为安全邮件网关和云网关配置 URL 过滤

目录

简介

本文档介绍如何在思科安全邮件网关和云网关上配置URL过滤以及使用URL过滤的最佳实践。

背景信息

URL过滤最初是随AsyncOS 11.1 for Email Security一起引入的。此版本允许配置Cisco Secure Email扫描邮件附件中的URL，并对此类邮件执行已配置的操作。邮件和内容过滤器使用URL信誉和URL类别检查邮件和附件中的URL。有关详细信息，请参阅《用户指南》或联机帮助中的“使用邮件过滤器实施邮件策略”、“内容过滤器”和“防止不受信任或不想要的URL”章。

针对不可信或不需要的链接的控制和保护功能已纳入反垃圾邮件、病毒爆发、内容和邮件过滤流程的工作队列。这些控件：

- 提高针对邮件和附件中的不受信任URL的防护效果。
- 此外，URL过滤已并入爆发过滤器。即使您的组织已经拥有思科网络安全设备或针对基于Web的威胁的类似保护，这种加强的保护也适用，因为它在进入点阻止威胁。
- 您还可以使用内容或邮件过滤器根据邮件中URL的基于Web的信誉评分(WBRS)采取行动。例如，您可以重写具有中立或未知信誉的URL，将其重定向到思科网络安全代理，进行点击时间

安全评估。
- 更好地识别垃圾邮件
- 设备使用邮件中的链接信誉和类别以及其他垃圾邮件识别算法来帮助识别垃圾邮件。例如，如果邮件中的链接属于营销网站，则邮件更可能是营销邮件。
- 支持实施企业可接受的使用策略
- URL类别（例如，成人内容或非法活动）可以与内容和邮件过滤器配合使用以实施可接受的企业使用策略。
- 允许识别组织中哪些用户最频繁点击已重写以保护邮件中的URL，以及最频繁点击的链接。

注意：在AsyncOS 11.1 for Email Security版本中,URL Filtering引入了对URL缩短的支持。使用CLI命令“websecurityadvancedconfig”可以查看和配置精简服务。此配置选项已在AsyncOS 13.5 for Email Security中更新。升级到此版本后，所有缩短的URL都会展开。没有选项可禁用缩短的URL的扩展。因此，思科建议使用适用于邮件安全的AsyncOS 13.5或更新版本，为URL防御提供最新保护。请参阅用户指南或联机帮助中的“防范恶意或不想要的URL”一章以及思科邮件安全设备AsyncOS的CLI参考指南。

注意：对于本文档，AsyncOS 14.2 for Email Security用于提供的示例和屏幕截图。

注意：思科安全电邮还提供了docs.ces.cisco.com上的深入URL防御指南。

先决条件

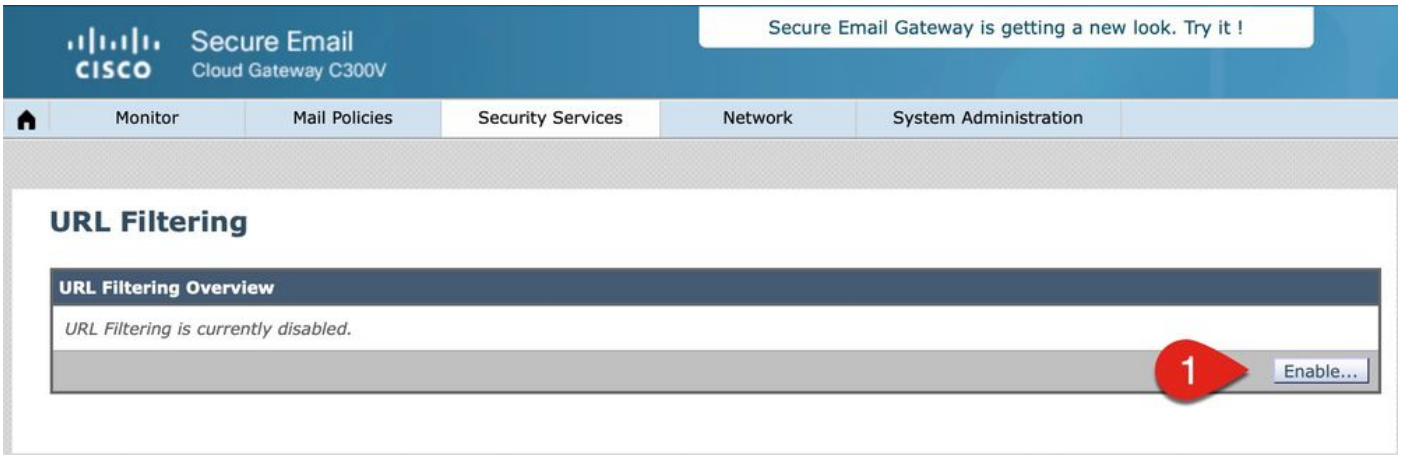
在思科安全邮件网关或云网关上配置URL过滤时，还必须配置其他取决于所需功能的功能。以下是与URL过滤一起启用的一些典型功能：

