BLOCKING INAPPROPRIATE WEB TRAFFIC WITH ADVANCED URL FILTERING

AVOID DANGEROUS NETWORK NEIGHBORHOODS

- Advanced URL Filtering Security Profiles
- Attaching Advanced URL Filtering Profiles to Policy Rules

EDU-210 Version A
PAN-OS® 10.2

paloalto NETWORKS

Learning Objectives

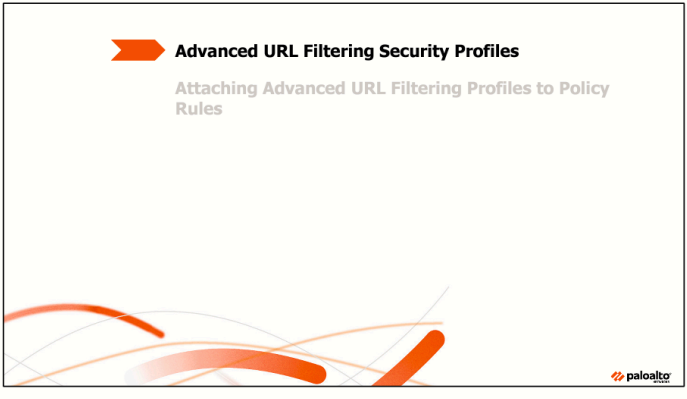
After you complete this module,
you should be able to:

- 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 Advanced URL filtering operations and options

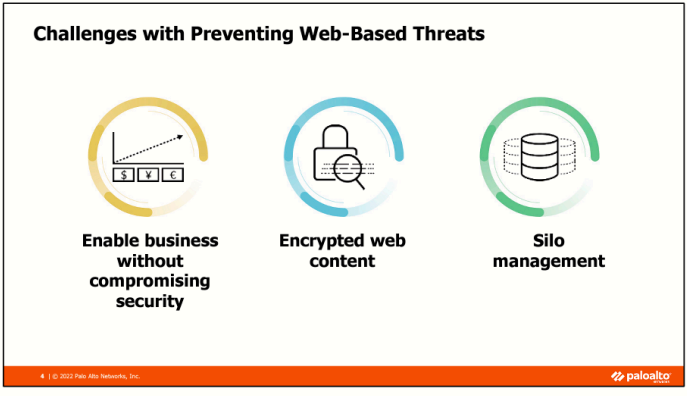
This module covers the topics listed here. Read through the list before proceeding.

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 Advanced URL filtering operations and options



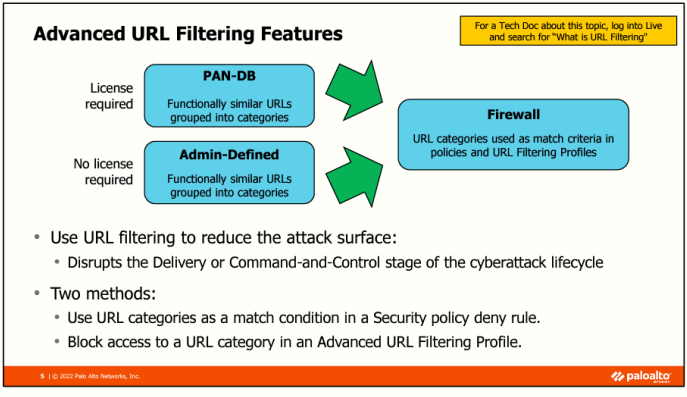
This section describes various methods available to block traffic to or from known-bad URLs.



Malicious webpages expose employees to phishing and credential theft, malware infection, and ransomware. Attackers use automation to dynamically generate thousands of malicious new URLs daily, overwhelming legacy protections such as standalone proxies or web filtering tools, which simply cannot keep up. In the minutes it takes to identify, classify, and protect against malicious websites, an infection can spread far enough to put a whole organization at risk. Adding additional products that do not integrate with the rest of your security stack means more policy sets to manage, and they can slow down your adoption of new business applications while requiring extra resources to maintain.

Enabling safe web access requires a natively integrated approach that extends your ML-Powered NGFW policy with easy-to-set web controls that automatically detect, prevent, and control threats. Beyond simply allowing and denying websites, Palo Alto Networks Advanced URL Filtering service uses machine learning to identify and prevent new and unknown attacks inline, blocking threats before your users can even access them.

