Configuration de la passerelle cloud Gold

Table des matières

Introduction

Ce document décrit une analyse approfondie de la configuration Gold fournie pour Cisco Secure Email Cloud Gateway.

Conditions préalables

Exigences

Cisco vous recommande de connaître les sujets suivants :

- Cisco Secure Email Gateway ou Cloud Gateway, administration de l'interface utilisateur et de l'interface de ligne de commande
- Cisco Secure Email and Web Manager, administration au niveau de l'interface utilisateur
- Les clients de Cisco Secure Email Cloud peuvent demander un accès CLI ; voir : Accès CLI (Command Line Interface)

Composants utilisés

Les informations contenues dans ce document proviennent de la configuration Gold et des meilleures pratiques recommandées pour les clients et les administrateurs de Cisco Secure Email Cloud.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Produits connexes

Ce document est également applicable avec :

- Cisco Secure Email Gateway sur site matériel ou appliance virtuelle
- Appareil virtuel et matériel sur site Cisco Secure Email and Web Manager

Quarantaines des stratégies

Les quarantaines sont configurées et gérées sur Email and Web Manager pour les clients Cisco Secure Email Cloud. Connectez-vous à votre gestionnaire de messagerie et Web pour afficher les quarantaines :

- PRISE_DE_COMPTE
- ANTI_USURPATION
- BLOC_PIÈCES JOINTES
- LISTE DE BLOCAGE
- ÉCHEC_DKIM
- DMARC_QUARANTINE

- DMARC_REJECT
- E-MAIL_FALSIFIÉ
- CONTENU_INAPPROPRIÉ
- MACRO
- RELAIS_OUVERT
- DONNÉES_SDR
- SPF_HARDFAIL
- SPF_SOFTFAIL
- TG_OUTBOUND_MALWARE
- URL_MALVEILLANTE

Configuration Gold de la passerelle cloud

Avertissement : toute modification apportée à une ou plusieurs configurations en fonction des meilleures pratiques décrites dans ce document doit être examinée et comprise avant de valider les modifications apportées à la configuration dans votre environnement de production. Veuillez consulter votre ingénieur Cisco CX, votre responsable de service désigné (DSM) ou votre équipe de compte avant de modifier la configuration.

Avant de commencer

La configuration Gold pour les clients du cloud Cisco Secure Email est la meilleure pratique et la configuration « zero-day » pour la passerelle cloud et Cisco Secure Email and Web Manager. Les déploiements Cisco Secure Email Cloud utilisent à la fois la ou les passerelles cloud et au moins un (1) gestionnaire de messagerie électronique et Web. Certaines parties de la configuration et des meilleures pratiques conseillent aux administrateurs d'utiliser les quarantaines situées sur le gestionnaire de messagerie et Web à des fins de gestion centralisée.

Configuration de base

Politiques de messagerie > Tableau d'accès aux destinataires (TAD)

Le tableau d'accès aux destinataires définit les destinataires acceptés par un écouteur public. Au minimum, la table spécifie l'adresse et indique si elle doit être acceptée ou rejetée. Vérifiez le TAD pour ajouter et gérer vos domaines selon les besoins.

Réseau > Routes SMTP

Si la destination de la route SMTP est Microsoft 365, consultez Office365 Throttling CES New

Instance with "4.7.500 Server busy. Veuillez réessayer ultérieurement".

Services de sécurité

Les services répertoriés sont configurés pour tous les clients Cisco Secure Email Cloud avec les valeurs fournies :

Antispam IronPort (IPAS)

- Activé et configuré Toujours analyser 1M et Jamais analyser 2M
- Délai d'attente pour l'analyse du message unique : 60 secondes

Filtrage des URL

- Activer la catégorisation des URL et les filtres de réputation
- (Facultatif) Créez et configurez la liste d'autorisation d'URL nommée « bypass_urls ».
- Activer le suivi des interactions Web
- Paramètres avancés :
  - Délai de recherche d'URL : 15 secondes
  - Nombre maximal d'URL analysées dans le corps et la pièce jointe : 400
  - Réécrire le texte et l'HREF de l'URL dans le message : Non
  - Journalisation des URL : activée
- (Facultatif) Depuis la version AsyncOS 14.2 pour Cloud Gateway, le verdict rétrospectif des URL et la correction des URL sont disponibles. Reportez-vous aux notes de version fournies et configurez le filtrage des URL pour Secure Email Gateway et Cloud Gateway

Détection Graymail

- Activer et configurer Toujours analyser 1M et Ne jamais analyser 2M
- Délai d'attente pour l'analyse du message unique : 60 secondes

Filtres contre les attaques

- Activer les règles adaptatives
- Taille maximale des messages à analyser : 2 millions
- Activer le suivi des interactions Web

