

SOPHOS

Security made simple.



Pocket Guide

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

Product: Sophos XG Firewall

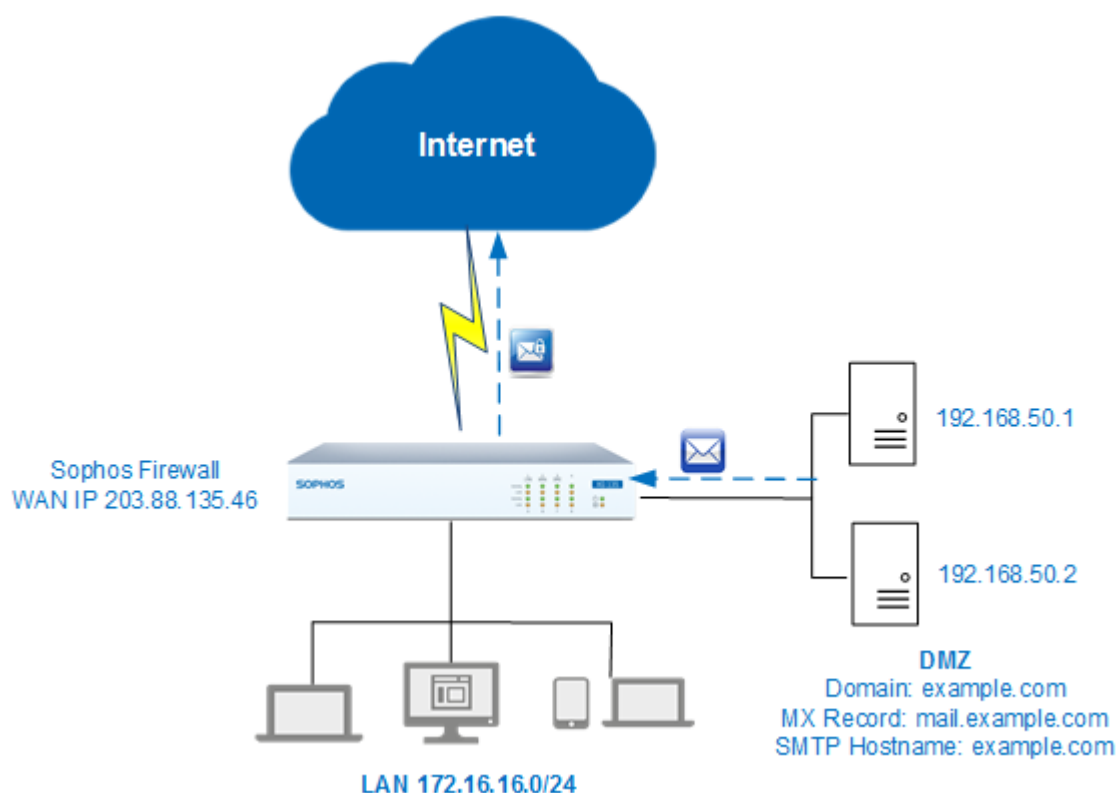
Contents

| | |
|----------------------------------------------------------------------------------------|----|
| Scenario | 2 |
| Prerequisites | 2 |
| Configuration..... | 3 |
| Step 1: Enable SMTP Relay for WAN zone..... | 3 |
| Step 2: Upload email server certificate..... | 3 |
| Step 3: Configure SMTP deployment mode and email settings..... | 3 |
| Step 4: Configure Relay Settings for Email Servers | 5 |
| Step 5: Add Custom Data Control List (DCL) | 6 |
| Step 6: Create SPX Template | 7 |
| Step 7: Create SMTP policy to SPX-encrypt emails containing financial information..... | 8 |
| Result..... | 9 |
| Copyright Notice | 10 |

