

Configurazione del filtro URL per Secure Email Gateway e Cloud Gateway

Sommario

[Introduzione](#)

[Premesse](#)

[Prerequisiti](#)

[Abilitazione del filtro URL](#)

[Definizione delle azioni del filtro URL](#)

[URL non attendibili](#)

[URL sconosciuti](#)

[URL con domande](#)

[URL neutri](#)

[Verifica messaggi](#)

[Segnalazione di URL non classificati o classificati in modo erraneo](#)

[Mancato rilevamento di URL dannosi o di messaggi di marketing da parte dei filtri antispam ed epidemie](#)

[Appendice](#)

[Abilitazione del filtro URL per gli URL abbreviati](#)

[Ulteriori informazioni](#)

[Documentazione di Cisco Secure Email Gateway](#)

[Documentazione su Secure Email Cloud Gateway](#)

[Documentazione di Cisco Secure Email e Web Manager](#)

[Documentazione del prodotto Cisco Secure](#)

Introduzione

In questo documento viene descritto come configurare il filtro URL su Cisco Secure Email Gateway e Cloud Gateway e le best practice da adottare.


Premesse

Il filtro URL è stato introdotto per la prima volta con [AsyncOS 11.1 for Email Security](#). Questa versione ha consentito alla configurazione di Cisco Secure Email di analizzare gli URL negli allegati ed eseguire sui messaggi che li contengono le azioni appositamente configurate. I filtri messaggi e contenuti utilizzano la reputazione e la categoria dell'URL per verificare la presenza di URL nei messaggi e negli allegati. Per ulteriori informazioni, vedere i capitoli della [Guida per l'utente](#) o della guida online dedicati all'uso dei filtri messaggi per applicare policy di posta, ai filtri contenuti e alla protezione da URL non attendibili o indesiderati.


Il controllo e la protezione da link non attendibili o indesiderati sono integrati nella coda di lavoro

per i filtri antispam, epidemie, contenuti e messaggi. Le caratteristiche di questi controlli sono:

- Aumentare l'efficacia della protezione da URL non attendibili inclusi nei messaggi e negli allegati.
- Inoltre, il filtro URL è integrato nei filtri epidemie. Ciò permette di bloccare le minacce basate sul Web nel punto di ingresso, per questo è utile anche nelle configurazioni che prevedono già l'uso di una simile protezione, come Cisco Web Security Appliance o analogo prodotto.
- I filtri contenuti o messaggi possono essere usati per prendere decisioni in base al punteggio Web-Based Reputation Score (WBRS) assegnato agli URL inclusi nei messaggi. Ad esempio, è possibile riscrivere gli URL con reputazione neutra o sconosciuta per reindirizzarli al proxy Cisco Web Security che valuterà in tempo reale se sono sicuri.
- Migliorare l'individuazione delle e-mail indesiderate.
- Per individuare le e-mail indesiderate, l'appliance usa la reputazione e la categoria dei link inclusi nei messaggi e altri algoritmi di identificazione. Ad esempio, se un collegamento in un messaggio appartiene a un sito Web di marketing, è più probabile che il messaggio sia un messaggio di marketing.
- Supportare l'applicazione delle policy aziendali sull'utilizzo accettabile.
- La categoria degli URL (contenuti per adulti, attività illecite, ecc.) può essere usata insieme ai filtri contenuti e messaggi per rendere più efficaci le policy aziendali sull'utilizzo accettabile.
- Permettere di identificare all'interno dell'azienda gli utenti che selezionano più spesso gli URL riscritti per finalità di protezione e di individuare i link più visitati.

 Nota: nella versione [AsyncOS 11.1 for Email Security](#), il filtro URL ha introdotto il supporto per gli URL abbreviati. Con il comando CLI 'websecurityadvancedconfig', è possibile visualizzare e configurare i servizi abbreviati. Questa opzione di configurazione è stata aggiornata in [AsyncOS 13.5 for Email Security](#). Dopo aver eseguito l'aggiornamento a questa release, tutti gli URL abbreviati vengono espansi. Non è possibile disabilitare l'espansione degli URL abbreviati. Per questo motivo, Cisco consiglia AsyncOS 13.5 for Email Security o versioni successive per fornire le protezioni più recenti per la difesa degli URL. Fare riferimento al capitolo "Protecting Against Malicious or Indesiderable URLs" (Protezione da URL dannosi o indesiderati) della guida per l'utente o della guida online e alla Guida di riferimento della CLI per AsyncOS per Cisco Email Security Appliance.

