**Back story**: In normal circumstances, no sender from own domain is expected from external

(Internet)

                  Emails from own domain should go internally between exchange and not outside

MTA/source.

e.g

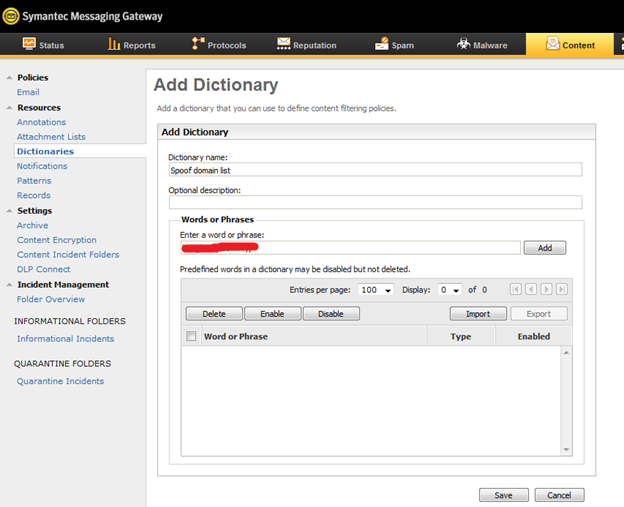
Fake sender example.com (Internet) 🡪 SMG 🡪 Exchange 🡪 Mailbox (example.com)

Mailbox (example.com) 🡪 Exchange 🡪 Mailbox (example.com)

**Objective:** Block spoofed sender

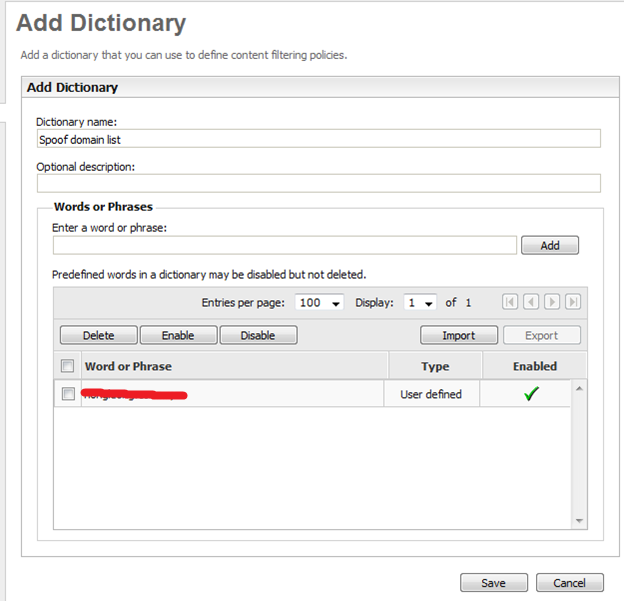
**Solution:** We may use SMG content filtering

