subsequent pages that might be included within the container page. URL Filtering can generate many log entries, so you might want to enable this option.

An HTTP request header might include the attribute-value pairs **User-Agent**, **Referer**, or **X-Forwarded-For**. To log these attribute-value pairs in the URL Filtering log, enable their corresponding options on the **URL Filtering Settings** tab. We highly recommend that you enable these options because enablement supports the analysis of indicators of compromise.

Configure Credential Phishing Prevention Method

Objects > Security Profiles > URL Filtering > Add



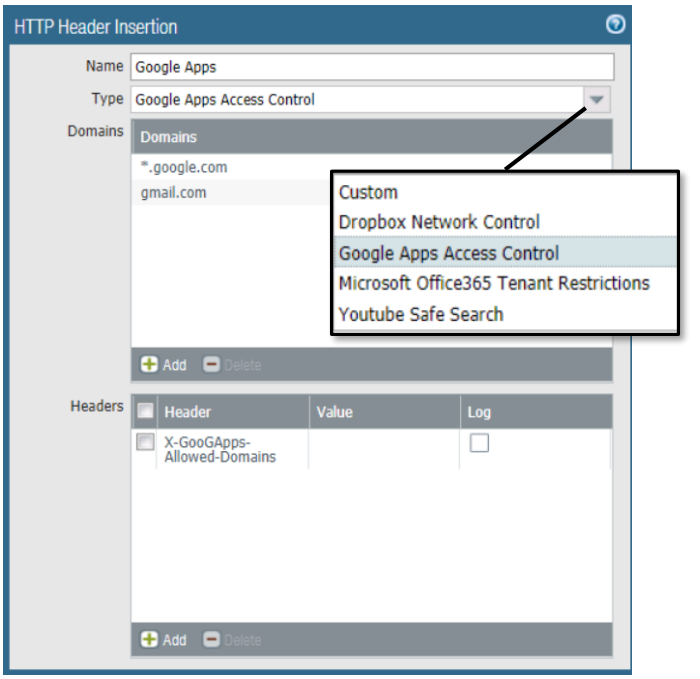
Beginning with PAN-OS 8.0 you can identify and prevent in-progress phishing attacks by controlling websites to which users can submit corporate credentials based on the site's URL category. The ability to control access to phishing websites enables you to block users from submitting credentials to untrusted sites while allowing users to continue to submit credentials to corporate and authorized sites.

Before you configure credential phishing prevention, decide which method you want the firewall to use to check if credentials submitted to a webpage are valid. Each method requires the configuration of User-ID technology. The Use IP User Mapping and Use Group Mapping methods check for valid username submissions only. In these cases, the firewall block or allow, based on your settings, the submission regardless of the accompanying password submitted. The Use Domain Credential Filter method checks for valid passwords submitted to a webpage:

- **IP User Mapping**: The firewall uses IP-address-to-user mappings that the PAN-OS integrated User-ID collects to check if a username submitted to a webpage matches the username of the logged-in user.
- **Group Mapping**: The PAN-OS integrated User-ID agent collects group mapping information from a directory server and retrieves a list of groups and the corresponding group members. It compares usernames submitted to a webpage against the group member usernames.
- **Domain Credential Filter**: The Windows-based User-ID agent is installed on a Read-Only Domain Controller, or RODC. The User-ID agent collects password hashes that correspond to users for which you want to enable credential detection, and sends these mappings to the firewall. The firewall then checks if the source IP address of a session matches a username and if the password submitted to the webpage belongs to that username. With this mode, the firewall blocks or alerts on the submission only when the password submitted matches a user password.