 Nota: per questo documento, viene usato [AsyncOS 14.2 for Email Security](#) per gli esempi e gli screenshot forniti.

 Nota: Cisco Secure Email offre anche una [Guida](#) approfondita alla [difesa degli URL all'indirizzo docs.ces.cisco.com](#).

Prerequisiti

Quando si configura il filtro URL su Cisco Secure Email Gateway o Cloud Gateway, è necessario configurare anche altre funzionalità in base al risultato che si desidera ottenere. Di seguito sono

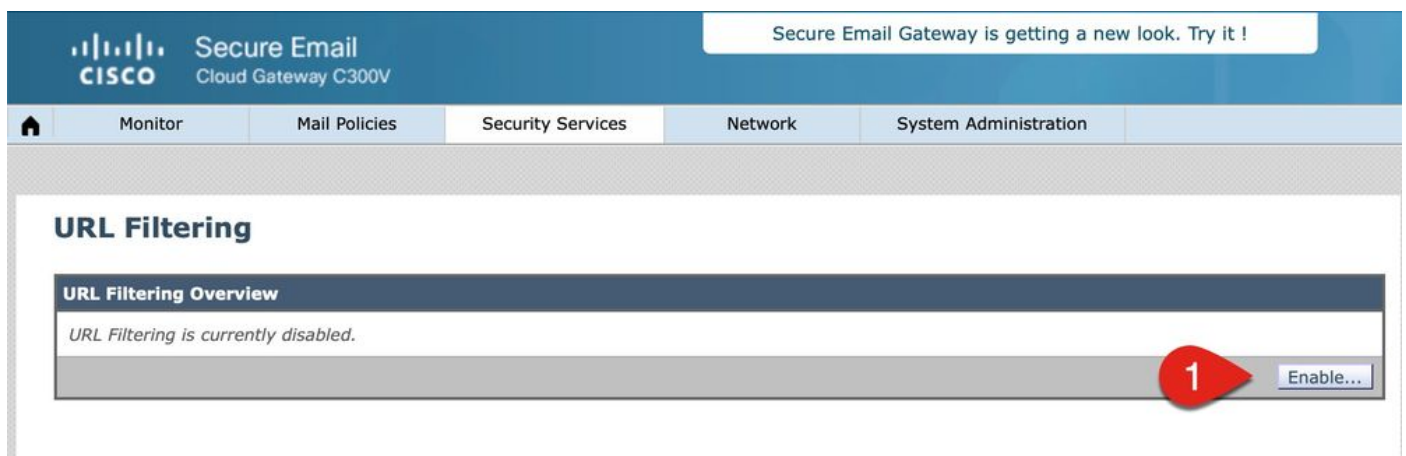
riportate alcune caratteristiche tipiche che vengono abilitate insieme al filtro URL:

- Per una protezione avanzata dalla posta indesiderata, è necessario abilitare la funzionalità di scansione della posta indesiderata a livello globale in base ai criteri di posta applicabili. La funzionalità Anti-Spam è considerata sia come Cisco IronPort Anti-Spam (IPAS) che come Cisco Intelligent Multi-Scan (IMS).
- Per una protezione avanzata dal malware, abilitare i filtri epidemie o i filtri epidemie di virus (VOF) a livello globale secondo la policy di posta applicabile.
- Per le azioni basate sulla reputazione dell'URL o per applicare le policy sull'utilizzo accettabile usando i filtri messaggi e contenuti, i filtri epidemie di virus (VOF) devono essere abilitati globalmente.

Abilitazione del filtro URL

È necessario prima abilitare la funzionalità per implementare il filtro URL su Cisco Secure Email Gateway o Cloud Gateway. Il filtro URL può essere abilitato dalla GUI o dalla CLI dall'amministratore.

