Configuración del filtrado de URL para Secure Email Gateway y Cloud Gateway

Contenido

Introducción

Este documento describe cómo configurar el filtrado de URL en Cisco Secure Email Gateway y Cloud Gateway y las prácticas recomendadas para el uso del filtrado de URL.

Antecedentes

El filtrado de URL se introdujo por primera vez con AsyncOS 11.1 for Email Security. Esta versión permitió que la configuración de Cisco Secure Email buscara direcciones URL en los archivos adjuntos de los mensajes y realizara acciones configuradas en dichos mensajes. Los filtros de mensajes y contenido utilizan Reputación de URL y Categoría de URL para comprobar las URL de los mensajes y los archivos adjuntos. Para obtener más información, consulte los capítulos sobre el uso de filtros de mensajes para aplicar políticas de correo electrónico, filtros de contenido y protección frente a URL no fiables o indeseables de la guía del usuario o la ayuda en línea.

El control y la protección frente a enlaces no fiables o indeseables se incorporan a la cola de trabajo para los procesos de filtrado de mensajes, contenido, brotes y antispam. Estos controles:

- Aumentar la eficacia de la protección frente a URL no fiables en mensajes y archivos

adjuntos.

- Además, el filtrado de URL se incorpora a los filtros de brote de virus. Esta protección reforzada es aplicable incluso si su organización ya dispone de un dispositivo de seguridad Cisco Web Security Appliance o de una protección similar frente a amenazas basadas en la Web, ya que bloquea las amenazas en el punto de entrada.
- También puede utilizar filtros de contenido o mensajes para realizar acciones basadas en la puntuación de reputación basada en Web (WBRS) de las URL de los mensajes. Por ejemplo, puede reescribir direcciones URL con una reputación neutra o desconocida para redirigirlas al proxy de Cisco Web Security para evaluar su seguridad al hacer clic.
- Identificar mejor el spam
- El dispositivo utiliza la reputación y la categoría de los enlaces en los mensajes y otros algoritmos de identificación de spam para ayudar a identificar el spam. Por ejemplo, si un vínculo de un mensaje pertenece a un sitio web de marketing, es más probable que el mensaje sea un mensaje de marketing.
- Respaldar la aplicación de políticas de uso aceptable corporativas
- La categoría de URL (contenido para adultos o actividades ilegales, por ejemplo) se puede utilizar con filtros de contenido y mensajes para aplicar políticas de uso corporativo aceptables.
- Permiten identificar a los usuarios de la organización que han hecho clic con más frecuencia en una dirección URL de un mensaje que se ha reescrito para ofrecer protección y los vínculos en los que se ha hecho clic con más frecuencia.

Nota: En la versión AsyncOS 11.1 for Email Security, el filtrado de URL introdujo la compatibilidad con URL más cortas. Con el comando CLI' websecurityadvancedconfig', se podían ver y configurar los servicios más cortos. Esta opción de configuración se actualizó en AsyncOS 13.5 para Email Security. Después de actualizar a esta versión, se expanden todas las URL abreviadas. No existe ninguna opción para desactivar la expansión de URL abreviadas. Por este motivo, Cisco recomienda AsyncOS 13.5 para Email Security o una versión más reciente para proporcionar las protecciones más recientes para la defensa de URL. Consulte el capítulo "Protección frente a URL malintencionadas o no deseadas" de la guía del usuario o la ayuda en línea y la guía de referencia de CLI para AsyncOS para Cisco Email Security Appliance.

Nota: Para este documento, se utiliza AsyncOS 14.2 for Email Security para los ejemplos y capturas de pantalla proporcionadas.

Nota: Cisco Secure Email también proporciona una guía detallada de defensa de URL en docs.ces.cisco.com.

