



Pocket Guide

Protect Internal Email Server
(MTA Mode)

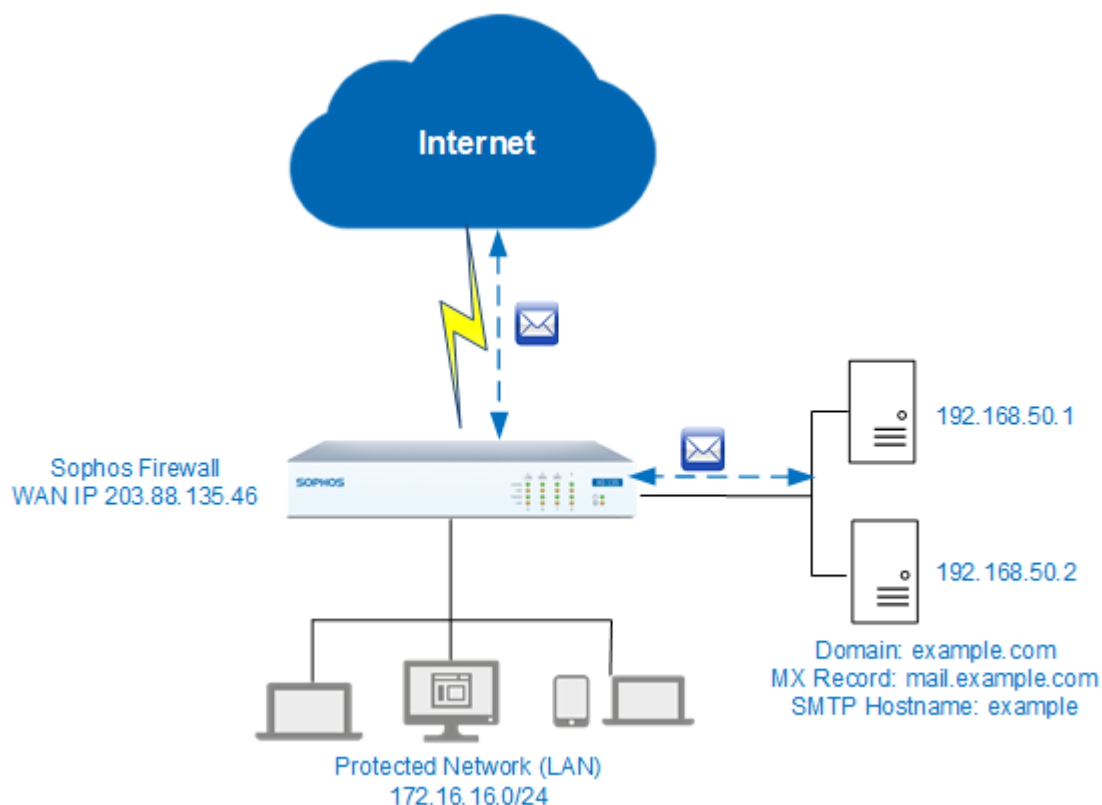
Product: Sophos XG Firewall

Contents

Scenario	2
Prerequisites	2
Configuration.....	3
Step 1: Switch to MTA Mode	3
Step 2: Enable SMTP Relay from WAN.....	4
Step 3: Configure SMTP TLS Certificate	4
Step 4: Configure Global Email Settings.....	4
Step 5: Scan and Filter Inbound Emails.....	6
Step 6: Scan and Filter Outbound Emails.....	7
Result.....	7
Copyright Notice.....	8

Scenario

Configure Sophos XG Firewall (SF-OS) to route emails between the Internet and an internal email domain, which can be hosted on multiple servers. Set policies to enable malware and spam scanning, and email filtering of inbound and outbound emails.