- 要增强垃圾邮件防护功能，必须根据适用的邮件策略全局启用反垃圾邮件扫描功能。反垃圾邮件被视为Cisco IronPort反垃圾邮件(IPAS)或思科智能多扫描(IMS)功能。
- 要增强恶意软件防护功能，必须根据适用的邮件策略全局启用爆发过滤器或病毒爆发过滤器(VOF)功能。
- 对于基于URL信誉的操作或使用邮件和内容过滤器实施可接受的使用策略，必须全局启用VOF。

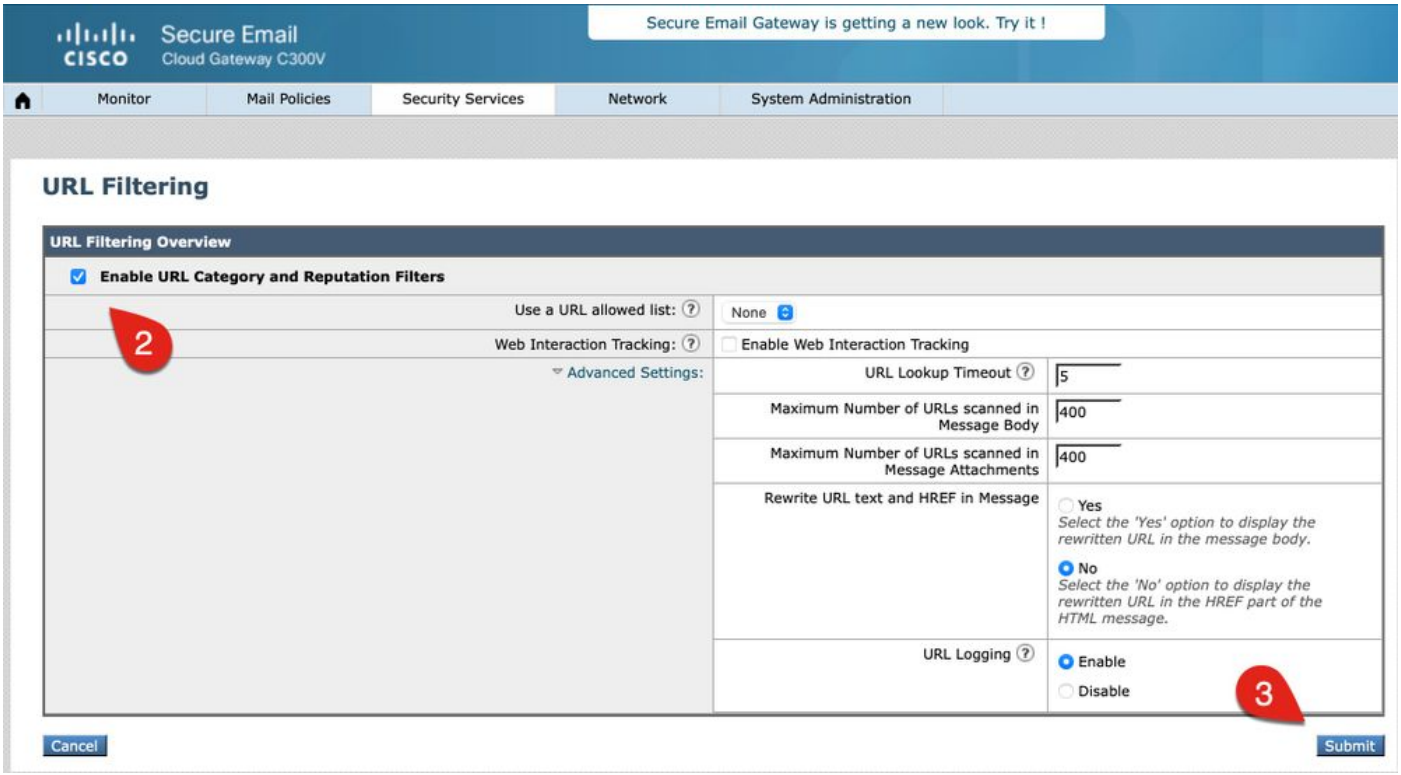
启用 URL 过滤

您必须首先启用此功能才能在思科安全邮件网关或云网关上实施URL过滤。管理员可以从GUI或CLI启用URL过滤。

要启用URL过滤，请从GUI导航到安全服务> URL过滤，然后单击启用：



接下来，单击Enable URL Category and Reputation Filters。此示例包括URL查找超时、已扫描的最大URL数的最佳实践值，并启用记录URL的选项：



注：请确保此时提交对配置的更改。

创建URL过滤操作

单独启用URL过滤时，它不会对邮件或带有附件的邮件中的URL执行操作。

评估传入和传出邮件策略的邮件和附件中包含的URL。URL的任何有效字符串都会经过计算，以包含具有以下组件的字符串：

- HTTP、HTTPS或WWW
- 域或IP地址
- 端口号前面带有冒号(:)
- 大写或小写字母

注意：大多数URL的mail_logs都显示URL日志条目。如果URL未记录在mail_logs中，请查看“邮件跟踪”(Message Tracking)以了解邮件ID(MID)。“邮件跟踪”(Message Tracking)包含“URL详细信息”(URL Details)选项卡。

