SOPHOS
Security made simple.

Pocket Guide

Protect Internal Email Server (Legacy Mode)

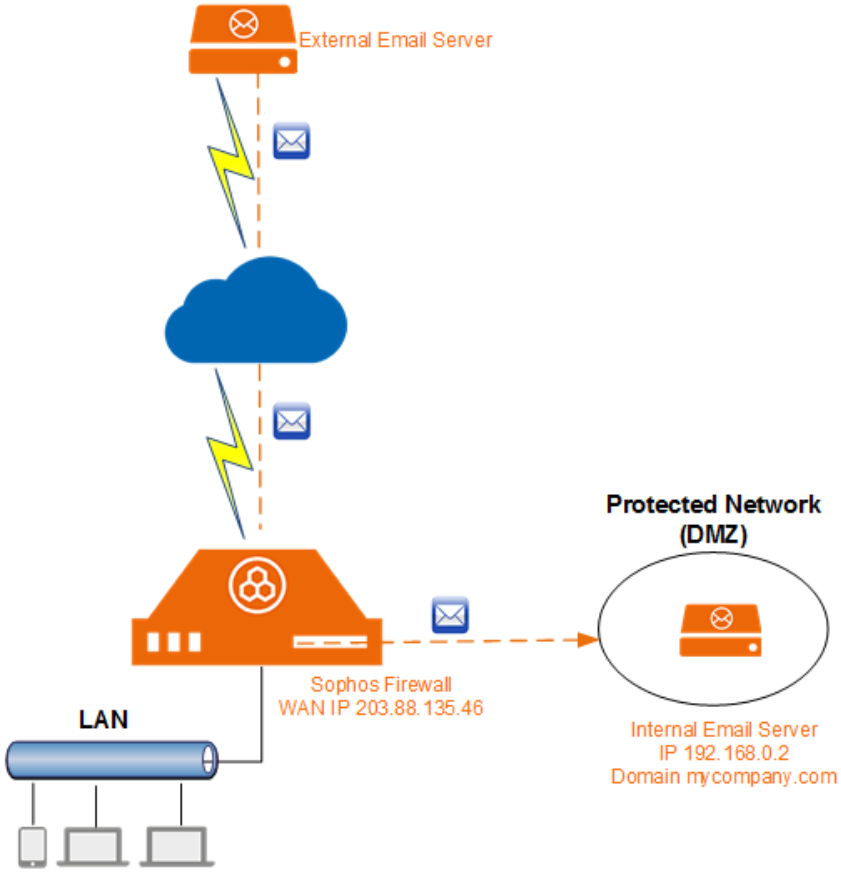
Product: Sophos XG Firewall

Contents

Scenario 2
Prerequisites 2
Configuration 3
Step 1: Create Business Application Rule to Route Emails to Internal Email Server 3
Step 2: Create Network Rule to allow all traffic to and from Protected Network (DMZ) 5
Step 3: Configure Global Email Settings 6
Step 4: Create Malware Scanning Policy 6
Step 5: Create SMTP and POP/IMAP Scanning Policies 7
Results 11
Suggested Reading 11
Copyright Notice 12

Scenario

Configure Sophos XG Firewall (SF-OS) to route emails from the Internet to an internal email server. Set Anti-virus, RBL, IP Reputation, Anti-spam and DLP scanning policies to scan and filter emails to and from the internal email server.



Prerequisites

- You must have read-write permissions on the SF-OS Admin Console for the relevant features.
- You must subscribe to and activate the Email Protection Module **(Administration > Licensing)**.
- You must plug in and connect the interfaces to WAN (Internet) and DMZ (containing the Email Server) zones **(Network > Interfaces)**.

