URL-filtering configureren voor beveiligde e-mailgateway en cloudgateway

Inhoud

Inleiding

Dit document beschrijft hoe u URL-filtering kunt configureren op Cisco Secure Email Gateway en Cloud Gateway en beste praktijken voor gebruik van URL-filtering.

Achtergrondinformatie

URL-filtering is eerst geïntroduceerd met AsyncOS 11.1 voor e-mailbeveiliging. Met deze release kon de configuratie van Cisco Secure Email worden gescand op URL's in berichtbijlagen en kunnen geconfigureerd acties op dergelijke berichten worden uitgevoerd. Bericht- en inhoudsfilters gebruiken de URL-reputatie en URL-categorie om te controleren op URL’s in berichten en bijlagen. Zie voor meer informatie de hoofdstukken "Berichtenfilters gebruiken om e-mailbeleid af te dwingen", "Contentfilters" en "Beschermen tegen onbetrouwbare of ongewenste URL’s" in de Gebruikersgids of online help.

Controle en bescherming tegen onbetrouwbare of ongewenste links worden opgenomen in de werkvoorraad voor antispam, uitbraak, inhoud en berichtfiltering processen. Deze functies:

- Vergroot de effectiviteit van bescherming tegen onbetrouwbare URL's in berichten en bijlagen.

- Daarnaast is URL-filtering opgenomen in Uitbraakfilters. Deze versterkte bescherming is van toepassing zelfs als uw organisatie al een Cisco Web Security Applicatie of vergelijkbare bescherming tegen webgebaseerde bedreigingen heeft, omdat bedreigingen op het punt van binnenkomst worden geblokkeerd.
- U kunt altijd content- of berichtfilters gebruiken om acties te nemen op basis van de webgebaseerde reputatiescore (WBRS) van URL's in berichten. U kunt bijvoorbeeld URL's met een neutrale of onbekende reputatie opnieuw schrijven en deze omleiden naar de Cisco web security proxy voor evaluatie van hun veiligheid bij het klikken.
- Verbeteren identificatie van spam.
- Het apparaat gebruikt de reputatie en categorie van links in berichten en andere algoritmen voor spamidentificatie om spam te helpen identificeren. Bijvoorbeeld, als een link in een bericht behoort tot een marketingwebsite, is het bericht waarschijnlijk eerder een marketingbericht.
- Ondersteunen handhaving van bedrijfsbeleid voor aanvaardbaar gebruik.
- De categorie URL's (bijvoorbeeld Adult Content of Illegal Activities) kan worden gebruikt met inhoud- en berichtfilters om een acceptabel beleid voor bedrijfsgebruik af te dwingen.
- Sta u toe om gebruikers in uw organisatie te identificeren die het vaakst een URL in een bericht klikten dat voor bescherming is herschreven en de verbindingen die het meest meestal zijn geklikt.

Opmerking: In AsyncOS 11.1 voor e-mail security release, URL filtering introduceerde ondersteuning voor verkorte URL's. Met de CLI commando' websecurity geavanceerde configuratie,' de kortere diensten kunnen worden gezien en geconfigureerd. Deze configuratieoptie is bijgewerkt in AsyncOS 13.5 voor Email Security. Nadat u aan deze versie bevordert, worden alle verkorte URLs uitgebreid. Er is geen optie om de uitbreiding van verkorte URLs onbruikbaar te maken. Om deze reden raadt Cisco AsyncOS 13.5 voor e-mail security of nieuwer aan om de nieuwste bescherming voor URL-verdediging te bieden. Raadpleeg het hoofdstuk "Beschermen tegen schadelijke of ongewenste URL's" in de gebruikershandleiding of online Help en de CLI-referentiegids voor AsyncOS voor Cisco e-mail security applicatie.

Opmerking: Voor dit document wordt AsyncOS 14.2 voor E-mail security gebruikt voor de voorbeelden en screenshots die worden geleverd.

Opmerking: Cisco Secure Email biedt ook een diepgaande URL-defensiegids op docs.cisco.com.

