Create Policies to Control Internet Requests

This topic contains the following sections:

Overview of Policies: Control Intercepted Internet Requests

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.

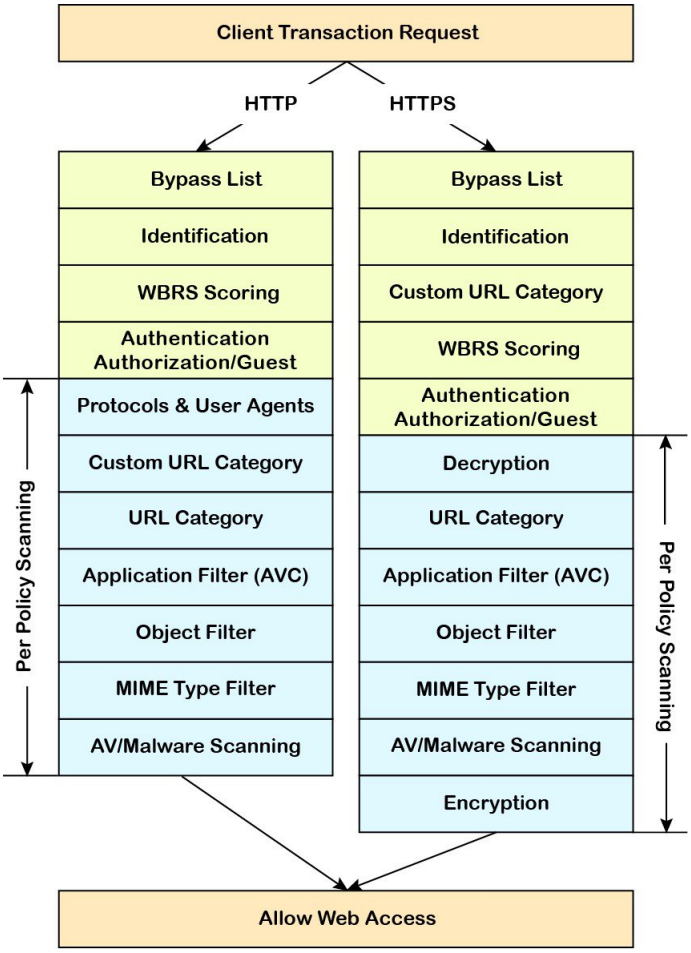
The Web Security Appliance uses multiple policy types to manage different aspects of web requests. Policy types might fully manage transactions by themselves or pass transactions along to other policy types for additional processing. Policy types can be groups by the functions they perform, such as access, 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 fail based on a DNS error.

Intercepted HTTP/HTTPS Request Processing

The following diagram depicts the flow of an intercepted Web request as it is processed by the appliance.

Figure 1: HTTP/HTTPS Transaction Flow



Also see the following diagrams depicting various transaction processing flows:

- Identification Profiles and Authentication Processing – No Surrogates and IP-based Surrogates
- Identification Profiles and Authentication Processing – Cookie-based Surrogates
- Figure 2: Policy Group Transaction Flow for Access Policies, on page 6
- Policy Group Transaction Flow for Decryption Policies
- Controlling HTTPS Traffic

Managing Web Requests Through Policies Task Overview

Step	Task List for Managing Web Requests through Policies	Links to Related Topics and Procedures
1	Set up and sequence Authentication Realms	Authentication Realms
2	(For upstream proxies) Create a proxy group.	Creating Proxy Groups for Upstream Proxies
2	(Optional) Create Custom Client Applications	Client Applications, on page 18
3	(Optional) Create Custom URL Categories	Creating and Editing Custom URL Categories
4	Create Identification Profiles	Classifying Users and Client Software
5	(Optional) Create time ranges to Limit Access by Time of Day	Time Ranges and Quotas, on page 20
6	Create and Order Policies	• Creating a Policy , on page 7 • Policy Order, on page 6

Managing Web Requests Through Policies Best Practices

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.

Policies

Policy Types

Policy Type	Request Type	Description	Link to task
Access	• HTTP • Decrypted HTTPS • FTP	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.	Creating a Policy , on page 7
SOCKS	• SOCKS	Allow or block SOCKS communication requests.	Creating a Policy , on page 7

Policy Type	Request Type	Description	Link to task
Application Authentication	• application	Allow or deny access to a Software as a Service (SaaS) application. Use single sign-on to authenticate users and increase security by allowing access to applications to be quickly disabled. To use the single sign-on feature of policies you must configure the Web Security Appliance as an identity provider and upload or generate a certificate and key for SaaS.	Creating SaaS Application Authentication Policies
Encrypted HTTPS Management	• HTTPS	Decrypt, pass through, or drop HTTPS connections. AsyncOS passes decrypted traffic to Access policies for further processing.	Creating a Policy , on page 7
Data Security	• HTTP • Decrypted HTTPS • FTP	Manage data uploads to the web. Data Security policies scan outbound traffic to ensure it complies to company rules for data uploads, based on its destination and content. Unlike External DLP policies, which redirect outbound traffic to external servers for scanning, Data Security policies use the Web Security Appliance to scan and evaluate traffic.	Creating a Policy , on page 7
External DLP (Data Loss Prevention)	• HTTP • Decrypted HTTPS • FTP	Send outbound traffic to servers running 3rd-party DLP systems, which scan it for adherence to company rules for data uploads. Unlike Data Security policies, which also manage data uploads, External DLP policies move scanning work away from the Web Security Appliance , which frees resources on the appliance and leverages any additional functionality offered by 3rd-party software.	Creating a Policy , on page 7
Outbound Malware Scanning	• HTTP • Decrypted HTTPS • FTP	Block, monitor, or allow requests to upload data that may contain malicious data. Prevent malware that is already present on your network from being transmitted to external networks.	Creating a Policy , on page 7

Policy Type	Request Type	Description	Link to task
Routing	• HTTP • HTTPS • FTP	Direct web traffic through upstream proxies or direct it to destination servers. You might want to redirect traffic through upstream proxies to preserve your existing network design, to off-load processing from the Web Security Appliance , or to leverage additional functionality provided by 3rd-party proxy systems. If multiple upstream proxies are available, the Web Security Appliance can use load balancing techniques to distribute data to them. Retian the client's source IP address, change it to the web proxy IP, or a custom IP using IP Spooing profile.	Creating a Policy , on page 7

Each policy type uses a policy table to store and manage its policies. Each policy table comes with a predefined, global policy, which maintains default actions for a policy type. Additional, user-defined policies are created and added to the policy table as required. Policies are processed in the order in which they are listed in the policy table.