Per abilitare il filtro URL, dalla GUI, selezionare Security Services > URL Filtering (Servizi di sicurezza > Filtro URL) e fare clic su Enable (Abilita):



Quindi, fare clic su Enable URL Category and Reputation Filters (Abilita filtri categorie URL e reputazione). In questo esempio vengono illustrati i valori delle procedure consigliate per Timeout ricerca URL, Numero massimo di URL analizzati e viene abilitata l'opzione per la registrazione degli URL:

Secure Email Gateway is getting a new look. Try it!

Secure Email
Cloud Gateway C300V

Monitor Mail Policies Security Services Network System Administration

URL Filtering

URL Filtering Overview

Enable URL Category and Reputation Filters


Use a URL allowed list:

Web Interaction Tracking: Enable Web Interaction Tracking

Advanced Settings:

| | |
|---|--|
| URL Lookup Timeout | <input type="text" value="5"/> |
| Maximum Number of URLs scanned in Message Body | <input type="text" value="400"/> |
| Maximum Number of URLs scanned in Message Attachments | <input type="text" value="400"/> |
| Rewrite URL text and HREF in Message | <input type="radio"/> Yes Select the 'Yes' option to display the rewritten URL in the message body. <input checked="" type="radio"/> No Select the 'No' option to display the rewritten URL in the HREF part of the HTML message. |
| URL Logging | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |

Cancel Submit


 Nota: accertarsi di eseguire il commit delle modifiche apportate alla configurazione in questo momento.

Definizione delle azioni del filtro URL

L'abilitazione del solo filtro URL non comporta alcuna azione sugli URL inclusi nei messaggi o nei messaggi con allegati.

Vengono valutati gli URL inclusi nei messaggi e negli allegati per i criteri di posta in arrivo e in uscita. Qualsiasi altra stringa valida viene analizzata per includere le stringhe con queste caratteristiche:

- HTTP, HTTPS o WWW
- Indirizzo di dominio o IP
- Numeri di porta preceduti da due punti (:)
- Lettere maiuscole o minuscole

 Nota: per la maggior parte degli URL, la voce del log URL è visibile da mail_logs. Se l'URL non è registrato in mail_logs, controllare Verifica messaggi per l'ID messaggio (MID). Verifica messaggi non include una scheda per Dettagli URL.

Quando il sistema analizza gli URL per stabilire se il messaggio è indesiderato, se lo ritiene necessario per la gestione dei carichi, assegna la priorità ai messaggi in arrivo e li analizza prima dei messaggi in uscita.

È possibile decidere le azioni da eseguire sui messaggi in base alla reputazione dell'URL o alla categoria dell'URL nel corpo del messaggio o sui messaggi con allegati.

Ad esempio, per scartare tutti i messaggi che includono URL con contenuti per adulti, aggiungere una condizione URL Category (Categoria URL) e selezionare la categoria Adult (Per adulti).

Se non si specifica una categoria, l'azione scelta viene applicata a tutti i messaggi.

L'intervallo dei punteggi che permettono di classificare gli URL in Attendibile, Preferibile, Neutro, Interrogabile e Non attendibile è predefinito e non modificabile. È possibile specificare un intervallo personalizzato. Utilizzare "Unknown" (Sconosciuto) nei casi in cui non sia ancora stato determinato un punteggio.

Per analizzare rapidamente gli URL e decidere le azioni da eseguire, è possibile creare un filtro contenuti in modo che se il messaggio ha un URL valido, allora l'azione viene applicata. Dalla GUI, selezionare Mail Policies > Incoming Content Filters > Add Filter (Policy di posta > Filtri contenuti in arrivo > Aggiungi filtro).

Le azioni associate agli URL sono le seguenti:

- URL di disinnesto
 - L'URL viene modificato per renderlo non selezionabile, ma il destinatario del messaggio può comunque leggere l'URL desiderato (caratteri aggiuntivi vengono inseriti nell'URL originale).
- Reindirizza a Cisco Security Proxy
 - L'URL viene riscritto quando si fa clic su di esso per passare attraverso il proxy di sicurezza Cisco e procedere a un'ulteriore verifica. In base al verdetto del proxy di sicurezza di Cisco, il sito potrebbe non essere accessibile per l'utente.
- Sostituisci URL con un SMS
 - Con questa opzione, un amministratore può riscrivere l'URL all'interno del messaggio e inviarlo esternamente per l'isolamento del browser remoto.

