為 Secure Email Gateway 和 Cloud Gateway 設定 URL 篩選

目錄

簡介

本文檔介紹如何在思科安全電子郵件網關和雲網關上配置URL過濾，以及使用URL過濾的最佳實踐。

背景資訊

URL過濾最初是隨AsyncOS 11.1 for Email Security一起引入的。此版本允許配置思科安全電子郵件掃描郵件附件中的URL，並對此類郵件執行已配置的操作。郵件和內容過濾器使用URL信譽和URL類別檢查郵件和附件中的URL。有關更多詳細資訊，請參閱《User Guide》或聯機幫助中的「Using Message Filters to Enforce Email Policies」、「Content Filters」和「Protecting Against Untrusted or Undesirable URLs」章節。

針對不可信或不需要的連結的控制和保護已併入工作隊列，用於反垃圾郵件、病毒爆發、內容和郵件過濾流程。這些控制元件：

- 提高針對郵件和附件中不受信任URL的保護的效率。

- 此外，URL過濾已併入爆發過濾器。即使您的組織已經擁有思科網路安全裝置或類似針對基於Web的威脅的防護，這種加強的保護也適用，因為它可在進入點阻止威脅。
- 您還可以使用內容或郵件過濾器根據郵件中URL的基於Web的信譽評分(WBRS)執行操作。例如，您可以重寫具有中立或未知信譽的URL，將其重定向到思科網路安全代理，以便點選時評估其安全性。
- 更好地識別垃圾郵件
- 裝置使用郵件中的連結的信譽和類別以及其他垃圾郵件識別演算法來幫助識別垃圾郵件。例如，如果郵件中的連結屬於市場行銷網站，則郵件更有可能是市場行銷郵件。
- 支援實施企業可接受的使用策略
- URL類別（例如，成人內容或非法活動）可與內容和郵件過濾器配合使用，以強制實施可接受的公司使用策略。
- 允許您識別組織中哪些使用者最頻繁點選已重寫以保護消息中的URL，以及最頻繁點選的連結。

注意：在AsyncOS 11.1 for Email Security發行版中,URL過濾引入了對縮短的URL的支援。使用CLI指令「websecurityadvancedconfig」，可以看到並設定縮短器服務。AsyncOS 13.5 for Email Security中更新了此配置選項。升級到此版本後，所有縮短的URL都會展開。沒有選項可以禁用縮短的URL的擴展。因此，思科建議使用適用於電子郵件安全的AsyncOS 13.5或更新版本，為URL防禦提供最新保護。請參閱使用手冊或聯機幫助中的「防範惡意或不需要的URL」一章以及適用於Cisco郵件安全裝置的AsyncOS的CLI參考指南。

注意：對於本文件,AsyncOS 14.2 for Email Security用於提供的示例和螢幕截圖。

注意：思科安全電子郵件還在docs.ces.cisco.com上提供了深入的URL防禦指南。

必要條件

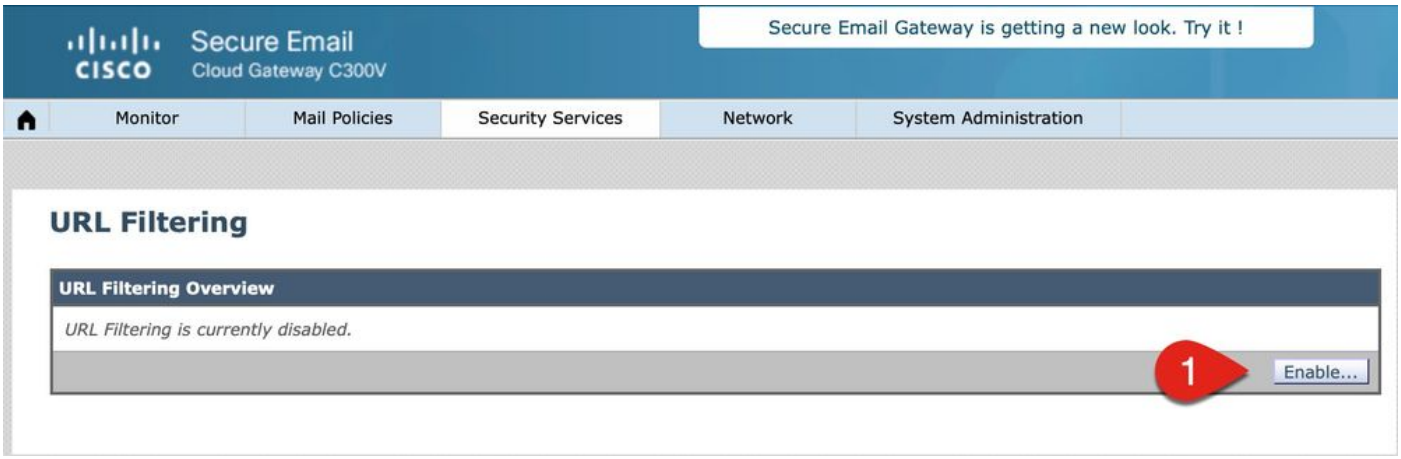
當您在思科安全電子郵件網關或雲網關上配置URL過濾時，還必須根據所需的功能配置其他功能。以下是與URL過濾一起啟用的一些典型功能：

