SOPHOS
Security made simple.

Pocket Guide

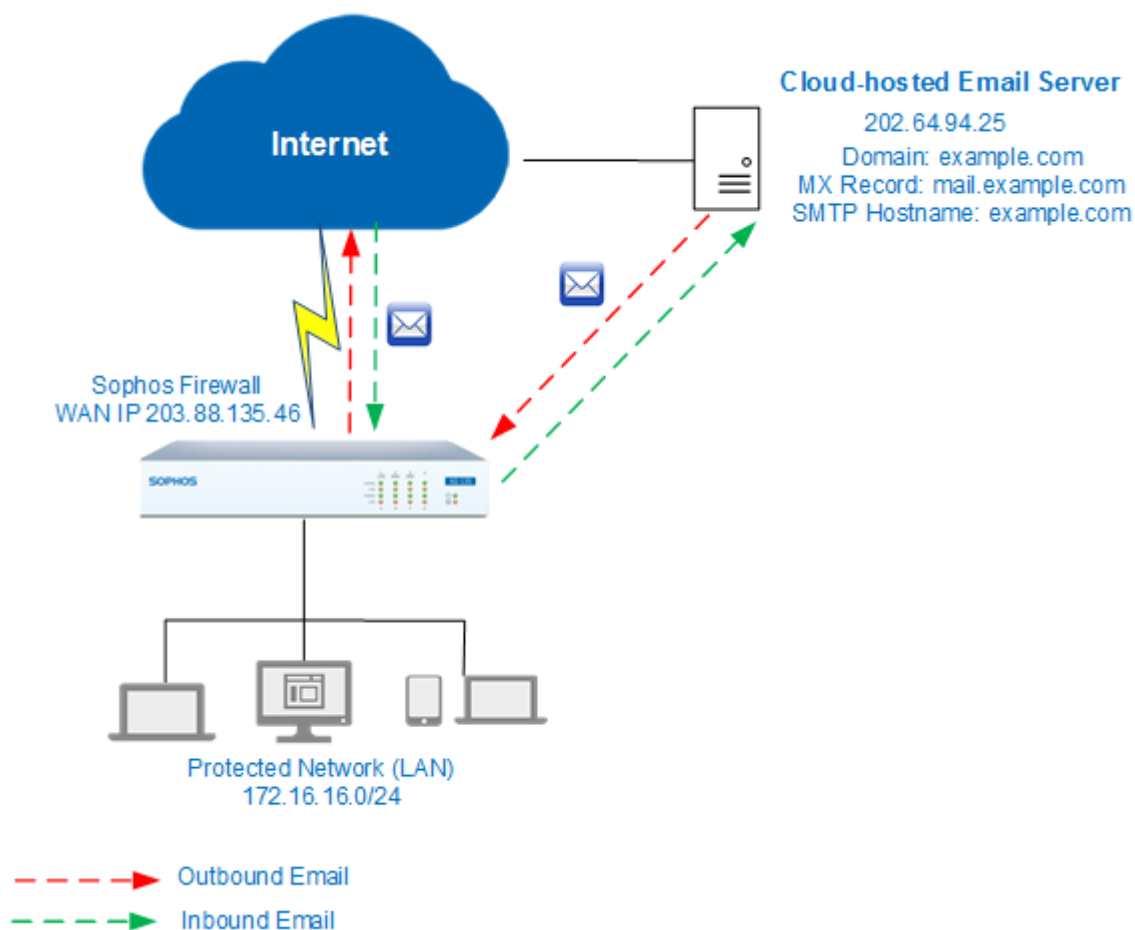## Protect Cloud-hosted Email Server (MTA Mode)

