Intercepting Web Requests

This topic contains the following sections:

Overview of Intercepting Web Requests

The Secure Web Appliance intercepts requests that are forwarded to it by clients or other devices over the network.

The appliance works in conjunction with other network devices to intercept traffic. These may be ordinary switches, transparent redirection devices network taps,and other proxy servers or Secure Web Appliances.

Tasks for Intercepting Web Requests

Steps	Task	Links to Related Topics and Procedures
Step 1	Review best practices.	• Best Practices for Intercepting Web Requests, on page 2

Steps	Task	Links to Related Topics and Procedures
Step 2	(Optional) Perform follow up networking tasks: • Connect and configure upstream proxies. • Configure network interface ports. • Configure transparent redirection devices. • Configure TCP/IP routes. • Configure VLANs.	• Upstream Proxies • Network Interfaces • Configuring Transparent Redirection • Configuring TCP/IP Traffic Routes • Increasing Interface Capacity Using VLANs
Step 3	(Optional) Perform follow up Web Proxy tasks: • Configure the web proxy to operate in either Forward or Transparent mode. • Decide if additional services are needed for the protocol types you want to intercept • Configure IP spoofing. • Manage the web proxy cache. • Use custom web request headers. • Bypass the proxy for some requests.	• Web Proxy Options for Intercepting Web Requests, on page 3 • Configuring Web Proxy Settings, on page 3 • Web Proxy Options for Intercepting Web Requests, on page 3 • Web Proxy Cache, on page 6 • Web Proxy IP Spoofing, on page 9 • Web Proxy Bypassing, on page 11
Step 4	Perform client tasks: • Decide how clients should redirect requests to the web proxy. • Configure clients and client resources.	• Client Options for Redirecting Web Requests, on page 17 • Using PAC Files with Client Applications, on page 17
Step 5	(Optional) Enable and Configure the FTP proxy.	• FTP Proxy Services, on page 20

Best Practices for Intercepting Web Requests

- Enable only the proxy services you require.
- Use the same forwarding and return method (either L2 or GRE) for all WCCP services defined in the Secure Web Appliance. This allows the proxy bypass list to work consistently.
- Ensure that users cannot access PAC files from outside the corporate network. This allows your mobile workers to use the web proxy when they are on the corporate network and to connect directly to web servers at other times.
- Allow a web proxy to accept X-Forwarded-For headers from trustworthy downstream proxies or load balancers only.
- Leave the web proxy in the default transparent mode, even if initially using only explicit forwarding. Transparent mode also accepts explicitly forwarded requests.

Web Proxy Options for Intercepting Web Requests

By itself, the Web Proxy can intercept web requests that use HTTP (including FTP over HTTP) and HTTPS. Additional proxy modules are available to enhance protocol management:

- **FTP Proxy.** The FTP Proxy allows the interception of native FTP traffic (rather than just FTP traffic that has been encoded within HTTP).
- **HTTPS Proxy.** The HTTPS proxy supports the decryption of HTTPS traffic and allows the web proxy to pass unencrypted HTTPS requests on to policies for content analysis.

Note When in transparent mode, the Web Proxy drops all transparently redirected HTTPS requests if the HTTPS proxy is not enabled. No log entries are created for dropped transparently redirected HTTPS requests.

- **SOCKS Proxy.** The SOCKS proxy allows the interception of SOCKS traffic.

Each of these additional proxies requires the Web Proxy in order to function.You cannot enable them if you disable the Web Proxy.

Note The Web proxy is enabled by default. All other proxies are disabled by default.

Related Topics

- FTP Proxy Services, on page 20
- SOCKS Proxy Services, on page 22

Configuring Web Proxy Settings

Before you begin

Enable the web proxy.

Step 1 Choose **Security Services** > **Web Proxy**.

Step 2 Click **Edit Settings**.

Step 3 Configure the basic web proxy settings as required.

Property	Description
HTTP Ports to Proxy	The ports that the web Proxy will listen on for HTTP connections
Caching	Specifies whether to enable or disable Web Proxy caching. The web proxy caches data to increase performance.

Property	Description
Proxy Mode	• **Transparent** (Recommended) — Allow the web proxy to name the internet target. The web proxy can intercept both transparent and explicitly forwarded web requests in this mode. • **Forward** — Allow the client browser to name the internet target. Requires individual configuration of each web browser to use the web proxy. The web proxy can intercept only explicitly forwarded web requests in this mode.
IP Spoofing Connection Type	If you have selected the Proxy Mode as **Transparent**, choose one of the IP spoofing connection types: • **For Transparent Connections Only** - To configure IP Spoofing for transparent connections only. • **For All Connections** - To configure IP Spoofing for Transparent and Explicit connections. If you have selected the Proxy Mode as **Forward**, then the IP Spoofing Connection Type is always Explicit. **Note** The IP spoofing connection type that you choose is applicable for all protocols - native FTP, HTTP, and HTTPS. To add IP spoofing profiles in routing policies, see Adding Routing Destination and IP Spoofing Profile to Routing Policy

Step 4 Complete the advanced web proxy settings as required.