Prerequisites

Al configurar el filtrado de URL en Cisco Secure Email Gateway o Cloud Gateway, también debe configurar otras funciones según la funcionalidad que desee. A continuación se indican algunas de las funciones típicas que se habilitan junto con el filtrado de URL:

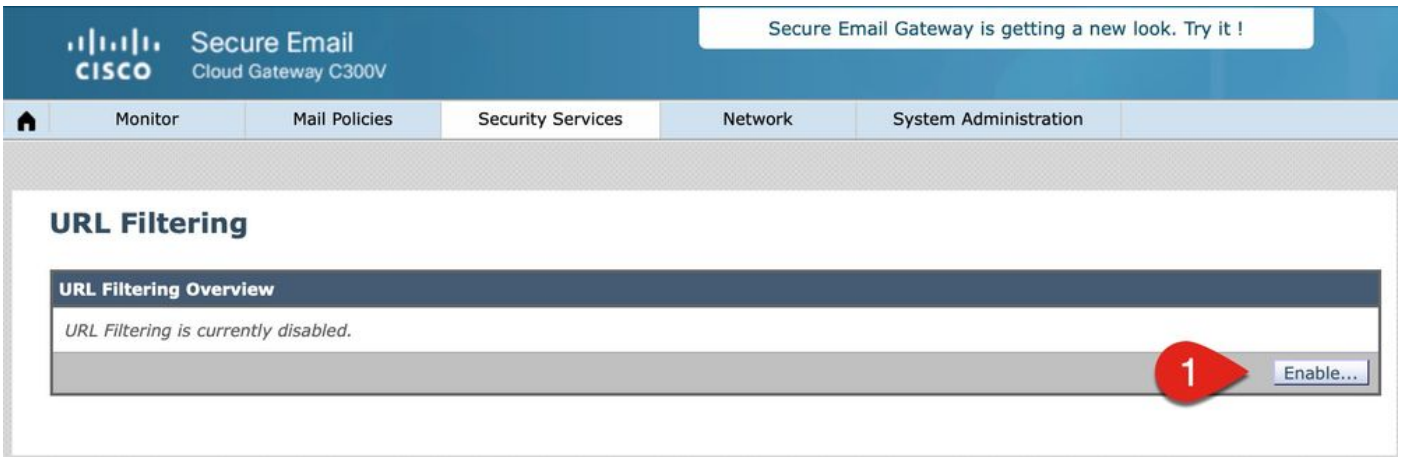
- Para mejorar la protección contra el spam, la función de análisis antispam **debe estar habilitada globalmente** según la política de correo aplicable. Anti-Spam se considera la función Cisco IronPort Anti-Spam (IPAS) o la función Cisco Intelligent Multi-Scan (IMS).

- Para mejorar la protección frente a malware, la función de filtros de brote de virus (VOF) **debe estar habilitada globalmente** según la política de correo aplicable.
- Para acciones basadas en la reputación de URL o para aplicar políticas de uso aceptable con el uso de filtros de mensajes y contenido, VOF **debe habilitarse globalmente**.