Product: Sophos XG Firewall

Contents

Scenario

Configure Sophos XG Firewall (SF-OS) to route emails between the Internet and a cloud-hosted email server. Set policies to enable malware and spam scanning, and email filtering of inbound and outbound emails.
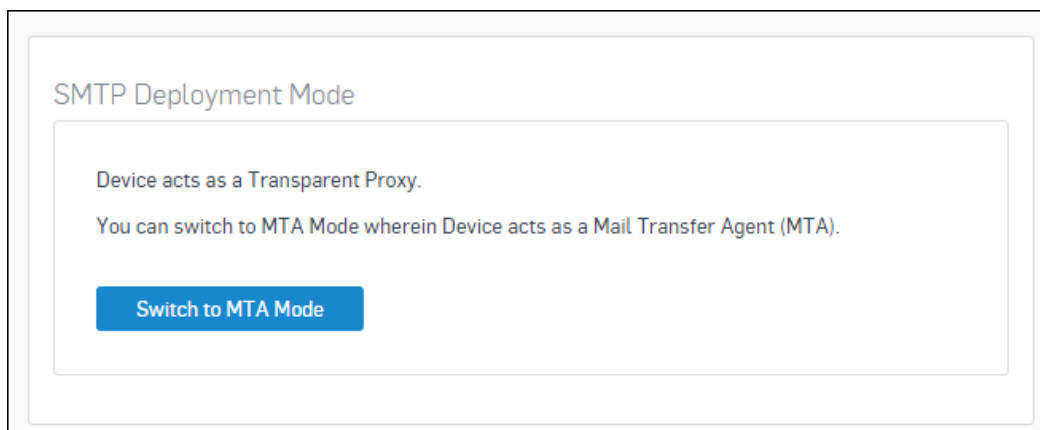

Prerequisites

- 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.
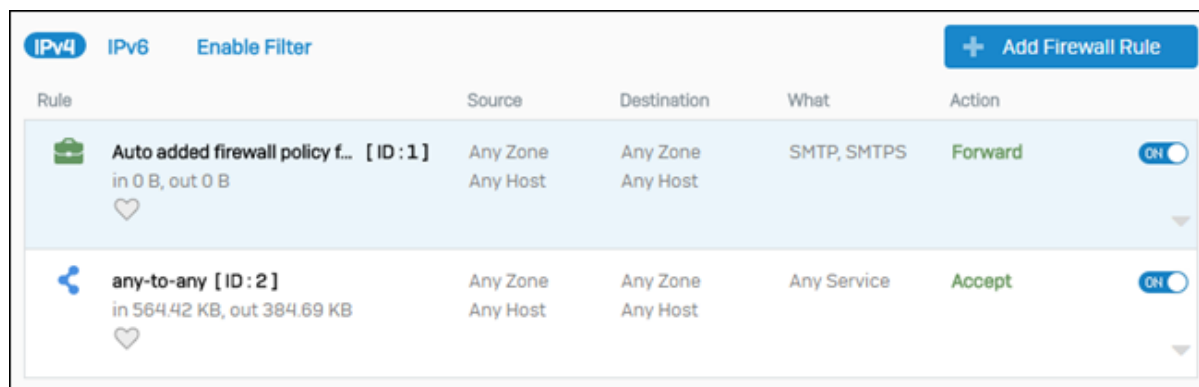- Email server to allow relay of emails to and from SF device.

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**.

