信頼できる送信者がスパム対策をバイパスできるようにする

内容

概要

このドキュメントでは、信頼できる送信者にアンチスパムスキャンをバイパスさせる方法の詳細と、セキュアEメールゲートウェイ（以前のEメールセキュリティアプライアンス）で同じ方法を選択できるさまざまな方法について説明します。

ALLOWED_LIST送信者グループの送信者ホスト名/IPアドレスの追加

信頼する送信者をALLOWED_LIST送信者グループに追加します。この送信者グループは$TRUSTEDメールフローポリシーを使用します。ALLOWED_LIST送信者グループのメンバーはレート制限の対象ではなく、これらの送信者からのコンテンツはアンチスパムエンジンによってスキャンされず、依然としてアンチウイルスによってスキャンされます。

> **注**：デフォルト設定では、アンチウイルススキャンは有効ですが、アンチスパムはオフになっています。

送信者がアンチスパムスキャンをバイパスできるようにするには、ホストアクセステーブル(HAT)のALLOWED_LIST送信者グループに送信者を追加します。GUIまたはCLIを使用してHATを設定できます。

GUI を使用する場合

1. [メールポリシー]タブを選択します。
2. [Host Access Table]セクションで、[HAT Overview]を選択します。
3. 右側で、InboundMailリスナーが現在選択されていることを確認してください。
4. [送信者グループ]列から、[ALLOWED_LIST]を選択します。
5. ページの下半分の近くにある[送信者の追加]ボタンを選択します。
6. バイパスを許可するIPまたはホスト名を最初のフィールドに入力します。

エントリの追加が完了したら、[送信]ボタンを選択します。変更を保存するには、[Commit

Changes]ボタンを選択してください。

CLI を使用する場合

```
example.com> listenerconfig
Currently configured listeners:
1. InboundMail (on PublicNet, 172.19.1.80) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 172.19.2.80) SMTP TCP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit
Enter the name or number of the listener you wish to edit.
[]> 1
Name: InboundMail
Type: Public
Interface: PublicNet (172.19.1.80/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
LDAP: Off

Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> hostaccess
Default Policy Parameters
==========================
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
```

```
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[]> edit
1. Edit Sender Group
2. Edit Policy
[1]> 1
Currently configured HAT sender groups:
1. ALLOWED_LIST (My trusted senders have no anti-spam scanning or rate limiting)
2. BLOCKED_LIST (Spammers are rejected)
3. SUSPECTLIST (Suspicious senders are throttled)
4. UNKNOWNLIST (Reviewed but undecided, continue normal acceptance)
5. (no name, first host = ALL) (Everyone else)
Enter the sender group number or name you wish to edit.
[]> 1

Choose the operation you want to perform:
- NEW - Add a new host.
- DELETE - Remove a host.
- MOVE - Reorder the hosts.
- POLICY - Change the policy settings and options.
- PRINT - Display the current definition.
- RENAME - Rename this sender group.
[]> new
Enter the hosts to add. CIDR addresses such as 10.1.1.0/24 are allowed. IP
address ranges such as 10.1.1.10-20 are allowed. IP subnets such as 10.2.3. are
allowed. Hostnames such as crm.example.com are allowed. Partial hostnames such
as .example.com are allowed.
Ranges of SenderBase Reputation scores such as SBRS[7.5:10.0] are allowed.
SenderBase Network Owner IDs such as SBO:12345 are allowed.
Remote blocklist queries such as dnslist[query.blocklist.example] are allowed.
Separate multiple hosts with commas
[]>
```

commitコマンドを必ず発行して、変更を保存してください。

信頼できるメールフローポリシーのアンチスパムおよびアンチウイルススキャンの確認

信頼できる送信者には、デフォルトで信頼できる存在として名付けられたメールフローポリシーがあります。信頼できるメールフローポリシーの接続動作は[Accept]になります（受信メールの他のメールフローポリシーの動作と同様）。

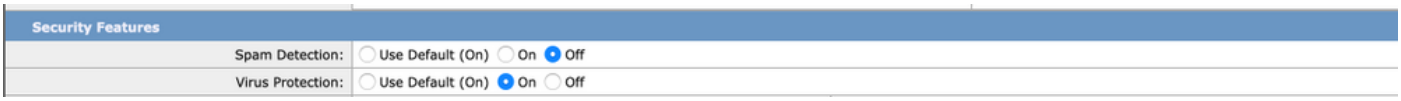
送信者がビジネス要件に対して信頼されている場合は、ウイルス対策とスパム対策のチェックを無効にすることもできます。これにより、信頼できる送信元から送信されていない電子メールをスキャンしながら、両方のスキャンエンジンの余分な処理負荷を軽減できます。

> **注**：無効にされたアンチスパムおよびアンチウイルスエンジンは、ESAで受信する電子メールに関するスパムまたはウイルス関連のスキャンをスキップします。これは、これらの信頼できる送信者のスキャンをスキップしてもリスクが生じないと完全に確信している場合にのみ行う必要があります。

[メールフローポリシー(Mail Flow Policies)]の[セキュリティ機能(Security Features)]タブで、エンジンを無効にできるオプションを使用できます。同じパスは、[GUI] > [Mail Policies] > [Mail Flow

Policies]です。TRUSTEMDMailフローポリシーをクリックし、次のページの[Security Features]までスクロールします。

必要に応じて調整を行った後、変更を確定してください。



セーフリストへの信頼できる送信者の追加

エンドユーザのセーフリストとブロックリストは、エンドユーザが作成し、アンチスパムスキャンの前にチェックしたデータベースに保存されます。各エンドユーザは、常にスパムとして扱うか、スパムとして扱わないドメイン、サブドメイン、または電子メールアドレスを特定できます。送信者アドレスがエンドユーザセーフリストの一部である場合、スパム対策スキャンはスキップされます