Voorwaarden

Wanneer u URL-filtering configureert op de Cisco Secure Email Gateway of Cloud Gateway, moet u ook andere functies configureren die afhankelijk zijn van uw gewenste functionaliteit. Hierna volgen enkele typische functies die naast URL-filtering worden ingeschakeld:

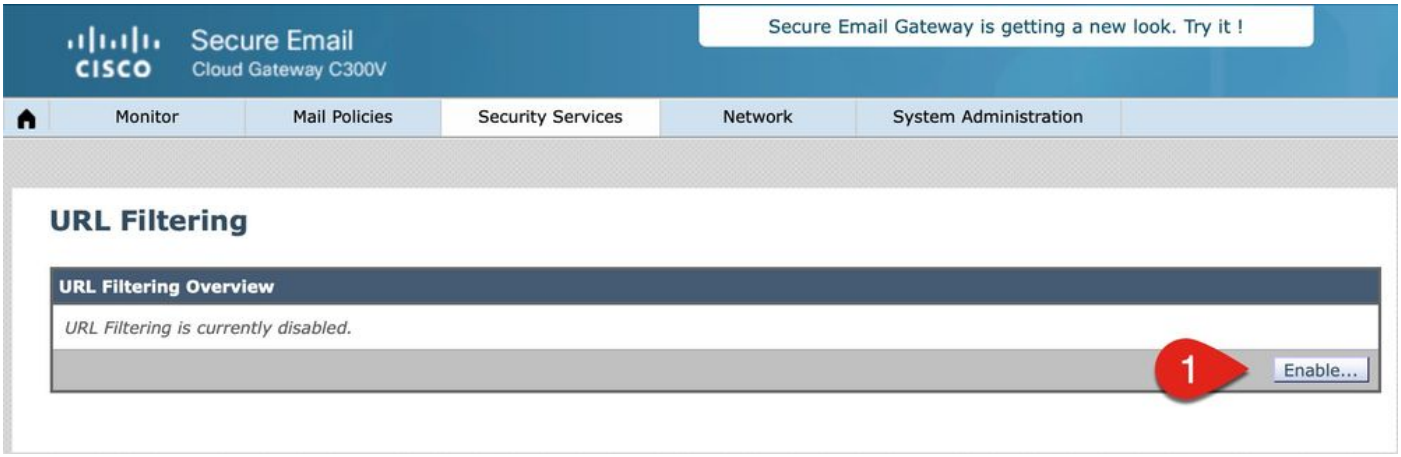
- Voor een betere bescherming tegen spam **moet** de functie Anti-Spam Scanning **wereldwijd zijn ingeschakeld** volgens het toepasselijke postbeleid. Anti-Spam wordt beschouwd als de Cisco IronPort Anti-Spam (IPAS) of de Cisco Intelligent Multi-Scan (IMS) optie.
- Voor een betere bescherming tegen malware **moet** de functie Uitbraakfilters of Virus Uitbraakfilters (VOF) **wereldwijd geactiveerd zijn** volgens het toepasselijke mailbeleid.

- Voor acties op basis van URL Reputation of om acceptabel gebruiksbeleid af te dwingen met het gebruik van bericht- en inhoudsfilters, **moet** VOF **globaal worden ingeschakeld**.

