URL-Filterung für sicheres E-Mail-Gateway und Cloud-Gateway konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die URL-Filterung auf dem Cisco Secure Email Gateway und Cloud Gateway konfigurieren. Außerdem werden Best Practices für die Verwendung der URL-Filterung beschrieben.

Hintergrundinformationen

Die URL-Filterung wurde erstmals mit AsyncOS 11.1 für Email Security eingeführt. Mit dieser Version konnte Cisco Secure Email nach URLs in Nachrichtenanhängen suchen und konfigurierte Aktionen für diese Nachrichten ausführen. Nachrichten- und Content-Filter verwenden die URL-Reputation und die URL-Kategorie, um in Nachrichten und Anhängen nach URLs zu suchen. Weitere Informationen finden Sie in den Kapiteln "Verwenden von Nachrichtenfiltern zum Durchsetzen von E-Mail-Richtlinien", "Inhaltsfilter" und "Schutz vor nicht vertrauenswürdigen oder unerwünschten URLs" im Benutzerhandbuch oder in der Online-Hilfe.

Die Steuerung und der Schutz vor nicht vertrauenswürdigen oder unerwünschten Links sind Teil der Arbeitswarteschlange für Anti-Spam-, Outbreak-, Content- und Nachrichtenfilterungsprozesse. Diese Kontrollen:

- Erhöhen Sie die Effektivität des Schutzes vor nicht vertrauenswürdigen URLs in Nachrichten und Anhängen.
- Darüber hinaus ist die URL-Filterung in die Outbreak-Filter integriert. Dieser verstärkte Schutz ist auch dann anwendbar, wenn Ihr Unternehmen bereits über eine Cisco Web Security Appliance oder einen ähnlichen Schutz vor webbasierten Bedrohungen verfügt, da Bedrohungen am Eintrittspunkt blockiert werden.
- Sie können auch Inhalts- oder Nachrichtenfilter verwenden, um Maßnahmen basierend auf der webbasierten Reputationsbewertung (WBRS) von URLs in Nachrichten zu ergreifen. Sie können beispielsweise URLs mit neutraler oder unbekannter Reputation umschreiben, um sie per Mausklick an den Cisco Web Security Proxy weiterzuleiten und so ihre Sicherheit zu bewerten.
- Spam besser identifizieren
- Die Appliance verwendet Reputation und Linkkategorie in Nachrichten und andere Spam-Identifizierungsalgorithmen, um Spam zu identifizieren. Wenn beispielsweise ein Link in einer Nachricht zu einer Marketing-Website gehört, ist die Nachricht mit höherer Wahrscheinlichkeit eine Marketing-Nachricht.
- Unterstützung der Durchsetzung von Unternehmensrichtlinien zur akzeptablen Nutzung
- Die Kategorie der URLs (z. B. Adult Content oder Illegal Activities) kann mit Content- und Nachrichtenfiltern verwendet werden, um Richtlinien zur akzeptablen Unternehmensnutzung durchzusetzen.
- Ermöglicht Ihnen, Benutzer in Ihrer Organisation zu identifizieren, die am häufigsten auf eine URL in einer Nachricht geklickt haben, die zum Schutz neu geschrieben wurde, sowie auf Links, auf die am häufigsten geklickt wurde.

Anmerkung: In der Version AsyncOS 11.1 für Email Security wurde die Unterstützung für kurze URLs durch die URL-Filterung eingeführt. Mit dem CLI-Befehl "websecurityadvancedconfig" konnten die Shorttener-Dienste angezeigt und konfiguriert werden. Diese Konfigurationsoption wurde in AsyncOS 13.5 für Email Security aktualisiert. Nach dem Upgrade auf diese Version werden alle verkürzten URLs erweitert. Es gibt keine Option, die Erweiterung von verkürzten URLs zu deaktivieren. Aus diesem Grund empfiehlt Cisco mindestens AsyncOS 13.5 für Email Security, um die neuesten Schutzfunktionen für URLs bereitzustellen. Weitere Informationen finden Sie im Kapitel "Schutz vor bösartigen oder unerwünschten URLs" im Benutzerhandbuch oder in der Online-Hilfe sowie im CLI-Referenzhandbuch für AsyncOS für die Cisco Email Security Appliance.