Individual policies define the user-request types they manage, and the actions they perform on those requests. Each policy definition has two main sections:

- **Identification Profiles and Users** – Identification Profiles are used in policy membership criteria and are particularly important as they contain many options for identifying web transaction. They also share many properties with policies.
- **Advanced** – The criteria used to identify users to which the policy applies. One or more criteria can be specified in a policy, and all must be match for the criteria to be met.
  - **Protocols** – Allow the transfer of data between various networking devices such as http, https, ftp, etc.
  - **Proxy Ports** – the numbered port by which the request accesses the web proxy,
  - **Subnets** – The logical grouping of connected network devices (such as geographic location or Local Area Network [LAN]), where the request originated
  - **Time Range** – Time ranges can be created for use in policies to identify or apply actions to web requests based on the time or day the requests were made. The time ranges are created as individual units.
  - **URL Categories** – URL categories are predefined or custom categories of websites, such as News, Business, Social Media, etc. These can be used to identify or apply actions to web requests.
  - **User Agents** – These are the client applications (such as updaters and Web browsers) used to make requests. You can define policy criteria based on user agents, and you can specify control settings based on user agents. You can also exempt user agents from authentication, which is useful for applications that cannot prompt for credentials. You can define custom user agents but cannot re-use these definitions other policies.

Note When you define multiple membership criteria, the client request must meet all criteria to match the policy.

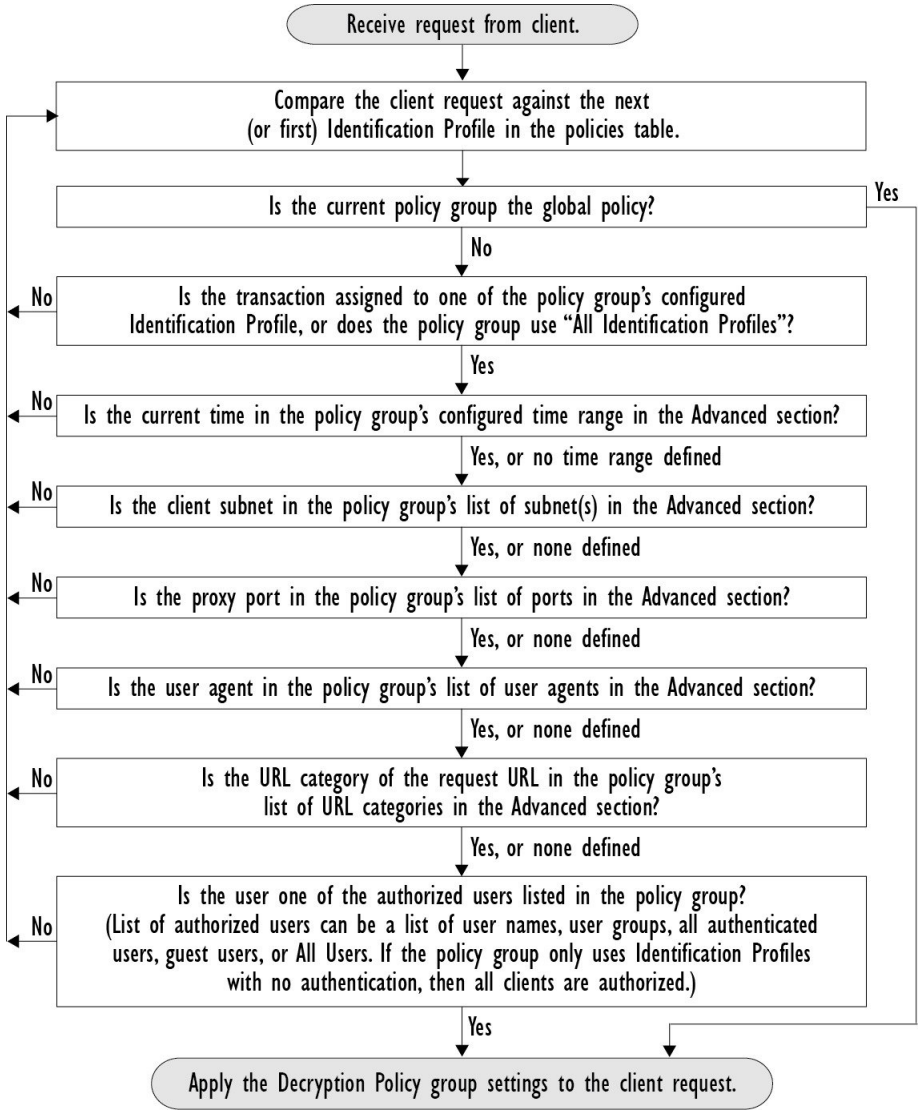
Policy Order

The order in which policies are listed in a policy table determines the priority with which they are applied to Web requests. Web requests are checked against policies beginning at the top of the table and ending at the first policy matched. Any policies below that point in the table are not processed.

If no user-defined policy is matched against a Web request, then the global policy for that policy type is applied. Global policies are always positioned last in Policy tables and cannot be re-ordered.

The following diagram depicts the flow of a client request through the Access policies table.

