SOPHOS
Security made simple.

Pocket Guide

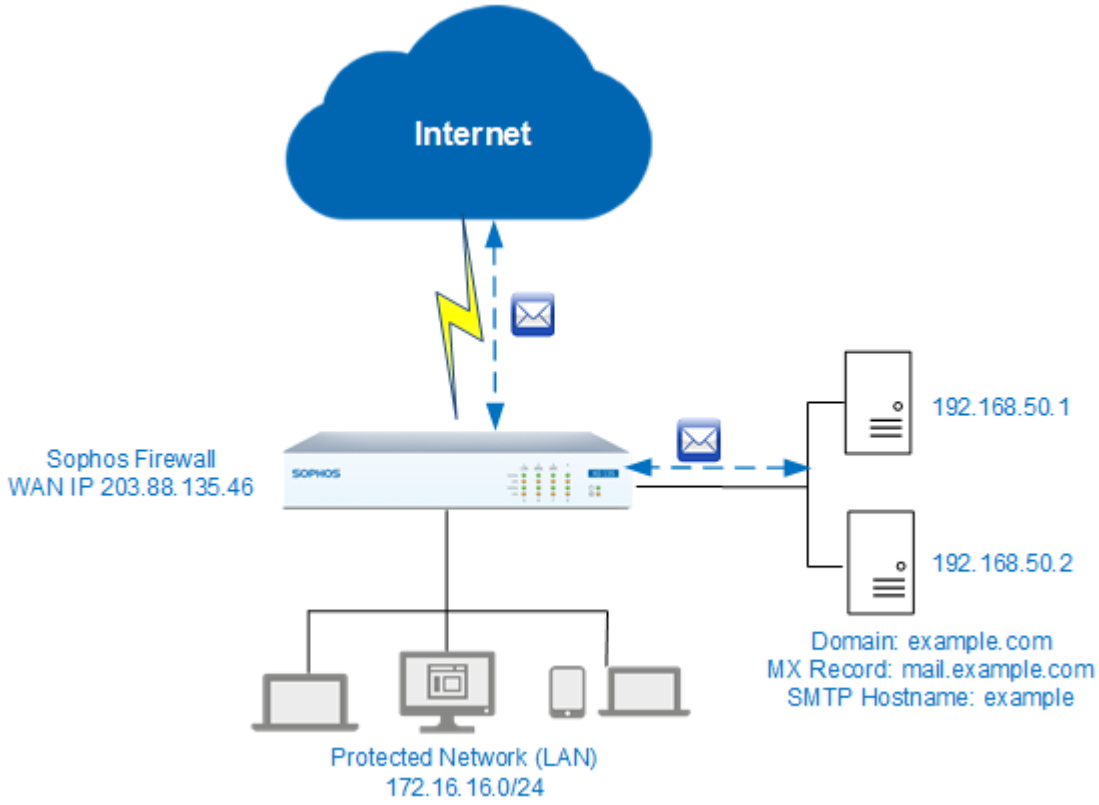
Protect Internal Email Server (MTA Mode)