当系统评估URL以确定邮件是否为垃圾邮件时（如有必要，进行负载管理），系统会优先处理入站邮件并筛选出出站邮件。

您可以根据URL信誉或邮件正文中的URL类别对邮件或带有附件的邮件执行操作。

例如，如果要将Drop(Final Action)操作应用于所有包含Adult类别中的URL的邮件，请添加URL Category类型的条件，并选中Adult类别。

如果未指定类别，则所选操作将应用于所有邮件。

“可信”(Trusted)、“有利”(Advantage)、“中性”(Neutral)、“可疑”(Problem)和“不可信”(Untrusted)的URL信誉得分范围是预定义且不可编辑的。您可以指定自定义范围。对于信誉得分尚未确定的URL，请使用“未知”。

要快速扫描URL并采取行动，可以创建内容过滤器，以便如果邮件具有有效的URL，则应用该操作。在GUI中，依次导航到邮件策略(Mail Policies)>传入内容过滤器(Incoming Content Filters)>添加过滤器(Add Filter)。

与URL关联的操作如下：

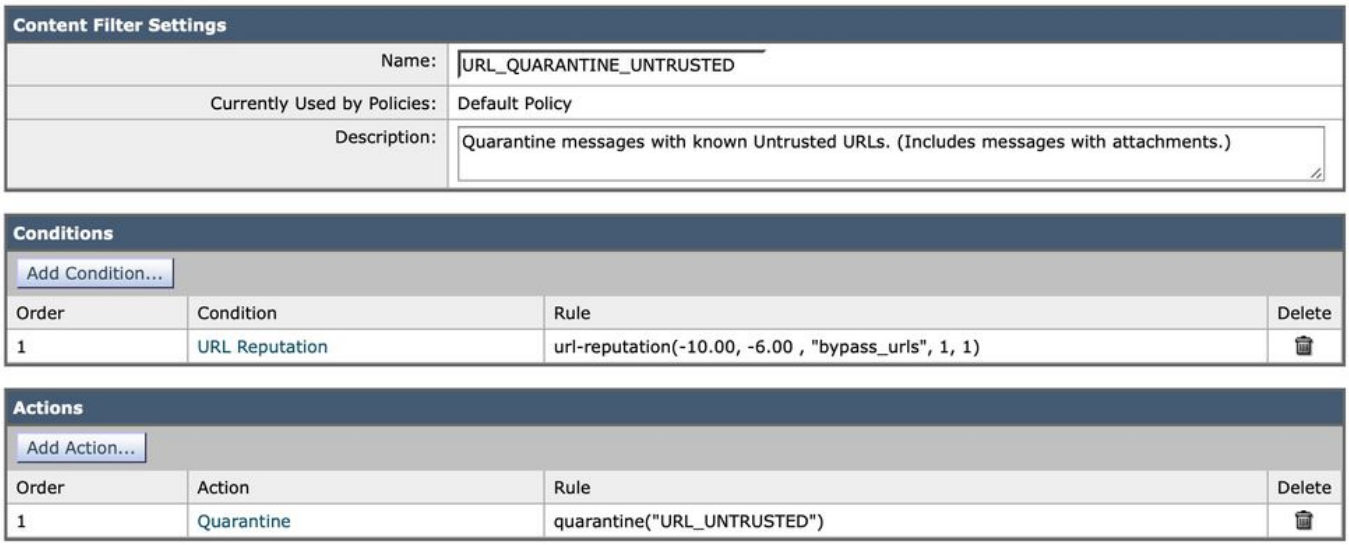
- Defang URL
  - 修改该URL使其不可单击，但邮件收件人仍然可以读取预期的URL。（在原始URL中插入额外的字符。）
- 重定向至思科安全代理
  - 点击该URL以通过思科安全代理进行其他验证时，该URL将被重写。根据思科安全代理判定，用户无法访问站点。
- 将URL替换为文本消息
  - 使用此选项，管理员可以在消息中重写URL，并将其发送到外部进行远程浏览器隔离。

不受信任的URL

不可信：特别恶劣、恶意或不理想的URL行为。这是最安全的建议阻止列表阈值；但是，也可能有未阻止的消息，因为其中的URL具有较低的威胁级别。将交付优先于安全性。

建议操作：阻止。（管理员可以完全隔离或丢弃邮件。）

此示例为URL过滤的内容过滤器提供上下文，以检测不受信任的URL:



Content Filter Settings

Name:	URL_QUARANTINE_UNTRUSTED
Currently Used by Policies:	Default Policy
Description:	Quarantine messages with known Untrusted URLs. (Includes messages with attachments.)

Conditions

Add Condition...

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

Actions

Add Action...

