Configurar a filtragem de URL para Secure Email Gateway e Cloud Gateway

Contents

Introdução

Este documento descreve como configurar a filtragem de URL no Cisco Secure Email Gateway e no Cloud Gateway e as práticas recomendadas para uso da filtragem de URL.

Informações de Apoio

A filtragem de URL foi introduzida pela primeira vez com o AsyncOS 11.1 para segurança de e-mail. Esta versão permitiu que a configuração do Cisco Secure Email verificasse URLs em anexos de mensagem e executasse ações configuradas nessas mensagens. Os filtros de mensagens e conteúdo usam a reputação de URL e a categoria de URL para verificar URLs em mensagens e anexos. Para obter mais detalhes, consulte os capítulos "Usando filtros de mensagens para aplicar políticas de e-mail", "Filtros de conteúdo" e "Protegendo contra URLs indesejáveis ou não confiáveis" no Guia do usuário ou na ajuda on-line.

O controle e a proteção contra links não confiáveis ou indesejáveis são incorporados na fila de

trabalho para processos de filtragem de mensagens, antispam, detecção e conteúdo. Esses controles:

- Aumentar a eficácia da proteção contra URLs não confiáveis em mensagens e anexos.
- Além disso, a filtragem de URL é incorporada nos filtros de detecção. Essa proteção reforçada é aplicável mesmo se a sua empresa já tiver um Cisco Web Security Appliance ou uma proteção semelhante contra ameaças baseadas na Web, pois bloqueia ameaças no ponto de entrada.
- Você também pode usar filtros de conteúdo ou de mensagens para tomar providências com base na escala de reputação baseada na Web (WBRS) dos URLs nas mensagens. Por exemplo, você pode reescrever os URLs com reputação neutra ou desconhecida para redirecioná-los ao proxy de segurança da Web da Cisco para avaliação de tempo de clique da segurança.
- Identificar melhor o spam
- O equipamento usa a reputação e a categoria de links em mensagens e outros algoritmos de identificação de spam para ajudar a identificar o spam. Por exemplo, se um link em uma mensagem pertencer a um site de marketing, a mensagem terá mais probabilidade de ser uma mensagem de marketing.
- Apoiar a aplicação de políticas corporativas de uso aceitável
- A categoria de URLs (conteúdo para adultos ou atividades ilegais, por exemplo) pode ser usada com filtros de conteúdo e mensagens para aplicar políticas de uso corporativo aceitáveis.
- Permitem identificar os usuários em sua organização que clicaram com mais frequência em uma URL em uma mensagem que foi reescrita para proteção e os links que foram clicados com mais frequência.

Observação: na versão do AsyncOS 11.1 for Email Security, a filtragem de URL introduziu suporte para URLs abreviados. Com o comando CLI websecurityadvancedconfig, os serviços mais curtos podem ser vistos e configurados. Esta opção de configuração foi atualizada no AsyncOS 13.5 para segurança de e-mail. Depois de atualizar para esta versão, todos os URLs abreviados são expandidos. Não há opção para desativar a expansão de URLs abreviados. Por esse motivo, a Cisco recomenda o AsyncOS 13.5 para segurança de e-mail ou versão mais recente para fornecer as proteções mais recentes para defesa de URL. Consulte o capítulo "Proteção contra URLs mal-intencionados ou indesejáveis" no guia do usuário ou na ajuda on-line e no Guia de Referência CLI para AsyncOS para Cisco Email Security Appliance.

Observação: para este documento, o AsyncOS 14.2 for Email Security é usado para os exemplos e capturas de tela fornecidos.

Observação: o Cisco Secure Email também fornece um Guia de defesa de URLs em docs.ces.cisco.com.

Pré-requisitos

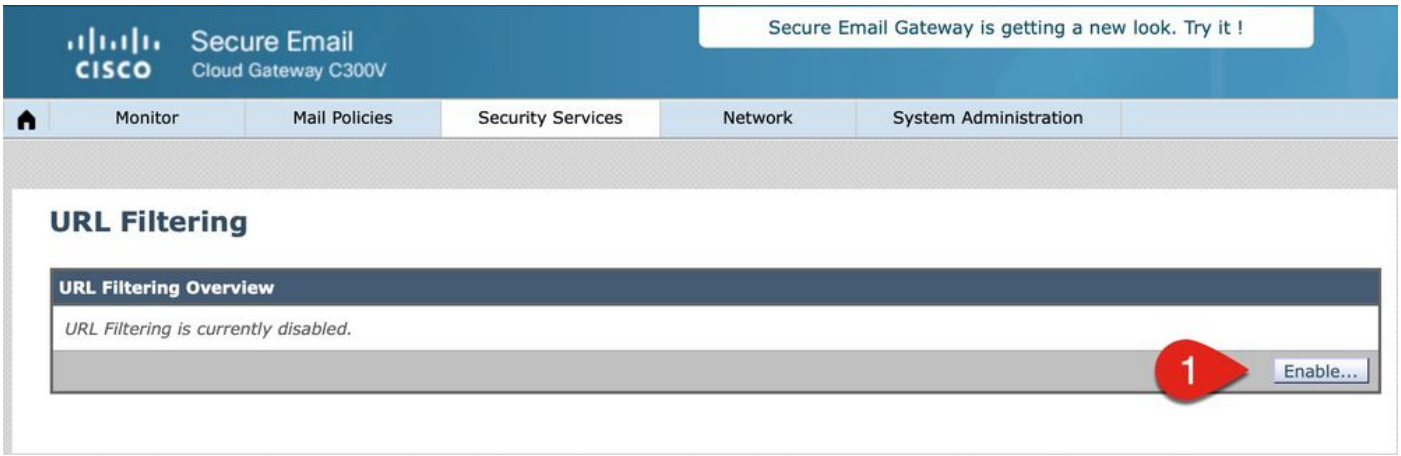
Ao configurar a filtragem de URL no Cisco Secure Email Gateway ou no Cloud Gateway, você também deve configurar outros recursos que dependem da funcionalidade desejada. Estes são alguns recursos típicos que são ativados juntamente com a filtragem de URL:

- Para maior proteção contra spam, o recurso de varredura antisspam deve ser ativado globalmente de acordo com a política de e-mail aplicável. O Anti-Spam é considerado o Cisco IronPort Anti-Spam (IPAS) ou o recurso Cisco Intelligent Multi-Scan (IMS).
- Para maior proteção contra malware, o recurso de filtros de detecção ou filtros de detecção de vírus (VOF) deve ser habilitado globalmente de acordo com a política de e-mail aplicável.
- Para ações baseadas na Reputação de URL ou para aplicar políticas de uso aceitável com o uso de filtros de mensagem e conteúdo, o VOF deve ser habilitado globalmente.

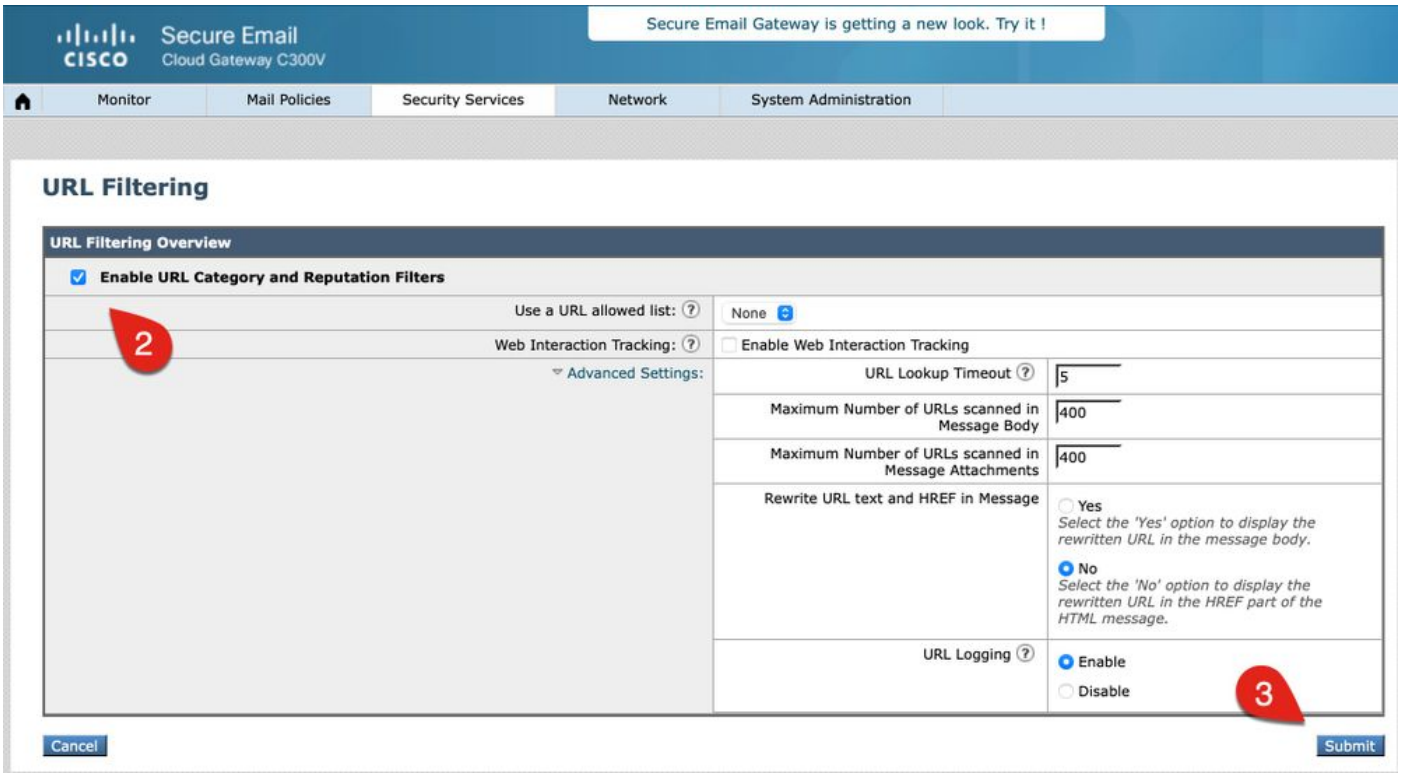
Ativar filtragem de URL

Primeiro você deve habilitar o recurso para implementar a filtragem de URL no Cisco Secure Email Gateway ou no Cloud Gateway. A filtragem de URL pode ser ativada a partir da GUI ou da CLI pelo administrador.

Para habilitar a filtragem de URL, na GUI, navegue para Serviços de segurança > Filtragem de URL e clique em Habilitar:



Em seguida, clique em Habilitar categoria de URL e filtros de reputação. Este exemplo inclui valores de práticas recomendadas para Tempo Limite de Pesquisa de URL, Número Máximo de URLs verificados e permite a opção de registrar URL(s):



Observação: certifique-se de confirmar suas alterações na configuração neste momento.

