Prevent Loss of Sensitive Data

This chapter contains the following sections:

Overview of Prevent Loss of Sensitive Data

The Web Security appliance secures your data by providing the following capabilities:

Option	Description
Cisco Data Security filters	The Cisco Data Security filters on the Web Security appliance evaluate data leaving the network over HTTP, HTTPS and FTP.
Third-party data loss prevention (DLP) integration	The Web Security appliance integrates with leading third party content-aware DLP systems that identify and protect sensitive data. The Web Proxy uses the Internet Content Adaptation Protocol (ICAP) which allows proxy servers to offload content scanning to external systems

When the Web Proxy receives an upload request, it compares the request to the Data Security and External DLP Policy groups to determine which policy group to apply. If both types of policies are configured, it compares the request to Cisco Data Security policies before external DLP policies. After it assigns the request to a policy group, it compares the request to the policy group's configured control settings to determine what to do with the request. How you configure the appliance to handle upload requests depends on the policy group type.

Note Upload requests that try to upload files with a size of zero (0) bytes are not evaluated against Cisco Data Security or External DLP policies.

To restrict and control data that is leaving the network, you can perform the following tasks:

Task	Link to Task
Create Cisco Data Security policies	Managing Upload Requests, on page 3
Create External DLP policies	Managing Upload Requests on an External DLP System, on page 3
Create Data Security and External DLP policies	Creating Data Security and External DLP Policies, on page 5
Control Upload Requests using Cisco Data Security policies	Managing Settings for Upload Requests, on page 7
Control Upload Requests Using External DLP policies	Controlling Upload Requests Using External DLP Policies, on page 11

Bypassing Upload Requests Below a Minimum Size

To help reduce the number of upload requests recorded in the log files, you can define a minimum request body size, below which upload requests are not scanned by the Cisco Data Security Filters or the external DLP server.

To do this, use the following CLI commands:

- `datasecurityconfig`. Applies to the Cisco Data Security filters.
- `externaldlpconfig`. Applies to the configured external DLP servers.

The default minimum request body size is 4 KB (4096 bytes) for both CLI commands. Valid values are 1 to 64 KB. The size you specify applies to the entire size of the upload request body.

Note All chunk encoded uploads and all native FTP transactions are scanned by the Cisco Data Security filters or external DLP servers when enabled. However, they can still be bypassed based on a custom URL category.

User Experience When Requests Are Blocked As Sensitive Data

When the Cisco Data Security filters or an external DLP server blocks an upload request, it provides a block page that the Web Proxy sends to the end user. Not all websites display the block page to the end user. For example, some Web 2.0 websites display dynamic content using javascript instead of a static Web page and are not likely to display the block page. Users are still properly blocked from performing data security violations, but they may not always be informed of this by the website.

Managing Upload Requests

Before you begin

Go to **Security Services > Data Security Filters** to enable the Cisco Data Security filters.

Create and configure Data Security Policy groups.

Cisco Data Security policies use URL filtering, Web reputation, and upload content information when evaluating the upload request. You configure each of these security components to determine whether or not to block the upload request.

When the Web Proxy compares an upload request to the control settings, it evaluates the settings in order. Each control setting can be configured to perform one of the following actions for Cisco Data Security policies:

Action	Description
Block	The Web Proxy does not permit the connection and instead displays an end user notification page explaining the reason for the block.
Allow	The Web Proxy bypasses the rest of the Data Security Policy security service scanning and then evaluates the request against the Access Policies before taking a final action. For Cisco Data Security policies, Allow bypasses the rest of data security scanning, but does not bypass External DLP or Access Policy scanning. The final action the Web Proxy takes on the request is determined by the applicable Access Policy (or an applicable external DLP Policy that may block the request).
Monitor	The Web Proxy continues comparing the transaction to the other Data Security Policy group control settings to determine whether to block the transaction or evaluate it against the Access Policies.

For Cisco Data Security policies, only the Block action is a final action that the Web Proxy takes on a client request. The Monitor and Allow actions are intermediary actions. In both cases, the Web Proxy evaluates the transaction against the External DLP Policies (if configured) and Access Policies. The Web Proxy determines which final action to apply based on the Access Policy group control settings (or an applicable external DLP Policy that may block the request).