The service analyzes URLs and classifies them into benign or malicious categories, which you can easily build into your ML-Powered NGFW policy. These categories trigger complementary capabilities across the firewall platform, enabling additional layers of protection, such as targeted SSL decryption and advanced logging. Alongside its own analysis, Advanced URL Filtering uses shared threat information from WildFire® malware prevention service and other sources to automatically update protections against malicious sites.



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.google.com website is assigned to the search-engines category. You can block user access to www.google.com through the firewall by denying access to the search-engines category. An administrator can create their own custom URL categories and use them as match criteria in firewall policy rules even if the firewall does not have a URL Filtering license. URL categories can be used in Authentication, Decryption, QoS, and Security policies.

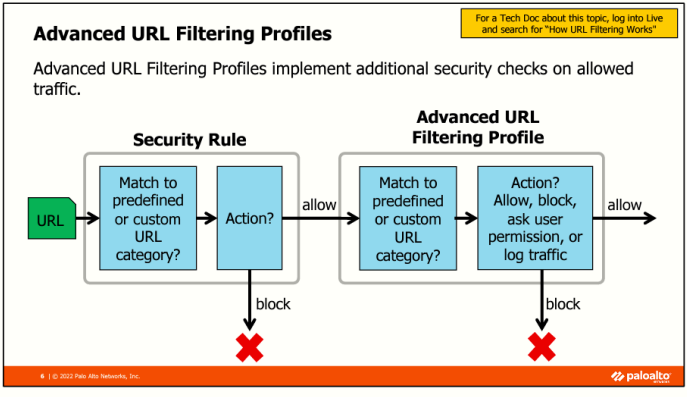
The size of the cache depends on the firewall model and ranges from a few hundred thousand URLs to a few million URLs. The firewall backs up the cache to disk every eight hours and after a firewall is rebooted by an administrator. Cached entries expire based on timeouts included in the database for each 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 Advanced 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.

Use Advanced URL Filtering to reduce your organization's attack surface and to disrupt the cyberattack lifecycle. For example, Advanced URL Filtering disrupts the Delivery or Command-and-Control stage of the cyberattack lifecycle. The Advanced URL Filtering feature controls access to specific URLs, websites, and website categories, or generates an alert in the URL Filtering log when URLs are accessed.

Two methods are available to block access to risky URL categories. The first method is to add the URL categories as match conditions to a Security policy deny rule. URL categories can be used as matching criteria in Security, QoS, Decryption, and Authentication policy. The second method is to control access to URL categories using an Advanced URL Filtering Profile attached to a Security policy allow rule.



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

URL Category: Policy Versus Profile

For a Tech Doc about this topic, log into Live and search for "Plan Your URL Filtering Deployment"

Policies > Security

	NAME	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE
1	Block-Social-Media-Access	universal	Users_Net	any	any	Internet	any	any	any	social-networking	Deny	none
2	Allow-Web-Mail	universal	Users_Net	any	any	Internet	any	any	any	web-based-email	Allow	

URL Category in a Policy	Advanced 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 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 category defined by Palo Alto Networks or it can contain custom user-defined URL categories. The **Action** column in the Captive Portal, Decryption, Authentication, and Security policy rules determines the action taken on the items listed in the **URL Category** column.

An URL Filtering Security Profile provides more granular control for traffic allowed by a Security policy rule. As is the case with 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

For a Tech Doc about this topic, log into Live and search for "URL Filtering Best Practices"