Criar ações de filtragem de URL

Quando você habilita a Filtragem de URL sozinha, ela não age contra URLs em mensagens ou mensagens com anexos.

Os URLs incluídos em mensagens e anexos para políticas de e-mail de entrada e saída são avaliados. Qualquer string válida para uma URL é avaliada para incluir strings com estes componentes:

- HTTP, HTTPS ou WWW
- Endereços IP ou de domínio
- Números de porta precedidos por dois-pontos (:)
- Letras maiúsculas ou minúsculas

Observação: a entrada do log de URL é visível em mail_logs para a maioria dos URLs. Se o URL não estiver registrado em mail_logs, revise o Rastreamento de mensagem para o ID da mensagem (MID). O Rastreamento de mensagens inclui uma guia para "Detalhes do URL".

Quando o sistema avalia URLs para determinar se uma mensagem é um spam, se necessário para o gerenciamento de carga, ele prioriza e filtra as mensagens de entrada em relação às mensagens de saída.

Você pode executar ações nas mensagens com base na reputação da URL ou na categoria da URL no corpo da mensagem ou nas mensagens com anexos.

Por exemplo, se você quiser aplicar a ação Ignorar (ação final) a todas as mensagens que incluem URLs da categoria Adulto, adicione uma condição de tipo Categoria de URL à categoria Adulto selecionada.

Se não for possível especificar uma categoria, a ação escolhida será aplicada a todas as mensagens.

A faixa de pontuação de reputação da URL para Confiável, Favorável, Neutro, Questionável e Não Confiável é predefinida e não editável. Você pode especificar um Intervalo personalizado. Use "Desconhecido" para URLs para os quais uma pontuação de reputação ainda precisa ser determinada.

Para verificar rapidamente URLs e tomar uma ação, você pode criar um filtro de conteúdo para que se a mensagem tiver um URL válido, então a ação seja aplicada. Na GUI, navegue para Políticas de e-mail > Filtros de conteúdo de entrada > Adicionar filtro.

As ações associadas a URLs são as seguintes:

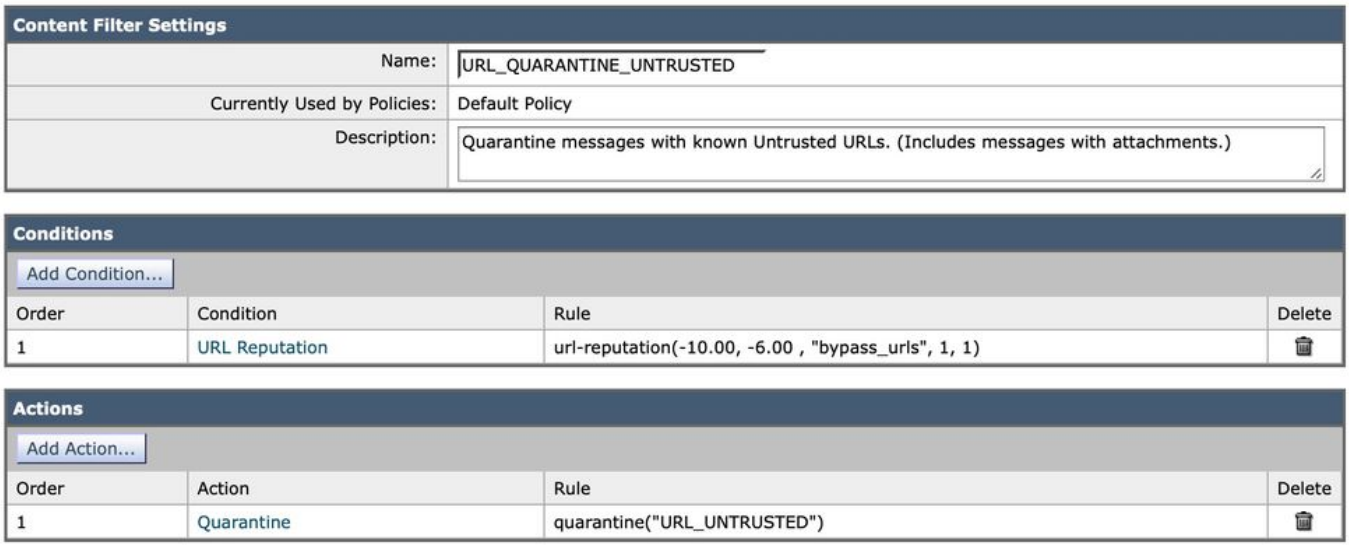
- Desativar URL
  - O URL é modificado para torná-lo inclicável, mas o destinatário da mensagem ainda pode ler o URL pretendido. (Caracteres extras são inseridos no URL original.)
- Redirecionar para o Cisco Security Proxy
  - O URL é regravado quando clicado para passar pelo Cisco Security Proxy para verificação adicional. Com base no veredito do Cisco Security Proxy, o site pode estar inacessível para o usuário.
- Substituir URL por uma mensagem de texto
  - Com essa opção, um administrador pode reescrever a URL na mensagem e enviá-la externamente para o Isolamento de navegador remoto.

URL(s) não confiável(is)

Não confiável: comportamento de URL excepcionalmente ruim, mal-intencionado ou indesejável. Esse é o limite de lista de bloqueio recomendado mais seguro; no entanto, pode haver mensagens que não são bloqueadas porque os URLs têm um nível de ameaça mais baixo. Prioriza a entrega em detrimento da segurança.

Ação recomendada: bloquear. (Um administrador pode colocar a mensagem totalmente em quarentena ou removê-la.)