- 要增強對垃圾郵件的防護，必須根據適用的郵件策略全域性啟用反垃圾郵件掃描功能。反垃圾郵件被視為Cisco IronPort反垃圾郵件(IPAS)或思科智慧多重掃描(IMS)功能。
- 為了增強針對惡意軟體的防護，必須根據適用的郵件策略全域性啟用爆發過濾器或病毒爆發過濾器(VOF)功能。
- 對於基於URL信譽的操作或使用郵件和內容過濾器實施可接受的使用策略，必須全域性啟用VOF。

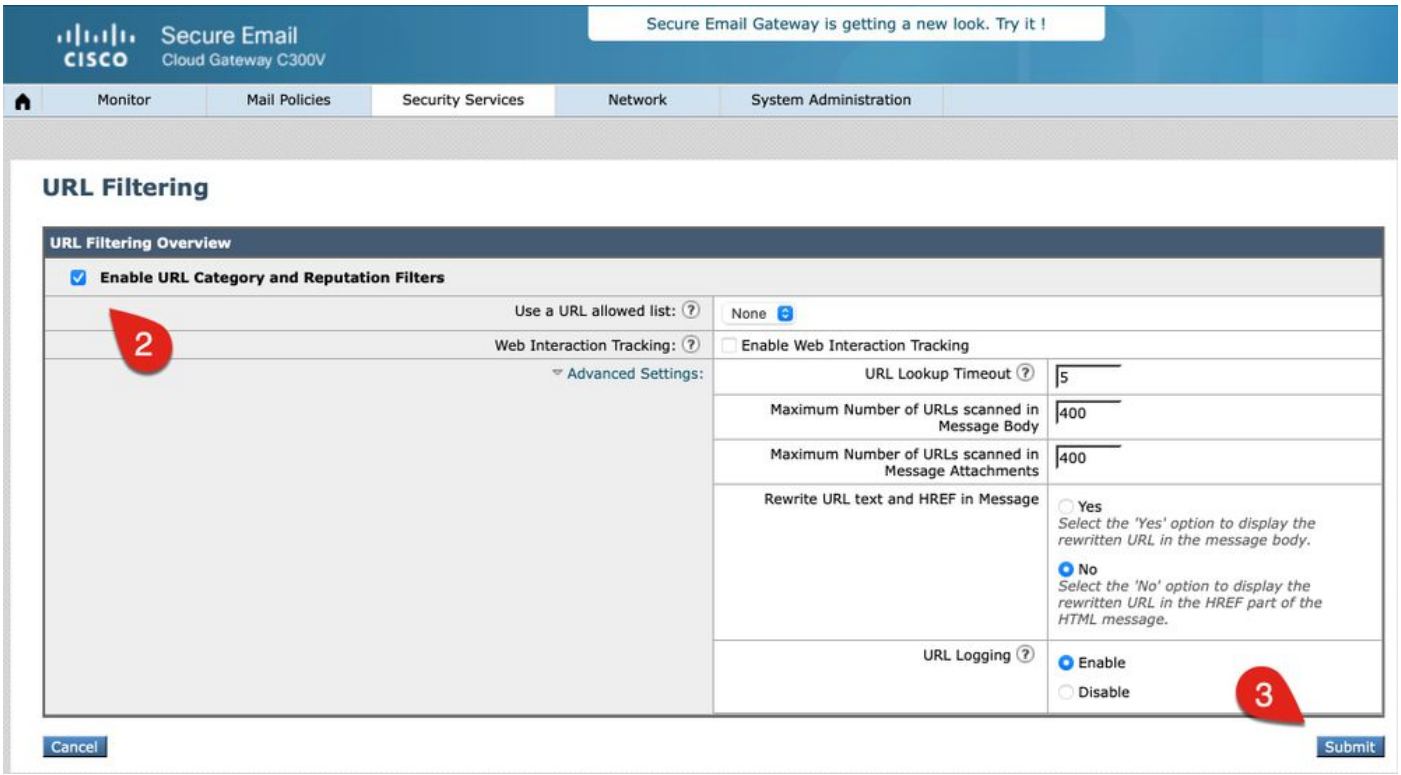
啟用URL篩選

您必須首先啟用此功能以在思科安全電子郵件網關或雲網關上實施URL過濾。管理員可以從GUI或CLI啟用URL過濾。

要啟用URL過濾，請從GUI導航到安全服務> URL過濾，然後點選啟用：



接下來，按一下「Enable URL Category and Reputation Filters」。此示例包括URL查詢超時、已掃描的最大URL數的最佳實踐值，並啟用記錄URL的選項：



註：請確保此時提交對配置的更改。

建立URL過濾操作

單獨啟用URL過濾時，它不會對郵件或帶有附件的郵件中的URL執行操作。

評估傳入和傳出郵件策略的郵件和附件中包含的URL。URL的任何有效字串都會經過計算，以包含

具有以下元件的字串：

- HTTP、HTTPS或WWW
- 域或IP地址
- 埠號前面帶有冒號(:)
- 大寫或小寫字母

注意：對於大多數URL，可從mail_logs中看到URL日誌條目。如果URL未記錄在mail_logs中，請檢視「郵件跟蹤」以瞭解郵件ID(MID)。郵件跟蹤確實包含「URL詳細資訊」頁籤。