What to do next

Related Topics

- Managing Upload Requests on an External DLP System, on page 3
- Managing Settings for Upload Requests, on page 7

Managing Upload Requests on an External DLP System

To configure the Web Security appliance to handle upload requests on an external DLP system, perform the following tasks:

Step 1 Choose **Network > External DLP Servers.** Define an external DLP system. To pass an upload request to an external DLP system for scanning, you must define at least one ICAP-compliant DLP system on the Web Security appliance.

Step 2 **Create and configure External DLP Policy groups.** After an external DLP system is defined, you create and configure External DLP Policy groups to determine which upload requests to send to the DLP system for scanning.

Step 3 When an upload request matches an External DLP Policy, the Web Proxy sends the upload request to the DLP system using the Internet Content Adaptation Protocol (ICAP) for scanning. The DLP system scans the request body content and returns a block or allow verdict to the Web Proxy. The allow verdict is similar to the Allow action for Cisco Data Security policies in that the upload request will be compared to the Access Policies. The final action the Web Proxy takes on the request is determined by the applicable Access Policy.

What to do next

Related Topics

- Controlling Upload Requests Using External DLP Policies, on page 11
- Defining External DLP Systems, on page 8

Evaluating Data Security and External DLP Policy Group Membership

Each client request is assigned to an Identity and then is evaluated against the other policy types to determine which policy group it belongs for each type. The Web Proxy evaluates *upload requests* against the Data Security and External DLP policies. The Web Proxy applies the configured policy control settings to a client request based on the client request's policy group membership.

Matching Client Requests to Data Security and External DLP Policy Groups

To determine the policy group that a client request matches, the Web Proxy follows a specific process for matching the group membership criteria. It considers the following factors for group membership:

- **Identity.** Each client request either matches an Identification Profile, fails authentication and is granted guest access, or fails authentication and gets terminated.
- **Authorized users.** If the assigned Identification Profile requires authentication, the user must be in the list of authorized users in the Data Security or External DLP Policy group to match the policy group. The list of authorized users can be any of the specified groups or users or can be guest users if the Identification Profile allows guest access.
- **Advanced options.** You can configure several advanced options for Data Security and External DLP Policy group membership. Some options (such as proxy port and URL category) can also be defined within the Identity. When an advanced option is configured in the Identity, it is not configurable in the Data Security or External DLP Policy group level.

The information in this section gives an overview of how the Web Proxy matches upload requests to both Data Security and External DLP Policy groups.

The Web Proxy sequentially reads through each policy group in the policies table. It compares the upload request status to the membership criteria of the first policy group. If they match, the Web Proxy applies the policy settings of that policy group.

If they do not match, the Web Proxy compares the upload request to the next policy group. It continues this process until it matches the upload request to a user defined policy group. If it does not match a user defined policy group, it matches the global policy group. When the Web Proxy matches the upload request to a policy group or the global policy group, it applies the policy settings of that policy group.

Creating Data Security and External DLP Policies

You can create Data Security and External DLP Policy groups based on combinations of several criteria, such as one or more Identification Profiles or the URL category of the destination site. You must define at least one criterion for policy group membership. When you define multiple criteria, the upload request must meet all criteria to match the policy group. However, the upload request needs to match only one of the configured Identification Profiles.

Step 1 Choose **Web Security Manager > Cisco Data Security** (for Defining Data Security Policy group membership) or **Web Security Manager > External Data Loss Prevention** (for Defining External DLP Policy group membership).

Step 2 Click **Add Policy**.

Step 3 In the **Policy Name** field, enter a name for the policy group, and in the Description field (optional) add a description.

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

Step 4 In the **Insert Above Policy** field, choose where in the policies table to place the policy group.

When configuring multiple policy groups you must specify a logical order for each group. Order your policy groups to ensure that correct matching occurs.

Step 5 In the **Identities and Users** section, choose one or more Identification Profile groups to apply to this policy group.

Step 6 (Optional) Expand the **Advanced** section to define additional membership requirements.