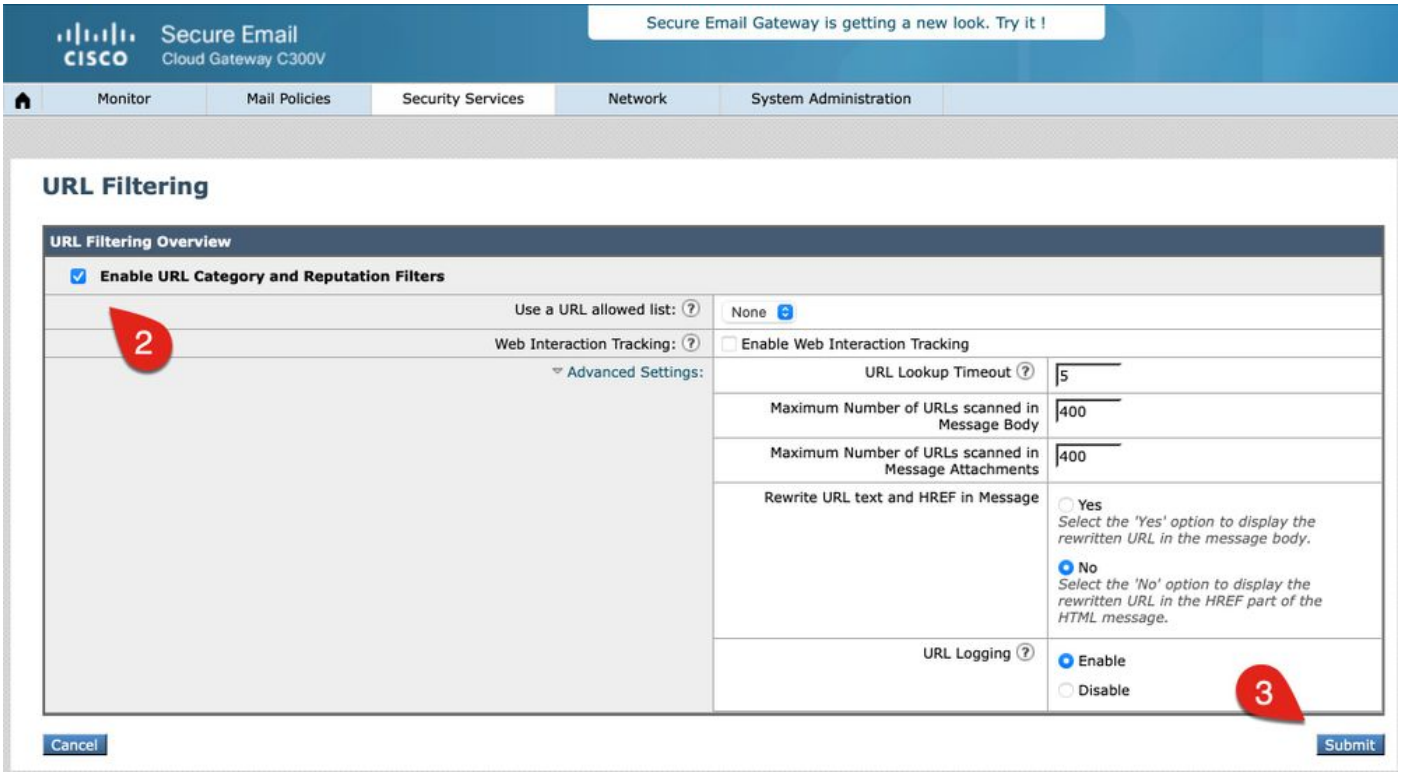
Habilitar filtrado de URL

Primero debe activar la función para implementar el filtrado de URL en Cisco Secure Email Gateway o Cloud Gateway. El administrador puede habilitar el filtrado de URL desde la GUI o la CLI.

Para habilitar el filtrado de URL, en GUI, navegue hasta **Servicios de seguridad > Filtrado de URL** y haga clic en **Habilitar:**



A continuación, haga clic en **Enable URL Category and Reputation Filters**. Este ejemplo incluye los valores de las prácticas recomendadas para el tiempo de espera de búsqueda de URL, el número máximo de URL analizadas y habilita la opción para registrar URL:



Nota: Asegúrese de **confirmar** los cambios en la configuración en este momento.

Crear acciones de filtrado de URL

Cuando habilita el filtrado de URL por sí solo, no realiza ninguna acción contra las URL de los mensajes o los mensajes con archivos adjuntos.

Se evalúan las direcciones URL incluidas en los mensajes y archivos adjuntos de las directivas de correo entrante y saliente. Cualquier cadena válida para una dirección URL se evalúa para incluir cadenas con estos componentes:

- HTTP, HTTPS o WWW
- Dominio o direcciones IP
- Números de puerto precedidos de dos puntos (:)
- Letras mayúsculas o minúsculas

Nota: La entrada de registro de URL es visible desde mail_logs para la mayoría de las URL. Si la URL no está registrada en mail_logs, revise Rastreo de mensajes para el ID de mensaje (MID). El rastreo de mensajes incluye una pestaña para "Detalles de URL".