Property	Description
Persistent Connection Timeout	The maximum time in seconds the web proxy keeps open a connection to a client or server after a transaction has been completed and no further activity is detected. • **Client side.** The timeout value for connections to clients. • **Server side.** The timeout value for connections to servers. If you increase these values connections will remain open longer and reduce the overhead used to open and close connections repeatedly. However, you also reduce the ability of the Web Proxy to open new connections if the maximum number of simultaneous persistent connections has been reached. After establishing a connection and performing an SSL handshake, if client requests are not sent to the proxy, the proxy waits for the persistent connection timeout, and then ceases its connection with the client. Cisco recommends keeping the default values.
In-Use Connection Timeout	The maximum time in seconds that the web proxy waits for more data from an idle client or server when the current transaction has not yet been completed. • **Client side.** The timeout value for connections to clients. • **Server side.** The timeout value for connections to servers.

Property	Description
Simultaneous Persistent Connections (Server Maximum Number)	The maximum number of connections (sockets) the Web Proxy keeps open with servers.
Maximum Connections Per Client	Restricts the number of concurrent connections initiated by the client to a configured value. When the number of connections exceed the configured limit, the connections are dropped, and an alert is sent to the administrator. **Note** By default, Maximum Connections Per Client is disabled. To configure the limit, check the **Maximum Connections Per Client** check box, and do the following: • **Connections**—Enter the number of permissible concurrent connections. • **Exempted Downstream Proxy or Load Balancer**—Enter the IP address of the downstream proxy, load balancer, or any other client IP address (you cannot configure the subnets or host names). The web proxy does not apply the restrictions of the concurrent connections on the IP addresses that are included in this exempted list.
Generate Headers	Generate and add headers that encode information about the request. • **X-Forwarded-For** headers encode the IP address of the client from which an HTTP request originated. **Note** • To turn header forwarding on or off, use the CLI `advancedproxyconfig` command, Miscellaneous option, "Do you want to pass HTTP X-Forwarded-For headers?" • Using an explicit forward upstream proxy to manage user authentication or access control with proxy authentication requires forwarding of these headers. • For transparent HTTPS requests, the appliance does not decrypt the XFF header. For explicit requests, the appliance uses the XFF header received in the CONNECT request, and does not decrypt the XFF inside the SSL tunnel, so identification of client IP Addresses using X-Forwarded-For is not applicable for HTTPS transparent requests. • **Request Side VIA** headers encode the proxies through which the request passed on its way from the client to the server. • **Response Side VIA** headers encode the proxies through which the request passed on its way from the server to the client.
Use Received Headers	Allows a Web proxy deployed as an upstream proxy to identify clients using X-Forwarded-For headers send by downstream proxies. The Web Proxy will not accept the IP address in a X-Forwarded-For header from a source that is not included in this list. If enabled, requires the IP address of a downstream proxy or load balancer (you cannot enter subnets or host names).

Property	Description
Range Request Forwarding	Use the **Enable Range Request Forwarding** check box to enable or disable forwarding of range requests. Refer to Managing Access to Web Applications for more information.

Step 5 Submit and commit your changes.

What to do next

- Web Proxy Cache, on page 6
- Configuring Transparent Redirection

Web Proxy Cache

The web proxy caches data to increase performance. AsyncOS includes defined caching modes that range from safe to aggressive, and also allows customized caching. You can also exclude specific URLs from being cached, either by removing them from the cache, or by configuring the cache to ignore them.

Clearing the Web Proxy Cache

Step 1 Choose **Security Services** > **Web Proxy**.

Step 2 Click **Clear Cache** and confirm your action.

Removing URLs from the Web Proxy Cache

Step 1 Access the CLI.

Step 2 Use the `webcache > evict` commands to access the required caching area:

```
example.com> webcache
Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> evict
Enter the URL to be removed from the cache.
[]>
```

Step 3 Enter the URL to be removed from the cache.

Note If you do not include a protocol in the URL, `http://` will be prepended to it (e.g., `www.cisco.com` will become `http://www.cisco.com`)

Specifying Domains or URLs that the Web Proxy never Caches

Step 1 Access the CLI.

Step 2 Use the `webcache` -> `ignore` commands to access the required submenus:

```
example.com> webcache
Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> ignore
Choose the operation you want to perform:
- DOMAINS - Manage domains
- URLS - Manage urls
[]>
```

Step 3 Enter the address type you wish to manage: `DOMAINS` or `URLS`.

```
[]> urls
Manage url entries:
Choose the operation you want to perform:
- DELETE - Delete entries
- ADD - Add new entries
- LIST - List entries
[]>
```

Step 4 Enter **add** to add new entries:

```
[]> add
Enter new url values; one on each line; an empty line to finish
[]>
```

Step 5 Enter domains or URLs, one per line; for example:

```
Enter new url values; one on each line; an empty line to finish
[]> www.example1.com
Enter new url values; one on each line; an empty line to finish
[]>
```

You can include certain regular expression (regex) characters when specifying a domain or URLs. With the `DOMAINS` option, you can use a preceding dot character to exempt an entire domain and its subdomains from caching. For example, you can enter `.google.com` rather than simply `google.com` to exempt www.google.com, docs.google.com, and so on.

With the `URLS` option, you can use the full suite of regular-expression characters. See Regular Expressions for more information about using regular expressions.

Step 6 When you are finished entering values, press Enter until you are returned to the main command-line interface.

Step 7 Commit your changes.

Choosing The Web Proxy Cache Mode

Step 1 Access the CLI.