Product: Sophos XG Firewall

Contents

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

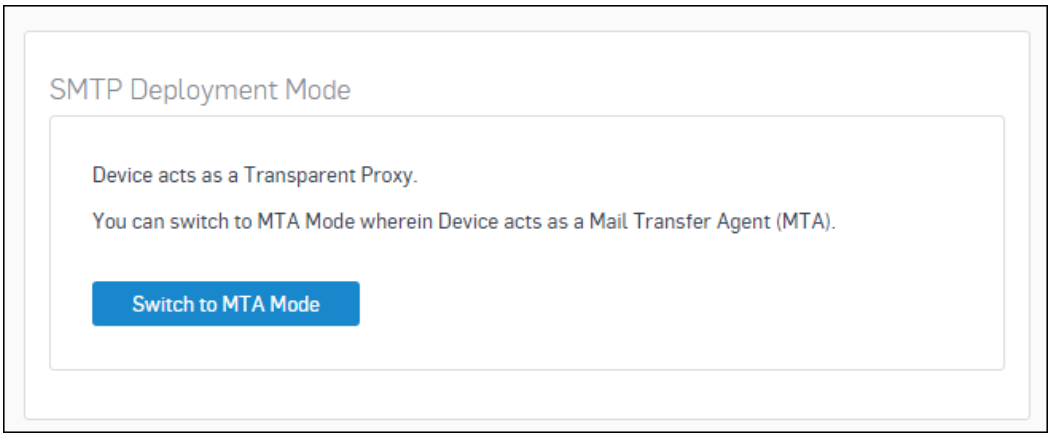
- Read-write permissions on the SF-OS Admin Console for the relevant features.
- Subscription to the Email Protection module **(Administration > Licensing)**.
- Plugged in and connected interfaces to WAN (Internet) and DMZ (containing the servers) zones **(Network > Interfaces)**.
- Email server's MX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

Configuration

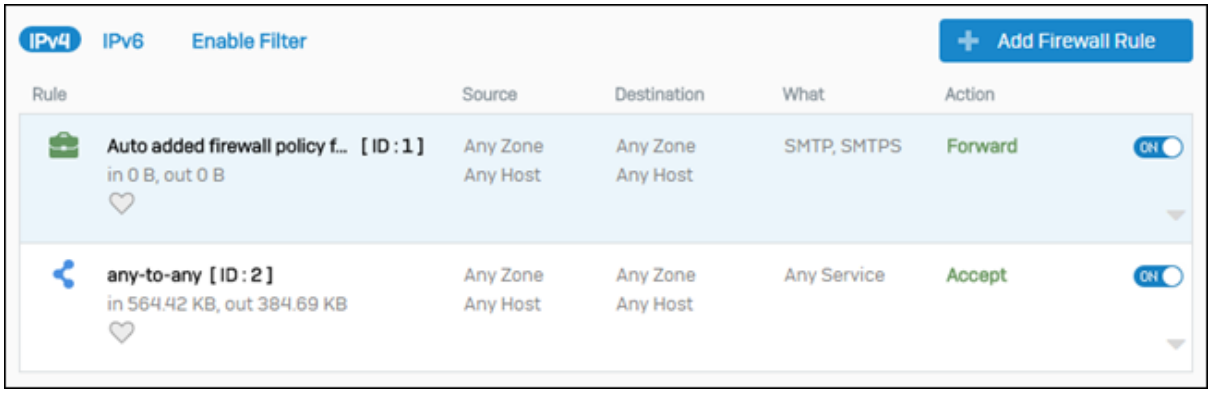
Log in to the SF-OS Admin Console.