Step 7 To define policy group membership by any of the advanced options, click the link for the advanced option and configure the option on the page that appears.

Advanced Option	Description
Protocols	Choose whether or not to define policy group membership by the protocol used in the client request. Select the protocols to include. "All others" means any protocol not listed above this option. **Note** When the HTTPS Proxy is enabled, only Decryption Policies apply to HTTPS transactions. You cannot define policy membership by the HTTPS protocol for Access, Routing, Outbound Malware Scanning, Data Security, or External DLP Policies.

Advanced Option	Description
Proxy Ports	Choose whether or not to 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. For explicit forward connections, this is the port configured in the browser. For transparent connections, this is the same as the destination port. 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. Cisco recommends only defining policy group membership by the proxy port when the appliance is deployed in explicit forward mode, or when clients explicitly forward requests to the appliance. If you define policy group membership by the proxy port when client requests are transparently redirected to the appliance, some requests might be denied. **Note** If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.
Subnets	Choose whether or not to define policy group membership by subnet or other addresses. You can choose to use the addresses that may be defined with the associated Identification Profile, or you can enter specific addresses here. **Note** If the Identification Profile 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 addresses defined in the Identification Profile. Adding addresses in the policy group further narrows down the list of transactions that match this policy group.
URL Categories	Choose whether or not to define policy group membership by URL categories. Select the user defined or predefined URL categories. **Note** If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.
User Agents	Choose whether to define policy group membership by the user agents (client applications such as updaters and Web browsers) used in the client request. You can select some commonly defined user agents, or define your own using regular expressions. Specify whether membership definition includes only the selected user agents, or specifically excludes the selected user agents. **Note** If the Identification Profile associated with this policy group defines Identification Profile membership by this advanced setting, the setting is not configurable at the non-Identification Profile policy group level.
User Location	Choose whether or not to define policy group membership by user location, either remote or local. This option only appears when the Secure Mobility is enabled.

Step 8 Submit your changes.

Step 9 If you are creating a Data Security Policy group, configure its control settings to define how the Web Proxy handles upload requests.

The new Data Security Policy group automatically inherits global policy group settings until you configure options for each control setting.

If you are creating an External DLP Policy group, configure its control settings to define how the Web Proxy handles upload requests.

The new External DLP Policy group automatically inherits global policy group settings until you configure custom settings.

Step 10 Submit and Commit Changes.

What to do next

Related Topics

- Evaluating Data Security and External DLP Policy Group Membership, on page 4
- Matching Client Requests to Data Security and External DLP Policy Groups, on page 4
- Managing Settings for Upload Requests, on page 7
- Controlling Upload Requests Using External DLP Policies, on page 11

Managing Settings for Upload Requests

Each upload request is assigned to a Data Security Policy group and inherits the control settings of that policy group. The control settings of the Data Security Policy group determine whether the appliance blocks the connection or evaluates it against the Access Polices.

Configure control settings for Data Security Policy groups on the Web Security Manager > Cisco Data Security page.

You can configure the following settings to determine what action to take on upload requests:

Option	Link
URL Categories	URL Categories, on page 7
Web Reputation	Web Reputation, on page 8
Content	Content Blocking, on page 8

After a Data Security Policy group is assigned to an upload request, the control settings for the policy group are evaluated to determine whether to block the request or evaluate it against the Access Policies.

URL Categories

AsyncOS for Web allows you to configure how the appliance handles a transaction based on the URL category of a particular request. Using a predefined category list, you can choose to monitor or block content by category. You can also create custom URL categories and choose to allow, monitor, or block traffic for a website in the custom category.

Web Reputation

The Web Reputation setting inherits the global setting. To customize web reputation filtering for a particular policy group, you can use the Web Reputation Settings pull-down menu to customize web reputation score thresholds.

Only negative and zero values can be configured for web reputation threshold settings for Cisco Data Security policies. By definition, all positive scores are monitored.

Content Blocking

You can use the settings on the Cisco Data Security > Content page to configure the Web Proxy to block data uploads based on the following file characteristics:

- **File size.** You can specify the maximum *upload* size allowed. All uploads with sizes equal to or greater than the specified maximum are blocked. You can specify different maximum file sizes for HTTP/HTTPS and native FTP requests.