Step 2 Use the `advancedproxyconfig -> caching` commands to access the required submenus:

```
example.com> advancedproxyconfig
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]> caching
Enter values for the caching options:
The following predefined choices exist for configuring advanced caching
options:
1. Safe Mode
2. Optimized Mode
3. Aggressive Mode
4. Customized Mode
Please select from one of the above choices:
[2]>
```

Step 3 Enter a number corresponding to the web proxy cache settings you require:

Entry	Mode	Description
1	Safe	The least caching and the most adherence to RFC #2616 compared to the other modes.
2	Optimized	Moderate caching and moderate adherence to RFC #2616. Compared to safe mode, in optimized mode the Web Proxy caches objects when no caching time is specified when a Last-Modified header is present. The Web Proxy caches negative responses.
3	Aggressive	The most caching and the least adherence to RFC #2616. Compared to optimized mode, aggressive mode caches authenticated content, ETag mismatches, and content without a Last-Modified header. The Web Proxy ignores the no-cache parameter.
4	Customized mode	Configure each parameter individually.

Step 4 If you chose option 4 (Customized mode), enter values (or leave at the default values) for each of the custom settings.

Step 5 Press **Enter** until you return to the main command interface.

Step 6 Commit your changes.

What to do next

Related Topics

- Web Proxy Cache, on page 6.

Web Proxy IP Spoofing

When the web proxy forwards a request, it changes the request source IP address to match its own address by default. This increases security, but you can change this behavior by implementing IP spoofing, so that requests appear to originate from client IP or any other routable custom IP address rather than from the Secure Web Appliance. You can configure Web Proxy IP Spoofing by creating IP spoofing profiles for custom IP addresses and adding them to the routing policies.

IP spoofing works for transparent and explicitly forwarded traffic. When the Web Proxy is deployed in transparent mode, you can configure the IP Spoofing Connection Type for transparently redirected connections only or for all connections (transparently redirected and explicitly forwarded). If explicitly forwarded connections use IP spoofing, you should ensure that you have appropriate network devices to route return packets back to the Secure Web Appliance.

When IP spoofing is enabled and the appliance is connected to a WCCP router, you must configure two WCCP services: one based on source ports and one based on destination ports.

IP spoofing profiles have a limitation when the HTTPS traffic is transparently redirected. See Accessing HTTPS Sites Using Routing Policies with URL Category Criteria.

Related Topics

- Creating IP Spoofing Profiles, on page 9
- Configuring Web Proxy Settings, on page 3
- Configuring WCCP Services

Creating IP Spoofing Profiles

Before you begin

Make sure that you have selected the proxy mode and IP spoofing connection type in the web proxy settings. For more information, see Configuring Web Proxy Settings, on page 3.

Step 1 Choose **Web Security Manager** > **IP Spoofing Profiles**.

Step 2 Click **Add Profile**.

Step 3 Enter a name for the IP spoofing profile.

Step 4 Enter the IP address that you want to assign to the spoofing profile name.

Step 5 Submit and commit your changes.

What to do next

Add the IP spoofing profile to a routing policy. For more information, see Adding Routing Destination and IP Spoofing Profile to Routing Policy.

Related Topics

Editing IP Spoofing Profiles, on page 10
Deleting IP Spoofing Profiles, on page 10

Editing IP Spoofing Profiles

Note Once you update an IP spoofing profile, it will be updated in all the routing policies associated with that profile.

Step 1 Choose **Web Security Manager** > **IP Spoofing Profiles**.

Step 2 Click the IP spoofing profile name link that you want to edit.

Step 3 Modify the profile details.

Step 4 Submit and commit your changes.

Deleting IP Spoofing Profiles

Step 1 Choose **Web Security Manager** > **IP Spoofing Profiles**.

Step 2 Click the trash can icon corresponding to the IP spoofing profile that you want to delete.

Note The appliance displays a warning if the IP spoofing profile that you are deleting is assigned to one or more routing policies. In this case, select a different IP spoofing profile to be assigned to all those affected routing policies.

Step 3 Submit and commit your changes.

Web Proxy Custom Headers

You can add custom headers to specific outgoing transactions to request special handling from destination servers. For example, if you have a relationship with YouTube for Schools, you can use a custom header to identify transaction requests to YouTube.com as coming from your network and as requiring special handling.

Adding Custom Headers To Web Requests

Step 1 Access the CLI.

Step 2 Use the `advancedproxyconfig -> customheaders` commands to access the required submenus:

```
example.com> advancedproxyconfig
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
```

```
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]> customheaders
Currently defined custom headers:
Choose the operation you want to perform:
- DELETE - Delete entries
- NEW - Add new entries
- EDIT - Edit entries
[]>
```

Step 3 Enter the required subcommand as follows:

Option	Description
`Delete`	Deletes the custom header you identify. Identify the header to delete using the number associated with the header in the list returned by the command.

`New`	Creates the header you provide for use with the domain or domains you specify.
	Example header:
	X-YouTube-Edu-Filter: ABCD1234567890abcdef
	(The value in this case is a unique key provided by YouTube.)
	Example domain:
	youtube.com
	The maximum length of the custom header is 16k and may contain arbitrary values as well except CR or LF.
	Example custom header:
	`Choose the operation you want to perform:`
	`- DELETE - Delete entries`
	`- NEW - Add new entries`
	`- EDIT - Edit entries`
	`[]> new`
	`Please enter the custom HTTP header (in the form field: value):`
	`[]>`
	`[:characters colon(:) and double quotes(") are not allowed]`

`Edit`	Replaces an existing header with one you specify. Identify the header to delete using the number associated with the header in the list returned by the command.

Step 4 Press **Enter** until you return to the main command interface.

Step 5 Commit your changes.

Web Proxy Bypassing

Web Proxy Bypassing for Web Requests

You can configure the Secure Web Appliance so that transparent requests from particular clients, or to particular destinations, bypass the Web Proxy.

Bypassing the web proxy allows you to:

- Prevent interference with non-HTTP-compliant (or proprietary) protocols that use HTTP ports but do not work properly when they connect to a proxy server.
- Ensure that traffic from a particular machine inside the network, such as a malware test machine, bypasses the Web Proxy and all its built-in security protection.

Bypassing only works for requests that are transparently redirected to the web proxy. The web proxy processes all requests that clients explicitly forward to it, whether the proxy is in transparent or forward mode.

Configuring Web Proxy Bypassing for Web Requests

Step 1 Choose **Web Security Manager > Bypass Settings**.

Step 2 Click **Edit Bypass Settings**.

Step 3 Enter the addresses for which you wish to bypass the web proxy.

Note When you configure /0 as a subnet mask for any IP in the bypass list, the appliance bypasses all the web traffic. In this case, the appliance interprets the configuration as 0.0.0.0/0.

Step 4 Choose the Custom URL Categories that you want to add to the proxy bypass list.

Note You cannot set the web proxy bypass for Regular Expressions.

Note Once you add the Custom URL Categories to the proxy bypass list, all the IP addresses and the domain names of the Custom URL categories are bypassed for both the source and destination.

Step 5 Submit and commit your changes.

Configuring Web Proxy Bypassing for Applications

Step 1 Choose **Web Security Manager > Bypass Settings**.

Step 2 Click **Edit Application Bypass Settings**.

Step 3 Select the application(s) you wish to bypass scanning for.

Step 4 Submit and commit your changes.

Note Webex bypass settings are only applicable to HTTPS traffic. However, for HTTP traffic the applications can be blocked via Access Policies.

Web Proxy Custom Headers Per Policy

You can configure custom header profiles for HTTP requests and can create multiple headers under a header rewrite profile. Each profile can have a maximum of 12 headers. You can also modify or delete the existing header profiles. You can add the header rewrite profile to an existing access policy to include the headers in all the transactions to which the particular access policy is applied.

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.

- Creating Header Rewrite Profiles for HTTP Web Requests, on page 13
- Modifying Username and Group Header Formats , on page 14 (optional)
- Adding Header Profiles To Access Policy, on page 15

Recommend not to create web proxy custom headers using the CLI command`advancedproxyconfig -> customheader` from AsynOS verion 14.0 onwards.

Creating Header Rewrite Profiles for HTTP Web Requests

Step 1 Choose **Web Security Manager** -> **HTTP Rewrite Profiles**

Step 2 Click **Add Profile**.

Step 3 Assign a unique name to the header rewrite profile that you want to create.

Step 4 In the **Headers** area, enter the following information:

Note You can enter empty or null header value in Header Rewrite Profiles. When you save and commit the header with null or no value, the header is not included in the outgoing requests. For example, if you want to hide header `Via` to outbound server, add header-name `Via` to HTTP Rewrite Profiles with value `""`.

- **Header Name** — Enter the header name that you want to add to the HTTP requests. Example: X-Client-IP, X-Authenticated-User, X-Authenticated-Groups, etc.
- **Header Value** —Enter the value to be included in the request header corresponding to the header name. Prefix the header variables with :
  - `$ReqMeta`— to fetch standard HTTP header variables such as client IP, user, group etc. For example, to include username in the request header, the format is `($ReqMeta[X-Authenticated-User])`
  - `$ReqHeader`— to use the values of the standard HTTP hearders or values of other headers defined under the same header rewrite profile.

    For example,

    ```
    Header1:32

    Header2: 44-($ReqHeader[Header1])-46
    ```

    Then the value of `Header 2` is `44-32-46`
- **Text Format**—Choose the text format for encoding. The available options are ASCII and UTF-8
- **Binary Encoding**— Choose whether you want binary encoding (Base64) or not for the request headers.

Note Based on the server type, the appliance displays an error message if the size of the request header field sent exceeds the maximum limit of the server. For example, different server types support different header lengths:

- Apache 2.0, 2.2: 8k
- Nginx: 4k - 8k
- IIS(varies by version): 8K - 16K
- Tomcat: (varies by version) 8K

In case of user identification using ISE, the global X-authentication headers settings i.e., X-Authenticated-User and X-Authenticated-Groups, do not apply domain and authentication mechanism as prefix.

You can enter UTF+8 as `($ReqMeta[HTTP_header])` value even if you select text format as ASCII. Currenlty, the following headers support `($ReqMeta[HTTP_header])` :

- X-Authenticated-User
- X-Authenticated-Groups
- X-Client-IP

The headers are not included in the outgoing requests, if the values of the headers are null. This happens when you do not :

- Enable proxy authentication
- Define groups in membership criteria for access policy, decryption policy, or routing policy.

Step 5 Submit and commit your changes.

Modifying Username and Group Header Formats

Step 1 Choose **Web Security Manager** > **HTTP Rewrite Profiles**

Step 2 Click **Edit Settings**.

Step 3 Modify the formats.