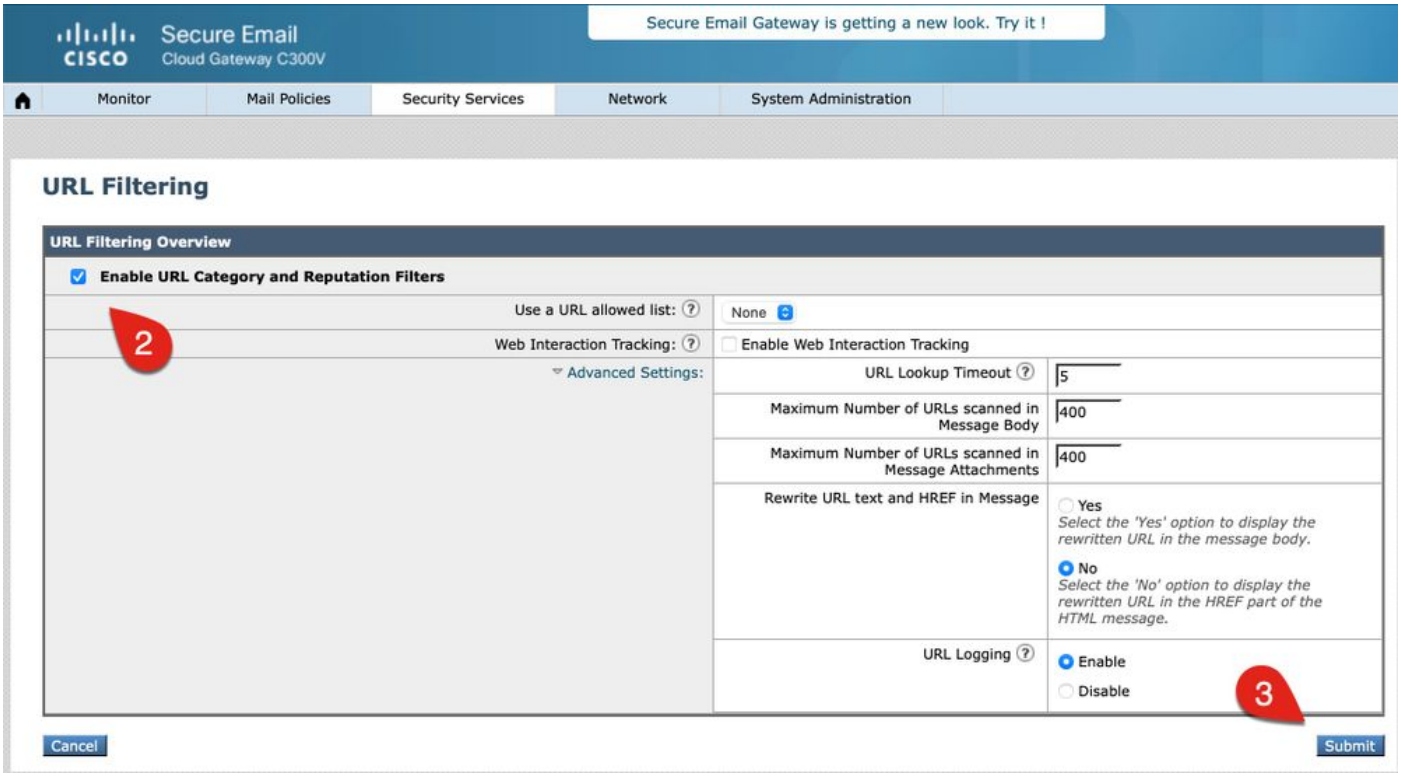
URL-filtering inschakelen

U moet deze functie eerst inschakelen om URL-filtering te implementeren op de Cisco Secure Email Gateway of Cloud Gateway. URL-filtering kan door de beheerder worden ingeschakeld vanuit GUI of CLI.

Als u URL-filtering vanuit GUI wilt inschakelen, navigeert u naar **Security Services > URL-filtering** en klikt u op **Inschakelen:**



Klik vervolgens op **URL-categorie- en reputatiefilters inschakelen**. Dit voorbeeld bevat de waarden van best practices voor URL Lookup-timeout, maximaal aantal gescande URL's en stelt de optie in staat om URL's te registreren:



Opmerking: Zorg ervoor dat u uw wijzigingen in de configuratie op dit moment **vastlegt**.

Acties voor URL-filtering definiëren

Wanneer u alleen URL-filtering inschakelt, onderneemt dit geen actie tegen URL's in berichten of berichten met bijlagen.

De URL('s) in berichten en bijlagen voor inkomend en uitgaand e-mailbeleid worden geëvalueerd. Elke geldige string voor een URL wordt geevalueerd en bevat strings met deze componenten:

- HTTP, HTTPS of WWW
- Domein- of IP-adressen
- Poortnummers voorafgegaan door dubbelepunt (:)
- Hoofdletters of kleine letters

Opmerking: De URL logboekvermelding is zichtbaar vanuit mail_logs voor de meeste URL's. Als de URL niet is ingelogd in de mail_logs, bekijk dan Berichttracering voor de Berichtid (MID). Berichttracering bevat een tabblad voor "URL-details".

Wanneer het systeem URLs evalueert om te bepalen of een bericht spam is, indien nodig voor lastbeheer, geeft het prioriteit en schermen inkomende berichten over uitgaande berichten.

U kunt acties uitvoeren op berichten op basis van de URL-reputatie of de URL-categorie in de berichttekst of berichten met bijlagen.

Als u bijvoorbeeld de actie **Drop (Final Action) (Weigeren (laatste actie)) wilt toepassen op alle berichten met URL's uit de categorie Adult (Volwassenen), voegt u een voorwaarde toe of typt u** URL Category met de geselecteerde categorie Adult (Volwassenen).

Als u geen categorie opgeeft, wordt de gekozen actie toegepast op alle berichten.

De URL-reputatiescore voor Trusted, Favorable, Neutral, Questionable en Unusted zijn vooraf gedefinieerd en kunnen niet worden bewerkt. U kunt een aangepast bereik opgeven. Gebruik "Onbekend" voor URL's waarvoor nog geen reputatiescore is vastgesteld.

Om URL's snel te scannen en actie te ondernemen, kunt u een inhoudsfilter maken zodat *als* het bericht een geldige URL heeft, *dan* de actie wordt toegepast. Navigeer vanuit de GUI **Mail Policies > Inkomende contentfilters > Filter toevoegen**.