Protection avancée contre les programmes malveillants > Analyse et réputation des fichiers

- Activer la réputation des fichiers
- Activer l'analyse des fichiers
  - Consultez les paramètres globaux pour passer en revue les types de fichiers pour l'analyse des fichiers

Suivi des messages

- Activer la consignation des connexions rejetées (si nécessaire)

Administration système

Utilisateurs (Administration système > Utilisateurs)

- N'oubliez pas de vérifier et de définir les stratégies de phrase de passe associées aux paramètres de compte d'utilisateur local et de phrase de passe
- Si possible, configurez et activez le protocole LDAP (Lightweight Directory Access Protocol) pour l'authentification (Administration système > LDAP)

Inscriptions au journal (Administration système > Inscriptions au journal)

- S'il n'est pas configuré, créez et activez :
  - Journaux de configuration
  - Journaux du client de réputation des URL
- Dans les paramètres globaux d'inscription au journal, modifiez les paramètres et ajoutez les en-têtes To, From, Reply-To, Sender.

Configuration supplémentaire (facultatif)

Services supplémentaires à examiner et à prendre en compte :

Administration système > LDAP

- Si vous configurez LDAP, Cisco recommande LDAP avec SSL activé

Défense des URL

- Consultez Configurer le filtrage des URL pour la passerelle de messagerie sécurisée et la passerelle cloud pour connaître les meilleures pratiques de configuration les plus récentes pour la défense des URL.
- Cisco étudie également en détail la défense contre les URL. Reportez-vous au Guide de défense contre les URL.
- Certains exemples inclus dans le Guide de défense contre les URL sont également incorporés dans ce document.

FPS

- Les enregistrements DNS SPF (Sender Policy Framework) sont créés en externe sur la passerelle cloud. Par conséquent, Cisco recommande vivement à tous les clients d'intégrer les meilleures pratiques SPF, DKIM et DMARC dans leur stratégie de sécurité. Pour plus d'informations sur la validation SPF, consultez Configuration SPF et Meilleures pratiques.
- Pour les clients Cisco Secure Email Cloud, une macro est publiée pour toutes les passerelles cloud par nom d'hôte d'allocation afin de faciliter l'ajout de tous les hôtes.
- Placez cette option avant ~all ou -all dans l'enregistrement DNS TXT (SPF) actuel, s'il existe :

```
exists:%{i}.spf.<allocation>.iphmx.com
```

✎ Remarque : assurez-vous que l'enregistrement SPF se termine par ~all ou -all. Validez les enregistrements SPF pour vos domaines avant et après toute modification !

- Informations et outils recommandés pour en savoir plus sur SPF :
  - Vérificateur d'enregistrement SPF - Recherche SPF gratuite (dmarcian.com)
  - Table de syntaxe d'enregistrement SPF - Tout SPF - dmarcian.com

Exemples SPF supplémentaires

- Un excellent exemple de SPF est la réception d'e-mails de votre Cloud Gateway et l'envoi d'e-mails sortants à partir d'autres serveurs de messagerie. Vous pouvez utiliser le mécanisme « a: » pour spécifier les hôtes de messagerie :

<#root>

```
v=spf1 mx a:mail01.yourdomain.com a:mail99.yourdomain.com ~
all
```

- Si vous envoyez uniquement des e-mails sortants via votre Cloud Gateway, vous pouvez utiliser :

<#root>

```
v=spf1 mx exists:%{i}.spf.<allocation>.iphmx.com ~
all
```

- Dans cet exemple, le mécanisme « ip4: » ou « ip6: » spécifie une adresse IP ou une plage d'adresses IP :

<#root>

```
v=spf1 exists:%{i}.spf.<allocation>.iphmx.com ip4:192.168.0.1/16
```

~all

Changements de niveau CLI

- Comme indiqué dans la section Conditions préalables, les clients de Cisco Secure Email Cloud peuvent demander un accès CLI ; reportez-vous à la section Accès à l'interface de ligne de commande (CLI).

Filtre Anti-Usurpation

- N'oubliez pas de consulter le Guide des meilleures pratiques pour l'anti-usurpation
- Ce guide fournit des exemples et des bonnes pratiques de configuration pour la prévention des usurpations de messagerie

Ajouter un filtre d'en-tête

- CLI uniquement, veuillez écrire et activer le filtre de message addHeaders :

```
addHeaders:  if (sendergroup != "RELAYLIST")
{
     insert-header("X-IronPort-RemoteIP", "$RemoteIP");
     insert-header("X-IronPort-MID", "$MID");
     insert-header("X-IronPort-Reputation", "$Reputation");
     insert-header("X-IronPort-Listener", "$RecvListener");
     insert-header("X-IronPort-SenderGroup", "$Group");
     insert-header("X-IronPort-MailFlowPolicy", "$Policy");
}
```

