URL过滤配置和最佳实践Cisco电子邮件安全的

Contents

Introduction

本文描述如何配置在Cisco电子邮件安全工具(ESA)上的URL过滤和最佳实践为其使用。

背景信息

控制和防护有恶意或不理想的链路合并到反垃圾邮件、爆发、内容和消息过滤过程里在工作队列。这些控制：

- 增加保护的效果免受在消息和附件的有恶意的URL。
- URL过滤合并到爆发过滤里。此被加强的保护是有用的，即使您的组织已经有Cisco Web安全工具或相似的保护免受基于Web的威胁，因为在条目阻拦威胁。
- 您能也使用内容或消息过滤器采取根据基于web的名誉评分的行动(WBRS)在消息的URL。例如，您能重写URL以中立或未知名誉重定向他们到他们的安全的点击时间评估的Cisco Web安全代理。
- 更请好识别垃圾邮件
- 工具在消息使用链路名誉和类别，与其他垃圾邮件证明算法一道，帮助识别垃圾邮件。例如，如果在消息的一条链路属于到营销网站，消息是可能是营销消息。
- 公司可接受的使用策略的支持实施
- URL类别(例如，成人内容或非法活动)可以与内容和消息过滤器一道用于强制执行公司可接受的使用策略。
- 允许您识别频繁地点击在消息的URL为保护重写，以及链路频繁地点击的您的组织的用户。

当您配置在ESA时的URL过滤，您必须也配置其它功能从属在您的期望功能。这是沿着URL过滤被启用的一些典型的功能：

- 对于垃圾邮件的高级保护，必须启用反垃圾邮件扫描功能全局符合可适用的邮件策略。这可以是Cisco IronPort反垃圾邮件(IPAS)或Cisco智能多扫描(IMS)功能。
- 对于malware的高级保护，必须启用爆发过滤器或病毒爆发过滤器(VOF)功能全局符合可适用的

邮件策略。

- 对于根据URL名誉的动作，或者为了强制执行与使用的可接受的使用策略消息和内容过滤器，您必须enable (event) VOF全局。

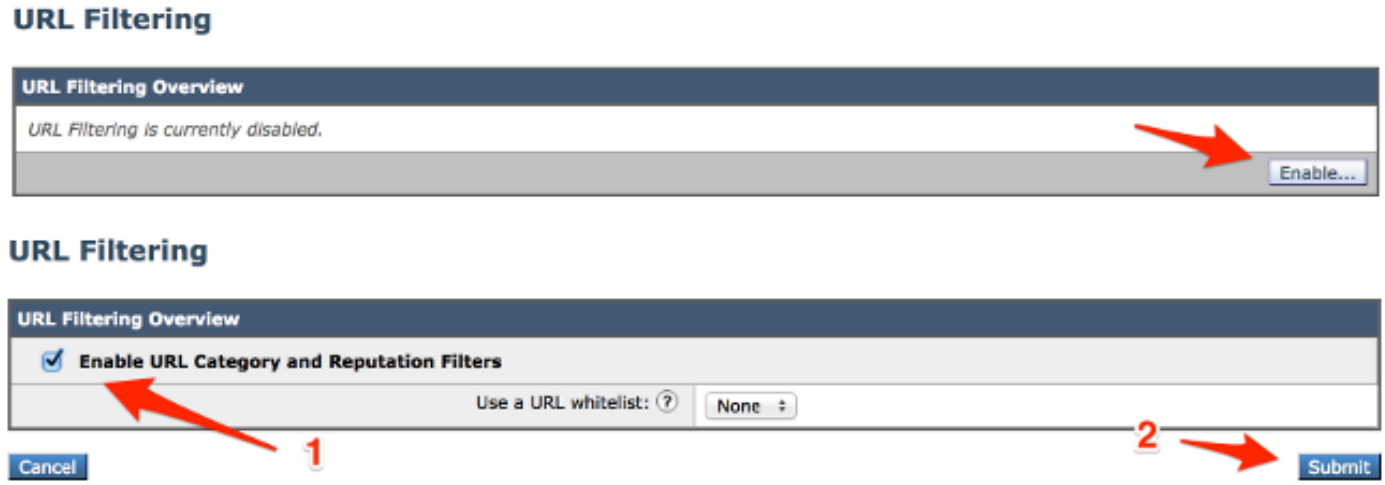
Note:自电子邮件安全的AsyncOS 11.1，扫描在附件的URL的技术支持当前是可用的。 您能当前配置您的工具为在消息附件的URL扫描，并且进行对这样消息的配置的动作。 您能使用URL名誉和URL类别内容和消息过滤器为在消息附件的URL扫描。欲了解更详细的信息，请参阅在用户指南或在线帮助的"使用消息过滤器强制执行电子邮件策略"，"内容过滤器"和"防止受到有恶意或不理想的URL"章节。