Step 1: Switch to MTA Mode

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

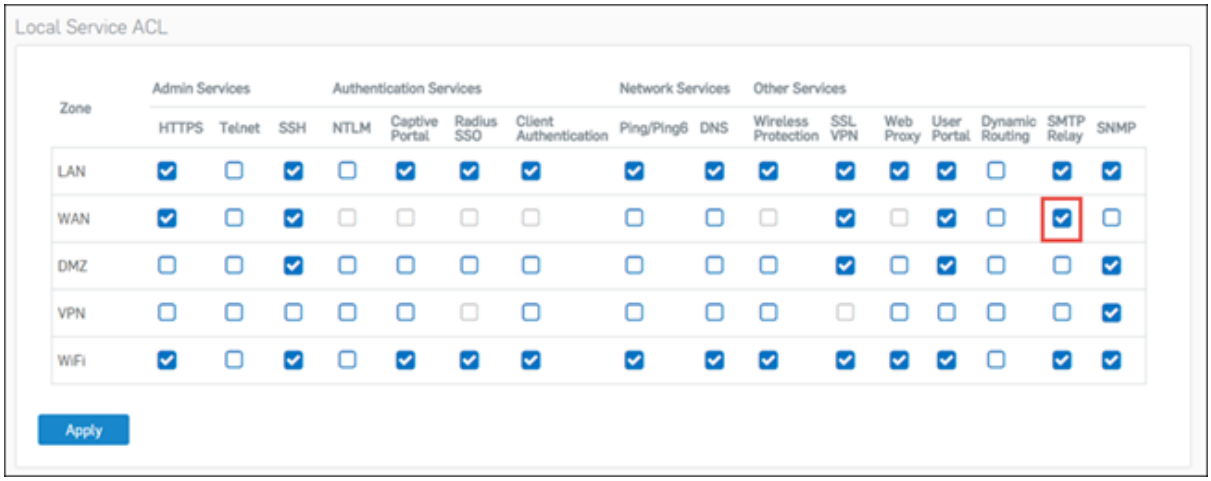


A firewall rule to forward SMTP/SMTPS traffic is automatically created.



