

# Configurer le filtrage des URL pour la passerelle de messagerie sécurisée et la passerelle cloud

## Contenu

[Introduction](#)

[Informations générales](#)

[Conditions préalables](#)

[Activer le filtrage URL](#)

[Créer des actions de filtrage URL](#)

[URL non approuvées](#)

[URL\(s\) inconnue\(s\)](#)

[URL\(s\) douteuse\(s\)](#)

[URL\(s\) neutres](#)

[Suivi des messages](#)

[Signalement des URL non classées et mal classées](#)

[Les URL et les messages marketing malveillants ne sont pas interceptés par les filtres antisпам ou contre les attaques](#)

[Annexe](#)

[Activer la prise en charge du filtrage des URL raccourcies](#)

[Additional Information](#)

[Documentation de Cisco Secure Email Gateway](#)

[Documentation sur Secure Email Cloud Gateway](#)

[Documentation de Cisco Secure Email and Web Manager](#)

[Documentation produit Cisco Secure](#)

## Introduction

Ce document décrit comment configurer le filtrage d'URL sur Cisco Secure Email Gateway et Cloud Gateway et les meilleures pratiques d'utilisation du filtrage d'URL.

## Informations générales

Le filtrage des URL a été introduit pour la première fois avec [AsyncOS 11.1 pour la sécurité de la messagerie](#). Cette version a permis la configuration de Cisco Secure Email pour rechercher des URL dans les pièces jointes des messages et effectuer des actions configurées sur ces messages. Les filtres de messages et de contenu utilisent la réputation et la catégorie d'URL pour rechercher les URL dans les messages et les pièces jointes. Pour plus d'informations, reportez-vous aux chapitres « Utilisation des filtres de messages pour appliquer les stratégies de messagerie », « Filtres de contenu » et « Protection contre les URL non fiables ou indésirables » du [Guide de l'utilisateur](#) ou de l'aide en ligne.

Le contrôle et la protection contre les liens non fiables ou indésirables sont intégrés dans la file d'attente de travail pour les processus de filtrage des messages, des messages, du contenu, des attaques et des messages antisпам. Ces contrôles :

- Augmenter l'efficacité de la protection contre les URL non fiables dans les messages et les pièces jointes.
- En outre, le filtrage des URL est intégré aux filtres contre les attaques. Cette protection renforcée est applicable même si votre entreprise dispose déjà d'un appareil de sécurité Web Cisco ou d'une protection similaire contre les menaces Web, car elle bloque les menaces au point d'entrée.
- Vous pouvez également utiliser des filtres de contenu ou de message pour effectuer des actions en fonction du score de réputation Web (WBRS) des URL des messages. Par exemple, vous pouvez réécrire des URL de réputation neutre ou inconnue pour les rediriger vers le proxy de sécurité Web Cisco afin d'évaluer leur sécurité en un clic.
- Mieux identifier le spam
- La solution matérielle-logicielle utilise la réputation et la catégorie des liens dans les messages et d'autres algorithmes d'identification du spam pour identifier le spam. Par exemple, si un lien dans un message appartient à un site Web marketing, le message est plus susceptible d'être un message marketing.
- Soutenir l'application des politiques d'utilisation acceptable
- La catégorie d'URL (contenu pour adultes ou activités illégales, par exemple) peut être utilisée avec des filtres de contenu et de message pour appliquer des politiques d'utilisation d'entreprise acceptables.
- Permet d'identifier les utilisateurs de votre organisation qui ont cliqué le plus souvent sur une URL dans un message qui a été réécrit pour la protection et les liens sur lesquels vous avez cliqué le plus souvent.