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

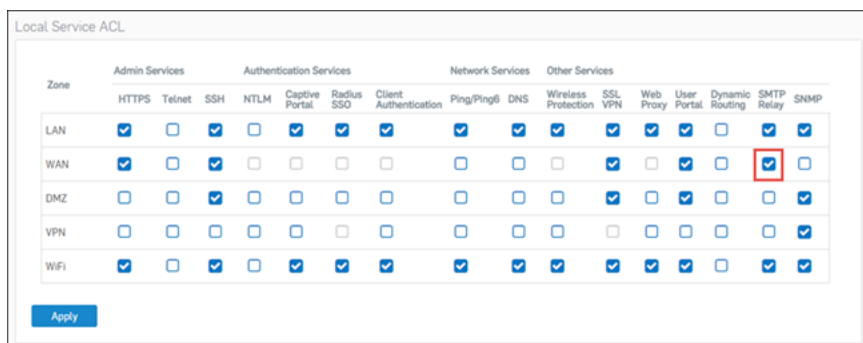
- Read-write permissions on the Sophos XG Firewall Admin Console for the relevant features.
- Valid Email Protection subscription (**Administration > Licensing**).
- Plugged in and connected interfaces to WAN (Internet) and DMZ (containing the servers) zones (**Network > Interfaces**).
- Email server's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

Configuration

Log in to the Sophos XG Firewall Admin Console.

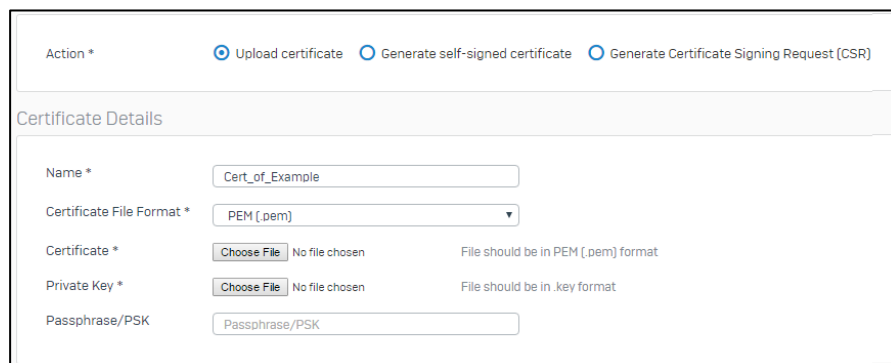
Step 1: Enable SMTP Relay for WAN zone

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



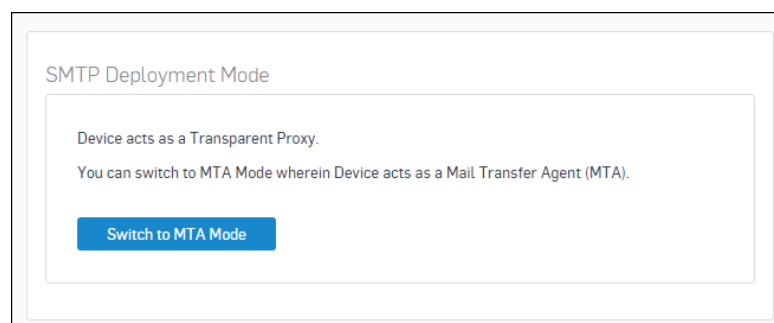
Step 2: Upload email server certificate

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.