Cuando el sistema evalúa las URL para determinar si un mensaje es spam, si es necesario para la gestión de la carga, da prioridad y filtra los mensajes entrantes sobre los salientes.

Puede realizar acciones en mensajes en función de la reputación de la URL o la categoría de URL del cuerpo del mensaje o en mensajes con archivos adjuntos.

Por ejemplo, si desea aplicar la acción **Drop (Final Action)** a todos los mensajes que incluyan direcciones URL en la categoría Adulto, agregue una condición de tipo URL Category con la categoría Adulto seleccionada.

Si no especifica una categoría, la acción que elija se aplicará a todos los mensajes.

El intervalo de puntuación de reputación de URL para fiable, favorable, neutra, cuestionable y no fiable está predefinido y no se puede editar. Puede especificar un rango personalizado. Utilice "Desconocido" para las URL para las que aún no se ha determinado una puntuación de reputación.

Para analizar rápidamente las URL y realizar acciones, puede crear un filtro de contenido de modo que *si* el mensaje tiene una URL válida, *entonces* se aplique la acción. Desde la GUI, navegue **Políticas de correo > Filtros de contenido entrante > Agregar filtro**.

Las acciones asociadas con las URL son las siguientes:

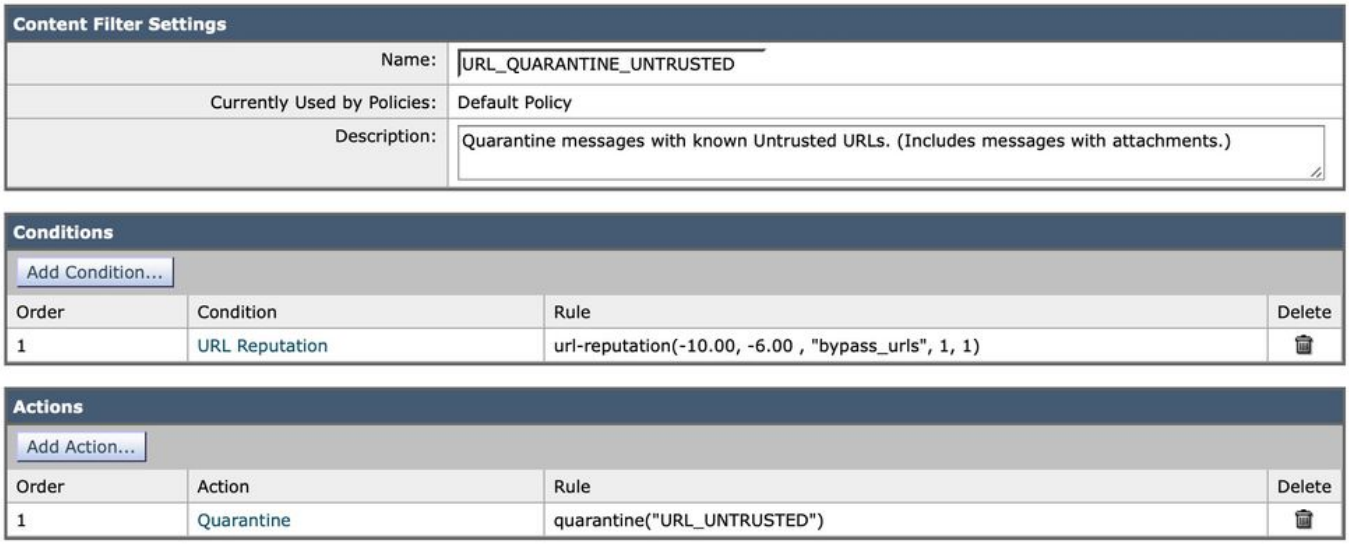
- Depurar URL La URL se modifica para que no se pueda hacer clic en ella, pero el destinatario del mensaje puede leer la URL deseada. (Se insertan caracteres adicionales en la URL original.)
- Redirigir al proxy de seguridad de Cisco La URL se reescribe al hacer clic para pasar a través del proxy de seguridad de Cisco para realizar una verificación adicional. Según el veredicto del proxy de seguridad de Cisco, el sitio podría ser inaccesible para el usuario.
- Reemplazar URL por un mensaje de texto Con esta opción, un administrador puede volver a escribir la dirección URL dentro del mensaje y enviarla externamente para el aislamiento del explorador remoto.

