SOPHOS
Security made simple.

Pocket Guide

How to SPX-Encrypt Outbound Emails Containing Financial Data (MTA Mode)

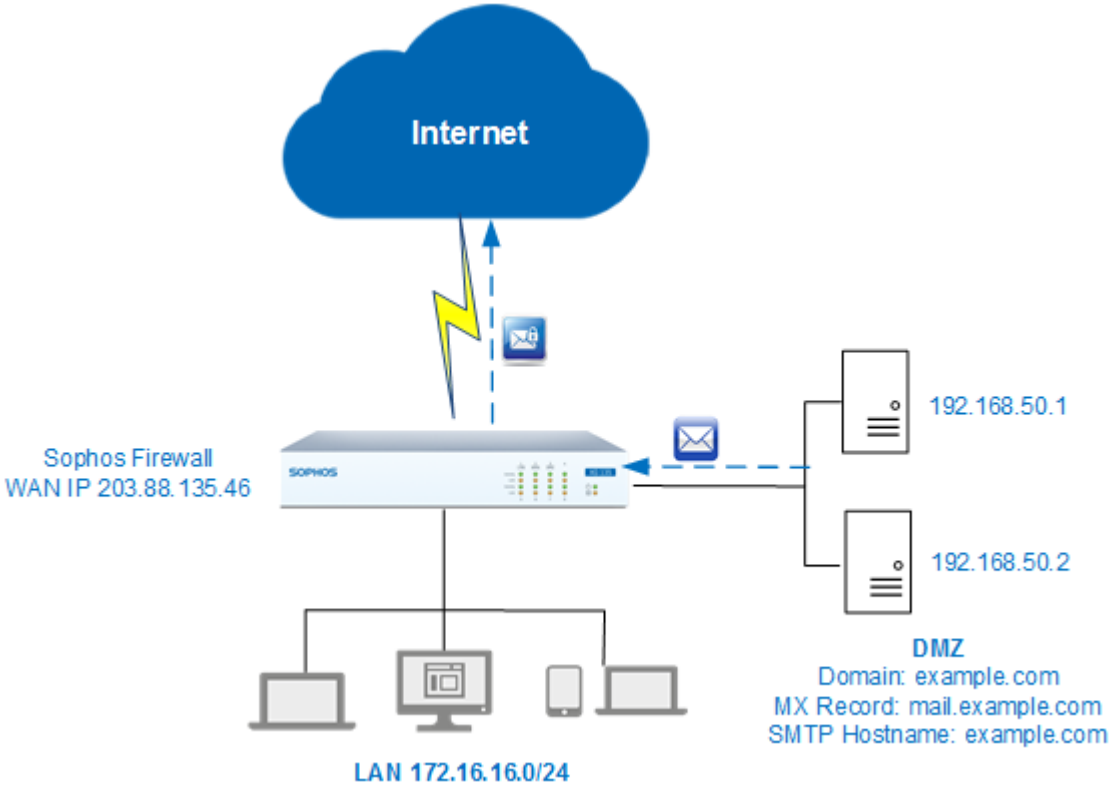
Product: Sophos XG Firewall

Contents

Scenario

Configure Sophos XG Firewall to SPX-encrypt all the outbound emails for confidential financial data. This example helps you encrypt emails containing confidential data sent from your email server hosted within DMZ.

This type of encryption is required in Banking and Finance sector where emails from finance department are required to be encrypted.



