

CISCO WEB SECURITY

- Setting up Policies



Handy Putra

October 2017

WEB SECURITY POLICIES OVERVIEW

When the user creates a web request the configured Web Security Appliance intercepts the requests and manages the process of which the request travels to get to its final outcome, be that accessing a particular web site, an email or even accessing an online application.

In configuring the Web Security Appliance policies are created to define the criteria and actions of requests made by the user.

Policies are the means by which the Web Security Appliance identifies and controls web requests. When a client sends a web request to a server, the Web Proxy receives the request, evaluates it, and determines to which policy it belongs. Actions defined in the policy are then applied to the request.

The Web Security Appliance uses multiple policy types to manage different aspects of web requests.

Policy types might fully manage transactions by themselves or pass transactions along to other policy types for additional processing. Policy types can be groups by the functions they perform, such as access, routing, or security.

AsyncOS evaluates transactions based on policies before it evaluates external dependencies to avoid unnecessary external communication from the appliance. For example, if a transaction is blocked based on a policy that blocks uncategorized URLs, the transaction will not also fail based on a DNS error.



WEB SECURITY POLICIES BEST PRACTICES

- When you define multiple membership criteria, the client request must meet all criteria to match the policy ("AND" condition).
- If you want to use Active Directory user objects to manage web requests, do not use primary groups as criteria. Active Directory user objects do not contain the primary group.
- Place policies with unique criteria on the top of general policy (read from top to bottom manner).
- Of the policy-configuration components, able to specify the "Warn" option only with URL Filtering.
- Not more than 25 – 30 Policies to avoid performance issues.



Most Common Web Security Policy Types

Access Policies



Decryption Policies



Custom Policy Elements

Custom and External URL Categories





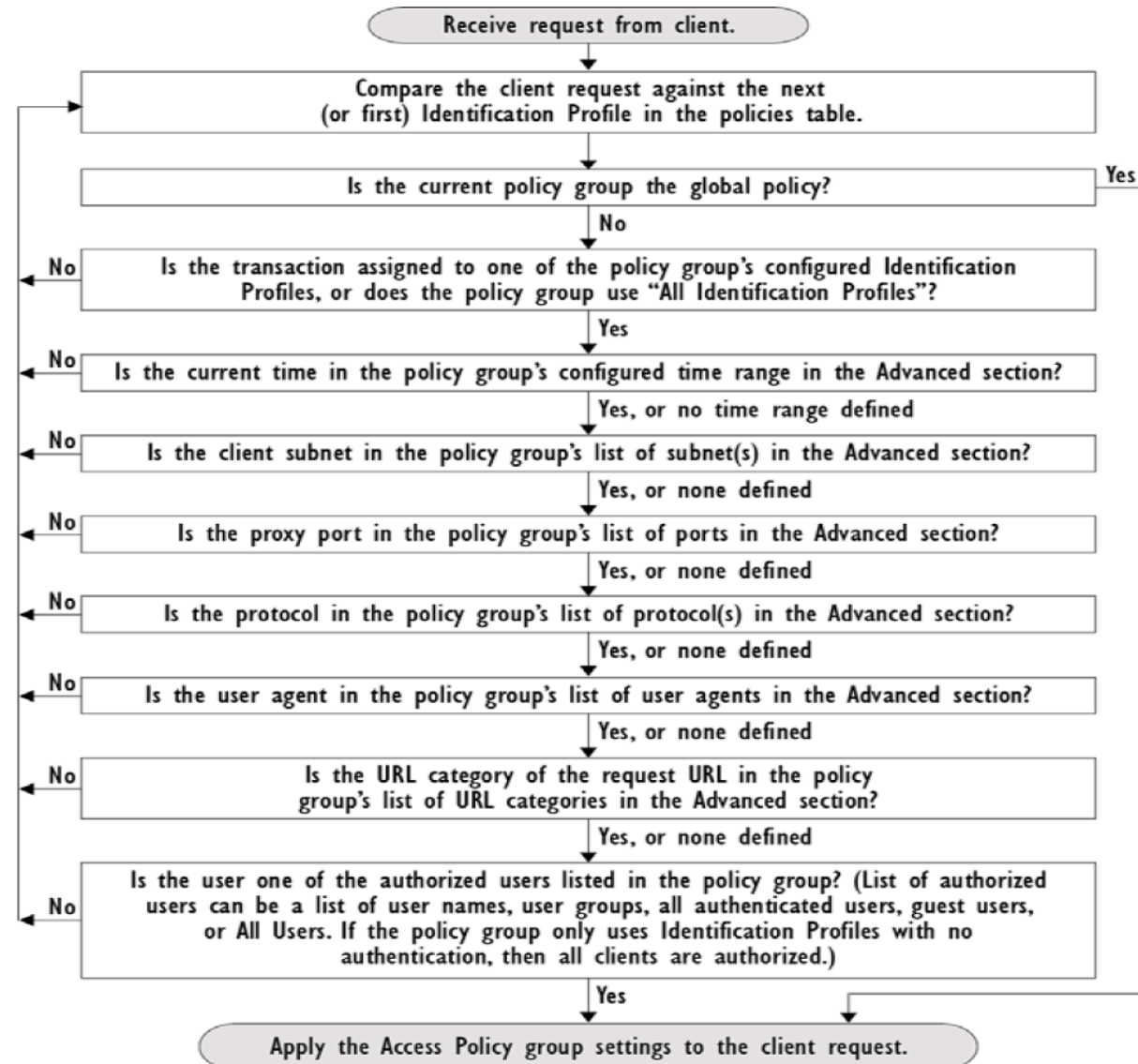
Access Policy

- Policies to Block, allow or redirect inbound HTTP, FTP, and decrypted HTTPS traffic.
- Access policies also manage inbound encrypted HTTPS traffic if the HTTPS proxy is disabled.
- Policies being read top to bottom and left to right manners and using 'AND' conditions to meet the conditions of policy.