Anmerkung: Für dieses Dokument wird AsyncOS 14.2 für Email Security für die bereitgestellten Beispiele und Screenshots verwendet.

Anmerkung: Cisco Secure Email bietet außerdem einen ausführlichen URL-Verteidigungsleitfaden unter docs.ces.cisco.com.

Voraussetzungen

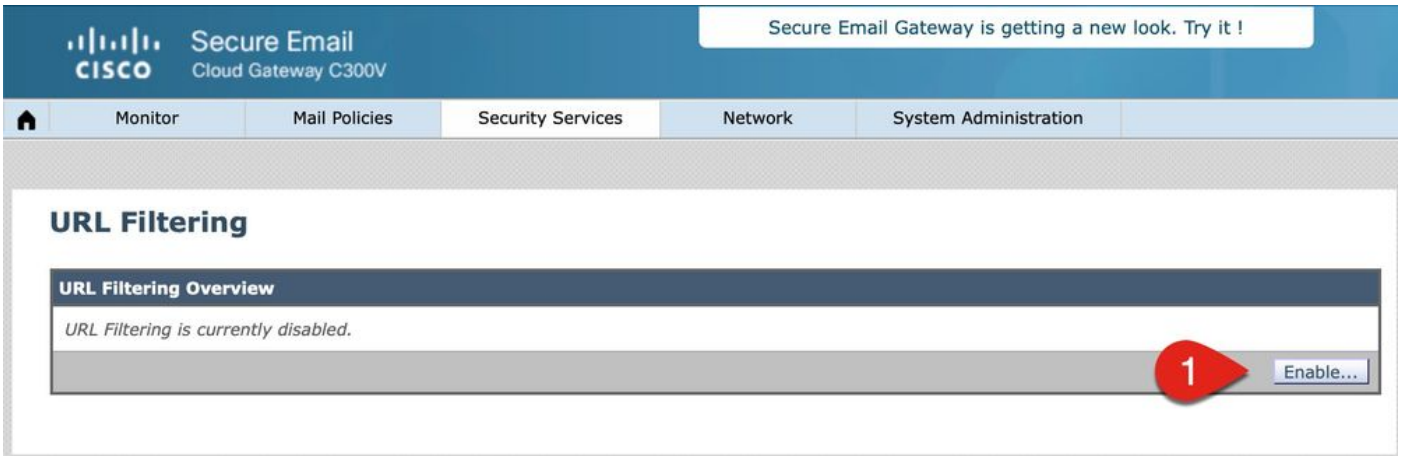
Wenn Sie die URL-Filterung auf dem Cisco Secure Email Gateway oder Cloud Gateway konfigurieren, müssen Sie je nach gewünschter Funktionalität auch andere Funktionen konfigurieren. Hier einige typische Funktionen, die zusammen mit der URL-Filterung aktiviert werden:

- Um einen besseren Schutz vor Spam zu gewährleisten, **muss** die Anti-Spam-Scan-Funktion **global** gemäß der entsprechenden Mail-Richtlinie **aktiviert werden**. Anti-Spam wird entweder als Cisco IronPort Anti-Spam (IPAS) oder Cisco Intelligent Multi-Scan (IMS) betrachtet.
- Um einen besseren Schutz vor Malware zu gewährleisten, **müssen** die Outbreak-Filter oder die VOF-Funktion (Virus-Outbreak-Filter) gemäß der entsprechenden E-Mail-Richtlinie **global aktiviert werden**.
- Für Aktionen, die auf der URL-Reputation basieren oder um mithilfe von Nachrichten- und Content-Filtern Richtlinien für die akzeptable Nutzung durchzusetzen, **muss** VOF **global aktiviert werden**.