Prerequisites

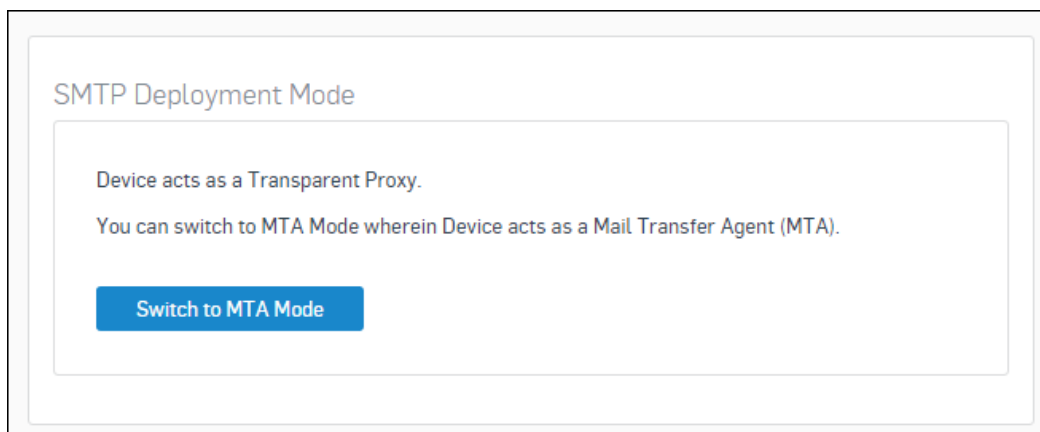
- Read-write permissions on the SF-OS Admin Console for the relevant features.
- Subscription to the Email Protection module (**Administration > Licensing**).
- Plugged in and connected interfaces to WAN (Internet) and DMZ (containing the servers) zones (**Network > Interfaces**).
- Email server's MX record to point to the SF-OS WAN interface.

Configuration

Log in to the SF-OS Admin Console.

Step 1: Switch to MTA Mode

If legacy mode is enabled, go to **Protect > Email > General Settings** and click **Switch to MTA Mode**.



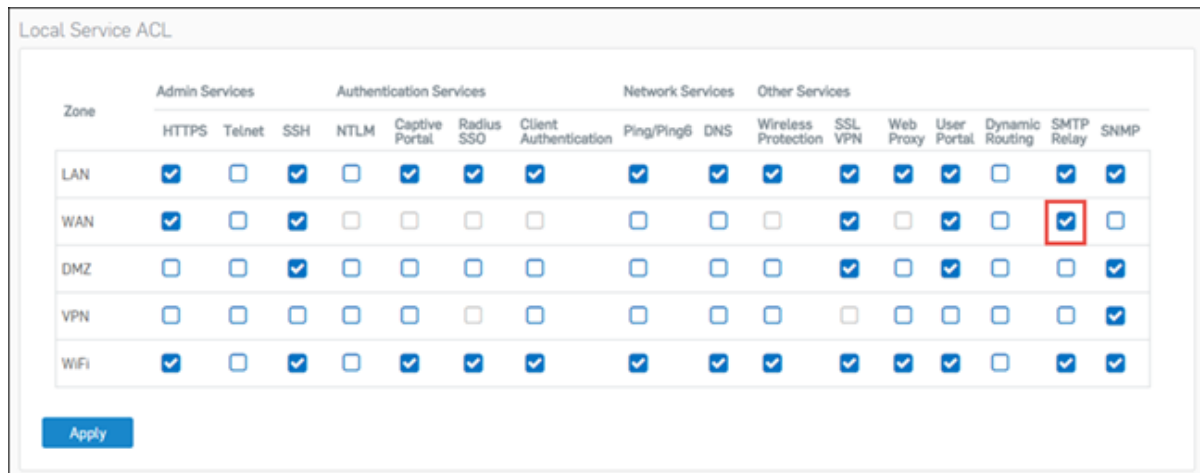
A firewall rule to forward SMTP/SMTSPS traffic is automatically created.

The screenshot shows the Firewall Rule configuration page. It features a table with columns for Rule, Source, Destination, What, and Action. There are two rules listed:

Rule	Source	Destination	What	Action
Auto added firewall policy f... [ID:1] in 0 B, out 0 B	Any Zone Any Host	Any Zone Any Host	SMTP, SMTSPS	Forward
any-to-any [ID:2] in 564.42 KB, out 384.69 KB	Any Zone Any Host	Any Zone Any Host	Any Service	Accept