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

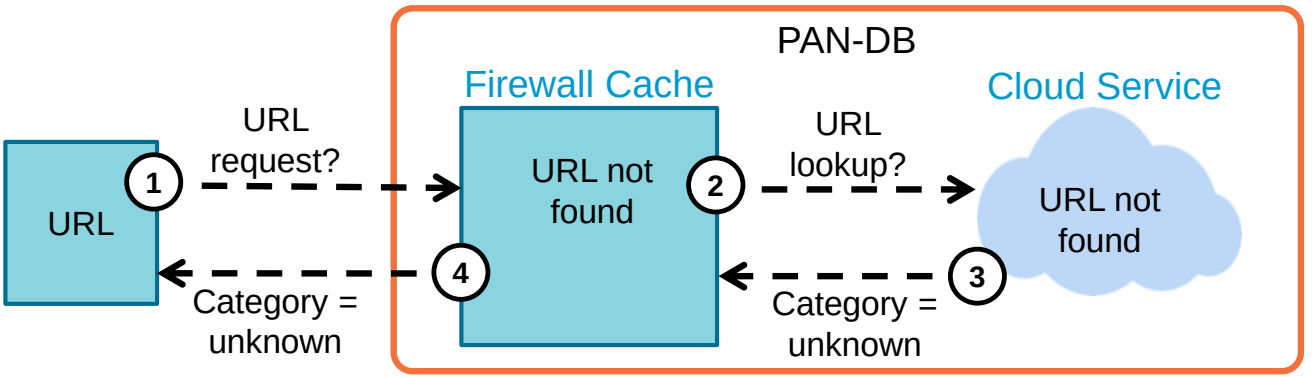


Software-as-a-service, or SaaS, applications are prone to data exfiltration through consumer versions of the application. With PAN-OS 8.1, firewalls now can perform HTTP header insertion as a way to enable access to only the enterprise version of the application while blocking access to the consumer version. HTTP header insertion occurs when an identified header is missing from the request. If the identified header exists, then the header is overwritten with the value that you defined.

You configure HTTP header insertion entries based on one of several predefined types. Predefined types are specific to a particular SaaS application. Four predefined types are available: Dropbox, Google, Office 365, and YouTube. If you want to perform HTTP header insertion for an application that has not been predefined, you can create a custom type. Custom types allow you to manage custom HTTP headers, but you also can use them to manage standard HTTP headers. Additional predefined types may be available in future content updates.

Handling Unknown URLs

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

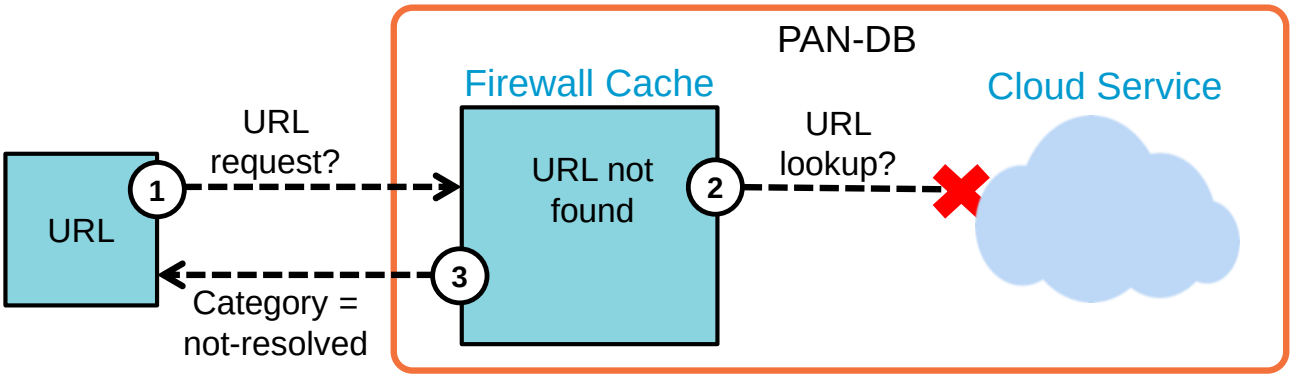


Recommendation: Set unknown URL category action to support your security requirements

A URL matched to the unknown URL category indicates that the URL has not yet been categorized, so it does not exist in the URL Filtering database on the firewall or in the URL cloud database. Although you might initially set the action to “alert” for unknown websites, you always should analyze the URL Filtering log to determine known good websites and create Security policy rules to allow them. Then you should considering blocking access to websites categorized as unknown.

