クラウドゲートウェイゴールド設定の設定

内容

概要

このドキュメントでは、Cisco Secure Email Cloud Gatewayに提供されるゴールド設定の詳細な分析について説明します。Cisco Secure Emailクラウドのお客様向けのゴールド構成は、クラウドゲートウェイとCisco Secure Email and Web Managerの両方に対するベストプラクティスであり、ゼロデイ構成です。Cisco Secure Email Cloudの導入では、クラウドゲートウェイと少なくとも1つのEメールおよびWeb Managerの両方を使用します。設定およびベストプラクティスの一部では、管理者はEメールおよびWeb Managerにある検疫を使用して一元管理を行います。

前提条件

要件

次の項目について理解しておくことをお勧めします。

- Cisco Secure Email GatewayまたはCloud Gateway（UI管理とCLI管理の両方）
- Cisco Secure Email Email and Web Manager、UIレベル管理
- Cisco Secure Email Cloudのお客様はCLIアクセスをリクエストできます。次を参照してください。コマンドラインインターフェイス(CLI)アクセス

使用するコンポーネント

このドキュメントの情報は、Cisco Secure Email Cloudのお客様と管理者に対するゴールド設定とベストプラクティスの推奨事項に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

関連製品

このドキュメントは、次の製品にも適用できます。

- Cisco Secure Email Gatewayオンプレミスのハードウェアまたは仮想アプライアンス
- Cisco Secure Email and Web Managerオンプレミスハードウェアおよび仮想アプライアンス

ポリシー隔離領域

隔離は、Cisco Secure Email Cloudのお客様向けのEmail and Web Managerで設定および維持されます。EメールおよびWebマネージャに口グインして、検疫を表示してください。

- ACCOUNT_TAKEOVER
- ANTI_SPOOF
- BLOCK_ATTACHMENTS
- ブロックリスト
- DKIM_FAIL
- DMARC_QUARANTINE
- DMARC_REJECT
- FORGED_EMAIL
- 不適切なコンテンツ

- マクロ
- OPEN_RELAY
- SDR_DATA
- SPF_HARDFAIL
- SPF_SOFTFAIL
- TG_OUTBOUND_MALWARE
- URL_MALICIOUS

クラウドゲートウェイゴールド設定

> **警告**：このドキュメントで提供されているベストプラクティスに基づいて設定を変更する場合は、実稼働環境で設定の変更をコミットする前に、変更を確認して理解する必要があります。設定を変更する前に、Cisco CXエンジニア、Designated Service Manager(DSM)、またはアカウントチームにお問い合わせください。

基本設定

[Mail Policies] > [Recipient Access Table (RAT)]

受信者アクセステーブルは、パブリックリスナーが受け入れる受信者を定義します。少なくとも、テーブルはアドレスと、それを受け入れるか拒否するかを指定します。必要に応じてドメインを追加および管理するには、RATを確認してください。

[Network] > [SMTP Routes]

SMTPルートの宛先がMicrosoft 365の場合は、「4.7.500 Server busy."Please try again later"".""

セキュリティ サービス

記載されているサービスは、Cisco Secure Email Cloudのすべてのお客様に対して、次の値で設定されています。

IronPort Anti-Spam（IPAS）

- [Always scan 1M]および[Never scan 2M]を有効にして設定します。
- 単一メッセージのスキャンのタイムアウト：60 秒

URL フィルタリング

- URL分類およびレピュテーションフィルタの有効化
- （オプション）「bypass_urls」という名前のURL許可リストを作成して設定します。
- Web インタラクション トラッキングを有効にします。

- 詳細設定： URLルックアップのタイムアウト：15 seconds本文と添付ファイルでスキャンされるURLの最大数：400メッセージ内のURLテキストとHREFを書き換える：NoURL ロギング:有効
- （オプション）AsyncOS 14.2 for Cloud Gatewayでは、URLレトロスペクティブ判定とURL修復が利用可能です。リリースノートおよび「セキュアEメールゲートウェイとクラウドゲートウェイのURLフィルタリングの設定」を参照してください。