當系統評估URL以確定郵件是否為垃圾郵件時（如果需要進行負載管理），系統會優先處理入站郵件並篩選出出站郵件。

您可以根據URL信譽或郵件正文中的URL類別或包含附件的郵件對郵件執行操作。

例如，如果要將Drop(Final Action)操作應用於所有包含Adult類別中的URL的郵件，請新增URL Category型別的條件，並選中Adult類別。

如果不指定類別，則選擇的操作將應用於所有消息。

「可信」(Trusted)、「有利」(Advantage)、「中性」(Neutral)、「可疑」(Probable)和「不可信」(Untrusted)的URL信譽得分範圍是預定義且不可編輯的。您可以指定自定義範圍。對於信譽得分尚未確定的URL，請使用「未知」。

要快速掃描URL並採取措施，可以建立內容過濾器，以便如果郵件具有有效的URL，則應用該操作。在GUI中，導航Mail Policies > Incoming Content Filters > Add Filter。

與URL關聯的操作如下：

- 預設URL
  - 該URL被修改為不可按一下，但郵件收件人仍可以讀取預定的URL。（在原始URL中插入額外的字元。）
- 重新導向至思科安全代理
  - 當按一下該URL以通過思科安全代理進行其他驗證時，將會重新寫入URL。根據思科安全代理判定結果，使用者無法訪問站點。
- 將URL替換為文本消息
  - 使用此選項，管理員可以重寫消息中的URL，並將其傳送到外部進行遠端瀏覽器隔離。