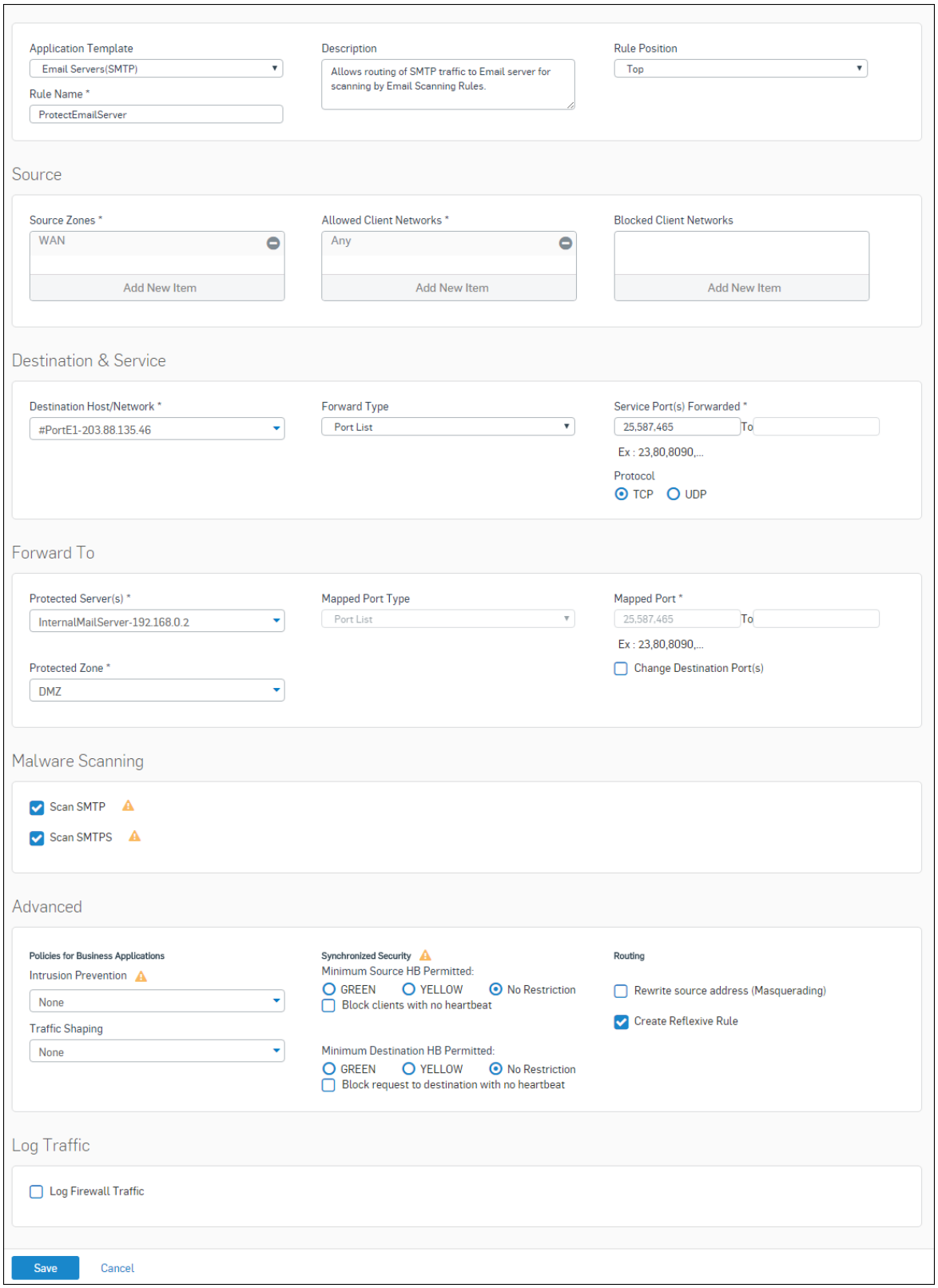
Configuration

Log in to the SF-OS Admin Console.

Step 1: Create Business Application Rule to Route Emails to Internal Email Server