グレイメール検出

- [Always scan 1M]および[Never scan 2M]を有効にして設定します。
- 単一メッセージのスキャンのタイムアウト：60 秒

アウトブレイク フィルタ

- アダプティブルールの有効化
- スキャンする最大メッセージサイズ：200万
- Web インタラクション トラッキングを有効にします。

[Advanced Malware Protection] > [File Reputation and Analysis]

- ファイルレピュテーションの有効化
- ファイル分析の有効化 ファイル分析のファイルタイプを確認するには、グローバル設定を参照してください。

メッセージ トラッキング

- 拒否された接続のロギングを有効にします（必要な場合）。

システム管理

ユーザ([System Administration] > [Users])

- ローカルユーザーアカウントとパスフレーズの設定に関連付けられたパスフ**レーズポリシーを確認して設定することを忘れないでください**
- 可能な場合は、認証用のLightweight Directory Access Protocol(LDAP)を設定して有効にします([System Administration] > [LDAP])。

ログサブスクリプション（[システム管理] > [ログサブスクリプション]）

- 設定されていない場合は、次を作成して有効にします。 設定履歴ログURLレピュテーションクライアントログ
- [Log Subscriptions Global Settings]で、設定を編集し、ヘッダー**To**、**From**、**Reply-To**、**Sender**を追加します。

追加設定（オプション）

検討する追加サービス：

[System Administration] > [LDAP]

- LDAPを設定する場合は、SSLを有効にしたLDAPを推奨します

URL防御

- URL防御の最新の設定ベストプラクティスについては、「セキュアEメールゲートウェイおよびクラウドゲートウェイのURLフィルタリングの設定」を参照してください。
- シスコはURL防御についても深く掘り下げています。『URL防御ガイド』を参照してください。
- URL防御ガイドに含まれる例の一部も、このドキュメントに組み込まれています。

SPF

- Sender Policy Framework(SPF)DNSレコードは、クラウドゲートウェイの外部で作成されます。したがって、シスコは、すべてのお客様がSPF、DKIM、およびDMARCのベストプラクティスをセキュリティポスチャに組み込むことを強く推奨します。SPFの検証の詳細については、「SPFの設定とベストプラクティス」を参照してください。
- Cisco Secure Email Cloudをご利用のお客様は、割り当てホスト名ごとにすべてのクラウドゲートウェイのマクロを公開することで、すべてのホストを簡単に追加できます。
- 現在のDNS TXT(SPF)レコード内で ~ allまたは – allの前に置きます（存在する場合）。

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

> **注**:SPFレコードが **~ all**または **– all**で終わっていることを確認します。変更の前後にドメインのSPFレコードを検証します。

- SPFの詳細に関する推奨情報とツール：
  SPFレコードチェッカー – 無料のSPFルックアップ(dmarcian.com)SPFレコード構文テーブル – すべてのSPF - dmarcian.com

その他のSPFの例

- SPFの優れた例は、クラウドゲートウェイから電子メールを受信し、他のメールサーバから送信する場合です。「a:」メカニズムを使用して、メールホストを指定できます。

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

- クラウドゲートウェイ経由で送信メールのみを送信する場合は、次の方法を使用できます。

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

- この例では、「ip4:」または「ip6:」メカニズムによって、IPアドレスまたはIPアドレス範囲が指定されます。

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

CLI レベルの変更

- 「前提条件」に記載されているように、Cisco Secure Email Cloudのお客様はCLIアクセスを要求できます。「コマンドラインインターフェイス(CLI)アクセス」を参照してください。

アンチ スプーフィング フィルタ

- 必ず『アンチスプーフィングのベストプラクティスガイド』を参照してください。
- このガイドでは、電子メールのスプーフィングを防止するための詳細な例と設定のベストプラクティスについて説明します