**Note:** Dans la version [AsyncOS 11.1 for Email Security](#), le filtrage des URL a introduit la prise en charge des URL raccourcies. Avec la commande CLI « `websecurityadvancedconfig` », les services de raccourcissement peuvent être vus et configurés. Cette option de configuration a été mise à jour dans [AsyncOS 13.5 pour la sécurité du courrier électronique](#). Après la mise à niveau vers cette version, toutes les URL raccourcies sont développées. Il n'y a aucune option pour désactiver l'expansion des URL raccourcies. Pour cette raison, Cisco recommande AsyncOS 13.5 for Email Security ou version ultérieure pour fournir les dernières protections pour la défense des URL. Reportez-vous au chapitre « Protection contre les URL malveillantes ou indésirables » du guide de l'utilisateur ou de l'aide en ligne, ainsi qu'au guide de référence de l'interface de ligne de commande pour AsyncOS pour l'appliance de sécurité de la messagerie Cisco.

**Note:** Pour ce document, [AsyncOS 14.2 for Email Security](#) est utilisé pour les exemples et les captures d'écran fournis.

**Note:** Cisco Secure Email fournit également un [guide](#) détaillé de [défense des URL sur docs.ces.cisco.com](#).

## Conditions préalables

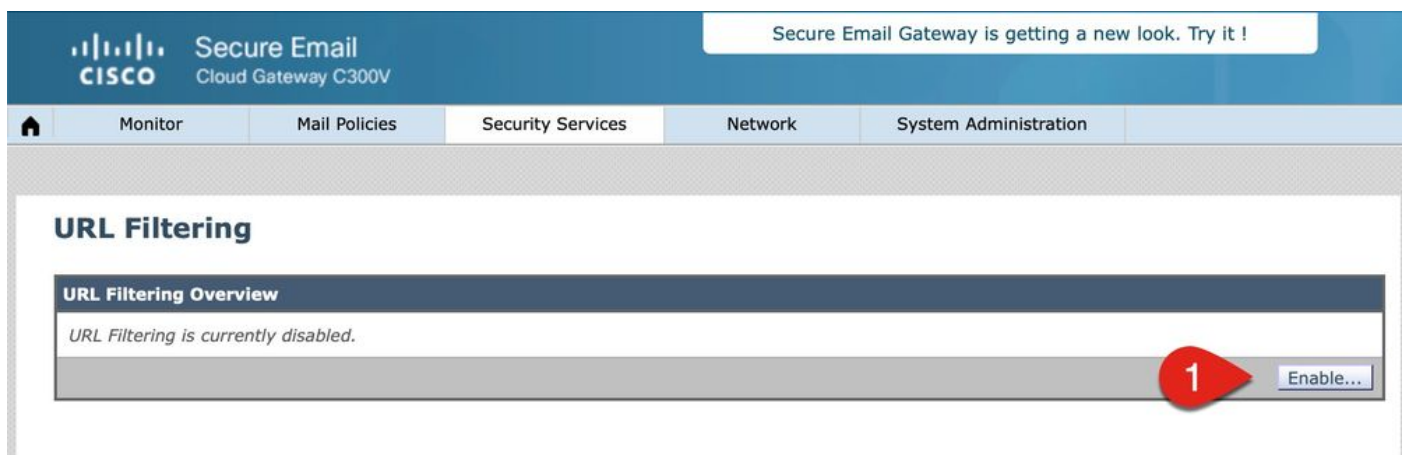
Lorsque vous configurez le filtrage des URL sur la passerelle de messagerie sécurisée Cisco ou sur la passerelle cloud, vous devez également configurer d'autres fonctionnalités en fonction de la fonctionnalité souhaitée. Voici quelques fonctionnalités typiques qui sont activées en parallèle au filtrage des URL :

- Pour une protection renforcée contre le spam, la fonction d'analyse antispam **doit être activée globalement** conformément à la politique de messagerie applicable. L'antispam est considéré comme étant la fonctionnalité Cisco IronPort Anti-Spam (IPAS) ou Cisco Intelligent Multi-Scan (IMS).
- Pour une protection renforcée contre les programmes malveillants, la fonction Filtres contre les attaques ou Filtres contre les attaques de virus (VOF) **doit être activée globalement**, conformément à la stratégie de messagerie applicable.
- Pour les actions basées sur la réputation d'URL ou pour appliquer des stratégies d'utilisation acceptables avec l'utilisation de filtres de messages et de contenu, VOF **doit être activé globalement**.