Order	Action	Rule	Delete
1	Quarantine	quarantine("URL_UNTRUSTED")	

通过此内容过滤器就位，思科安全邮件会扫描具有Untrusted信誉（–10.00到–6.00）的URL，并将邮件放入隔离区URL_UNTRUSTED。以下是mail_logs中的示例：

<#root>

```
Tue Jul 5 15:01:25 2022 Info: ICID 5 ACCEPT SG MY_TRUSTED_HOSTS match 127.0.0.1 SBRS None country Unite
Tue Jul 5 15:01:25 2022 Info: ICID 5 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jul 5 15:01:25 2022 Info: Start MID 3 ICID 5
Tue Jul 5 15:01:25 2022 Info: MID 3 ICID 5 From: <test@test.com>
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Domains for which SDR is requested: reverse DNS host: example.
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/
Tue Jul 5 15:01:25 2022 Info: MID 3 ICID 5 RID 0 To: <end_user>
Tue Jul 5 15:01:25 2022 Info: MID 3 Message-ID '<20220705145935.1835303@ip-127-0-0-1.internal>'
Tue Jul 5 15:01:25 2022 Info: MID 3 Subject "test is sent you a URL => 15504c0618"
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0-
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Tracker Header : 62c45245_jTikQ2lV2NYfmrGzMwQMBd68fxqFFueNmElw
Tue Jul 5 15:01:25 2022 Info: MID 3 ready 3123 bytes from <test@test.com>
Tue Jul 5 15:01:25 2022 Info: MID 3 matched all recipients for per-recipient policy DEFAULT in the inbo
Tue Jul 5 15:01:25 2022 Info: ICID 5 close
```

Tue Jul 5 15:01:25 2022 Info: MID 3 URL https://www.ihaveabadreputation.com/ has reputation -9.5 matched

Tue Jul 5 15:01:25 2022 Info: MID 3 quarantined to "Policy" (content filter:URL_QUARANTINE_UNTRUSTED)

```
Tue Jul 5 15:01:25 2022 Info: Message finished MID 3 done
```

URL ihaveabadreputation.com被视为UNTRUSTED，其评分为 — 9.5。URL过滤检测到不受信任的URL，并将其隔离到URL_UNTRUSTED。

如果URL过滤的内容过滤器仅对传入邮件策略启用，则来自mail_logs的上一个示例将提供一个示例。如果同一邮件策略启用了其他服务（如反垃圾邮件），则其他服务会指示是否已从这些服务及其规则中检测到URL。在同一个URL示例中，为传入邮件策略启用思科反垃圾邮件引擎(CASE)，并对邮件正文进行扫描并确定为垃圾邮件。这首先在mail_logs中指明，因为反垃圾邮件是邮件处理管道中的第一个服务。内容过滤器稍后将进入邮件处理管道：

<#root>

```
Tue Jul 5 15:19:48 2022 Info: ICID 6 ACCEPT SG MY_TRUSTED_HOSTS match 127.0.0.1 SBRS None country Unite
Tue Jul 5 15:19:48 2022 Info: ICID 6 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jul 5 15:19:48 2022 Info: Start MID 4 ICID 6
Tue Jul 5 15:19:48 2022 Info: MID 4 ICID 6 From: <test@test.com>
Tue Jul 5 15:19:48 2022 Info: MID 4 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0-
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/
Tue Jul 5 15:19:49 2022 Info: MID 4 ICID 6 RID 0 To: <end_user>
Tue Jul 5 15:19:49 2022 Info: MID 4 Message-ID '<20220705151759.1841272@ip-127-0-0-1.internal>'
Tue Jul 5 15:19:49 2022 Info: MID 4 Subject "test is sent you a URL => 646aca13b8"
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0-
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Tracker Header : 62c45695_mqwplhpxGDqtgUp/XTLGFKD60hwNKKsghUKA
Tue Jul 5 15:19:49 2022 Info: MID 4 ready 3157 bytes from <test@test.com>
Tue Jul 5 15:19:49 2022 Info: MID 4 matched all recipients for per-recipient policy DEFAULT in the inbo
Tue Jul 5 15:19:49 2022 Info: ICID 6 close
```

Tue Jul 5 15:19:49 2022 Info: MID 4 interim verdict using engine: CASE spam positive

Tue Jul 5 15:19:49 2022 Info: MID 4 using engine: CASE spam positive

```
Tue Jul 5 15:19:49 2022 Info: ISQ: Tagging MID 4 for quarantine
Tue Jul 5 15:19:49 2022 Info: MID 4 URL https://www.ihaveabadreputation.com/ has reputation -9.5 matche
Tue Jul 5 15:19:49 2022 Info: MID 4 quarantined to "URL_UNTRUSTED" (content filter:URL_QUARANTINE_UNTRU
Tue Jul 5 15:19:49 2022 Info: Message finished MID 4 done
```

有时，CASE和IPAS规则包含与特定发件人、域或邮件内容匹配的规则、信誉或分数，以单独检测URL威胁。在本示例中，看到ihaveabadreputation.com，它被标记为垃圾邮件隔离区(ISQ)，并被URL_QUARANTINE_UNTRUSTED内容过滤器标记为URL_UNTRUSTED隔离区。邮件首先进入URL_UNTRUSTED隔离区。当管理员从该隔离区放行邮件或符合URL_UNTRUSTED隔离区的时间限制/配置条件时，邮件将随后移入ISQ。