  When the upload request size is greater than both the maximum upload size and the maximum scan size (configured in the "DVS Engine Object Scanning Limits" field on Security Services > Anti-Malware page), the upload request is still blocked, but the entry in the data security logs does not record the file name and content type. The entry in the access logs is unchanged.

- **File type.** You can block predefined file types or custom MIME types you enter. When you block a predefined file type, you can block all files of that type or files greater than a specified size. When you block a file type by size, the maximum file size you can specify is the same as the value for the "DVS Engine Object Scanning Limits" field on Security Services > Anti-Malware page. By default, that value is 32 MB.

  Cisco Data Security filters do not inspect the contents of archived files when blocking by file type. Archived files can be blocked by its file type or file name, not according to its contents.

  

  Note For some groups of MIME types, blocking one type blocks all MIME types in the group. For example, blocking application/x-java-applet blocks all java MIME types, such as application/java and application/javascript.

- **File name.** You can block files with specified names. You can use text as a literal string or a regular expression for specifying file names to block.

  

  Note Only enter file names with 8-bit ASCII characters. The Web Proxy only matches file names with 8-bit ASCII characters.

Defining External DLP Systems

The Web Security appliance can integrate with multiple external DLP servers from the same vendor by defining multiple DLP servers in the appliance. You can define the load-balancing technique the Web Proxy uses when

contacting the DLP systems. This is useful when you define multiple DLP systems. See SSL Configurationfor information about specifying the protocols used to secure communications with external DLP servers.

Note Verify the external DLP server does not send the Web Proxy modified content. AsyncOS for Web only supports the ability to block or allow upload requests. It does not support uploading content modified by an external DLP server.

Configuring External DLP Servers

Step 1 Choose **Network > External DLP Servers**.

Step 2 Click **Edit Settings**.

Setting	Description
Protocol for External DLP Servers	Choose either: • **ICAP** – DLP client/server ICAP communications are not encrypted. • **Secure ICAP** – DLP client/server ICAP communications are via an encrypted tunnel. Additional related options appear.

External DLP Servers	Enter the following information to access an ICAP compliant DLP system:
	• **Server address** and **Port** – The hostname or IP address and TCP port for accessing the DLP system.
	• **Reconnection attempts** – The number of times the Web Proxy tries to connect to the DLP system before failing.
	• **Service URL** – The ICAP query URL specific to the particular DLP server. The Web Proxy includes what you enter here in the ICAP request it sends to the external DLP server. The URL must start with the ICAP protocol: icap://
	• Certificate (optional) – The certificate provided to secure each External DLP Server connection can be Certificate Authority (CA)-signed or self-signed. Obtain the certificate from the specified server, and then upload it to the appliance:
	  • Browse to and select the certificate file, and then click **Upload File**.
	  Note This single file must contain both the client certificate and private key in unencrypted form.
	  • **Use this certificate for all DLP servers using Secure ICAP** – Check this box to use the same certificate for all External DLP Servers you define here. Leave the option unchecked to enter a different certificate for each server.
	• Start Test – You can test the connection between the Web Security appliance and the defined external DLP server(s) by clicking **Start Test**.