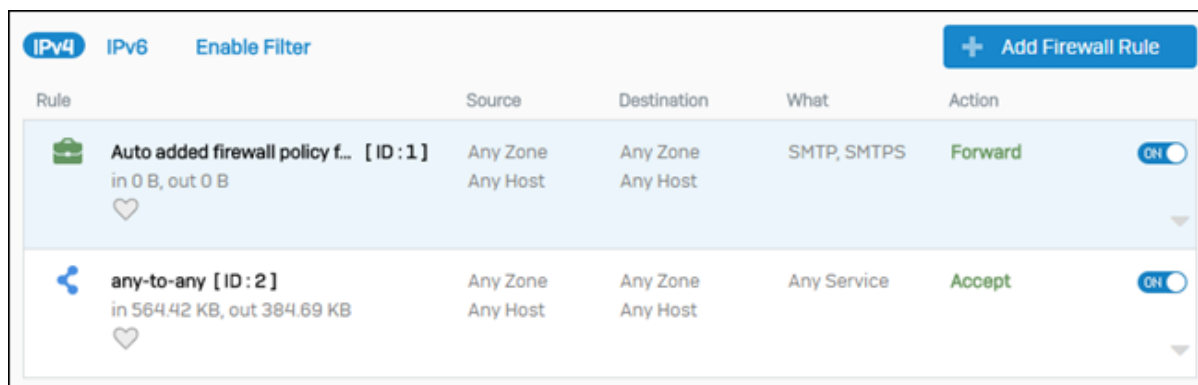






Step 3: Configure SMTP deployment mode and email settings

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



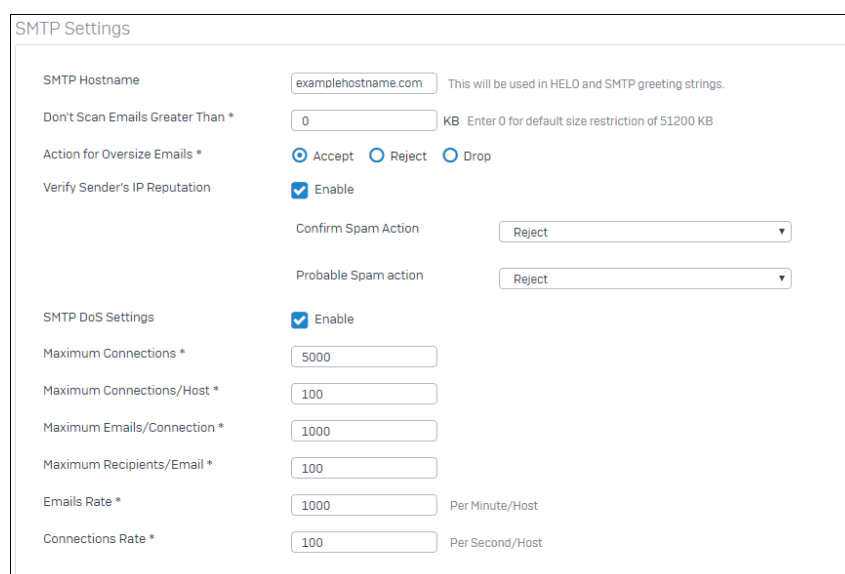
This creates firewall rule to forward SMTP/SMTPS traffic automatically.



| 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, SMTPS | Forward | <input checked="" type="checkbox"/> |
|  any-to-any [ID:2] in 564.42 KB, out 384.69 KB  | Any Zone Any Host | Any Zone Any Host | Any Service | Accept | <input checked="" type="checkbox"/> |

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.



SMTP Settings

SMTP Hostname: This will be used in HELO and SMTP greeting strings.

Don't Scan Emails Greater Than *: KB Enter 0 for default size restriction of 51200 KB

Action for Oversize Emails *: Accept Reject Drop

Verify Sender's IP Reputation: Enable

Confirm Spam Action:

Probable Spam action:

SMTP DoS Settings: Enable

Maximum Connections *:

Maximum Connections/Host *:

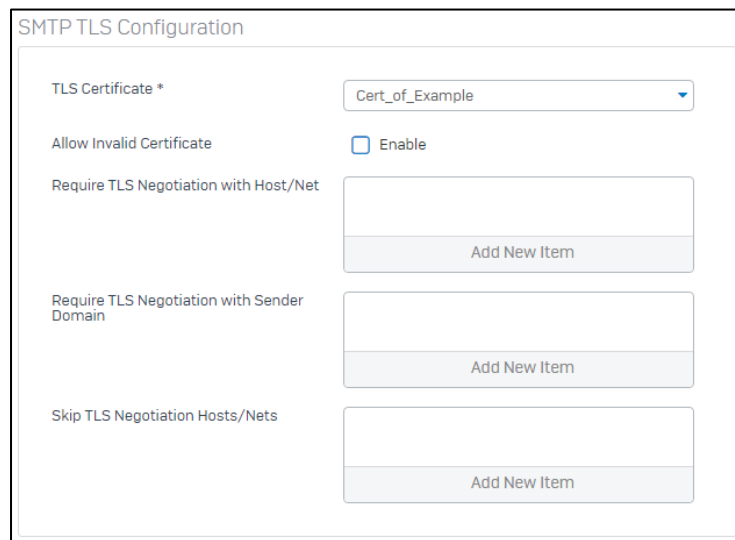
Maximum Emails/Connection *:

Maximum Recipients/Email *:

Emails Rate *: Per Minute/Host

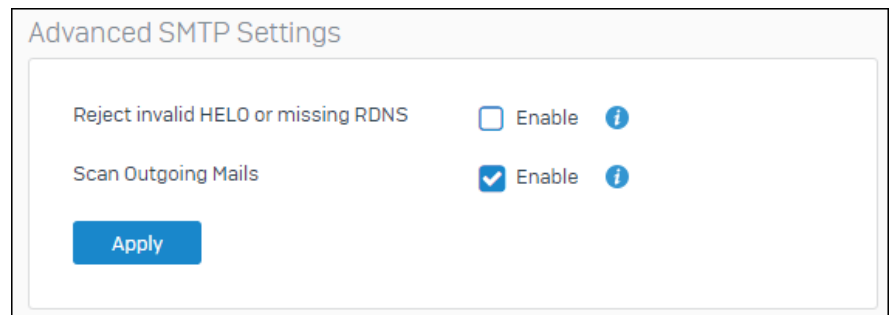
Connections Rate *: Per Second/Host

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



The screenshot shows the 'SMTP TLS Configuration' interface. It includes a dropdown menu for 'TLS Certificate *' set to 'Cert_of_Example'. Below it, the 'Allow Invalid Certificate' checkbox is unchecked. There are three sections for negotiation requirements: 'Require TLS Negotiation with Host/Net', 'Require TLS Negotiation with Sender Domain', and 'Skip TLS Negotiation Hosts/Nets', each with an 'Add New Item' button.

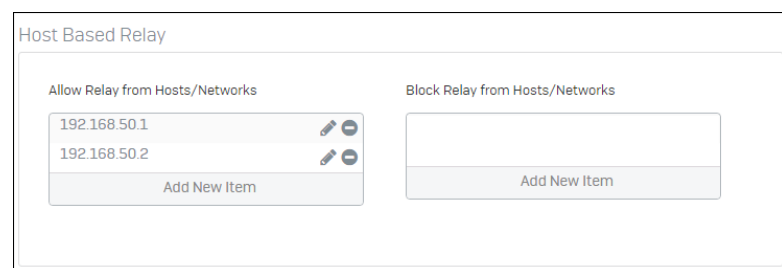
Under **Advanced SMTP Settings**, select **Scan Outgoing Mails**.



The screenshot shows the 'Advanced SMTP Settings' interface. It features two settings: 'Reject invalid HELO or missing RDNS' with an unchecked 'Enable' checkbox, and 'Scan Outgoing Mails' with a checked 'Enable' checkbox. An 'Apply' button is located at the bottom left.

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.