根据管理员首选项，可以为内容过滤器配置其他条件和操作。

未知URL

未知:之前未评估或没有显示用于断言威胁级别裁决的功能。URL信誉服务没有足够的数据来建立信誉。此判定不适用于URL信誉策略中的直接操作。

推荐的操作：使用后续引擎扫描以检查其他潜在恶意内容。

未知URL或“无信誉”可以是包含新域的URL或发现流量很少或没有流量且无法评估信誉和威胁级别判定的URL。当获取更多有关其域和来源的信息时，这些选项可能会变为不受信任。对于此类URL，思科建议记录内容过滤器或包含未知URL检测的内容过滤器。从AsyncOS 14.2开始，未知URL将发送到Talos情报云服务，以便根据各种威胁指示触发深入的URL分析。此外，未知URL的邮件日志条目为管理员提供包含在MID中的URL指示以及使用URL保护的可能补救。(请参阅如何为Microsoft Azure(Microsoft 365)API - Cisco配置思科安全电子邮件帐户设置了解更多信息。)

此示例为URL过滤的内容过滤器提供情景，以检测未知URL:

通过此内容过滤器就位，思科安全邮件扫描具有Unknown信誉的URL，并将日志行写入mail_logs。以下是mail_logs中的示例：

<#root>

```
Tue Jul 5 16:51:53 2022 Info: ICID 20 ACCEPT SG MY_TRUSTED_HOSTS match 127.0.0.1 SBRS None country Unit
Tue Jul 5 16:51:53 2022 Info: ICID 20 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jul 5 16:51:53 2022 Info: Start MID 16 ICID 20
Tue Jul 5 16:51:53 2022 Info: MID 16 ICID 20 From: <test@test.com>
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N
Tue Jul 5 16:51:53 2022 Info: MID 16 ICID 20 RID 0 To: <end_user>
Tue Jul 5 16:51:53 2022 Info: MID 16 Message-ID '<20220705165003.1870404@ip-127-0-0-1.internal>'
Tue Jul 5 16:51:53 2022 Info: MID 16 Subject "test is sent you a URL => e835eadd28"
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Tracker Header : 62c46c29_vrAqZZys2Hqk+BFINVrzdNLLn81kuIf/K6o
```

```
Tue Jul 5 16:51:53 2022 Info: MID 16 ready 3208 bytes from <test@test.com>
Tue Jul 5 16:51:53 2022 Info: MID 16 matched all recipients for per-recipient policy DEFAULT in the inb
Tue Jul 5 16:51:53 2022 Info: ICID 20 close
Tue Jul 5 16:51:54 2022 Info: MID 16 interim verdict using engine: CASE spam negative
Tue Jul 5 16:51:54 2022 Info: MID 16 using engine: CASE spam negative

Tue Jul 5 16:51:54 2022 Info: MID 16 URL http://mytest.example.com/test_url_2022070503 has reputation no


Tue Jul 5 16:51:54 2022 Info: MID 16 Custom Log Entry: <<<=== LOGGING UNKNOWN URL FOR MAIL_LOGS ===>>>


Tue Jul 5 16:51:54 2022 Info: MID 16 queued for delivery
Tue Jul 5 16:51:54 2022 Info: Delivery start DCID 13 MID 16 to RID [0]
Tue Jul 5 16:51:56 2022 Info: Message done DCID 13 MID 16 to RID [0]
Tue Jul 5 16:51:56 2022 Info: MID 16 RID [0] Response '2.6.0 <20220705165003.1870404@ip-127-0-0-1.inter
Tue Jul 5 16:51:56 2022 Info: Message finished MID 16 done
Tue Jul 5 16:52:01 2022 Info: DCID 13 close
```

URL mytest.example.com/test_url_2022070503没有信誉，显示为“noscore”。 URL_UNKNOWN内容过滤器将配置的日志行写入mail_logs。