ヘッダーフィルタの追加

- CLIのみ、addHeadersメッセージフィルタを記述して有効にしてください。

```
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");
}
```

ホストアクセステーブル([メールポリシー(Mail Policies)] > [ホストアクセステーブル(HAT)(Host Access Table (HAT))])

HAT Overview > Additional Sender Groups

- ESAユーザガイド：メッセージ処理用の送信者グループの作成 BYPASS_SBRS – レピュテーションをスキップする送信元には高い値を設定MY_TRUSTED_SPOOF_HOSTS – スプーフィングフィルタの一部TLS_REQUIRED:TLS強制接続の場合

定義済みの SUSPECTLIST 送信者グループにおいて

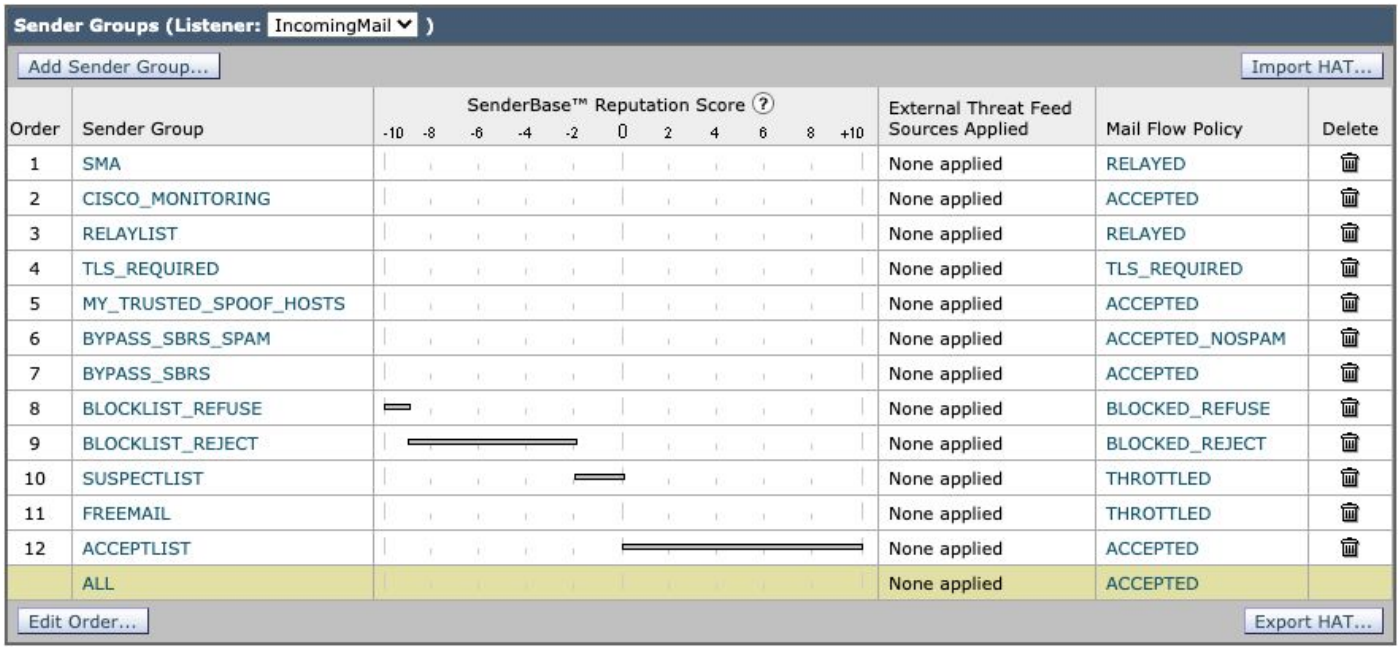
- ESA ユーザ ガイド：送信者検証：ホスト [SBRS Scores on None]を有効にします。（オプション）[Connecting host PTR record lookup fails due to temporary DNS failure]を有効にします。

