How do I blocklist or drop a sending domain using Incoming Mail Policy and Content Filter?

Contents

Introduction

This document describes how to blocklist or drop a sending domain using Incoming Mail Policy and Content Filter.

How do I blocklist or drop a sending domain using Incoming Mail Policy and Content Filter?

You cannot match a sender's email domain via the Blocklist Sender Group since it refers to the hostname or IP address of the connecting server, not necessarily the sender's domain.

To blocklist or drop the mail when you see a certain sender's email address or domain, you need to use a combination of a new Incoming Mail Policy and Incoming Content Filter.

1. From the Web GUI, choose Mail Policies > Incoming Mail Policy. Create a new Incoming Mail Policy. You can label the policy, "Block-Sender-Domains." Select the "Sender" option and put in the sender's email address or domain that you want to block. (e.g. user@example.com, user@, @example.com, @.example.com)
2. Submit and Commit Changes.
3. Go back to Mail Policies > Incoming Mail Policy. You should now see an additional incoming mail policy called "Block-Sender-Domain" that is above the Default Policy. All mail coming from this sender's domain will be matching only this incoming mail policy.
4. Now create an incoming content filter that will drop the message. Choose Mail Policies > Incoming Content Filter. Create a new filter called "Always_drop."
5. For the condition, leave this empty.
6. For the action, set it to drop the message.
7. Click Submit.
8. After creating the incoming content filter, enable it on the correct incoming mail policy. Also, when you were modifying the "Block-Sender-Domains" mail policy, you should disable the anti-spam, anti-virus, and virus outbreak filters to not waste resources. So, for the "Block-Sender-Domains" mail policy click on the anti-spam link and select Disable and Submit. Repeat for the anti-virus scanning and outbreak filter. For the content filters, set it to Yes and enable the content filter that was created in Step 4, "Always_drop."

9. Submit and Commit the changes.

Result: What this is doing is creating an Incoming Policy for domains you want to block/drop. You're basically creating a separate path for these emails and then simply dropping them.

You may alternatively create a message filter from the CLI to block one or more email addresses.

From the CLI, perform similar:

```
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.
```

Although you can type the filter in directly, most customers will keep it in a text editor on their desktop and use copy and paste to create it. In the example above you would paste from the name (BlockEmail) through the ending dot.

To block multiple users from the same domain, replace the "if" line with:

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

To block multiple users from multiple domains, replace the "if" line with:

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

> **Note**: This filter uses a drop action. Be careful to avoid loss of good email! It is highly recommended that you test first with one of the below actions instead of the drop action.

To send message(s) to the policy quarantine:

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

To send message(s) to an alternate email address:

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

Either one of these actions would replace the "drop();" action line in the message filter example above.

Related Information

- **Technical Support & Documentation - Cisco Systems**