Figure 2: Policy Group Transaction Flow for Access Policies



Creating a Policy

Before you begin

- Enable the appropriate proxy:
  - Web Proxy (for HTTP, decrypted HTTPS, and FTP)
  - HTTPS Proxy
  - SOCKS Proxy
- Create associated Identification Profiles.
- Understand Policy Order, on page 6.
- (Encrypted HTTPS only) Upload or generate a Certificate and Key.
- (Data Security only) Enable Cisco Data Security Filters Settings.
- (External DLP only) Define an External DLP server.
- (Routing only) Define the associated upstream proxy on the Web Security Appliance .
- (Optional) Create associated client applications.
- (Optional) Create associated time ranges. See Time Ranges and Quotas, on page 20.
- (Optional) Create associated URL categories. See Creating and Editing Custom URL Categories.

Step 1 In the **Policy Settings** section, use the **Enable Identity** check box to enable this policy, or to quickly disable it without deleting it.

Step 2 Assign a unique policy **Name**.

Step 3 A **Description** is optional.

Step 4 From the Insert Above drop-down list, choose where this policy is to appear in the table.

Note Arrange policies such that, from top to bottom of the table, they are in most-restrictive to least-restrictive order. See Policy Order, on page 6 for more information.

Step 5 In the **Policy Expires** area, check the **Set Expiration for Policy** check box to set the expiry time for the policy. Enter the date and time for the policy expiration that you want to set. The policies are automatically disabled once they exceed the set expiry time.

Note System checks the policies every minute to disable the policies which get expired during the minute. For example, if a policy is set to expire at 11:00, at maximum it will be disabled by 11:01.

Policy Expiry feature is applicable only for Access, Decryption, and Web Traffic Tap policies.

You will receive an email prior to three days of the policy expiry and another one upon policy expiry.

Note To receive alerts, you must enable Policy Expiration alerts using **System Administration** > **Alerts** . See Policy Expiration Alerts

You can set the policy expiration time through Cisco Content Security Management Appliances as well. The policies will get expired after the set expiry time but will not be shown as disabled in the Cisco Content Security Management Appliances GUI.

Once you set the policy expiration feature, the expiry happens based on the appliance's local time settings.

Step 6 In the **Policy Member Definition** section, specify how user and group membership is defined: from the Identification Profiles and Users list, choose one of the following:

- **All Identification Profiles** – This policy will apply to all existing profiles. You must also define at least one **Advanced** option.
- **Select One or More Identification Profiles** – A table for specifying individual Identification Profiles appears, one profile-membership definition per row.

Step 7 If you chose **All Identification Profile**s:

a) Specify the authorized users and groups to which this policy applies by selecting one of the following options:

- **All Authenticated Users** – All users identified through authentication or transparent identification.
- **Selected Groups and Users** – Specified users and groups are used.

  To add or edit the specified **ISE Secure Group Tags** (SGTs) and the specified Users, click the link following the appropriate label. For example, click the list of currently specified users to edit that list. See Adding and Editing Secure Group Tags for a Policy, on page 10 for more information.

  If you use ISE, you can add or edit ISE Secure Group Tags. This is not supported in ISE-PIC deployments. To add or edit the specified **ISE Groups**, click the link following the label. This option is specific to ISE-PIC.
- **Guests** – Users connected as guests and those failing authentication.
- **All Users** – All clients, whether authenticated or not. If this option is selected, at least one **Advanced** option also must be provided.

Step 8 If you chose **Select One or More Identification Profiles**, a profile-selection table appears.

a) Choose an Identification Profile from the Select Identification Profile drop-down list in the Identification Profiles column.

b) Specify the Authorized Users and Groups to which this policy applies:

- **All Authenticated Users** – All users identified through authentication or transparent identification.
- **Selected Groups and Users** – Specified users and groups are used.

  To add or edit the specified ISE Secure Group Tags (SGTs) and the specified Users, click the link following the appropriate label. For example, click the list of currently specified users to edit that list. See Adding and Editing Secure Group Tags for a Policy, on page 10 for more information.
- **Guests** – Users connected as guests and those failing authentication.

c) To add a row to the profile-selection table, click **Add Identification Profile**. To delete a row, click the trash-can icon in that row.

Repeat steps (a) through (c) as necessary to add all desired Identification Profiles.

Step 9 Expand the **Advanced** section to define additional group membership criteria. (This step may be optional depending on selection in the **Policy Member Definition** section. Also, some of the following options will not be available, depending on the type of policy you are configuring.) .

Advanced Option	Description
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. **Note** 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. **Note** 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.
Time Range	You can apply time ranges for policy membership: • Time Range – Choose a previously defined time range (Time Ranges and Quotas, on page 20). • 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. See Creating and Editing Custom URL Categories for information about custom 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.

Adding and Editing Secure Group Tags for a Policy

To change the list of Secure Group Tags (SGTs) assigned to a particular Identification Profile in a policy, click the link following the ISE Secure Group Tags label in the Selected Groups and Users list on the Add/Edit Policy page. (See Creating a Policy , on page 7.) This link is either "No tags entered," or it is a list of currently assigned tags. The link opens the Add/Edit Secure Group Tags page.

All SGTs currently assigned to this policy are listed in the Authorized Secure Group Tags section. All SGTs available from the connected ISE server are listed in the Secure Group Tag Search section.

Step 1 To add one or more SGTs to the Authorized Secure Group Tags list, select the desired entries in the Secure Group Tag Search section, and then click **Add**.

Note
- The SGTs already added, are highlighted in green. To quickly find a specific SGT in the list of those available, enter a text string in the **Search** field.
- When a Web Security Appliance is connected to ISE/ISE-PIC, default SGTs from ISE/ISE-PIC are also displayed. These SGTs will not have users assigned. Ensure that you select the correct SGTs.