Note:当前另外自电子邮件安全的AsyncOS 11.1， URL过滤技术支持的技术支持的可用缩短的URL。 您能当前配置您的工具执行在缩短的URIs的URL过滤，并且从缩短的URL检索实际URL。基于原始URL的URL名誉评分，一个配置的动作在缩短的URL采取。对缩短的URL的enable (event) URL过滤在您的工具，请参阅在用户指南或在线帮助的"防止受到有恶意或不理想的URL"章节和CLI参考指南关于Cisco电子邮件安全工具的AsyncOS。

Enable (event) URL过滤

为了实现在ESA的URL过滤，您首先必须enable (event)功能。 URL过滤可能是从GUI或CLI的enable (event)由ESA管理员。

对与使用的enable (event) URL过滤GUI，请连接对**安全服务> URL过滤> Enable (event)** ：



从CLI，请运行命令， **websecurityconfig** ：

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

Note:URL记录是一个子功能从VOF内。使用**outbreakconfig**，这是必须启用如显示这里的一个仅CLI功能， ：

```
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:保证您**确认**对您的配置的*任意*更改，在您从GUI或CLI进行在您的ESA前。

Enable (event)缩短的URL的URL过滤技术支持

使用**websecurityadvancedconfig**，启用缩短的URL的URL过滤技术支持能由仅CLI完成， ：

```
myesa.local> 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:
bit.ly, tinyurl.com, ow.ly, tumblr.com, ff.im, youtu.be, tl.gd, plurk.com, url4.eu, j.mp,
goo.gl, yfrog.com, fb.me, alturl.com, wp.me, chatter.com, tiny.cc, ur.ly
```

Cisco推荐有为URL过滤配置最佳实践启用的此。 一旦启用，邮件日志将反射，缩短的URL在消息内使用：