Table d’accès aux hôtes (Politiques de messagerie > Table d’accès aux hôtes (HAT))

Présentation de HAT > Groupes d'expéditeurs supplémentaires

- Guide de l'utilisateur ESA : Création d'un groupe d'expéditeurs pour la gestion des messages
  - BYPASS_SBRS - Placer plus haut pour les sources qui ignorent la réputation
  - MY_TRUSTED_SPOOF_HOSTS - Partie du filtre d'usurpation
  - TLS_REQUIRED - Pour les connexions TLS forcées

Dans le groupe d'expéditeurs SUSPECTLIST prédéfini

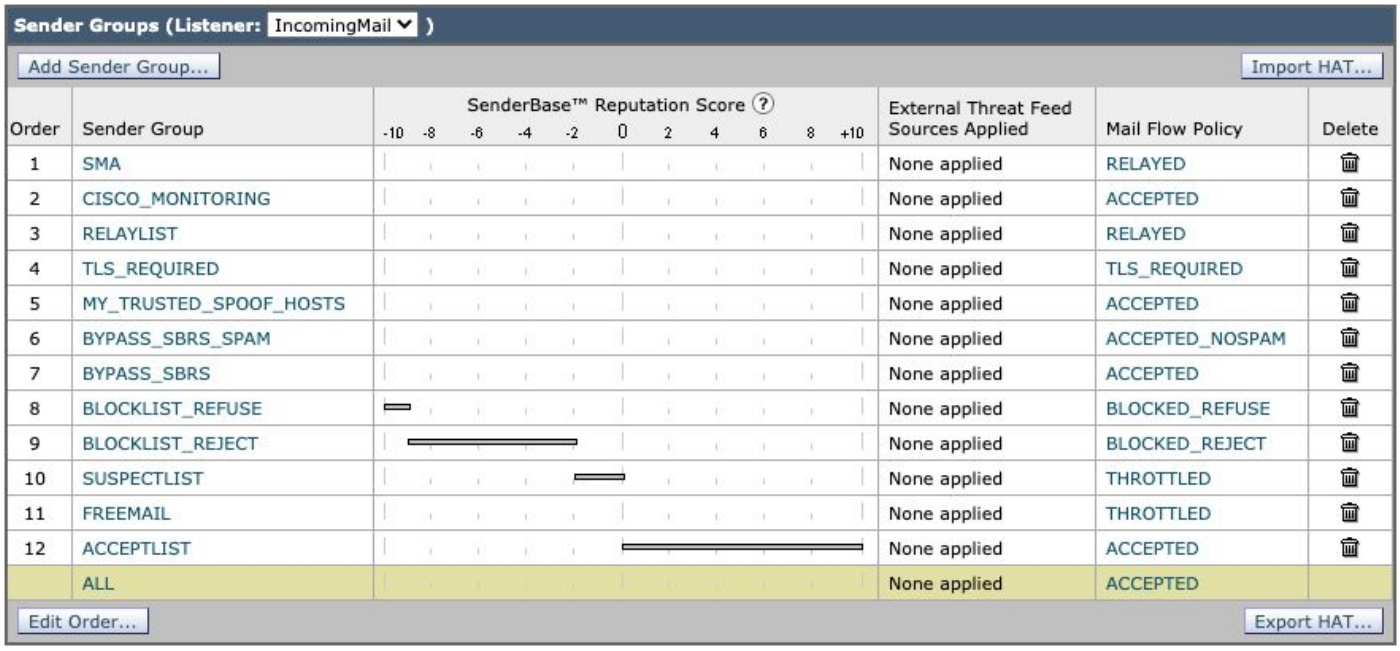
- Guide de l'utilisateur ESA : Vérification de l'expéditeur : Hôte
  - activer "Scores SBRS sur Aucun."
  - (Facultatif) enable "La recherche d'enregistrements PTR de l'hôte de connexion échoue en raison d'une défaillance DNS temporaire."

Échantillon HAT agressif

- POLITIQUE BLOCKLIST_REFUSE [-10.0 à -9.0] : BLOCKED_REFUSE
- POLITIQUE BLOCKLIST_REJECT [-9.0 à -2.0] : BLOCKED_REJECT
- SUSPECTLIST [-2.0 à 0.0 et scores SBRS de « Aucun »] POLITIQUE : LIMITÉE
- POLITIQUE ACCEPTLIST [0.0 à 10.0] : ACCEPTÉE

Remarque : les exemples HAT montrent des stratégies de flux de messages (MFP) configurées en plus. Pour obtenir des informations complètes sur MFP, reportez-vous à la section « Understanding the Email Pipeline > Incoming/Receiving » du Guide de l'utilisateur pour la version appropriée d'AsyncOS pour la passerelle de messagerie sécurisée Cisco que vous avez déployée.