Allowed formats are:

- Username -`$authMechanism://$domainName/$userName, $authMechanism:\\$domainName\$userName, $domainName/$userName, $domainName\$userName, $userName`
- Group- `$authMechanism://$domainName/$groupName, $authMechanism:\\$domainName\$groupName, $domainName/$groupName, $domainName\$groupName, $groupName`

  You can also modify the delimiter such as comma (,), colon (:), semicolon (;), backslash(\), vertical bar (|), and so on.

Step 4 Submit and commit your changes.

Adding Header Profiles To Access Policy

Before you begin

Configure access policy. See Creating a Policy.

Step 1 Choose **Web Security Manager** > **Access Policies**

Step 2 In the Access Policies page, click the link for HTTP Rewrite Profile.

You can also create a new access policy and add the Header Rewrite profile to it. To create a new access policy, seeCreating a Policy

Step 3 Select the header rewrite profile that you want to add to the policy. After you add, the headers are included in the HTTP transaction to which the particular access policy is applied.

Step 4 Submit and commit your changes.

You can delete a header rewrite profile linked to an access policy. Before you delete, choose another profile and the selected profile will be applied to the access policies automatically.

Web Proxy Usage Agreement

You can configure the Secure Web Appliance to inform users that it is filtering and monitoring their web activity. The appliance does this by displaying an end-user acknowledgment page when a user first accesses a browser after a certain period of time. When the end-user acknowledgment page appears, users must click a link to access the original site requested or any other website.

Related Topics

- Notify End-Users of Proxy Actions

Domain Map

You can configure the Secure Web Appliance so that transparent HTTPS requests from particular clients, or to particular destinations, bypass the HTTPS Proxy.

You can use passthrough for applications that require traffic to pass through the appliance, without undergoing any modification, or certificate checks of the destination servers.

Domain Map for Specific Applications

Before you begin

Ensure you have an identification policy defined for the devices that require pass through traffic to specific servers. See Classifying Users and Client Software for more information. Specifically, you must:

- Choose **Exempt from authentication/identification**.

- Specify the addresses to which this Identification Profile should apply. You can use IP addresses, CIDR blocks, and subnets.

Step 1 Enable HTTPS Proxy. See Enabling the HTTPS Proxy for more information.

Step 2 Choose **Web Security Manager** > **Domain Map**.

a) Click **Add Domain**.
b) Enter the **Domain Name** or the destination server.
c) Choose the order of the priority if there are existing domains specified.
d) Enter the IP addresses.
e) Click **Submit**.

Step 3 Choose **Web Security Manager** > **Custom and External URL Categories**.

a) Click **Add Category**.
b) Provide the following information.

Setting	Description
Category Name	Enter an identifier for this URL category. This name appears when you configure URL filtering for policy groups.
List Order	Specify the order of this category in the list of custom URL categories. Enter "1" for the first URL category in the list. The URL filtering engine evaluates a client request against the custom URL categories in the order specified.
Category Type	Choose **Local Custom Category**.
Advanced	You can enter regular expressions in this section to specify additional sets of addresses. You can use regular expressions to specify multiple addresses that match the patterns you enter. See Regular Expressions for more information about using regular expressions.

c) Submit and commit the changes.

Step 4 Choose **Web Security Manager** > **Decryption Policies**.

a) Create a new decryption policy.
b) Choose the identification profile that you created for bypassing HTTPS traffic for specific applications.
c) In the **Advanced** panel, click the link for URL Categories.
d) In the **Add** column, click to add the custom URL category created in step 3.
e) Click **Done**.
f) In the Decryption Policies page, click the link for **URL Filtering**.
g) Choose **Pass Through**.
h) Submit and commit the changes.

You can use the **%(** format specifier to view access log information. See Customizing Access Logs for more information.

Note

- The Domain Map feature works in HTTPS Transparent mode.
- This feature does not work in Explicit mode and for HTTP traffic.
- Local Custom Category must be configured to allow the traffic using this feature.
- Enabling this feature will modify or assign the server name as per the server name configured in the Domain Map, even if SNI information is available.
- This feature does not block traffic based on domain name if that traffic matches the Domain Map and corresponding custom category, decryption policy and passthrough action are configured.
- Authentication does not work with this pass through feature. Authentication requires decryption, but traffic will not be decrypted in this case.
- UDP traffic is not monitored. You must configure UDP traffic not to come to the Secure Web Appliance, instead it should go directly through firewall to the internet for applications like WhatsApp, Telegram etc.
- WhatsApp, Telegram and Skype works in Transparent mode. However, some apps like WhatsApp do not work in Explicit mode due to restrictions on the app.

Client Options for Redirecting Web Requests

If you choose to have clients explicitly forward requests to the web proxy, you must also decide how to configure the clients to do this. Choose from the following methods:

- **Configure Clients Using Explicit Settings.** Configure clients with the web proxy hostname and port number. See individual client documentation for details on how to do this.

Note The web proxy port uses port numbers 80 and 3128 by default. Clients can use either port.

- **Configure Clients Using a Proxy Auto-Config (PAC) File.** PAC files provide clients with instructions on where to direct web requests. This options allows you to centrally manage subsequent changes to the proxy details.

If you choose to use PAC files, you must also choose where to store them and how clients will find them.