- 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

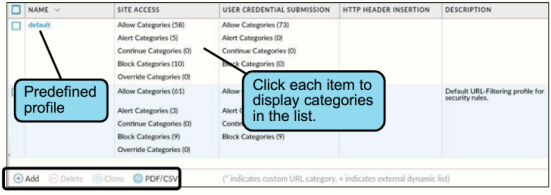
	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE	DESTINATION	APPLICATION	ACTION
	03/23 19:24:22	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	hidester.com/fav...	Users_Net	Internet	192.168.1.20	104.26.13.83	web-browsing	block-url
	03/23 19:24:22	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	hidester.com/log...	Users_Net	Internet	192.168.1.20	104.26.13.83	web-browsing	block-url
	03/23 19:24:22	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	hidester.com/	Users_Net	Internet	192.168.1.20	104.26.13.83	web-browsing	block-url
	03/23 19:24:22	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	hidester.com/	Users_Net	Internet	192.168.1.20	104.26.13.83	web-browsing	block-url
	03/23 19:20:47	hacking	hacking,low-risk	hacker9.com/fav...	Users_Net	Internet	192.168.1.20	159.89.148.144	web-browsing	block-url
	03/23 19:20:47	hacking	hacking,low-risk	hacker9.com/log...	Users_Net	Internet	192.168.1.20	159.89.148.144	web-browsing	block-url
	03/23 19:20:47	hacking	hacking,low-risk	hacker9.com/	Users_Net	Internet	192.168.1.20	159.89.148.144	web-browsing	block-url
	03/23 19:20:47	hacking	hacking,low-risk	hacker9.com/	Users_Net	Internet	192.168.1.20	159.89.148.144	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



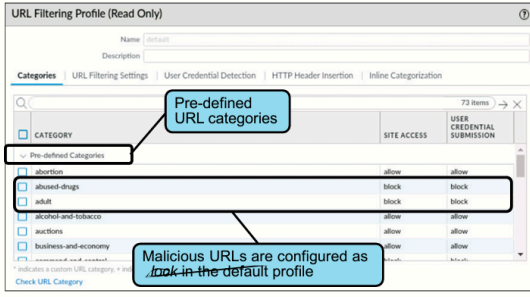
- To create customized profiles:
  - Clone the default read-only profile and edit the clone, or
  - Add a brand-new profile

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.

URL Filtering Security Default Categories

For a Tech Doc about this topic, log into Live and search for "URL Categories"



10 | © 2022 Palo Alto Networks, Inc.

PAN-DB classifies websites based on site content, features, and safety. A URL can have up to four categories, including risk categories (high, medium, and low), which indicate how likely it is that the site will expose you to threats.

The Security-focused URL categories can help you reduce your attack surface by providing targeted decryption and enforcement for sites that pose varying levels of risk but are not confirmed malicious. Websites are classified with a security-related category as long as they meet the criteria for that category; but as site content changes, policy enforcement dynamically adapts. You cannot submit a change request for security-focused URL Categories.

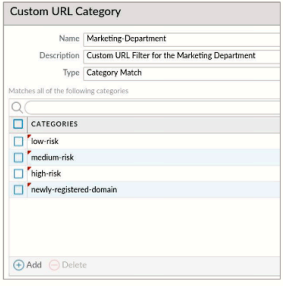
The Malicious URL Categories identify URLs as having malicious or exploitive content. Malicious URL Categories include malware, phishing, and command-and-control URL categories which are blocked in the default profile. The default URL Filtering profile also blocks the abused-drugs, adult, gambling, hacking, questionable, and weapons URL categories.

The Verified URL Categories includes URLs that are verified by Palo Alto Networks to be a part of a specific group of categories that do not possess an associated risk level. A risk level is only applicable to URLs that have *not* been verified. Verified URLs in certain categories are considered malicious and are blocked by default because access to these URLs presents a risk that is beyond an acceptable level for most environments.

For information about PAN-DB URL Filtering categories, log into Live and search for "URL Filtering Categories" or see the documentation at https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm5hCAC

Multi-Category and Risk-Based URL Filtering

Objects > Custom Objects > URL Category



- PAN-DB Advanced 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 *new-registered-domain*.

For a Tech Doc about this topic, log into Live and search for "Multi-Category URL Filtering"

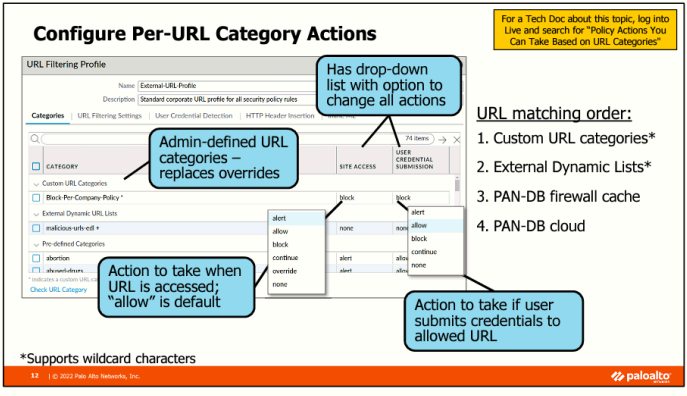
The PAN-DB Advanced URL Filtering cloud assigns multiple categories to websites to indicate recently registered domains, how risky a website is, the website's content, and the website's purpose or function.