Prerequisites

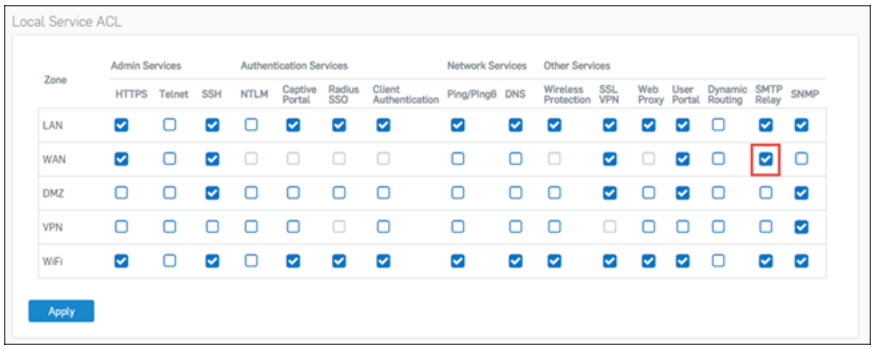
- Read-write permissions on the Sophos XG Firewall Admin Console for the relevant features.
- Valid Email Protection subscription **(Administration > Licensing)**.
- Plugged in and connected interfaces to WAN (Internet) and DMZ (containing the servers) zones **(Network > Interfaces)**.
- Email server's MX record pointing to the XG Firewall WAN interface.

Configuration

Log in to the Sophos XG Firewall Admin Console.

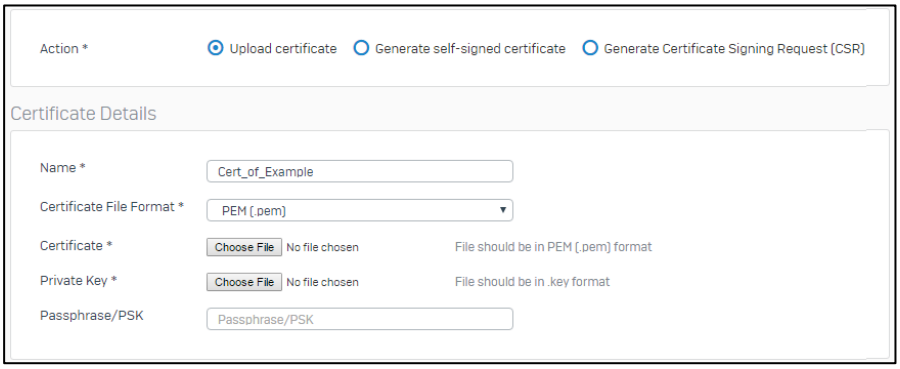
Step 1: Enable SMTP Relay for WAN zone

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



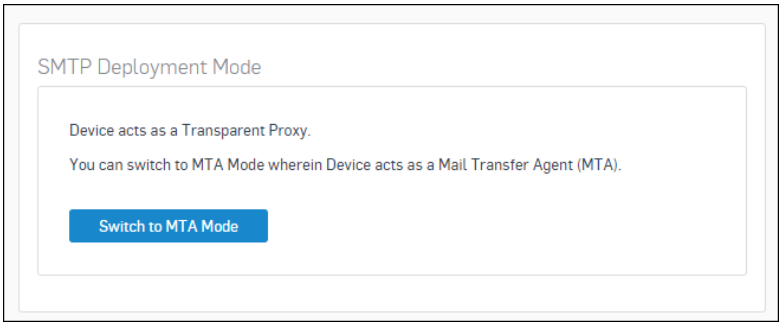
Step 2: Upload email server certificate

Go to **System > Certificates > Certificates > Add** to upload the email server certificate. This certificate must be used as the SMTP TLS Certificate in step 3.