Step 2 To remove one or more SGTs from the Authorized Secure Group Tags list, select those entries and then click **Delete**.

Step 3 Click Done to return to the Add/Edit Group page.

What to do next

Related Topics

- Time Ranges and Quotas, on page 20
- Using Client Applications in Policies, on page 19

Adding Routing Destination and IP Spoofing Profile to Routing Policy

You can configure how the web proxy forwards the web traffic and the requests the source IP address by configuring the routing destination and IP spoofing profile in routing policies.

Note
- The global routing policy is enabled by default even if an upstream proxy group is not configured on the appliance.
- IP spoofing profiles are not related to routing destination, and can be configured independently.
- Routing Policy can be enabled without configuring an upstream proxy.

Note To configure an upstream proxy group for a routing policy in Security Management appliance, save the configuration file of the Web Security Appliance and import it on the Security Management appliance. Otherwise, the Security Management appliance shows the upstream proxy as "Not Found" and the routing policy will be disabled after the config push.

Step 1 Choose **Web Security Manager** > **Routing Policies**.

Step 2 On the **Routing Policies** page, click the link under **Routing Destination** column for the routing policy that you want to configure the upstream proxy group.

Step 3 Choose an appropriate upstream proxy group for the selected policy from the following:

Action	Description
Use Global Policy Settings	The web proxy uses the settings defined in the Global Policy. This is the default action for user defined policy groups. By default, the routing destination for Global Routing Policy is set as **Direct Connection**. Applies to user defined policy groups only.
Direct Connection	The web proxy forwards web traffic directly to its destination web server.
Custom upstream proxy group	The web proxy redirects the web traffic to an external upstream proxy group. For more information about creating upstream proxy groups, see Upstream Proxies.

Step 4 On the **Routing Policies** page, click the link under **IP Spoofing** column for the routing policy that you want to configure the IP spofing profile.

Step 5 Choose an appropriate IP spoofing profile for the selected policy from the following:

Action	Description
Use Global Policy Settings	The web proxy uses the settings defined in the Global Policy. This is the default action for user defined policy groups. By default, the IP spoofing is disabled for the Global Routing Policy. Applies to user defined policy groups only.
Do No Use IP Spoofing	The web proxy changes the request source IP address to match its own address to increase security.
Use Client IP	The web proxy retains the source address so that it appears to originate from the source client rather than from the Web Security Appliance .
Custom spoofing profile name	The web proxy changes the request source IP address to custom IP defined in the selected custom IP spoofing profile name.

Step 6 **Submit** and **Commit** your changes.

What to do next

Related Topics

- Upstream Proxies
- Web Proxy IP Spoofing

Policy Configuration

Each row in a table of policies represents a policy definition, and each column displays current contains a link to a configuration page for that element of the policy.

Note Of the following policy-configuration components, you can specify the "Warn" option only with URL Filtering.

Option	Description
Protocols and User Agents	Used to control policy access to protocols and configure blocking for particular client applications, such as instant messaging clients, web browsers, and Internet phone services. You can also configure the appliance to tunnel HTTP CONNECT requests on specific ports. With tunneling enabled, the appliance passes HTTP traffic through specified ports without evaluating it.
URL Filtering	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. See Creating and Editing Custom URL Categories for information about creating custom URL categories. In addition, you can add exceptions to blocking of embedded or referred content.
Applications	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. See Managing Access to Web Applications for configuration information.
Objects	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. See Access Policies: Blocking Objects, on page 13 for information about specifying blocked objects.

Option	Description
Anti-Malware and Reputation	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. There are also global settings for file reputation and analysis services. For more information, see Anti-Malware and Reputation Settings in Access Policies and Configuring File Reputation and Analysis Features.
HTTP ReWrite Profile	You can configure custom header profiles for HTTP requests and can create multiple headers under a header rewrite profile. The header rewrite profile feature enables the appliance to pass the user and group information to another upstream device after successful authentication. The upstream proxy considers the user as authenticated, bypasses further authentication, and provides access to the user based on the defined access policies. See Web Proxy Custom Headers Per Policy.
Delete	Deletes the created policy.

Access Policies: Blocking Objects

You can use the options on the Access Policies: Objects page 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 specify a number of types of objects to be blocked by each individual Access policy, and by the Global policy. These object types include Archives, Document Types, Executable Code, Web Page Content, and so on.

Step 1 On the Access Policies page (**Web Security Manager** > **Access Policies**), click the link in the **Objects** column of the row representing the policy you wish to edit.

Step 2 Choose the desired type of object blocking for this Access policy:

- **Use Global Policy Objects Blocking Settings** – This policy uses the object-blocking settings defined for the Global Policy; these settings are displayed in read-only mode. Edit the settings for the Global Policy to change them.
- **Define Custom Objects Blocking Settings** – You can edit all object-blocking settings for this policy.
- **Disable Object Blocking for this Policy** – Object blocking is disabled for this policy; no object-blocking options are presented.

Step 3 If you chose **Define Custom Objects Blocking Settings** in the previous step, select and deselect object-blocking options on the Access Policies: Objects page as needed.

Object Size	You can block objects based on their download size: • **HTTP/HTTPS Max Download Size** – Either provide the maximum object size for HTTP/HTTPS download (objects larger than this will be blocked), or indicate that there is no maximum size for object download via HTTP/HTTPS. • **FTP Max Download Size** – Either provide the maximum object size for FTP download (objects larger than this will be blocked), or indicate that there is no maximum size for object download via FTP.
Block Object Type	
Archives	Expand this section to select types of Archive files that are to be blocked. This list includes Archive types such as ARC, BinHex, and StuffIt.

Inspectable Archives	Expand this section to select whether to **Allow**, **Block**, or **Inspect** specific types of Inspectable Archive files. Inspectable Archives are archive or compressed files that the Web Security Appliance can inflate to inspect each of the contained files in order to apply the file-type block policy. The Inspectable Archives list includes archive types such as 7zip, Microsoft CAB, RAR, and TAR.
	