URL non attendibili

Non attendibile: comportamento URL eccezionalmente dannoso, dannoso o indesiderato. Si tratta della soglia più sicura consigliata per gli elenchi di blocco. Tuttavia, potrebbero esserci messaggi non bloccati perché gli URL contengono un livello di minaccia più basso. Assegna priorità alla distribuzione rispetto alla sicurezza.

Azione consigliata: blocco. Un amministratore può mettere in quarantena o eliminare completamente il messaggio.

In questo esempio viene illustrato il contesto per un filtro contenuti per il rilevamento di URL non attendibili:

| 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") | |

Con il filtro dei contenuti applicato, Cisco Secure Email cerca gli URL la cui reputazione è Untrusted (punteggio compreso tra -10,00 e -6,00) e mette il messaggio in quarantena, URL_UNTRUSTED. Di seguito è riportato un esempio dai log_di_posta:

<#root>

```
Tue Jul 5 15:01:25 2022 Info: ICID 5 ACCEPT SG MY_TRUSTED_HOSTS match 127.0.0.1 SBRS None country United States
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.com
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/A
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-127-0-0-1.internal
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/A
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Tracker Header : 62c45245_jTikQ21V2NYfmrGzMwQMBd68fxqFFueNmElw
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 inbound
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
```

L'URL [ihaveabadreputation.com](https://www.ihaveabadreputation.com) è considerato NON ATTENDIBILE e valutato con un punteggio pari a -9,5. Il filtro URL ha rilevato l'URL non attendibile e lo ha messo in quarantena in URL_UNTRUSTED.

Nell'esempio precedente di mail_logs viene illustrato un esempio in cui SOLO il filtro contenuti per il filtro URL è abilitato per il criterio di posta in arrivo. Se nello stesso criterio di posta sono abilitati servizi aggiuntivi, ad esempio la protezione dalla posta indesiderata, gli altri servizi indicano se l'URL è stato rilevato da tali servizi e dalle relative regole. Nello stesso esempio di URL, Cisco Anti-Spam Engine (CASE) è abilitato per i criteri della posta in arrivo e il corpo del messaggio viene analizzato e valutato come posta indesiderata. Questo è indicato per primo nei log di posta poiché Anti-Spam è il primo servizio nella pipeline di elaborazione della posta. I filtri contenuti vengono forniti più avanti nella pipeline di elaborazione della posta:

<#root>

```
Tue Jul 5 15:19:48 2022 Info: ICID 6 ACCEPT SG MY_TRUSTED_HOSTS match 127.0.0.1 SBRS None country United States
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-127-0-0-1
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/A
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-127-0-0-1
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/A
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 inbound
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 matches
Tue Jul 5 15:19:49 2022 Info: MID 4 quarantined to "URL_UNTRUSTED" (content filter:URL_QUARANTINE_UNTRUSTED)
Tue Jul 5 15:19:49 2022 Info: Message finished MID 4 done
```

In alcuni casi, le regole CASE e IPAS contengono regole, reputazione o punteggi che corrispondono a un mittente, un dominio o un messaggio specifico per rilevare da sole le minacce URL. Nell'esempio, è stato rilevato [ihaveabadreputation.com](https://www.ihaveabadreputation.com), contrassegnato per la quarantena della posta indesiderata (ISQ) e la quarantena URL_UNTRUSTED dal filtro del contenuto URL_QUARANTINE_UNTRUSTED. Il messaggio viene prima messo in quarantena URL_UNTRUSTED. Quando il messaggio viene rilasciato dalla quarantena da un amministratore o il limite di tempo/i criteri di configurazione della quarantena URL_UNTRUSTED sono stati

soddisfatti, il messaggio viene successivamente spostato nell'ISQ.

In base alle preferenze dell'amministratore, è possibile configurare condizioni e azioni aggiuntive per il filtro dei contenuti.


URL sconosciuti


Sconosciuto: non è stato valutato in precedenza o non visualizza funzionalità per l'asserzione di un verdetto a livello di minaccia. Dati insufficienti per stabilire la reputazione del servizio URL. Questo verdetto non è adatto per azioni dirette in una policy sulla reputazione dell'URL.