Handling Not-Resolved URLs

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



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

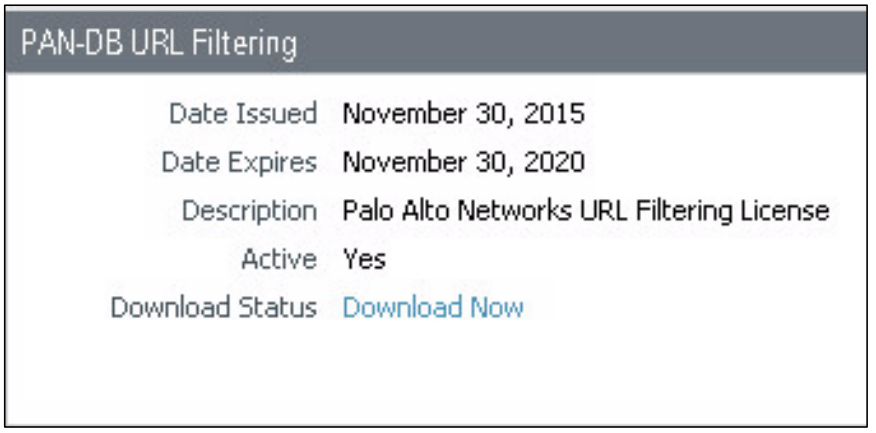
A URL matched to the not-resolved category indicates that the URL was not found in the local URL filtering database and the firewall was unable to connect to the cloud database to check the category. Configuration of the “block” action for traffic that is categorized as not-resolved might be disruptive to users. You could configure the action as “alert” so that users are not blocked by company policy yet log entries indicate that URLs are not being resolved to URL categories.

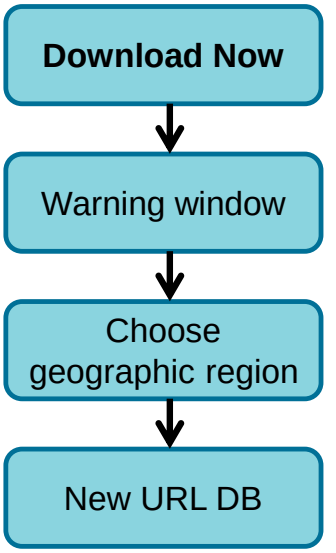
To verify current connectivity to the PAN-DB cloud service, use the command-line command **`show url-cloud status`**. It should report **`connected`**. The connection problem could be temporary because of a lack of management plane CPU resources. Use the **System Resources** widget on the web interface **Dashboard** to check management plane CPU use.

Downloading the URL Seed Database

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

Device > Licenses





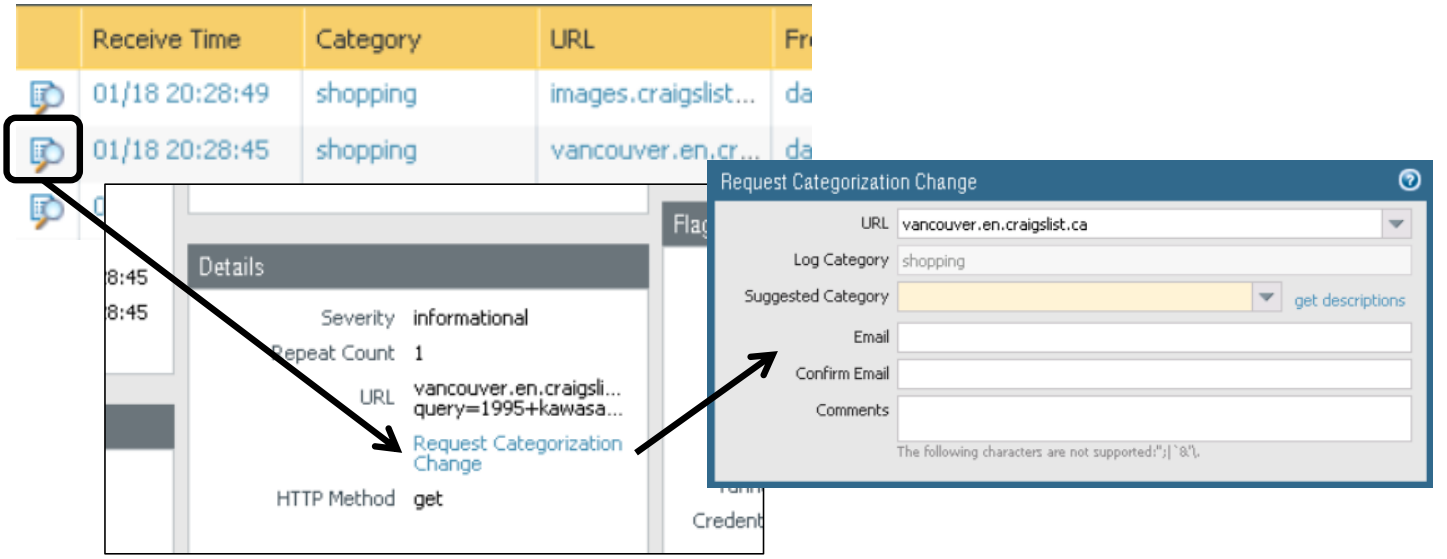
The initial seed database that you download to the firewall is a small subset of the PAN-DB database that is maintained on the Palo Alto Networks URL cloud servers. You download only a seed database because the full database contains millions of URLs and many of these URLs might never be accessed by your users.