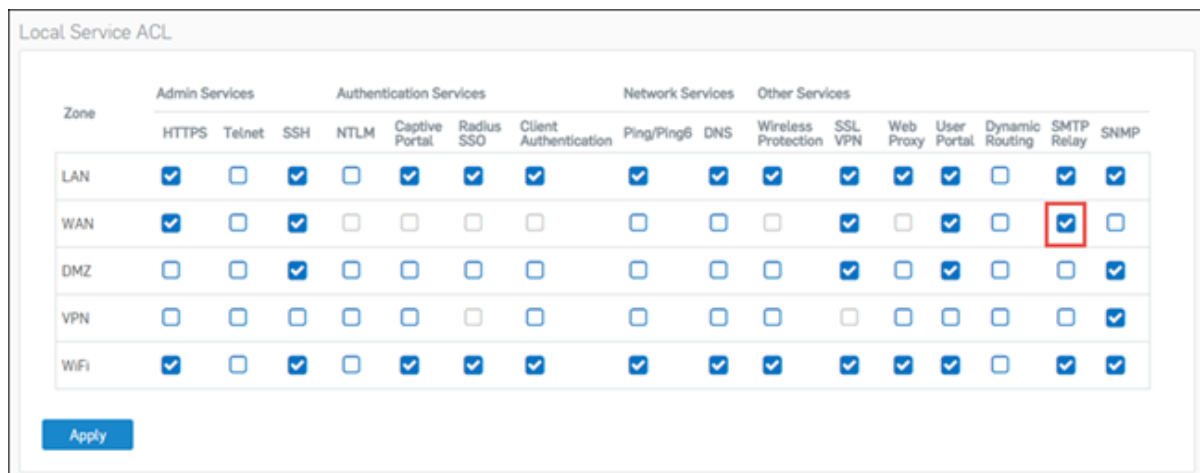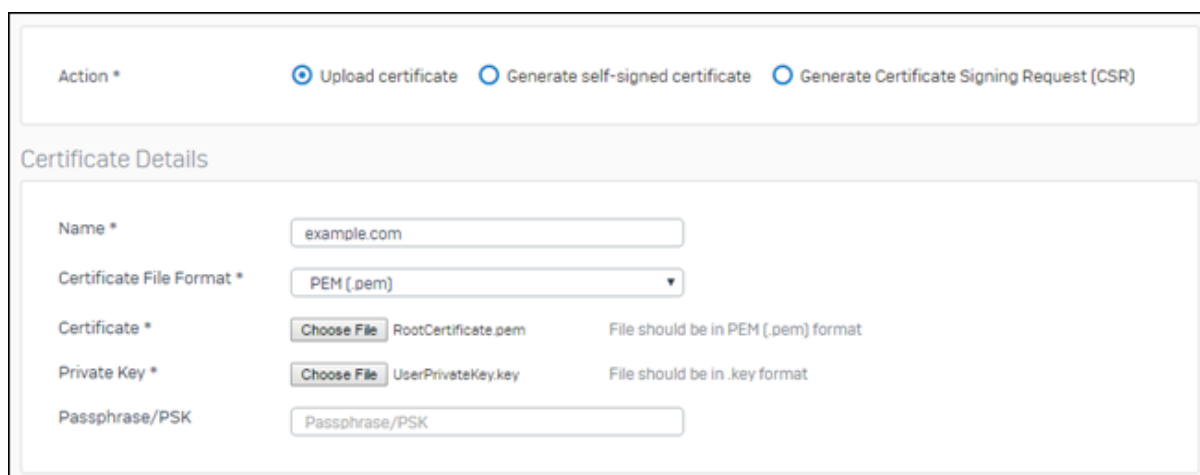A firewall rule to forward SMTP/SMTPS traffic is automatically created.

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.

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

Step 5: Scan and Filter Inbound Emails

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

Select the cloud-hosted domain and enter its static IP address.