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 multi-category and risk-based URL filtering, you must enable the firewall to connect to the PAN-DB server. Best practice is to block high-risk and new-registered-domain in URL Filtering Profiles.



You can configure each URL Filtering Profile with specific actions to take for individual URL category matches. 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. 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 the firewall logs the action to the URL Filtering log.

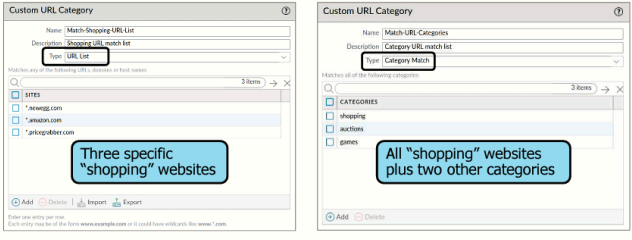
- none: (for a custom URL category only) Allows the firewall to inherit the URL Filtering category assignment from the URL database vendor

Configure a Custom URL Category

For a Tech Doc about this topic, log into Live and search for "Create a Custom URL Category"

Configure URL filtering based on specific URLs or URL categories.

Objects > Custom Objects > URL Category > Add



13 | © 2022 Palo Alto Networks, Inc.

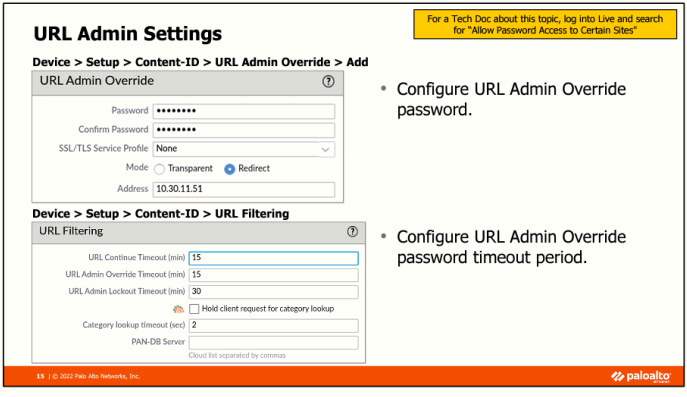
With the release of PAN-OS 9.0, you can define a **Custom URL Category** by specifying a list of one or more specific URLs or a list of one or more URL categories. After you create a **Custom URL Category**, you can use it in the **Custom URL Category** section of the URL Filtering Profile. Custom URL categories can be used in the Security policy or in a URL Filtering Profile to control access to websites.

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 during that time it will not be 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 URL Filtering response pages, log into Live and search for "Customize the URL Filtering Response Pages" or see https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/url-filtering/customize-the-url-filtering-response-pages.html.



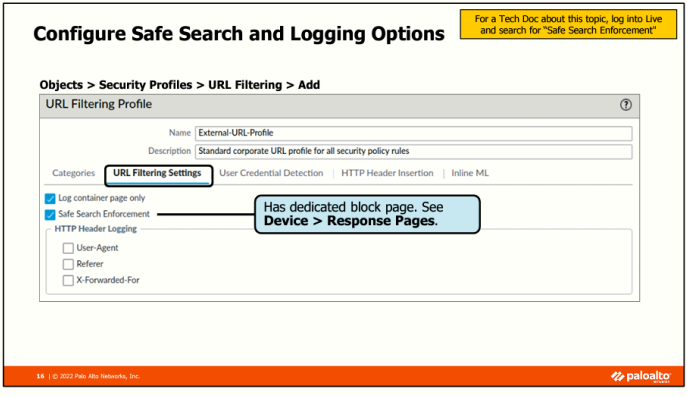
A user must enter the URL Admin Override password to access a URL assigned to a URL with the "override" action configured. A firewall can have only one URL Admin Override password at a time.

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**.