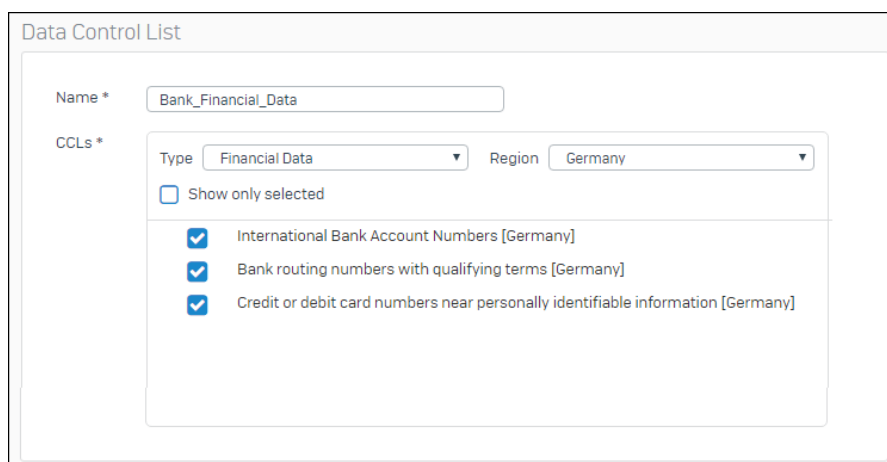


The screenshot shows the 'Host Based Relay' configuration. It has two columns: 'Allow Relay from Hosts/Networks' and 'Block Relay from Hosts/Networks'. The 'Allow' column contains a list with IP addresses '192.168.50.1' and '192.168.50.2', each with edit and delete icons, and an 'Add New Item' button. The 'Block' column is currently empty with an 'Add New Item' button.

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 screenshot shows the 'Data Control List' configuration window. The 'Name' field is set to 'Bank_Financial_Data'. Under 'CCLs', the 'Type' is set to 'Financial Data' and the 'Region' is set to 'Germany'. There is a checkbox for 'Show only selected' which is currently unchecked. Three CCLs are listed and checked: 'International Bank Account Numbers [Germany]', 'Bank routing numbers with qualifying terms [Germany]', and 'Credit or debit card numbers near personally identifiable information [Germany]'.

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.

The image shows a web-based configuration form titled "SPX Templates". The form is organized into several sections:

- Name ***: A text input field containing "Specified_by_Recipient".
- Description**: An empty text area.
- Organization Name**: An empty text input field.
- PDF Encryption**: A dropdown menu set to "AES / 128".
- Page Size**: A dropdown menu set to "A4".
- Password Settings**: A section header.
- Password Type ***: A dropdown menu set to "Specified by recipient".
- Notification Subject**: A text area containing "SPX Registration Request from %ORGANIZATION_NAME%".
- Notification Body**: A text area containing HTML-formatted text: "<p>SPX Registration Request from %ORGANIZATION_NAME%</p><p>%SENDER% has sent you an encrypted message. Before you can receive and view this Email you will need to register a password by clicking here</p><p>After you have completed the registration, you can use the same password to view other SPX-encrypted Emails.</p><small>Note: if your Email program does not support active links, you can register by copying and pasting the text below into your internet browser.</small><p>%REG_LINK%</p>".
- Recipient Instructions**: A section header.
- Instructions for recipient**: A text area containing HTML-formatted text: "<p>Encrypted email notification from %ORGANIZATION_NAME%</p><p>Encrypted email message from %SENDER%</p><p>This email contains a message that has been sent as an encrypted PDF document in order to ensure the secure delivery of its contents.</p><p>Open the encrypted PDF attachment to view your secure message.</p><p>To access this message, you should open the attached PDF using Adobe Acrobat Reader, version 7.0 or higher. In order to view its contents, you must enter the</p>".
- SPX Portal Settings**: A section header.
- Enable SPX Reply Portal**: A checkbox that is checked, with the label "Enable".
- Include Original Body Into Reply**: A checkbox that is checked, with the label "Enable".

At the bottom of the form, there are "Save" and "Cancel" buttons.

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]

SMTP Policy

Name *
Protect_Example

Domains And Routing Target

Protected Domain *
example

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

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 Protection

Data Control List
Bank_Financial_Data

Data Control List Action
Accept with SPX

Accept with SPX
Specified_by_Recipient

Notify Sender

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

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.