Related Topics

- Using PAC Files with Client Applications, on page 17

Using PAC Files with Client Applications

Options For Publishing Proxy Auto-Config (PAC) Files

You must publish PAC files where clients can access them. Valid locations are:

- **Web servers.**

- **Secure Web Appliance**.You can place PAC files on a Secure Web Appliance, which appears to clients as a web browser. The appliance also offers additional options to manage PAC files, including the ability to service requests that use different hostnames, ports, and file names.
- **Local machines.** You can place the PAC file locally on a client's hard disk. Cisco does not recommend this as a general solution, and it is not suited to automatic PAC file detection methods, but it can be useful for testing.

Related Topics

- Hosting PAC Files on the Secure Web Appliance, on page 18
- Specifying PAC Files in Client Applications, on page 19
- Hosting PAC Files on the Secure Web Appliance, on page 18
- Specifying PAC Files in Client Applications, on page 19

Client Options For Finding Proxy Auto-Config (PAC) Files

If you choose to use PAC files for your clients, you must also choose how clients will find the PAC files. You have two options:

- **Configure client with the PAC file location.** Configure the client with a URL that specifically points to the PAC file.
- **Configure clients to detect the PAC file location automatically.** Configure clients to find PAC files automatically using the WPAD protocol along with DHCP or DNS.

Automatic PAC File Detection

WPAD is a protocol that allows the browser determine the location of a PAC file using DHCP and DNS.

- **To use WPAD with DHCP**, you must set up option 252 on the DHCP server's with the url of the PAC file location. Not all browsers support DHCP, however.
- **To use WPAD with DNS**, you must configure a DNS record to point to the PAC file's host server.

You can configure either or both options. WPAD will first try to find PAC files using DHCP, and if it cannot, it will then try DNS.

Related Topics

- Detecting the PAC File Automatically in Clients, on page 20

Hosting PAC Files on the Secure Web Appliance

Step 1 Choose **Security Services > PAC File Hosting**

Step 2 Click **Enable and Edit Settings**.

Step 3 (Optional) Complete the following basic settings:

Option	Description
PAC Server Ports	The ports that the Secure Web Appliance will use to listen for PAC file requests.

Option	Description
PAC File Expiration	Allows the PAC file to expire after a specified number of minutes in the browser's cache.

Step 4 Click **Browse** in the PAC Files section and select a PAC file from your local machine for upload to the Secure Web Appliance.

Note If the file you select is called `default.pac` , you do not have to specify the file name when configuring its location in a browser. The Secure Web Appliance looks for a file called `default.pac` if no name is specified.

Step 5 Click **Upload** to upload the PAC file selected in step 4 to the Secure Web Appliance.

Step 6 (Optional) In the Hostnames for Serving PAC Files Directly section, configure hostnames and associated file names for PAC file requests that do not include a port number:

Option	Description
Hostname	The hostname that the PAC file request must include if the Secure Web Appliance is to service the request. As the request does not include a port number, it will be processed through the Web Proxy HTTP ports (e.g. port 80) and must be distinguishable as a PAC file request through this hostnamevalue.
Default PAC File for "Get/" Request through Proxy Port	The PAC file name that will be associated with the hostname on the same row. Request to the hostname will return the PAC file specified here. Only PAC files that have been uploaded are available for selection.
Add Row	Adds another row to specify additional hostnames and PAC file names.

Step 7 Submit and commit your changes.

Specifying PAC Files in Client Applications

Configuring a PAC File Location Manually in Clients

Step 1 Create and publish a PAC file.

Step 2 Enter a URL in your browser's PAC file configuration area that points to the PAC file location.

The following are valid URL formats if the Secure Web Appliance is hosting the PAC file:

```
http://server_address[.domain][:port][/filename] | http://WSAHostname[/filename]
```

where *WSAHostname* is the **hostname** value configured when hosting the PAC file on a Secure Web Appliance. Otherwise the URL format will depend on the storage location and, in some cases, on the client.

What to do next

- Hosting PAC Files on the Secure Web Appliance, on page 18

Detecting the PAC File Automatically in Clients

Step 1 Create a PAC file called wpad.dat and publish it to a web server or Secure Web Appliance (the file must be placed in a web server's root folder if you intend using WPAD with DNS).

Step 2 Configure the web server to set up .dat files with the following MIME type:

```
application/x-ns-proxy-autoconfig
```

Note A Secure Web Appliance does this for you automatically.

Step 3 To support DNS lookup, create an internally resolvable DNS name beginning with ' `wpad` ' (for example, `wpad.example.com`) and associate it with the IP address of the server hosting the `wpad.dat` file.

Step 4 To support DHCP lookup, configure your DHCP server's option 252 with the url of the wpad.dat file location (for example: " `http://wpad.example.com/wpad.dat` "). The URL can use any valid host address, including an IP address, and does not require a specific DNS entry.

What to do next

- Using PAC Files with Client Applications, on page 17
- Hosting PAC Files on the Secure Web Appliance, on page 18
- WPAD Not Working With Firefox

FTP Proxy Services

- Overview of FTP Proxy Services, on page 20
- Enabling and Configuring the FTP Proxy, on page 21

Overview of FTP Proxy Services

The web proxy can intercept two types of FTP requests:

- **Native FTP.** Native FTP requests are generated by dedicated FTP clients (or by browsers using built-in FTP clients). Requires the FTP proxy.
- **FTP over HTTP.** Browsers sometimes encode FTP requests inside HTTP requests, rather than using native FTP. Does not require the FTP proxy.