URL(s) no fiables

No confiable: comportamiento de URL que es excepcionalmente malo, malintencionado o indeseable. Este es el umbral de lista de bloqueo recomendado más seguro; sin embargo, puede haber mensajes que no estén bloqueados porque las URL que contienen tienen un nivel de amenaza menor. Prioriza la entrega sobre la seguridad.

Acción Recomendada: Bloqueo. (Un administrador puede poner el mensaje en cuarentena o descartarlo por completo.)

Este ejemplo proporciona contexto para un filtro de contenido para que el filtrado de URL detecte las URL no fiables:



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 este filtro de contenido implementado, Cisco Secure Email busca una URL con una reputación *no fiable* (-10.00 a -6.00) y pone el mensaje en cuarentena, URL_UNTRUSTED. Aquí hay un ejemplo de mail_logs:

```
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, helo: ip-127-0-0-1.internal, env-from: test.com, header-from: Not Present, reply-
to: Not Present
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Consolidated Sender Threat Level: Neutral, Threat
Category: N/A, Suspected Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days
(or greater) for domain: test.com
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, helo:ip-127-0-0-1.internal, env-from: test.com, header-from:
test.com, reply-to: Not Present
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Consolidated Sender Threat Level: Neutral, Threat
Category: N/A, Suspected Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days
(or greater) for domain: test.com
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Tracker Header :
62c45245_jTikQ2lV2NYfmrGzMwQMBd68fxqFFueNmElwb5kQOt89QH1tn2s+wyqFO0Bg6qJenrPTndlyp+zb0xjKxrK3Cw=
=
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 table
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 Condition: URL Reputation Rule
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
```

La dirección URL ihaveabadreputation.com se considera **NO FIABLE** y tiene una puntuación de **-**

9.5. El filtrado de URL detectó la dirección URL no fiable y la colocó en cuarentena en URL_UNTRUSTED.

El ejemplo anterior de mail_logs proporciona un ejemplo si SÓLO está habilitado el filtro de contenido para el filtrado URL para la política de correo entrante. Si la misma política de correo tiene servicios adicionales habilitados, como Anti-Spam, los otros servicios indican si la URL se ha detectado de ESOS servicios y sus reglas. En el mismo ejemplo de URL, se habilita Cisco Anti-Spam Engine (CASE) para la política de correo entrante y se analiza el cuerpo del mensaje y se determina que es spam positivo. Esto se indica primero en mail_logs ya que Anti-Spam es el primer servicio en la canalización de procesamiento de correo. Los filtros de contenido se encuentran más adelante en la canalización de procesamiento de correo:

```
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.internal, helo:ip-127-0-0-1.internal, env-from: test.com, header-from: Not
Present, reply-to: Not Present
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Consolidated Sender Threat Level: Neutral, Threat
Category: N/A, Suspected Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days
(or greater) for domain: test.com
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.internal, helo:ip-127-0-0-1.internal, env-from: test.com, header-from:
test.com, reply-to: Not Present
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Consolidated Sender Threat Level: Neutral, Threat
Category: N/A, Suspected Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days
(or greater) for domain: test.com
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Tracker Header :
62c45695_mqwplhpxGDqtgUp/XTLGFKD60hwNKKsghUKAMFOYVv9l32gncZX7879qf3FGzWfP1mc6ZH3iLMpcKwCBJXhmIg=
=
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 table
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
matched Condition: URL Reputation Rule
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
```