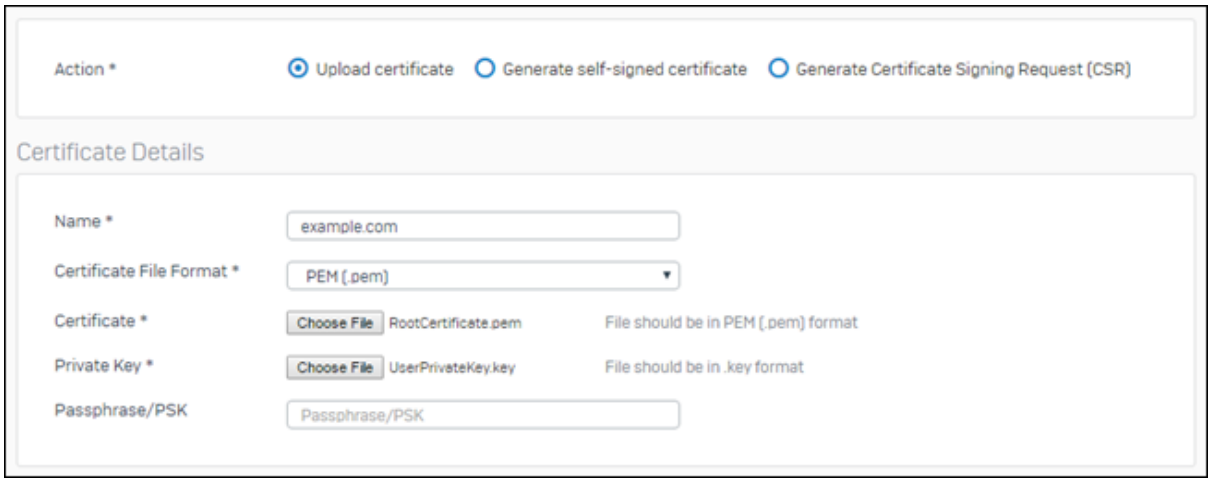
Step 2: Enable SMTP Relay from WAN

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



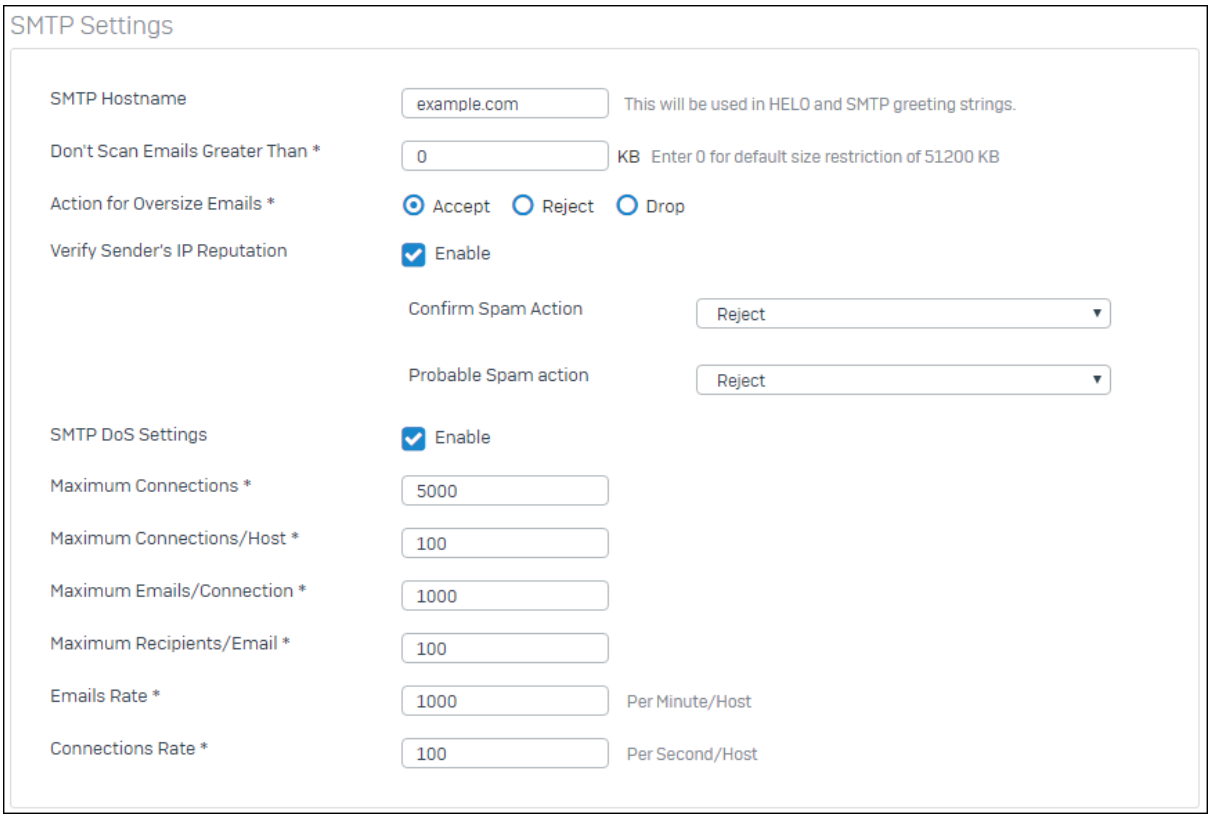
Step 3: Configure SMTP TLS Certificate

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