When you download the initial seed database, you must select a region (North-America, Europe, APAC, Japan, Latin-America, Russia), each of which contains a subset of URLs most accessed for the given region. If you download a geographic-specific seed file, the firewall can then store a smaller URL database, which will greatly improve lookup performance. If a user accesses a website that is not in the local URL database, the full cloud database is queried and the firewall will cache the new URL in its local database.

Although the cache normally is persistent, note that the local URL database with its cached entries will be cleared if you re-download the seed database.

Recategorization Request: Via Log Entries

Monitor > Logs > URL Filtering



Sometimes URLs are miscategorized in the PAN-DB database, which can block user access that should be allowed.

Requests for recategorization can be submitted through the **Request Categorization Change** link in the **Details** window of a URL Filtering log entry. The link redirects the browser to the **Request Categorization Change** form that submits change requests to Palo Alto Networks.

The requests are reviewed by a human, so you must include comments. Requests often are processed within 24 hours.

Recategorization Requests: Via Webpage

You can submit recategorization requests using the Palo Alto Networks **Test A Site** website. To access the website, browse to **Objects** > **Security Profiles** > **URL Filtering** > **Add** and then click the **Check URL Category** link to open the **Test A Site** webpage. Alternatively, type the URL **`https://urlfiltering.paloaltonetworks.com`** into a web browser to open the **Test A Site** webpage.

On the **Test A Site** webpage, type your URL and click **Search**. The details of your URL are displayed along with a **Request Change** link. To request a recategorization, click the **Request Change** link, complete the web form with the details of your change request, and then click **Submit**.

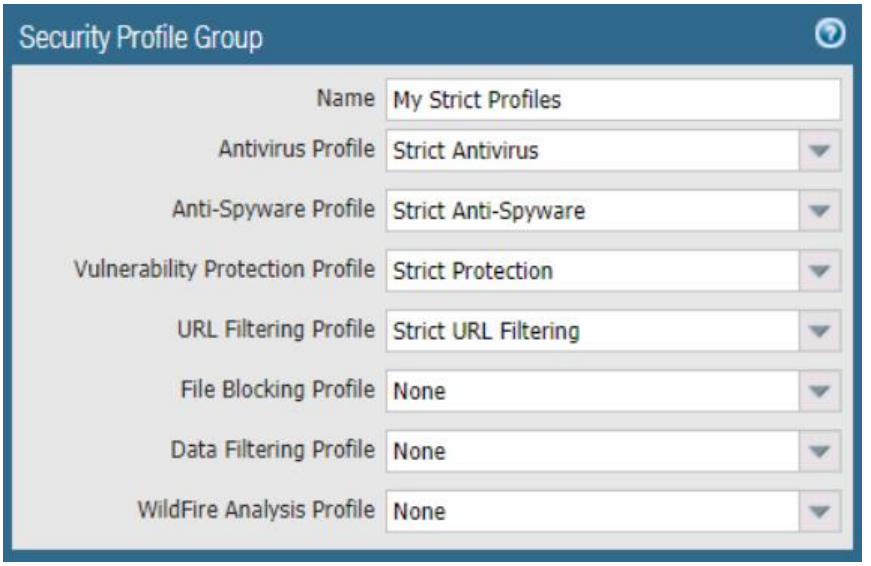
The **Test A Site** webpage also is useful for discovering a URL's assigned URL category. Knowledge of a URL's assigned category is useful for configuring the **URL Category** field in Security policy rules and also for configuring the URL categories in the URL Filtering Security Profiles.