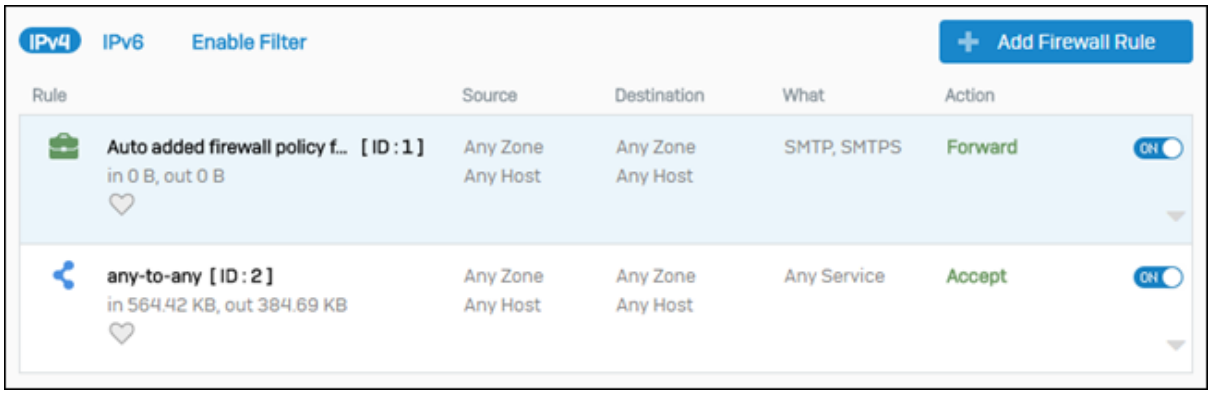


Step 3: Configure SMTP deployment mode and email settings

Go to **Protect > Email > General Settings** and click **Switch to MTA Mode** if device is functioning in legacy mode.

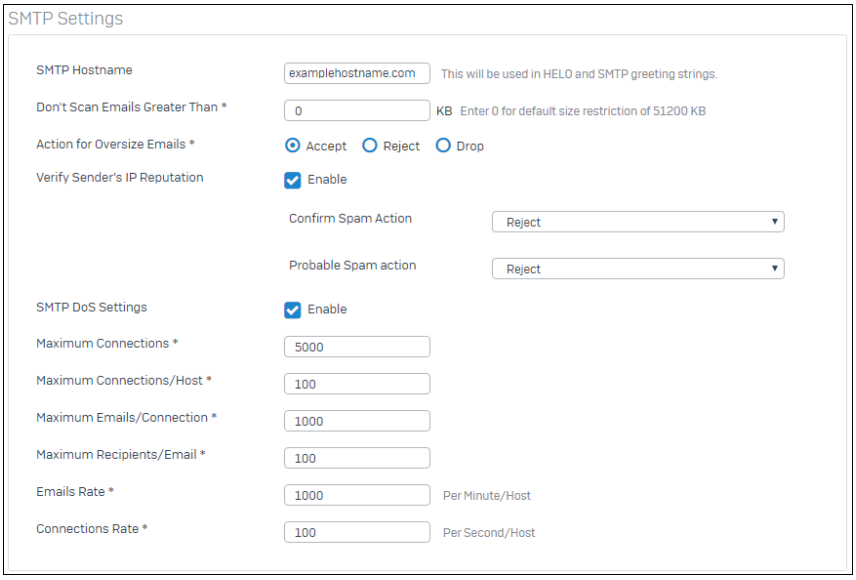


This creates firewall rule to forward SMTP/SMTPS traffic automatically.

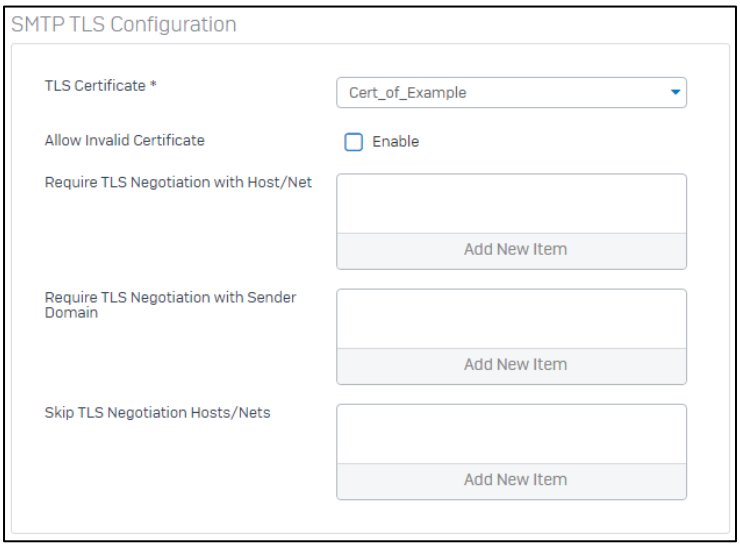


Under **SMTP Settings**:

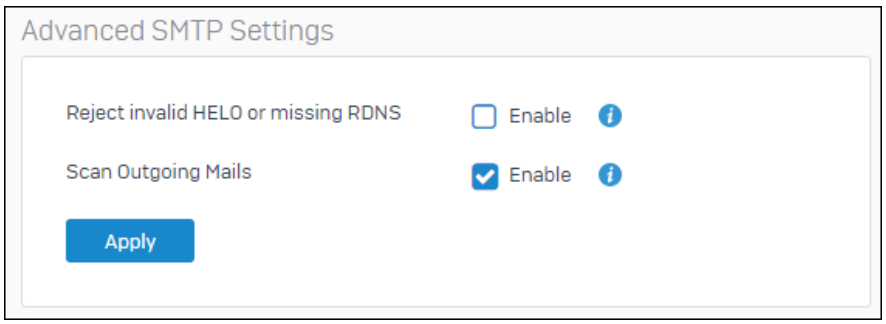
- Configure the **SMTP Hostname.**
- Select **Verify Sender's IP Reputation** and retain the default action setting. This will reject all the spam mails if Sender's IP address is in the IP reputation list.
- Select **SMTP DoS Settings** to protect from SMTP DoS attacks.



Under **SMTP TLS Configuration**, set **TLS Certificate** to the email server certificate uploaded in step 2. Deselect **Allow Invalid Certificate**.

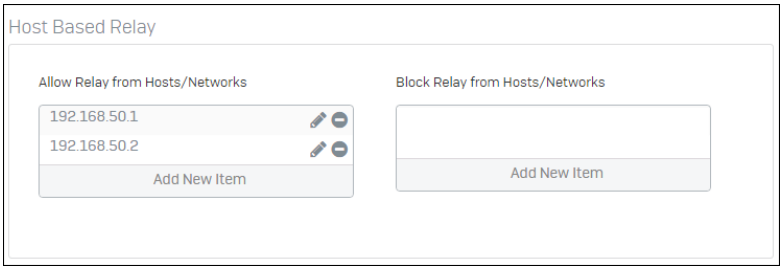


Under **Advanced SMTP Settings**, select **Scan Outgoing Mails**.



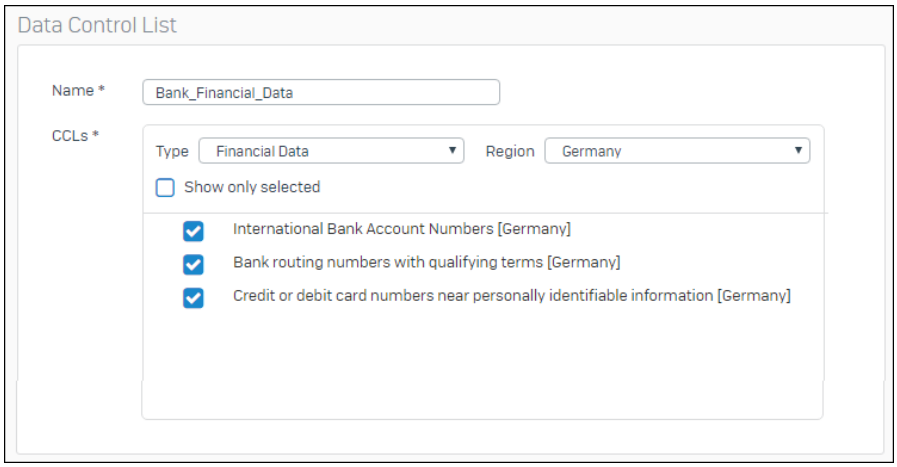
Step 4: Configure Relay Settings for Email Servers

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



Step 5: Add Custom Data Control List (DCL)

You can create a custom list as per your requirement or can use from one of the predefined DCLs – Confidential information, Financial information and Postal addresses. As an example, we have created a DCL for Type Financial Data.