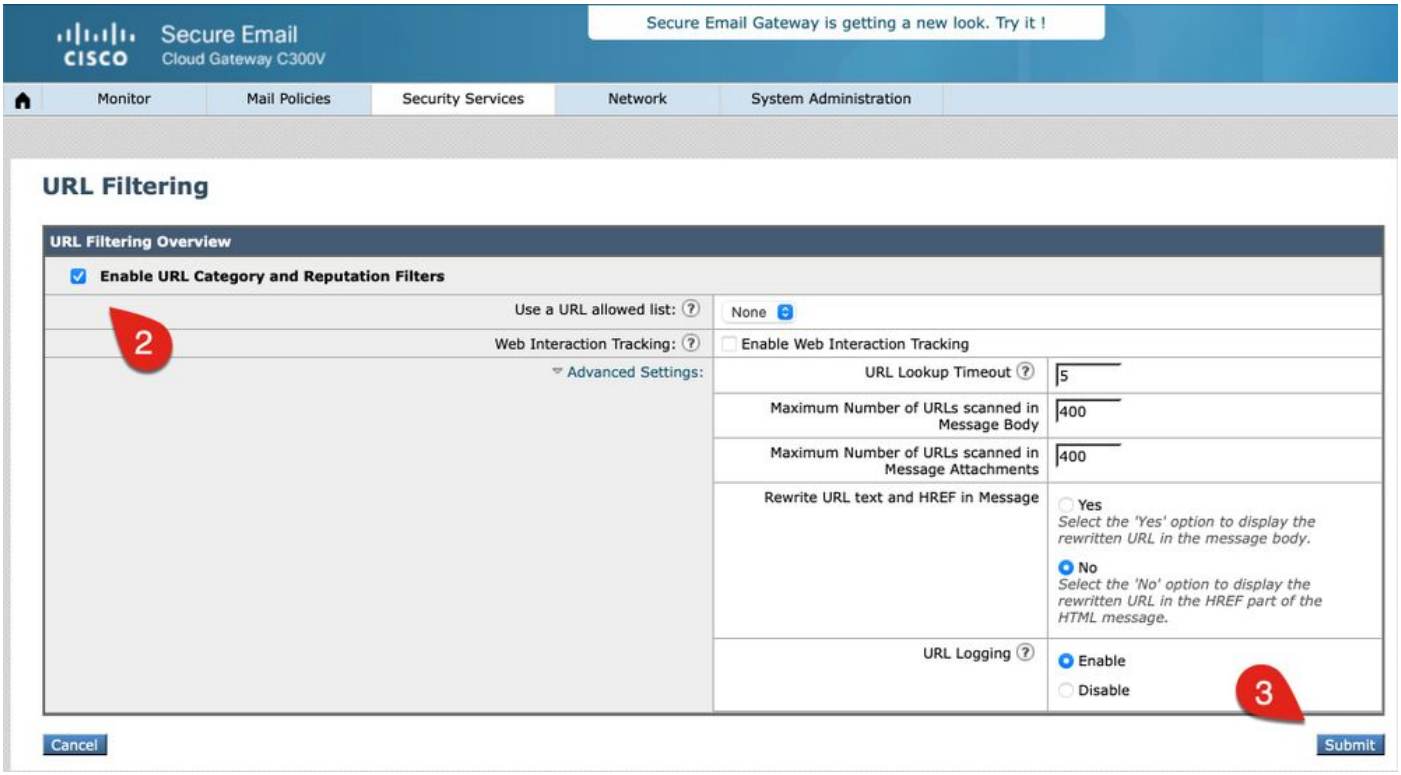
URL-Filterung aktivieren

Sie müssen diese Funktion zunächst aktivieren, um die URL-Filterung auf dem Cisco Secure Email Gateway oder Cloud Gateway zu implementieren. Die URL-Filterung kann vom Administrator über die GUI oder CLI aktiviert werden.

Um die URL-Filterung zu aktivieren, navigieren Sie von der GUI zu **Sicherheitsdienste > URL-Filterung,** und klicken Sie auf **Aktivieren:**



Klicken Sie anschließend auf **URL-Kategorie und Reputationsfilter aktivieren**. Dieses Beispiel enthält Best Practices-Werte für das Timeout für die URL-Suche und die maximale Anzahl der gescannten URLs. Außerdem wird die Option zum Protokollieren von URL(s) aktiviert:



Anmerkung: Stellen Sie sicher, dass Sie Ihre Änderungen an der Konfiguration **bestätigen**.