URL Filtering Security Profiles

Attaching URL Filtering Profiles

Security Profile Groups

Objects > Security Profile Groups > Add

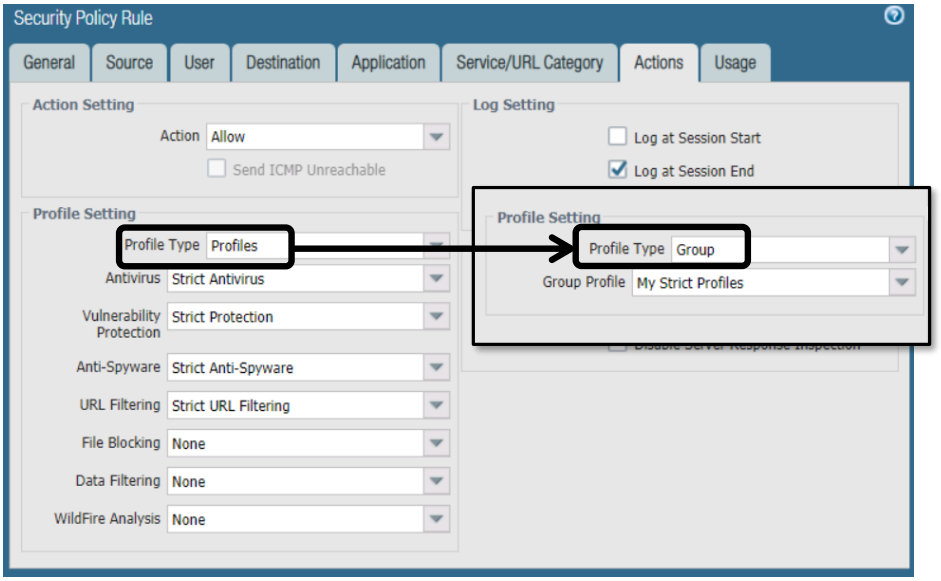


- Add Security Profiles that commonly are used together
- Simplifies security rule administration

The firewall supports the ability to create Security Profile Groups, which specify sets of Security Profiles that you can add in one step to a Security policy rule. For example, you can create a Security Profile Group that includes Security Profiles for Antivirus, Anti-Spyware, URL Filtering, and Vulnerability Protection, and then assign that Security Profile Group to a Security policy rule. Use of Security Profile Groups simplifies Security policy rule administration.

Assigning Security Profiles to Security Rules

Policies > Security > Add



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

You can assign either individual Security Profiles or a Security Profile Group to a Security policy rule. To assign individual Security Profiles to a Security policy rule, select **Profiles** as the **Profile Type**. To assign a Security Profile Group to a Security policy rule, select **Group** as the **Profile Type**.

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

Now that you have completed the 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?

Review Questions

1. Which four actions results in a URL Filtering log entry? (Choose four.)
   a. alert
   b. allow
   c. block
   d. continue
   e. override
2. True or false? URLs always are matched to a PAN-DB URL category before they match a custom URL category.
   a. true
   b. false
3. Which three statements are true regarding Safe Search Enforcement? (Choose three.)
   a. Safe search is a web server setting.
   b. Safe search is a web browser setting.
   c. Safe search is a best-effort setting.
   d. Safe search is designed to block violent web content.
4. True or false? A URL Filtering license is not required to define and use custom URL categories.
   a. true
   b. false
5. True or false? The **User Credential Detection** tab can be used to block traffic when users submit their corporate credentials to a website.
   a. true
   b. false

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.

Answers to Review Questions

1. a, c, d, e
2. b (false)
3. b, c, d
4. a (true)
5. a (true)