Redirect mode ensures that the block page originates from a Layer 3 or loopback interface on the firewall. The configured IP address or DNS hostname that you enter must match the Layer 3 or loopback interface IP address. You must assign to the interface an Interface Management Profile that permits response pages. The firewall intercepts the user's HTTP request and redirects it to the configured IP address on the firewall. The firewall responds by sending a webpage to the user requesting the URL Admin Override password. If the user enters the correct password, then the firewall redirects the user back to the original URL that they requested. Otherwise, the user is denied access. **Redirect** mode also supports session cookies and is the recommended mode.

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 the connection is to an SSL-enabled website and the browser does not trust the firewall's SSL forward trust certificate, the user's browser reports a certificate error. **Transparent** mode is required only if no Layer 3 interfaces are configured on the firewall. **Transparent** mode does not require you to configure an IP **Address**.

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.

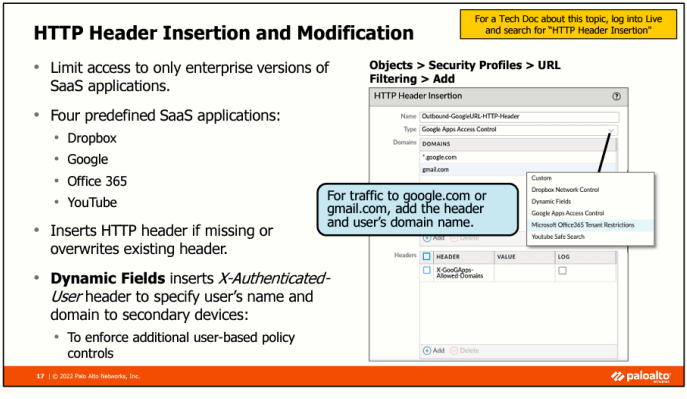


Safe search is a best-effort setting in web browsers that is used to prevent sexually explicit content from appearing within search results. The search provider (not Palo Alto Networks) determines what is considered explicit. The capability of the firewall to detect a browser's safe search setting is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

The **Safe Search Enforcement** option, 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. Advanced URL Filtering can generate many log entries, so you might want to leave this option enabled.

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. Palo Alto Networks highly recommends that you enable these options because enablement supports the analysis of indicators of compromise.

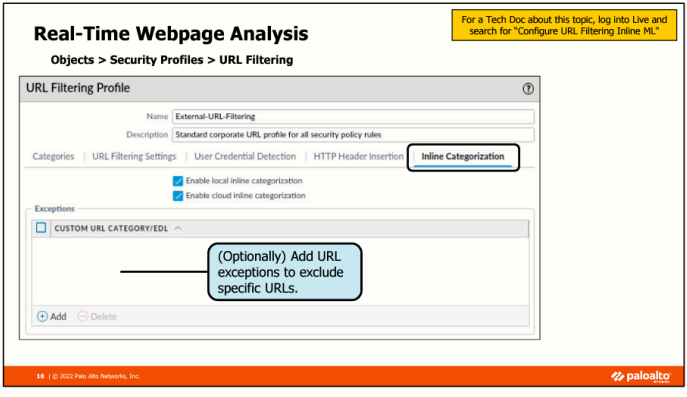


Software-as-a-service (or SaaS) applications are prone to data exfiltration through consumer versions of the application. Firewalls can perform HTTP header insertion to limit access to only the enterprise version of the application while blocking access to the consumer version. You can have the firewall insert SaaS application-defined headers that the SaaS servers use to determine whether a user gets access to the application. The value associated with the header typically is a username, a domain name, or both. HTTP header insertion occurs when the domain in the web request matches a domain you specified for insertion and the specified header is missing from the request. If the specified header exists, then the header value is overwritten with the value that you defined.

You configure HTTP header insertion entries for four predefined SaaS applications: 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 insert custom HTTP headers, but you also can use them to manage standard HTTP headers. Additional predefined types may be available in future content updates.

Starting with PAN-OS 9.1, you can use the **Dynamic Fields** option to have the firewall insert an *X-Authenticated-User* header that specifies the user's name, domain name, or both. The reason you might insert this HTTP header is to enable a secondary device to receive the user's information and enforce additional user-based policy. When you configure a secondary enforcement device to help enforce user-based policy, the secondary device must have a way to receive user information. Transmission of user information to downstream devices often requires deployment of redundant methods that can result in a negative user experience—for example, users having to log in multiple times. If you share the user's identity by having the firewall insert it in an HTTP header, you can enforce user-based policy without negatively impacting the user's experience.

