

Pocket Guide

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

Product: Sophos XG Firewall

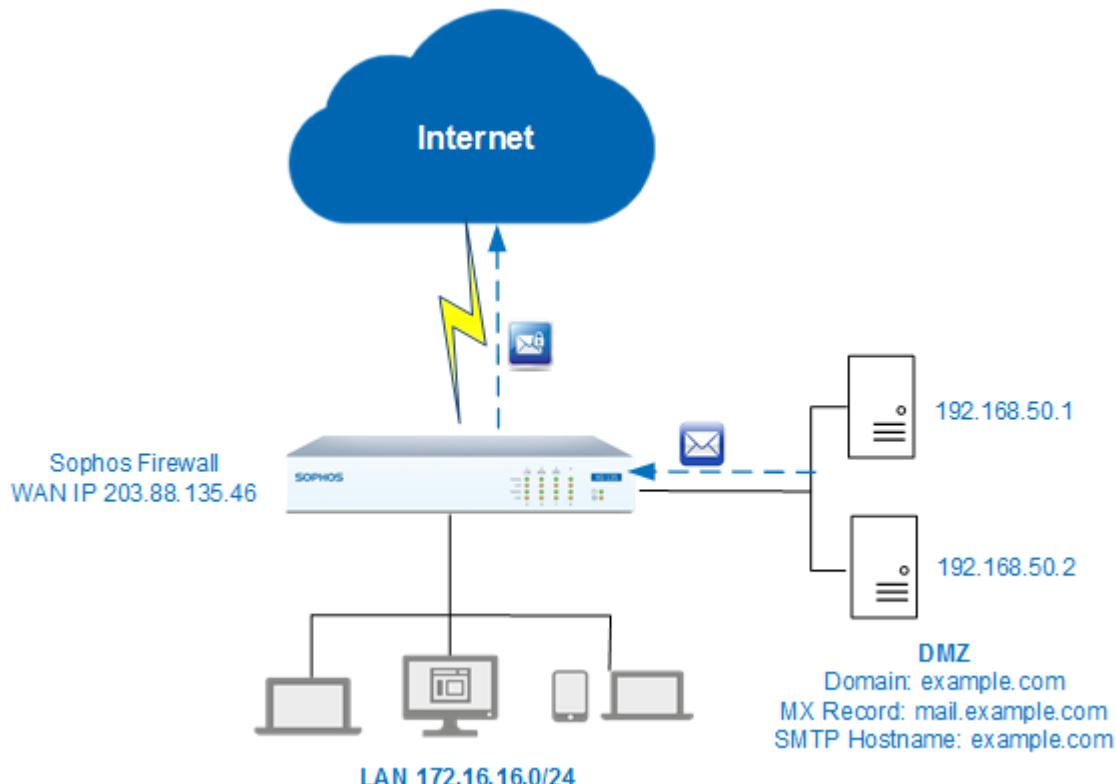
Contents

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.

Zone	Admin Services				Authentication Services				Network Services				Other Services			
	HTTPS	Telnet	SSH	NTLM	Captive Portal	Radius	SSO	Client Authentication	Ping/Ping6	DNS	Wireless Protection	SSL VPN	Web Proxy	User Portal	Dynamic Routing	SMTP Relay
LAN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>											
WAN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DMZ	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
VPN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WiFi	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>											

Apply

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.

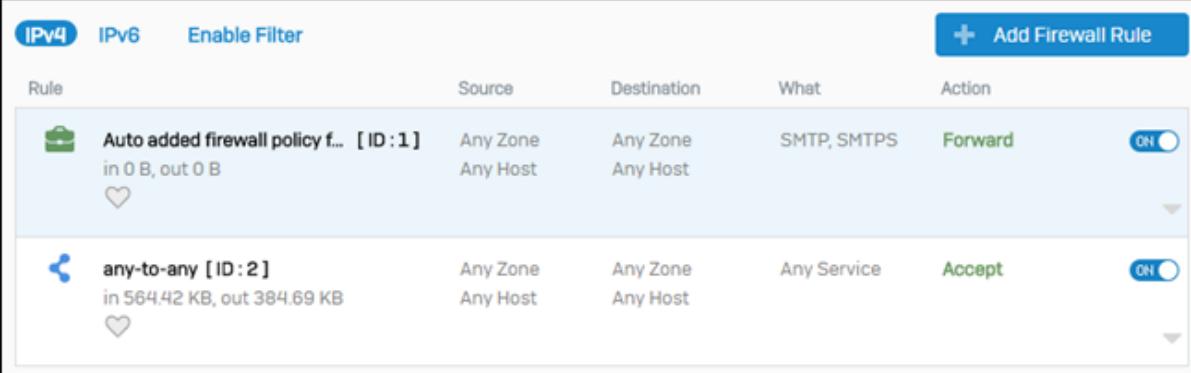
Action *	<input checked="" type="radio"/> Upload certificate <input type="radio"/> Generate self-signed certificate <input type="radio"/> Generate Certificate Signing Request (CSR)
Certificate Details	
Name *	<input type="text" value="Cert_of_Example"/>
Certificate File Format *	<input type="text" value="PEM (.pem)"/>
Certificate *	<input type="file"/> No file chosen <small>File should be in PEM (.pem) format</small>
Private Key *	<input type="file"/> No file chosen <small>File should be in .key format</small>
Passphrase/PSK	<input type="text" value="Passphrase/PSK"/>

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.