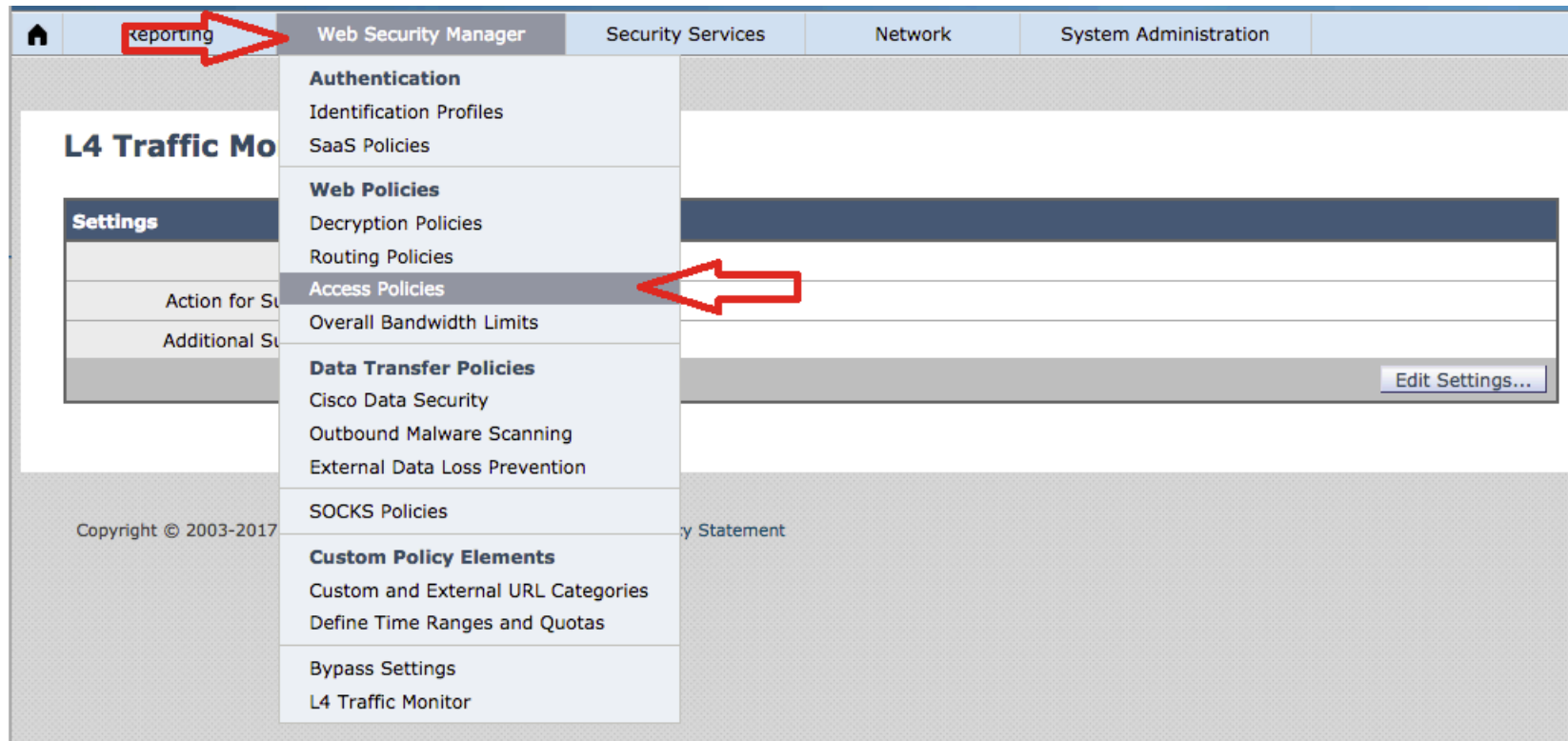
Access Policy Workflows.





Access Policy cont.

- In the WEB GUI of WSA, go to 'Web Security Manager' tab then go to 'Access Policies'





Access Policy cont.

- Click 'Add Policy' button to add new Access Policy

Access Policies

Policies

[Add Policy...](#)

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
	Global Policy Identification Profile: All	No blocked items	Monitor: 85 Allow: 1	Monitor: 364	No blocked items	Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled	

[Edit Policy Order...](#)





Access Policy cont.

- Give the new Access Policy a Name
- Give the new Access Policy a Description
- Set the position of the new Access Policy – “Insert Above”
- Select the Identification Profiles and Users:

All Identification Profiles – Appliance will match the conditions automatically by comparing all Identification Profiles from top to bottom manners.

Select One or More Identification Profiles – Select which Identification Profile to use for this policy

- Select Identification Profile drop down box to select the Identity to use
- Click on “Submit” button





Access Policy cont.

Access Policy: Add Group

Policy Settings

☒ **Enable Policy**

Policy Name: ?

(e.g. my IT policy)

Description:

Insert Above Policy:

1 (Global Policy)

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

Select One or More Identification Profiles

Identification Profile

Select Identification Profile...

✓ Global Identification Profile

Authorized Users and Groups

No authentication required

Advanced

Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Protocols: None Selected

Proxy Ports: None Selected

Subnets: None Selected

Time Range: No Time Range Definitions Available
(see Web Security Manager > Defined Time Ranges)

URL Categories: None Selected

User Agents: None Selected

Cancel



Access Policy Advanced.

"Advanced" section:

- **Protocols** - Select the protocols to which this policy will apply. All others means any protocol not selected. If the associated identification profile applies to specific protocols, this policy applies to those same protocols.
- **Proxy Ports** - Applies this policy only to traffic using specific ports to access the web proxy. Enter one or more port numbers, separating multiple ports with commas. For explicit forward connections, this is the port configured in the browser. For transparent connections, this is the same as the destination port. If the associated **identification profile** applies only to specific proxy ports, you cannot enter proxy ports here.
- **Subnets** - Applies this policy only to traffic on specific subnets. Select Specify subnets and enter the specific subnets, separated by commas. Leave Use subnets from selected Identities selected if you do not want additional filtering by subnet. If the associated identity applies to specific subnets, you can further restrict the application of this policy to a subset of the addresses to which the identity applies.





Access Policy Advanced cont.