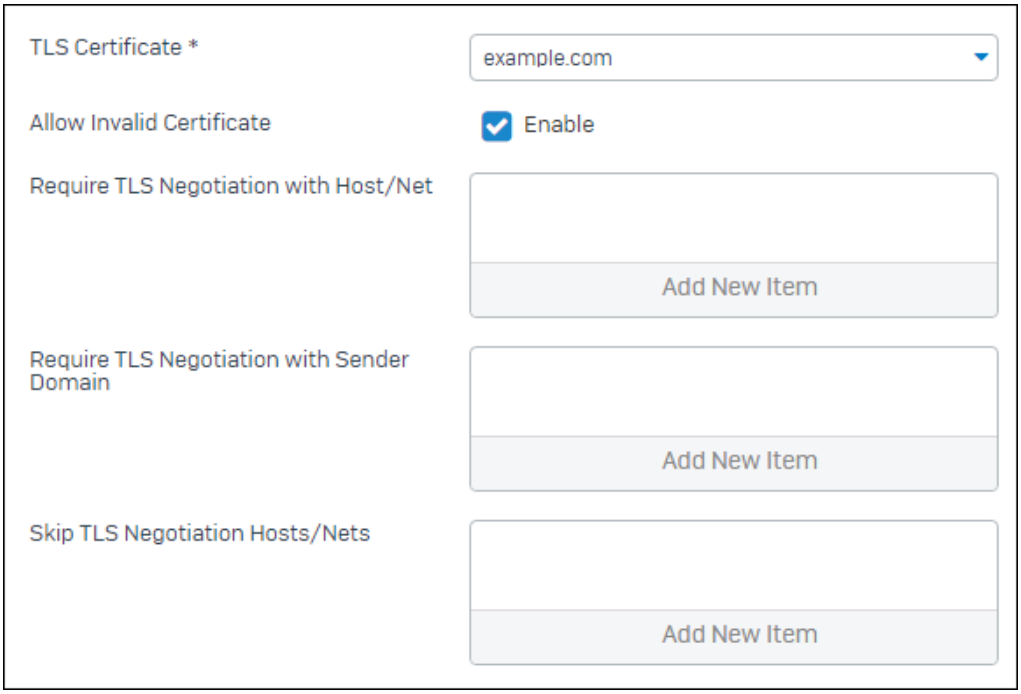


Step 4: Configure Global Email Settings

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



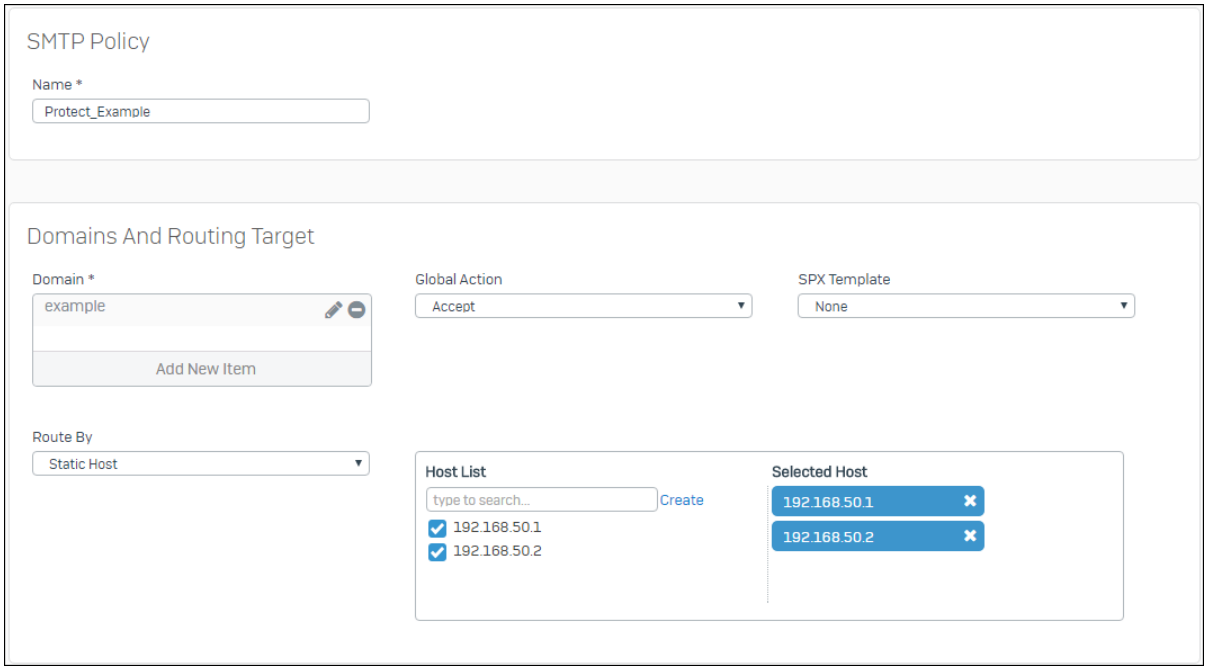
In **SMTP TLS Configuration**, set **TLS Certificate** to the uploaded certificate.