Exemple HAT :



Stratégie de flux de messagerie (paramètres de stratégie par défaut)

Paramètres de stratégie par défaut

Paramètres de sécurité

- Définir la sécurité de la couche transport (TLS) sur favori
- Activer Sender Policy Framework (SPF)
- Activer la messagerie identifiée par les clés de domaine (DKIM)
- Activer la vérification de l'authentification des messages, des rapports et de la conformité (DMARC) basée sur le domaine et envoyer des rapports de commentaires agrégés

---

Remarque : DMARC nécessite des réglages supplémentaires pour être configuré. Pour plus d'informations sur DMARC, veuillez vous reporter à la section « Authentification de messagerie électronique > Vérification DMARC » dans le Guide de l'utilisateur pour la version appropriée d'AsyncOS pour la passerelle de messagerie sécurisée Cisco que vous avez déployée.

Stratégies de messages entrants

La stratégie par défaut est configurée comme suit :

Antispam

- Activé, avec les seuils restants aux seuils par défaut. (La modification de la notation peut augmenter le nombre de faux positifs.)

Antivirus

- Analyse des messages : analyse antivirus uniquement
  - assurez que la case « Inclure un en-tête X » est cochée
- Pour les messages non analysables et les messages infectés par un virus, définissez Archiver le message d'origine sur Non

AMPLI

- Pour les Actions non analysables sur les erreurs de message, utilisez Avancé et Ajouter un en-tête personnalisé au message, X-TG-MSGERROR, valeur : True.
- Pour les actions non analysables sur la limite de débit, utilisez Avancé et Ajouter un en-tête personnalisé au message, X-TG-RATELIMIT, valeur : True.
- Pour les messages dont l'analyse de fichier est en attente, utilisez Action appliquée au message : « Quarantaine ».

Graymail

- L'analyse est activée pour chaque verdict (Marketing, Social, Bulk), avec Prepend pour Add Text to Subject et l'action est Deliver.
- Pour Action on Bulk Mail, utilisez Advanced et Add Custom Header (facultatif) : X-Bulk, value

: True.

Filtres de contenu

- Enabled et URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPCIOUS, URL_INAPPROPRIATE, DKIM_FAILURE, SPF_HARDFAIL, EXECUTIVE_SPOOF, DOMAIN_SPOOF, SDR, TG_RATE_LIMIT sont sélectionnés
- Ces filtres de contenu sont fournis plus loin dans ce guide

Filtres contre les attaques

- Le niveau de menace par défaut est 3. Veuillez vous adapter à vos exigences de sécurité.
  - Si le niveau de menace d'un message est égal ou supérieur à ce seuil, le message passe dans la quarantaine des attaques. (1 = menace la plus faible, 5 = menace la plus élevée)
- Activer la modification des messages
- Jeu de réécriture d'URL pour « Activer pour tous les messages ».
- Modifier le préfixe de l'objet en : [Possible $threat_category Fraud]

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
1	BLOCKLIST	Disabled	Disabled	(use default)	Disabled	BLOCKLIST_QUARANTINE	Disabled	(use default)	
2	ALLOWLIST	Disabled	(use default)	(use default)	Disabled	(use default)	Disabled	(use default)	
3	ALLOW_SPOOF	(use default)	(use default)	(use default)	(use default)	URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE SDR	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine	Sophos McAfee Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop ...	File Reputation Malware File: Drop Pending Analysis: Quarantine Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not	Graymail Detection Unsubscribe: Disabled Marketing: Deliver Social: Deliver Bulk: Deliver ...	URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE DKIM_FAILURE SPF_HARDFAIL EXECUTIVE_SPOOF ...	Retention Time: Virus: 1 day Other: 4 hours	Not Available	

Noms des stratégies (affichés)

- Stratégie de messagerie BLOCKLIST

  La stratégie de messagerie BLOCKLIST est configurée avec tous les services désactivés, à l'exception d'Advanced Malware Protection, et établit un lien vers un filtre de contenu avec l'action de QUARANTINE.

- Stratégie de messagerie ALLOWLIST

  La stratégie de messagerie ALLOWLIST a les options Antispam, Graymail désactivé et Filtres de contenu activés pour URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, DKIM_FAILURE, SPF_HARDFAIL, EXECUTIVE SPOOF, DOMAIN_SPOOF, SDR, TG_RATE_LIMIT ou les filtres de contenu de votre choix et de votre configuration.

- Politique de messagerie ALLOW_SPOOF

La stratégie de messagerie ALLOW_SPOOF a tous les services par défaut activés, avec les filtres de contenu activés pour les filtres URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, SDR ou de contenu de votre choix et de votre configuration.