	The following points apply to archive inspection:
	• Only archive types marked **Inspect** will be inflated and inspected.
	• Only one archive will be inspected at a time, Additional concurrent inspectable archives may not be inspected.
	• If an inspected archive contains a file type that is assigned the Block action by the current policy, the entire archive will be blocked, regardless of any allowed file types it may contain.
	• An inspected archive that contains an unsupported archive type will be marked as "unscannable." If it contains a blocked archive type, it will be blocked.
	• Password-protected and encrypted archives are not supported and will be marked as "unscannable."
	• An inspectable archive which is incomplete or corrupt is marked as "unscannable."
	• The **DVS Engine Object Scanning Limits** value specified for the **Anti-Malware and Reputation** global settings also applies to the size of an inspectable archive; an object exceeding this size is marked as "unscannable." See Enabling Anti-Malware and Reputation Filters for information about this object size limit.
	• An inspectable archive marked as "unscannable" can be either Blocked in its entirety or Allowed in its entirety.
	• When access policies are configured to block custom MIME types, and archive inspection is enabled:
	  • If the appliance directly downloads a file with the custom MIME type as part of the content-type header, access is blocked.
	  • If the same file is part of a ZIP/archive file, the appliance inspects the archive and determines the MIME type based on its own MIME evaluation. If the MIME evaluated by the appliance's engine does not match the configured custom MIME type, the content is not blocked.
	• The appliance can inspect configured archives but it has the limitation to inspect certain archives such as RAR and 7-Zip.
	
	See Archive Inspection Settings, on page 16 for information about configuring archive inspection.

Document Types	Expand this section to select types of text documents to be blocked. This list includes document types such as FrameMaker, Microsoft Office, and PDF.
Executable Code	Expand this section to select types of executable code to be blocked. The list includes Java Applet, UNIX Executable and Windows Executable.

Installers	Types of installers to be blocked; the list includes UNIX/LINUX Packages.
Media	Types of media files to be blocked. The list includes Audio, Video and Photographic Image Processing Formats (TIFF/PSD).
P2P Metafiles	This list includes BitTorrent Links (`.torrent`).
Web Page Content	This list includes Flash and Images.
Miscellaneous	This list includes Calendar Data.
Custom MIME Types	You can define additional objects/files to be blocked based on MIME type. Enter one or more MIME types in the **Block Custom MIME Types** field, one per line.

Step 4 Click **Submit**.

Archive Inspection Settings

You can Allow, Block, or Inspect specific types of Inspectable Archives for individual Access policies. Inspectable Archives are archive or compressed files that the Web Security Appliance can inflate to inspect each of the contained files in order to apply the file-type block policy. See Access Policies: Blocking Objects, on page 13 for more information about configuring archive inspection for individual Access policies.

Note During archive inspection, nested objects are written to disk for examination. The amount of disk space that can be occupied at any given time during file inspection is 1 GB. Any archive file exceeding this maximum disk-use size will be marked unscannable.

The Web Security Appliance 's Acceptable Use Controls page provides system-wide Inspectable Archives Settings; that is, these settings apply to archive extraction and inspection whenever enabled in an Access policy.

Step 1 Choose **Security Services** > **Acceptable Use Controls**.

Step 2 Click the **Edit Archives Settings** button.

Step 3 Edit the Inspectable Archives Settings as needed.

- **Maximum Encapsulated Archive Extractions** – Maximum number of "encapsulated" archives to be extracted and inspected. That is, maximum depth to inspect an archive containing other inspectable archives. An encapsulated archive is one that is contained in another archive file. This value can be zero through five; depth count begins at one with the first nested file.

  The external archive is considered file zero. If the archive has files nested beyond this maximum nested value, the archive is marked as unscannable. Note that this will impact performance.

- **Block Uninspectable Archives** – If checked, the Web Security Appliance will block archives it failed to inflate and inspect.

Step 4 **Submit** and **Commit Changes**.

Block, Allow, or Redirect Transaction Requests

The web proxy controls web traffic based on the policies that you create for groups of transaction requests.

- **Allow.** The Web Proxy permits the connection without interruption. Allowed connections may not have been scanned by the DVS engine.
- **Block.** The Web Proxy does not permit the connection and instead displays an end user notification page explaining the reason for the block.
- **Redirect.** The Web Proxy does not allow the connection to the originally requested destination server and instead connects to a different specified URL, see Redirecting Traffic in the Access Policies.

Note The preceding actions are final actions that the Web Proxy takes on a client request. The Monitor action that you can configure for Access Policies is not a final action.