アグレッシブ HAT の例

- BLOCKLIST_REFUSE [-10.0 to -9.0]ポリシー：BLOCKED_REFUSE
- BLOCKLIST_REJECT [-9.0から–2.0]ポリシー：BLOCKED_REJECT
- SUSPECTLIST [-2.0 ～ 0.0およびSBRSスコアが「なし」の場合]ポリシー：THROTTLED
- ACCEPTLIST [0.0 から 10.0] POLICY:ACCEPTED

> **注：**HATの例は、追加で設定されたメールフローポリシー(MFP)を示しています。 MFPの詳細については、導入したCisco Secure Email GatewayのAsyncOSの適切なバージョンについて、『ユーザガイド』の「Understanding the Email Pipeline > Incoming/Receiving」を参照してください。

HATの例：



メール フロー ポリシー (デフォルト ポリシー パラメータ)

デフォルトポリシーパラメータ

セキュリティ設定

- Transport Layer Security (TLS) を優先に設定します。
- Sender Policy Framework (SPF) を有効にします。
- DomainKeys Identified Mail (DKIM) を有効にします。
- Domain-based Message Authentication, Reporting, and Conformance(DMARC)検証の有効化と集約フィードバックレポートの送信

> **注**：DMARC では、追加の調整を設定する必要があります。DMARCの詳細については、導入したCisco Secure Email GatewayのAsyncOSの適切なバージョンについて、『ユーザガイド』の「Email Authentication > DMARC Verification」を参照してください。

受信メール ポリシー

デフォルトポリシーは次のように設定されます。

スパム対策

- 有効。デフォルトのしきい値のままになります。（採点を変更すると、誤検出が増加する可能性があります）。

ウイルス対策

- メッセージスキャン：**ウイルスのみのスキャン** [Xヘッダーを含める]チェックボックスが有効になっていることを確認します
- [Unscannable Messages] と[Virus Infected Messages] の場合は、[Archive Original Message] を[No] に設定します

AMP

- メッセージエラーに対する**スキャン不能アクション**については、[Advanced] と[Add Custom Header to Message] の[X-TG-MSGERROR]値を使用します。True に設定します。
- [Unscannable Actions on Rate Limit] では、[Advanced] と[Add Custom Header to Message] の[X-TG-RATELIMIT]の値を使用します。True に設定します。
- **ファイル分析が保留中のメッセージ**には、[Action Applied to Message: "Quarantine" を使用します。

グレイメール

- スキャンは各判定(Marketing、Social、Bulk)に対して有効になっており、[Add Text to Subject] の[Prepend] とアクションが[Deliver] になっています。
- [Action on Bulk Mail] では、[Advanced] と[Add Custom Header]（オプション）を使用します。X-Bulk、値：True に設定します。

コンテンツ フィルタ

- EnabledおよびURL_QUARANTINE_MALICIOUS、URL_REWRITE_SUSPICIOUS、URL_INAPPROPRIATE、DKIM_FAILURE、SPF_HARDFAIL、EXECUTIVE_SPOOF、DOMAIN_SPOOF、SDR、TG_RATE_LIMITが選択されています
- これらのコンテンツフィルタについては、このガイドの後半で説明します

アウトブレイク フィルタ

- デフォルトの脅威レベルは3です。セキュリティ要件に合わせて調整してください。 メッセージの脅威レベルがこのしきい値と等しいか、しきい値を超えると、メッセージはアウトブレイク隔離に移動します。（1 = 最小の脅威、5 = 最大の脅威）
- メッセージの変更を有効にする
- 「Enable for all messages」のURL書き換え設定。
- 付加される件名を以下に変更します： [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	

ポリシー名（図）

- **BLOCKLISTメールポリシー**
  BLOCKLISTメールポリシーは、Advanced Malware Protectionを除くすべてのサービスを無効にして設定され、QUARANTINEのアクションでコンテンツフィルタにリンクされます。