Setting	Description
Load Balancing	If multiple DLP servers are defined, select which load-balancing technique the Web Proxy uses to distribute upload requests to different DLP servers. You can choose the following load balancing techniques: • **None (failover).** The Web Proxy directs upload requests to one DLP server. It tries to connect to the DLP servers in the order they are listed. If one DLP server cannot be reached, the Web Proxy attempts to connect to the next one in the list. • **Fewest connections.** The Web Proxy keeps track of how many active requests are with the different DLP servers and it directs the upload request to the DLP server currently servicing the fewest number of connections. • **Hash based.** The Web Proxy uses a hash function to distribute requests to the DLP servers. The hash function uses the proxy ID and URL as inputs so that requests for the same URL are always directed to the same DLP server. • **Round robin.** The Web Proxy cycles upload requests equally among all DLP servers in the listed order.
Service Request Timeout	Enter how long the Web Proxy waits for a response from the DLP server. When this time is exceeded, the ICAP request has failed and the upload request is either blocked or allowed, depending on the Failure Handling setting. Default is 60 seconds.
Maximum Simultaneous Connections	Specifies the maximum number of simultaneous ICAP request connections from the Web Security appliance to each configured external DLP server. The Failure Handling setting on this page applies to any request which exceeds this limit. Default is 25.
Failure Handling	Choose whether upload requests are blocked or allowed (passed to Access Policies for evaluation) when the DLP server fails to provide a timely response. Default is allow (“Permit all data transfers to proceed without scanning”).
Trusted Root Certificate	Browse to and select the trusted-root certificate for the certificate(s) provided with the External DLP Servers, and then click Upload File. See Certificate Managementfor additional information.
Invalid Certificate Options	Specify how various invalid certificates are handled: **Drop** or **Monitor**.
Server Certificates	This section displays all DLP server certificates currently available on the appliance.

Step 3 (Optional) You can add another DLP server by clicking **Add Row** and entering the DLP Server information in the new fields provided.

Step 4 Submit and Commit Changes.

Controlling Upload Requests Using External DLP Policies

Once the Web Proxy receives the upload request headers, it has the information necessary to decide if the request should go to the external DLP system for scanning. The DLP system scans the request and returns a verdict to the Web Proxy, either block or monitor (evaluate the request against the Access Policies).

Step 1 Choose **Web Security Manager > External Data Loss Prevention**.

Step 2 Click the link under the Destinations column for the policy group you want to configure.

Step 3 Under the **Edit Destination Settings** section, choose "**Define Destinations Scanning Custom Settings**."

Step 4 In the **Destination to scan** section, choose one of the following options:

- **Do not scan any uploads.** No upload requests are sent to the configured DLP system(s) for scanning. All upload requests are evaluated against the Access Policies.
- **Scan all uploads.** All upload requests are sent to the configured DLP system(s) for scanning. The upload request is blocked or evaluated against the Access Policies depending on the DLP system scanning verdict.
- **Scan uploads except to specified custom and external URL categories.** Upload requests that fall in specific custom URL categories are sent to the configured DLP system for scanning. The upload request is blocked or evaluated against the Access Policies depending on the DLP system scanning verdict. Click **Edit custom categories list** to select the URL categories to scan.

Step 5 Submit and Commit Changes.

Logging of Data Loss Prevention Scanning

The access logs indicate whether or not an upload request was scanned by either the Cisco Data Security filters or an external DLP server. The access log entries include a field for the Cisco Data Security scan verdict and another field for the External DLP scan verdict based.

In addition to the access logs, the Web Security appliance provides the following log file types to troubleshoot Cisco Data Security and External DLP Policies:

- **Data Security Logs.** Records client history for upload requests that are evaluated by the Cisco Data Security filters.
- **Data Security Module Logs.** Records messages related to the Cisco Data Security filters.
- **Default Proxy Logs.** In addition recording errors related to the Web Proxy, the default proxy logs include messages related to connecting to external DLP servers. This allows you to troubleshoot connectivity or integration problems with external DLP servers.

The following text illustrates a sample Data Security Log entry:

```
Mon Mar 30 03:02:13 2009 Info: 303 10.1.1.1 - -
<<bar,text/plain,5120><foo,text/plain,5120>>
BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting ns server.com nc
```

Field Value	Description
`Mon Mar 30 03:02:13 2009 Info:`	Timestamp and trace level

Field Value	Description
`303`	Transaction ID
`10.1.1.1`	Source IP address
`-`	User name
`-`	Authorized group names
`<<bar,text/plain,5120><foo,text/plain,5120>>`	File name, file type, file size for each file uploaded at once **Note** This field does not include text/plain files that are less than the configured minimum request body size, the default of which is 4096 bytes.
`BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting`	Cisco Data Security policy and action
`ns`	Web reputation score
`server.com`	Outgoing URL
`nc`	URL category

Note To learn when data transfer, such as a POST request, to a site was blocked by the external DLP server, search for the IP address or hostname of the DLP server in the access logs.