在从思科安全邮件网关到Talos情报云服务的轮询周期后，系统会扫描该URL并确定为Untrusted。这可以在“Trace”级别的ECS日志中看到：

```
Tue Jul  5 16:54:42 2022 Debug: ECS: Finish polling
Tue Jul  5 16:55:42 2022 Debug: ECS: Remediation service notified.
Tue Jul  5 16:55:42 2022 Debug: ECS: Initiating remediation
Tue Jul  5 16:55:42 2022 Info: ECS: Initiating message remediation:
{'from': ['test@test.com'], 'URL': 'http://mytest.example.com/test_url_2022070503', 'message ID':
'<20220705165003.1870404@ip-172-31-43-120.us-east-2.compute.internal>', 'MID': 16, 'verdict':
'MALICIOUS', 'message UUID': 'e90dec74-f50b-4a63-9ab2-6adda4fcf422'}
Tue Jul  5 16:55:42 2022 Debug: ECS: Unprocessed Remediation Data : [{'url_hash':
'8c6915e2ebbc9225ff8958db06db33beb4e932ae9e0d8c5b35805a2fxxyyxxyy', 'message_details': '{"mid": 16,
"birth_time": "1657039913", "from_addrs": ["test@test.com"], "recipients": ["[redacted]"],
"delivery_status": 1, "remediation_req_status": 3}', 'created_at': '2022-07-05 16:52:42.04515',
'verdict': '{"url": "http://mytest.example.com/test_url_2022070503", "verdict": "MALICIOUS"}',
'message_uuid': 'e90dec74-f50b-4a63-9ab2-6adda4fcf422', 'message_id':
'<20220705165003.1870404@ip-127-0-0-1.internal>'}]
Tue Jul  5 16:55:42 2022 Debug: ECS: Remediation records: [
    [
        16,
        "<20220705165003.1870404@ip-127-0-0-1.internal>",
        1657039913,
        "delete",
        3,
        "[{\"url\": \"http://mytest.example.com/test_url_2022070503\", \"conviction_timestamp\":
\"2022-07-05 16:52:42.04515\", \"url_hash\":
\"8c6915e2ebbc9225ff8958db06db33beb4e932ae9e0d8c5b35805a2fxxyyxxyy\"}]",
        [
            "[redacted]"
        ],
        [
            "test@test.com"
        ]
    ]
]
Tue Jul  5 16:55:42 2022 Debug: ECS: Remediation initiated.
Tue Jul  5 16:55:42 2022 Debug: ECS: Successfully recorded remediation initiation status into datastore.
```

然后，在mail_logs中，当调用并完成补救本身时：

```
Tue Jul 5 16:55:42 2022 Info: Message 16 containing URL 'http://mytest.example.com/test_url_2022070503'
Tue Jul 5 16:55:55 2022 Info: Message 16 was processed due to URL retrospection by Mailbox Remediation
```

管理员必须酌情考虑对未知URL执行的操作。如果发现与网络钓鱼相关的电子邮件和附件增加，请查看mail_logs和内容过滤器报告。此外，管理员可以配置将未知URL重定向到思科安全代理服务以进行点击时间评估。在本示例中，导航到URL_UNKNOWN内容过滤器中的Add Action > URL Reputation:

URL Reputation

Help

What is the reputation of the URL in the message body, subject or the message attachments? This rule evaluates the URL using either the Web Based Reputation Score (WBRS) or using information from the External Threat Feed engine.

Matching Condition

- (•) URL Reputation
  - ( ) Untrusted (-10.0 to -6.0)
  - ( ) Questionable (-5.9 to -3.1)
  - ( ) Neutral (-3.0 to 0.0)
  - ( ) Favorable (0.1 to 5.9)
  - ( ) Trusted (6.0 to 10.0)
  - ( ) Custom Range (min to max)
  - (•) Unknown
- ( ) External Threat Feeds

This option is currently unavailable because no threat feed sources have been configured. To create one, go to Mail Policies > External Threat Feeds Manager.

Use a URL allowed list: None

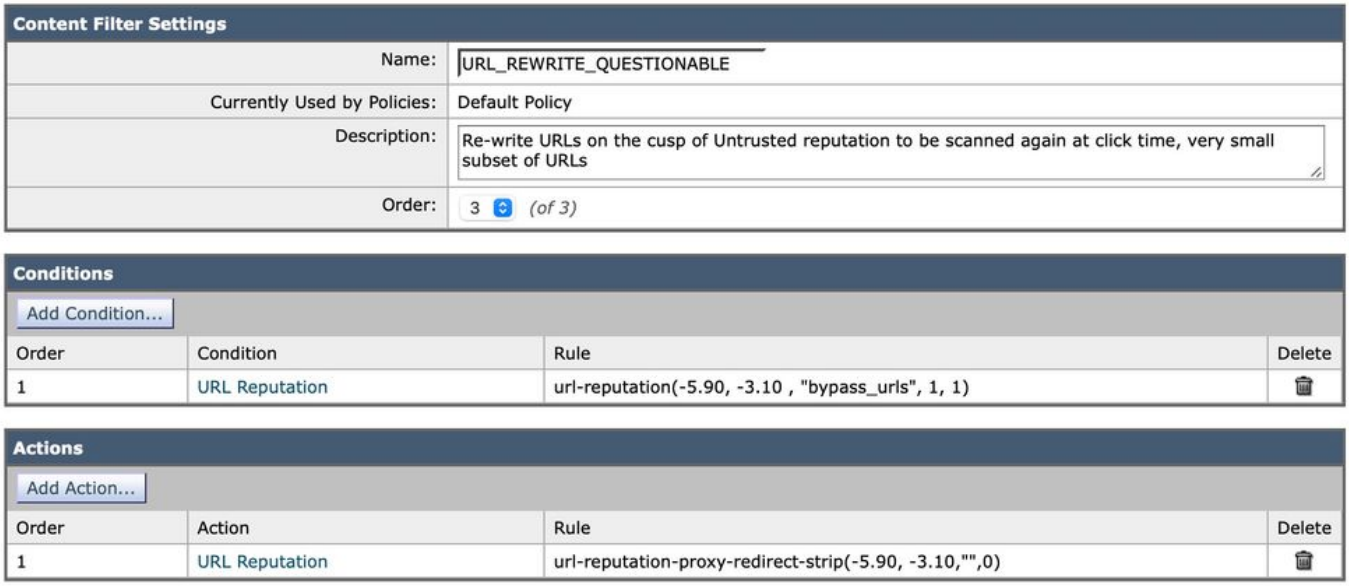
Check URLs within

- ( ) Message Body and Subject
- ( ) Attachments
- (•) All (Message Body, Subject and Attachments)

