Symantec WebFilter to PAN-DB URL Filtering Migration Guide

TABLE OF CONTENTS

INTRODUCTION

This document is designed to assist you in migrating your environment from using Symantec Web Filter categories on ProxySG to using URL Filtering capabilities in the Palo Alto Next Generation Firewall enabled by PAN-DB, Palo Alto Networks Cloud based URL Categorization service.

The first part of this document contains category mappings to assist you in selecting which PAN-DB URL Categories to use. In most cases, there is a one to one mapping between the URL categorization commonly used in Symantec Web Filter and the categorization provided by Palo Alto Networks.

The second part of the document contains examples on how to migrate from Symantec Web Filter categories to PAN-DB categories and how to use them in the security policies of the Next Generation Firewall. During the migration, it is a recommended best practice to configure a URL filtering profile with all categories set to “alert” in parallel with your Web Filtering solution. This allows you to run reports in PAN-OS and Proxy-SG to verify policies and category mappings before switching the URL filtering functions over completely to PAN-DB URL Categorization on our Next Generation Firewall.

The third part of this document contains usage examples and recommended security best practices when using PAN-DB based URL Categorization in the Next Generation Firewall.

CATEGORY MAPPINGS FOR MOVING FROM SYMANTEC WEBFILTER TO PAN-DB

To start the migration, the first thing we recommend you to do is to review the categories that are blocked by policy with the Symantec WebFilter and map them to the corresponding PAN-DB URL categories.

The Symantec WebFilter Database is organized into 85 URL categories. You can find the complete listing and definitions of the categories at this link:

https://sitereview.bluecoat.com/category-descriptions

PAN-DB is organized into more than 65 URL categories. You can find the complete listing and definitions of the categories at this link:

https://live.paloaltonetworks.com/t5/Management-Articles/Complete-List-of-PAN-DB-URL-Filtering-Categories/ta-p/129799

Symantec WebFilter offers a service called “Site Review.” The purpose of “Site Review” is to allow Symantec customers to check the current database categorization of WebFilter URLs and report sites that they believe are incorrectly categorized.

https://sitereview.bluecoat.com/

PAN-DB URL Filter also offers a service called “Test a Site.” The purpose of “Test a Site” is to allow Palo Alto Networks customers to check the current database categorization of PAN-DB URLs and report sites that they believe are incorrectly categorized.

https://urlfiltering.paloaltonetworks.com/

The table below will help you with the category mapping exercise.

Symantec	Palo Alto Networks	Differences	Recommendations
Abortion	Abortion		
Adult/Mature Content	Adult or Questionable		
Alcohol	Alcohol and Tobacco		
Alternative Spirituality/Belief	Religion		
Art/Culture	Entertainment and Arts		
Auctions	Auctions		
Audio/Video Clips	Streaming Media or Music		
Brokerage/Trading	Stock Advice and Tools or Financial Services		
Business/Economy	Business and Economy		
Charitable Organizations	Society		
Chat (IM)/SMS	Internet Communications and Telephony		
Child Pornography	Adult		
Computer/Information Security	Computer and Internet Info or Hacking		

Content Servers	Content Delivery Networks		
Controlled Substances	Abused Drugs		
Dynamic DNS Host	Dynamic-DNS		Best Practice recommendation, Block “dynamic-dns” category
E-Card/Invitations	Shareware-and-Freeware		
Education	Educational Institutions		
Email	Web-based Email		
Entertainment	Entertainment and Arts		
Extreme	Extremism		Best Practice recommendation, Block “extremism” category
File Storage/Sharing	Online Storage and Backup		
Financial Services	Financial Services		
For Kids	Society	This Symantec category is not a stand-alone category.	
Gambling	Gambling		
Games	Games		
Government/Legal	Government		
Hacking	Hacking		
Health	Health and Medicine		
Humor/Jokes	Entertainment and Arts or Questionable		

Informational	N/A	This Symantec category is not a stand-alone category.	Recommended action: - Use "Test a Site" to find corresponding PAN-DB category for matching websites. - Or Create a Custom URL category and control matching websites.
Internet Connected Devices	Computer and Internet Info	There is no one-to-one mapping for this category. This is a subset of "computer-and-internet-info" category.	Recommended action: - Use "Test a Site" to find corresponding PAN-DB category for matching websites. - Or Create a Custom URL category and control matching websites.
Internet Telephony	Internet Communications and Telephony		
Intimate Apparel/Swimsuit	Swimsuits and Intimate Apparel		
Job Search/Careers	Job Search		
Malicious Outbound Data/Botnets	Command-and-Control		Best Practice recommendation, Block "Command-and-Control" category
Malicious Sources/Malnets	Malware		Best Practice recommendation, Block "malware" category.
Marijuana	Abused Drugs		
Media Sharing	Streaming Media or Online Storage and Backup		
Military	Military		
Mixed Content/ Potentially Adult	Adult, Nudity or Questionable	Based on the category description provided by	