Este exemplo fornece contexto para um filtro de conteúdo para Filtragem de URLs para detectar URLs Não Confiáveis:



Com esse filtro de conteúdo em vigor, o Cisco Secure Email verifica um URL com uma reputação Não confiável (-10.00 a -6.00) e coloca a mensagem em quarentena, URL_UNTRUSTED. Aqui está um exemplo dos mail_logs:

<#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
```

A URL ihaveabadreputation.com é considerada NÃO CONFIÁVEL e pontuada em -9,5. A filtragem de URL detectou o URL não confiável e o colocou em quarentena em URL_UNTRUSTED.

O exemplo anterior de mail_logs fornece um exemplo se SOMENTE o filtro de conteúdo para Filtragem de URL estiver ativado para a política de e-mail de entrada. Se a mesma política de e-mail tiver serviços adicionais ativados, como o Anti-Spam, os outros serviços indicarão se a URL foi detectada nesses serviços e em suas regras. No mesmo exemplo de URL, o Cisco Anti-Spam Engine (CASE) é ativado para a política de e-mail de entrada, e o corpo da mensagem é verificado e determinado como spam positivo. Isso é indicado primeiro em mail_logs, já que o Anti-Spam é o primeiro serviço no pipeline de processamento de e-mail. Os filtros de conteúdo são fornecidos mais tarde no pipeline de processamento de email:

<#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/XTLGFKD6OhwNKKsghUKA
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
```

Às vezes, as regras CASE e IPAS contêm regras, reputação ou pontuações que correspondem a um remetente, domínio ou conteúdo de mensagem específico para detectar ameaças de URL isoladamente. Neste exemplo, ihaveabadreputation.com foi visto, marcado para a Quarentena de spam (EUQ) e a quarentena URL_UNTRUSTED pelo filtro de conteúdo URL_QUARANTINE_UNTRUSTED. A mensagem entra primeiro na quarentena URL_UNTRUSTED. Quando a mensagem é liberada dessa quarentena por um administrador ou os critérios de limite/configuração de tempo da quarentena URL_UNTRUSTED foram atendidos, a

mensagem é movida para EUQ.

Com base nas preferências do administrador, condições e ações adicionais podem ser configuradas para o filtro de conteúdo.

URL(s) desconhecida(s)

Desconhecido: Não avaliado anteriormente ou não exibe recursos para afirmar um veredito de nível de ameaça. O serviço de reputação de URL não tem dados suficientes para estabelecer uma reputação. Este veredito não é adequado para ações diretamente em uma política de Reputação de URL.

Ação recomendada: verifique com os mecanismos subsequentes se há outros conteúdos potencialmente mal-intencionados.

URL(s) desconhecidos ou "sem reputação" podem ser URLs que contêm novos domínios ou URL(s) que tiveram pouco ou nenhum tráfego e não podem ter uma reputação avaliada e um veredito de nível de ameaça. Eles podem se tornar Não Confiáveis à medida que mais informações são obtidas para seu domínio e origem. Para esses URLs, a Cisco recomenda um filtro de conteúdo para registrar ou um que inclua a detecção do URL desconhecido. A partir do AsyncOS 14.2, URL(s) desconhecida(s) é(são) enviada(s) ao Talos Intelligence Cloud Service para análise detalhada de URL acionada em vários indicadores de ameaça. Além disso, uma entrada de log de e-mail do(s) URL(s) desconhecido(s) fornece ao administrador uma indicação do(s) URL(s) incluído(s) em um MID e uma possível correção com a Proteção de URL. (Consulte [Como configurar as definições da conta de e-mail segura da Cisco para a API do Microsoft Azure (Microsoft 365) - Cisco] para obter mais informações.)

Este exemplo fornece contexto para um filtro de conteúdo para Filtragem de URLs para detectar URLs Desconhecidos:

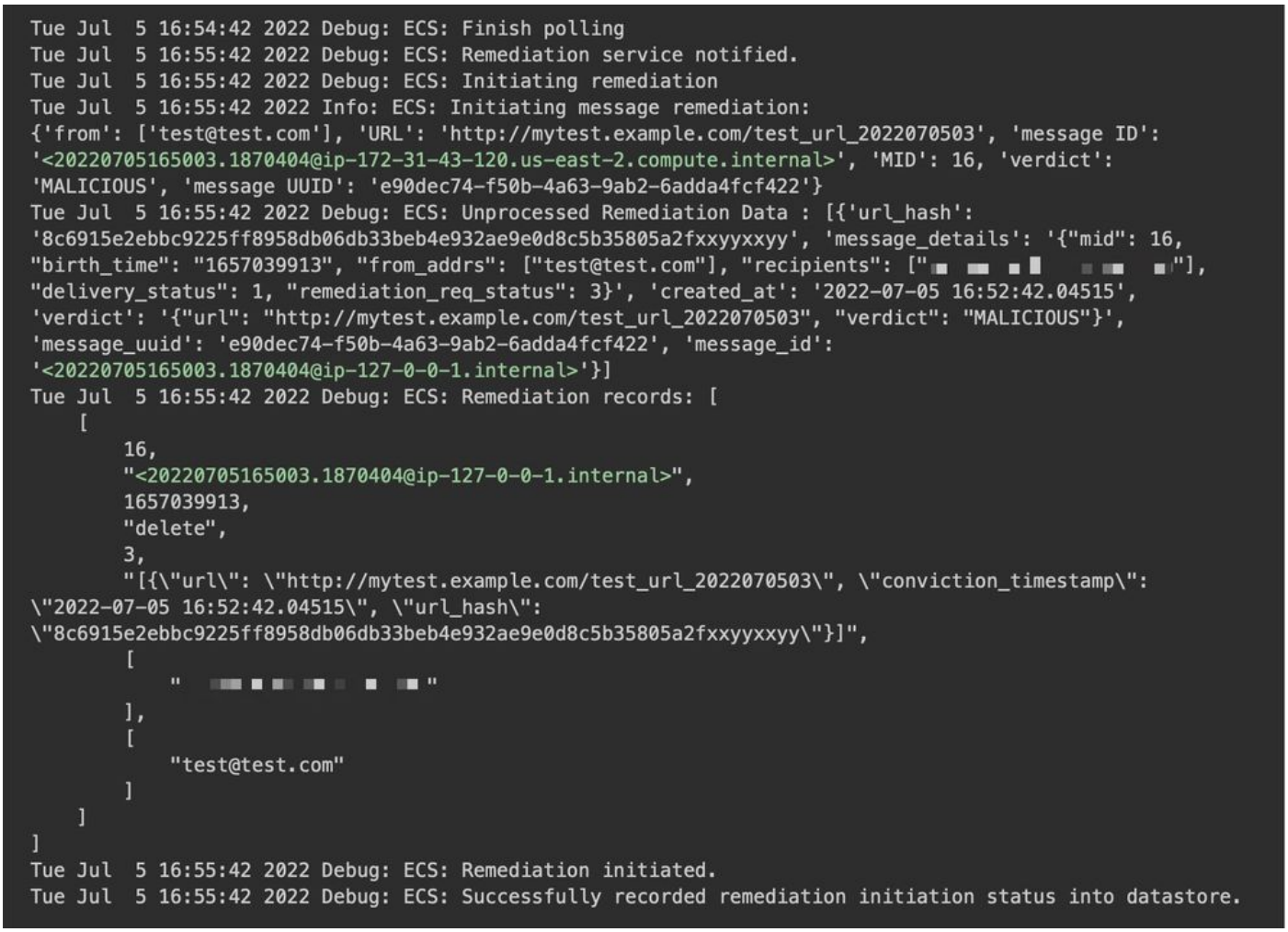
Com esse filtro de conteúdo em vigor, o Cisco Secure Email verifica um URL com uma reputação Desconhecida e grava uma linha de registro no mail_logs. Aqui está um exemplo dos mail_logs:

<#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
```

O URL mytest.example.com/test_url_2022070503 não tem reputação e é visto com "noscore". O filtro de conteúdo URL_UNKNOWN gravou a linha de log como configurada para mail_logs.

Após um ciclo de pesquisa do Cisco Secure Email Gateway para o Talos Intelligence Cloud Service, a URL é verificada e determinada como não confiável. Isso pode ser visto nos logs do ECS no nível de "rastreamento":



```
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.
```

Em seguida, nos mail_logs, quando a correção em si é chamada e concluída:

```
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
```

Os administradores devem considerar a ação para URLs desconhecidos a seu critério. Se houver um aumento visível nos e-mails e anexos relacionados a phishing, analise o relatório mail_logs e Filtros de conteúdo. Além disso, os administradores podem configurar o redirecionamento de URLs desconhecidos para o serviço proxy Cisco Security para avaliação em tempo de clique. Neste exemplo, navegue para Adicionar ação > Reputação de URL em nosso filtro de conteúdo 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 (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

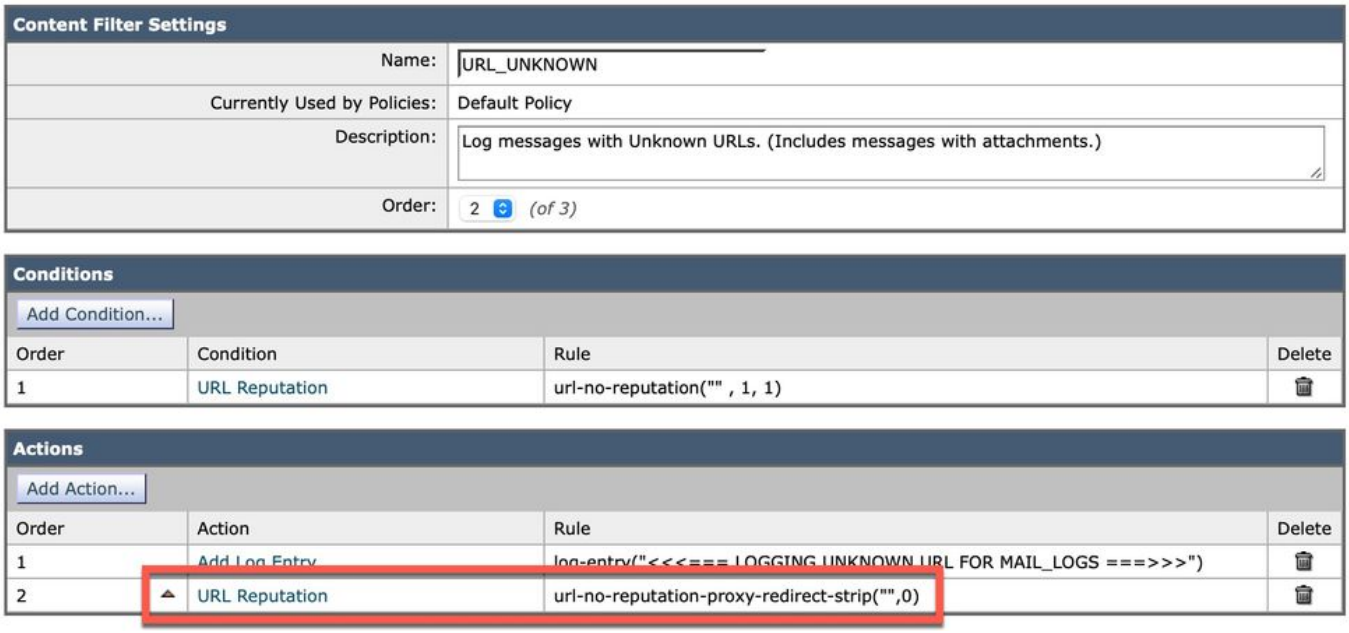
Check URLs within

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

Action on URL within the message body and subject:

. A opção de desencapar anexos para alguns administradores não é preferível. Revise a ação e considere apenas a opção para configurar Corpo da mensagem e Assunto.

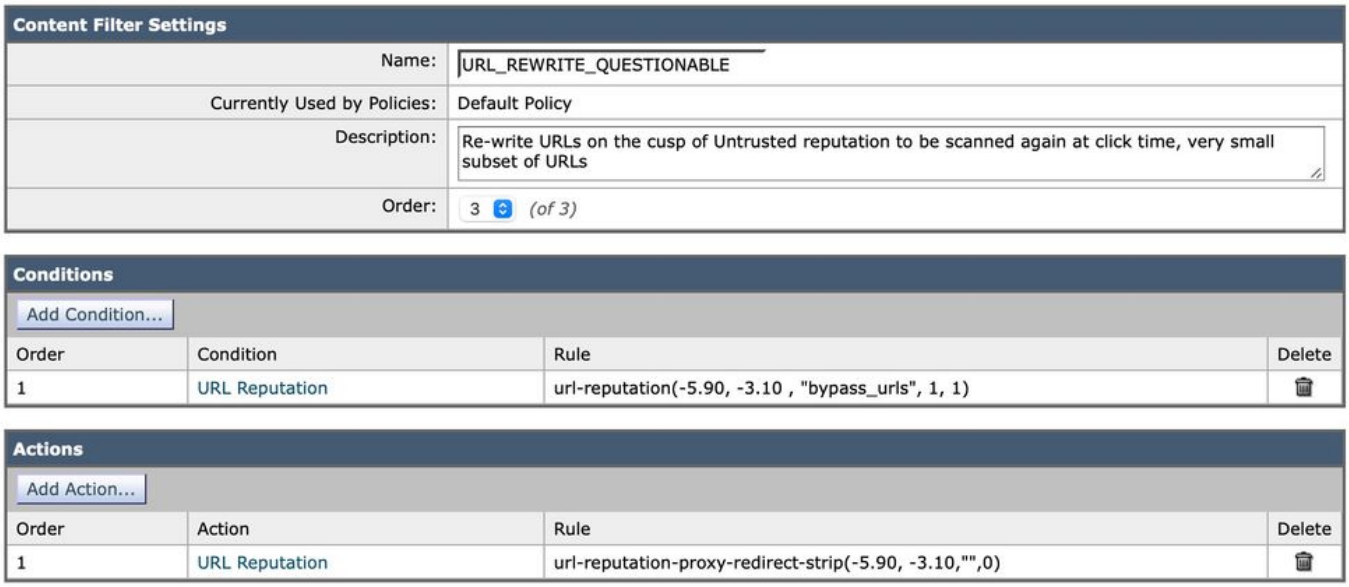
O filtro de conteúdo atualizado agora se parece com este exemplo, com a adição da ação Redirect to Cisco Secure Proxy:



URL(s) questionável(is)

Questionável: comportamento de URL que pode indicar risco ou pode ser indesejável. Embora não seja seguro para todas as organizações, esse veredito tem uma taxa de falsos positivos (FP) baixa e relativamente segura. Um veredito não bloqueado prioriza a entrega em detrimento da segurança, o que pode resultar em mensagens que contêm URLs arriscadas.
Ação recomendada: Verificar com mecanismos subsequentes e bloquear após revisão.

Como configuramos em URL(s) Desconhecido(s), os administradores podem achar útil enviar URL(s) Questionável(is) ao Proxy de Segurança da Cisco ou utilizar a ação para definir totalmente o(s) URL(s).



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

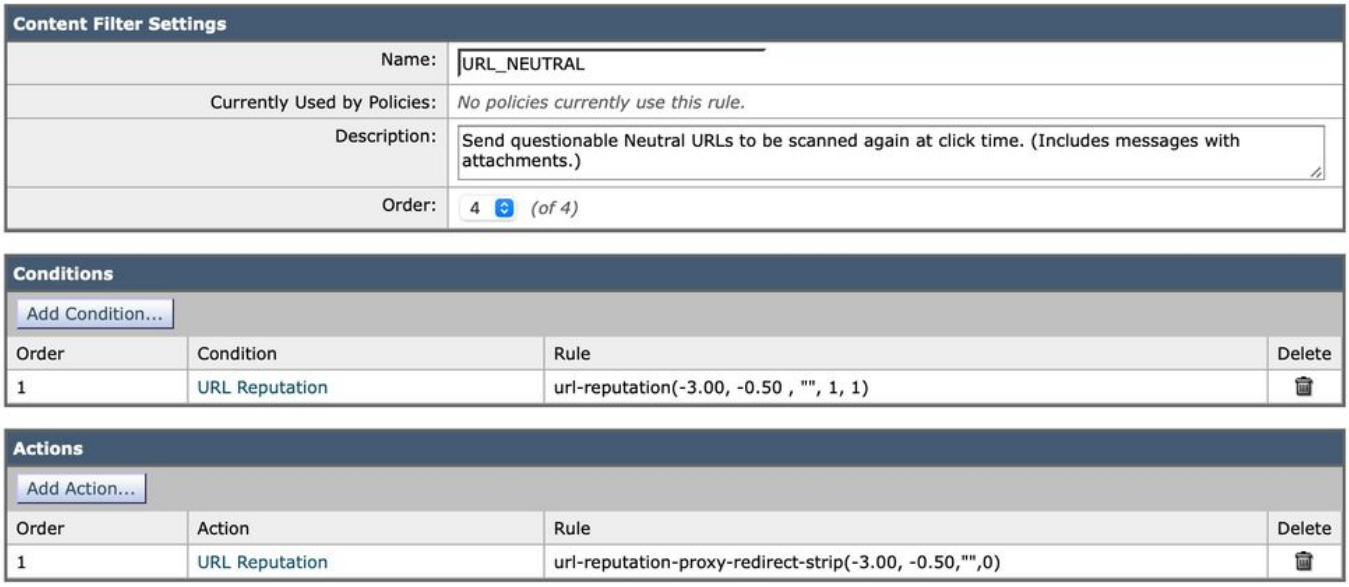
Add Action...

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

URL(s) neutro(s)