Action on URL within the message body and subject:

行为可能指示风险或可能是不理想的。虽然并非所有组织都安全，但此裁决具有较低且相对安全的误报(FP)率。未阻止的裁决会将传送优先于安全性，这可能导致包含有风险的URL的邮件。
建议的操作：使用后续引擎进行扫描，复查后将其阻止。

正如我们在未知URL中配置的一样，管理员会发现将可疑的URL发送到思科安全代理或利用操作来完全去除URL是有益的。



中性URL

中性：URL既没有正行为，也没有负行为。但是，已对其进行了评估。即，该URL当前没有已知风险。因此，这是信誉裁决的绝大部分。
推荐的操作：使用后续引擎扫描以检查其他潜在恶意内容。

管理员可以将分数为负的中立URL视为威胁。根据您的判断评估中性URL的邮件数量和出现次数。与我们更新未知URL和可疑URL以利用操作将URL发送到思科安全代理的方式类似，可以考虑中性URL或包含Neutral负面子集的自定义范围。此示例显示通过实施此入站内容过滤器扫描中性URL:

Content Filter Settings

Name:	URL_NEUTRAL
Currently Used by Policies:	*No policies currently use this rule.*
Description:	Send questionable Neutral URLs to be scanned again at click time. (Includes messages with attachments.)
Order:	4 *(of 4)*

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-3.00, -0.50 , "", 1, 1)	

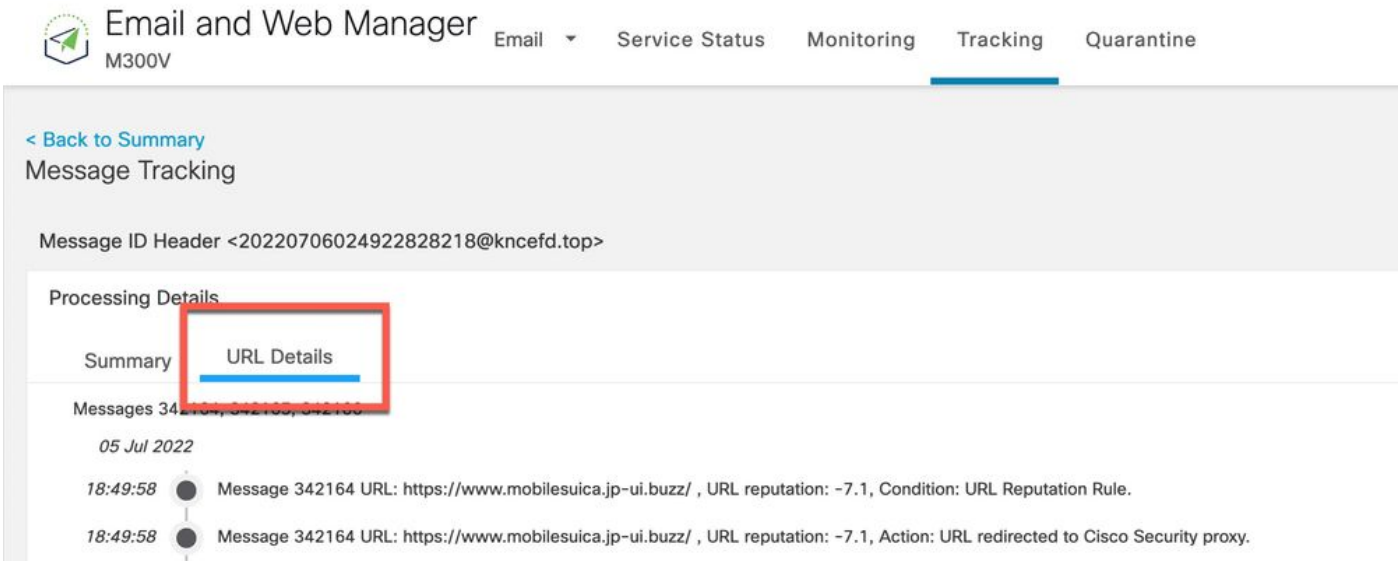
Actions

Add Action...