- **ALLOWLISTメールポリシー**
  ALLOWLISTメールポリシーには、URL_QUARANTINE_MALICIOUS、URL_REWRITE_SUSPICIOUS、URL_INAPPROPRIATE、DKIM_FAILURE、SPF_HARDFAIL、EXECUTIVE SPOOF、DOMAIN_SPOOF、SDR、TG_RATE_LIMIT、または選択と構成のコンテンツフィルタに対して、スパム対策、グレイメール無効、コンテンツフィルタがあります。

- **ALLOW_SPOOFメールポリシー**
  ALLOW_SPOOFメールポリシーでは、すべてのデフォルトサービスが有効になっており、URL_QUARANTINE_MALICIOUS、URL_REWRITE_SUSPICIOUS、URL_INAPPROPRIATE、SDR、または任意の選択および設定のコンテンツフィルタに対してコンテンツフィルタが有効になっています。

送信メール ポリシー

デフォルトポリシーは次のように設定されます。

スパム対策

- Disabled

ウイルス対策

- メッセージのスキャン：**ウイルススキャンのみ** [Xヘッダーを含める]のチェックボックスをオフにします。
- （オプション）すべてのメッセージについて、次の手順を実行します。[Advanced] > [Other Notification] の順に選択し、[Others]を有効にして、管理者/SOCの連絡先の電子メールアドレスを入力します

高度なマルウェア防御

- ファイルレピュテーションのみを有効にする
- **レート制限に対するスキャン不能アクション**：[Advanced] と[Add Custom Header to Message] を使用します。X-TG-RATELIMIT、値：「その通りだ」
- **マルウェアが添付されたメッセージ**:[Advanced] と[Add Custom Header to Message] を使用します。X-TG-OUTBOUND、値：「マルウェアが検出されました。」

グレイメール

- Disabled

コンテンツ フィルタ

- EnabledおよびTG_OUTBOUND_MALICIOUS、Strip_Secret_Header、EXTERNAL_SENDER_REMOVE、ACCOUNT_TAKEOVER、または選択したコンテンツフィ

ルタが選択されます。

アウトブレイク フィルタ

- Disabled

DLP

- DLPライセンスとDLP設定に基づいて有効にします。

その他の設定

辞書([メールポリシー(Mail Policies)] > [辞書(Dictionaries)])

- ProfanityおよびSexual_Contentディクショナリの有効化とレビュー
- すべての経営幹部の名前を使用した偽造電子メール検出用のExecutive_FED辞書の作成
- ポリシー、環境、セキュリティ制御に必要な制限キーワードまたはその他のキーワード用の追加の辞書を作成します。

宛先制御([メールポリシー(Mail Policies)] > [宛先制御(Destination Controls)])

- デフォルトドメインで、**TLSサポート**を**優先**として設定します
- Webメールドメインの宛先を追加し、低いしきい値を設定できます
- 詳細については、『宛先制御によるアウトバウンドメールのレート制限の設定』ガイドを参照してください。

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.

コンテンツ フィルタ

注：コンテンツフィルタの詳細については、導入したCisco Secure Email GatewayのAsyncOSの適切なバージョンの『ユーザガイド』の「コンテンツフィルタ」を参照してください。

受信コンテンツフィルタ

URL_QUARANTINE_MALICIOUS

[Condition]：URLレピュテーション：url-reputation(-10.00, -6.00 , "bypass_urls", 1, 1)

Action:検疫：quarantine("URL_MALICIOUS")

URL_REWRITE_SUSPICIOUS

[Condition]：URLレピュテーション：url-reputation(-5.90, -5.60 , "bypass_urls", 0, 1)

Action:URLレピュテーション；url – レピュテーション – プロキシリダイレクト(-5.90, -5.60,",0)