Related Topics

- Enabling and Configuring the FTP Proxy, on page 21
- Configuring FTP Notification Messages

Enabling and Configuring the FTP Proxy

Note To configure proxy settings that apply to FTP over HTTP connections, see Configuring Web Proxy Settings, on page 3.

Step 1 Choose **Security Services** > **FTP Proxy**.

Step 2 Click **Enable and Edit Settings** (if the only available option is **Edit Settings** then the FTP proxy is already enabled).

Step 3 (Optional) Configure the basic FTP Proxy settings.

Property	Description
Proxy Listening Port	The port that the FTP Proxy will listen to for FTP control connections. Clients should use this port when configuring an FTP proxy (not as the port for connecting to FTP servers, which normally use port 21).
Caching	Whether of not data connections from anonymous users are cached. **Note** Data from non-anonymous users is never cached.
Server Side IP Spoofing	Allows the FTP Proxy to imitate the FTP server's IP address. This supports FTP clients that do not allow transactions when the IP address is different for the control and data connections.
Client IP Spoofing	Allows the FTP Proxy to imitate the FTP client's source IP address. When enabled, the FTP requests appear to originate from the FTP client rather than the FTP Proxy.
Authentication Format	Allows a choice of authentication format the FTP Proxy can use when communicating with FTP clients.
Passive Mode Data Port Range	The range of TCP ports that FTP clients should use to establish a data connection with the FTP Proxy for passive mode connections.
Active Mode Data Port Range	The range of TCP ports FTP servers should use to establish a data connection with the FTP Proxy for active mode connections. This setting applies to both native FTP and FTP over HTTP connections. Increasing the port range accommodates more requests from the same FTP server. Because of the TCP session TIME-WAIT delay (usually a few minutes), a port does not become available again for the *same* FTP server immediately after being used. As a result, any given FTP server cannot connect to the FTP Proxy in active mode more than *n* times in a short period of time, where *n* is the number of ports specified in this field.
Welcome Banner	The welcome banner that appears in FTP clients during connection. Choose from: • **FTP server message.** The message will be provided by the destination FTP server. This option is only available when the web proxy is configured for transparent mode, and only applies for transparent connections. • **Custom message.** When selected, this custom message is displayed for all native FTP connections. When not selected, this is still used for explicit forward native FTP connections.

Step 4 (Optional) Configure the advanced FTP Proxy settings:

Property	Description
Control Connection Timeouts	The maximum number of seconds the FTP Proxy waits for more communication in the control connection from an idle FTP client or FTP server when the current transaction has not been completed. • **Client side.** The timeout value for control connections to idle FTP clients. • **Server side.** The timeout value for control connections to idle FTP servers.
Data Connection Timeouts	How long the FTP Proxy waits for more communication in the data connection from an idle FTP client or FTP server when the current transaction has not been completed. • **Client side.** The timeout value for data connections to idle FTP clients. • **Server side.** The timeout value for data connections to idle FTP servers.

Step 5 Submit and commit your changes.

What to do next

- Overview of FTP Proxy Services, on page 20

SOCKS Proxy Services

Overview of SOCKS Proxy Services

The Secure Web Appliance includes a SOCKS proxy to process SOCKS traffic. SOCKS policies are the equivalent of access policies that control SOCKS traffic. Similar to access policies, you can make use of Identification Profiles to specify which transactions are governed by each SOCKS policy. Once SOCKS policies are applied to transactions, routing policies can then govern routing of the traffic.

Note the following regarding the SOCKS proxy:

- The SOCKS protocol only supports direct forward connections.
- The SOCKS proxy does not support (will not forward to) upstream proxies.
- The SOCKS proxy does not support scanning services, which are used by Application Visibility and Control (AVC), Application Discovery and Control (ADC), Data Loss Prevention (DLP), and malware detection.
- The SOCKS proxy does not support policy tracing.
- The SOCKS proxy does not decrypt SSL traffic; it tunnels from client to server.

Enabling Processing of SOCKS Traffic

Before you begin

Enable the Web Proxy.

Step 1 Choose **Security Services** > **SOCKS Proxy**.

Step 2 Click **Edit Settings**.

Step 3 Select **Enable SOCKS Proxy**.

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

Configuring the SOCKS Proxy

Step 1 Choose **Security Services** > **SOCKS Proxy**.

Step 2 Click **Edit Settings**.

Step 3 Select **Enable SOCKS Proxy**.

Step 4 Configure the basic and advanced SOCKS Proxy settings.

SOCKS Proxy	Enabled.
SOCKS Control Ports	Ports that accept SOCKS requests. Default is 1080.
UDP Request Ports	UDP ports on which the SOCKS server should listen. Default is 16000-16100.
Proxy Negotiation Timeout	Time to wait (in seconds) to send or receive data from a SOCKS client in the negotiation phase. Default is 60.
UDP Tunnel Timeout	Time to wait (in seconds) for data from a UDP client or server before closing the UDP tunnel. Default is 60.

Creating SOCKS Policies

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

Step 2 Click **Add Policy**.

Step 3 Assign a name in the **Policy Name** field.

Note Each policy group name must be unique and only contain alphanumeric characters or the space character.

Step 4 (Optional) Add a description.

Step 5 In the **Insert Above Policy** field, choose where in the SOCKS policies table to insert this SOCKS policy.

Note When configuring multiple SOCKS policies, determine a logical order for each policy. Order your policies to ensure that correct matching occurs.

