URL Filtering Configuration and Best Practices for Cisco Email Security

Contents

Introduction
Background Information
Enable URL Filtering
Enable URL Filtering Support for Shortened URLs
Create URL Filtering Actions
Content Filters for Malicious URLs
Content Filters for Neutral or Suspect URLs
Content Filters for Clean URLs
Content Filters for URLs with "No Score"
Report Uncategorized and Misclassified URLs
Malicious URLs and Marketing Messages Are Not Caught by Anti-Spam or Outbreak Filters
Related Information

Introduction

This document describes how to configure URL Filtering on the Cisco Email Security Appliance (ESA) and best practices for its use.

Background Information

Control and protection against malicious or undesirable links is incorporated into the anti-spam, outbreak, content, and message filtering processes in the work queue. These controls:

- Increase the effectiveness of protection from malicious URLs in messages and attachments.
- URL filtering is incorporated into Outbreak Filtering. This strengthened protection is useful even if your organization already has a Cisco Web Security Appliance or similar protection from web-based threats, because it blocks threats at the point of entry.
- You can also use content or message filters to take action based on the Web Based Reputation Score (WBRS) of URLs in messages. For example, you can rewrite URLs with neutral or unknown reputation to redirect them to the Cisco Web Security Proxy for click-time evaluation of their safety.
- Better identify spam
- The appliance uses the reputation and category of links in messages, in conjunction with other spam-identification algorithms, to help identify spam. For example, if a link in a message belongs to a marketing web site, the message is more likely to be a marketing message.
- Support enforcement of corporate acceptable use policies
- The category of URLs (for example, Adult Content or Illegal Activities) can be used in conjunction with content and message filters to enforce corporate acceptable use policies.
- Allow you to identify users in your organization who most frequently clicked a URL in a
message that has been rewritten for protection, as well as links that have most frequently
been clicked.

When you configure URL Filtering on the ESA, you must also configure other features dependent
upon your desired functionality. Here are some typical features that are enabled alongside URL Filtering:

- For enhanced protection against spam, the Anti-Spam Scanning feature must be enabled
globally in accordance with the applicable mail policy. This can be either the Cisco IronPort
Anti-Spam (IPAS) or the Cisco Intelligent Multi-Scan (IMS) feature.
- For enhanced protection against malware, the Outbreak Filters or Virus Outbreak Filters
(VOF) feature must be enabled globally in accordance with the applicable mail policy.
- For actions based on the URL reputation, or in order to enforce acceptable use policies with
the use of message and content filters, you must enable VOF globally.

**Note:** As of AsyncOS 11.1 for Email Security, support for URL scanning in attachments is
now available. You can now configure your appliance to scan for URLs in message
attachments, and perform configured actions on such messages. You can use the URL
Reputation and URL Category content and message filters to scan for URLs in message
attachments. For more details, see the “Using Message Filters to Enforce Email Policies”,
“Content Filters” and “Protecting Against Malicious or Undesirable URLs” chapters in the
user guide or online help.

**Note:** Additionally as of AsyncOS 11.1 for Email Security, support for URL filtering support
for shortened URLs now available. You can now configure your appliance to perform URL
filtering on shortened URLs, and retrieve the actual URL from the shortened URL. Based on
the URL reputation score of the original URL, a configured action is taken on the shortened
URL. To enable URL filtering for shortened URLs in your appliance, see the “Protecting
Against Malicious or Undesirable URLs” chapter in the user guide or online help and the CLI
Reference Guide for AsyncOS for Cisco Email Security Appliance.

**Enable URL Filtering**

In order to implement URL Filtering on the ESA, you must first enable the feature. URL Filtering
may be enable from GUI or CLI by the ESA administrator.