		Symantec, most URLs should be mapped to “adult”. But the URLs could also be part of “nudity” or “questionable”	
News/Media	News		
Newsgroups/Forums	News or Personal-Sites-And-Blogs		
Non-Viewable/Infrastructure	Insufficient Content		
Nudity	Nudity		
Office/Business Applications	Computer and Internet Info		
Online Meetings	Internet Communications and Telephony		
Peer-to-Peer (P2P)	Peer-to-Peer		
Personals/Dating	Dating		
Personal Sites	Personal Sites and Blogs		
Phishing	Phishing		Best Practice recommendation, Block “phishing” category
Piracy/Copyright Concerns	Copyright-Infringement		Best Practice recommendation, Block “copyright-infringement“ category.
Placeholders	Parked		Best Practice recommendation, Block “parked” category

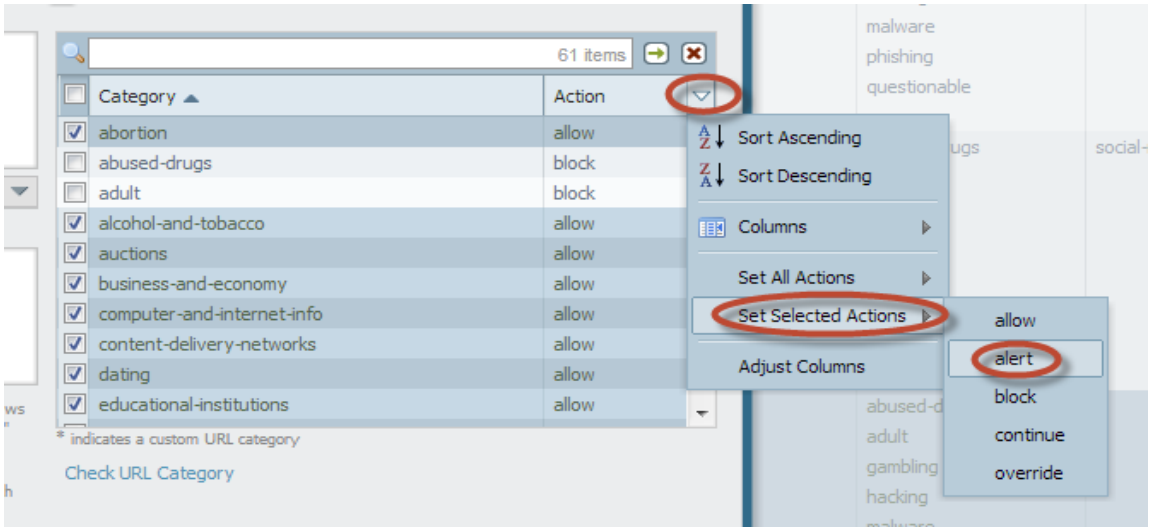
Political/Social Advocacy	Philosophy and Political Advocacy		
Pornography	Adult		
Potentially Unwanted Software	Shareware and Freeware or Questionable		
Proxy Avoidance	Proxy Avoidance and Anonymizers		Best Practice recommendation, Block "proxy-avoidance-and-anonymizers" category
Radio/Audio Streams	Streaming Media		
Real Estate	Real Estate		
Reference	Reference and Research		
Religion	Religion		
Remote Access Tools	Internet Communications and Telephony		
Restaurants/Dining/Food	Society		
Scam/Questionable/Illegal	Questionable		
Search Engines/Portals	Search Engines		
Sex Education	Sex Education		
Sexual Expression	Adult or Society	If the website content pertains to sexual identity then the category will	

		be “society”. If not, the category will be “adult”.	
Shopping	Shopping		
Social Networking	Social Networking		
Society/Daily Living	Society		
Software Downloads	Shareware and Freeware or Computer and Internet Info		
Spam	Questionable	URLs related to spam are included in the category “questionable. This category also includes websites with illegal, immoral and offensive content.	
Sports/Recreation	Sports		
Suspicious	Insufficient Content or Questionable		
Technology/Internet	Computer and Internet Info		
Tobacco	Alcohol and Tobacco		
Translation	Translation		
Travel	Travel		
TV/Video Streams	Streaming Media		
Uncategorized	Unknown		Best Practice recommendation, Block “unknown” category
Vehicles	Motor Vehicles		

Violence/Hate/Racism	Extremism		Best Practice recommendation, Block “extremism” category
Weapons	Weapons		
Web Ads/Analytics	Web Advertisements		
Web Hosting	Web Hosting		

ROLL OUT URL CATEGORY ENFORCEMENT

- The recommended practice for deploying URL filtering in your organization is to first start with a “passive" URL filtering profile that will create log entries by employing the “alert” policy action on all categories in parallel with your existing Web Filter appliance.
  - On the Palo Alto Networks Firewall, create a new URL Filtering profile.
    - Select **Objects -> Security Profiles -> URL Filtering**.
    - Select the default profile and then click **Clone**. The new profile will be named **default-1**.
    - Select the **default-1** profile and rename it. For example, rename it to URL-Monitoring.
  - Configure the action for all categories to alert
    - In the section that lists all URL categories, select all categories.
    - To the right of the *Action* column heading, mouse over and select the down arrow and then select **Set Selected Actions** and choose **alert**.
    - Click OK to save the profile.