1. Logon to SMG and then go to Content 🡪 Dictionaries 🡪 Add Dictionary

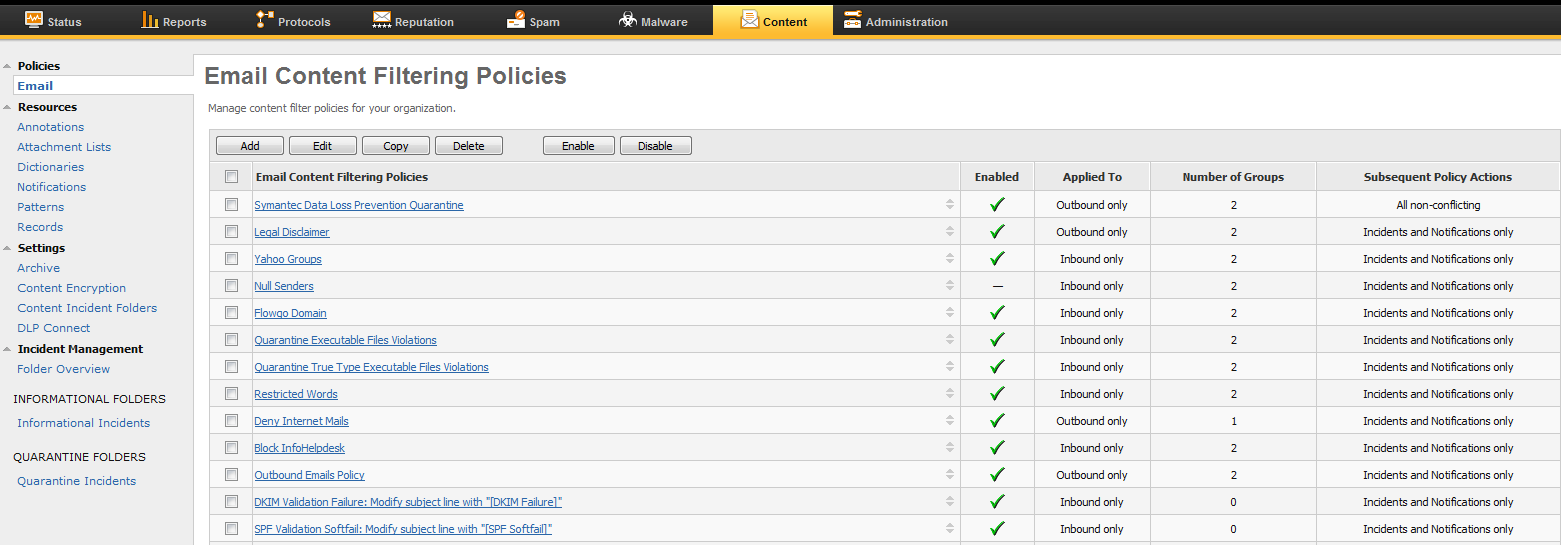


1. Create a new dictionary list with name e.g Spoof domain list

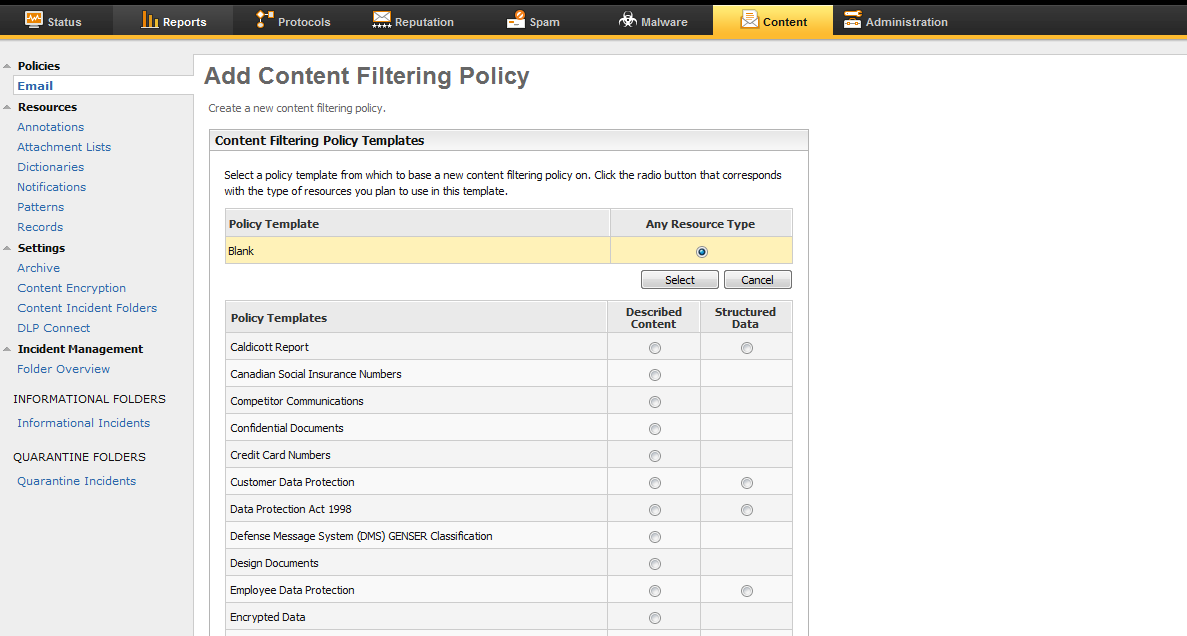
Add the potential domain name that can be spoofed by external party then save it