URL-Filterungsaktionen erstellen

Wenn Sie nur die URL-Filterung aktivieren, werden keine Maßnahmen gegen URLs in Nachrichten oder Nachrichten mit Anhängen ergriffen.

Die URL(s) in Nachrichten und Anhängen für Richtlinien für eingehende und ausgehende E-Mails werden ausgewertet. Jede gültige Zeichenfolge für eine URL wird so ausgewertet, dass sie Zeichenfolgen mit folgenden Komponenten enthält:

- HTTP, HTTPS oder WWW
- Domänen- oder IP-Adressen
- Portnummern, denen ein Doppelpunkt (:) voransteht
- Groß- oder Kleinbuchstaben

Anmerkung: Der URL-Protokolleintrag wird in mail_logs für die meisten URLs angezeigt. Wenn die URL nicht in mail_logs angemeldet ist, überprüfen Sie die Nachrichtenverfolgung für die Nachrichten-ID (MID). Die Nachrichtenverfolgung enthält eine Registerkarte für "URL-Details".

Wenn das System URLs auswertet, um festzustellen, ob es sich bei einer Nachricht um eine Spam-Nachricht handelt, werden eingehende Nachrichten gegenüber ausgehenden Nachrichten

priorisiert und überprüft.

Sie können Aktionen für Nachrichten ausführen, die auf der URL-Reputation oder der URL-Kategorie im Nachrichtentext oder auf Nachrichten mit Anhängen basieren.

Wenn Sie beispielsweise die Aktion **Drop (Final Action)** auf alle Nachrichten anwenden möchten, die URLs in der Kategorie Erwachsene enthalten, fügen Sie eine Bedingung vom Typ URL-Kategorie mit der ausgewählten Kategorie Erwachsene hinzu.

Wenn Sie keine Kategorie angeben, wird die ausgewählte Aktion auf alle Nachrichten angewendet.

Die Werte für die URL-Reputationsbewertung für Trusted, Favorable, Neutral, Questionable und Untrusted sind vordefiniert und können nicht bearbeitet werden. Sie können einen benutzerdefinierten Bereich angeben. Verwenden Sie "Unbekannt" für URLs, deren Reputationsbewertung noch nicht ermittelt wurde.

Um URLs schnell zu durchsuchen und Maßnahmen zu ergreifen, können Sie einen Content-Filter erstellen, sodass die Aktion angewendet wird, *wenn* die Nachricht eine gültige URL *hat*. Navigieren Sie in der GUI zu **Mail-Policys > Filter für eingehende Inhalte > Filter hinzufügen**.

URLs sind folgende Aktionen zugeordnet:

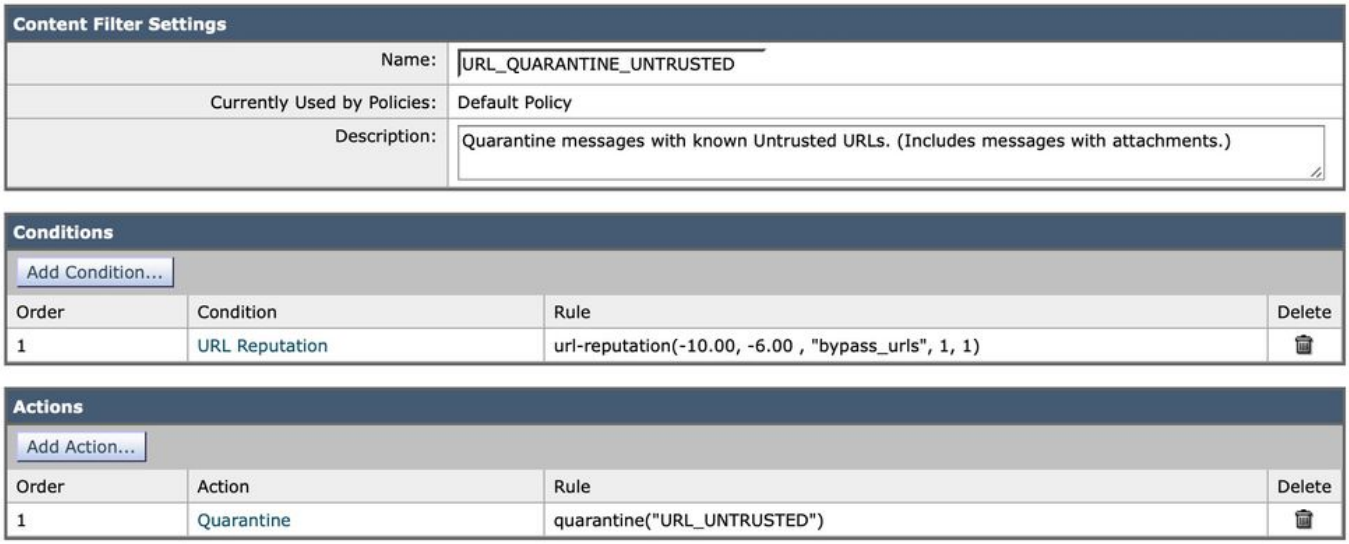
- Defang-URL Die URL wird so geändert, dass sie nicht mehr angeklickt werden kann, aber der Empfänger der Nachricht kann die beabsichtigte URL immer noch lesen. (In die ursprüngliche URL werden zusätzliche Zeichen eingefügt.)
- Umleitung zu Cisco Security Proxy Die URL wird neu geschrieben, wenn Sie darauf klicken, um sie zur weiteren Überprüfung an den Cisco Security Proxy weiterzuleiten. Laut Cisco Security Proxy-Urteil ist der Zugriff auf die Website für den Benutzer möglicherweise nicht möglich.
- URL durch eine Textnachricht ersetzen Mit dieser Option kann ein Administrator die URL in der Nachricht umschreiben und zur Remote-Browser-Isolierung extern senden.