- After setting the “alert" action, you can monitor user web activity through URL Filtering Reports on both appliances for a few days or weeks to determine accuracy of the provided category mappings. Palo Alto Networks recommends to validate accuracy for top 1k websites seen by your organization.

    - Apply the URL Filtering profile to the security policy rule(s) that allows web traffic for users.
        - Select **Policies -> Security** and select the appropriate security policy to modify it.
        - Select the **Actions** tab and in the **Profile Setting** section, click the drop-down for **URL Filtering** and select the new profile.
        - Click **OK** to save.

    - View the URL filtering logs to determine all of the website categories that your users are accessing.

    - For information on viewing the logs and generating reports, see Monitor Web Activity .

        - Select **Monitor -> Logs -> URL Filtering**. A log entry will be created for any website that exists in the URL filtering database that is in a category that is set to any action other than **allow**

- In this procedure all categories will be set to alert, which will cause all websites traffic to be logged. This may potentially create a large amount of log files, so it is best to do this for initial monitoring purposes to determine the types of websites your users are accessing and compare URL Categories triggered.

- Collect all URL Category objects used in the Symantec Web Filter Policy Manager and map them into PAN-DB URL Categories using the provided URL Category Map after vetting them for accuracy using the above steps.

- After determining the categories that your organization allows users to access, set the policy action to “allow” for these URL Categories on the Next Generation Firewall. The firewall does not generate logs for traffic matching these URL Categories.

- You can then make decisions on the URL Categories that should be controlled according to Company Policy by setting the appropriate policy action to each of these categories in the URL Filtering profile(s). The Recommended actions column of the URL Category table in the previous section and the Best Practices section at the end of this document are provided to further assist you in making policy decisions.

- If possible, it is recommended to use a “slow roll” approach using USER-ID as described below when deploying these newly created URL Filtering profile(s) to Security Policies.

    - Clone an existing policy that allows web access and add an additional match criteria on User set to a single department [Eg: IT, Marketing, Engineering, etc].
    - Add the new URL Filtering Profile to this Security policy and move the policy above all policies that allow web access since Policy Rules are matched top down.
    - Monitor the above policy for usage and get feedback from the users belonging to the Group Object.
    - Incorporate changes as necessary to the URL Filtering Profile before adding it to all other applicable security policies.

BEST PRACTICE URL FILTERING PROFILE

- Attach a URL Filtering profile to all rules that allow access to web-based applications to protect against URLs that have been observed hosting malware or exploitive content.
- As a best practice, use PAN-DB URL filtering to prevent access to web content that is at high-risk for being malicious.
- These include command-and-control, copyright-infringement, dynamic-dns, extremism, malware, phishing, proxy-avoidance-and-anonymizers, unknown, and parked. The best practice URL Filtering profile sets all known dangerous URL categories to block.
- Failure to block these dangerous categories puts you at risk for exploit infiltration, malware download, command and control activity, and data exfiltration.
- In addition to blocking known bad categories, you should also alert on all other categories so that you have visibility into the sites your users are visiting.
- If you need to phase in a block policy, set categories to continue and create a custom response page to educate users on your acceptable use policies and alert them to the fact that they are visiting a site that may pose a threat.
- This will pave the way for you to outright block the categories after a monitoring period.

What if I can’t block all of the recommended categories?

If you find that users need access to sites in the blocked categories, consider creating an allow list for just the specific sites, if you feel the risk is justified. On categories you decide to allow, make sure you set up credential phishing prevention to ensure that users aren’t submitting their corporate credentials to a site that may be hosting a

phishing attack. Allowing traffic to a recommended block category poses the following risks:

malware—Sites known to host malware or used for command and control (C2) traffic. May also exhibit Exploit Kits.

phishing—Known to host credential phishing pages or phishing for personal identification.

dynamic-dns—Hosts and domain names for systems with dynamically assigned IP addresses and which are oftentimes used to deliver malware payloads or C2 traffic. Also, dynamic DNS domains do not go through the same vetting process as domains that are registered by a reputable domain registration company and are therefore less trustworthy.

unknown—Sites that have not yet been identified by PAN-DB, perhaps because they were just registered. However, oftentimes these are sites that are generated by domain generation algorithms and are later found to exhibit malicious behavior.

command-and-control—Command-and-control URLs and domains used by malware and/or compromised systems to surreptitiously communicate with an attacker's remote server to receive malicious commands or exfiltrate data.

copyright-infringement—Domains with illegal content, such as content that allows illegal download of software or other intellectual property. This category was introduced to enable adherence to child protection laws required in the education industry as well as laws in countries that require internet providers to prevent users from sharing copyrighted material through their service.

extremism—Websites promoting terrorism, racism, fascism or other extremist views discriminating people or groups of different ethnic backgrounds, religions or other beliefs. This category was introduced to enable adherence to child protection laws required in the education industry.

proxy-avoidance-and-anonymizers—URLs and services often used to bypass content filtering products.

parked—Domains registered by individuals, oftentimes later found to be used for credential phishing. These domains may be similar to legitimate domains, for example, pal0alto0netw0rks.com, with the intent of phishing for credentials or personal identify information. Or, they may be domains that an individual purchases rights to in hopes that it may be valuable someday, such as panw.net.

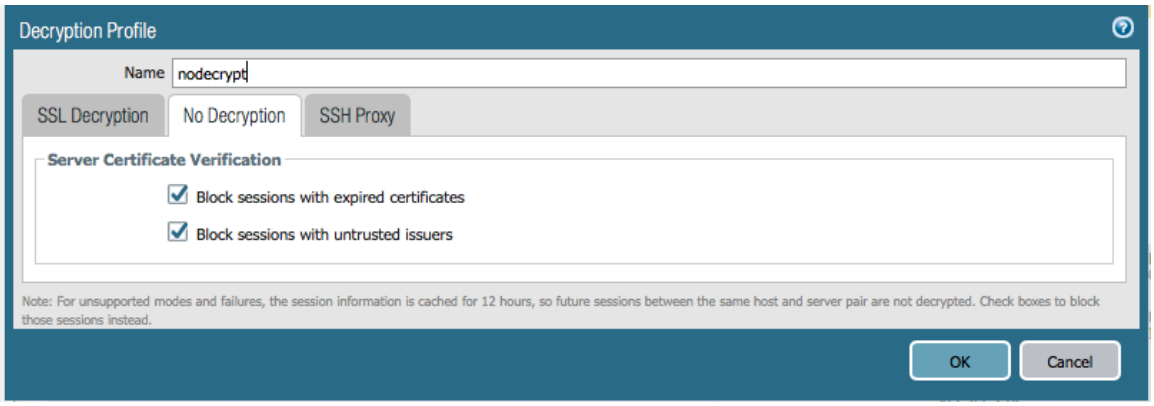
USE URL CATEGORIES TO DEFINE TRAFFIC TO DECRYPT OR NOT DECRYPT

Plan to decrypt as much traffic that is not private or sensitive as your firewall resources allow to reduce the attack surface by exposing and preventing encrypted threats. Understand local laws and regulations about the traffic you can legally decrypt and user notification requirements.

Please see documentation for *SSL Decryption deployment* and pre-requisites. The below steps describe Decryption policy definitions only.

1) Create a "*no-decrypt*" policy that will prevent any website mapping to the Recommended no decrypt URL Category list [*financial-services, health-and-medicine, government*] from being decrypted.

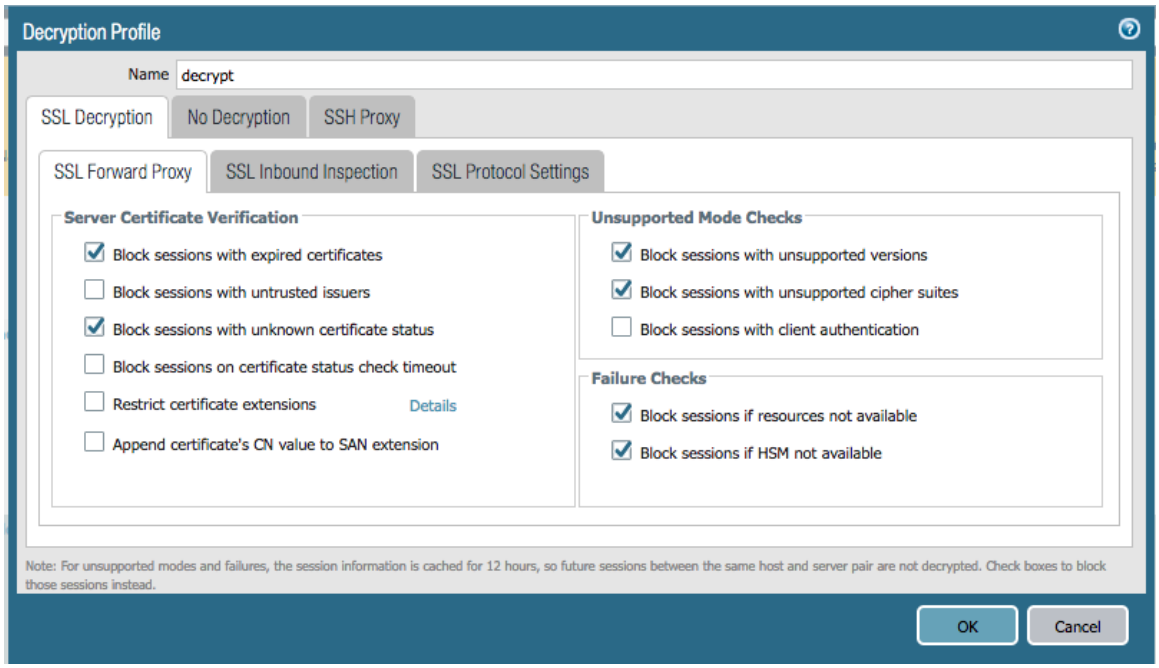
- Even while not using decryption it is a Recommended Best Practice to create a Decryption profile to block sessions with expired certificates or untrusted issuers and use it with your no-decrypt policy.
- Navigate to Objects -> Decryption Profile.
- Add a Profile called "nodecrypt" and check "Block sessions with expired certificates" and "Block sessions with untrusted issuers" under No Decryption tab.