Stratégies de messages sortants

La stratégie par défaut est configurée comme suit :

Antispam

- Désactivé

Antivirus

- Analyse des messages : analyse antivirus uniquement
  - désactivez la case à cocher « Inclure un en-tête X ».
- (Facultatif) Pour tous les messages : Avancé > Autre notification, activez « Autres » et indiquez votre adresse e-mail de contact admin/SOC

Protection avancée contre les malwares

- Activer la réputation des fichiers uniquement
- Actions non analysables sur la limite de débit : utilisez Avancé et Ajouter un en-tête personnalisé au message : X-TG-RATELIMIT, valeur : "True".
- Messages avec pièces jointes de programme malveillant : utilisez Advanced et Add Custom Header to Message : X-TG-OUTBOUND, valeur : "MALWARE DETECTED."

Graymail

- Désactivé

Filtres de contenu

- Activé et TG_OUTBOUND_MALICIOUS, Strip_Secret_Header, EXTERNAL_SENDER_REMOVE, ACCOUNT_TAKEOVER ou les filtres de contenu de votre choix sont sélectionnés.

Filtres contre les attaques

- Désactivé

DLP

- Activez, en fonction de votre licence DLP et de votre configuration DLP.

Autres paramètres

Dictionnaires (Politiques De Messagerie > Dictionnaires)

- Activer et vérifier le dictionnaire Profanity et Sexual_Content
- Créer un dictionnaire Executive_FED pour la détection des e-mails falsifiés avec tous les noms de dirigeants
- Créez des dictionnaires supplémentaires pour les mots-clés restreints ou autres, selon les besoins de vos stratégies, de votre environnement et de votre contrôle de sécurité

Contrôles de destination (Politiques de messagerie > Contrôles de destination)

- Pour le domaine par défaut, configurez la prise en charge TLS comme Préféré
- Vous pouvez ajouter des destinations pour les domaines de messagerie Web et définir des seuils inférieurs
- Consultez notre guide Rate Limit Your Outbound Mail with Destination Control Settings pour plus d'informations.

Destination Control Table — Items per page: 20

Add Destination... | Import Table

Domain	IP Address Preference	Destination Limits	TLS Support	DANE Support ^	Bounce Verification *	Bounce Profile	All Delete
.protection.outlook.com	Default	500 concurrent connections, 50 messages per connection, Default recipient limit	Required	Default	Default	Default	
gmail.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	
hotmail.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	
yahoo.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	
Default	IPv4 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	Preferred	None	Off	Default	

Export Table | Delete

** Bounce Verification settings apply only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.*
^ DANE will not be enforced for domains that have SMTP Routes configured.

Filtres de contenu

Remarque : pour plus d'informations sur les filtres de contenu, reportez-vous à la section « Filtres de contenu » du Guide de l'utilisateur pour connaître la version appropriée d'AsyncOS pour la passerelle de messagerie sécurisée Cisco que vous avez déployée.

Filtres de contenu entrant

URL_QUARANTAINE_MALVEILLANTE

Condition : Réputation d'URL ; url-reputation(-10.00, -6.00, "bypass_urls", 1, 1)

Action : Quarantaine : quarantine("URL_MALICIOUS")

URL_REWRITE_SUSPECT

Condition : Réputation d'URL ; url-reputation(-5.90, -5.60, "bypass_urls", 0, 1)

Action : Réputation d'URL ; url-reputation-proxy-redirect(-5.90, -5.60,"",0)

URL_INAPPROPRIÉE

Condition : URL Category ; url-category (['Adulte', 'Contenu pédopornographique', 'Extrême', 'Discours haineux', 'Activités illégales', 'Téléchargements illégaux', 'Drogues illégales', 'Pornographie', 'Évitement de filtre'], "bypass_urls", 1, 1)

Action : quarantaine ; duplicata-quarantine("INAPPROPRIATE_CONTENT")

ÉCHEC_DKIM

Condition : Authentification DKIM ; dkim-authentication == hardfail

Action : Quarantaine ; duplicate-quarantine("DKIM_FAIL")

SPF_HARDFAIL

Condition : vérification SPF ; état spf == échec

Action : Quarantaine ; duplicate-quarantine("SPF_HARDFAIL")

SPOOF_EXÉCUTIF

Condition : Détection des e-mails falsifiés ; forged-email-detection("Executive_FED", 90, "")

Condition : Autre en-tête ; header("X-IronPort-SenderGroup") != "(?i)allowspoof"

* set Apply rule : uniquement si toutes les conditions correspondent

Action : Ajouter/Modifier un en-tête ; edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1")

Action : Quarantaine ; duplicata-quarantine("FORGED_EMAIL")

