



Pocket Guide

Protect Internal Email Server
(Legacy Mode)

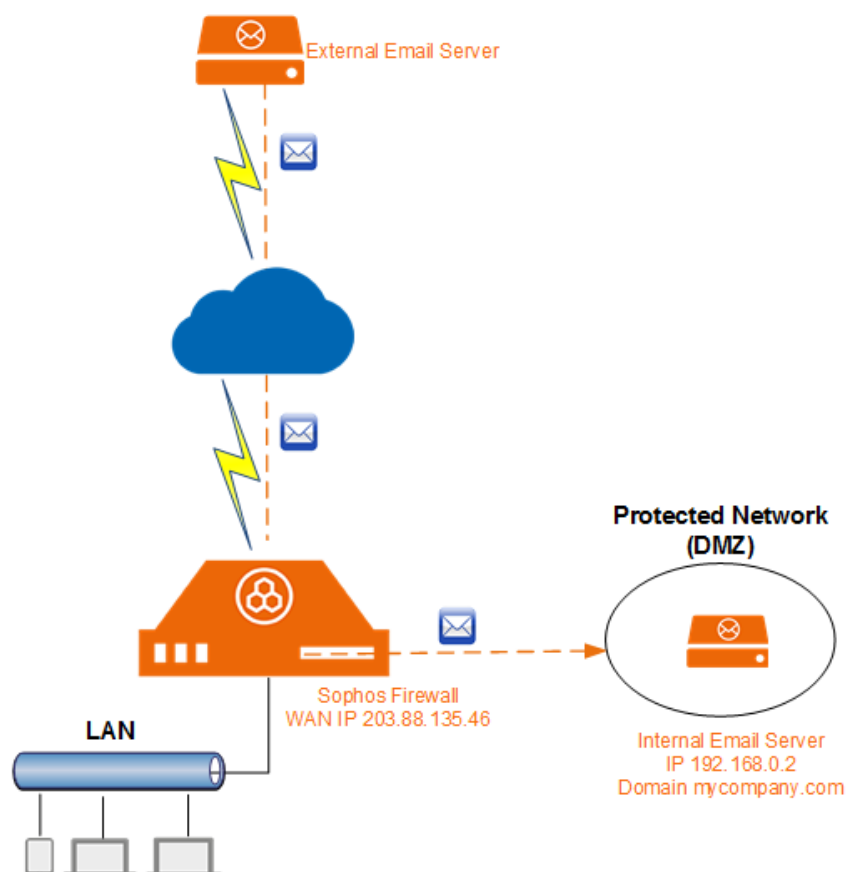
Product: Sophos XG Firewall

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.

Protect Internal Email Server (Legacy Mode)

Application Template Email Servers(SMTP)	Description Allows routing of SMTP traffic to Email server for scanning by Email Scanning Rules.	Rule Position Top
Rule Name * ProtectEmailServer		
Source		
Source Zones * WAN	Allowed Client Networks * Any	Blocked Client Networks
Add New Item	Add New Item	Add New Item
Destination & Service		
Destination Host/Network * #PortE1-203.88.135.46	Forward Type Port List	Service Port(s) Forwarded * 25,587,465 To
		Ex : 23,80,8090,...
		Protocol <input checked="" type="radio"/> TCP <input type="radio"/> UDP
Forward To		
Protected Server(s) * InternalMailServer-192.168.0.2	Mapped Port Type Port List	Mapped Port * 25,587,465 To
Protected Zone * DMZ		Ex : 23,80,8090,...
		<input type="checkbox"/> Change Destination Port(s)
Malware Scanning		
<input checked="" type="checkbox"/> Scan SMTP		
<input checked="" type="checkbox"/> Scan SMTPS		
Advanced		
Policies for Business Applications Intrusion Prevention None	Synchronized Security Minimum Source HB Permitted: <input type="radio"/> GREEN <input type="radio"/> YELLOW <input checked="" type="radio"/> No Restriction <input type="checkbox"/> Block clients with no heartbeat	Routing <input type="checkbox"/> Rewrite source address (Masquerading) <input checked="" type="checkbox"/> Create Reflexive Rule
Traffic Shaping None	Minimum Destination HB Permitted: <input type="radio"/> GREEN <input type="radio"/> YELLOW <input checked="" type="radio"/> No Restriction <input type="checkbox"/> Block request to destination with no heartbeat	
Log Traffic		
<input type="checkbox"/> Log Firewall Traffic		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

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.