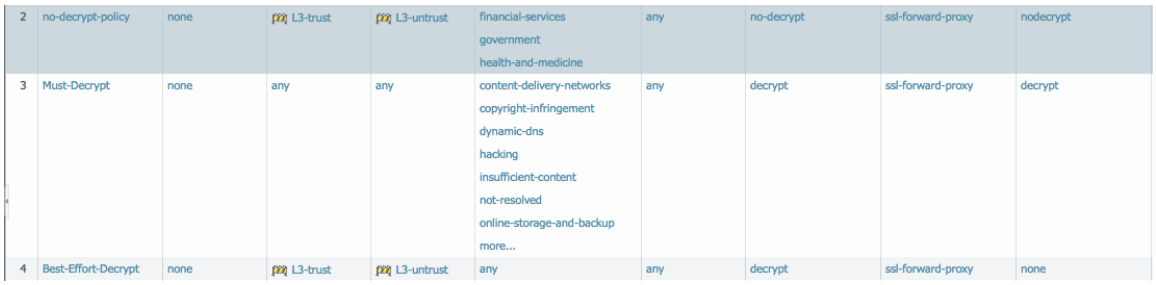
- Navigate to Policies -> Decryption and click Add.
- Enter a Name and optionally enter a Description and Tag(s).
- On the Source tab, enter the zone where the users are connected.
- On the Destination tab, enter the zone that is connected to the Internet.
- On the URL Category tab, click Add and select the financial-services, government, and health-and-medicine URL categories.
- On the Options tab, set the action to No Decrypt.
- Also set Decryption Profile to a "nodecrypt".
- Click OK to save the policy rule.

2) Create a "*must-decrypt*" policy that will decrypt any website mapping to the Recommended must decrypt URL Category list. [*Malware, Phishing, Unknown, Command-and-control, Copyright-infringement, Proxy-avoidance-and-anonymizers, Content-deliver-networks, Parked, Web-based-email, Social Networking, Personal-sites-blogs, Web-hosting, Insufficient-content, Not-resolved, Online-storage and backup, Hacking, Questionable, Dynamic DNS]*

- Navigate to Policies -> Decryption and click Add.
- Enter a Name and optionally enter a Description and Tag(s).
- On the Source tab, enter the zone where the users are connected.
- On the Destination tab, enter the zone that is connected to the Internet.
- On the Service/URL Category tab, enter all the Recommended URL Categories
- On the Options tab, set the action to Decrypt and the Type to SSL Forward Proxy.
- Use a decryption profile along with your decryption policy to block sessions that fail on SSL Decryption.
- Ensure that this must-decrypt policy is listed after the no-decrypt policy to ensure that rule processing occurs in the correct order.



3) Create a "best-effort-decrypt" policy that will decrypt all other traffic using the same steps as above but with URL Categories set to Any and a decryption profile with options under Failure Checks section unchecked. This ensures that sessions are allowed even if SSL Decryption fails.



2	no-decrypt-policy	none	L3-trust	L3-untrust	financial-services government health-and-medicine	any	no-decrypt	ssl-forward-proxy	nodecrypt
3	Must-Decrypt	none	any	any	content-delivery-networks copyright-infringement dynamic-dns hacking insufficient-content not-resolved online-storage-and-backup more...	any	decrypt	ssl-forward-proxy	decrypt
4	Best-Effort-Decrypt	none	L3-trust	L3-untrust	any	any	decrypt	ssl-forward-proxy	none

With these three decrypt policies in place, any traffic destined for the financial-services or health-and-medicine or government URL categories will not be decrypted. All other traffic will be decrypted.

