着信メールポリシーとコンテンツフィルタを使用して送信ドメインをブロックリストまたはドロップするにはどうすればよいですか。

内容

概要

このドキュメントでは、着信メールポリシーとコンテンツフィルタを使用して送信ドメインをブロックリストまたはドロップする方法について説明します。

着信メールポリシーとコンテンツフィルタを使用して送信ドメインをブロックリストまたはドロップするにはどうすればよいですか。

Blocklist Sender Groupを使用して送信者の電子メールドメインを照合することはできません。これは、送信者のドメインではなく、接続サーバのホスト名またはIPアドレスを参照するためです。

特定の送信者の電子メールアドレスまたはドメインが表示されたときにメールをブロックリストまたはドロップするには、新しい着信メールポリシーと着信コンテンツフィルタの組み合わせを使用する必要があります。

1. Web GUI から、[Mail Policies] > [Incoming Mail Policy]を選択します。 新しい着信メール ポリシーを作成します。 ポリシーに「Block-Sender-Domains」というラベルを付けることができます。 [Sender] オプションを選択して、ブロックする送信者の電子メール アドレスまたはドメインを指定します(例：user@example.com、user@、@example.com、@.example.com)
2. 送信し、変更を確定します。
3. [Mail Policies] > [Incoming Mail Policy]に戻ります。[Default Policy] の上に、追加した「Block-Sender-Domain」という着信メール ポリシーが表示されます。 この送信者のドメインから送信されるすべてのメールは、この着信メール ポリシーにのみ一致します。
4. メッセージをドロップする着信コンテンツフィルタを作成します。[メールポリシー] > [着信コンテンツフィルタ]を選択します。「Always_drop」という新しいフィルタを作成します。
5. 条件は、空のままにします。
6. アクションは、メッセージを廃棄するよう設定します。
7. [Submit] をクリックします。

8. 着信コンテンツ フィルタを作成した後、正しい着信メール ポリシーでそのフィルタを有効にします。 また、「Block-Sender-Domains」メール ポリシーを変更した場合、リソースを消費しないようにスパム対策、ウイルス対策、およびウイルス アウトブレイク フィルタを無効にします。 そのため、「Block-Sender-Domains」メール ポリシーで、スパム対策リンクをクリックし、[Disable] および [Submit]を選択します。 ウイルス対策スキャンおよびアウトブレイクフィルタについて繰り返します。コンテンツフィルタの場合は、[はい]に設定し、手順4「Always_drop」で作成したコンテンツフィルタを有効にします。
9. 変更を [Submit] して [Commit] します。

Result:ブロック/ドロップするドメインの着信ポリシーを作成します。基本的に、これらの電子メールに対して別のパスを作成し、単純に削除します。

または、CLI からメッセージ フィルタを作成して、1 つまたは複数の電子メール アドレスをブロックすることができます。

CLI から、次のように実行します。

```
Machine_name> filters
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> new
Enter filter script.  Enter '.' on its own line to end.
BlockEmail: if(mail-from == "(?i)user1@example\\.com$") {
drop();
}
.
1 filters added.
```

フィルタを直接入力できますが、ほとんどのお客様はフィルタをデスクトップのテキスト エディタに保存して、コピー アンド ペーストを使用して作成します。前述の例では、名前（BlockEmail）から最後のドットまで貼り付けています。

同一ドメインからの複数のユーザをブロックするには、「if」行を次のように置き換えます。

```
if(mail-from == "(?i)(user1|user2|user3)@example\\.com$")
```

複数のドメインからの複数のユーザをブロックするには、「if」行を次のように置き換えます。

```
if(mail-from == "(?i)(user1@example1\\.com|user2@example2\\.com)$")
```

> **注：**このフィルタでは、廃棄アクションを使用します。 適切な電子メールが失われないように注意してください。ドロップ操作の代わりに次のいずれかの操作を使用して、最初にテストすることを強く推奨します。

ポリシー検疫にメッセージを送信するには、次のコマンドを使用します。

```
quarantine("Policy");
```
代替電子メール アドレスにメッセージを送信するには、次のコマンドを使用します。

```
alt-rcpt-to(some_email_address@yourdomain.com);
```
上記のメッセージフィルタの例では、いずれかのアクションが「drop();」アクション行に置き換えられます。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems