

Wie kann ich eine sendende Domäne mit der Richtlinie für eingehende E-Mails und dem Content-Filter blockieren oder verwerfen?

Inhalt

[Einführung](#)

[Wie kann ich eine sendende Domäne mit der Richtlinie für eingehende E-Mails und dem Content-Filter blockieren oder verwerfen?](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie eine sendende Domäne mit der Richtlinie für eingehende E-Mails und dem Inhaltsfilter blockiert oder gelöscht wird.

Wie kann ich eine sendende Domäne mit der Richtlinie für eingehende E-Mails und dem Content-Filter blockieren oder verwerfen?

Sie können die E-Mail-Domäne eines Absenders nicht über die Absendergruppe der Sperrliste abgleichen, da sie sich auf den Hostnamen oder die IP-Adresse des verbindenden Servers bezieht, nicht notwendigerweise auf die Absenderdomäne.

Um die E-Mail-Adresse oder -Domäne eines bestimmten Absenders zu blockieren oder zu löschen, müssen Sie eine Kombination aus einer neuen Richtlinie für eingehende E-Mails und einem Filter für eingehende Inhalte verwenden.

1. Wählen Sie in der Web-GUI Mail Policies > Incoming Mail Policy (Mail-Policys > Richtlinien für eingehende E-Mails) aus. Erstellen Sie eine neue Richtlinie für eingehende E-Mails. Sie können die Richtlinie als "Block-Sender-Domains" bezeichnen. Wählen Sie die Option "Sender" aus, und geben Sie die E-Mail-Adresse oder Domäne des Absenders ein, die Sie blockieren möchten. (z. B. user@example.com, benutzer@, @beispiel.com, @.example.com)
2. Änderungen senden und bestätigen.
3. Gehen Sie zurück zu Mail-Policys > Mail Policy für eingehende E-Mails. Sie sollten jetzt eine zusätzliche Richtlinie für eingehende E-Mails mit dem Namen "Block-Sender-Domain" sehen, die über der Standardrichtlinie liegt. Alle E-Mails, die von der Domäne dieses Absenders stammen, entsprechen nur dieser Richtlinie für eingehende E-Mails.
4. Erstellen Sie jetzt einen Filter für eingehende Inhalte, der die Nachricht verwirft. Wählen Sie Mail Policies > Incoming Content Filter (Mail-Policys > Filter für eingehende Inhalte) aus. Erstellen Sie einen neuen Filter mit dem Namen "Always_drop".

5. Lassen Sie diese Voraussetzung leer.
6. Legen Sie für die Aktion fest, dass die Nachricht verworfen wird.
7. Klicken Sie auf Senden.
8. Aktivieren Sie den Filter für eingehende Inhalte nach dem Erstellen in der richtigen Richtlinie für eingehende E-Mails. Wenn Sie die Mail-Richtlinie "Blockieren-Absender-Domänen" ändern, sollten Sie außerdem die Filter für Spam-, Anti-Virus- und Virenangriffe deaktivieren, um Ressourcen nicht zu verschwenden. Klicken Sie für die E-Mail-Policy "Blockieren-Absender-Domänen" auf den Spam-Schutz und wählen Sie Deaktivieren und Senden aus. Wiederholen Sie den Anti-Virus-Scan und den Outbreak-Filter. Legen Sie für die Inhaltsfilter Yes fest, und aktivieren Sie den Content-Filter, der in Schritt 4, "Always_drop", erstellt wurde.
9. Senden und Übernehmen der Änderungen

Ergebnis: Dadurch wird eine Richtlinie für eingehende Domänen erstellt, die Sie blockieren/löschen möchten. Sie erstellen im Grunde einen separaten Pfad für diese E-Mails und lassen sie dann einfach fallen.

Sie können alternativ einen Nachrichtenfilter aus der CLI erstellen, um eine oder mehrere E-Mail-Adressen zu blockieren.

Führen Sie über die CLI ähnliche Schritte aus:

```
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.
```

Sie können den Filter zwar direkt eingeben, aber die meisten Kunden behalten ihn in einem Texteditor auf ihrem Desktop und verwenden ihn in Kopieren und Einfügen, um ihn zu erstellen. Im obigen Beispiel fügen Sie vom Namen (BlockEmail) bis zum Endpunkt ein.

Um mehrere Benutzer derselben Domäne zu blockieren, ersetzen Sie die "if"-Zeile durch:

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

Um mehrere Benutzer aus mehreren Domänen zu blockieren, ersetzen Sie die "if"-Zeile durch:

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

Hinweis: Dieser Filter verwendet eine Drop-Aktion. Achten Sie darauf, den Verlust guter E-Mails zu vermeiden! Es wird dringend empfohlen, zuerst eine der unten aufgeführten

Aktionen anstatt der Drop-Aktion zu testen.

So senden Sie eine oder mehrere Nachrichten an die Richtlinienquarantäne:

```
quarantine("Policy");
```

So senden Sie eine oder mehrere Nachrichten an eine andere E-Mail-Adresse:

```
alt-rcpt-to(some_email_address@yourdomain.com);
```

Eine dieser Aktionen ersetzt die Aktionszeile "drop();" im Nachrichtenfilterbeispiel oben.

Zugehörige Informationen

- [Technischer Support und Dokumentation - Cisco Systems](#)