```
myesa.local> 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:
bit.ly, tinyurl.com, ow.ly, tumblr.com, ff.im, youtu.be, tl.gd, plurk.com, url4.eu, j.mp,
goo.gl, yfrog.com, fb.me, alturl.com, wp.me, chatter.com, tiny.cc, ur.ly
```

一旦URL过滤是启用的正如此条款所描述，从邮件记录的上面的例子，我们能看到bit.ly链路记录的和扩展对也记录的原始链路。

创建URL过滤动作

当您单独enable (event) URL过滤，它不采取行动也许包含实际和有效的URL的消息。

在Inbound和Outbound消息包括的URL被评估。URL的所有有效字符串被评估，包括与这些组件的字符串：

- HTTP、HTTPS或者WWW
- 域或IP地址
- 冒号之后的端口号(：)
- 大写或小写字母

当系统评估URL为了确定时消息是否是垃圾邮件，如果需要，负荷管理的，优先安排并且筛选在出局的消息的入站消息。

您在消息正文和消息附件可进行对根据URL名誉或类别的消息的动作。除修改URL或他们的工作情况之外，如果要进行任何动作，请添加一个URL名誉或URL类别情况并且选择您要申请动作的名誉评分或URL类别。

例如，如果要适用丢弃(最后的行动)动作于在成人类别包括URL的所有消息，请添加类型与所选的成人类别的URL类别的情况。

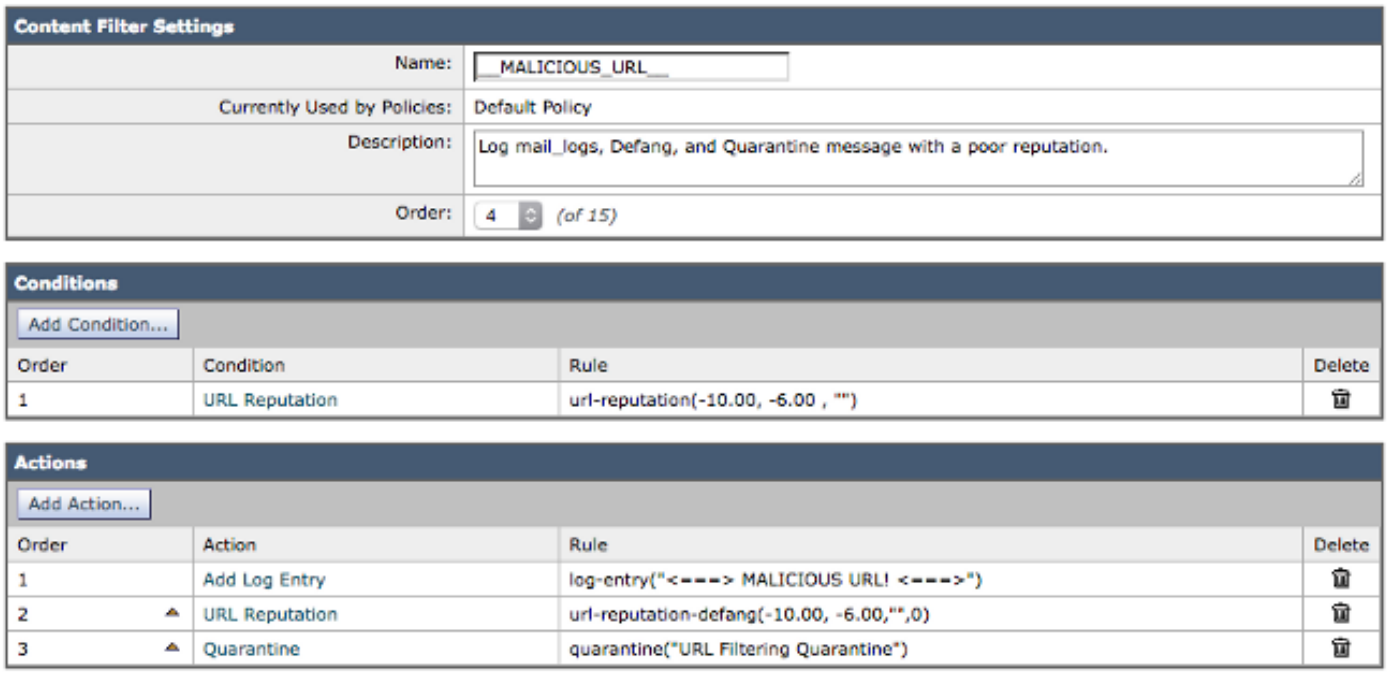
如果不指定类别，您选择的动作适用于所有消息。

URL名誉评分为干净排列，中立，并且有恶意的URL预定义和不编辑可能。然而，您能指定一个自定义范围。指定的终端在您指定的范围包括。例如，如果创建从-8的一个自定义范围到-10，然后-8和-10在范围包括。请勿请使用“评分”名誉评分不可能确定的URL。

为了迅速扫描URL和采取行动，您能创建内容过滤器，以便，*如果*消息有有效URL，*然后*动作适用。从GUI，请连接**邮寄策略>流入内容过滤器>Add过滤器**。

使有恶意的URL的过滤器满意

此示例显示有恶意的URL的一扫描与此入站内容过滤器的实施：



Content Filter Settings

Name:	__MALICIOUS_URL__
Currently Used by Policies:	Default Policy
Description:	Log mail_logs, Defang, and Quarantine message with a poor reputation.
Order:	4 (of 15)

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-10.00, -6.00 , "")	

Actions

Add Action...

Order	Action	Rule	Delete
1	Add Log Entry	log-entry("<===> MALICIOUS URL! <===>")	
2	URL Reputation	url-reputation-defang(-10.00, -6.00,"",0)	
3	Quarantine	quarantine("URL Filtering Quarantine")	

使用到位此过滤器，URL的系统扫瞄与*有恶意的*名誉(-10.00到-6.00)，添加日志条目到邮件日志，使用*拔去的尖牙*动作为了使链路非clickable，并且放置此到URL过滤检疫。这是从邮件日志的一个示例：