## Activer le filtrage URL

Vous devez d'abord activer la fonctionnalité pour implémenter le filtrage des URL sur la passerelle de messagerie sécurisée Cisco ou la passerelle cloud. Le filtrage des URL peut être activé par l'administrateur à partir de l'interface utilisateur graphique ou de la CLI.

Pour activer le filtrage d'URL, à partir de l'interface utilisateur graphique, accédez à **Services de sécurité > Filtrage d'URL** et cliquez sur **Enable** :



Cliquez ensuite sur **Enable URL Category and Reputation Filters**. Cet exemple inclut les valeurs des meilleures pratiques pour le délai de recherche d'URL, le nombre maximal d'URL analysées et active l'option de journalisation des URL :

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

Secure Email  
Cloud Gateway C300V

Monitor Mail Policies Security Services Network System Administration

## URL Filtering

**URL Filtering Overview**

Enable URL Category and Reputation Filters

Use a URL allowed list: ? None

Web Interaction Tracking: ?  Enable Web Interaction Tracking

Advanced Settings:

URL Lookup Timeout ? 5

Maximum Number of URLs scanned in Message Body 400

Maximum Number of URLs scanned in Message Attachments 400

Rewrite URL text and HREF in Message

Yes  
Select the 'Yes' option to display the rewritten URL in the message body.

No  
Select the 'No' option to display the rewritten URL in the HREF part of the HTML message.

URL Logging ?  Enable  Disable

Cancel Submit

**Note:** Assurez-vous de **valider** vos modifications dans la configuration à ce stade.

## Créer des actions de filtrage URL

Lorsque vous activez le filtrage des URL seul, il n'agit pas sur les URL des messages ou des messages avec pièces jointes.

Les URL incluses dans les messages et les pièces jointes pour les stratégies de messages entrants et sortants sont évaluées. Toute chaîne valide pour une URL est évaluée pour inclure des chaînes avec ces composants :

- HTTP, HTTPS ou WWW
- Domaine ou adresses IP
- Numéros de port précédés de deux-points (:)
- Lettres majuscules ou minuscules

**Note:** L'entrée du journal d'URL est visible depuis mail\_logs pour la plupart des URL. Si l'URL n'est pas consignée dans les journaux de messagerie, vérifiez le suivi des messages pour l'ID de message (MID). Le suivi des messages inclut un onglet pour « Détails URL ».

Lorsque le système évalue les URL pour déterminer si un message est un spam, si cela est nécessaire pour la gestion de la charge, il hiérarchise et filtre les messages entrants par rapport aux messages sortants.

Vous pouvez effectuer des actions sur les messages en fonction de la réputation d'URL ou de la catégorie d'URL dans le corps du message ou des messages avec pièces jointes.

Par exemple, si vous souhaitez appliquer l'action **Supprimer (action finale)** à tous les messages qui incluent des URL dans la catégorie Adulte, ajoutez une condition de type Catégorie d'URL avec la catégorie Adulte sélectionnée.

Si vous ne spécifiez pas de catégorie, l'action choisie est appliquée à tous les messages.

La plage de scores de réputation des URL pour les paramètres Approuvé, Favorable, Neutre, Questionable et Untrusted est prédéfinie et non modifiable. Vous pouvez spécifier une plage personnalisée. Utilisez « Inconnu » pour les URL pour lesquelles un score de réputation n'a pas encore été déterminé.

Pour analyser rapidement les URL et prendre des mesures, vous pouvez créer un filtre de contenu de sorte que *si* le message a une URL valide, *alors* l'action est appliquée. Dans l'interface graphique utilisateur, naviguez **Politiques de messagerie > Filtres de contenu entrant > Ajouter un filtre**.

Les actions associées aux URL sont les suivantes :

- URL de définition L'URL est modifiée pour qu'il soit impossible de cliquer dessus, mais le destinataire du message peut toujours lire l'URL souhaitée. (Des caractères supplémentaires sont insérés dans l'URL d'origine.)
- Rediriger vers Cisco Security Proxy L'URL est réécrite lorsque vous cliquez dessus pour passer par le proxy de sécurité Cisco pour une vérification supplémentaire. Selon le verdict du proxy de sécurité Cisco, le site peut être inaccessible pour l'utilisateur.
- Remplacer l'URL par un message texte Avec cette option, un administrateur peut réécrire l'URL dans le message et l'envoyer en externe pour l'isolation du navigateur distant.