Neutro: URL sem comportamento positivo ou negativo. No entanto, ela foi avaliada. Ou seja, o URL não tem nenhum risco conhecido. Portanto, esta é a maior parte dos veredictos de reputação.
Ação recomendada: verifique com os mecanismos subsequentes se há outros conteúdos potencialmente mal-intencionados.

Os administradores podem ver uma URL neutra com uma pontuação negativa como uma ameaça. Avalie o número de mensagens e ocorrências de URLs Neutros a seu critério. Da mesma forma como atualizamos URL(s) Desconhecido(s) e URL(s) Questionável(is) para utilizar a ação para enviar o(s) URL(s) para o Proxy de Segurança da Cisco, URL(s) Neutro(s) ou um Intervalo Personalizado que inclua um subconjunto do lado negativo de Neutro pode ser considerado. Este exemplo mostra uma verificação de URLs neutros com a implementação deste filtro de conteúdo de entrada:



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)	

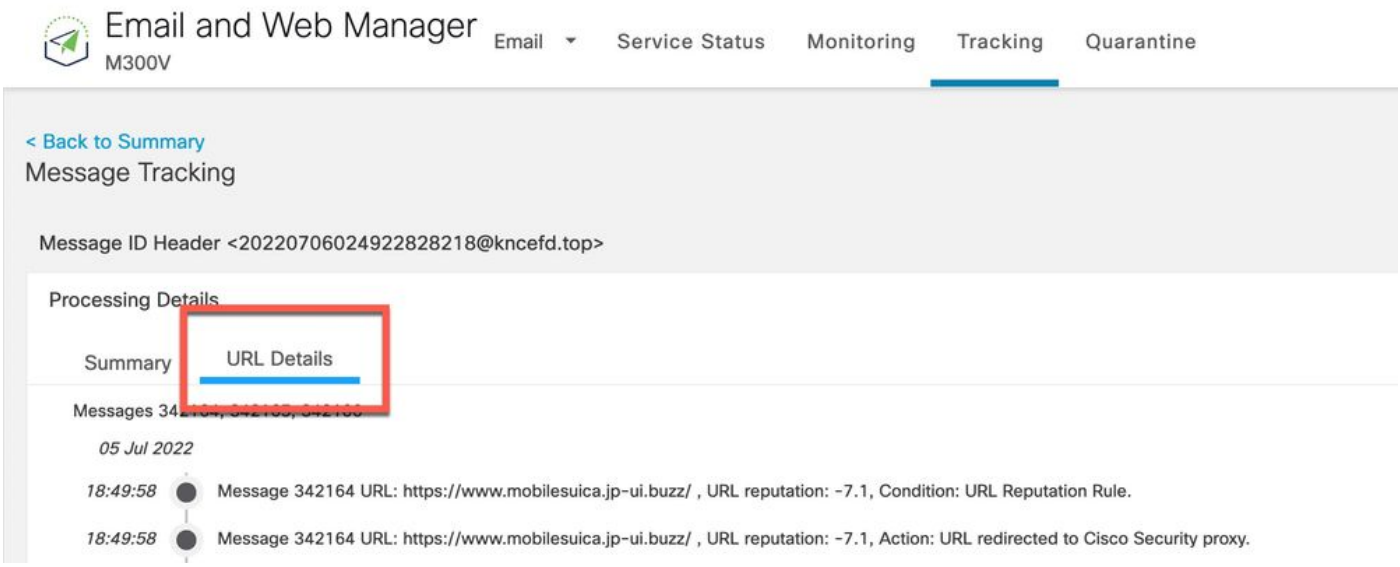
Actions

Add Action...

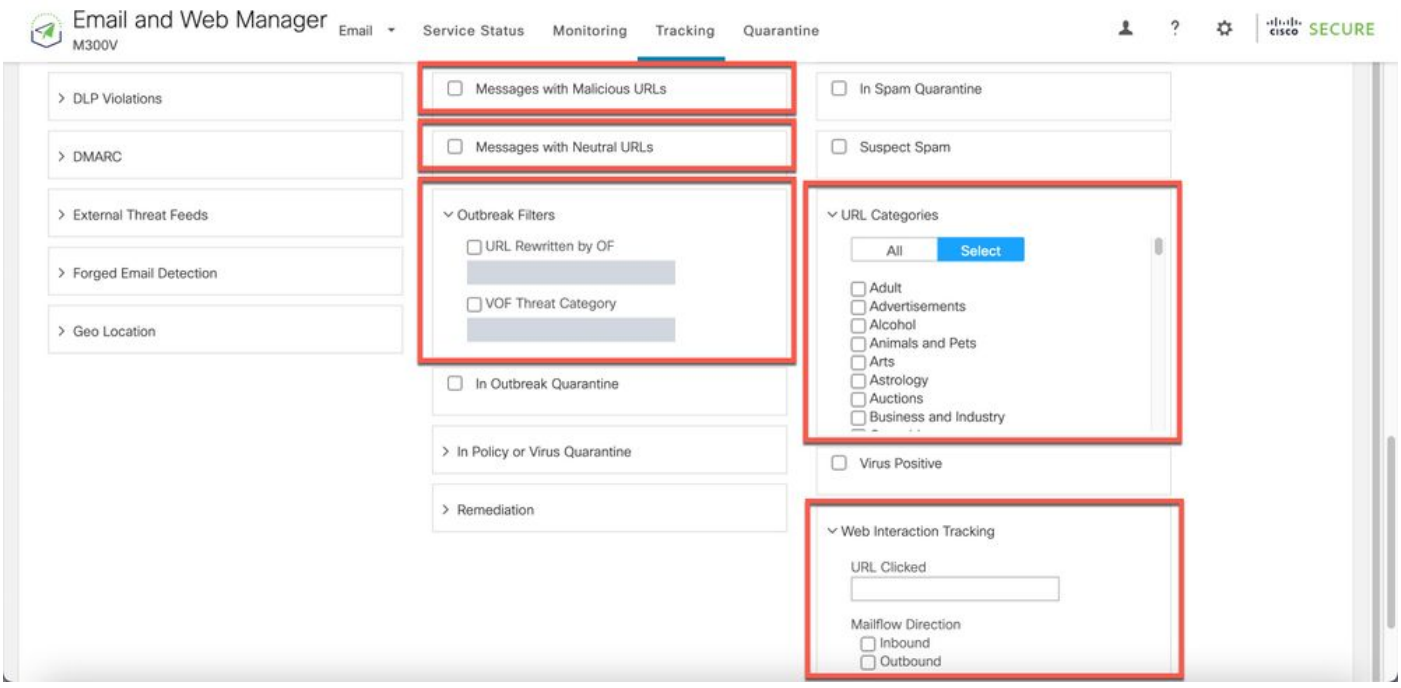
Order	Action	Rule	Delete
1	URL Reputation	url-reputation-proxy-redirect-strip(-3.00, -0.50,"",0)	

Rastreamento de mensagem

Revise as opções de Rastreamento de mensagem para URLs associados a MIDs. Às vezes, os URLs não registram nos mail_logs e você pode localizá-los nos detalhes de Rastreamento de mensagem. Por exemplo:



O Rastreamento de mensagens também fornece opções de Pesquisa avançada para mensagens com defesa e interação de URL:



Relatando URLs sem categoria e classificados incorretamente

Às vezes, uma URL pode relatar como sem uma reputação ou classificação. Há também URL(s) que estão mal categorizados. Para relatar esses avistamentos de URLs, visite a página de Solicitações de Categorização da Web do Cisco Talos na página de Suporte do Reputation Center do Talos.

Depois de relatar um URL, você pode exibir o status em seu Meus tíquetes

URLs mal-intencionados e mensagens de marketing não são detectados por filtros de invasão ou anti-spam