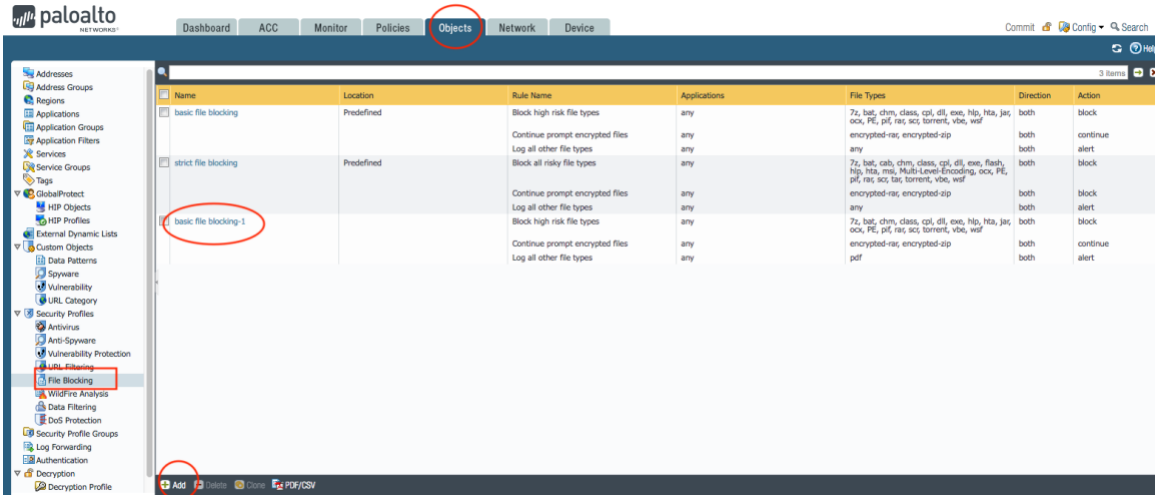
URL FILTERING USE CASES

Case-1: Policy to block download of High Risk file types from certain categories [Decryption + URL Filtering + File-Blocking + Threat Prevention]

1) Please refer to *SSL Decryption Best Practices* to enable SSL Decryption. This is necessary to accurately inspect, classify and block encrypted traffic.

2) Create a File Blocking Security Profile

- The default basic file blocking profile can be used or we can create a custom profile based on the basic file blocking profile
- Select Objects -> Security Profiles -> File Blocking
- Select “basic file blocking” or “strict file blocking” profile and click Clone
- Rename the profile and edit to select appropriate file types for Block, Continue and Alert actions based on your Company Policy or use the default profile provided.
- Click OK



3) Create the security policy rule that will block risky file downloads from specific categories

- This rule must precede other rules because, it is a specific rule. More specific rules must precede other rules.
- Select Policies -> Security and click Add.
- Enter a Name and optionally a Description and Tag(s).
- On the Source tab add the zone where the users are connected.
- On the Destination tab, select the zone that is connected to the Internet.
- On the Service/URL Category tab Add the specific categories from which risky file download needs to be blocked. [Web-hosting, Personal-sites-blogs, Social Networking, Peer-to-Peer, Online-storage and backup, Web-based-email, Copyright-infringement, Shareware-and-freeware].
- On the Actions tab, select Action “Allow” and add the default profiles for Antivirus, Vulnerability Protection, Anti-Spyware, URL Filtering and the newly created File Blocking profile.
- Click OK to save the security profile.
- Commit the Configuration.

4) With this security policy rule in place, any user trying to download executable files or other risky files from Dropbox, Box or any free Software download websites will be blocked.

5) Because this rule will also allow access to the Internet, threat prevention profiles are applied to the rule, so traffic that matches the policy will be scanned for threats. This is important because the allow rule is terminal and will not continue to check other rules if there is a traffic match.

Case-2: Policy to Control Web Access [Decryption + User-ID + App-ID + URL Filtering + Data Filtering + Threat Prevention]

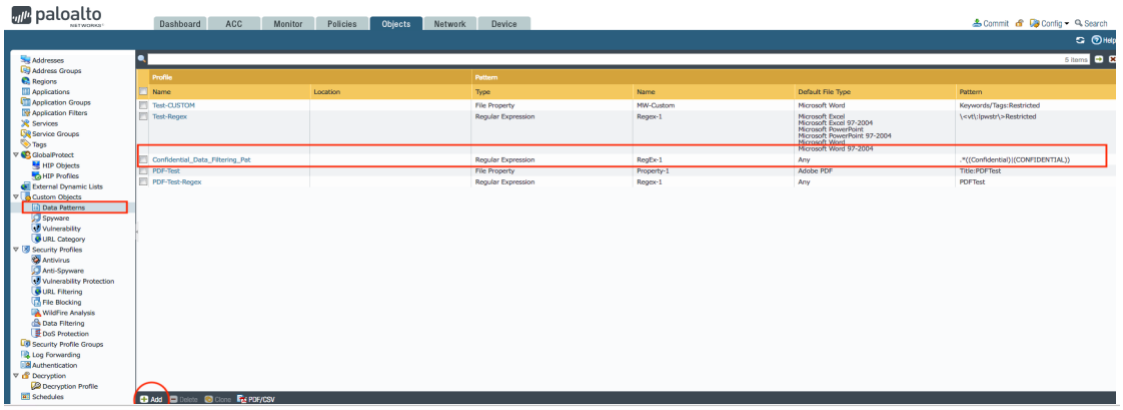
In this use case, users belonging to the Marketing group for example, have access to Box for collaboration but not to any of the other "online-storage-and backup" vendors. All other users are blocked from all "online-storage-and-backup" applications. The company policy also states that documents marked "Confidential" should not be shared on Box by the Marketing Group.