To enable URL Filtering with the use of the GUI, navigate to **Security Services > URL Filtering >
Enable:**

**URL Filtering**

<table>
<thead>
<tr>
<th>URL Filtering Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL Filtering is currently disabled.</td>
</tr>
</tbody>
</table>
From the CLI, run the command, `websecurityconfig`:

```
myesa.local> websecurityconfig
Enable URL Filtering? [N] > y
```

**Note:** URL Logging is a sub-feature from within VOF. This is a CLI-only feature that must be enabled as shown here, using `outbreakconfig`:

```
myesa.local> outbreakconfig
Outbreak Filters: Enabled
Choose the operation you want to perform:
- SETUP - Change Outbreak Filters settings.
- CLUSTERSET - Set how the Outbreak Filters are configured in a cluster.
- CLUSTERSHOW - Display how the Outbreak Filters are configured in a cluster.
[>] > setup
Outbreak Filters: Enabled
Would you like to use Outbreak Filters? [Y]>
Outbreak Filters enabled.
Outbreak Filter alerts are sent when outbreak rules cross the threshold (go above or back down below), meaning that new messages of certain types could be quarantined or will no longer be quarantined, respectively.

```
...
```

Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N] > y

Logging of URLs has been enabled.

The Outbreak Filters feature is now globally enabled on the system. You must use the 'policyconfig' command in the CLI or the Email Security Manager in the GUI to enable Outbreak Filters for the desired Incoming and Outgoing Mail Policies.

**Note:** Ensure that you commit any and all changes to your configuration before you proceed from either the GUI or the CLI on your ESA.

### Enable URL Filtering Support for Shortened URLs

Enabling URL filtering support for shortened URLs is able to be done by CLI only, using `websecurityadvancedconfig`:
Do you want to enable URL filtering for shortened URLs? [N] > Y

For shortened URL support to work, please ensure that ESA is able to connect to following domains:
Cisco recommends to have this enabled for URL filtering configuration best practices. Once enabled, the mail logs will reflect anytime a shortened URL is used with-in the message:

Once URL filtering is enabled as described in this article, from the mail logs example above, we can see the bit.ly link recorded AND the original link that it expands out to also recorded.

Create URL Filtering Actions

When you enable URL filtering alone, it does not take action against messages that might contain live and valid URLs.

The URLs included in inbound and outbound messages are evaluated. Any valid string for a URL is evaluated, to include strings with these components:

- HTTP, HTTPS, or WWW
- Domain or IP addresses
- Port numbers preceded by a colon (:)  
- Uppercase or lowercase letters

When the system evaluates URLs in order to determine whether a message is spam, if necessary for load management, it prioritizes and screens inbound messages over outbound messages.

You can perform actions on messages based on the reputation or category of URLs in the message body and message attachments. If you want to perform any action other than modifying URLs or their behavior, add a URL Reputation or URL Category condition and select the reputation scores or URL categories for which you want to apply the action.

For example, if you want to apply the Drop (Final Action) action to all messages that include URLs in the Adult category, add a condition of type URL Category with the Adult category selected.

If you do not specify a category, the action you choose is applied to all messages.

URL reputation score ranges for clean, neutral, and malicious URLs are predefined and not editable. However, you can specify a custom range instead. The specified endpoints are included
in the range you specify. For example, if you create a custom range from -8 to -10, then -8 and -10 are included in the range. Use “No Score” for URLs for which a reputation score cannot be determined.

In order to quickly scan URLs and take action, you can create a content filter so that if the message has a valid URL, then the action is applied. From the GUI, navigate to Mail Policies > Incoming Content Filters > Add Filter.

**Content Filters for Malicious URLs**

This example shows a scan for malicious URLs with the implementation of this inbound content filter:

With this filter in place, the system scans for a URL with a *Malicious* reputation (-10.00 to -6.00), adds a log entry to the mail logs, uses the *defang* action in order to make the link un-clickable, and places this into a URL Filtering quarantine. Here is an example from the mail logs:

```
Wed Nov 5 21:27:18 2014 Info: MID 186 ICID 606 From: <bad_user@that.domain.net>
Wed Nov 5 21:27:18 2014 Info: MID 186 ICID 606 RID 0 To: <joe.user@goodmailguys.com>
Wed Nov 5 21:27:18 2014 Info: MID 186 Message-ID 'COL128-W95DE5520A96FD9D69FAC2D9D0840@phx.gbl'
Wed Nov 5 21:27:18 2014 Info: MID 186 Subject 'URL Filter test malicious'
Wed Nov 5 21:27:18 2014 Info: MID 186 ready 2230 bytes from <bad_user@that.domain.net>
Wed Nov 5 21:27:18 2014 Info: MID 186 matched all recipients for per-recipient policy DEFAULT in the inbound table
Wed Nov 5 21:27:19 2014 Info: MID 186 antivirus negative
```
This URL for peekquick.com is MALICIOUS and scored at a -6.77. An entry is made in the mail logs, where you can see all of the processes in action. The URL filter detected the malicious URL, defanged, and quarantined it. The VOF also scored it positive based on its rule set, and provided details that this was a related Phish.

If VOF is not enabled, the same message is processed through, but URL scans are not acted upon without the added ability of VOF to drive scans and action. However, in this example the message body is scanned by the Cisco Anti-Spam Engine (CASE) and deemed as spam-positive.

This detection via CASE alone does not always occur. There are times when CASE and IPAS rules might contain that match against a certain sender, domain, or message contents in order to detect this threat alone.

**Content Filters for Neutral or Suspect URLs**
Neutral URL reputation means that URLs are currently clean, but may turn malicious in future, as they are prone to attacks. For such URLs, administrators can create non-blocking policies, for example, redirecting them to the Cisco Web Security Proxy for click-time evaluation.

**Note:** In AsyncOS 9.7 for Email Security and later, URLs that were formerly labeled “Suspicious” are now labeled “Neutral.” Only the labeling has changed; the underlying logic and processing have not changed.

This example shows a scan for neutral/suspect URLs with the implementation of this inbound content filter:

![Content Filter Settings](image)

With this filter in place, the system searches for a URL with a Neutral, or Suspect, reputation (-5.90 to -3.1) and adds a log entry to the mail logs. This example shows a modified subject in order to prepend "[SUSPECT URL]". Here is an example from the mail logs:

```plaintext
Wed Nov 5 21:22:23 2014 Info: MID 185 ICID 605 From: <bad_user@that.domain.net>
Wed Nov 5 21:22:23 2014 Info: MID 185 ICID 605 RID 0 To: <joe.user@goodmailguys.com>
Wed Nov 5 21:22:23 2014 Info: MID 185 Message-ID 'D0804586.24BAE%bad_user@that.domain.net'
Wed Nov 5 21:22:23 2014 Info: MID 185 Subject 'Middle of the road?'
Wed Nov 5 21:22:23 2014 Info: MID 185 ready 4598 bytes from <bad_user@that.domain.net>
Wed Nov 5 21:22:23 2014 Info: MID 185 matched all recipients for per-recipient policy DEFAULT in the inbound table
Wed Nov 5 21:22:24 2014 Info: MID 185 antivirus negative
drid.com&utm_medium=email has reputation -5.08 matched url-reputation-rule
Wed Nov 5 21:22:24 2014 Info: Delivery start DCID 26 MID 185 to RID [0]
**Note:** The URL that is embedded in the previous example has extra spaces included in the URL body, so it does not trip any web scans or proxy detection.

The Udemy link in the previous example does not appear clean, and it is scored **SUSPECT** at -5.08. As shown in the mail logs entry, this message is allowed to be delivered to the end user.