- **Time Range** - You can apply time ranges for policy membership:
 - Time Range – Choose a previously defined time range
 - Match Time Range – Use this option to indicate whether this time range is inclusive or exclusive. In other words, whether to match only during the range specified, or at all times except those in the specified range.
- **URL Categories** - You can restrict policy membership by specific destinations (URLs) and by categories of URLs. Select all desired custom and predefined categories
- **User Agents** - You can select specific user agents, and define custom agents using regular expressions, as part of membership definition for this policy.
 - Common User Agents
 - Browsers – Expand this section to select various Web browsers.
 - Others – Expand this section to select specific non-browser agents such as application updaters.
 - Custom User Agents – You can enter one or more regular expressions, one per line, to define custom user agents.
 - Match User Agents – Use this option to indicate whether these user-agent specifications are inclusive or exclusive. In other words, whether membership definition includes only the selected user agents, or specifically excludes the selected user agents





Access Policy cont.

Once new Access Policy has been created, proceed in configuring the new policy left to right manner



Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	accesspolicy.ap Identification Profile: Global All identified users	(global policy)	(global policy)	(global policy)	(global policy)	(global policy)	
	Global Policy Identification Profile: All	No blocked items	Monitor: 85 Allow: 1	Monitor: 364	No blocked items	Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled	

Click on the table's name above to configure each element in the new policy created.
For example: click on the "Protocol and User Agents"






Access Policy: Protocol and User Agents.


- Protocols and User Agents

Access Policies: Protocols and User Agents: Global Policy


Edit Protocols and User Agents Settings

Define Custom Settings 

Protocol Controls

Block Protocols:	<input type="checkbox"/> FTP over HTTP <input type="checkbox"/> HTTP <input type="checkbox"/> Native FTP <small><i>Note: Blocking of HTTPS is not available in Access policies when the HTTPS proxy is enabled. If the HTTPS proxy is enabled, use Decryption policies to control HTTPS access.</i></small>
HTTP CONNECT Ports: 	<input type="text" value="8080, 21, 443, 563, 8443, 20"/> <small>Enter 1-65535 to allow all ports via HTTP CONNECT. Leave field blank to block all ports.</small>

Custom User Agents

Example User Agent Patterns 

Block Custom User Agents:	<div></div> <small>(Enter any regular expression, one regular expression per line, to block user agents.)</small>
---------------------------	--

Cancel Submit



■ Protocols and User Agents

The next option in this section is to “Block Custom User Agents” using regular expression to identify the user agents such as: “Mozilla/. * Gecko/. * Firefox/” to match all Firefox browser versions.

Access Policies

Success — The policy group "accesspolicy.ap" was added.

Policies							
Add Policy...							
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	accesspolicy.ap Identification Profile: Global All identified users	(global policy)	(global policy)	(global policy)	(global policy)	(global policy)	
	Global Policy Identification Profile: All	No blocked items	Monitor: 85 Allow: 1	Monitor: 364	No blocked items	Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled	
Edit Policy Order...							



Access Policy: URL Filtering.

Access Policies: URL Filtering: Global Policy

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Block 	Redirect 	Allow ? 	Monitor 	Warn ? 	Quota-Based 	Time-Based
		Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
test	Custom (Local)						—	—
<input type="text" value="Select Custom Categories..."/>								

Predefined URL Category Filtering					
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.					
Category	Block 	Monitor 	Warn ? 	Quota-Based 	Time-Based
	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Adult				—	—
Advertisements				—	—
Alcohol				—	—
Arts				—	—
Astrology				—	—
Auctions				—	—
Business and Industry				—	—
Chat and Instant Messaging				—	—
Cheating and Plagiarism				—	—
Child Abuse Content				—	—
Computer Security				—	—
Computers and Internet				—	—
DIY Projects				—	—
Dating				—	—



Access Policy: URL Filtering cont.

AsyncOS for Web allows you to configure how the appliance handles a transaction based on the URL category of a particular HTTP or HTTPS request.

Using a predefined category list, you can choose to block, monitor, warn, or set quota-based or time-based filters.

You can also create custom URL categories and then choose to block, redirect, allow, monitor, warn, or apply quota-based or time-based filters for Websites in the custom categories

In addition, you can add exceptions to blocking of embedded or referred content.

Note:

- Monitor action will scan the traffic further and apply further scanning such as application, objects and ant-malware and reputation scanning (direction is left to right).
- Redirect action - Web Proxy does not allow the connection to the originally requested destination server and instead connects to a different specified URL,

Click on the “Custom Categories” button below on how to create custom and external URL categories

Custom and External URL Categories





Access Policy: Applications.

Access Policies: Applications Visibility and Control: Global Policy

Default Actions for Application Types	
Application Types	Default Action for Type
Blogging	
Collaboration	
Enterprise Applications	
Facebook	Bandwidth Limit:
File Sharing	
Games	
Google+	
Instant Messaging	
Internet Utilities	
iTunes	
LinkedIn	
Media	Bandwidth Limit:
Myspace	
Office Suites	
Presentation / Conferencing	
Proxies	
Social Networking	
Software Updates	
Webmail	





Access Policy: Applications cont.

The Application Visibility and Control engine (AVC) engine is an Acceptable Use policy component that inspects Web traffic to gain deeper understanding and control of Web traffic used for applications.

The appliance allows the Web Proxy to be configured to block or allow applications by Application Types, and by individual applications.

You can also apply controls to particular application behaviors, such as file transfers, within a particular application

To Edit the Application Settings, Click the “+” sign to expand each Applications Categories and set the action for each application.





Access Policy: Applications cont.

Edit Applications Settings

Browse Application Types

Applications Info

To identify some applications, inspection of HTTPS content may be required. For best efficacy, enable the HTTPS Proxy, then select the option that enables decryption for application visibility and control (see Security Services > HTTPS Proxy).

Applications	Settings
Edit all...	
File Sharing	56 Monitor
Edit all...	
Games	
Evony	<div>Set action for application Evony<ul style="list-style-type: none"><input checked="" type="radio"/> Use Setting from Type (Monitor)<input type="radio"/> Monitor<input type="radio"/> Block<div>Cancel Apply</div></div>
Game Center	Use Default for Type (Monitor)
games.mail.ru	Use Default for Type (Monitor)
Hangame.co.jp	Use Default for Type (Monitor)
Pogo	Use Default for Type (Monitor)
Wii	Use Default for Type (Monitor)
Edit all...	