1. Go to **Protect > Firewall**, click **Add Firewall Rule** and click **Business Application Rule**.

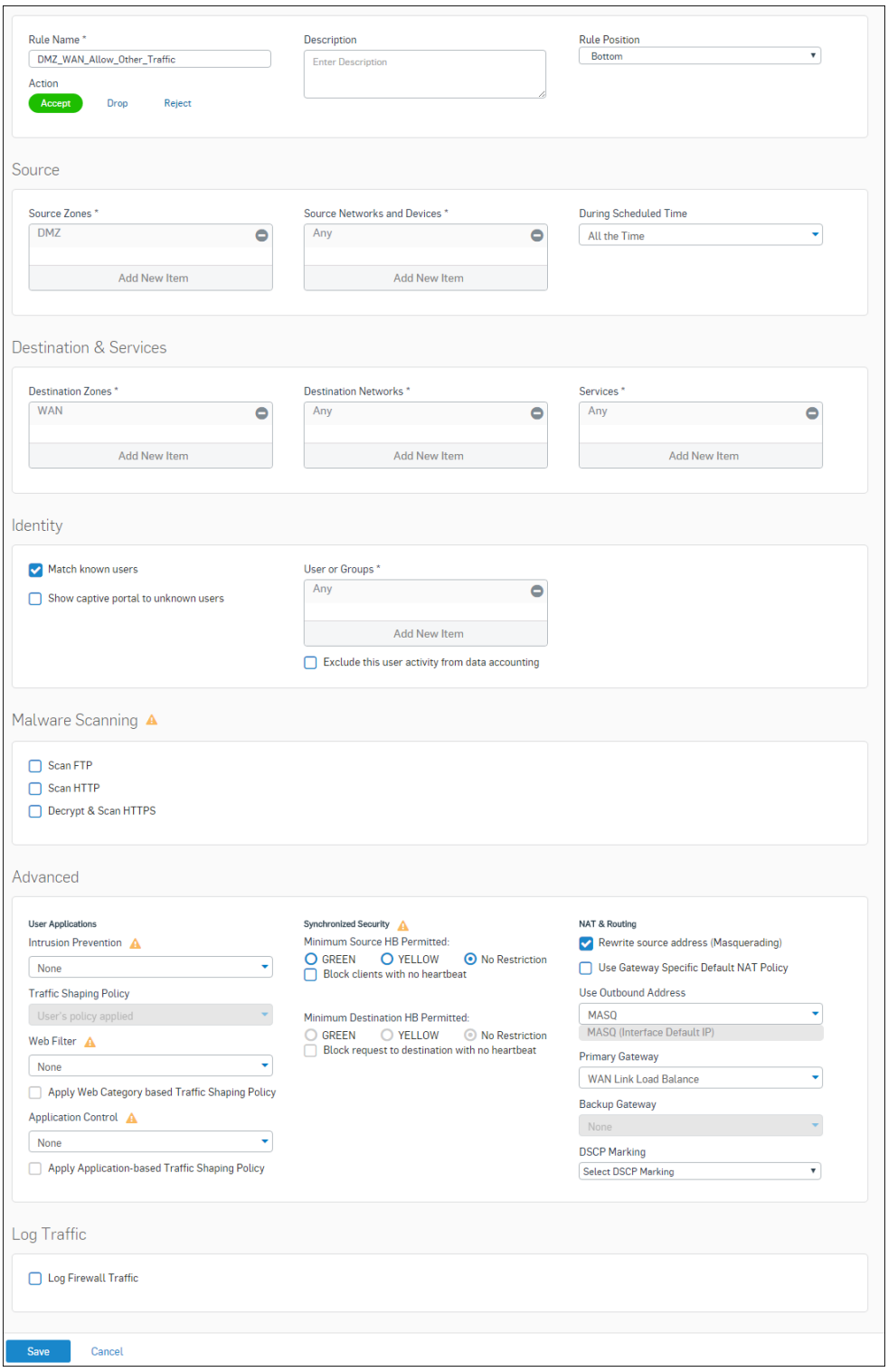
2. Set **Application Template** to **Email Servers (SMTP)** and enter the details.



Note:
EmailServer(SMTP) applies only to SMTP/S traffic. To enable scanning of POP/S-IMAP/S traffic, use the application template EmailClients(POP & IMAP).

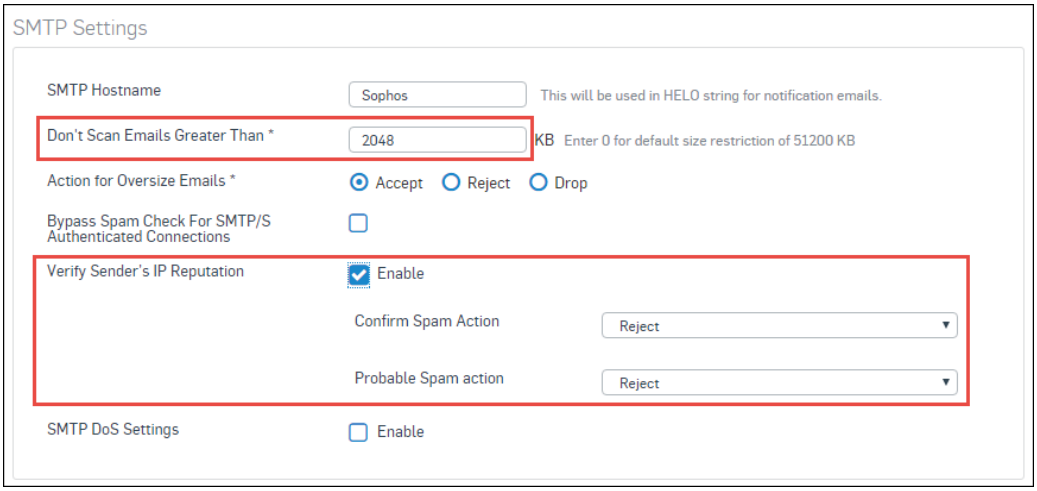
Step 2: Create Network Rule to allow all traffic to and from Protected Network (DMZ)

