Scan Outbound Traffic for Existing Infections

This topic contains the following sections:

Overview of Scanning Outbound Traffic

To prevent malicious data from leaving the network, the Web Security Appliance provides the Outbound Malware Scanning feature. Using policy groups, you can define which uploads are scanned for malware, which anti-malware scanning engines to use for scanning, and which malware types to block.

The Cisco Dynamic Vectoring and Streaming (DVS) engine scans transaction requests as they leave the network. By working with the Cisco DVS engine, the Web Security Appliance enables you to prevent users from unintentionally uploading malicious data.

You can perform the following tasks:

Task	Link to Task
Create policies to block malware	Creating Outbound Malware Scanning Policies, on page 3
Assign upload requests to outbound malware policy groups	Controlling Upload Requests , on page 4

User Experience When Requests Are Blocked by the DVS Engine

When the Cisco DVS engine blocks an upload request, the Web Proxy sends a block page to the end user. However, not all Websites display the block page to the end user. Some Web 2.0 Websites display dynamic content using Javascript instead of a static Webpage and are not likely to display the block page. Users are still properly blocked from uploading malicious data, but they may not always be informed of this by the Website.

Understanding Upload Requests

Outbound Malware Scanning Policies define whether or not the Web Proxy blocks HTTP requests and decrypted HTTPS connections for transactions that upload data to a server (upload requests). An upload request is an HTTP or decrypted HTTPS request that has content in the request body.

When the Web Proxy receives an upload request, it compares the request to the Outbound Malware Scanning policy groups to determine which policy group to apply. After it assigns the request to a policy group, it compares the request to the policy group's configured control settings to determine whether to block the request or monitor the request. When an Outbound Malware Scanning Policy determines to monitor a request, it is evaluated against the Access Policies, and the final action the Web Proxy takes on the request is determined by the applicable Access Policy.

Note Upload requests that try to upload files with a size of zero (0) bytes are not evaluated against Outbound Malware Scanning Policies.

Criteria for Group Membership

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

The Web Proxy follows a specific process for matching the group membership criteria. It considers the following factors for group membership:

Criteria	Description
Identification Profile	Each client request either matches an **Identification Profile**, fails authentication and is granted guest access, or fails authentication and is terminated.
Authorized users	If the assigned **Identification Profile** requires authentication, the user must be in the list of authorized users in the Outbound Malware Scanning 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 Outbound Malware Scanning Policy group membership. Some options, such as proxy port and URL category, can also be defined within the **Identification Profile**. When an advanced option is configured in the **Identification Profile**, it is not configurable in the Outbound Malware Scanning Policy group level.

Matching Client Requests to Outbound Malware Scanning Policy Groups

The Web Proxy 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 Outbound Malware Scanning Policies

You can create Outbound Malware Scanning Policy groups based on combinations of several criteria, such as one or more Identities 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 Identities.

Step 1 Choose **Web Security Manager > Outbound Malware Scanning**.

Step 2 Click **Add Policy**.

Step 3 Enter a name and an optional description for the policy group.

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, select where in the policies table to place the policy group.

When configuring multiple policy groups, you must specify a logical order for each group.

Step 5 In the **Identification Profiles** and Users section, select one or more Identity 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.
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. 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.

Advanced Option	Description
Subnets	Choose whether or not to define policy group membership by subnet or other addresses. You can select 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 addresses defined in the Identity. 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.

Step 8 Submit your changes.

Step 9 Configure Outbound Malware Scanning Policy group control settings to define how the Web Proxy handles transactions.

The new Outbound Malware Scanning Policy group automatically inherits global policy group settings until you configure options for each control setting.

Step 10 Submit and Commit Changes.

Controlling Upload Requests

Each upload request is assigned to an Outbound Malware Scanning Policy group and inherits the control settings of that policy group. After the Web Proxy receives the upload request headers, it has the information necessary to decide if it should scan the request body. The DVS engine scans the request and returns a verdict to the Web Proxy. The block page appears to the end user, if applicable.

Step 1 Choose **Web Security Manager > Outbound Malware Scanning**.

Step 2 In the **Destinations** column, click the link for the policy group you want to configure.

Step 3 In the **Edit Destination Settings** section, select **Define Destinations Scanning Custom Settings** from the drop-down menu.

Step 4 In the **Destinations to Scan** section, select one of the following:

Option	Description
Do not scan any uploads	The DVS engine scans no upload requests. All upload requests are evaluated against the Access Policies
Scan all uploads	The DVS engine scans all upload requests. The upload request is blocked or evaluated against the Access Policies, depending on the DVS engine scanning verdict
Scan uploads to specified custom URL categories	The DVS engine scans upload requests that belong in specific custom URL categories. The upload request is blocked or evaluated against the Access Policies, depending on the DVS engine scanning verdict. Click **Edit custom categories list** to select the URL categories to scan

Step 5 Submit your changes.

Step 6 In the **Anti-Malware Filtering** column, click the link for the policy group.

Step 7 In the **Anti-Malware Settings** section, select **Define Anti-Malware Custom Settings**.

Step 8 In the **Cisco DVS Anti-Malware Settings** section, select which anti-malware scanning engines to enable for this policy group.

Step 9 In the **Malware Categories** section, select whether to monitor or block the various malware categories.

The categories listed in this section depend on which scanning engines you enable.

Note URL transactions are categorized as unscannable when the configured maximum time setting is reached or when the system experiences a transient error condition. For example, transactions might be categorized as unscannable during scanning engine updates or AsyncOS upgrades. The malware scanning verdicts SV_TIMEOUT and SV_ERROR are considered unscannable transactions.

Step 10 Submit and Commit Changes.

Logging of DVS Scanning

The access logs indicate whether or not the DVS engine scanned an upload request for malware. The scanning verdict information section of each access log entry includes values for the DVS engine activity for scanned uploads. You can also add one of the fields to the W3C or access logs to more easily find this DVS engine activity:

Table 1: Log Fields in W3C Logs and Format Specifiers in Access Logs

W3C Log Field	Format Specifier in Access Logs
x-req-dvs-scanverdict	%X2
x-req-dvs-threat-name	%X4
x-req-dvs-verdictname	%X3

When the DVS engine marks an upload request as being malware and it is configured to block malware uploads, the ACL decision tag in the access logs is BLOCK_AMW_REQ.

However, when the DVS engine marks an upload request as being malware and it is configured to *monitor* malware uploads, the ACL decision tag in the access logs is actually determined by the Access Policy applied to the transaction.

To determine whether or not the DVS engine scanned an upload request for malware, view the results of the DVS engine activity in the scanning verdict information section of each access log entry.