Contents

Introduction

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

Background Information

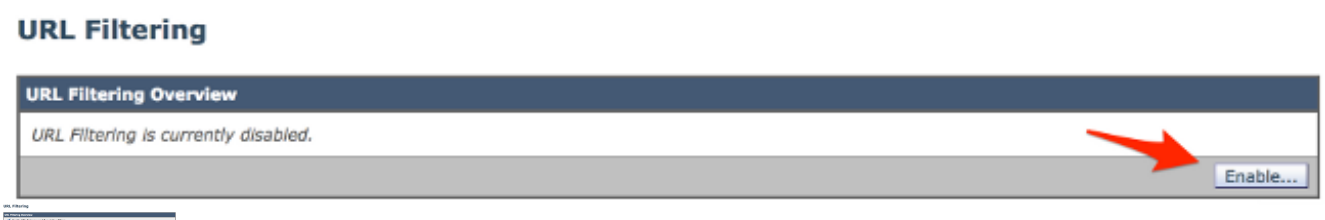
When you enable URL Filtering on the ESA, you must also enable other features, dependent upon your desired functionality. Here are some typical features that are enabled alongside URL Filtering:

- 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.

Enable URL Filtering

In order to implement URL Filtering on the ESA, you must first enable the feature. There are two different methods that you can use in order to enable this feature: With the use of either the GUI or the CLI.

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



In order to enable URL Filtering with the use of the CLI, enter the **websecurityconfig** command:

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

It is important to note that you must also enable URL Logging from within the VOF. This is a CLI-only feature that must be enabled as shown here:

```
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.

Would you like to receive Outbreak Filter alerts? [N]>

What is the largest size message Outbreak Filters should scan?
[2097152]>

Do you want to use adaptive rules to compute the threat level of messages? [Y]>

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.

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 (with the exclusion of attachments) are evaluated. Any valid string for a URL is evaluated, to include strings with these components:

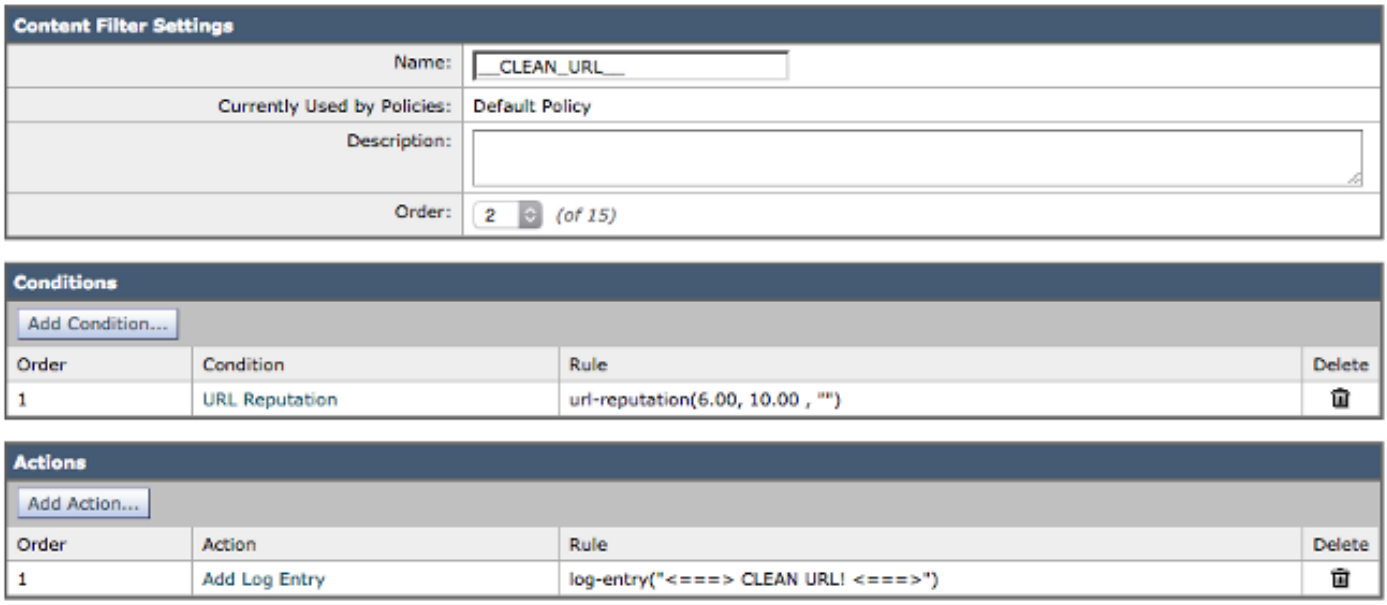
- HTTP, HTTPS, or WWW
- Domain or IP addresses
- Port numbers preceded by a colon (:)
- Uppercase or lowercase letters

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.

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 Clean URLs

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



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:

```
Wed Nov 5 21:11:10 2014 Info: Start MID 182 ICID 602
Wed Nov 5 21:11:10 2014 Info: MID 182 ICID 602 From: <bad_user@that.domain.net>
Wed Nov 5 21:11:10 2014 Info: MID 182 ICID 602 RID 0 To: <joe.user@goodmailguys.com>
Wed Nov 5 21:11:10 2014 Info: MID 182 Message-ID
'<D08042EA.24BA4%bad_user@that.domain.net>'
Wed Nov 5 21:11:10 2014 Info: MID 182 Subject 'Starting at the start!'
Wed Nov 5 21:11:10 2014 Info: MID 182 ready 2798 bytes from
<bad_user@that.domain.net>
Wed Nov 5 21:11:10 2014 Info: MID 182 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Wed Nov 5 21:11:11 2014 Info: MID 182 interim AV verdict using Sophos CLEAN
Wed Nov 5 21:11:11 2014 Info: MID 182 antivirus negative
Wed Nov 5 21:11:11 2014 Info: MID 182 URL http:// www .yahoo.com has reputation 8.39
matched url-reputation-rule
Wed Nov 5 21:11:11 2014 Info: MID 182 Custom Log Entry: <===> CLEAN URL! <===>
Wed Nov 5 21:11:11 2014 Info: MID 182 Outbreak Filters: verdict negative
Wed Nov 5 21:11:11 2014 Info: MID 182 queued for delivery
Wed Nov 5 21:11:11 2014 Info: New SMTP DCID 23 interface 192.168.0.199 address
192.168.0.200 port 25
Wed Nov 5 21:11:11 2014 Info: Delivery start DCID 23 MID 182 to RID [0]
Wed Nov 5 21:11:11 2014 Info: Message done DCID 23 MID 182 to RID [0] [('X-IronPort-AV',
'E=Sophos;i="5.07,323,1413259200"; \r\n d="scan\'208,217";a="182"'), ('x-ironport-av',
'E=Sophos;i="5.07,323,1413244800"; \r\n d="scan\'208,217";a="93839309"')]
Wed Nov 5 21:11:11 2014 Info: MID 182 RID [0] Response '2.0.0 Ok: queued as 7BAF5801C2'
Wed Nov 5 21:11:11 2014 Info: Message finished MID 182 done
Wed Nov 5 21:11:16 2014 Info: ICID 602 close
Wed Nov 5 21:11:16 2014 Info: DCID 23 close
```

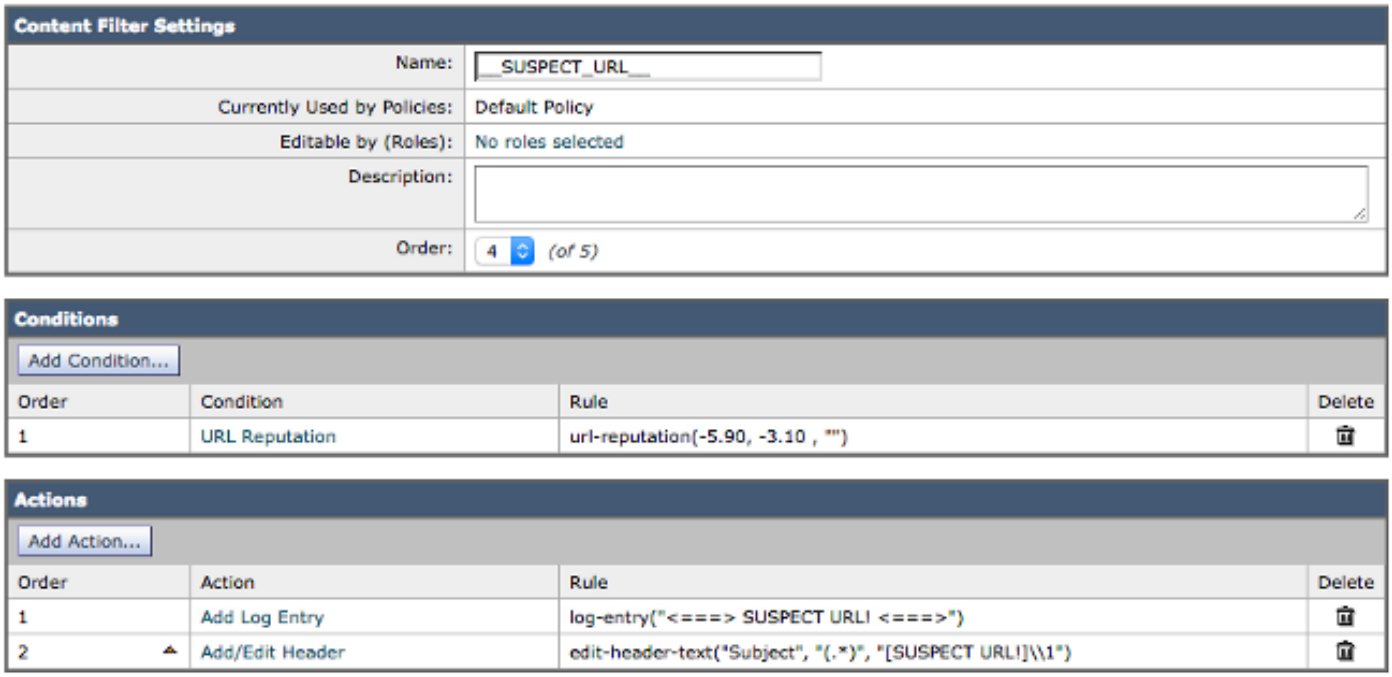
Note: The URL that is embedded in the previous example has extra spaces included in the URL body, so it does not trip any web scans or proxy detection.

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 Neutral or Suspect URLs

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:



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:

```
Wed Nov 5 21:22:23 2014 Info: Start MID 185 ICID 605
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 interim AV verdict using Sophos CLEAN
Wed Nov 5 21:22:24 2014 Info: MID 185 antivirus negative
Wed Nov 5 21:22:24 2014 Info: MID 185 URL https:// www.udemy.com/official-udemy-
instructor-course/?refcode=slfgiacoitvbfgl7tawqoxwqrdqcerbhub1flhsmfilcfku1te5x
ofictyrmwfcfxcvfgdkobgbcjv4bxcqbfmzcrymamwauxcuydtksayhpovebpvmdllxgxsu5vx8wzkj
hiwazhg5m&utm_campaign=email&utm_source=sendgrid.com&utm_medium=email has
```

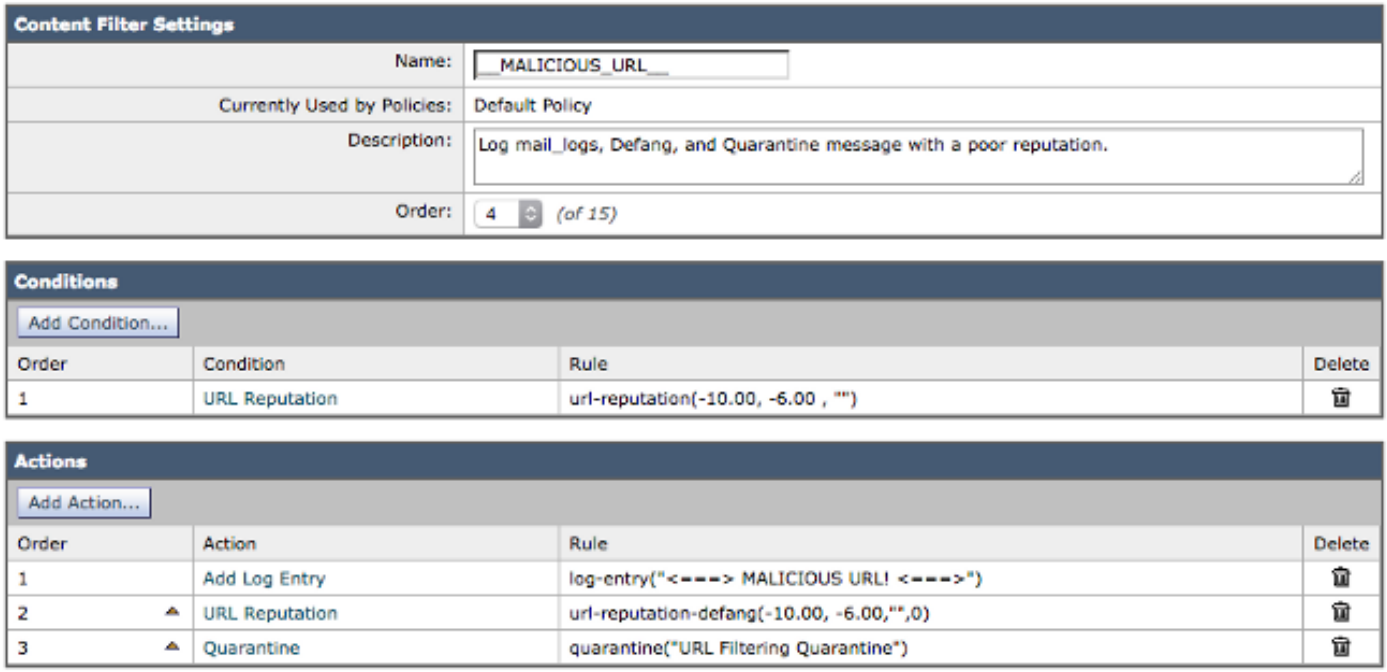
```
reputation -5.08 matched url-reputation-rule
Wed Nov 5 21:22:24 2014 Info: MID 185 Custom Log Entry: <===> SUSPECT URL! <===>
Wed Nov 5 21:22:24 2014 Info: MID 185 Outbreak Filters: verdict negative
Wed Nov 5 21:22:24 2014 Info: MID 185 queued for delivery
Wed Nov 5 21:22:24 2014 Info: New SMTP DCID 26 interface 192.168.0.199 address
192.168.0.200 port 25
Wed Nov 5 21:22:24 2014 Info: Delivery start DCID 26 MID 185 to RID [0]
Wed Nov 5 21:22:24 2014 Info: Message done DCID 26 MID 185 to RID [0]
[('X-IronPort-AV', 'E=Sophos;i="5.07,323,1413259200"; \r\n d="scan\'208,217";a="185"'),
('x-ironport-av', 'E=Sophos;i="5.07,323,1413244800"; \r\n d="scan\
'208,217";a="93843786"')]
Wed Nov 5 21:22:24 2014 Info: MID 185 RID [0] Response '2.0.0 Ok: queued as 0F8F9801C2'
Wed Nov 5 21:22:24 2014 Info: Message finished MID 185 done
```

> **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 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 unclickable, and places this into a URL Filtering quarantine. Here is an example from the mail logs:

```
Wed Nov 5 21:27:18 2014 Info: Start MID 186 ICID 606
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-W95DE5520A96FD9D69FAC2D9D840@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 21:27:18 2014 Info: ICID 606 close
Wed Nov 5 21:27:19 2014 Info: MID 186 interim verdict using engine: CASE spam positive
Wed Nov 5 21:27:19 2014 Info: MID 186 using engine: CASE spam positive
Wed Nov 5 21:27:19 2014 Info: ISQ: Tagging MID 186 for quarantine
Wed Nov 5 21:27:19 2014 Info: MID 186 interim AV verdict using Sophos CLEAN
Wed Nov 5 21:27:19 2014 Info: MID 186 antivirus negative
Wed Nov 5 21:27:19 2014 Info: MID 186 URL http:// peekquick .com /sdeu/cr.sedin/sdac/
denc.php has reputation -6.77 matched url-reputation-rule
Wed Nov 5 21:27:19 2014 Info: MID 186 Custom Log Entry: <===> MALICIOUS URL! <===>
Wed Nov 5 21:27:19 2014 Info: MID 186 URL http:// peekquick .com/sdeu/cr.sedin/sdac/
denc.php has reputation -6.77 matched url-reputation-defang-action
Wed Nov 5 21:27:19 2014 Info: MID 186 URL http:// peekquick .com /sdeu/cr.sedin/sdac/
denc.php has reputation -6.77 matched url-reputation-defang-action
Wed Nov 5 21:27:19 2014 Info: MID 186 rewritten to MID 187 by
url-reputation-defang-action filter '__MALICIOUS_URL__'
Wed Nov 5 21:27:19 2014 Info: Message finished MID 186 done
Wed Nov 5 21:27:19 2014 Info: MID 187 Outbreak Filters: verdict positive
Wed Nov 5 21:27:19 2014 Info: MID 187 Threat Level=5 Category=Phish Type=Phish
Wed Nov 5 21:27:19 2014 Info: MID 187 rewritten URL u'http:// peekquick .com
/sdeu/cr.sedin/sdac/denc.php-Robert'
Wed Nov 5 21:27:19 2014 Info: MID 187 rewritten to MID 188 by url-threat-protection
filter 'Threat Protection'
Wed Nov 5 21:27:19 2014 Info: Message finished MID 187 done
Wed Nov 5 21:27:19 2014 Info: MID 188 Virus Threat Level=5
Wed Nov 5 21:27:19 2014 Info: MID 188 quarantined to "Outbreak"
(Outbreak rule:Phish: Phish)
Wed Nov 5 21:27:19 2014 Info: MID 188 quarantined to "URL Filtering Quarantine"
(content filter:__MALICIOUS_URL__)
Wed Nov 5 21:28:20 2014 Info: SDS_CLIENT: Generated URL scanner configuration
Wed Nov 5 21:28:21 2014 Info: SDS_CLIENT: URL scanner enabled=1
Wed Nov 5 21:28:21 2014 Info: SDS_CLIENT: Generated URL scanner configuration
Wed Nov 5 21:28:21 2014 Info: SDS_CLIENT: URL scanner enabled=1
```

> **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.

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:

```
Wed Nov 5 21:40:49 2014 Info: Start MID 194 ICID 612
Wed Nov 5 21:40:49 2014 Info: MID 194 ICID 612 From: <bad_user@that.domain.net>
Wed Nov 5 21:40:49 2014 Info: MID 194 ICID 612 RID 0 To: <joe.user@goodmailguys.com>
Wed Nov 5 21:40:49 2014 Info: MID 194 Message-ID
'<COL128-W145FD8B772C824CEF33F859D840@phx.gbl>'
Wed Nov 5 21:40:49 2014 Info: MID 194 Subject 'URL Filter test malicious'
Wed Nov 5 21:40:49 2014 Info: MID 194 ready 2230 bytes from <bad_user@that.domain.net>
Wed Nov 5 21:40:49 2014 Info: MID 194 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Wed Nov 5 21:40:50 2014 Info: ICID 612 close
Wed Nov 5 21:40:50 2014 Info: MID 194 interim verdict using engine: CASE spam positive
Wed Nov 5 21:40:50 2014 Info: MID 194 using engine: CASE spam positive
Wed Nov 5 21:40:50 2014 Info: ISQ: Tagging MID 194 for quarantine
Wed Nov 5 21:40:50 2014 Info: MID 194 interim AV verdict using Sophos CLEAN
```

```
Wed Nov 5 21:40:50 2014 Info: MID 194 antivirus negative
Wed Nov 5 21:40:50 2014 Info: MID 194 queued for delivery
Wed Nov 5 21:40:52 2014 Info: RPC Delivery start RCID 20 MID 194 to local IronPort
Spam Quarantine
Wed Nov 5 21:40:52 2014 Info: ISQ: Quarantined MID 194
Wed Nov 5 21:40:52 2014 Info: RPC Message done RCID 20 MID 194
Wed Nov 5 21:40:52 2014 Info: Message finished MID 194 done
```

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.

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**