DOMAINE_USURPATION

Condition : Autre en-tête ; header("X-Spoof")

Action : Quarantaine ; duplicate-quarantine("ANTI_SPOOF")

DTS

Condition : Réputation de domaine ; sdr-reputation (['awful'], "")

Condition : Réputation de domaine ; sdr-age ("days", <, 5, "")

* set Apply rule : si une ou plusieurs conditions correspondent

Action : Quarantaine ; duplicate-quarantine("SDR_DATA")

LIMITE_VITESSE_TG

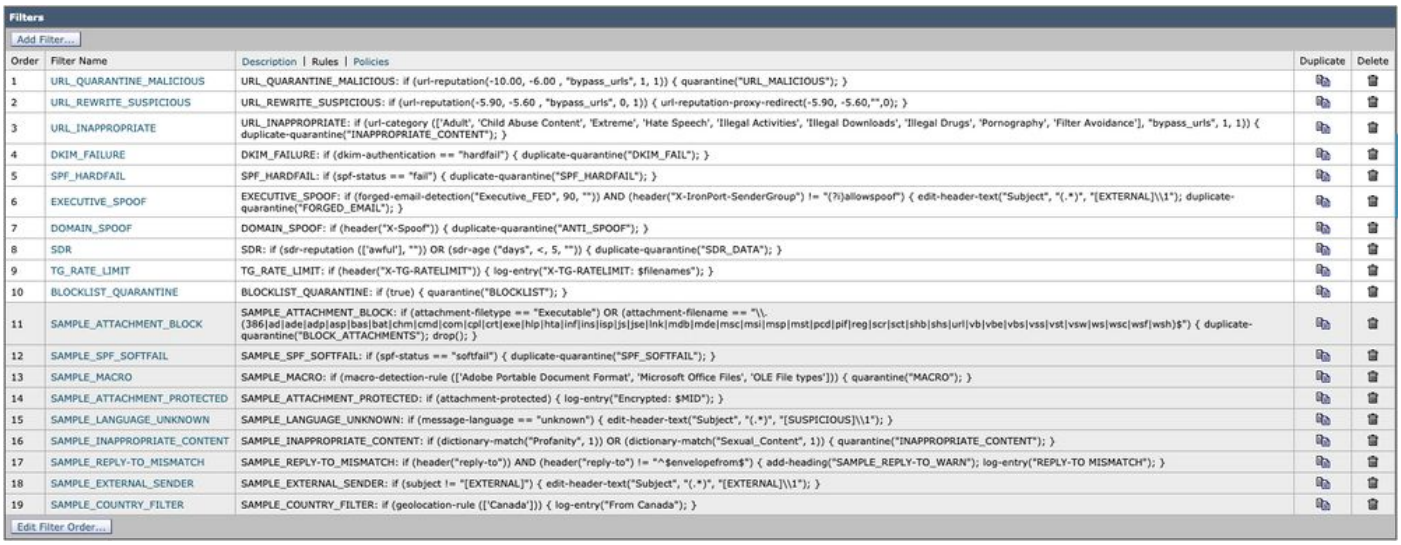
Condition : Autre en-tête ; header("X-TG-RATELIMIT")

Action : Ajouter une entrée de journal ; log-entry("X-TG-RATELIMIT: $filenames")

BLOCKLIST_QUARANTINE

Condition : (Aucun)

Action : Quarantaine ; quarantine("BLOCKLIST")



Filters

Add Filter...