Go to **Protect > Firewall**, click **Add Firewall Rule** and click **User/Network Rule**. Enter the details to create the rule.



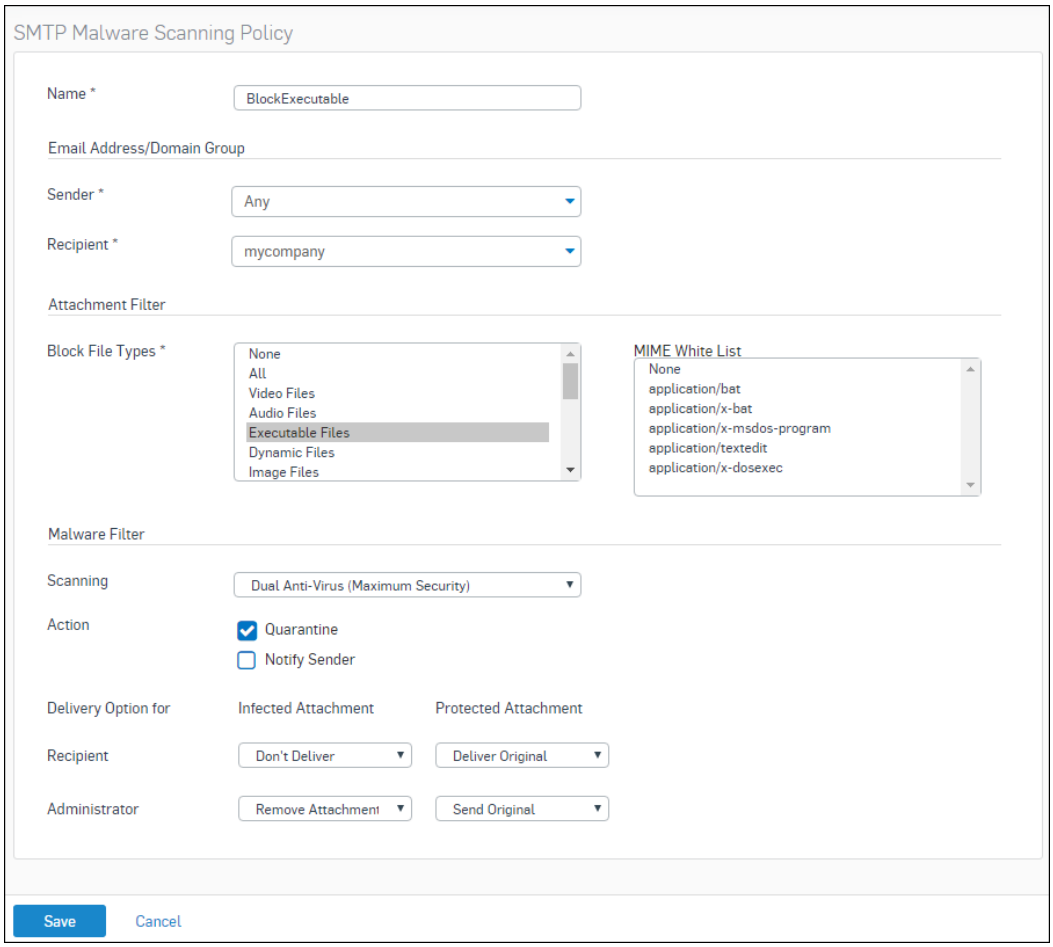
Step 3: Configure Global Email Settings

Go to **Email > Common Settings** and configure the required global settings to be applied on Email traffic. Example: We have enabled IP Reputation and set the restriction on email size for scanning to 2 MB (2048 KB).