```
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:URL在的前一个示例被嵌入有在URL正文包括的额外空间，因此它不绊倒任何Web扫瞄或代理检测。

peekquick.com的此URL是**有恶意**和计分在**-6.77**。条目在邮件日志被做，您能看到所有在动作的进程。URL过滤发现了有恶意的URL，拔去，并且检疫它的尖牙。VOF也计分了它根据其规则集的正，和，假设详细资料这是相关Phish。

如果VOF不是启用的，同一个消息通过被处理得，但是URL扫瞄没有操作没有VOF的被添加的能力驱动扫瞄和动作。然而，在本例中消息正文由Cisco反垃圾邮件引擎(案件)扫描并且视为作为垃圾邮件正：

```
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
```

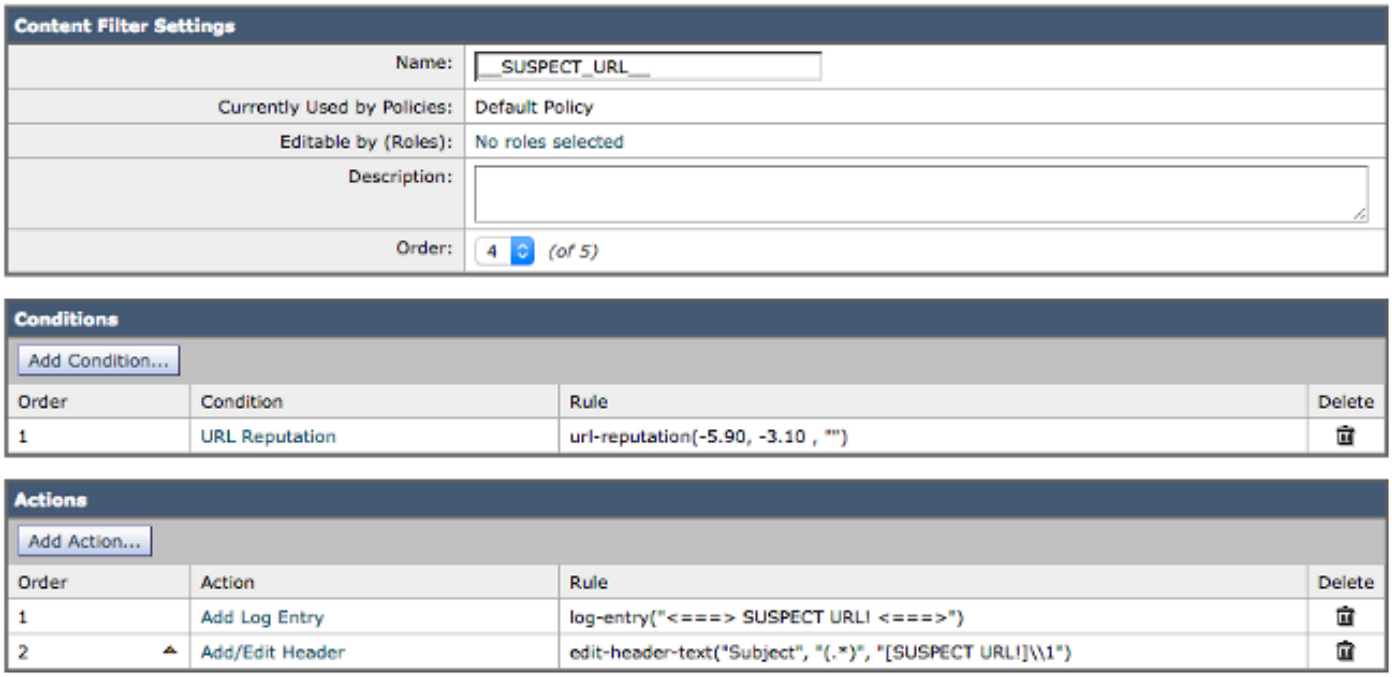
此检测通过单独案件总是不发生。当案件和IPAS规则也许包含该匹配某些发送方、域或者消息内容为了发现单独时，此威胁有时期。