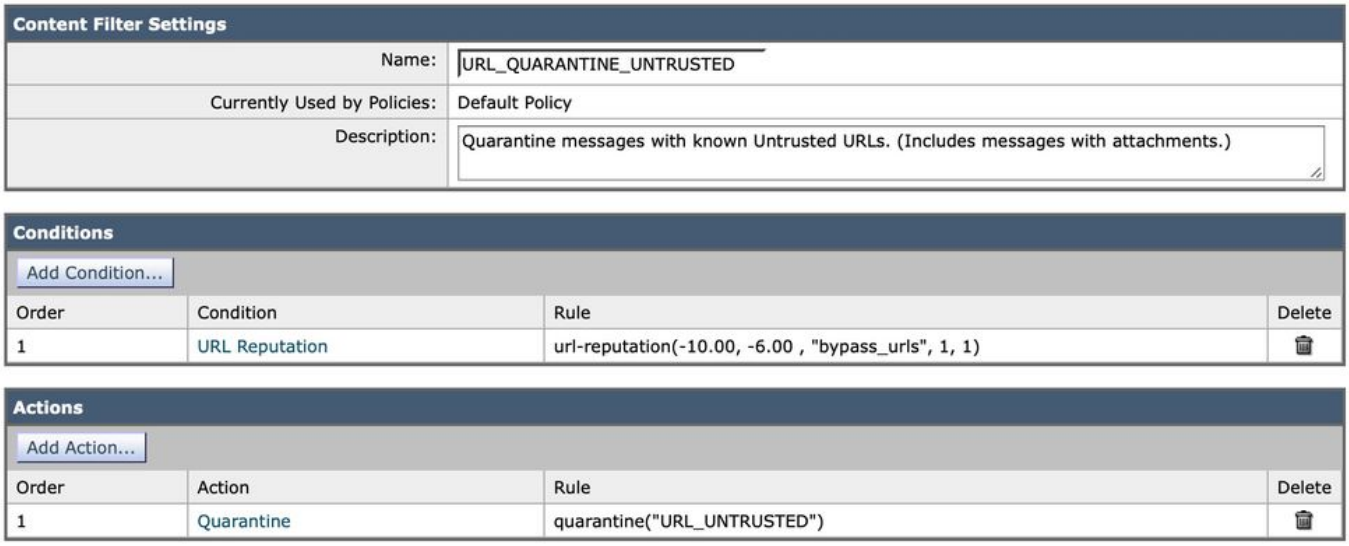
不受信任的URL

不可信：異常惡劣、惡意或不期望的URL行為。這是最安全的建議阻止清單閾值；但是，可能會有

未阻止的消息，因為其中的URL的威脅級別較低。將交付優先於安全性。

建議的操作：阻止。（管理員可以隔離或完全刪除郵件。）

此示例為URL過濾的內容過濾器提供上下文，以檢測不受信任的URL:



使用此內容過濾器後，思科安全電子郵件掃描具有Untrusted信譽（–10.00到–6.00）的URL，並將郵件放入隔離區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被視為UNTRUSTED，其分數為-9.5。URL篩選檢測到不受信任的URL並將其隔離到URL_UNTRUSTED。

如果URL過濾的內容過濾器僅對傳入郵件策略啟用，則mail_logs中的上一個示例將提供一個示例。如果同一郵件策略啟用了其他服務（如反垃圾郵件），則其他服務會指示是否已從這些服務及其規則中檢測到URL。在同一個URL示例中，為傳入郵件策略啟用思科反垃圾郵件引擎(CASE)，並且掃描郵件正文並確定郵件正文。這首先在mail_logs中指示，因為Anti-Spam是郵件處理管道中的第一個服務。在郵件處理管道中，內容過濾器稍後提供：

<#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
```

有時，CASE和IPAS規則包含與特定發件人、域或郵件內容相匹配的規則、信譽或分數以單獨檢測URL威脅。在此示例中，看到ihaveabadreputation.com，它通過URL_QUARANTINE_UNTRUSTED內容過濾器為垃圾郵件隔離區(ISQ)和URL_UNTRUSTED隔離區進行標籤。郵件首先進入URL_UNTRUSTED隔離區。當管理員從該隔離區放行郵件，或者已滿足URL_UNTRUSTED隔離區的時間限制/配置條件時，郵件將隨後移入ISQ。

根據管理員首選項，可以為內容過濾器配置其他條件和操作。

未知URL

未知:先前未評估或沒有顯示用於斷言威脅級別判定結果的功能。URL信譽服務沒有足夠的資料來建立信譽。此判定不適合於直接在URL信譽策略中執行的操作。

建議操作：使用後續引擎掃描以檢查其他潛在惡意內容。

未知URL或「無信譽」可以是包含新域的URL或看不到多少流量或沒有流量且無法評估信譽和威脅級別判定的URL。當獲取更多有關其域和來源的資訊時，這些域可以啟用Untrusted。對於此類URL，思科建議記錄內容過濾器，或包含未知URL檢測的內容過濾器。自AsyncOS 14.2起，將未知URL傳送到Talos智慧雲服務以根據各種威脅指示觸發深度的URL分析。此外，未知URL的郵件日誌條目為管理員提供包含在MID中的URL指示，以及使用URL保護可能進行的補救。(如需詳細資訊，請參閱如何為Microsoft Azure(Microsoft 365)API - Cisco配置思科安全電子郵件帳戶設定。)

此示例為URL過濾的內容過濾器提供上下文，以檢測未知URL:

使用此內容過濾器後，思科安全電子郵件將掃描具有未知信譽的URL，並將日誌行寫入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沒有信譽且顯示為「noscore」。
URL_UNKNOWN內容過濾器將配置的日誌行寫入mail_logs。

從思科安全電子郵件網關到Talos智慧雲服務的輪詢週期結束後，URL將被掃描並確定為不可信。可從「Trace」級別的ECS日誌中看到這種情況：