Nicht vertrauenswürdige URL(s)

Nicht vertrauenswürdig: URL-Verhalten, das außergewöhnlich schlecht, schädlich oder unerwünscht ist. Dies ist der sicherste empfohlene Schwellenwert für Sperrlisten. Es kann jedoch vorkommen, dass Nachrichten nicht blockiert werden, da die URLs eine niedrigere Bedrohungsstufe aufweisen. Priorisierung der Bereitstellung gegenüber der Sicherheit.

Empfohlene Aktion: Blockieren. (Ein Administrator kann die Nachricht ganz in Quarantäne verschieben oder löschen.)

In diesem Beispiel wird der Kontext für einen Inhaltsfilter für die URL-Filterung bereitgestellt, um nicht vertrauenswürdige URLs zu erkennen:



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")	

Mit diesem Content-Filter sucht Cisco Secure Email nach einer URL mit einer *nicht vertrauenswürdigen* Reputation (-10,00 bis -6,00) und verschiebt die Nachricht in die Quarantäne: URL_UNTRUSTED. Hier ein Beispiel aus 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
```

Die URL ihaveabadreputation.com wird als **NICHT VERTRAUENSWÜRDIG** angesehen und mit

einer Bewertung von -9,5 bewertet. Die URL-Filterung hat die nicht vertrauenswürdige URL erkannt und in die Quarantäne verschoben: URL_UNTRUSTED.

Das vorherige Beispiel aus mail_logs bietet ein Beispiel, wenn NUR der Inhaltsfilter für die URL-Filterung für die Richtlinie für eingehende E-Mails aktiviert ist. Wenn für dieselbe Mail-Policy zusätzliche Services wie Anti-Spam aktiviert sind, geben die anderen Services an, ob die URL von diesen Services und ihren Regeln erkannt wurde. Im gleichen URL-Beispiel ist die Cisco Anti-Spam Engine (CASE) für die Richtlinie für eingehende E-Mails aktiviert, und der Nachrichtentext wird gescannt und als Spam-positiv eingestuft. Dies wird zuerst in mail_logs angegeben, da Anti-Spam der erste Dienst in der Mail-Verarbeitungspipeline ist. Content-Filter werden später in der E-Mail-Verarbeitungspipeline bereitgestellt:

```
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
```

Manchmal enthalten CASE- und IPAS-Regeln Regeln, Reputation oder Bewertungen, die mit einem bestimmten Absender, einer bestimmten Domäne oder einem bestimmten Nachrichteninhalt übereinstimmen, um nur URL-Bedrohungen zu erkennen. In diesem Beispiel wurde ihaveabadreputation.com mit Tags für die Spam-Quarantäne (ISQ) und die URL_UNTRUSTED-Quarantäne mit dem URL_QUARANTINE_UNTRUSTED-Inhaltsfilter angezeigt. Die Nachricht wird zuerst in die URL_UNTRUSTED-Quarantäne verschoben. Wenn die Nachricht von einem Administrator aus dieser Quarantäne freigegeben wurde oder die Zeitlimit-/Konfigurationskriterien von URL_UNTRUSTED erfüllt wurden, wird die Nachricht als Nächstes in

die ISQ verschoben.

Je nach den Voreinstellungen des Administrators können zusätzliche Bedingungen und Aktionen für den Content-Filter konfiguriert werden.

Unbekannte URL(s)

Unbekannt: Wurde nicht bereits evaluiert oder zeigt keine Funktionen an, die ein Urteil auf Bedrohungsebene bestätigen. Der URL-Reputationsdienst verfügt nicht über genügend Daten, um eine Reputation zu erstellen. Dieses Verdict eignet sich nicht für Aktionen in einer URL-Reputationsrichtlinie direkt.

Empfohlene Aktion: Scannen Sie das System mit nachfolgenden Engines, um nach anderen potenziell schädlichen Inhalten zu suchen.

Bei unbekannten URLs oder "ohne Reputation" kann es sich um URLs handeln, die neue Domänen oder URLs enthalten, bei denen wenig bis kein Datenverkehr aufgetreten ist und bei denen keine Reputation und kein Urteil über die Bedrohungsstufe vorliegen. Diese können nicht vertrauenswürdig sein, wenn weitere Informationen zu ihrer Domäne und ihrem Ursprung eingeholt werden. Für diese URL(s) empfiehlt Cisco einen Content-Filter zur Protokollierung oder einen, der die Erkennung der unbekannten URL umfasst. Ab AsyncOS 14.2 werden unbekannte URLs an den Talos Intelligence Cloud Service gesendet, um eine detaillierte URL-Analyse anhand verschiedener Bedrohungsindikatoren durchzuführen. Darüber hinaus kann der Administrator durch einen E-Mail-Protokolleintrag der unbekannten URL(s) feststellen, welche URL(s) in einer MID enthalten sind, und eine mögliche Problembehebung mit URL-Schutz vornehmen. (Weitere Informationen finden Sie unter Konfigurieren der Cisco Secure Email Account-Einstellungen für die Microsoft Azure (Microsoft 365)-API - Cisco.)

In diesem Beispiel wird der Kontext für einen Inhaltsfilter für die URL-Filterung bereitgestellt, um unbekannte URLs zu erkennen:

Mit diesem Content-Filter sucht Cisco Secure Email nach einer URL mit *unbekannter* Reputation

und schreibt eine Protokollzeile in mail_logs. Hier ein Beispiel aus 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
```

Die URL mytest.example.com/test_url_2022070503 hat keine Reputation und wird mit "noscore" angezeigt. Der URL_UNKNOWN-Inhaltsfilter hat die Protokollzeile wie konfiguriert in mail_logs geschrieben.

Nach einem Abfragezyklus vom Cisco Secure Email Gateway zum Talos Intelligence Cloud-Service wird die URL gescannt und als nicht vertrauenswürdig eingestuft. Dies ist in den ECS-Protokollen auf "Trace"-Ebene zu sehen:

```
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.
```

Und dann, in den mail_logs, wenn die Sanierung selbst aufgerufen und abgeschlossen wird:

```
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.
```

Administratoren müssen Maßnahmen für unbekannte URLs nach eigenem Ermessen in Betracht ziehen. Wenn die Anzahl der Phishing-E-Mails und -Anhänge zugenommen hat, lesen Sie den Bericht mail_logs und Content Filters (Inhaltsfilter). Darüber hinaus können Administratoren festlegen, dass unbekannte URLs zur Click-Time-Auswertung an den Cisco Security-Proxydienst umgeleitet werden. Navigieren Sie in diesem Beispiel zu **Add Action > URL Reputation** in unserem URL_UNKNOWN-Inhaltsfilter:

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.