**Content Filters for Clean URLs**

This example shows a scan for clean URLs with the implementation of this inbound content filter:

![Content Filter Settings](image)

With this filter in place, the system searches for a URL with a *clean* reputation (6.00 to 10.00) and simply adds a log entry to the mail logs in order to trigger and record the Web Based Reputation Score (WBRS). This log entry also helps to identify the process that is triggered. Here is an example from the mail logs:

**Content Filters for Clean URLs**

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wed Nov 5</td>
<td>21:11:10</td>
<td>Info: Start MID 182 ICID 602</td>
</tr>
<tr>
<td>Wed Nov 5</td>
<td>21:11:10</td>
<td>Info: MID 182 ICID 602 From: <a href="mailto:bad_user@that.domain.net">bad_user@that.domain.net</a></td>
</tr>
<tr>
<td>Wed Nov 5</td>
<td>21:11:10</td>
<td>Info: MID 182 ICID 602 To: <a href="mailto:joe.user@goodmailguys.com">joe.user@goodmailguys.com</a></td>
</tr>
<tr>
<td>Wed Nov 5</td>
<td>21:11:10</td>
<td>Info: MID 182 Message-ID '<a href="mailto:D08042EA.24BA46bad_user@that.domain.net">D08042EA.24BA46bad_user@that.domain.net</a>'</td>
</tr>
<tr>
<td>Wed Nov 5</td>
<td>21:11:10</td>
<td>Info: MID 182 Subject 'Starting at the start!'</td>
</tr>
<tr>
<td>Wed Nov 5</td>
<td>21:11:10</td>
<td>Info: MID 182 ready 2798 bytes from <a href="mailto:bad_user@that.domain.net">bad_user@that.domain.net</a></td>
</tr>
<tr>
<td>Wed Nov 5</td>
<td>21:11:10</td>
<td>Info: MID 182 matched all recipients for per-recipient policy DEFAULT in the inbound table</td>
</tr>
<tr>
<td>Wed Nov 5</td>
<td>21:11:11</td>
<td>Info: MID 182 interim AV verdict using Sophos CLEAN</td>
</tr>
<tr>
<td>Wed Nov 5</td>
<td>21:11:11</td>
<td>Info: MID 182 antivirus negative</td>
</tr>
<tr>
<td>Wed Nov 5</td>
<td>21:11:11</td>
<td>Info: MID 182 Custom Log Entry: &lt;====&gt; CLEAN URL! &lt;====&gt;</td>
</tr>
<tr>
<td>Wed Nov 5</td>
<td>21:11:11</td>
<td>Info: MID 182 Outbreak Filters: verdict negative</td>
</tr>
<tr>
<td>Wed Nov 5</td>
<td>21:11:11</td>
<td>Info: MID 182 queued for delivery</td>
</tr>
<tr>
<td>Wed Nov 5</td>
<td>21:11:11</td>
<td>Info: Delivery start DCID 23 MID 182 to RID [0]</td>
</tr>
</tbody>
</table>
Note: The URL that is embedded in the previous example has extra spaces included in the URL body, so it does not trip any web scans or proxy detection.

As shown in the example, Yahoo.com is deemed CLEAN and given a score of 8.39, is noted in the mail logs, and is delivered to the end user.

Content Filters for URLs with "No Score"

“No Score” is given for URLs when a reputation score cannot be determined. These may be URLs that contain new domains, or URLs that have seen little to no traffic and are not able to have a current score.

Administrators may wish to handle URLs with no score at their own discretion. If there is a seen increase in Phish-related emails and attachments, please review the URL score associated. Administrators may wish to have no score URLs redirected to the Cisco cloud Web Security proxy service for click-time evaluation.

Report Uncategorized and Misclassified URLs

At times, a URL might not be classified yet, or it might be miscategorized. In order to report URLs that have been miscategorized, and URLs that are not categorized but should be, visit the Cisco URL categorization requests page.

You might also desire to check the status of submitted URLs. In order to do this, click the Status on the Submitted URLs tab of this page.

Malicious URLs and Marketing Messages Are Not Caught by Anti-Spam or Outbreak Filters

This can occur because the web site reputation and category are only two criteria among many that anti-spam and outbreak filters use in order to determine their verdicts. In order to increase the sensitivity of these filters, lower the thresholds that are required to take action, such as rewriting or replacing URLs with text, or quarantining or dropping messages.

Alternatively, you can create content or message filters based on the URL reputation score.

Related Information

- Cisco Email Security Appliance - End-User Guides
- Technical Support & Documentation - Cisco Systems