ESA URL过滤能力提升计划和最佳实践

目录

[简介](#)
[背景信息](#)
[启用 URL 过滤](#)
[创建URL过滤操作](#)
[使干净的URL的过滤器满意](#)
[使中立或可疑的URL的过滤器满意](#)
[使有恶意的URL的过滤器满意](#)
[报告Uncategorized和被错误分类的URL](#)
[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](#)
[相关信息](#)

简介

本文描述如何启用在思科电子邮件安全工具(ESA)的URL过滤和最佳实践为其使用。

背景信息

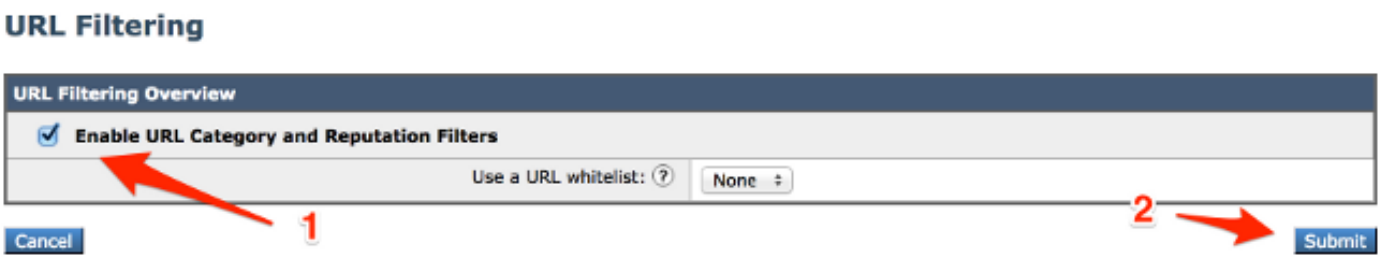
当您启用在ESA时的URL过滤，您必须也启用其它特性，从属在您的希望的功能。这是沿着URL过滤启用的一些典型的功能：

- 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。这可以是思科IronPort反垃圾邮件(IPAS)或思科智能多扫描(IMS)功能。
- 对于恶意软件的高级保护，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名誉的操作，或者为了强制执行与使用的可接受使用策略消息和内容过滤器，您必须启用VOF全局。

启用 URL 过滤

为了实现在ESA的URL过滤，您必须首先启用功能。有您能使用为了启用此功能的两不同的说法：使用使用GUI或CLI。

为了启用与使用的URL过滤GUI，请导航对**安全服务> URL过滤>enable** ：



为了启用与使用的URL过滤CLI，请输入**websecurityconfig**命令：

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

请注意您必须也启用记录从VOF的内部URL。这是必须启用如显示此处的一个仅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.

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.
```

注意：保证您**确认**对您的配置的*任意*更改，在您从GUI或CLI继续在您的ESA前。

创建URL过滤操作

当您启用单独时URL过滤，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 (与附件排除)被评估。URL的所有有效字符串被评估，包括字符串用这些组件：

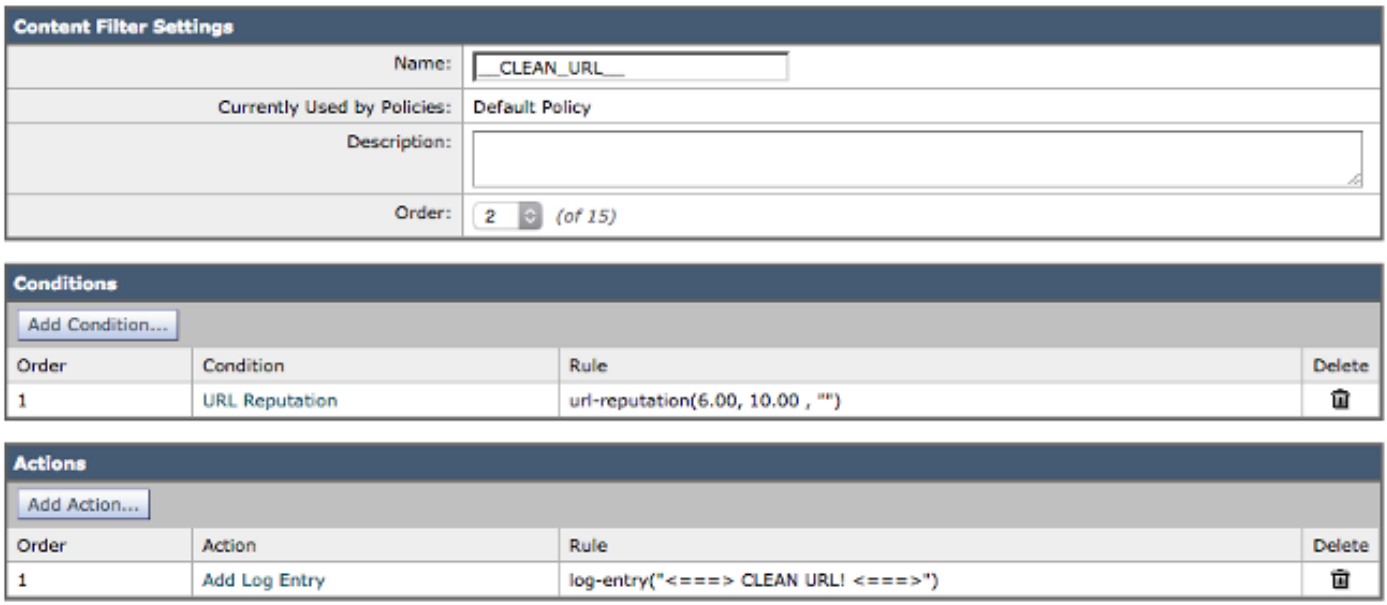
- HTTP、HTTPS或者WWW
- 域或IP地址
- 冒号之后的端口号(：)
- 大写或小写字母

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

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*操作应用。从GUI，请导航**邮寄策略>流入内容过滤器>Add过滤器**。

使干净的URL的过滤器满意

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：



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的名誉斯克尔(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
```