1. Go to Content 🡪 Policies 🡪 Email

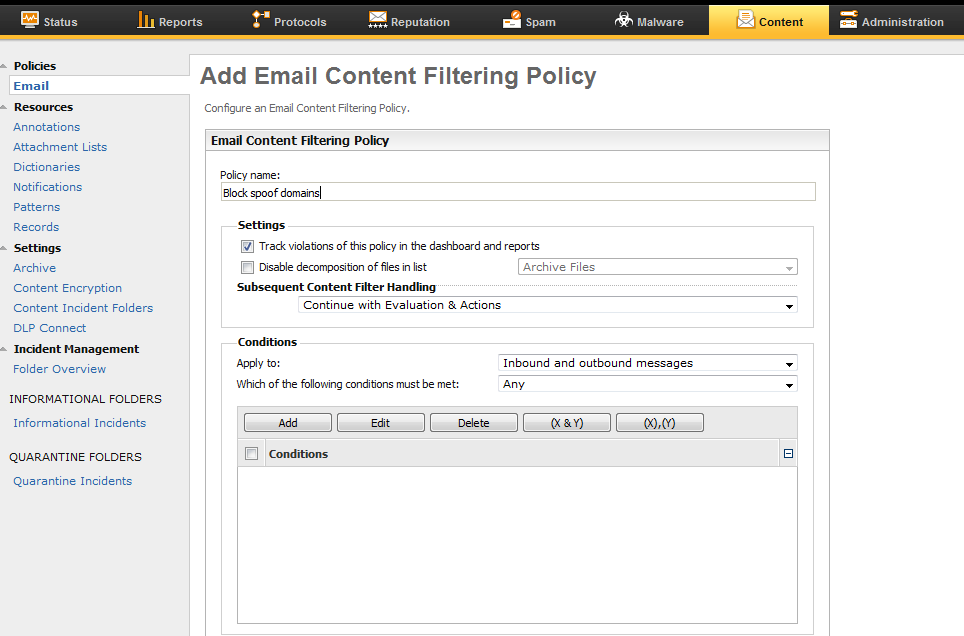


1. Click Add and select a new blank policy template



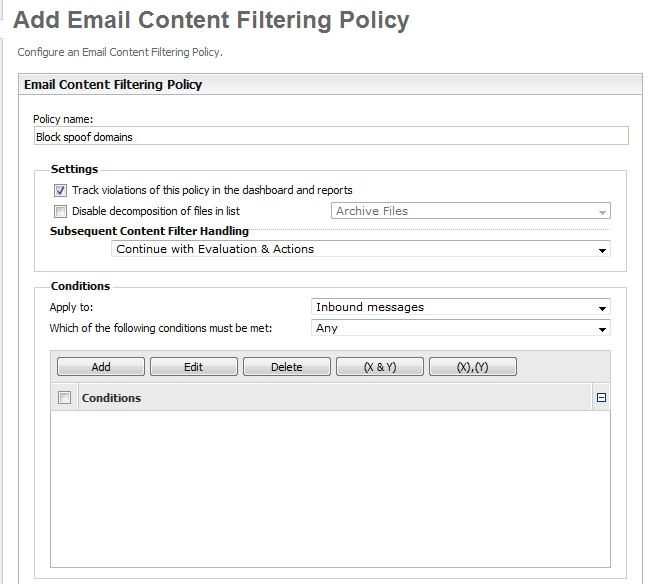
1. Name the policy to e.g Block spoof domains

Tick the option **Track violations of this policy in the dashboard and reports**



1. Edit the conditions and select Apply to **Inbound messages**

Select **Any** in Which of the following conditions must be met



1. Click Edit in the conditions tab

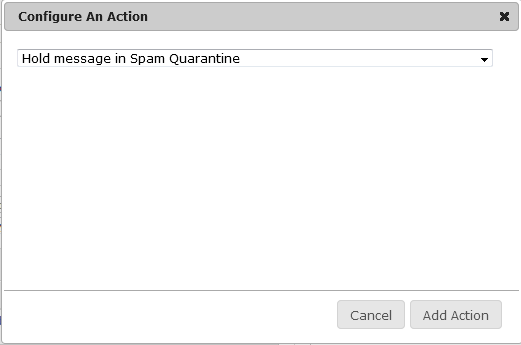
Go to “Text in the specific part of the message header” and select **Envelope sender**

**Contains** **Domain name** from dictionary **Spoof domain list (custom)**



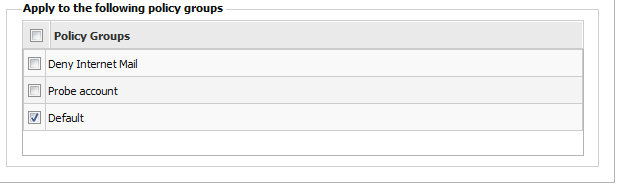
1. Go to Action and then click Add

Select **Hold message in Spam Quarantine** then click Add Action



1. In the last option, select the Policy Group that you wanted to Apply

(Default in this example)



1. Then verify everything before clicking **save**