Step 5: Scan and Filter Inbound Emails

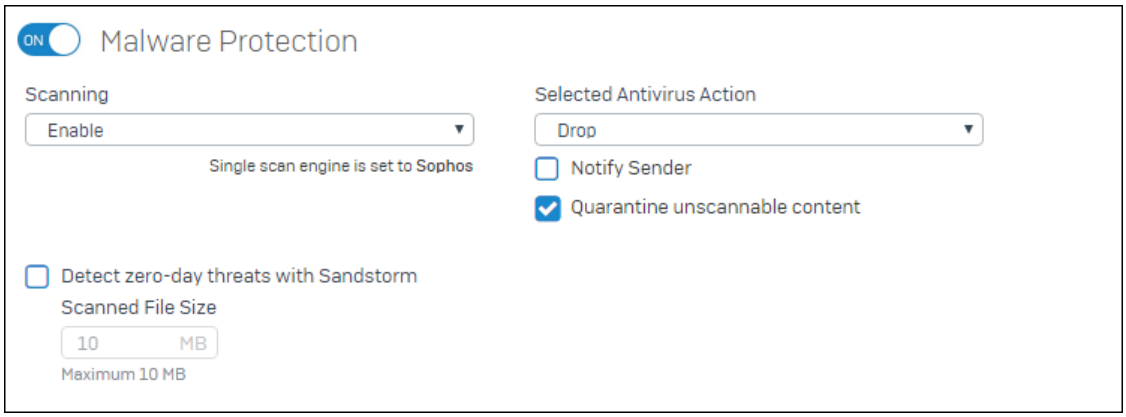
Go to **Protect > Email > Policies**, click **Add Policy** and click **Add SMTP Policy**.

Select the internal domain and enter its static IP addresses.



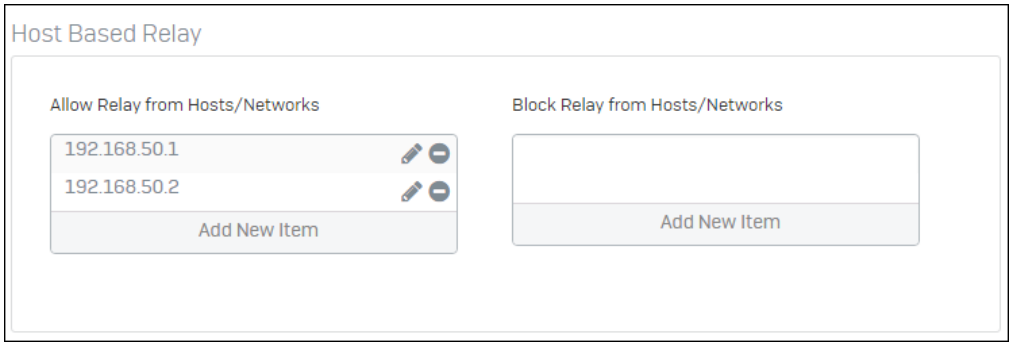
Turn on **Spam Protection** and retain the default settings.

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

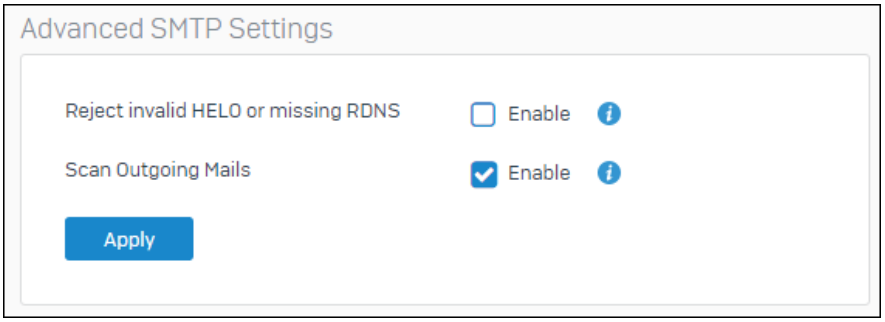


Step 6: Scan and Filter Outbound Emails

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