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	URL_QUARANTINE_MALICIOUS	URL_QUARANTINE_MALICIOUS: if (url-reputation(-10.00, -6.00 , "bypass_urls", 1, 1)) { quarantine("URL_MALICIOUS"); }		
2	URL_REWRITE_SUSPICIOUS	URL_REWRITE_SUSPICIOUS: if (url-reputation(-5.90, -5.60 , "bypass_urls", 0, 1)) { url-reputation-proxy-redirect(-5.90, -5.60,"",0); }		
3	URL_INAPPROPRIATE	URL_INAPPROPRIATE: if (url-category (['Adult', 'Child Abuse Content', 'Extreme', 'Hate Speech', 'Illegal Activities', 'Illegal Downloads', 'Illegal Drugs', 'Pornography', 'Filter Avoidance'], "bypass_urls", 1, 1)) { duplicate-quarantine("INAPPROPRIATE_CONTENT"); }		
4	DKIM_FAILURE	DKIM_FAILURE: if (dkim-authentication == "hardfail") { duplicate-quarantine("DKIM_FAIL"); }		
5	SPF_HARDFAIL	SPF_HARDFAIL: if (spf-status == "fail") { duplicate-quarantine("SPF_HARDFAIL"); }		
6	EXECUTIVE_SPOOF	EXECUTIVE_SPOOF: if (forged-email-detection("Executive_FED", 90, "")) AND (header("X-IronPort-SenderGroup") != "(?i)allowspoof") { edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1"); duplicate-quarantine("FORGED_EMAIL"); }		
7	DOMAIN_SPOOF	DOMAIN_SPOOF: if (header("X-Spoof")) { duplicate-quarantine("ANTI_SPOOF"); }		
8	SDR	SDR: if (sdr-reputation (['awful'], "")) OR (sdr-age ("days", <, 5, "")) { duplicate-quarantine("SDR_DATA"); }		
9	TG_RATE_LIMIT	TG_RATE_LIMIT: if (header("X-TG-RATELIMIT")) { log-entry("X-TG-RATELIMIT: $filenames"); }		
10	BLOCKLIST_QUARANTINE	BLOCKLIST_QUARANTINE: if (true) { quarantine("BLOCKLIST"); }		
11	SAMPLE_ATTACHMENT_BLOCK	SAMPLE_ATTACHMENT_BLOCK: if (attachment-filetype == "Executable") OR (attachment-filename == "\\.(386|ad|ade|adp|asp|bas|bat|chm|cmd|com|cpl|crt|exe|hlp|hta|inf|ins|isp|js|jse|lnk|mdb|mde|msc|msi|msp|mst|pcd|pif|reg|scr|sct|shb|shs|url|vb|vbe|vbs|vss|vst|vsw|ws|wsc|wsf|wsh)$") { duplicate-quarantine("BLOCK_ATTACHMENTS"); drop(); }		
12	SAMPLE_SPF_SOFTFAIL	SAMPLE_SPF_SOFTFAIL: if (spf-status == "softfail") { duplicate-quarantine("SPF_SOFTFAIL"); }		
13	SAMPLE_MACRO	SAMPLE_MACRO: if (macro-detection-rule (['Adobe Portable Document Format', 'Microsoft Office Files', 'OLE File types'])) { quarantine("MACRO"); }		
14	SAMPLE_ATTACHMENT_PROTECTED	SAMPLE_ATTACHMENT_PROTECTED: if (attachment-protected) { log-entry("Encrypted: $MID"); }		
15	SAMPLE_LANGUAGE_UNKNOWN	SAMPLE_LANGUAGE_UNKNOWN: if (message-language == "unknown") { edit-header-text("Subject", "(.*)", "[SUSPICIOUS]\\1"); }		
16	SAMPLE_INAPPROPRIATE_CONTENT	SAMPLE_INAPPROPRIATE_CONTENT: if (dictionary-match("Profanity", 1)) OR (dictionary-match("Sexual_Content", 1)) { quarantine("INAPPROPRIATE_CONTENT"); }		
17	SAMPLE_REPLY-TO_MISMATCH	SAMPLE_REPLY-TO_MISMATCH: if (header("reply-to")) AND (header("reply-to") != "^$envelopefrom$") { add-heading("SAMPLE_REPLY-TO_WARN"); log-entry("REPLY-TO MISMATCH"); }		
18	SAMPLE_EXTERNAL_SENDER	SAMPLE_EXTERNAL_SENDER: if (subject != "[EXTERNAL]") { edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1"); }		
19	SAMPLE_COUNTRY_FILTER	SAMPLE_COUNTRY_FILTER: if (geolocation-rule (['Canada'])) { log-entry("From Canada"); }		

Edit Filter Order...

Filtres de contenu sortant

TG_OUTBOUND_MALICIOUS

Condition : Autre en-tête ; header("X-TG-OUTBOUND") == MALWARE

Action : Quarantaine ; quarantaine("TG_OUTBOUND_MALWARE")

En-tête_secret_dépouille

Condition : Autre en-tête ; header("PLACEHOLDER") == PLACEHOLDER

Action : en-tête de bande ; strip-header("X-IronPort-Tenant")

EXTERNAL_SENDER_REMOVE

Condition : (Aucun)

Action : Ajouter/Modifier un en-tête ; edit-header-text("Subject", "\\[EXTERNAL\\]\\s ?", "")

PRISE_DE_COMPTE

Condition : Autre en-tête ; en-tête("X-AMP-Result") == (?i)malveillant

Condition : Réputation d'URL ; url-reputation(-10.00, -6.00, "", 1, 1)

*Définir la règle d'application : si une ou plusieurs conditions correspondent

Action : Notify;notify ("<Insérer l'adresse e-mail de l'administrateur ou du distributeur>", "POSSIBLE ACCOUNT TAKEOVER", "", "ACCOUNT_TAKEOVER_WARNING")

Action : duplicate-quarantine("ACCOUNT_TAKEOVER")

Filters

Add Filter...