## URL non approuvées

**Non approuvé** : Comportement d'URL exceptionnellement mauvais, malveillant ou indésirable. Il s'agit du seuil de liste de blocage recommandé le plus sûr ; cependant, il peut y avoir des messages qui ne sont pas bloqués parce que les URL qu'ils contiennent ont un niveau de menace plus faible. Priorise la livraison sur la sécurité.

**Action recommandée** : Block. (Un administrateur peut mettre le message en quarantaine ou le supprimer entièrement.)

Cet exemple fournit le contexte d'un filtre de contenu pour le filtrage des URL afin de détecter les URL non approuvées :

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			
<a href="#">Add Condition...</a>			
Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-10.00, -6.00 , "bypass_urls", 1, 1)	

Actions			
<a href="#">Add Action...</a>			
Order	Action	Rule	Delete
1	Quarantine	quarantine("URL_UNTRUSTED")	

Une fois ce filtre de contenu en place, Cisco Secure Email recherche une URL avec une réputation *non approuvée* (-10.00 à -6.00) et place le message dans une quarantaine, URL\_UNTRUSTED. Voici un exemple tiré 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
```

L'URL [ihaveabadreputation.com](https://www.ihaveabadreputation.com/) est considérée comme **NON FIABLE** et notée à **-9.5**. Le filtrage

d'URL a détecté l'URL non fiable et l'a mise en quarantaine à URL\_UNTRUSTED.

L'exemple précédent de mail\_logs fournit un exemple si SEUL le filtre de contenu pour le filtrage URL est activé pour la stratégie de courrier entrant. Si d'autres services sont activés pour la même stratégie de messagerie, par exemple l'antispam, les autres services indiquent si l'URL a été détectée à partir de ces services et de leurs règles. Dans le même exemple d'URL, Cisco Anti-Spam Engine (CASE) est activé pour la stratégie de courrier entrant, et le corps du message est analysé et déterminé comme étant du spam positif. Ceci est indiqué en premier dans mail\_logs car Anti-Spam est le premier service dans le pipeline de traitement du courrier. Les filtres de contenu viennent plus tard dans le pipeline de traitement du courrier :

```
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/XTLGFKD60hwnKKsghUKAMFOYVv9l32gncZX7879qf3FGzWfPlmc6ZH3iLMpcKwCBjXhmIg=
=
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
```

Il arrive que les règles CASE et IPAS contiennent des règles, une réputation ou des scores qui correspondent à un expéditeur, un domaine ou un contenu de message spécifique pour détecter les menaces d'URL uniquement. Dans cet exemple, ihaveabadreputation.com a été vu, marqué pour la quarantaine du spam (ISQ) et la quarantaine URL\_UNTRUSTED par le filtre de contenu URL\_QUARANTINE\_UNTRUSTED. Le message passe d'abord dans la quarantaine URL\_UNTRUSTED. Lorsque le message est libéré de cette quarantaine par un administrateur ou que les critères de limite de temps/configuration de la quarantaine URL\_UNTRUSTED sont satisfaits, il est ensuite déplacé vers la file d'attente d'informations de service.

Selon les préférences de l'administrateur, des conditions et actions supplémentaires peuvent être configurées pour le filtre de contenu.


## URL(s) inconnue(s)

**Inconnu** : Non évalué précédemment ou n'affiche pas les fonctionnalités permettant d'affirmer un verdict au niveau de la menace. Le service de réputation d'URL ne dispose pas de suffisamment de données pour établir une réputation. Ce verdict ne convient pas directement aux actions d'une stratégie de réputation d'URL.

**Action recommandée** : Analyser avec les moteurs suivants pour rechercher d'autres contenus potentiellement malveillants.

Les URL inconnues ou « sans réputation » peuvent être des URL qui contiennent de nouveaux domaines ou des URL qui ont peu ou pas vu de trafic et qui ne peuvent pas avoir une réputation évaluée et un verdict de niveau de menace. Ceux-ci peuvent devenir non approuvés lorsque davantage d'informations sont obtenues pour leur domaine et leur origine. Pour ces URL, Cisco recommande un filtre de contenu à enregistrer ou un filtre qui inclut la détection de l'URL inconnue. Depuis la version 14.2 d'AsyncOS, les URL inconnues sont envoyées au Talos Intelligence Cloud Service pour une analyse approfondie des URL déclenchée sur divers indicateurs de menace. En outre, une entrée de journal de messagerie des URL inconnues fournit à l'administrateur une indication des URL incluses dans un MID et une éventuelle correction avec la protection des URL. (Consultez [Comment configurer les paramètres de compte de messagerie sécurisée Cisco pour l'API Microsoft Azure \(Microsoft 365\) - Cisco](#) pour plus d'informations.)


Cet exemple fournit le contexte d'un filtre de contenu pour le filtrage des URL afin de détecter les URL inconnues :

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

Conditions			
<a href="#">Add Condition...</a>			
Order	Condition	Rule	Delete
1	URL Reputation	url-no-reputation("", 1, 1)	

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

Une fois ce filtre de contenu en place, Cisco Secure Email recherche une URL avec une réputation *inconnue* et écrit une ligne de journal dans mail\_logs. Voici un exemple tiré 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