Azione consigliata: eseguire la scansione con i motori successivi per verificare la presenza di altri contenuti potenzialmente dannosi.

Per URL sconosciuti o "senza reputazione" si intendono gli URL contenenti nuovi domini o URL che non sono frequentati spesso e che non possono essere valutati per la reputazione o il livello di minaccia. Questi possono diventare Non attendibili man mano che si ottengono ulteriori informazioni sul loro dominio e la loro origine. Per questo tipo di URL, Cisco consiglia di utilizzare un filtro contenuti per la registrazione o uno che includa il rilevamento dell'URL sconosciuto. A partire dalla versione AsyncOS 14.2, gli URL sconosciuti vengono inviati al Talos Intelligence Cloud Service per un'analisi approfondita degli URL attivata su diversi indicatori di minaccia. Inoltre, una voce registrata nel log di posta degli URL sconosciuti fornisce all'amministratore un'indicazione degli URL inclusi in un MID e un possibile rimedio con la protezione degli URL. Per ulteriori informazioni, vedere [Come configurare le impostazioni dell'account di posta elettronica sicuro Cisco per l'API Microsoft Azure \(Microsoft 365\)](#).

In questo esempio viene illustrato il contesto di un filtro contenuti per il rilevamento di URL sconosciuti:

| Content Filter Settings | |
|-----------------------------|--|
| Name: | URL_UNKNOWN |
| Currently Used by Policies: | Default Policy |
| Description: | Log messages with Unknown URLs. (Includes messages with attachments.) |
| Order: | 2  (of 2) |

| Conditions | | | |
|----------------------------------|----------------|-----------------------------|---|
| Add Condition... | | | |
| Order | Condition | Rule | Delete |
| 1 | URL Reputation | url-no-reputation("", 1, 1) |  |

| Actions | | | |
|-------------------------------|---------------|--|---|
| Add Action... | | | |
| Order | Action | Rule | Delete |
| 1 | Add Log Entry | log-entry("<<<=== LOGGING UNKNOWN URL FOR MAIL_LOGS ===>>>") |  |

Con il filtro dei contenuti applicato, Cisco Secure Email cerca gli URL la cui reputazione è Sconosciuta e scrive una riga di log nei mail_logs. Di seguito è riportato un esempio dai log_di_posta:

<#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
```

L'URL mytest.example.com/test_url_2022070503 non ha alcuna reputazione e viene visualizzato con "noscore" (nessun punteggio). Il filtro del contenuto URL_UNKNOWN ha scritto la riga di registro come configurata in mail_logs.

Dopo un ciclo di polling da Cisco Secure Email Gateway al servizio cloud Talos Intelligence, l'URL viene analizzato e valutato come non attendibile. Questa condizione può essere rilevata nei log ECS al livello "Traccia":

```

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':
'8c6915e2ebbc9225ff8958db06db33beb4e932ae9e0d8c5b35805a2fxyxyxyy', 'message_details': '{"mid": 16,
"birth_time": "1657039913", "from_addrs": ["test@test.com"], "recipients": ["██████████"],
"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":
    "8c6915e2ebbc9225ff8958db06db33beb4e932ae9e0d8c5b35805a2fxyxyxyy"}]",
    [
      "██████████"
    ],
    [
      "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.

```

E successivamente, nei log_di_posta, quando il rimedio stesso viene chiamato e completato:

```

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

```

Gli amministratori devono valutare l'opportunità di intraprendere un'azione per gli URL sconosciuti a loro discrezione. In caso si dovesse notare un aumento di e-mail o allegati di phishing, riesaminare il report mail_logs and Content Filters. Inoltre, gli amministratori possono configurare il reindirizzamento degli URL sconosciuti al servizio proxy Cisco Security che li valuterà in tempo reale. Nell'esempio, passare a Add Action > URL Reputation (Aggiungi azione > Reputazione URL) all'interno del filtro contenuti URL_UNKNOWN:

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 (WBR) 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:  

Check URLs within


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

Action on URL within the message body and subject:

 . L'opzione di rimuovere gli allegati per alcuni amministratori non è preferibile. Esaminare l'azione e considerare solo l'opzione per la configurazione del corpo e dell'oggetto del messaggio.


Il filtro dei contenuti aggiornato è ora simile a questo esempio, con l'aggiunta dell'azione Reindirizza a Cisco Secure Proxy:

Content Filter Settings

| | |
|-----------------------------|--|
| Name: | URL_UNKNOWN |
| Currently Used by Policies: | Default Policy |
| Description: | Log messages with Unknown URLs. (Includes messages with attachments.) |
| Order: | 2  (of 3) |




Conditions

[Add Condition...](#)

| Order | Condition | Rule | Delete |
|-------|----------------|-----------------------------|---|
| 1 | URL Reputation | url-no-reputation("", 1, 1) |  |

Actions

[Add Action...](#)

| Order | Action | Rule | Delete |
|-------|--|--|---|
| 1 | Add Log Entry | log-entry("<<=== LOGGING UNKNOWN URL FOR MAIL_LOGS ===>>") |  |
| 2 |  URL Reputation | url-no-reputation-proxy-redirect-strip("",0) |  |


URL con domande


Aspetto discutibile: comportamento dell'URL che può indicare rischi o essere indesiderato.


Sebbene non sia sicuro per tutte le organizzazioni, questo verdetto ha un tasso di falsi positivi (FP) basso e relativamente sicuro. Un verdetto non bloccato assegna la priorità al recapito rispetto alla sicurezza, il che può comportare messaggi che contengono URL rischiosi.

Azione consigliata: eseguire la scansione con i motori successivi e bloccare dopo la revisione.

Come è stato configurato in URL sconosciuti, per gli amministratori può essere utile inviare URL dubbi al proxy di sicurezza Cisco o utilizzare l'azione per disinnescare completamente gli URL.

| 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) |  |


URL neutri


Neutro: URL senza comportamento positivo o negativo. Tuttavia, è stato valutato. In altre parole, l'URL non presenta rischi noti. Quindi, questo è il grosso dei verdetti sulla reputazione.

Azione consigliata: eseguire la scansione con i motori successivi per verificare la presenza di altri contenuti potenzialmente dannosi.