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	Stop_O365_OpenRelay	Stop_O365_OpenRelay: if (header("X-IronPort-Tenant") != "placeholder") { duplicate-quarantine("OPEN_RELAY"); }		
2	TG_OUTBOUND_MALICIOUS	TG_OUTBOUND_MALICIOUS: if (header("X-TG-OUTBOUND") == "MALWARE") { quarantine("TG_OUTBOUND_MALWARE"); }		
3	Strip_Secret_Header	Strip_Secret_Header: if (header("PLACEHOLDER") == "PLACEHOLDER") { strip-header("X-IronPort-Tenant"); }		
4	EXTERNAL_SENDER_REMOVE	EXTERNAL_SENDER_REMOVE: if (true) { edit-header-text("Subject", "\\[EXTERNAL\\]\\s?", ""); }		
5	ACCOUNT_TAKEOVER	ACCOUNT_TAKEOVER: if (header("X-AMP-Result") == "(?i)malicious") OR (url-reputation(-10.00, -6.00 , "", 1, 1)) { notify ("myit@mycompany.com", "POSSIBLE ACCOUNT TAKEOVER", "", "ACCOUNT_TAKEOVER_WARNING"); duplicate-quarantine("ACCOUNT_TAKEOVER"); }		
6	ENCRYPT_OUT	ENCRYPT_OUT: if (subject == "(?i)*encrypt*") { edit-header-text("Subject", "(?i)*encrypt*\\s?", ""); encrypt-deferred ("CRES_HIGH", "$Subject", 0); }		
7	TG_RATE_LIMIT	TG_RATE_LIMIT: if (header("X-TG-OUTBOUND-RATELIMIT")) { tag-message ("NOOP"); }		

Edit Filter Order...

Pour les clients Cisco Secure Email Cloud, nous proposons des exemples de filtres de contenu inclus dans la configuration Gold et des recommandations de meilleures pratiques. En outre, veuillez consulter les filtres « SAMPLE_ » pour plus d'informations sur les conditions et les actions associées qui peuvent être bénéfiques dans votre configuration.

Cisco Live

Cisco Live héberge de nombreuses sessions dans le monde entier et propose des sessions en personne et des sessions techniques qui couvrent les meilleures pratiques de sécurisation de la messagerie électronique Cisco. Pour accéder aux sessions précédentes, rendez-vous sur Cisco Live (connexion CCO requise) :

- Sécurité de la messagerie électronique Cisco : bonnes pratiques et réglage fin - BRKSEC-2131

- DMARCate Your Email Perimeter - BRKSEC-2131
- Réparation du courrier électronique ! - Dépannage avancé de la sécurité de la messagerie Cisco - BRKSEC-3265
- Intégrations d'API pour la sécurité de la messagerie Cisco - DEVNET-2326
- Sécurisation des services de messagerie SaaS avec la sécurité de messagerie cloud de Cisco - BRKSEC-1025
- Sécurité de la messagerie électronique : bonnes pratiques et réglage fin - TECSEC-2345
- 250 Pas d'accord - Passez à la défensive avec Cisco Email Security - TECSEC-2345
- Cisco Domain Protection et Cisco Advanced Phishing Protection : exploitez pleinement la nouvelle couche de sécurité de la messagerie ! - BRKSEC-1243
- SPF n'est pas un acronyme pour "Spoof" ! Tirons le meilleur parti de la couche suivante de

la sécurité de la messagerie ! - DGTL-BRKSEC-2327

Si une session n'est pas disponible, Cisco Live se réserve le droit de la supprimer en raison de l'âge de la présentation.

Additional Information

Documentation de Cisco Secure Email Gateway

- notes de version
- Guide de l'utilisateur
- Guide de référence CLI
- Guides de programmation d'API pour Cisco Secure Email Gateway
- Open Source utilisé dans Cisco Secure Email Gateway
- Guide d'installation de l'appliance virtuelle de sécurité du contenu Cisco (inclut vESA)

Documentation sur Secure Email Cloud Gateway

- notes de version
- Guide de l'utilisateur

Documentation de Cisco Secure Email and Web Manager

- Notes de version et matrice de compatibilité
- Guide de l'utilisateur
- Guides de programmation API pour Cisco Secure Email and Web Manager
- Guide d'installation de l'appliance virtuelle de sécurité du contenu Cisco (inclut vSMA)

Documentation sur les produits Cisco Secure

- Architecture d'attribution de noms Cisco Secure

Informations connexes

- Conformité Cisco Secure Email Security
- Description de l'offre : e-mail sécurisé
- Conditions relatives au cloud universel Cisco
- Assistance et téléchargements Cisco
- [EXTERNE] OpenSPF : informations de base et avancées sur SPF

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.