En ocasiones, las reglas CASE e IPAS contienen reglas, reputación o puntuaciones que coinciden con el contenido de un remitente, dominio o mensaje específico para detectar únicamente las amenazas de URL. En este ejemplo, se ha visto ihaveabadreputation.com, etiquetado para Spam Quarantine (ISQ) y la cuarentena URL_UNTRUSTED por el filtro de contenido URL_QUARANTINE_UNTRUSTED. El mensaje entra primero en la cuarentena URL_UNTRUSTED. Cuando un administrador libera el mensaje de esa cuarentena o se cumplen los criterios de límite de tiempo/configuración de la cuarentena URL_UNTRUSTED, el mensaje pasa a la ISQ.

Según las preferencias del administrador, se pueden configurar condiciones y acciones adicionales para el filtro de contenido.

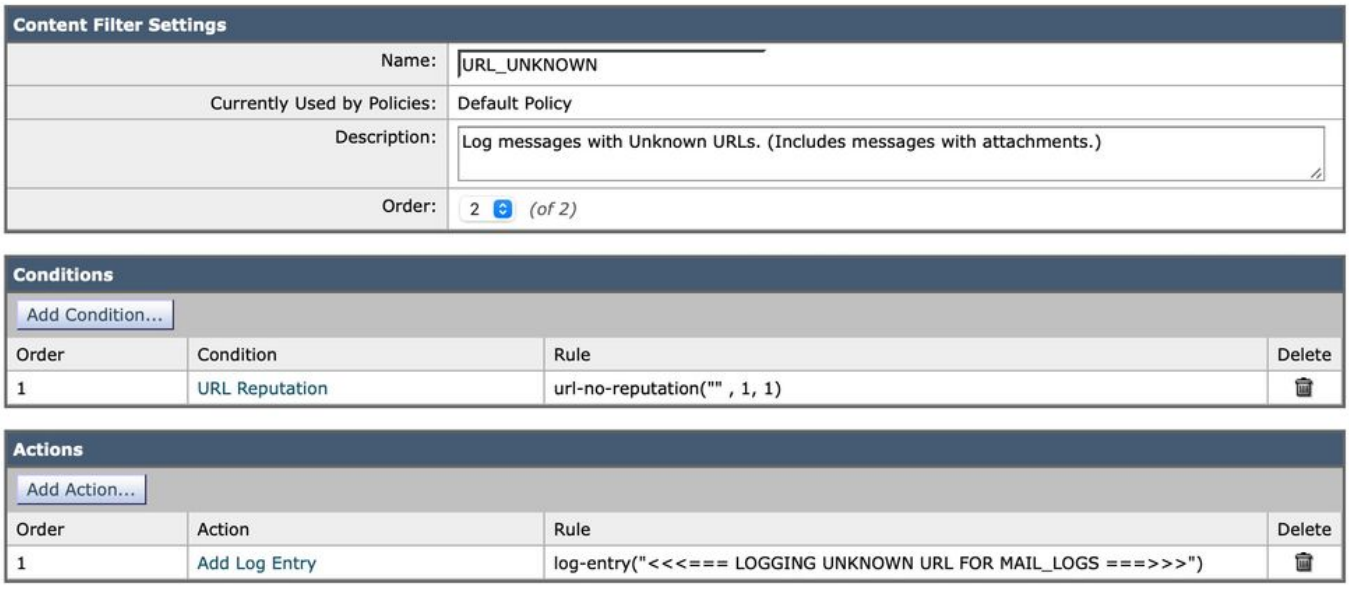
URL(s) desconocidas

Desconocido: no se ha evaluado anteriormente o no muestra funciones para afirmar un veredicto de nivel de amenaza. El servicio de reputación de URL no tiene suficientes datos para establecer una reputación. Este veredicto no es adecuado para acciones en una política de reputación de URL directamente.

Acción Recomendada: Escanee con los motores siguientes para buscar otro contenido potencialmente malintencionado.