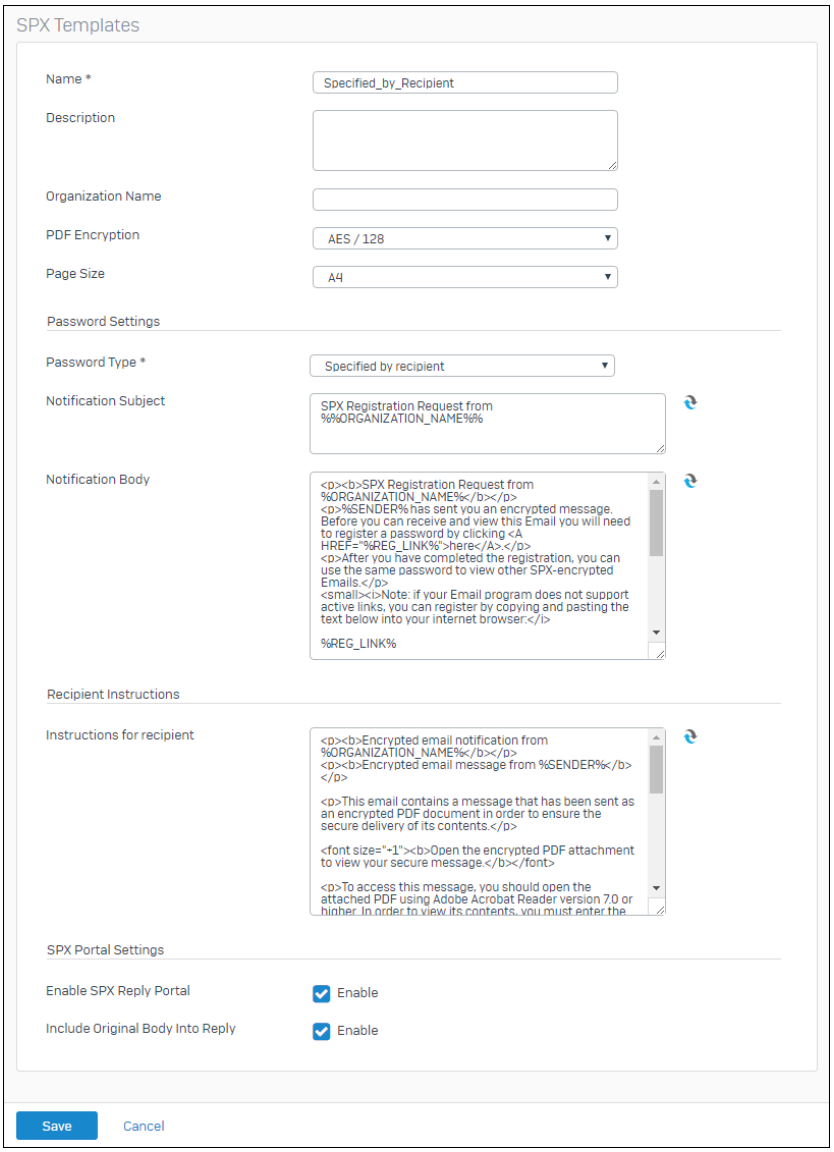
- Go to **Protect > Email > Data Control List** and click **Add**.
- Set **Type** to **Financial Data** and **Region** to **Germany**.
- Select the following **CCLs** (Sophos Content Control List):
    - International Bank Account Numbers [Germany]
    - Bank routing numbers with qualifying terms [Germany]
    - Credit or debit card numbers near personally identifiable information [Germany]
- Click **Save**.