Access Policy: Objects.

Access Policies: Objects: Global Policy

Edit Objects Blocking Settings

Define Custom Objects Blocking Settings

Objects Blocking Settings

Object Size

HTTP/HTTPS Max Download Size:

☐ 0 MB ☒ No Maximum

FTP Max Download Size:

☐ 0 MB ☒ No Maximum

Block Object Type

Object and MIME Type Reference

☒ Archives

☐ ARC

☐ ARJ

☐ BinHex

☐ LHARC

☐ StuffIt

☒ Inspectable Archives

☒ Document Types

☒ Executable Code

☒ Installers

☒ Media

☒ P2P Metatables

☒ Web Page Content

☒ Miscellaneous




Access Policy: Objects cont.

These options let you configure the Web Proxy to block file downloads based on file characteristics, such as file size, file type, and MIME type.

An object is, generally, any item that can be individually selected, uploaded, downloaded and manipulated

You can also block custom MIME Types in below configuration. For example: audio/x-mpeg3 for Mpeg file extension or audio/* for any audio MIME type.

Custom MIME Types	
Object and MIME Type Reference 	
Block Custom MIME Types:	<div></div> <p><i>(Enter multiple entries on separate lines. Example: audio/x-mpeg3 or audio/* are valid entries.)</i></p>





Access Policy: Anti-Malware and Reputation.

Access Policies: Anti-Malware and Reputation Settings: Global Policy

Web Reputation Settings

Web Reputation Filters will automatically block transactions with a low Web Reputation score. For transactions with a higher Web Reputation score, scanning will be performed using the services selected by Adaptive Scanning.

If Web Reputation Filtering is disabled in this policy, transactions will not be automatically blocked based on low Web Reputation Score. Blocking of sites that contain malware or other high-risk content is controlled by the settings below.

☒ Enable Web Reputation Filtering

Advanced Malware Protection Settings

☒ Enable File Reputation Filtering and File Analysis

File Reputation Filters will identify transactions containing known malicious or high-risk files. Files that are unknown may be forwarded to the cloud for File Analysis.

	Monitor	Block
File Reputation		
Known Malicious and High-Risk Files		





Access Policy: Anti-Malware and Reputations cont

Cisco DVS Anti-Malware Settings		
Sophos is currently disabled globally.		
<input checked="" type="checkbox"/> Enable Suspect User Agent Scanning <input checked="" type="checkbox"/> Enable Anti-Malware Scanning (Webroot, McAfee)		
Malware Categories	Monitor 	Block
	Select all	Select all
Adware	✓	
Browser Helper Object	✓	
Commercial System Monitor	✓	
Dialer	✓	
Generic Spyware	✓	
Hijacker	✓	
Other Malware	✓	
Phishing URL	✓	
System Monitor	✓	
Trojan Downloader	✓	
Trojan Horse	✓	
Trojan Phisher	✓	
Virus	✓	
Worm	✓	
Other Categories	Monitor 	Block
	Select all	Select all
Encrypted File	✓	
Outbreak Heuristics		✓
Suspect User Agents	✓	
Unscannable	✓	





Access Policy: Anti-Malware and Reputations cont

Web reputation filters allow for a web-based reputation score to be assigned to a URL to determine the probability of it containing URL-based malware.

Anti-malware scanning identifies and stops web-based malware threats.

Advanced Malware Protection identifies malware in downloaded files.

The Anti-Malware and Reputation policy inherits global settings respective to each component.

Within Security Services > Anti-Malware and Reputation, malware categories can be customized to monitor or block based on malware scanning verdicts and web reputation score thresholds can be customized.

Malware categories can be further customized within a policy.

- Note: when the action set to “Monitor”, Cisco Web Security Appliance will log the threat information in the logs when threat is found, however will not blocks it.





Decryption Policy.

Decryption policies define the handling of HTTPS traffic within the Web proxy:

- When to decrypt HTTPS traffic.
- How to handle requests that use invalid or revoked security certificates.
- Policies being read top to bottom and left to right manners and using 'AND' conditions to meet the conditions of policy

You can create decryption policies to handle HTTPS traffic in the following ways:

- Pass through encrypted traffic.
- Decrypt traffic and apply the content-based access policies defined for HTTP traffic. This also makes malware scanning possible.
- Drop the HTTPS connection.
- Monitor the request (take no final action) as the Web proxy continues to evaluate the request against policies that may lead to a final drop, pass through, or decrypt action.





Decryption Policy cont.

Best Practices:

- Create fewer, more general Decryption Policy groups that apply to all users or fewer, larger groups of users on the network.
- If need to apply more granular control to decrypted HTTPS traffic, use more specific Access Policy groups.
- If need to block certain HTTPS sites or categories and need to display the Web Proxy block page, recommend to either enable the “Decrypt for End-User Notification” option from the Security Services -> HTTPS Proxy page or set the Decryption policy to “decrypt” and blocks it from Access Policy.
- Not more than 25 – 30 Policies to avoid performance issues.





Decryption Policy cont.