Select the **Log** check box to ensure that the header insertion event is recording in the firewall's URL Filtering log.

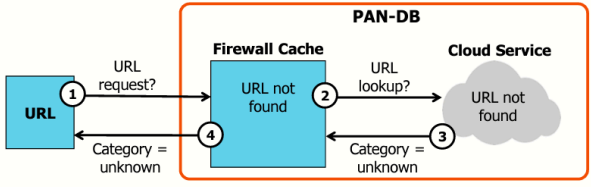


With the release of PAN-OS 10.2, Advanced URL Filtering now operates a series of inline cloud-based deep learning detectors that evaluate suspicious web page contents in real-time to protect users against zero-day threats. This includes cloaked websites, multi-step attacks, CAPTCHA challenges, and previously unseen one-time-use URLs.

When the firewall processes a URL request containing suspicious web page contents, it forwards the HTTP response data to the cloud and analyzes the contents of the web page that are deemed suspicious and is categorized accordingly. The deep learning detectors and analyzers used to categorize websites are updated and deployed automatically as Palo Alto Networks threat researchers improve the detection logic, and does not require the administrator to download and deploy update packages. Cloud inline categorization is enabled and configured through the URL Filtering Profile and requires an active Advanced URL Filtering license.

Recommendations for Unknown URL Category

Category column in URL Filtering log lists *unknown*.



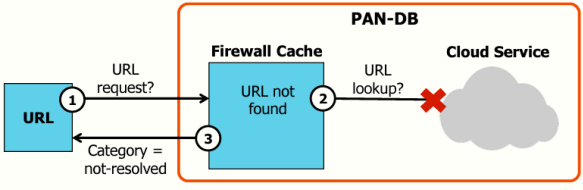
Recommendation: Set unknown URL category action to support your security requirements.

For a Tech Doc about this topic, log into Live and search for "Malicious URL Categories"

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 initially might 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 consider blocking access to websites categorized as *unknown*.

Recommendations for Not-Resolved URL Category

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

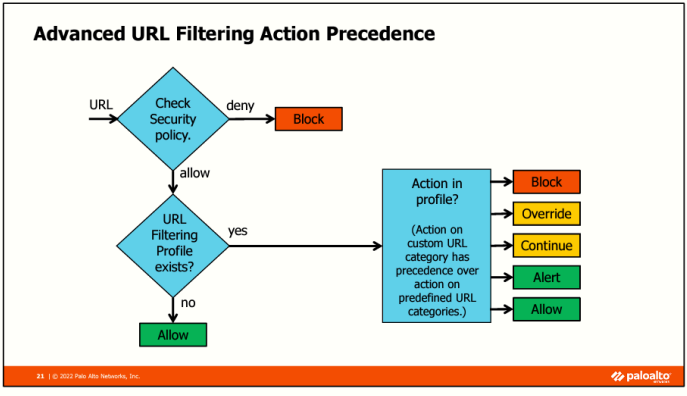


Recommendation: Set *not-resolved* URL category match action to "alert."

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 interface **`show url-cloud status`** command. 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.

Note: A *not-resolved* category could also be caused by an expired URL Filtering subscription license.

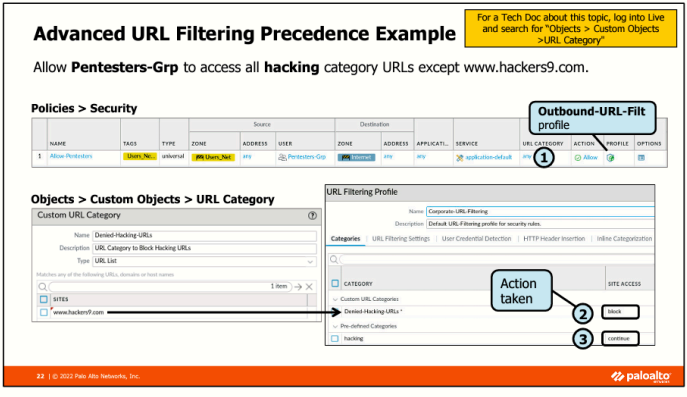


Configure Advanced URL Filtering by using a combination of Security policy rules and Advanced URL Filtering Profiles. The Security policy and the Advanced URL Filtering Profiles include several configuration options that include the actions to be taken by the firewall. You should understand these configuration options and how they interact when you create or interpret a firewall configuration. The flowchart illustrates Advanced URL Filtering action precedence.