```
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.
```

然後，在mail_logs中，當補救本身被呼叫並完成時：

```
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
```

管理員必須自行決定對未知URL執行的操作。如果與網路釣魚相關的電子郵件和附件有所增加，請檢視mail_logs和內容過濾器報告。此外，管理員可以配置將未知URL重定向到思科安全代理服務以進行點選時間評估。在本示例中，導航到URL_UNKNOWN內容過濾器中的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

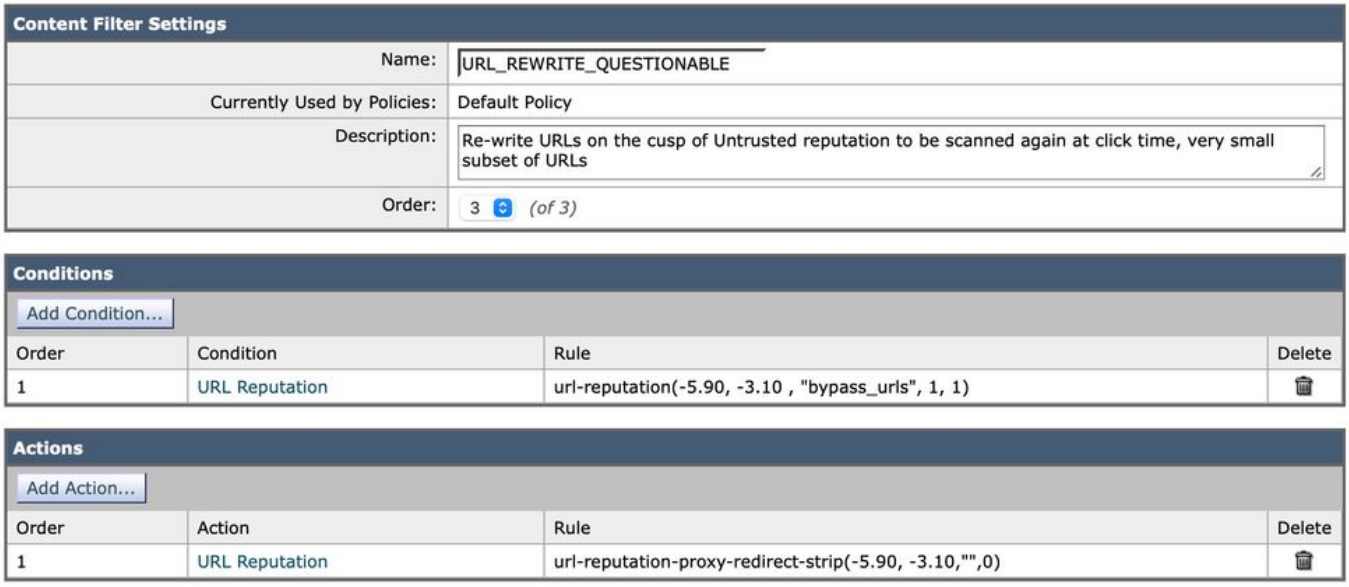
Check URLs within

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

Action on URL within the message body and subject:

建議操作：使用後續引擎掃描，並在檢查後阻止。

由於我們在未知URL中進行了配置，管理員可以發現將可疑的URL傳送到思科安全代理或利用操作來完全刪除URL是有益的。



Content Filter Settings

Name:	URL_REWRITE_QUESTIONABLE
Currently Used by Policies:	Default Policy
Description:	Re-write URLs on the cusp of Untrusted reputation to be scanned again at click time, very small subset of URLs
Order:	3 (of 3)