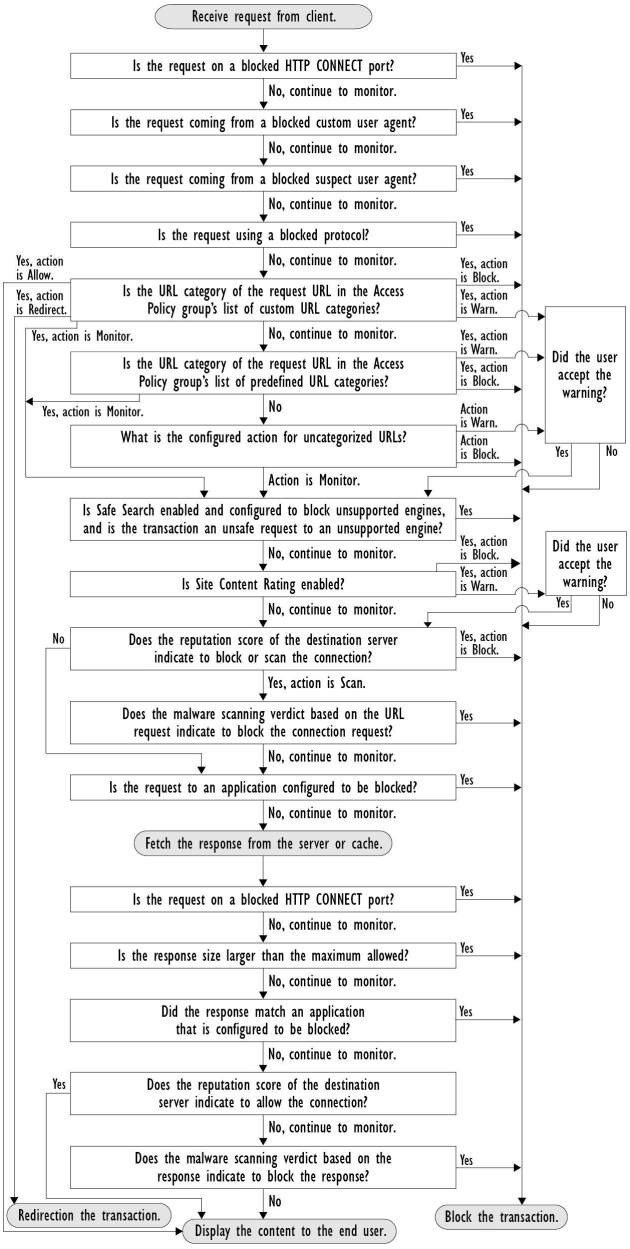
Generally, different types of policies control traffic based on the transport protocol.

Policy Type	Protocols				Actions Supported			
	HTTP	HTTPS	FTP	SOCKS	Block	Allow	Redirect	Monitor
Access	x	x	x		x	x	x	x
SOCKS				x	x	x		
SAAS	x	x						
Decryption	x	x						x
Data Security	x	x	x		x			x
External DLP	x	x	x				x	
Outbound Malware Scanning	x	x	x		x			x
Routing	x	x	x				x	

Note Decryption policy takes precedence over Access policy.

The following diagram shows how the Web Proxy determines which action to take on a request after it has assigned a particular Access Policy to the request. The Web reputation score of the destination server is evaluated only once, but the result is applied at two different points in the decision flow.

Figure 3: Applying Access Policy Actions



Client Applications

About Client Applications

Client Applications (such as a web browser) are used to make requests. You can define policy membership based on client applications, and you can specify control settings and exempt client applications from authentication, which is useful for applications that cannot prompt for credentials.

Using Client Applications in Policies

Defining Policy Membership Using Client Applications

Step 1 Choose a policy type from the Web Security Manager menu.

Step 2 Click a policy name in the policies table.

Step 3 Expand the Advanced section and click the link in the Client Applications field.

Step 4 Define one or more of the client applications:

Option	Method
Choose a predefined client application	Expand the Browser and Other sections and check the required client application check boxes. **Tip** Choose only the Any Version options when possible, as this provides better performance than having multiple selections.
Define a custom client application	Enter an appropriate regular expression in the Custom Client Applications field. Enter additional regular expressions on new lines as required. **Tip** Click **Example Client Applications Patterns** for examples of regular expressions.

Step 5 (Optional) Click the Match All Except The Selected **Client Applications** Definitions radio button to base the policy membership on all client applications **except** those you have defined.

Step 6 Click **Done**.

Defining Policy Control Settings Using Client Applications

Step 1 Choose a policy type from the Web Security Manager menu.

Step 2 Find the required policy name in the policies table.

Step 3 Click the cell link in the Protocols and Client Applications column on the same row.

Step 4 Choose **Define Custom Settings** from the drop-down list in the Edit Protocols and Client Applications Settings pane (if not already set).

Step 5 Enter a regular expression in the Custom Client Applications field that matches the client application you wish to define. Enter additional regular expressions on new lines as required.

Tip Click **Example Client Application Patterns** for examples of regular expressions.

Step 6 Submit and commit your changes.

Exempting Client Applications from Authentication

Procedure

	Command or Action	Purpose
Step 1	Create an Identification Profile that does not require authentication.	Classifying Users and Client Software
Step 2	Set the Identification Profile membership as the client application to exempt.	Using Client Applications in Policies, on page 19
Step 3	Place the Identification Profile above all other Identification Profiles in the policies table that require authentication.	Policy Order, on page 6

Time Ranges and Quotas

You can apply time ranges and time and volume quotas to access policies and decryption policies to restrict when a user has access, as well as their maximum connection time or data volume (also referred to as a "bandwidth quota").

- Time Ranges for Policies and Acceptable Use Controls, on page 20
- Time and Volume Quotas, on page 21

Time Ranges for Policies and Acceptable Use Controls

Time ranges are defined periods of time during which policies and acceptable use controls apply.

Note You cannot use time ranges to define the times at which users must authenticate. Authentication requirements are defined in Identification Profiles, which do not support time ranges.

- Creating a Time Range, on page 20

Creating a Time Range

Step 1 Choose **Web Security Manager** > **Define Time Ranges and Quotas**.

Step 2 Click **Add Time Range**.

Step 3 Enter a name for the time range.

Step 4 Choose a **Time Zone** option:

- Use **Time Zone Setting From Appliance** – Use the same time zone as the Web Security Appliance .
- **Specify Time Zone for this Time Range** – Define a different time zone, either as a GMT Offset, or as a region, country and a specific time zone in that country.

Step 5 Check one or more **Day of Week** check boxes.

Step 6 Select a **Time of Day** option:

- **All Day** – Use the full 24-hour period.
- **From** and **To** – Define a specific range of hours: enter a start time and end time in HH:MM (24-hour format).

Tip Each time range defines a start time and an end-time boundary. For example, entering 8:00 through 17:00 matches 8:00:00 through 16:59:59, but not 17:00:00. Midnight must be specified as 00:00 for a start time, and as 24:00 for an end time.