Requirements:

- HTTPS Proxy is enabled (Security Services -> HTTPS Proxy)
- Using valid Root Certificates (not server certificate)

Cisco S300V Web Security Virtual Appliance

Reporting Web Security Manager **Security Services** Network System Administration

HTTPS Proxy

HTTPS Proxy Settings

HTTPS Proxy:	E
HTTPS Ports to Proxy:	4
Root Certificate and Key for Signing:	U

Decryption Options

Decrypt for End-User Notification:	Enabled
Decrypt for End-User Acknowledgement:	Enabled
Decrypt for Application Detection:	Disabled

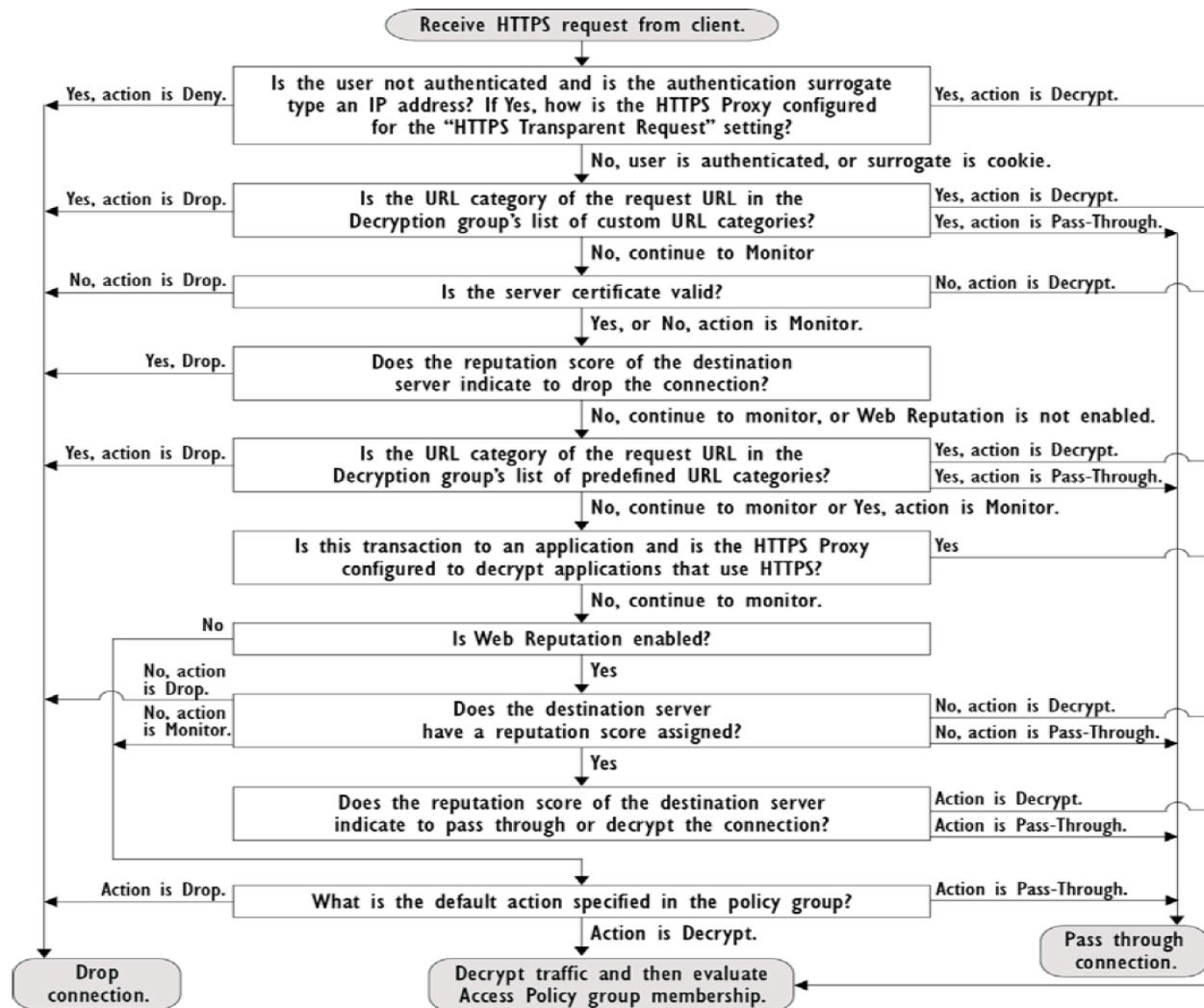
Invalid Certificate Options

Invalid Certificate Handling:	Expired: Monitor
	Mismatched Hostname: Monitor
	Unrecognized Root Authority / Issuer: Drop
	Invalid Signing Certificate: Drop
	Invalid Leaf Certificate: Drop
	All other error types: Drop



Decryption Policy cont.

Workflow:





Decryption Policy cont.

- In the WEB GUI of WSA, go to 'Web Security Manager' tab then go to 'Decryption Policies'

The screenshot shows the Cisco S300V Web Security Virtual Appliance GUI. The top navigation bar includes tabs for Reporting, Web Security Manager, Security Services, Network, and System Administration. The 'Web Security Manager' tab is selected, and a dropdown menu is open, showing various policy categories. The 'Decryption Policies' option is highlighted. On the left, a 'Policies' sidebar shows 'Global Policy Identification' selected. The main content area displays a table of decryption policies.

ng	Web Reputation	Default Action	Delete
5	Enabled	Decrypt	

Copyright © 2003-2017





Decryption Policy cont.

- Click 'Add Policy' button to add new 'Decryption Policy'

Decryption Policies

Policies					
Add Policy...					
Order	Group	URL Filtering	Web Reputation	Default Action	Delete
	Global Policy Identification Profile: All	Monitor: 85	Enabled	Decrypt	
Edit Policy Order...					





Decryption Policy cont.

- Give the new Access Policy a Name
- Give the new Access Policy a Description
- Set the position of the new Access Policy – “Insert Above”
- Select the Identification Profiles and Users:

All Identification Profiles – Appliance will match the conditions automatically by comparing all Identification Profiles from top to bottom manners.

Select One or More Identification Profiles – Select which Identification Profile to use for this policy

- Select Identification Profile drop down box to select the Identity to use
- Click on “Submit” button





Decryption Policy cont.

Decryption Policy: Add Group

Policy Settings

☒ **Enable Policy**

Policy Name: ?

(e.g. my IT policy)

Description:

Insert Above Policy:

1 (Global Policy) ▾

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

All Identification Profiles

✓ Select One or More Identification Profiles

Identification Profile

Global Identification Profile ▾

Authorized Users and Groups

No authentication required

Add Identification Profile

Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

Advanced

Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Proxy Ports: None Selected

Subnets: None Selected

Time Range: No Time Range Definitions Available
(see Web Security Manager > Defined Time Ranges)

URL Categories: None Selected

User Agents: None Selected

Cancel

Submit



Decryption Policy Advanced.