```

L'URL [mytest.example.com/test\\_url\\_2022070503](http://mytest.example.com/test_url_2022070503) n'a pas de réputation et apparaît avec « noscore ». Le filtre de contenu URL\_UNKNOWN a écrit la ligne de connexion telle que configurée dans mail\_logs.

Après un cycle d'interrogation de Cisco Secure Email Gateway vers Talos Intelligence Cloud Service, l'URL est analysée et considérée comme non fiable. Ceci peut être vu dans les journaux ECS au niveau "Trace" :

```
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':
'8c6915e2ebbc9225ff8958db06db33beb4e932ae9e0d8c5b35805a2fxxyyxyy', 'message_details': '{"mid": 16,
"birth_time": "1657039913", "from_addr": ["test@test.com"], "recipients": ["■ ■ ■ ■ ■ ■ ■ ■"],
"delivery_status": 1, "remediation_req_status": 3}', 'created_at': '2022-07-05 16:52:42.04515',
'verdict': '{"url": "http://mytest.example.com/test_url_2022070503", "verdict": "MALICIOUS"}',
'message_uuid': 'e90dec74-f50b-4a63-9ab2-6adda4fcf422', 'message_id':
'<20220705165003.1870404@ip-127-0-0-1.internal>'}]
Tue Jul 5 16:55:42 2022 Debug: ECS: Remediation records: [
  [
    16,
    "<20220705165003.1870404@ip-127-0-0-1.internal>",
    1657039913,
    "delete",
    3,
    [{"url": "http://mytest.example.com/test_url_2022070503", "conviction_timestamp":
    "2022-07-05 16:52:42.04515", "url_hash":
    "8c6915e2ebbc9225ff8958db06db33beb4e932ae9e0d8c5b35805a2fxxyyxyy"}],
    [
      " ■ ■ ■ ■ ■ ■ ■ ■ "
    ],
    [
      "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.
```

Ensuite, dans les journaux de messagerie, lorsque la résolution elle-même est appelée et terminée :

```
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.
```

Les administrateurs doivent envisager des actions pour les URL inconnues à leur discrétion. Si le nombre d'e-mails et de pièces jointes associés au hameçonnage augmente, consultez le rapport mail\_logs et Content Filters. En outre, les administrateurs peuvent configurer de manière à ce que les URL inconnues soient redirigées vers le service proxy de sécurité Cisco pour l'évaluation du temps de clic. Dans cet exemple, naviguez jusqu'à **Add Action > URL Reputation** dans notre filtre de contenu URL\_UNKNOWN :



À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.