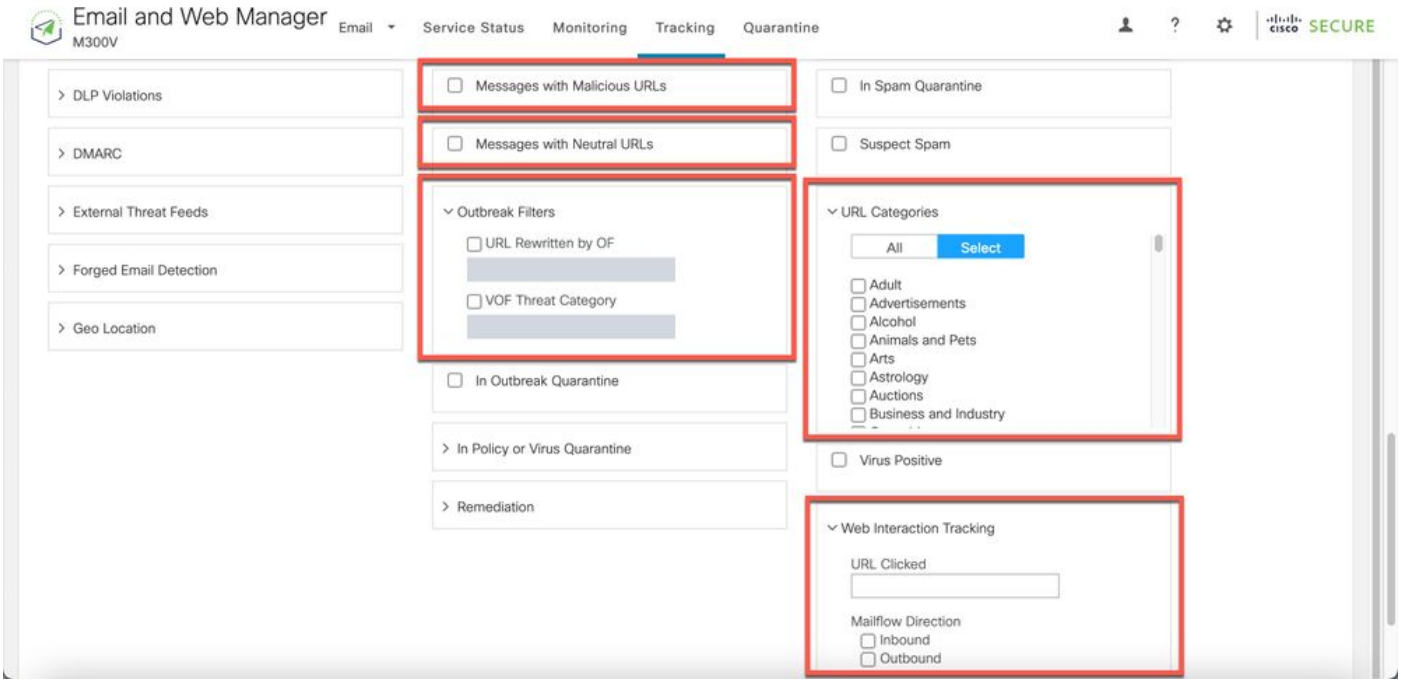
Order	Action	Rule	Delete
1	URL Reputation	url-reputation-proxy-redirect-strip(-3.00, -0.50,"",0)	

邮件跟踪

查看与MID关联的URL的邮件跟踪选项。 有时，URL不会记录到mail_logs，您可以在“邮件跟踪”(Message Tracking)详细信息中找到它们。例如：



邮件跟踪还为包含URL防御和交互的邮件提供高级搜索选项：



报告未分类和错误分类的URL

URL有时可以报告为没有信誉或分类。还有一些URL分类错误。要报告这些URL发现，请访问Talos信誉中心支持页面上的思科Talos的网络分类请求。

在报告URL后，您可以查看 我的票证 页码.

反垃圾邮件或爆发过滤器不会捕获恶意URL和营销邮件

发生这种情况的原因是，站点信誉和类别只是反垃圾邮件和爆发过滤器用于确定其裁决的众多标准中的两个标准。要提高这些过滤器的敏感度，请降低采取操作（例如用文本、隔离或丢弃邮件重写或替换URL）所需的阈值。

或者，您可以根据URL信誉分数创建内容或邮件过滤器。

Appendix

为缩短的URL启用URL过滤支持

注：本节仅适用于邮件安全的AsyncOS 11.1到13.0。

仅可使用websecurityadvancedconfig命令通过CLI执行对缩短的URL的URL过滤支持：

```
<#root>

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
```

Cisco建议为URL过滤配置最佳实践启用此功能。启用后，邮件日志会在邮件中使用缩短的URL时反映以下情况：

```
Mon Aug 27 14:56:49 2018 Info: MID 1810 having URL: http://bit.ly/2tztQUi has been expanded to https://
```

启用URL过滤后（如本文所述），我们可以从mail_logs示例中看到bit.ly链接已记录，并且其展开到的原始链接也已记录。

其他信息

思科安全电子邮件网关文档

- 版本说明
- 用户指南
- CLI参考指南
- 思科安全邮件网关的API编程指南
- 思科安全邮件网关中使用的开源
- 思科内容安全虚拟设备安装指南（包括vESA）

安全邮件云网关文档

- 版本说明
- 用户指南

Cisco Secure Email and Web Manager文档

- 版本说明和兼容性列表
- 用户指南
- Cisco Secure Email and Web Manager的API编程指南
- 思科内容安全虚拟设备安装指南（包括vSMA）

Cisco Secure产品文档

- 思科安全产品组合命名架构

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。