Isso pode ocorrer porque a reputação e a categoria do site são apenas dois critérios entre muitos que os filtros antisspam e de ataque usam para determinar seus vereditos. Para aumentar a sensibilidade desses filtros, reduza os limites necessários para agir, como regravar ou substituir URLs por texto, quarentena ou descartar mensagens.

Como alternativa, você pode criar filtros de conteúdo ou de mensagens com base na escala de reputação do URL.

Appendix

Ativar suporte de filtragem de URLs abreviados

Observação: esta seção se aplica somente ao AsyncOS 11.1 a 13.0 para segurança de e-mail.

O suporte à filtragem de URL para URLs abreviados pode ser feito apenas pela CLI, com o comando websecurityadvancedconfig:

```
<#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
```

A Cisco recomenda que isso seja ativado para as melhores práticas de configuração de filtragem de URL. Uma vez ativados, os logs de e-mail refletem sempre que um URL abreviado é usado na mensagem:

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

Uma vez que a filtragem de URL é ativada, conforme descrito neste artigo, a partir do exemplo mail_logs, podemos ver que o link bit.ly é gravado, E o link original para o qual ele se expande também é gravado.

Informações adicionais

Documentação do Cisco Secure Email Gateway

- Notas de versão
- Guia do usuário
- Guia de referência CLI
- Guias de programação de API para Cisco Secure Email Gateway
- Fonte aberta usada no Cisco Secure Email Gateway
- Guia de instalação do Cisco Content Security Virtual Appliance(inclui vESA)

Documentação do Secure Email Cloud Gateway

- Notas de versão
- Guia do usuário

Documentação do Cisco Secure Email and Web Manager

- Notas de versão e matriz de compatibilidade
- Guia do usuário
- Guias de programação de API para Cisco Secure Email e Web Manager
- Guia de instalação do Cisco Content Security Virtual Appliance(inclui vSMA)

Documentação do produto Cisco Secure

- Arquitetura de nomenclatura do portfólio Cisco Secure

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.