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-5.90, -3.10 , "bypass_urls", 1, 1)	

Actions

Add Action...

Order	Action	Rule	Delete
1	URL Reputation	url-reputation-proxy-redirect-strip(-5.90, -3.10,"",0)	

中性URL

中性：沒有正行為或負行為的URL。不過，已對此進行了評估。即，該URL當前沒有已知風險。因此，這是有關聲譽的裁決的主體。
建議操作：使用後續引擎掃描以檢查其他潛在惡意內容。

管理員可以將得分為負的中性URL視為威脅。根據您的判斷評估消息數和中性URL的出現次數。與我們更新未知URL和可疑URL以利用操作將URL傳送到思科安全代理類似，可以考慮中性URL或包含Neutral負面子集的自定義範圍。此範例顯示透過此傳入內容篩選器的實作掃描中性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)	

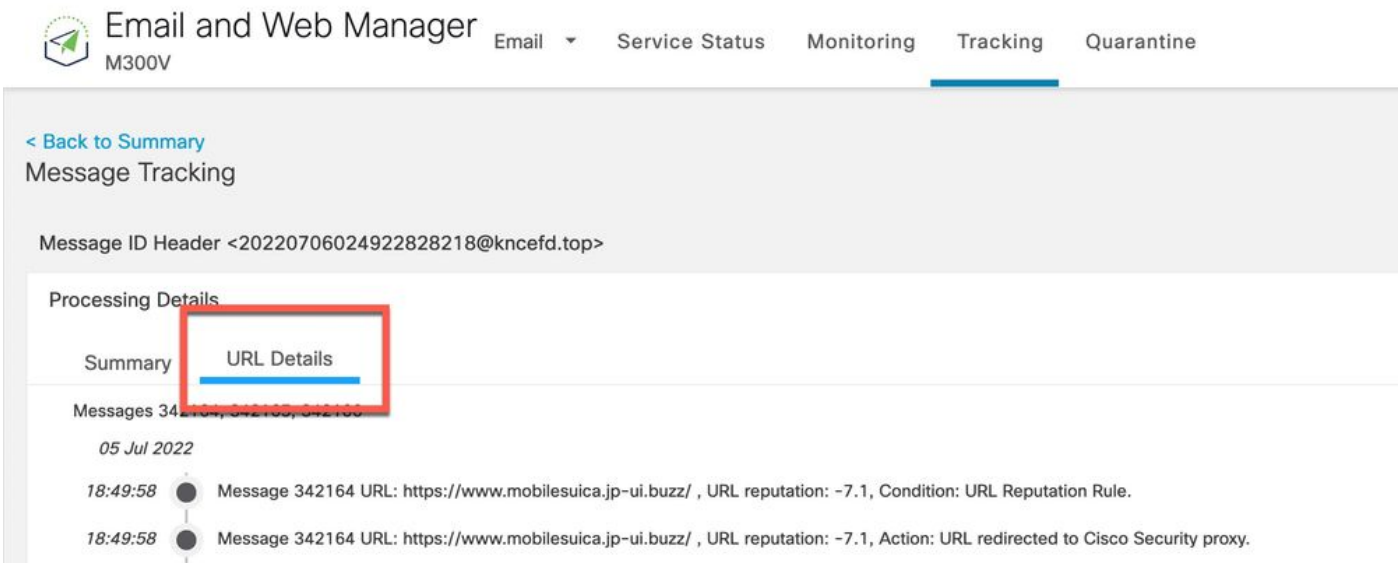
Actions

Add Action...

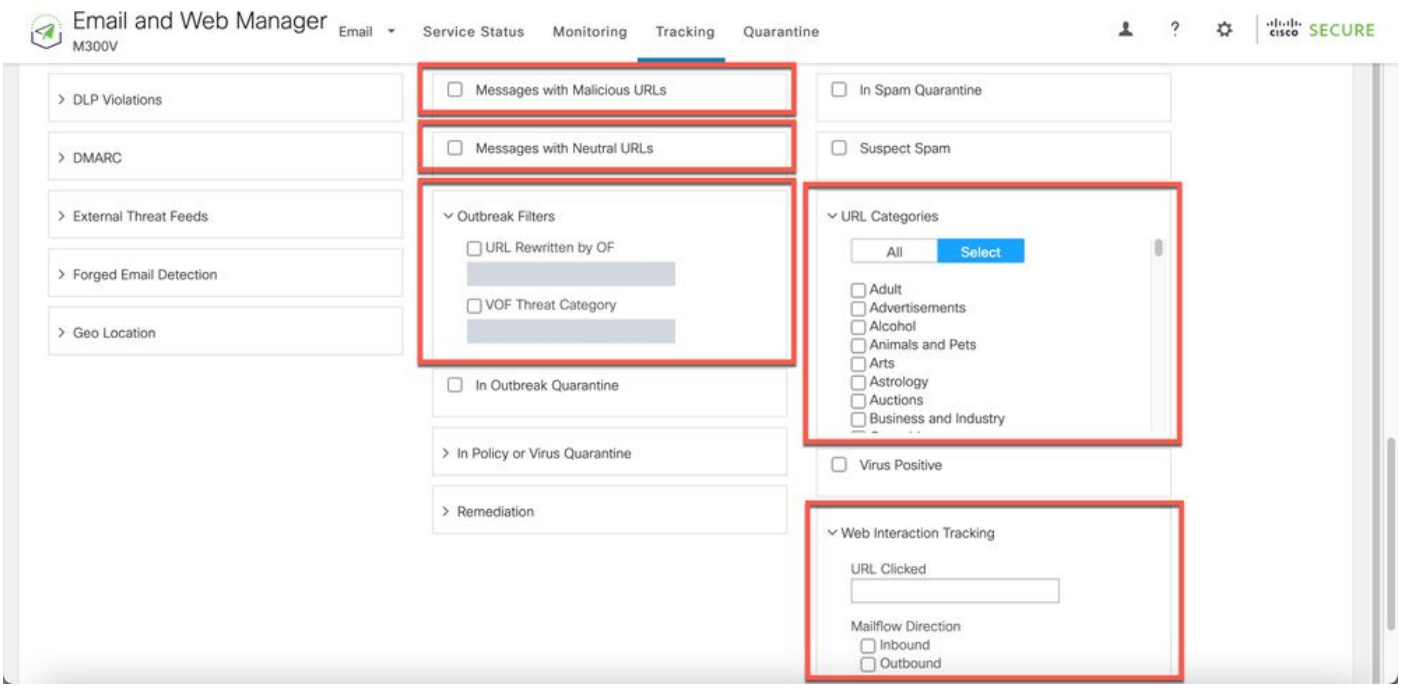
Order	Action	Rule	Delete
1	URL Reputation	url-reputation-proxy-redirect-strip(-3.00, -0.50,"",0)	

郵件跟蹤

檢視與MID關聯的URL的郵件跟蹤選項。 有時，URL不會記錄到mail_logs，您可以在「郵件跟蹤」詳細資訊中找到它們。舉例來說：



郵件跟蹤還為具有URL防禦和互動的郵件提供高級搜尋選項：



報告未分類和錯誤分類的URL

URL有時可以報告為沒有信譽或分類。還有一些URL分類錯誤。要報告這些URL發現，請訪問Talos信譽中心支援頁面上的Cisco Talos的Web分類請求。