中立或可疑的URL的内容过滤器

中立URL名誉意味着URL当前是干净的，但是可能启用有恶意今后，因为他们是倾向的对攻击。对于这样URL，管理员能创建无阻塞策略，例如，重定向他们对点击时间评估的Cisco Web安全代理。

Note:在电子邮件安全的AsyncOS 9.7和以后，以前被标记“可疑”的URL当前被标记“中性”。 只标记更改了;基础逻辑和处理未更改。

此示例显示中立/嫌疑犯URL的一扫描与此入站内容过滤器的实施：



使用到位此过滤器，系统搜索与*中性*或者*嫌疑犯的*URL，名誉(-5.90到-3.1)并且添加日志条目到邮件日志。此示例显示一个被修改的主题为了加在前面**"[SUSPECT URL!]"**。这是从邮件日志的一个示例：

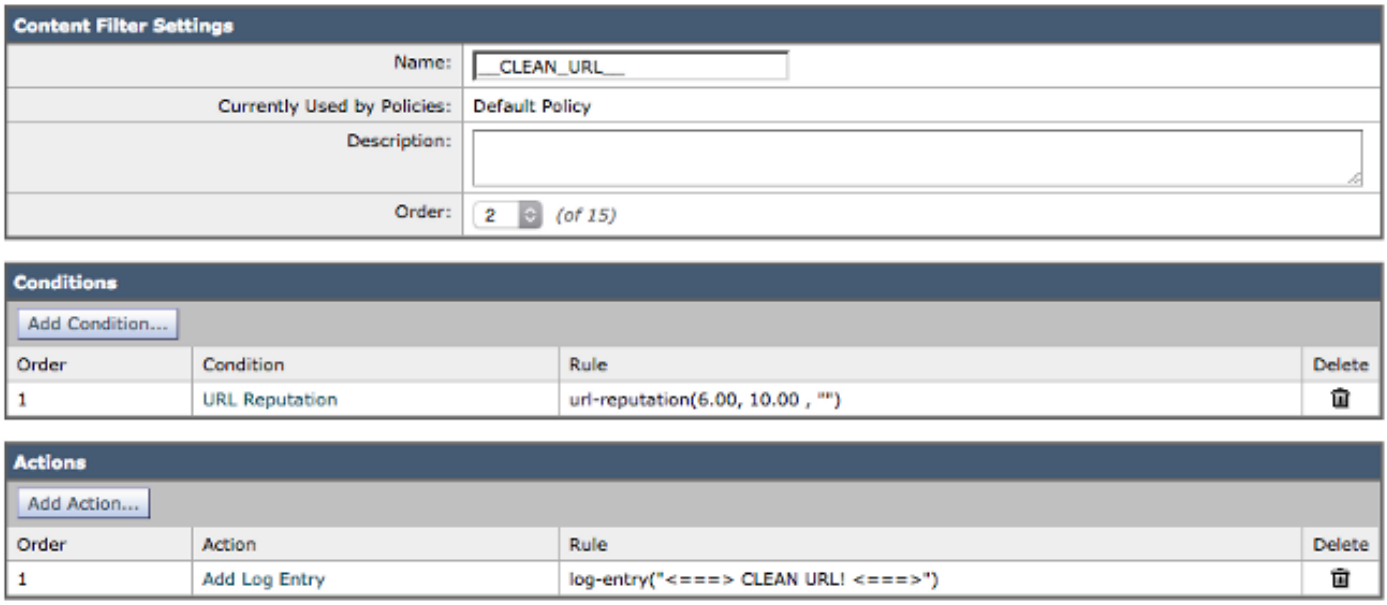
```
Wed Nov 5 21:22:23 2014 Info: Start MID 185 ICID 605
Wed Nov 5 21:22:23 2014 Info: MID 185 ICID 605 From: <bad_user@that.domain.net>
Wed Nov 5 21:22:23 2014 Info: MID 185 ICID 605 RID 0 To: <joe.user@goodmailguys.com>
Wed Nov 5 21:22:23 2014 Info: MID 185 Message-ID '<D0804586.24BAE%bad_user@that.domain.net>'
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=s1fgiacoitvbfgl7tawqoxwqrdqcerbhub1flhsmfilcfku1te5xofictyrmwfcfxcvfgdkobgbcjv4b
xcqbfmzcrymamwauxcuydtksayhpovebpvmdllxgxsu5vx8wzkjhiwazhg5m&utm_campaign=email&utm_source=sendg
rid.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**:URL在的前一个示例被嵌入有在URL正文包括的额外空间，因此它不绊倒任何Web扫瞄或代理检测。

在前一个示例的Udemy链路不看上去干净，并且它是被计分的**嫌疑犯**在- **5.08**。如邮件日志条目所显示，此消息允许被提供到终端用户。

干净的URL的内容过滤器

此示例显示干净的URL的一扫描与此入站内容过滤器的实施：



Content Filter Settings