Step 7 Submit and commit your changes.

Time and Volume Quotas

Quotas allow individual users to continue accessing an Internet resource (or a class of Internet resources) until they exhaust the data volume or time limit imposed. AsyncOS enforces defined quotas on HTTP, HTTPS and FTP traffic.

As a user approaches either their time or volume quota, AsyncOS displays first a warning, and then a block page.

Please note the following regarding use of time and volume quotas:

- If AsyncOS is deployed in transparent mode and HTTPS proxy is disabled, there is no listening on port 443, and requests are dropped. This is standard behavior. If AsyncOS is deployed in explicit mode, you can set quotas in your access policies.

  When HTTPS proxy is enabled, possible actions on a request are pass-through, decrypt, drop, or monitor. Overall, quotas in decryption policies are applicable only to the pass-through categories.

  With pass-through, you will also have the option to set quotas for tunnel traffic. With decrypt, this option is not available, as the quotas configured in the access policy will be applied to decrypted traffic.

- If URL Filtering is disabled or if its feature key is unavailable, AsyncOS cannot identify the category of a URL, and the **Access Policy** > **URL Filtering** page is disabled. Thus, the feature key needs to be present, and Acceptable Use Policies enabled, to configure quotas..
- Many websites such as Facebook and Gmail auto-update at frequent intervals. If such a website is left open in an unused browser window or tab, it will continue to consume the user's quota of time and volume.
- When you restart the proxy and the high-performance mode is:
  - **Enabled** - Time and volume quotas are not reset. Quotas are automatically reset once within the 24-hour window based on the configured time.
  - **Disabled** - Time and volume quotas are reset. The reset impact remains only for the current 24-hour window as the quotas are automatically reset once within 24 hours. Proxy may restart due to configuration changes or proxy process crash.
- Your EUN pages (both warning and block) cannot be displayed for HTTPS even when decrypt-for-EUN option is enabled.

Note The most restrictive quota will always apply when more than one quota applies to any given user.

Volume Quota Calculations

Calculation of volume quotas is as follows:

- HTTP and decrypted HTTPS traffic – The HTTP request and response body are counted toward quota limits. The request headers and response headers will not be counted toward the limits.
- Tunnel traffic (including tunneled HTTPS) – AsyncOS simply shuttles the tunneled traffic from the client to the server, and vice versa. The entire data volume of the tunnel traffic is counted toward quota limits.
- FTP – The control-connection traffic is not counted. The size of the file uploaded and downloaded is counted toward quota limits.

Note Only client-side traffic is counted toward quota limits. Cached content also counts toward the limit, as client-side traffic is generated even when a response is served from the cache.

Time Quota Calculations

Calculation of time quotas is as follows:

- HTTP and decrypted HTTPS traffic – The duration of each connection to the same URL category, from formation to disconnect, plus one minute, is counted toward the time quota limit. If multiple requests are made to the same URL category within one minute of each other, they are counted as one continuous session and the one minute is added only at the end of this session (that is, after at least one minute of "silence").
- Tunnel traffic (including tunneled HTTPS) – The actual duration of the tunnel, from formation to disconnect, counts toward quota limits. The above calculation for multiple requests applies to tunneled traffic as well.
- FTP – The actual duration of the FTP control session, from formation to disconnect, counts toward quota limits. The above calculation for multiple requests applies to FTP traffic as well.

Defining Time and Volume Quotas

Before you begin

- Go to **Security Services** > **Acceptable Use Controls** to enable Acceptable Use Controls.
- Define a time range unless you want the quota to apply as a daily limit.

Step 1 Navigate to **Web Security Manager > Define Time Ranges and Quotas**.

Step 2 Click **Add Quota**.

Step 3 Enter a unique **Quota Name** in the field.

Step 4 To reset the Time and Volume quota every day, select **Reset this quota daily at** and enter a time in the 12-hour format in the field, then choose **AM** or **PM** from the menu. Alternatively, select **Select a predefined time range profile**.

Step 5 To set a time quota, select the **Time Quota** check box and choose the number of hours from the **hrs** menu and the number of minutes from the **mins** menu, from zero (always blocked) to 23 hours and 59 minutes.

Step 6 To set a volume quota enter a number in the field and choose **KB** (kilobytes), MB (megabytes), or **GB** (gigabytes) from the menu.

Step 7 Click **Submit** and then click **Commit Changes** to apply your changes. Alternatively, click **Cancel** to abandon your changes.

What to do next

(Optional) Navigate to **Security Services > End-User Notification** to configure end-user notifications for quotas.

Access Control by URL Category

You can identify and action Web requests based on the category of Website they address. The Web Security Appliance ships with many predefined URL categories, such as Web-based Email and others.

Predefined categories, and the Websites associated with them, are defined within filtering databases that reside on the Web Security Appliance . These databases are automatically kept up to date by Cisco. You can also create custom URL categories for host names and IP addresses that you specify.

URL categories can be used by all policies except policies to identify requests. They can also be used by Access, Encrypted HTTPS Management and Data Security policies to apply actions to requests.

See Creating and Editing Custom URL Categories for information about creating custom URL categories.

Using URL Categories to Identify Web Requests

Before you begin

- Enable Acceptable Use Control, see Configuring the URL Filtering Engine.
- (Optional) Create Custom URL Categories, see Creating and Editing Custom URL Categories.

Step 1 Choose a policy type (except SaaS) from the Web Security Manager menu.

Step 2 Click a policy name in the policies table (or add a new policy).

Step 3 Expand the **Advanced** section and click the link in the URL Categories field.

Step 4 Click the Add column cells corresponding to URL Categories you wish to identify web requests by. Do this for the Custom URL Categories and Predefined URL Categories lists as required.

Step 5 Click **Done**.

Step 6 Submit and commit your changes.