The screenshot displays the configuration page for a Firewall Rule. The fields are as follows:

- Rule Name:** DMZ_WAN_Allow_Other_Traffic
- Description:** Enter Description
- Rule Position:** Bottom
- Action:** Accept (selected), Drop, Reject
- Source:**
 - Source Zones: DMZ
 - Source Networks and Devices: Any
 - During Scheduled Time: All the Time
- Destination & Services:**
 - Destination Zones: WAN
 - Destination Networks: Any
 - Services: Any
- Identity:**
 - Match known users:
 - Show captive portal to unknown users:
 - User or Groups: Any
 - Exclude this user activity from data accounting:
- Malware Scanning:**
 - Scan FTP:
 - Scan HTTP:
 - Decrypt & Scan HTTPS:
- Advanced:**
 - User Applications:** Intrusion Prevention: None; Traffic Shaping Policy: User's policy applied; Web Filter: None; Application Control: None.
 - Synchronized Security:** Minimum Source HB Permitted: No Restriction; Minimum Destination HB Permitted: No Restriction.
 - NAT & Routing:** Rewrite source address (Masquerading): ; Use Gateway Specific Default NAT Policy: ; Use Outbound Address: MASQ; Primary Gateway: WAN Link Load Balance; Backup Gateway: None; DSCP Marking: Select DSCP Marking.
- Log Traffic:** Log Firewall Traffic:

Buttons: Save, Cancel

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).

The screenshot shows the 'SMTP Settings' configuration page. The 'SMTP Hostname' is set to 'Sophos'. The 'Don't Scan Emails Greater Than *' field is set to '2048' KB. The 'Action for Oversize Emails *' is set to 'Accept'. The 'Bypass Spam Check For SMTP/S Authenticated Connections' checkbox is unchecked. The 'Verify Sender's IP Reputation' checkbox is checked and labeled 'Enable'. Below this, the 'Confirm Spam Action' and 'Probable Spam action' dropdown menus are both set to 'Reject'. The 'SMTP DoS Settings' checkbox is unchecked.

Step 4: Create Malware Scanning Policy

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

SMTP Malware Scanning Policy

Name *

Email Address/Domain Group _____

Sender *

Recipient *

Attachment Filter

Block File Types *
MIME White List

Malware Filter

Scanning

Action Quarantine Notify Sender

Delivery Option for Infected Attachment Protected Attachment

Recipient

Administrator

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.

Protect Internal Email Server (Legacy Mode)

Name	Sender	Recipient	Details	Action	Manage
default-smtp-av <small>(as/smtp)</small>	Any	Any	Enable	Receiver Action Infected : Don't ... Protected : Del ... Notify Admin Infected : Don't ... Protected : Don ...	
inbound SMTP_policy1 <small>(as/smtp)</small>	Any	mycompany	Mail is identified as Spam by Inbound Anti Spam Module	Drop	
inbound SMTP_policy2 <small>(as/smtp)</small>	Any	mycompany	Mail is identified as Virus Outbreak by Inbound Anti Spam Mo ...	Drop	
inbound SMTP_policy3 <small>(as/smtp)</small>	Any	mycompany	Sender IP Address Black Listed By Premium RBL Services	Prefix Subject To ...	
DOMAIN_ACCEPT_inb... <small>(as/smtp)</small>	Any	mycompany	None	Accept	
outbound SMTP_pol... <small>(as/smtp)</small>	mycompany	Any	Mail is identified as Spam by Outbound Anti Spam Module	Drop	
outbound SMTP_pol... <small>(as/smtp)</small>	mycompany	Any	Data Control List	Drop	
DOMAIN_ACCEPT_out... <small>(as/smtp)</small>	mycompany	Any	None	Accept	
No Open Relay <small>(as/smtp)</small>	Any	Any	None	Drop	
inbound POPIMAP p... <small>(pop3/imap)</small>	Any	mycompany	Mail is identified as Spam by Inbound Anti Spam Module	Prefix Subject To ...	
inbound POPIMAP p... <small>(pop3/imap)</small>	Any	mycompany	Mail is identified as Virus Outbreak by Inbound Anti Spam Mo ...	Prefix Subject To ...	
default-pop-av <small>(pop3/imap)</small>	Any	Any	Enable	Accept	
rule2 <small>(pop3/imap)</small>	Any	Any	Mail is identified as probable Virus Outbreak by Inbound Ant ...	Prefix Subject To ...	
rule1 <small>(pop3/imap)</small>	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**.

SMTP Scanning Policy

Name *

Email Address/Domain Group

Sender *

Recipient *

Filter Criteria

Inbound Email is

Outbound Email is

Source IP/Network Address

Destination IP/Network Address

Sender Remote Blacklist

Message Size KB

Message Header

Data Control List

None

Action

Action To Quarantine

SPX Templates

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

Copyright 2015-2016 Sophos Limited. All rights reserved.

Sophos is registered trademark of Sophos Limited and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.