Name:	__CLEAN_URL__
Currently Used by Policies:	Default Policy
Description:	
Order:	2 (of 15)

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(6.00, 10.00 , "")	

Actions

Add Action...

Order	Action	Rule	Delete
1	Add Log Entry	log-entry("<===> CLEAN URL! <===>")	

使用到位此过滤器，系统搜索与*干净的*名誉(6.00到10.00)的URL和添加日志条目到邮件登录顺序触发和记录基于web的名誉评分(WBRS)。此日志条目也帮助识别被触发的进程。这是从邮件日志的一个示例：

```
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**:URL在的前一个示例被嵌入有在URL正文包括的额外空间，因此它不绊倒任何Web扫瞄或代理检测。

如示例所显示， Yahoo.com在邮件日志视为**干净**并且产生评分**8.39**，注释和被传送到终端用户。

URL的内容过滤器与"没有评分"

当不可能确定时，“评分”没有为URL产生名誉评分。 这些可能是包含新的域少许看到了对没有数据流并且不能有当前评分的URL，或者URL。

管理员可能希望处理URL没有评分在他们自己的谨慎。 如果有在Phish有关的电子邮件和附件的一个被看到的增量，请查看被关联的URL评分。 管理员可能不希望有评分URL重定向对点击时间评估的Cisco网云Web安全代理服务。

报告Uncategorized和被错误分类的URL

通常， URL也许不被分类，或者也许miscategorized。为了报告miscategorized没有分类，然而应该是的URL和URL，请访问Cisco URL目录请求页。

您也许也希望检查被提交的URL的状态。为了执行此，点击在此页被提交的URL选项的**状态**。

有恶意的URL和营销消息没有由反垃圾邮件或爆发过滤器捉住

这能发生，因为网站名誉和类别只是在反垃圾邮件和爆发过滤器使用为了确定他们的判决的许多中的两个标准。为了增加要求采取行动，例如重写或与文本的替换URL或者检疫的或投下通信这些过滤器的区分，请降低阈值。

或者，您能创建根据URL名誉评分的内容或消息过滤器。

Related Information

- Cisco电子邮件安全工具-终端用户指南
- Technical Support & Documentation - Cisco Systems