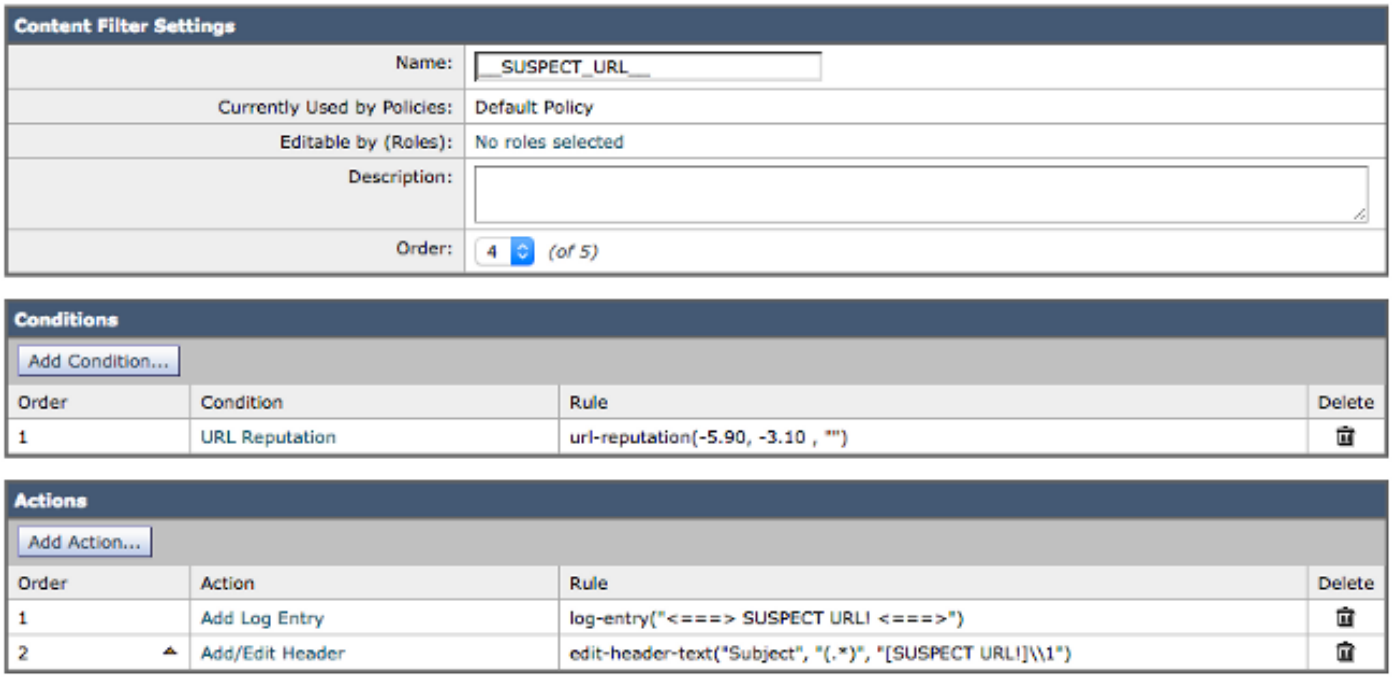
注意：URL在的前一个示例被嵌入有在URL正文包括的额外空间，因此它不绊倒任何Web扫瞄或代理检测。

如示例所显示，**Yahoo.com**在邮件日志视为**干净**并且给分数**8.39**，注释和传送给最终用户。

中立或可疑的URL的内容过滤器

注意：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;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。此示例显示一个已修改主题为了加在前面**“[SUSPECT URL!]”**。这是从邮件日志的一示例：

```
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=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
```

> **注意**：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，此消息允许传送对最终用户。

有恶意的URL的内容过滤器

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*操作为了使链路unclickable，并且放置此到URL过滤检疫。这是从邮件日志的一示例：

```
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
```

注意：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，您能看到所有在操作的进程。URL过滤检测有恶意的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，假设详细信息这是相关Phish。

如果VOF没有启用，同一个消息通过处理，但是URL扫瞄没有操作没有VOF的已添加能力驱动扫瞄和操作。然而，在本例中消息主题乘思科反垃圾邮件引擎(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规则也许包含匹配某些发送方、域或者消息内容为了检测单独时，此威胁有时期。

报告Uncategorized和被错误分类的URL

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

您也许也希望检查已提交URL状态。为了执行此，点击在此页已提交URL选项卡的**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名誉分数的内容或消息过滤器。

相关信息

- **思科电子邮件安全工具-最终用户指南**
- **技术支持和文档 - Cisco Systems**