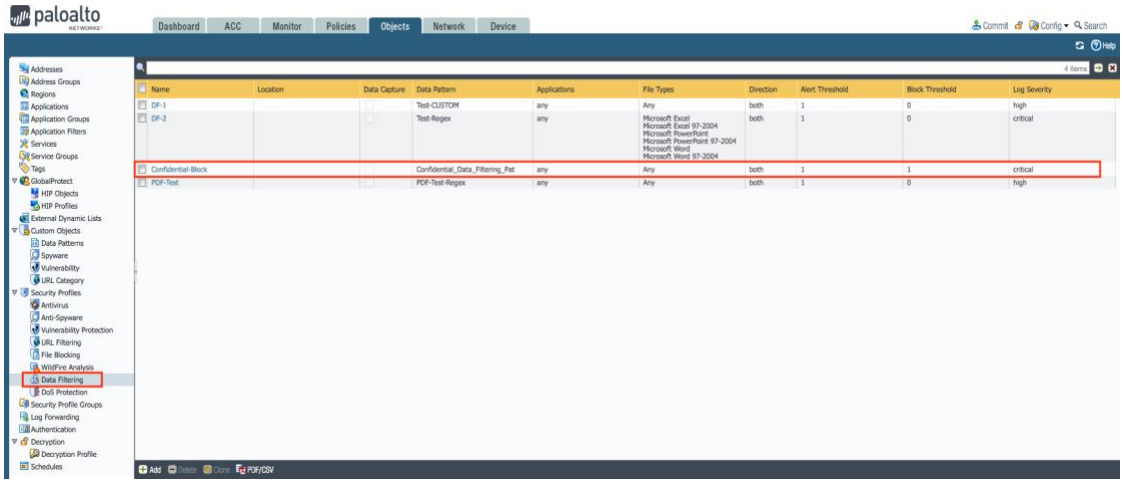
1) Please refer to the *SSL Decryption Best Practices* to enable SSL Decryption. This is necessary to accurately inspect, classify and block encrypted traffic.

2) Create a security policy that will block all users from accessing "online-backup-and-storage" Applications. This can be done either using a specific security policy or as part of a URL Filtering Profile that would be included in all security policies that allow internet access.
   - Select Policies > Security and click Add.
   - Enter a Name and optionally a Description and Tag(s).
   - On the Source tab add the zone where the users are connected.
   - On the Destination tab, select the zone that is connected to the Internet.
   - On the Service/URL Category tab, click Add and add the online-storage-and-backup category.
   - On the Actions tab, select Action Deny
   - Click OK to save the security profile.

3) Create a Data Pattern Custom Object and add it to a Data Filtering Security Profile

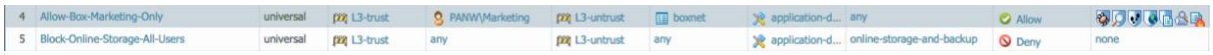
   - Select Objects -> Custom Objects -> Data Patterns and *click Add*
   - Select Pattern Type as "Regular Expression"
   - Select File Type as "Any"
   - Set Data Pattern to ".*((Confidential)|(CONFIDENTIAL))"
   - Click OK
   - Select Objects -> Security Profiles -> Data Filtering and *click Add*
   - Set the Data Pattern Field to the above created object.
   - Set Alert/Block Threshold to 1 and Log Severity to Critical and Click OK.





4) Create the security policy that will allow Marketing group to access Box Application. Because this allow rule will also allow access to the Internet, threat prevention profiles are applied to the rule, so traffic that matches the policy will be scanned for threats.

- This rule must precede other rules because it is more specific than the other policies.
- Select Policies > Security and click Add.
- Enter a Name and optionally a Description and Tag(s).
- On the Source tab add the zone where the users are connected.
- On the User tab in the Source User section click Add.
- Select the directory group that contains your marketing users.
- On the Destination tab, select the zone that is connected to the Internet.
- On the Applications tab, click Add and add the boxnet App-ID signature.
- On the Actions tab, add the default profiles for Antivirus, Vulnerability Protection and Anti-Spyware.
- Also add the Data Filtering Profile that was created in the previous step.
- Click OK to save the security profile and commit the configuration.



5) With these policies in place, any user who is part of the Marketing group will have full access to Box application and any user that is not part of the Marketing group will be blocked from all online-storage-and-backup websites.