Gli amministratori possono considerare un URL neutro con un punteggio negativo come una minaccia. Valutare a propria discrezione il numero di messaggi e le occorrenze degli URL neutri. Analogamente, la procedura di aggiornamento degli URL sconosciuti e degli URL con domande consente di usare l'azione di invio degli URL al proxy di sicurezza Cisco, è possibile prendere in considerazione gli URL neutri o un intervallo personalizzato che includa un sottoinsieme del lato negativo di Neutral. L'esempio mostra come viene eseguita una ricerca di URL neutri con il seguente filtro dei contenuti in arrivo:

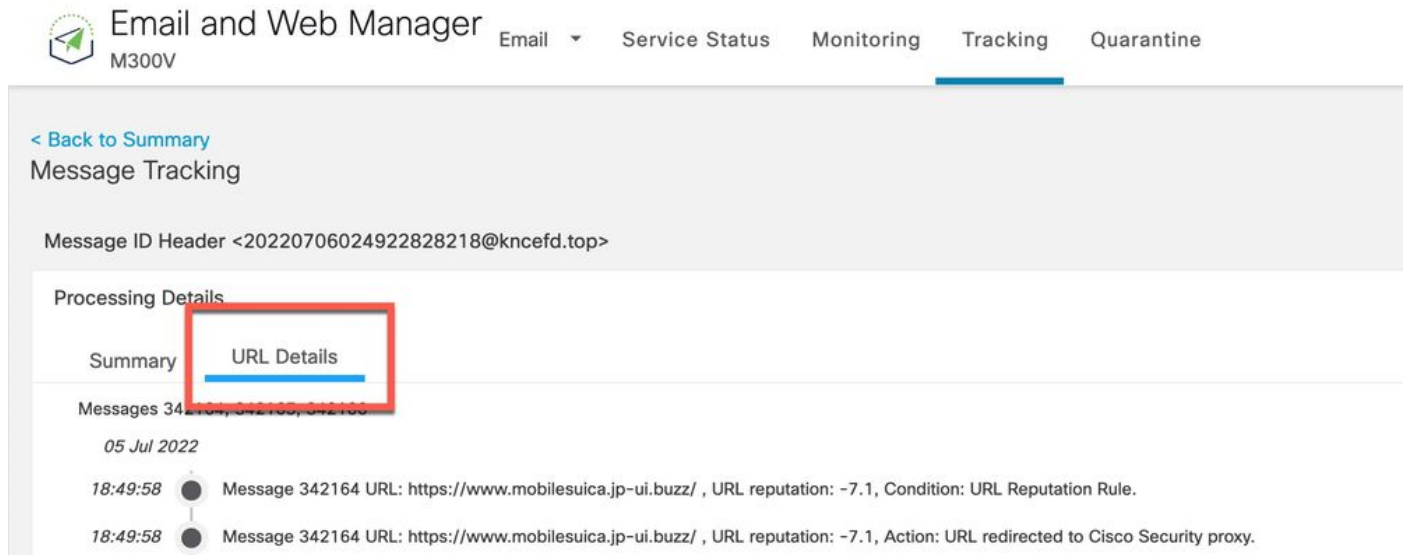
| Content Filter Settings | |
|-----------------------------|---|
| Name: | URL_NEUTRAL |
| Currently Used by Policies: | No policies currently use this rule. |
| Description: | Send questionable Neutral URLs to be scanned again at click time. (Includes messages with attachments.) |
| Order: | 4  (of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

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

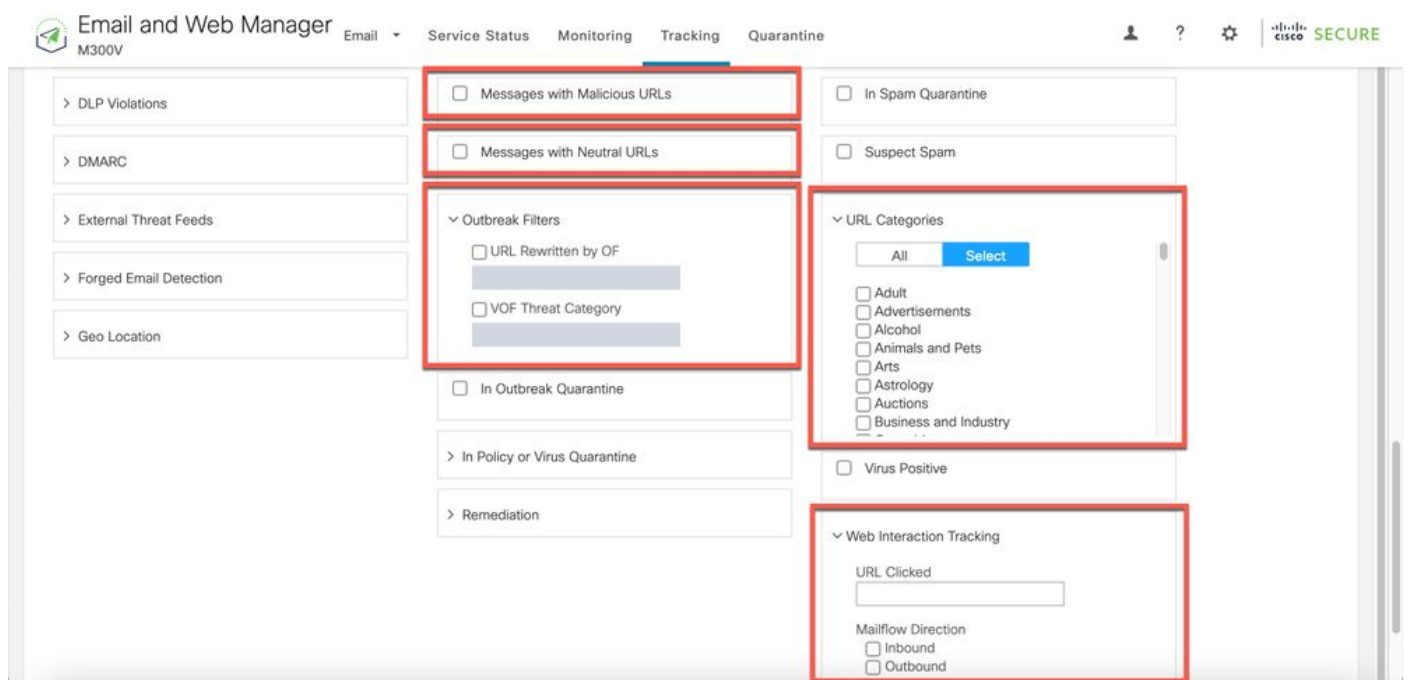
| Actions | | | |
|-------------------------------|----------------|--|---|
| Add Action... | | | |
| Order | Action | Rule | Delete |
| 1 | URL Reputation | url-reputation-proxy-redirect-strip(-3.00, -0.50,"",0) |  |

Verifica messaggi

Esaminare le opzioni di verifica messaggi per gli URL associati con MID. A volte gli URL non vengono registrati nei log di posta ed è possibile individuarli nei dettagli di verifica messaggi. Ad esempio:



La funzione di verifica dei messaggi fornisce anche opzioni di ricerca avanzata per i messaggi con difesa e interazione degli URL:



Segnalazione di URL non classificati o classificati in modo

erroneo

In alcuni casi l'URL può indicare che non si ha reputazione o classificazione. Sono inoltre presenti URL classificati in modo erroneo. Per segnalare gli URL rilevati, visitare la pagina di [supporto](#) del [Talos](#) dedicata alle richieste di classificazione Web [nella stessa](#) pagina.

Dopo aver segnalato un URL, è possibile visualizzarne lo stato sul [Biglietti](#) pagina.

Mancato rilevamento di URL dannosi o di messaggi di marketing da parte dei filtri antispam ed epidemie

Questa situazione può verificarsi perché la reputazione e la categoria di un sito sono solo due dei numerosi criteri usati dai filtri antispam ed epidemie per emettere un verdetto. Per aumentare la sensibilità di questi filtri, abbassare le soglie necessarie per l'esecuzione di un'azione, ad esempio riscrivere o sostituire gli URL con testo, mettere in quarantena o eliminare messaggi.

In alternativa, è possibile creare filtri contenuti o messaggi basati sul punteggio di reputazione dell'URL.

Appendice

Abilitazione del filtro URL per gli URL abbreviati

 Nota: questa sezione si applica solo ad AsyncOS versione 11.1 e 13.0 for Email Security.

Il supporto di URL abbreviati da parte del filtro URL può essere eseguito solo dalla CLI con il comando `websecurityadvancedconfig`:

```
<#root>
```

```
myesa.local>
```

```
websecurityadvancedconfig
```

```
...
```

```
Do you want to enable URL filtering for shortened URLs? [N]>
```

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, t1.gd, plurk.com, url4.eu, j.mp, goo.gl, yfrog

Cisco consiglia di abilitare questa funzionalità per una configurazione ottimale del filtro URL. Dopo aver abilitato la funzione, ogni volta che si rileva un URL abbreviato in un messaggio, sui log di posta viene registrata un'apposita voce:

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

Se il filtro URL è stato abilitato come descritto in questo articolo, come si osserva nel log di esempio mail_logs, nel log vengono registrati il link bit.ly E il link originale nel formato esteso.

• Ulteriori informazioni

Documentazione di Cisco Secure Email Gateway

- [Note sulla release](#)
- [Guida dell'utente](#)
- [Guida di riferimento CLI](#)
- [Guide alla programmazione API per Cisco Secure Email Gateway](#)
- [Open Source utilizzato in Cisco Secure Email Gateway](#)
- [Guida all'installazione di Cisco Content Security Virtual Appliance](#) (include vESA)

Documentazione su Secure Email Cloud Gateway

- [Note sulla release](#)
- [Guida dell'utente](#)

Documentazione di Cisco Secure Email e Web Manager

- [Note sulla versione e matrice di compatibilità](#)
- [Guida dell'utente](#)
- [Guide alla programmazione API per Cisco Secure Email e Web Manager](#)
- [Guida all'installazione di Cisco Content Security Virtual Appliance](#) (include vSMA)

Documentazione del prodotto Cisco Secure

- [Architettura di denominazione del portafoglio Cisco Secure](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).