URL_INAPPROPRIATE

[Condition]：URLカテゴリ； url-category (['Adult', 'Child Abuse Content', 'Extreme', 'Hate Speech', 'Illegal Activities', 'Illegal Downloads', 'Illegal Drugs', 'Pornography', 'Filter Avoidance'], "bypass_urls", 1, 1)

Action:検疫；duplicate-quarantine("INAPPROPRIATE_CONTENT")

DKIM_FAILURE

[Condition]：DKIM認証、dkim-authentication == hardfail

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

SPF_HARDFAIL

[Condition]：SPFの検証、spf-status == fail

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

EXECUTIVE_SPOOF

[Condition]：Forged Email Detection、forged-email-detection("Executive_FED", 90, "")

[Condition]：Other Header; header("X-IronPort-SenderGroup") != "(?i)allowspoof"

* set **Apply rule:すべての条件が一致する場合のみ**

Action:ヘッダーの追加/編集；edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1")

Action:検疫；duplicate-quarantine("FORGED_EMAIL")

DOMAIN_SPOOF

[Condition]：その他のヘッダーheader("X-Spoof")

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

SDR

[Condition]：ドメインレピュテーション； sdr-reputation (['awful'], "")

[Condition]：ドメインレピュテーション、sdr-age("days", <, 5, "")

* set **Apply rule:1つ以上の条件が一致する場合**

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

TG_RATE_LIMIT

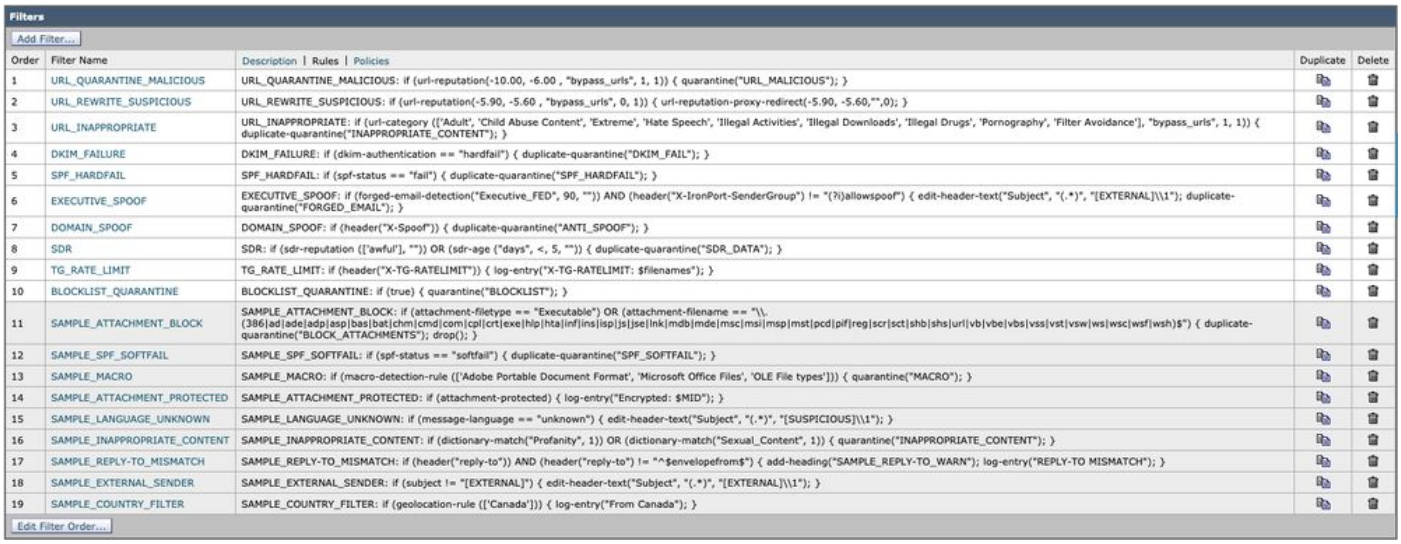
[Condition]：Other Header;header("X-TG-RATELIMIT")

Action:ログエントリを追加します。log-entry("X-TG-RATELIMIT:$filenames")

BLOCKLIST_QUARANTINE

[Condition]：(None)

Action:検疫；検疫("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...