The selected data control list is used in the SMTP Route & Scan Policy in step 7.

Step 6: Create SPX Template

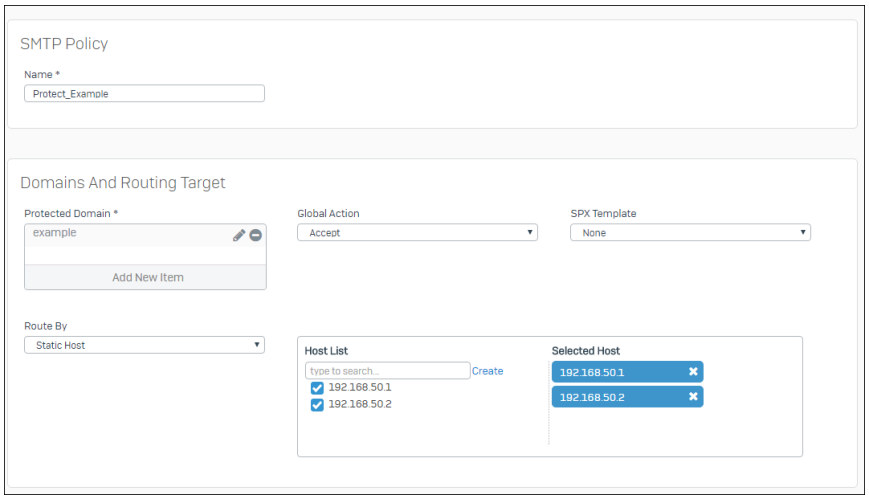
- Go to **Protect > Email > Encryption. Under SPX Templates,** click **Add.**
- Set **Password Type** as **Specified by Recipient**
- Select **Enable SPX Reply Portal** and **Include Original Body Into Reply**. This will allow users to securely reply using the SPX Reply Portal and include original content in the reply.
- Click **Save.**

This SPX Template must be used in an SMTP Route & Scan Policy in step 7.



Step 7: Create SMTP route and scan policy to SPX-encrypt emails containing financial information

- Go to **Protect > Email > Policies**, click **Add Policy** and click **SMTP Route & Scan**.



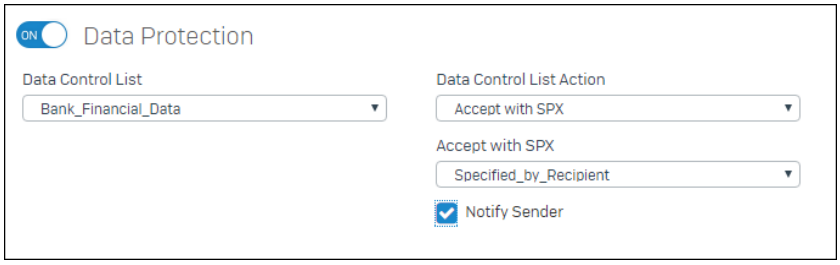
- Under Domain and Routing Target set:

  Domain to **example** (Policy applies to mails sent and received from this domain)

  Global Action to **Accept**

  SPX Template to **None** (Template selected here is applied to the traffic to and from the specified domain. In this scenario we want to use template only for the traffic that matches the Data Protection profile and hence we do not select any template here)

- Turn on **Data Protection** and set:



  Data Control List to **Bank_Financial_Data** (created in step 5)

  Data Control List Action to **Accept with SPX**

  Accept with SPX to **Specified_by_Recipient** (created in step 6)

- Click **Save**.

Result

All outbound emails will be scanned for confidential financial data.

When SFOS detects an email containing confidential data, the recipient will receive an email asking them to register a password. Once password is registered, SFOS encrypts the email with that password and then sends it to the recipient.

The configuration in this article can be used for scanning other types of confidential data, like data related to identification and postal addresses. The steps remain the same except of step 5 where you need to create the relevant Data Control List.

Copyright Notice