SMTP Policy

Name *

Protect_Example

Domains And Routing Target

Domain *	Global Action	SPX Template
example	Accept ▼	None ▼
Add New Item		

Route By

Static Host ▼

Host List

type to search... Create

☑ 202.64.94.25

Selected Host

202.64.94.25 ✖

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

ON ◯ Spam Protection

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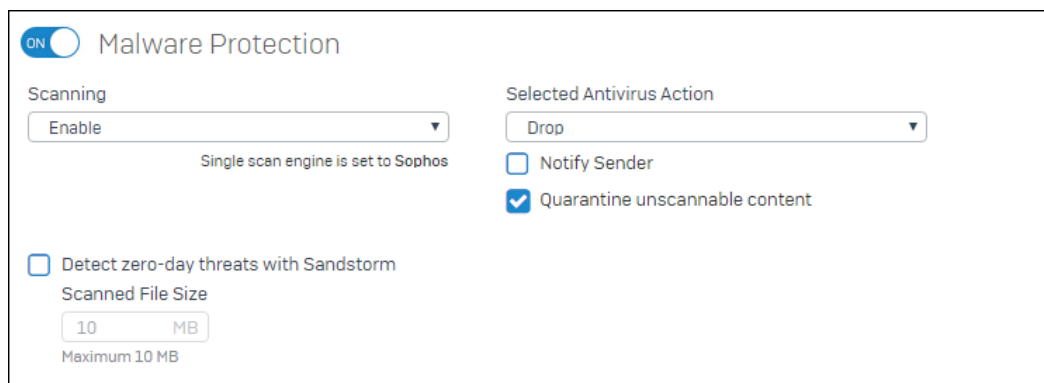☑ Check for Outbound Spam
☑ Check for RBL

Premium RBL Services ⊖
Standard RBL Services ⊖
Add New Item

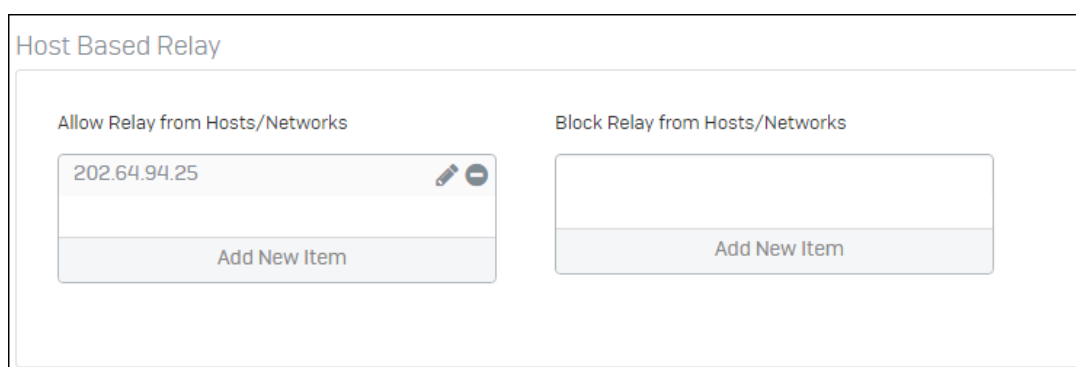| Spam Action	Probable Spam Action
Drop ▼	Warn ▼

Prefix Subject

[SPAM]

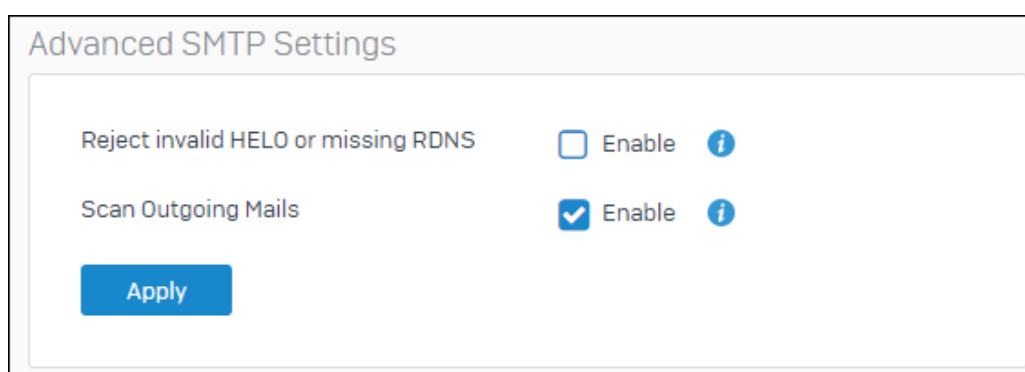Turn on **Malware Protection** and retain the default settings.

Step 6: Scan and Filter Outbound Emails

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

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

Results

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

Copyright Notice