Las URL desconocidas o "sin reputación" pueden ser aquellas que contienen nuevos dominios o URL que han visto poco o ningún tráfico y no pueden tener una reputación evaluada ni un veredicto de nivel de amenaza. Estos pueden convertirse en no fiables a medida que se obtiene más información sobre su dominio y origen. Para dichas URL, Cisco recomienda un filtro de contenido para registrar o uno que incluya la detección de la URL desconocida. A partir de la versión 14.2 de AsyncOS, se envían URL desconocidas al servicio Talos Intelligence Cloud Service para realizar un análisis profundo de URL activado en varios indicadores de amenazas. Además, una entrada de registro de correo de las URL desconocidas proporciona al administrador una indicación de las URL incluidas en una MID y una posible solución con protección de URL. (Consulte Cómo configurar la configuración de la cuenta de correo electrónico seguro de Cisco para la API de Microsoft Azure (Microsoft 365) - Cisco para obtener más información.)

Este ejemplo proporciona contexto para un filtro de contenido para que el filtrado de URL detecte las URL desconocidas:



Con este filtro de contenido implementado, Cisco Secure Email busca una URL con una reputación *Unknown* y escribe una línea de registro en mail_logs. Aquí hay un ejemplo de mail_logs:

```
Tue Jul 5 16:51:53 2022 Info: ICID 20 ACCEPT SG MY_TRUSTED_HOSTS match 127.0.0.1 SBRS None
country United States
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-127-0-0-1.internal, helo:ip-127-0-0-1.internal, env-from: test.com, header-from: Not
Present, reply-to: Not Present
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Consolidated Sender Threat Level: Neutral, Threat
Category: N/A, Suspected Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days
(or greater) for domain: test.com
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-127-0-0-1.internal, helo:ip-127-0-0-1.internal, env-from: test.com, header-from:
test.com, reply-to: Not Present
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Consolidated Sender Threat Level: Neutral, Threat
Category: N/A, Suspected Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days
(or greater) for domain: test.com
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Tracker Header :
62c46c29_vrAqZZys2Hqk+BFINVrzdNLLn81kuIf/K6o71YZLVE5c2s8v9M9pKpQZSgtz7a531Dw39F6An2x6tMSucDegqA=
=
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 inbound table
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 noscore matched Condition: URL Reputation Rule
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.internal> [InternalId=1198295889556, Hostname=<my>.prod.outlook.com] 15585 bytes in 0.193,
78.747 KB/sec Queued mail for delivery'
Tue Jul 5 16:51:56 2022 Info: Message finished MID 16 done
Tue Jul 5 16:52:01 2022 Info: DCID 13 close
```

La URL mytest.example.com/test_url_2022070503 no tiene reputación y se ve con "noscore". El filtro de contenido URL_UNKNOWN escribió la línea de registro según lo configurado para mail_logs.

Después de un ciclo de sondeo desde Cisco Secure Email Gateway al servicio Talos Intelligence Cloud Service, se analiza la URL y se determina que no es de confianza. Esto se puede ver en los registros de ECS en el nivel "Seguimiento":

```
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.
```

Y posteriormente, en mail_logs, cuando se llama y se completa la corrección:

```
Tue Jul 5 16:55:42 2022 Info: Message 16 containing URL
'http://mytest.example.com/test_url_2022070503' was initiated for remediation.
Tue Jul 5 16:55:55 2022 Info: Message 16 was processed due to URL retrospection by Mailbox
Remediation with 'Delete' remedial action for recipient <end_user>. Profile used to remediate:
MSFT_365 Remediation status: Remediated.
```

Los administradores deben considerar la acción de las URL desconocidas a su discreción. Si se observa un aumento de correos electrónicos y archivos adjuntos relacionados con Phish, revise el informe mail_logs y filtros de contenido. Además, los administradores pueden configurar para que se redirijan las URL desconocidas al servicio proxy de seguridad de Cisco para la evaluación del tiempo del clic. En este ejemplo, navegue hasta **Add Action > URL Reputation** dentro de nuestro filtro de contenido URL_UNKNOWN:

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).