Step 6 In the **Identities and Users** section, choose one or more Identities to apply to this policy group.

Step 7 (Optional) Expand the Advanced section to define additional membership requirements.

Proxy Ports	The port configured in the browser. (Optional) Define policy group membership by the proxy port used to access the Web Proxy. Enter one or more port numbers in the Proxy Ports field. Separate multiple ports with commas. You might want to define policy group membership on the proxy port if you have one set of clients configured to explicitly forward requests on one port, and another set of clients configured to explicitly forward requests on a different port. **Note** If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the SOCKS policy group level.
Subnets	(Optional) Define policy group membership by subnet or other addresses. You can choose to use the **addresses** that may be **defined** with the associated **Identity**, or you can enter **specific addresses** here. **Note** If the Identity associated with this policy group defines its membership by addresses, then in this policy group you must enter addresses that are a subset of the Identity's addresses. Adding addresses in the policy group further narrows down the list of transactions that match this policy group.
Time Range	(Optional) Define policy group membership by time range: **a.** Select a time range from the **Time Range** field. **b.** Specify whether this policy group should apply to the times inside or outside the selected time range.

Step 8 Submit and Commit Changes.

What to do next

- (Optional) Add an Identity for use with SOCKS Policies.
- Add one or more SOCKS Policies to manage SOCKS traffic.

Cisco Umbrella Seamless ID

The Cisco Umbrella Seamless ID feature enables the appliance to pass the user identification information to the Cisco Umbrella Secure Web Gateway (SWG) after successful authentication. The Cisco Umbrella SWG checks the user information in the Active Directory based on the authenticated identification information received from the Secure Web Appliance. The Cisco Umbrella SWG considers the user as authenticated and provides access to the user based on the defined security policies.

The Secure Web Appliance passes the user identification information to the Cisco Umbrella SWG using the HTTP headers; X-USWG-PKH, X-USWG-SK, and X-USWG-Data.

Note

- The Cisco Umbrella Seamless ID headers overwrite the headers with the same names on the Secure Web Appliance, if any.
- The Cisco Umbrella Seamless ID feature supports authentication scheme with Active Directory only. This feature does not support LDAP, Cisco Identity Services Engine (ISE), and Cisco Context Directory Agent (CDA).
- The Cisco Umbrella SWG does not support FTP and SOCKS traffic.

Table 1: HTTPs Traffic Behavior

Deployment Mode	Surrogate	Decrypt for Authentication	Secure Web Appliance Authentication	Cisco Umbrella Seamless ID Sharing
Explicit	IP surrogate	Yes/No	Yes	Yes
Transparent	IP surrogate	Yes	Yes	Yes
Transparent	IP surrogate	No	Skips authentication	No
Explicit	Cookie, without credential encryption	Yes/No	Yes	Yes
Explicit	Cookie, with credential encryption	Yes/No	Yes	No
Transparent	Cookie with/without credential encryption	Yes/No	Skips authentication	No

Note The Secure Web Appliance retrieves the UPN value for the authenticated user from the active directory and allows the Cisco Umbrella Seamless ID to apply the correct web policies for the users. For this functionality to work, you must assign all the active directory users with default or customized UPN values.

This section contains the following topics:

- Configuring Cisco Umbrella Seamless ID
- Configuring Routing Destination for Cisco Umbrella SWG

Configuring Cisco Umbrella Seamless ID

Before you begin

- Upload the root or custom Umbrella certificate to the appliance manually through **Network** > **Certificate Management** > **Manage Trusted Root Certificates**. See Certificate Management.
- Ensure you have configured identification profiles for authentication.
- Define routing policies with configured identification profiles.

Step 1 Choose **Web Security Manager** > **Cisco Umbrella Seamless ID** .

Step 2 Click **Edit Settings**.

Step 3 Enter the Cisco Umbrella SWG hostname or IP address.

Step 4 Enter the port numbers of the SWG for HTTP and HTTPS traffic.

You can enter a maximum of six port numbers.

Step 5 (Optional) Click **Connectivity Test** to ensure the successful connectivity of the Cisco Umbrella SWG over ports and validation of certificates.

Step 6 Enter the unique customer organization ID of Cisco Umbrella SWG.

Step 7 Submit and commit.

Configuring Routing Destination for Cisco Umbrella SWG

To create a new routing policy, see Adding Routing Destination and IP Spoofing Profile to Routing Policy

.

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 Cisco Umbrella Seamless ID with the required port.

Step 3 Select the appropriate Cisco Umbrella Seamless ID with port as the Upstream Proxy Group for the policy. The Upstream Proxy Group drop-down list displays all the Cisco Umbrella Seamless ID with ports that you have configured through the **Cisco Umbrella Seamless ID** page (**Web Security Manager** > **Cisco Umbrella Seamless ID**).

Note If you remove a **Cisco Umbrella Seamless ID** with port number (**Web Security Manager** > **Cisco Umbrella Seamless ID**) which is already linked to a routing policy, then the routing destination is automatically changed to 'Direct Connection'.

Step 4 Submit and commit your changes.

Troubleshooting Intercepting Requests

- URL Categories Do Not Block Some FTP Sites

- Large FTP Transfers Disconnect
- Zero Byte File Appears On FTP Servers After File Upload
- Unable to Route FTP Requests Via an Upstream Proxy
- 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