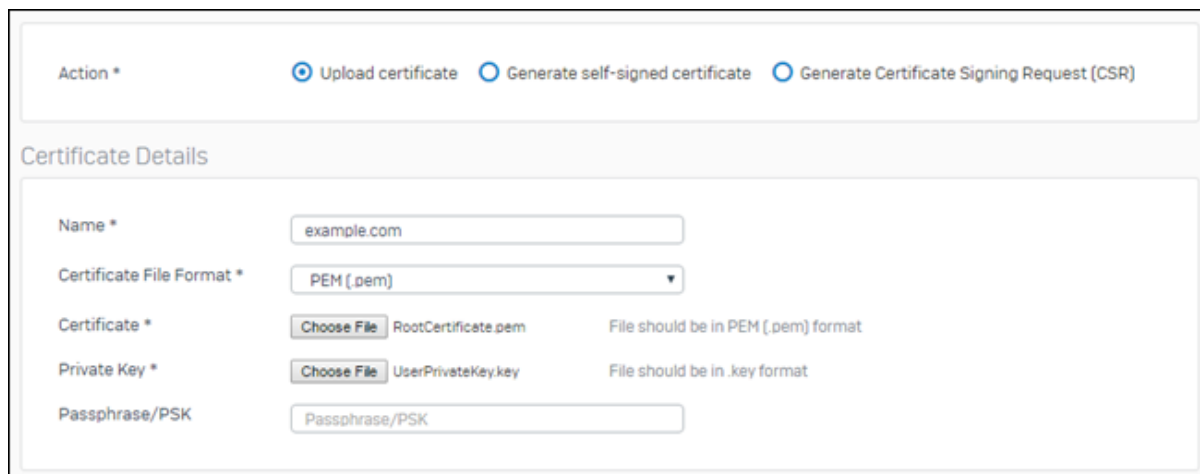
Step 2: Enable SMTP Relay from WAN

Go to **System > Administration > Device Access**. Enable SMTP Relay for WAN zone to allow emails from WAN to LAN.



Step 3: Configure SMTP TLS Certificate

Go to **System > Certificates > Certificates > Add** to upload the email server certificate to SF-OS.



Step 4: Configure Global Email Settings

Go to **Protect > Email > General Settings**. In SMTP Settings, configure the SMTP hostname, IP Reputation and SMTP DoS settings.

SMTP Settings

SMTP Hostname	<input type="text" value="example.com"/>	This will be used in HELO and SMTP greeting strings.
Don't Scan Emails Greater Than *	<input type="text" value="0"/>	KB Enter 0 for default size restriction of 51200 KB
Action for Oversize Emails *	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Verify Sender's IP Reputation	<input checked="" type="checkbox"/> Enable	
	Confirm Spam Action	<input type="text" value="Reject"/>
	Probable Spam action	<input type="text" value="Reject"/>
SMTP DoS Settings	<input checked="" type="checkbox"/> Enable	
Maximum Connections *	<input type="text" value="5000"/>	
Maximum Connections/Host *	<input type="text" value="100"/>	
Maximum Emails/Connection *	<input type="text" value="1000"/>	
Maximum Recipients/Email *	<input type="text" value="100"/>	
Emails Rate *	<input type="text" value="1000"/>	Per Minute/Host
Connections Rate *	<input type="text" value="100"/>	Per Second/Host

In SMTP TLS Configuration, set TLS Certificate to the uploaded certificate.

TLS Certificate *	<input type="text" value="example.com"/>
Allow Invalid Certificate	<input checked="" type="checkbox"/> Enable
Require TLS Negotiation with Host/Net	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <div style="text-align: center; background-color: #f0f0f0; padding: 5px;">Add New Item</div>
Require TLS Negotiation with Sender Domain	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <div style="text-align: center; background-color: #f0f0f0; padding: 5px;">Add New Item</div>
Skip TLS Negotiation Hosts/Nets	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <div style="text-align: center; background-color: #f0f0f0; padding: 5px;">Add New Item</div>

Step 5: Scan and Filter Inbound Emails

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

Select the internal domain and enter its static IP addresses.

SMTP Policy

Name *
Protect_Example

Domains And Routing Target

Domain *
example
Add New Item

Global Action
Accept

SPX Template
None

Route By
Static Host

Host List
type to search... Create
192.168.50.1
192.168.50.2

Selected Host
192.168.50.1
192.168.50.2

Turn on **Spam Protection** and retain the default settings.

Spam Protection

Check for Inbound Spam
 Check for Virus Outbreak
 Check for Outbound Spam
 Check for RBL

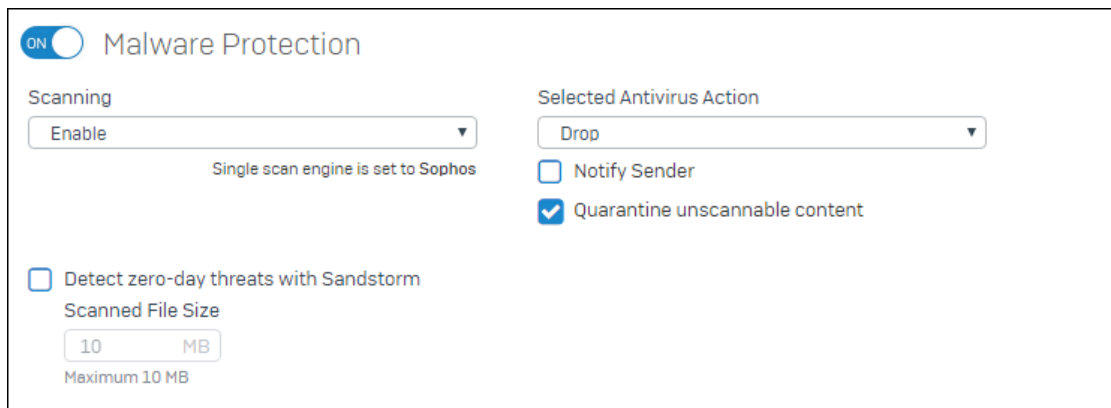
Premium RBL Services
Standard RBL Services
Add New Item

Spam Action
Drop

Probable Spam Action
Warn

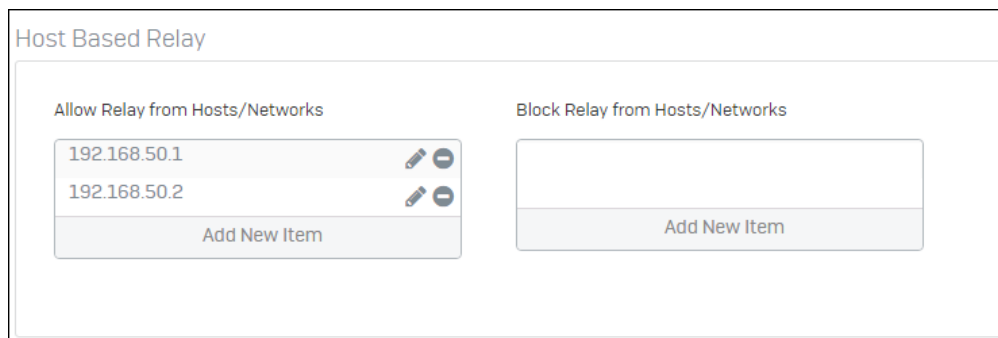
Prefix Subject
[SPAM]

Turn on **Malware Protection** and retain the default settings.

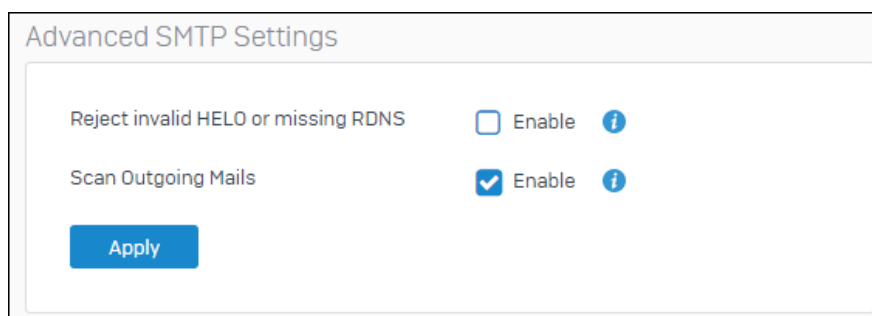


Step 6: Scan and Filter Outbound Emails

- a. Go to **Protect > Email > Relay Settings**. In Host Based Relay, enter the IP addresses of both the email servers in **Allow Relay from Hosts/Networks**.



- b. Go to **Protect > Email > General Settings**. In Advanced SMTP Settings, enable **Scan Outgoing Mails**.



Result

All emails to and from the servers will be scanned and filtered.

Copyright Notice

Copyright 2016-2017 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.