"Advanced" section:

- **Proxy Ports** - Applies this policy only to traffic using specific ports to access the web proxy. Enter one or more port numbers, separating multiple ports with commas. For explicit forward connections, this is the port configured in the browser. For transparent connections, this is the same as the destination port. If the associated **identification profile** applies only to specific proxy ports, you cannot enter proxy ports here.
- **Subnets** - Applies this policy only to traffic on specific subnets. Select Specify subnets and enter the specific subnets, separated by commas. Leave Use subnets from selected Identities selected if you do not want additional filtering by subnet. If the associated identity applies to specific subnets, you can further restrict the application of this policy to a subset of the addresses to which the identity applies.





Decryption Policy Advanced cont.

- **Time Range** - You can apply time ranges for policy membership:
 - Time Range – Choose a previously defined time range
 - Match Time Range – Use this option to indicate whether this time range is inclusive or exclusive. In other words, whether to match only during the range specified, or at all times except those in the specified range.
- **URL Categories** - You can restrict policy membership by specific destinations (URLs) and by categories of URLs. Select all desired custom and predefined categories
- **User Agents** - You can select specific user agents, and define custom agents using regular expressions, as part of membership definition for this policy.
 - Common User Agents
 - Browsers – Expand this section to select various Web browsers.
 - Others – Expand this section to select specific non-browser agents such as application updaters.
 - Custom User Agents – You can enter one or more regular expressions, one per line, to define custom user agents.
 - Match User Agents – Use this option to indicate whether these user-agent specifications are inclusive or exclusive. In other words, whether membership definition includes only the selected user agents, or specifically excludes the selected user agents





Decryption Policy cont.

- Once new Decryption Policy has been created, proceed in configuring the new policy left to right manner

Decryption Policies



Policies					
Add Policy...					
Order	Group	URL Filtering	Web Reputation	Default Action	Delete
1	decryptionpolicy.dp Identification Profile: Global All identified users	(global policy)	(global policy)	(global policy)	
	Global Policy Identification Profile: All	Monitor: 85	Enabled	Decrypt	
Edit Policy Order...					

Click on the table's name above to configure each element in the new policy created. For example: click on the "URL Filtering"





Decryption Policy: URL Filtering.

Decryption Policies: URL Filtering: decryptionpolicy.dp

Custom and External URL Category Filtering

No Custom Categories are included for this Policy.

Select Custom Categories...

Predefined URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Use Global Settings	Override Global Settings					
		Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
		Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Adult						—	—
Advertisements						—	—
Alcohol						—	—
Arts						—	—
Astrology						—	—
Auctions						—	—
Business and Industry						—	—
Chat and Instant Messaging						—	—
Cheating and Plagiarism						—	—
Child Abuse Content						—	—
Computer Security						—	—
Computers and Internet						—	—
DIY Projects						—	—
Dating						—	—



Decryption Policy: URL Filtering cont.

The appliance can perform any of the following actions on an HTTPS connection request:

- Monitor

Monitor is an intermediary action that indicates the Web Proxy should continue evaluating the transaction against the other control settings to determine which final action to ultimately apply.

- Drop

The appliance drops the connection and does not pass the connection request to the server. The appliance does not notify the user that it dropped the connection.

- Pass Through

The appliance passes through the connection between the client and the server without inspecting the traffic content.

However, with a standard pass-through policy, the WSA does check the validity of the requested server by initiating an HTTPS handshake with the server. This validity check includes server certificate validation. If the server fails the check, the transaction is blocked.

You can skip validation checks for specific sites by configuring policies that incorporate custom categories which include these sites, thereby indicating that these sites are trustworthy—these sites are passed through without validity checks. Exercise care when configuring policies that allow validity checks to be skipped.





Decryption Policy: URL Filtering cont.

■ Decrypt

The appliance allows the connection, but inspects the traffic content. It decrypts the traffic and applies Access Policies to the decrypted traffic as if it were a plain-text HTTP connection. By decrypting the connection and applying Access Policies, you can scan the traffic for malware.

Click on the “Custom Categories” button below on how to create custom and external URL categories

Custom and External URL Categories





Decryption Policy: Web Reputation.

Decryption Policies: Reputation Settings: decryptionpolicy.dp

Web Reputation Settings

- Use Global Web Reputation Settings
- ✓ Define Custom Web Reputation Settings
- Disable Web Reputation for this Policy

Web Reputation Settings

Web Reputation Score

DROP -10.0 to -6.0	DECRYPT -5.9 to 5.9	PASS THROUGH 6.0 to 10.0
-10 -8 -6 -4 -2 0 2 4 6 8 +10		

Drop	Decrypt	Pass Through
The requested HTTPS connection is immediately dropped. No end-user notification will be provided. Use this setting with caution.	The HTTPS transaction will be decrypted for scanning and re-encrypted to ensure user privacy and security. The scanning defined in the applicable Web Access Policy will be performed.	The HTTPS request is passed through without decryption. No scanning will be performed.

Sites with No Score

Specify an action for sites that do not have a Web Reputation Score.

Sites with No Score: Monitor

Cancel

Submit



Decryption Policy: Web Reputation cont.

- You can specify certain Web Reputation scores and the actions for them.
- Default value (same apply in Access Policy):
 - 10 to -6.0 Drop
 - 5.9 to 5.9 Decrypt
 - 6.0 to 10.0 Pass Through
- This section will require that the Web Reputation Service is enabled in the Security Services -> Anti-Malware and Reputation -> Web Reputation Filtering is Enabled.





Decryption Policy: Default Action.

HTTPS Default Action: decryptionpolicy.dp

Policy Group Settings

Default HTTPS Action: ?

☐ Use Global Setting (Decrypt)

☐ Decrypt

☒ Pass through without decrypting

☐ Drop Connection

No end-user notification will be provided for dropped HTTPS connections unless the option to decrypt for end-user notification is enabled (see Security Services > HTTPS Proxy).

Cancel

Submit





Decryption Policy: Default Action cont.

The default action is used when no decision is made based on URL category or Web Reputation score.