Network traffic trying to access a URL first is checked against the Security policy. If a matching rule is found, then the action specified in that rule is taken. If the Security policy rule denies the traffic, then the traffic is blocked. If the Security policy rule allows the traffic, then the firewall checks for the presence of a URL Filtering Profile. If no profile exists, then the traffic is allowed. In either case, if the rule has logging enabled, then the traffic is logged to the Traffic log.

If a URL Filtering Profile does exist, then the firewall checks the profile's configured actions in the **Site Access** column for each URL category. The **Site Access** column lists all custom and predefined URL categories. Each category has a default action listed, but you can specify an alternate action. The actions are "alert," "allow," "block," "continue," and "override." The traffic is matched to a category, and the firewall takes the action specified for that category. If a URL is matched to a custom URL category and a predefined URL category, the action for the custom URL category has precedence.

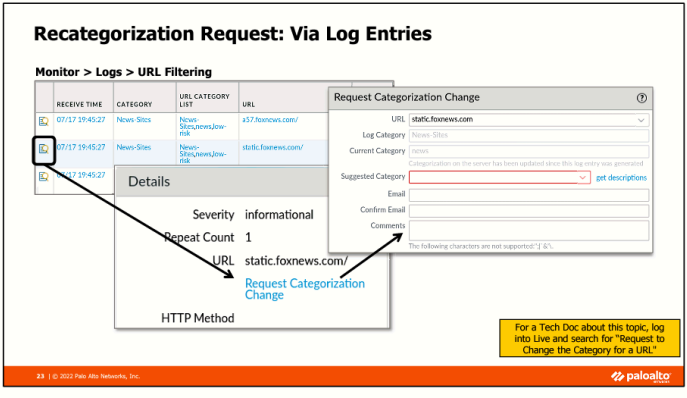
The URL Filtering Profile logs information about the traffic and the action taken to the URL Filtering log. If a URL is matched to multiple URL categories, then the **Category** column lists the URL category that triggered the action taken. The **URL Category List** column lists all URL categories the URL matched.



This example might help you to better understand the precedence order of the Advanced URL Filtering feature. The firewall evaluates the Advanced URL Filtering settings in the order shown here: 1, 2, and then 3.

In this example, Security policy rule 1 allows members of **Pentesters-Grp** to access *any* URL category. However, the rule has an attached URL Filtering Profile. The attached URL Filtering Profile includes the custom URL category named **Denied-Hacking-URLs** that includes the URL www.hackers9.com. However, the URL www.hackers9.com also belongs to the predefined **hacking** URL category. The action assigned to the custom URL category is "block," but the action assigned to the predefined URL category is "continue." Because the URL www.hackers9.com belongs to both URL categories, which action will the firewall take when traffic to the URL is detected?

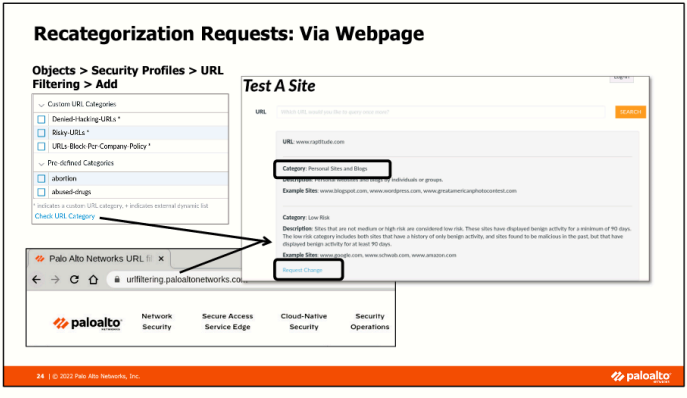
The action assigned to a URL in a custom URL category is evaluated before and has precedence over the action assigned to a URL in a predefined URL category. So in this example access to www.hackers9.com is blocked.