Step 4: Create Malware Scanning Policy

Go to **Email Protection > Policies**, click **Add Policy** and click **Add SMTP Malware Scanning Policy**.



Step 5: Create SMTP and POP/IMAP Scanning Policies

You can create multiple scanning policies to define the actions that SF-OS must take if an email is identified as spam. We recommend that you create all the rules listed in the table to protect your network against spam. Scanning policies are processed in a top down manner and the first suitable rule is applied. Hence, when adding multiple rules, place the specific rules above the general rules.

Rule	Type of Rule	Purpose
inbound_SMTP_policy1	SMTP Scanning Policy	Drops emails destined to mycompany.com identified as spam over SMTP/S
inbound_SMTP_policy2	SMTP Scanning Policy	Drops emails destined to mycompany.com identified as Virus Outbreak over SMTP/S.
inbound_SMTP_policy3	SMTP Scanning Policy	Adds prefix “Spam (RBL):” to the subject in emails destined to mycompany.com which are

		identified as spam by the configured RBL(s).
DOMAIN_ACCEPT _inbound_SMTP	SMTP Scanning Policy	Accepts all emails destined to mycompany.com.
outbound_SMTP_policy1	SMTP Scanning Policy	Drops all emails originating from mycompany.com detected as spam.
outbound_SMTP_policy2	SMTP Scanning Policy	Drops all emails originating from mycompany.com with content that matches the configured Data Protection Policy.
DOMAIN_ACCEPT _outbound_SMTP	SMTP Scanning Policy	Accepts all emails originating from mycompany.com.
No_Open_Relay	SMTP Scanning Policy	Drops all emails over SMTP/S. This rule prevents the email server from being used as an open relay.
inbound_POPIMAP_policy1	POP-IMAP Scanning Policy	Adds prefix "POPIMAPSpam:" to subject in emails destined to mycompany.com identified as spam over POP/S-IMAP/S.
inbound_POPIMAP_policy2	POP-IMAP Scanning Policy	Adds prefix "POPIMAPVirusOutbreak:" to subject in emails destined to mycompany.com which are identified as Virus Outbreak over POP/S-IMAP/S.

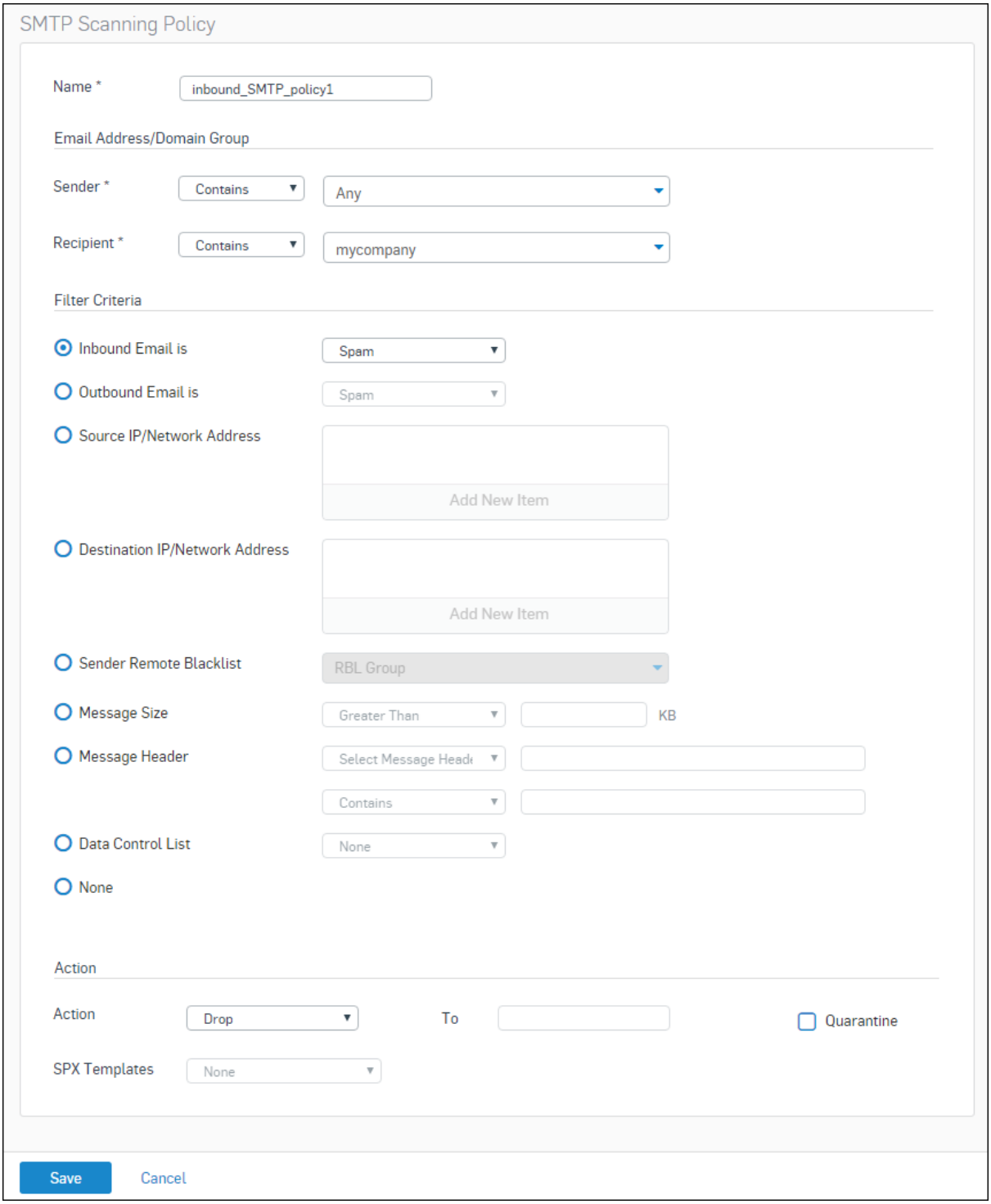
Note:

Since we have created a Business Application Rule with the template "EmailServer(SMTP)", only SMTP/S traffic is scanned through the scanning policies.

Name	Sender	Recipient	Details	Action	Manage
default-smtp-av av/smtp	Any	Any	Enable	Receiver Action Infected : Don't . . . Protected : Del. . . Notify Admin Infected : Don't . . . Protected : Don. . .	
inbound_SMTP_policy1 as/smtp	Any	mycompany	Mail is identified as Spam by Inbound Anti Spam Module	Drop	
inbound_SMTP_policy2 as/smtp	Any	mycompany	Mail is identified as Virus Outbreak by Inbound Anti Spam Mo . . .	Drop	
inbound_SMTP_policy3 as/smtp	Any	mycompany	Sender IP Address Black Listed By Premium RBL Services	Prefix Subject To. . .	
DOMAIN_ACCEPT_inb . . . as/smtp	Any	mycompany	None	Accept	
outbound_SMTP_pol . . . as/smtp	mycompany	Any	Mail is identified as Spam by Outbound Anti Spam Module	Drop	
outbound_SMTP_pol . . . as/smtp	mycompany	Any	Data Control List	Drop	
DOMAIN_ACCEPT_out . . . as/smtp	mycompany	Any	None	Accept	
No_Open_Relay as/smtp	Any	Any	None	Drop	
inbound_POPIMAP_p . . . pop3/imap	Any	mycompany	Mail is identified as Spam by Inbound Anti Spam Module	Prefix Subject To. . .	
inbound_POPIMAP_p . . . pop3/imap	Any	mycompany	Mail is identified as Virus Outbreak by Inbound Anti Spam Mo . . .	Prefix Subject To. . .	
default-pop-av pop3/imap	Any	Any	Enable	Accept	
rule2 pop3/imap	Any	Any	Mail is identified as probable Virus Outbreak by Inbound Ant . . .	Prefix Subject To. . .	
rule1 pop3/imap	Any	Any	Mail is identified as Virus Outbreak by Inbound Anti Spam Mo . . .	Prefix Subject To. . .	

Example: Create inbound_SMTP_policy1 to drop emails destined to mycompany.com which are identified as spam over SMTP/S.

Go to **Email Protection > Policies**, click **Add Policy** and click **Add SMTP Scanning Policy**.



Results

Your internal email server is now protected. All emails to and from the server will be scanned and filtered.

Suggested Reading

- Deploy SF-OS in MTA Mode
- Ensure Scanning of Outgoing Email Traffic

Copyright Notice