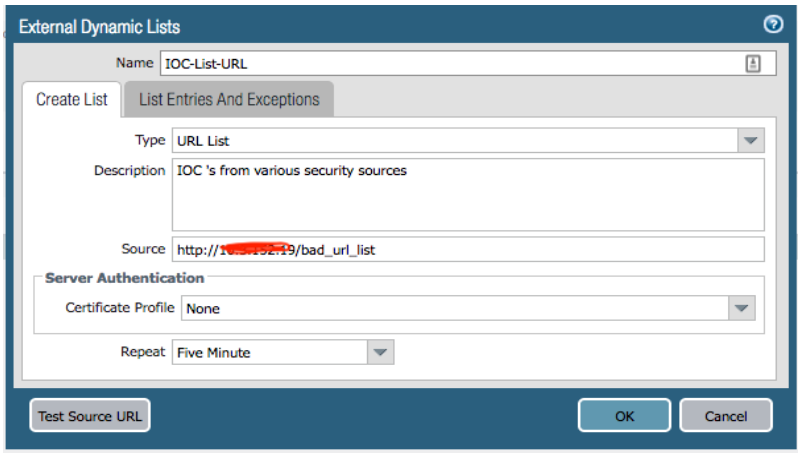
6) Additionally, all files that are shared on Box will be scanned for the keyword "Confidential" and blocked if found. An entry will also be logged under Monitor -> Logs -> Data Filtering.

Case-3: Subscribe to an external malicious URL feed [URL Filtering + External Dynamic Lists]

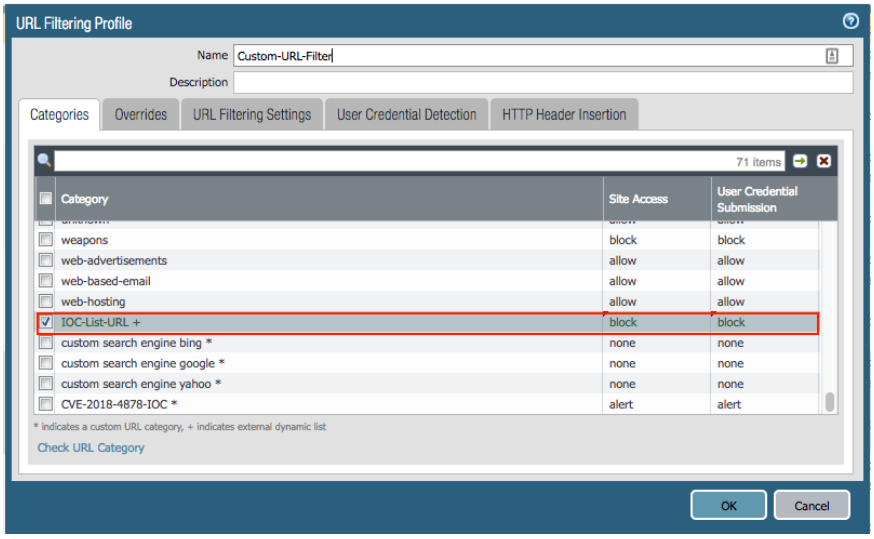
In this use case, Administrator wants the Firewall to ingest an external feed that provides IOC's or Indicators of Compromise in the form of URL's. This dynamic list of URL's has to be continuously updated in policy and blocked by Palo Alto Networks Next Generation Firewall without any manual intervention.

To protect your network from new sources of threat or malware, you can use External Dynamic List in URL Filtering profiles to block or allow, or to define granular actions such as continue, alert, or override for URLs, before you attach the profile to a Security policy rule. Unlike the allow list, block list, or a custom URL category on the firewall, an external dynamic list gives you the ability to update the list without a configuration change or commit on the firewall.

- Navigate to Objects -> External Dynamic Lists
- Click Add
- Sect Type "URL List"
- Enter Source [this could be a web server hosting a file of URL's]
- Select appropriate Frequency of checks using the Repeat field.
- Click OK



- Navigate to Objects -> Security Profiles -> URL Filtering
- Select appropriate URL Filtering Profile
- The above created EDL should be seen as a *custom category*.
- Assign appropriate policy action to this category
- This URL filtering profile can now be added to a security policy(s)



With this security policy in place, any user attempting to connect to websites part of the URL feed will be blocked. This URL list is dynamically updated by the Firewall without any commit required by the Administrator. Any attempt to connect to these URL's is also logged under Monitor -> Logs -> URL Filtering.

USEFUL RESOURCES

1. PAN-DB URL Categorization Workflow
2. Monitor Web Activity
3. Configure URL Filtering
4. Customize URL Filtering Response Pages
5. Create Custom URL Categories
6. Use an External Dynamic List in a URL Filtering Profile
7. Safe Search Enforcement
8. Prevent Credential Phishing
9. Troubleshoot URL Filtering
10. Incorrect Categorization
11. SSL Decryption Overview