発信コンテンツフィルタ

TG_OUTBOUND_MALICIOUS

[Condition]：その他のヘッダー、ヘッダー(「X-TG-OUTBOUND」)==マルウェア

Action:検疫；検疫("TG_OUTBOUND_MALWARE")

Strip_Secret_Header

[Condition]：Other Header; header("PLACEHOLDER") == PLACEHOLDER

Action:ストリップヘッダー；ストリップヘッダー("X-IronPort-Tenant")

EXTERNAL_SENDER_REMOVE

[Condition]：(None)

Action:ヘッダーの追加/編集； edit-header-text("Subject", "\\[EXTERNAL\\]\\s?", "")

ACCOUNT_TAKEOVER

[Condition]：Other Header; header("X-AMP-Result") == (?i)malicious

[Condition]：URLレピュテーション；url-reputation(-10.00, -6.00 , "", 1, 1)

*適用ルールの設定：1つ以上の条件が一致する場合

Action:Notify;notify ("<管理者またはディストリビューションのメールアドレスを挿入>"、"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...

Cisco Secure Email Cloudをご利用のお客様には、ゴールド構成とベストプラクティスの推奨事項にコンテンツフィルタの例が含まれています。また、構成に役立つ条件とアクションの詳細については、「SAMPLE_」フィルタを参照してください。

Cisco Live

Cisco Liveは世界中で多くのセッションをホストしており、Cisco Secure Emailのベストプラクティスをカバーする対面式セッションやテクニカルブレークアウトを提供しています。過去のセッションおよびアクセスについては、Cisco Live（CCOログインが必要）を参照してください。

- Cisco E メール セキュリティ：ベストプラクティスと微調整 – BRKSEC-2131
- DMARC電子メール境界の作成 – BRKSEC-2131
- Eメールの修正- Cisco Eメールセキュリティの高度なトラブルシューティング – BRKSEC-3265
- Cisco EメールセキュリティのAPI統合 – DEVNET-2326
- Securing SaaS Mailbox Services with Cloud Email Security from Cisco - BRKSEC-1025
- Eメールセキュリティ：ベストプラクティスと微調整 – TECSEC-2345
- 250 not OK - Going on the Defensive with Cisco Email Security - TECSEC-2345
- Cisco Domain ProtectionおよびCisco Advanced Phishing Protection:Eメールセキュリティの次のレイヤを最大限に活用- BRKSEC-1243
- SPFは「Spoof」の頭文字ではありません！Eメールセキュリティの次のレイヤを最大限に活用- DGTL-BRKSEC-2327

追加情報

Cisco Secure Email Gatewayのドキュメント

- リリース ノート
- ユーザガイド
- CLIリファレンスガイド
- Cisco Secure Email GatewayのAPIプログラミングガイド
- Cisco Secure Email Gatewayで使用されるオープンソース
- Ciscoコンテンツセキュリティ仮想アプライアンスインストールガイド（vESAを含む）

Secure Email Cloud Gatewayドキュメント

- リリース ノート
- ユーザガイド

Cisco Secure Email and Web Managerのドキュメント

- リリースノートと互換性マトリクス
- ユーザガイド
- Cisco Secure Email and Web ManagerのAPIプログラミングガイド
- Ciscoコンテンツセキュリティ仮想アプライアンスインストールガイド（vSMAを含む）

Cisco Secure製品ドキュメント

- Cisco Secureポートフォリオの命名アーキテクチャ

関連情報

- Cisco Secure Email Securityコンプライアンス
- オファーの説明：安全な電子メール
- シスコ ユニバーサル クラウド チーム
- シスコのサポートとダウンロード
- [外部] OpenSPF:SPFの基本と詳細情報

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。