Sometimes URLs are miscategorized in the PAN-DB database and user access that should be allowed is blocked.

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.



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. Or you can 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.

This section describes various methods available to block traffic to or from known-bad URLs.

Use a URL Filtering Profile

For a Tech Doc about this topic, log into Live and search for "URL Categories"

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

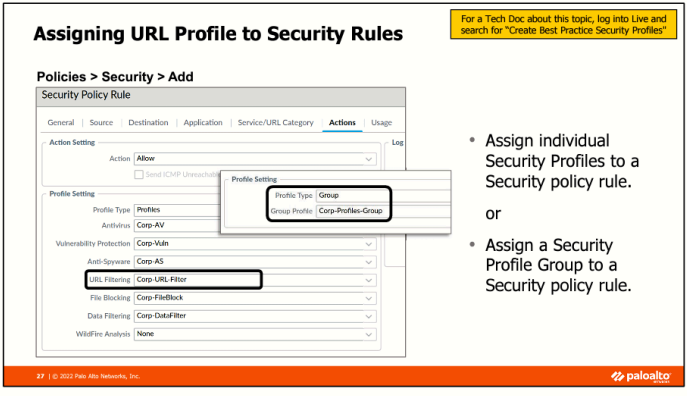
Policies > Security

	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source US..	Destination ZONE	Destination ADDRESS	APPLICATI...	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
1	Allow-Some-Web-Access	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.

After you have configured firewall Security policy rules, further reduce the overall attack surface by adding a URL Filtering Profile to any rules that allow outbound web access. An easy starting point is to block access to those URL categories or sites that are undeniably classified as malicious. The URL categories that Palo Alto Networks recommends to block are command-and-control, dynamic-dns, hacking, high-risk, malware, phishing, and unknown. You also can consider blocking access to adult, extremism, new-registered-domain, parked, proxy-avoidance-and-anonymizers, and questionable.

Create custom URL Filtering Profiles to filter URL categories according to your organization's security or acceptable-use policies.



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:

- 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 Advanced URL Filtering operations and options

Now that you have completed the module, you should be able to perform the tasks listed.

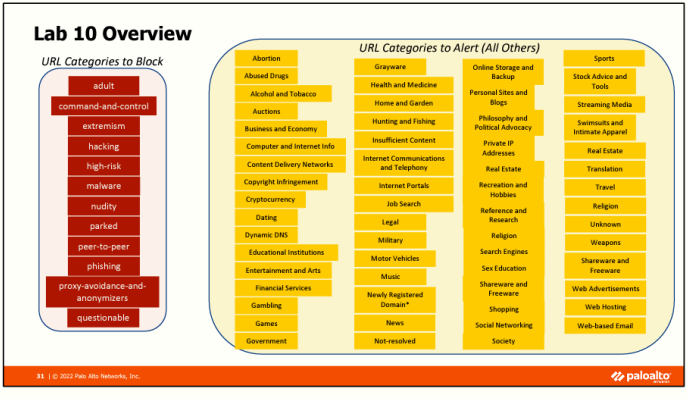
Additional Resources

For a digital review of this module, log into Beacon and search for:

"Security Rule Tuning"

Review Questions

1. Which URL Filtering Profile action will result in a user being interactively prompted for a password?
    a. alert
    b. allow
    c. continue
    d. override
2. According to best practices, which two URL filtering categories should be blocked in most URL Filtering Profiles? (Choose two.)
    a. high-risk
    b. medium-risk
    c. new-registered-domain
    d. adult
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.
    e. Safe search works only in conjunction with credential submission websites.
4. True or false? A URL Filtering license is not required to define and use custom URL categories.
    a. true
    b. false



Your instructor can provide an overview of the lab environment and the details needed for this lab. See the following page for a list of tasks that you will carry out in this lab.

Lab 10: Blocking Inappropriate Web Traffic with Advanced URL Filtering

- Test access to inappropriate web content without URL blocking in place
- Create a Security Policy rule to block inappropriate web content using the URL Category
- Test the Security Policy rule and examine the results
- Disable the Security Policy rule
- Create and apply a URL Filtering Profile to block access to a malicious URL
- Test the Security Profile and examine the results

Answers to Review Questions

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