SMTP Deployment Mode
Device acts as a Transparent Proxy.
You can switch to MTA Mode wherein Device acts as a Mail Transfer Agent (MTA).
Switch to MTA Mode

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

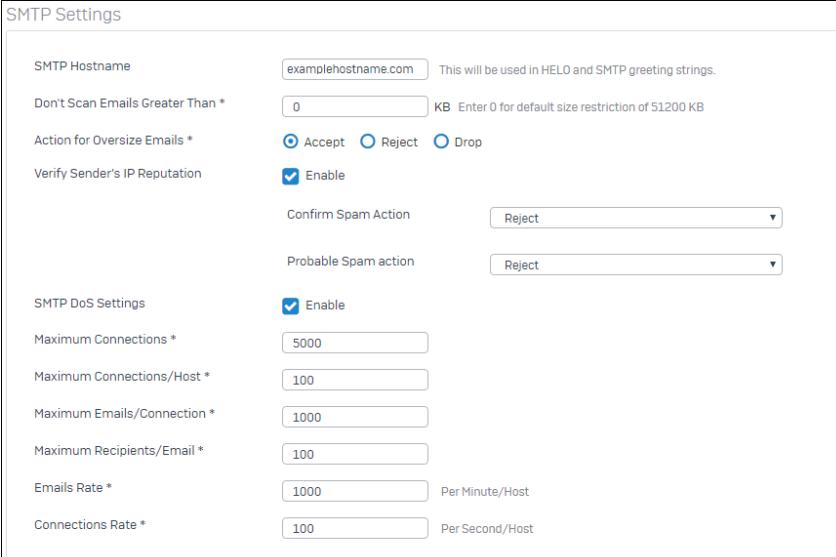


The screenshot shows a firewall rule configuration interface. At the top, there are tabs for 'IPv4' (selected), 'IPv6', and 'Enable Filter'. A blue button on the right says '+ Add Firewall Rule'. The table below lists two rules:

Rule	Source	Destination	What	Action	On/Off
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.



The screenshot shows the 'SMTP Settings' configuration page. It includes fields for SMTP Hostname (examplehostname.com), size restrictions for oversized emails (0 KB), and actions for oversize emails (Accept, Reject, Drop). It also includes a 'Verify Sender's IP Reputation' section with a checked checkbox. The 'SMTP DoS Settings' section contains various connection and rate limit parameters, all of which are checked and enabled.

Setting	Value	Description
SMTP Hostname	examplehostname.com	This will be used in HELO and SMTP greeting strings.
Don't Scan Emails Greater Than *	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	Reject	
Probable Spam action	Reject	
SMTP DoS Settings	<input checked="" type="checkbox"/> Enable	
Maximum Connections *	5000	
Maximum Connections/Host *	100	
Maximum Emails/Connection *	1000	
Maximum Recipients/Email *	100	
Emails Rate *	1000	Per Minute/Host
Connections Rate *	100	Per Second/Host

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

SMTP TLS Configuration

TLS Certificate *	<input type="text" value="Cert_of_Example"/> <input type="button" value="▼"/>
Allow Invalid Certificate	<input type="checkbox"/> Enable
Require TLS Negotiation with Host/Net	<input type="button" value="Add New Item"/>
Require TLS Negotiation with Sender Domain	<input type="button" value="Add New Item"/>
Skip TLS Negotiation Hosts/Nets	<input type="button" value="Add New Item"/>

Under Advanced SMTP Settings, select Scan Outgoing Mails.

Advanced SMTP Settings

Reject invalid HELO or missing RDNS	<input type="checkbox"/> Enable
Scan Outgoing Mails	<input checked="" type="checkbox"/> Enable
<input type="button" value="Apply"/>	

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.

Host Based Relay

Allow Relay from Hosts/Networks	Block Relay from Hosts/Networks						
<table border="1"><tr><td>192.168.50.1</td><td></td></tr><tr><td>192.168.50.2</td><td></td></tr><tr><td colspan="2"><input type="button" value="Add New Item"/></td></tr></table>	192.168.50.1		192.168.50.2		<input type="button" value="Add New Item"/>		<input type="button" value="Add New Item"/>
192.168.50.1							
192.168.50.2							
<input type="button" value="Add New Item"/>							

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 populated with 'Bank_Financial_Data'. The 'Type' dropdown is set to 'Financial Data' and the 'Region' dropdown is set to 'Germany'. The 'Show only selected' checkbox is unchecked. Under the 'CCLs' section, three items are selected: 'International Bank Account Numbers [Germany]', 'Bank routing numbers with qualifying terms [Germany]', and 'Credit or debit card numbers near personally identifiable information [Germany]'. All three items have a checked checkbox next to them.

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.

SPX Templates

Name *	Specified_by_Recipient
Description	
Organization Name	
PDF Encryption	AES / 128
Page Size	A4
Password Settings	
Password Type *	Specified by recipient
Notification Subject	SPX Registration Request from %%&ORGANIZATION_NAME%%
Notification Body	<p><D>SPX Registration Request from %%&ORGANIZATION_NAME%%</D></p> <p><D>%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</D></p> <p><D>After you have completed the registration, you can use the same password to view other SPX-encrypted Emails.</D></p> <p><small><i>Note: If your Email program does not support active links, you can register by copying and pasting the text below into your Internet browser:</i></small></p> <p style="border: 1px solid black; padding: 5px;">%REG_LINK%</p>
Recipient Instructions	
Instructions for recipient	<p><p>Encrypted email notification from %%&ORGANIZATION_NAME%%</p></p> <p><p>Encrypted email message from %SENDER%</p></p> <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> <p>Open the encrypted PDF attachment to view your secure message.</p> <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	
Enable SPX Reply Portal	<input checked="" type="checkbox"/> Enable
Include Original Body Into Reply	<input checked="" type="checkbox"/> Enable
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

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

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.