在報告URL後，您可以檢視 我的票證 頁面。

反垃圾郵件或爆發過濾器不會捕獲惡意URL和行銷郵件

發生這種情況的原因是，站點信譽和類別只是反垃圾郵件和爆發過濾器用於確定其裁決的眾多標準中的兩個標準。要增加這些過濾器的敏感度，請降低採取操作所需的閾值，例如使用文本、隔離或丟棄郵件重寫或替換URL。

或者，您可以根據URL信譽得分建立內容或郵件過濾器。

附錄

為縮短的URL啟用URL過濾支援

注意：本節僅適用於AsyncOS 11.1到13.0的郵件安全。

僅可使用websecurityadvancedconfig命令通過CLI完成針對縮短型URL的URL過濾支援：

```
<#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
```

思科建議為URL過濾配置最佳實踐啟用此功能。啟用後，郵件日誌會反映郵件中使用縮短的URL的任何時間：

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

啟用URL過濾後，從mail_logs示例中，我們可以看到bit.ly連結已記錄，並且它展開到的原始連結也已記錄。

其他資訊

思科安全電子郵件閘道檔案

- 版本資訊
- 使用手冊
- CLI參考指南
- 思科安全電子郵件網關API程式設計指南
- 思科安全電子郵件網關中使用的開源
- 思科內容安全虛擬裝置安裝指南（包括vESA）

安全電子郵件雲網關文檔

- 版本資訊
- 使用手冊

Cisco Secure Email and Web Manager文檔

- 發行說明和相容表
- 使用手冊
- Cisco Secure Email and Web Manager的API程式設計指南
- 思科內容安全虛擬裝置安裝指南（包括vSMA）

思科安全產品檔案

- 思科安全產品組合命名架構

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。