Using URL Categories to Action Web Request

Before you begin

- Enable Acceptable Use Control, see Configuring the URL Filtering Engine.
- (Optional) Create Custom URL Categories, see Creating and Editing Custom URL Categories.

Note If you have used URL categories as criteria within a policy then those categories alone are available to specify actions against within the same policy. Some of the options described below may differ or be unavailable because of this.

Step 1 Choose one of **Access Policies**, **Cisco Data Security Policies**, or **Encrypted HTTPS Management** from the Web Security Manager menu.

Step 2 Find the required policy name in the policies table.

Step 3 Click the cell link in the URL Filtering column on the same row.

Step 4 (Optional) Add custom URL categories:

a) Click **Select Custom Categories**.

b) Choose which custom URL categories to include in this policy and click **Apply**.

Choose which custom URL categories the URL filtering engine should compare the client request against. The URL filtering engine compares client requests against included custom URL categories, and ignores excluded custom URL categories. The URL filtering engine compares the URL in a client request to included custom URL categories before predefined URL categories.

The custom URL categories included in the policy appear in the Custom URL Category Filtering section.

Step 5 Choose an action for each custom and predefined URL category.

Note Available actions vary between custom and predefined categories and between policy types.

Step 6 In the Uncategorized URLs section, choose the action to take for client requests to web sites that do not fall into a predefined or custom URL category.

Step 7 Submit and commit your changes.

Remote Users

About Remote Users

Cisco AnyConnect Secure Mobility extends the network perimeter to remote endpoints, enabling the integration of web filtering services offered by the Web Security Appliance .

Remote and mobile users use the Cisco AnyConnect Secure VPN (virtual private network)client to establish VPN sessions with the Adaptive Security Appliance (ASA). The ASA sends web traffic to the Web Security Appliance along with information identifying the user by IP address and user name. The Web Security Appliance scans the traffic, enforces acceptable use policies, and protects the user from security threats. The security appliance returns all traffic deemed safe and acceptable to the user.

When Secure Mobility is enabled, you can configure identities and policies to apply to users by their location:

- **Remote users.** These users are connected to the network from a remote location using VPN. The Web Security Appliance automatically identifies remote users when both the Cisco ASA and Cisco AnyConnect client are used for VPN access. Otherwise, the Web Security Appliance administrator must specify remote users by configuring a range of IP addresses.
- **Local users.** These users are connected to the network either physically or wirelessly.

When the Web Security Appliance integrates with a Cisco ASA, you can configure it to identify users by an authenticated user name transparently to achieve single sign-on for remote users.

How to Configure Identification of Remote Users

Task	Further information
1. Configure identification of remote users.	Configuring Identification of Remote Users, on page 25
2. Create an identity for remote users.	Classifying Users and Client Software **1.** In the "Define Members by User Location" section, select Remote Users Only. **2.** In the "Define Members by Authentication" section, select "Identify Users Transparently through Cisco ASA Integration."
3. Create a policy for remote users.	Creating a Policy , on page 7

Configuring Identification of Remote Users

Step 1 Security Services > AnyConnect Secure Mobility, and click **Enable**.

Step 2 Read the terms of the AnyConnect Secure Mobility License Agreement, and click **Accept**.

Step 3 Configure how to identify remote users.

Option	Description	Additional Steps
IP Address	Specify a range of IP addresses that the appliance should consider as assigned to remote devices.	**a.** Enter a range of IP addresses in the IP Range field. **b.** Go to step 4

Option	Description	Additional Steps
Cisco ASA Integration	Specify one or more Cisco ASA the Web Security Appliance communicates with. The Cisco ASA maintains an IP address-to-user mapping and communicates that information with the Web Security Appliance . When the Web Proxy receives a transaction, it obtains the IP address and determines the user by checking the IP address-to-user mapping. When users are determined by integrating with a Cisco ASA, you can enable single sign-on for remote users.	**a.** Enter the Cisco ASA host name or IP address. **b.** Enter the port number used to access the ASA. The default port number for the Cisco ASA is 11999. **c.** If multiple Cisco ASA are configured in a cluster, click **Add Row** and configure each ASA in the cluster. **Note** If two Cisco ASA are configured for high availability, enter only one host name or IP address for the *active* Cisco ASA. **d.** Enter the access passphrase for the Cisco ASA. **Note** The passphrase you enter here must match the access passphrase configured for the specified Cisco ASA. **e.** Optional, click **Start Test** to verify the Web Security Appliance can connect to the configured Cisco ASA.

Step 4 Submit and Commit Changes.

Note Enable AnyConnect Security Mobility (**Security Services** > **AnyConnect Security Mobility**) to make the Define Members by User Location option available on the Web Security Appliance . By default, this option is available on the Cisco Content Security Management Appliance (**Web** > **Configuration Master** > **Identification Profiles**). When you use the Define Members by User Location option to configure an identification profile in the Security Management Appliance and publish that configuration to the Web Security Appliance where AnyConnect Security Mobility is not enabled, the identification profile is disabled.

Display Remote User Status and Statistics for ASAs

Use this command to display information related to Secure Mobility when the Web Security Appliance is integrated with an ASA.

Command	Description
`musstatus`	This command displays the following information: • The status of the Web Security Appliance connection with each ASA. • The duration of the Web Security Appliance connection with each ASA in minutes. • The number of remote clients from each ASA. • The number of remote clients being serviced, which is defined as the number of remote clients that have passed traffic through the Web Security Appliance . • The total number of remote clients.

Troubleshooting Policies

- Access Policy not Configurable for HTTPS
- Some Microsoft Office Files Not Blocked
- Blocking DOS Executable Object Types Blocks Updates for Windows OneCare
- Identification Profile Disappeared from Policy
- Policy is Never Applied
- HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication
- User Matches Global Policy for HTTPS and FTP over HTTP Requests
- User Assigned Incorrect Access Policy
- Policy Troubleshooting Tool: Policy Trace