このセットアップにより、エンドユーザは、スパム対策スキャンを除外するための要件に従って、送信者をセーフリストに登録できます。電子メールパイプラインのウイルス対策スキャンおよびその他のスキャンは、この設定に影響されず、メールポリシーの設定に従って続行されます。この設定により、エンドユーザが送信者のスパムスキャンを免除する必要があるたびに、管理者の関与が減ります。

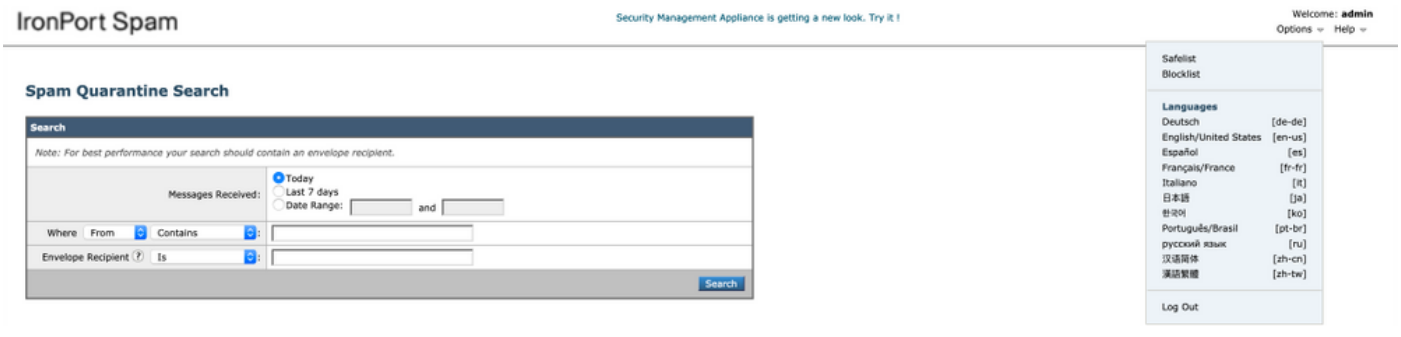
セーフリストの場合、エンドユーザの隔離アクセスとエンドユーザのセーフリスト/ブロックリスト（ESAまたはSMAの両方）に対して有効にする必要があります。 これにより、スパム隔離ポータルにアクセスし、隔離された電子メールのリリース/削除と同時に、Safelistの送信者の追加/削除も可能になります。

エンドユーザ検疫アクセスは、次のように有効にできます。

ESA:[GUI] > [Monitor] > [Spam Quarantine]に移動します。[End-User Quarantine Access]の[Radio]ボタンをチェックインします。必要に応じて、アクセスの認証方法を選択します([なし(None)]、[LDAP]、[SAML]、[IMAP]、または[POP])。 これを投稿し、エンドユーザのセーフリスト/ブロックリストを有効にします。

SMA:[GUI] > [Centralized Services] > [Spam Quarantine]に移動します。エンドユーザー検疫アクセスのラジオボタンをチェックインします。必要に応じて、アクセスの認証方法を選択します([なし(None)]、[LDAP]、[SAML]、[IMAP]、または[POP])。 これを投稿し、エンドユーザのセーフリスト/ブロックリストを有効にします。

有効にすると、エンドユーザーがスパム検疫ポータルに移動したときに、右上のドロップダウンオプションから選択した方法でセフェリストを追加または変更できます。



信頼できる送信者と受信メールポリシー

また、信頼できる送信者を受信メールポリシーに追加し、要件に従ってウイルス**対策/スパム**対策スキャンを無効にすることもできます。カスタマイズされた新しいメールポリシーは、**信頼できる送信者/安全な送信者**などの名前を使用して作成できます。その後、ドメイン名や送信者の電子メールアドレスなどの送信者の詳細をこのカスタムポリシーに追加できます。

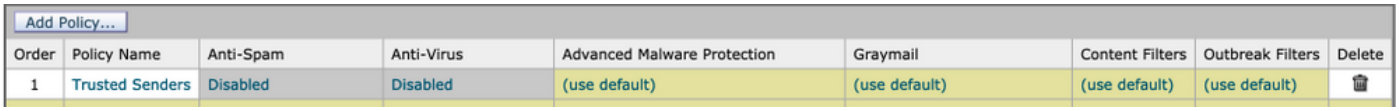
必要な追加後にポリシーを送信したら、[スパム対策]または[ウイルス対策]の列をクリックして、次のページで[無効]を選択**します**。

この設定により、このメールポリシーに追加された信頼できる送信者ドメインまたは電子メールアドレスは、スパム対策スキャンまたはウイルス対策スキャンから除外されます。

> **注**：無効にされたアンチスパムおよびアンチウイルスエンジンは、このカスタムメールポリシーで処理されたESAの受信メールに関するスパムまたはウイルス関連のスキャンをスキップします。これは、これらの信頼できる送信者のスキャンをスキップしてもリスクが生じないと完全に確信している場合にのみ行う必要があります。

カスタムメールポリシーは、[ESA GUI] > [メールポ**リシー] > [受信メールポリシー] > [ポリシーの追加]から作成できます**。必要に応じてポリシー名を入力し、[ユーザーの追加]を**選択します**。[次の送信者]のオプションボタンをチ**ェックインします**。ボックスに必要なドメインまたは電子メールアドレスを追加し、[OK]をクリ**ックします**。

メールポリシーの作成後、ビジネス要件に応じてウイルス対策スキャンとスパム対策スキャンを無効にするよう選択できます。次にスクリーンショットの例を示します。



関連情報

- Cisco E メール セキュリティ アプライアンス：エンドユーザ ガイド
- テクニカル サポートとドキュメント – Cisco Systems