Acties die aan URL's zijn gekoppeld, zijn als volgt:

- Defang URL De URL wordt aangepast om deze uit te schakelen, maar de ontvanger van het

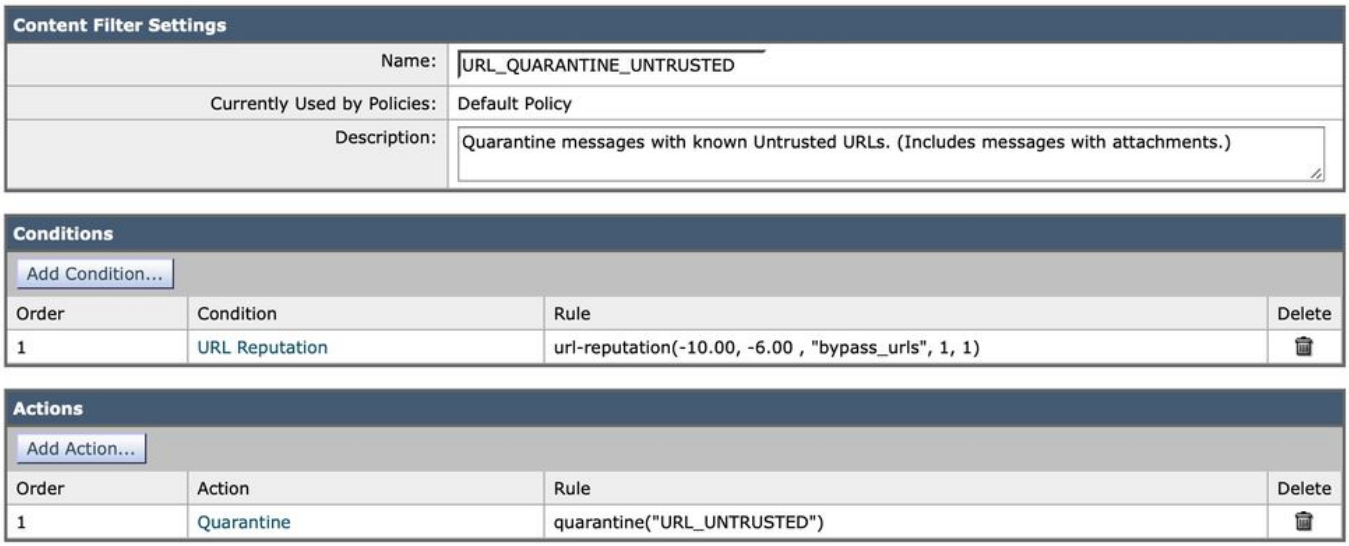
bericht kan nog steeds de bedoelde URL lezen. (Er worden extra tekens ingevoegd in de oorspronkelijke URL.)
- Omleiden naar Cisco security proxy De URL wordt herschreven wanneer erop wordt geklikt om door de Cisco Security Proxy te gaan voor extra verificatie. Gebaseerd op het vonnis van Cisco Security Proxy kan de site ontoegankelijk zijn voor de gebruiker.
- URL vervangen met een tekstbericht Met deze optie kan een beheerder de URL binnen het bericht herschrijven en deze extern verzenden voor Remote Browser Isolation.

Onvertrouwde URL(’s)

Onbetrouwbaar: URL-gedrag dat uitzonderlijk slecht, kwaadaardig of ongewenst is. Dit is de veiligste aanbevolen drempelwaarde voor een blokklijst; er kunnen echter berichten zijn die niet worden geblokkeerd omdat de URL's daarin een lager bedreigingsniveau hebben. Geeft voorrang aan levering boven beveiliging.

Aanbevolen actie: Blok. (Een beheerder kan het bericht volledig in quarantaine plaatsen of laten vallen.)

Dit voorbeeld biedt context voor een inhoudsfilter voor URL-filtering om onbetrouwbare URL’s te detecteren:



Met dit inhoudsfilter, scant Cisco Secure Email naar een URL met een *onbetrouwbare* reputatie (-10.00 tot -6.00) en plaatst het bericht in een quarantaine, URL_UNTRUSTED. Hier is een voorbeeld uit 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
```

De URL ihaveabadreputation.com wordt beschouwd als ONBETROUWBAAR en gescoord op a-9.5. URL-filtering heeft de onbetrouwbare URL gedetecteerd en in quarantaine geplaatst op URL_UNTRUSTED.

Het vorige voorbeeld van mail_logs biedt een voorbeeld als ALLEEN het inhoudsfilter voor URL-filtering is ingeschakeld voor het inkomende mailbeleid. Als hetzelfde postbeleid aanvullende diensten heeft ingeschakeld, zoals Anti-Spam, geven de andere diensten aan of de URL is gedetecteerd van die diensten en hun regels. In hetzelfde URL-voorbeeld is Cisco Anti-Spam Engine (CASE) ingeschakeld voor het inkomende e-mailbeleid en wordt de berichttekst gescand en als positief bevonden voor spam. Dit wordt als eerste aangegeven in de mail_logs omdat Anti-Spam de eerste service is in de postverwerkingspijplijn. Content Filters komen later in de postverwerkingspipeline:

```
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
```

Er zijn tijden wanneer de regels van de ZAAK en IPAS regels, reputatie, of scores bevatten die tegen een specifieke afzender, een domein, of een berichtinhoud aanpassen om bedreigingen URL alleen te ontdekken. In dit voorbeeld, werd ihaveabadreputation.com gezien, geëtiketteerd voor de Spam Quarantaine (ISQ), en URL_UNTRUSTED quarantaine door URL_QUARANTAINE_UNTRUSTED inhoudsfilter. Het bericht gaat eerst naar de URL_UNTRUSTED quarantaine. Wanneer het bericht door een beheerder uit die quarantaine wordt vrijgegeven of aan de tijdslimiet/configuratiecriteria van de URL_UNTRUSTED quarantaine is voldaan, wordt het bericht vervolgens naar de ISQ verplaatst.

Gebaseerd op beheerdersvoorkeuren kunnen extra voorwaarden en acties worden geconfigureerd voor het filter.

Onbekende URL(s)

Onbekend: Niet eerder geëvalueerd of toont geen functies om een oordeel op bedreigingsniveau te bevestigen. De URL Reputation Service heeft niet genoeg gegevens om een reputatie op te bouwen. Dit oordeel is niet geschikt voor acties in een URL Reputation beleid direct.

Aanbevolen actie: Scan de volgende machines om te controleren op andere mogelijk schadelijke inhoud.

Onbekende URL's of "geen reputatie" kunnen URL's zijn die nieuwe domeinen of URL's bevatten die weinig tot geen verkeer hebben gezien en die geen beoordeelde reputatie en oordeel op bedreigingsniveau kunnen hebben. Deze kunnen onbetrouwbaar als meer informatie wordt verkregen voor hun domein en oorsprong. Voor dergelijke URL's raadt Cisco een inhoudsfilter aan om te loggen of een filter dat de detectie van de onbekende URL bevat. Vanaf AsyncOS 14.2 worden onbekende URL's naar de Talos Intelligence Cloud Service gestuurd voor diepe URL-analyse die wordt geactiveerd op verschillende bedreigingsindicatoren. Bovendien geeft een e-maillogbestand van de onbekende URL('s) de beheerder een indicatie van de URL(s) die in een MID zijn opgenomen en mogelijke herstel met URL-bescherming. (Zie Hoe u Cisco Secure Email Account Settings voor Microsoft Azure (Microsoft 365) API - Cisco configureert voor meer informatie.)

Dit voorbeeld biedt context voor een inhoudsfilter voor URL-filtering om onbekende URL's te detecteren:

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 ===>>>")	

Met dit inhoudfilter scant Cisco Secure Email naar een URL met een *onbekende* reputatie en schrijft u een logregel in de mail_logs. Hier is een voorbeeld uit 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
```

De URL mytest.example.com/test_url_2022070503 heeft geen reputatie en wordt gezien met "noscore." Het URL_UNKNOWN inhoudsfilter schreef de logline zoals die aan mail_logs wordt gevormd.

Na een enquêtecyclus van de Cisco Secure Email Gateway naar de Talos Intelligence Cloud Service wordt de URL gescand en onbetrouwbaar bevonden. Dit is te zien in de ECS-logboeken op "Trace"-niveau:

```
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.
```

En vervolgens, in mail_logs, wanneer de sanering zelf wordt geroepen en voltooid:

```
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.
```

Beheerders moeten naar eigen goeddunken actie overwegen voor onbekende URL's. Als er een duidelijke toename is van Phish-gerelateerde e-mails en bijlagen, bekijk dan het mail_logs- en Content Filters rapport. Bovendien kunnen beheerders zo configureren dat onbekende URL's worden omgeleid naar de Cisco Security proxy-service voor een kliktijdevaluatie. In dit voorbeeld, navigeer om **Actie > URL Reputation** binnen onze URL_UNKNOWN inhoudsfilter toe te voegen:

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.