If Web Reputation filtering is disabled, the default action will apply to all transactions that match a Monitor action in URL Filtering. If Web Reputation filtering is enabled, the default action will be used only if the Monitor action is selected for sites with no score.





Custom and External URL Categories

- You can create custom and external live-feed URL categories that describe specific host names and IP addresses.
- You can edit and delete existing URL categories.
- When you include custom URL categories in the same Access, Decryption, or Cisco Data Security Policy group and assign different actions to each category, the action of the higher included custom URL category takes precedence.
- You can use regular expressions to the Custom URL Categories to specify specific destination URI for the category.





Custom and External URL Categories cont.

Best Practices:

- You can use no more than five External Live Feed files in these URL category definitions, and each file should contain no more than 1000 entries. Increasing the number of external feed entries causes performance degradation.
- No more than 25 – 30 Custom URL Categories to avoid performance degradation.
- Restrict of using lots of expensive regular expressions such as '*' functions to avoid performance degradation.
- The Web Security appliance uses the first four characters of custom URL category names preceded by "c_" in the access logs. Consider the custom URL category name if you use Sawmill/Splunk to parse the access logs. If the first four characters of the custom URL category include a space, Sawmill/Splunk might not properly parse the access log entry. Instead, only use supported characters in the first four characters. If you want to include the full name of a custom URL category in the access logs, add the %XF format specifier to the access logs.
- Make sure to use different name in the first four characters of custom URL category for the ease identifying the custom URL category from the access logs for troubleshooting purposes.





Custom and External URL Categories cont.

Custom URL Category



External Live Feed Category





- In the WEB GUI of WSA, go to 'Web Security Manager' tab then go to 'Custom and External URL Categories'





Custom URL Categories cont.

- Click 'Add Category' button to add new custom URL category.

The screenshot displays the Cisco S300V Web Security Virtual Appliance interface. The top navigation bar includes a home icon, a reporting icon, and tabs for Reporting, Web Security Manager, Security Services, Network, and System Administration. The main content area is titled "Custom and External URL Categories". Below this title is a "Categories List" section. Within this section, there is a button labeled "Add Category..." which is highlighted by a red arrow. Below the button, a message states: "No Custom and External URL Categories are defined."





Custom URL Categories cont.

- Give the new Custom URL Category a Name
- Enter the position of the Custom URL Category by entering the “List Order”, URL filtering engine evaluates a client request against the custom URL categories in the order specified
- On “Category Type” select “Local Custom Category”

Custom and External URL Categories: Add Category

Edit Custom and External URL Category

Category Name:

List Order:

1

Category Type:

Local Custom Category

Sites: ?

Sort URLs

Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

Advanced

Regular Expressions: ?

Enter one regular expression per line.





Custom URL Categories cont.

■ Sites section:

Enter one or more Site addresses for this custom category. You can enter multiple addresses separated by line breaks or commas. These addresses can be in any of the following formats:

- IPv4 address, such as 10.1.1.0
- IPv6 address, such as 2001:0db8::
- IPv4 CIDR address, such as 10.1.1.0/24
- IPv6 CIDR address, such as 2001:0db8::/32
- Domain name, such as example.com
- Hostname, such as crm.example.com
- Partial hostname, such as .example.com; this will also match www.example.com and crm.example.com

Note It is possible to use the same address in multiple custom URL categories, but the order in which the categories are listed is relevant. If you include these categories in the same policy, and define different actions for each, the action defined for the category listed highest in the custom URL categories table will be the one applied.

(Optional) Click Sort URLs to sort all addresses in the Sites field.

Note Once you sort the addresses, you cannot retrieve their original order.





Custom URL Categories cont.

■ Regular Expressions

Regular expressions can be entered in the Advanced section.

Regular expressions are rules that typically use the word “matches” in the expression. They can be applied to match specific URL destinations or web servers. For example, the following regular expression matches any pattern containing blocksite.com:

```
\.blocksite\.com
```

Consider the following regular expression example:

```
server[0-9]\.example\.com
```

In this example, server[0-9] matches server0, server1, server2, ..., server9 in the domain example.com.

In the following example, the regular expression matches files ending in .exe, .zip, and .bin in the downloads directory.

```
/downloads/.*\.(exe|zip|bin)
```

Avoid using regular expressions strings that are redundant because they can cause higher CPU usage on the Web Security appliance. A redundant regular expression is one that starts or ends with “.*”.

Note You must enclose regular expressions that contain blank spaces or non-alphanumeric characters in ASCII quotation marks.





Custom URL Categories cont.

■ Regular Expression Character Table

Character	Description
.	Matches a single character.
*	Matches zero or more occurrences of the preceding regular expression . For example: [0-9]* matches any number of digits “.*” matches any arbitrary string of characters
^	Matches the beginning of a line as the first character of a regular expression .
\$	Matches the end of a line as the last character of a regular expression .
+	Matches one or more occurrences of the preceding regular expression .
?	Matches zero or one occurrence of the preceding regular expression .
	Matches the preceding regular expression or the following regular expression . For example: <u>x</u> <u>y</u> matches either x or y <u>abc</u> <u>xyz</u> matches either of the strings <u>abc</u> or <u>xyz</u>
[]	Matches the characters or digits that are enclosed within the brackets. For example: [a-z] matches any character between a and z [r-u] matches any of the characters r, s, t, or u [0-3] matches any of the single digits 0, 1, 2, 3
{ }	Specifies the number of times to match the previous pattern. For example: D{1,3} matches one to three occurrences of the letter D
()	Group characters in a regular expression . For example: (<u>abc</u>)* matches <u>abc</u> or <u>abcabcabc</u>
“...”	Literally interprets any characters enclosed within the quotation marks.
\	Escape character.





External Live Feed Category.

- In the WEB GUI of WSA, go to 'Web Security Manager' tab then go to 'Custom and External URL Categories'

Cisco S300V
Web Security Virtual Appliance

Home Reporting **Web Security Manager** Security Services Network System Administration

Custom and External URL Categories

Categories List

[Add Category...](#)

Order	Category
1	test

Copyright © 2003-2017

Authentication
Identification Profiles
SaaS Policies

Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits

Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention

SOCKS Policies

Custom Policy Elements
Custom and External URL Categories
Define Time Ranges and Quotas

Bypass Settings
L4 Traffic Monitor

Type	Last Updated	Feed Content	Delete
Local	N/A	-	

Privacy Statement



External Live Feed Category cont.

- Click 'Add Category' button to add new custom URL category.

The screenshot displays the Cisco S300V Web Security Virtual Appliance interface. The top navigation bar includes a home icon, a reporting icon, and tabs for Reporting, Web Security Manager, Security Services, Network, and System Administration. The main content area is titled 'Custom and External URL Categories'. Below this title is a 'Categories List' section. Within this section, there is a button labeled 'Add Category...' which is highlighted by a red rectangular box and a red arrow. Below the button, a message states: 'No Custom and External URL Categories are defined.'





External Live Feed Category cont.

Cisco Feed Format



Office 365 Feed Format





External Live Feed Category: Cisco Feed Format.

Custom and External URL Categories: Add Category

Edit Custom and External URL Category

Category Name:	<input type="text"/>	
List Order:	<input type="text" value="1"/>	
Category Type:	External Live Feed Category	
Routing Table:	Management	
Feed File Location: ?	<input checked="" type="radio"/> Cisco Feed Format ? <input type="radio"/> Office 365 Feed Format ?	
	HTTPS	<input type="text"/>
Advanced		
Authentication (optional):		
	Username:	<input type="text" value="admin"/>
	Password:	<input type="password" value="....."/>
	Retype Password:	<input type="password"/>
	<input type="button" value="Get File"/>	
	<div></div>	
Auto Update the Feed:	<input checked="" type="radio"/> Do not auto update <input type="radio"/> Hourly Every <input type="text" value="01:00"/> (HH:MM)	



External Live Feed Category: Cisco Feed

Format cont.

If you choose External Live Feed Category for the Category Type, provide the Feed File Location information; that is, locate and download the file containing the addresses for this custom category:

Select either Cisco Feed Format, and then provide the appropriate feed-file information.

Cisco Feed Format :

- Choose the transport protocol to be used—either HTTPS or HTTP—and then enter the URL of the live-feed file.

This file must be a comma-separated values (.csv)-formatted file.

- Optionally, provide Authentication credentials in the Advanced section.

Provide a Username and Passphrase to be used for connection to the specified feed server.





External Live Feed Category: Cisco Feed

Format cont.

Cisco Feed Format – This must be a comma-separated values (.csv) file; that is, a text file with a .csv extension.

Each entry in the .csv file must be on a separate line, formatted as address/comma/addresstype (for example: www.cisco.com,site or ad2.*\.com,regex).

Valid addresstypes are site and regex. Here is an excerpt from a Cisco Feed Format .csv file:

```
www.cisco.com,site
```

```
\.xyz,regex
```

```
ad2.*\.com,regex
```

```
www.trafficholder.com,site
```

```
2000:1:1:11:1:1::200,site
```

Do not include http:// or https:// as part of any site entry in the file, or an error will occur.









In other words, www.example.com is parsed correctly, while http://www.example.com produces an error.





External Live Feed Category.

Custom and External URL Categories: Add Category

Edit Custom and External URL Category	
Category Name:	<input type="text"/>
List Order:	<input type="text" value="1"/>
Category Type:	External Live Feed Category  
Routing Table:	Management
Feed File Location: 	<div><input type="radio"/> Cisco Feed Format  <input checked="" type="radio"/> Office 365 Feed Format  </div> <div> Office 365 Feed Location: <input type="text"/></div> <div><input type="button" value="Get File"/></div> <div><div></div></div>
Auto Update the Feed:	<div><input checked="" type="radio"/> Do not auto update</div> <div><input type="radio"/> <div>Hourly </div> Every <div>01:00 (HH:MM)</div></div>

Cancel

Submit





External Live Feed Category cont.

Office 365 Feed Format:

- Select either Cisco Feed Format or Office 365 Feed Format , and then provide the appropriate feed-file information.
- Enter the Office 365 Feed Location (URL) of the live-feed file.

This file must be an XML-formatted file;

- Click Get File to test the connection to the feed server, and then parse and download the feed file from the server.

Progress is displayed in the text box below the Get File button. If an error occurs, the problem is indicated and must be rectified before trying again.

After you save your changes to this live-feed category, you can click View in the Feed Content column for this entry on the Custom and External URL Categories page (Web Security Manager > Custom and External URL Categories) to open a window that displays the addresses contained in the Cisco Feed Format or Office 365 Feed Format feed file you downloaded here.





External Live Feed Category cont.

Office 365 Feed Format – This is an XML file located on a Microsoft Office 365 server, or a local server to which you saved the file. It is provided by the Office 365 service and cannot be modified.

The network addresses in the file are enclosed by XML tags, following this structure: products > product > addresslist > address.

In the current implementation, an addresslist type can be IPv6, IPv4, or URL (which can include domains and regex patterns).

- Below is the feed address from Microsoft for Office 365 Feed:

<https://support.content.office.net/en-us/static/O365IPAddresses.xml>

- Below is the Cisco official guide for Office 365 External Feed:

<https://www.cisco.com/c/dam/en/us/products/collateral/security/web-security-appliance/guide-c07-738382.pdf>





External Live Feed Category cont.

Snippet of an Office 365 feed file:

```
<products updated="4/15/2016">
  <product name="o365">
    <addresslist type="IPv6">
      <address>2603:1040:401::d:80</address>
      <address>2603:1040:401::a</address>
      <address>2603:1040:401::9</address>
    </addresslist>
    <addresslist type="IPv4">
      <address>13.71.145.72</address>
      <address>13.71.148.74</address>
      <address>13.71.145.114</address>
    </addresslist>
    <addresslist type="URL">
      <address>*.aadrm.com</address>
      <address>*.azurerms.com</address>
      <address>*.cloudapp.net2</address>
    </addresslist>
  </product>
  <product name="LYO">
    <addresslist type="URL">
      <address>*.broadcast.skype.com</address>
      <address>*.Lync.com</address>
    </addresslist>
  </product>
</products>
```

