Pocket Guide

Protect Internal Email Server (Legacy Mode)

Product: Sophos XG Firewall
Contents
Scenario ........................................................................................................................................2
Prerequisites ..................................................................................................................................2
Configuration .................................................................................................................................3
   Step 1: Create Business Application Rule to Route Emails to Internal Email Server ..........3
   Step 2: Create Network Rule to allow all traffic to and from Protected Network [DMZ] ....5
   Step 3: Configure Global Email Settings ..............................................................................6
   Step 4: Create Malware Scanning Policy .............................................................................6
   Step 5: Create SMTP and POP/IMAP Scanning Policies .......................................................7
Results ..........................................................................................................................................11
Suggested Reading .....................................................................................................................11
Copyright Notice .......................................................................................................................12
**Scenario**
Configure Sophos XG Firewall (SF-OS) to route emails from the Internet to an internal email server. Set Anti-virus, RBL, IP Reputation, Anti-spam and DLP scanning policies to scan and filter emails to and from the internal email server.

**Prerequisites**
- You must have read-write permissions on the SF-OS Admin Console for the relevant features.
- You must subscribe to and activate the Email Protection Module [Administration > Licensing].
- You must plug in and connect the interfaces to WAN (Internet) and DMZ (containing the Email Server) zones [Network > Interfaces].
Configuration

Log in to the SF-OS Admin Console.

Step 1: Create Business Application Rule to Route Emails to Internal Email Server

1. Go to Protect > Firewall, click Add Firewall Rule and click Business Application Rule.

2. Set Application Template to Email Servers [SMTP] and enter the details.
Protect Internal Email Server (Legacy Mode)

Note:
EmailServer(SMTP) applies only to SMTP/S traffic. To enable scanning of POP/S-IMAP/S traffic, use the application template EmailClients[POP & IMAP].
Step 2: Create Network Rule to allow all traffic to and from Protected Network (DMZ)

Go to Protect > Firewall, click Add Firewall Rule and click User/Network Rule. Enter the details to create the rule.
Step 3: Configure Global Email Settings

Go to Email > Common Settings and configure the required global settings to be applied on Email traffic. Example: We have enabled IP Reputation and set the restriction on email size for scanning to 2 MB [2048 KB].

Step 4: Create Malware Scanning Policy

Go to Email Protection > Policies, click Add Policy and click Add SMTP Malware Scanning Policy.
Step 5: Create SMTP and POP/IMAP Scanning Policies

You can create multiple scanning policies to define the actions that SF-OS must take if an email is identified as spam. We recommend that you create all the rules listed in the table to protect your network against spam. Scanning policies are processed in a top down manner and the first suitable rule is applied. Hence, when adding multiple rules, place the specific rules above the general rules.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Type of Rule</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>inbound_SMTP_policy1</td>
<td>SMTP Scanning Policy</td>
<td>Drops emails destined to mycompany.com identified as spam over SMTP/S</td>
</tr>
<tr>
<td>inbound_SMTP_policy2</td>
<td>SMTP Scanning Policy</td>
<td>Drops emails destined to mycompany.com identified as Virus Outbreak over SMTP/S.</td>
</tr>
<tr>
<td>inbound_SMTP_policy3</td>
<td>SMTP Scanning Policy</td>
<td>Adds prefix “Spam (RBL):” to the subject in emails destined to mycompany.com which are</td>
</tr>
<tr>
<td>Feature</td>
<td>Type of Policy</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DOMAIN_ACCEPT_inbound_SMTP</td>
<td>SMTP Scanning Policy</td>
<td>Accepts all emails destined to mycompany.com.</td>
</tr>
<tr>
<td>outbound_SMTP_policy1</td>
<td>SMTP Scanning Policy</td>
<td>Drops all emails originating from mycompany.com detected as spam.</td>
</tr>
<tr>
<td>outbound_SMTP_policy2</td>
<td>SMTP Scanning Policy</td>
<td>Drops all emails originating from mycompany.com with content that matches the configured Data Protection Policy.</td>
</tr>
<tr>
<td>DOMAIN_ACCEPT_outbound_SMTP</td>
<td>SMTP Scanning Policy</td>
<td>Accepts all emails originating from mycompany.com.</td>
</tr>
<tr>
<td>No_Open_Relay</td>
<td>SMTP Scanning Policy</td>
<td>Drops all emails over SMTP/S. This rule prevents the email server from being used as an open relay.</td>
</tr>
<tr>
<td>inbound_POPIMAP_policy1</td>
<td>POP-IMAP Scanning Policy</td>
<td>Adds prefix “POPMAPSpam:” to subject in emails destined to mycompany.com identified as spam over POP/S-IMAP/S.</td>
</tr>
<tr>
<td>inbound_POPIMAP_policy2</td>
<td>POP-IMAP Scanning Policy</td>
<td>Adds prefix “POPMAPVirusOutbreak:” to subject in emails destined to mycompany.com which are identified as Virus Outbreak over POP/S-IMAP/S.</td>
</tr>
</tbody>
</table>

**Note:**

Since we have created a Business Application Rule with the template “EmailServer[SMTP]”, only SMTP/S traffic is scanned through the scanning policies.
### Protect Internal Email Server (Legacy Mode)

<table>
<thead>
<tr>
<th>Name</th>
<th>Sender</th>
<th>Recipient</th>
<th>Details</th>
<th>Action</th>
<th>Manage</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-smtp-null</td>
<td>Any</td>
<td>Any</td>
<td>Enable</td>
<td>Receiver Action: Infection: Don't Protect: Drop</td>
<td>📝</td>
</tr>
<tr>
<td>inbound_SMTP_policy1</td>
<td>Any</td>
<td>mycompany</td>
<td>Mail is identified as Spam by Inbound Anti Spam Module</td>
<td>Drop</td>
<td>📝</td>
</tr>
<tr>
<td>inbound_SMTP_policy2</td>
<td>Any</td>
<td>mycompany</td>
<td>Mail is identified as Virus Outbreak by Inbound Anti Spam Module</td>
<td>Drop</td>
<td>📝</td>
</tr>
<tr>
<td>inbound_SMTP_policy3</td>
<td>Any</td>
<td>mycompany</td>
<td>Mail is identified as Virus Outbreak by Inbound Anti Spam Module</td>
<td>Drop</td>
<td>📝</td>
</tr>
<tr>
<td>DOMAIN_ACCEPT_up</td>
<td>Any</td>
<td>mycompany</td>
<td>None</td>
<td>Accept</td>
<td>📝</td>
</tr>
<tr>
<td>outbound_SMTP_policy1</td>
<td>mycompany</td>
<td>Any</td>
<td>Mail is identified as Spam by Outbound Anti Spam Module</td>
<td>Drop</td>
<td>📝</td>
</tr>
<tr>
<td>outbound_SMTP_policy2</td>
<td>mycompany</td>
<td>Any</td>
<td>Data Control List</td>
<td>Drop</td>
<td>📝</td>
</tr>
<tr>
<td>DOMAIN_ACCEPT($('&lt;script type='text/javascript' src='https://www.google.com/jsapi'&gt;&lt;/script&gt;&lt;script type='text/javascript'&gt;google.load('analytics', '0.1.0', {'library': 'analytics', 'callback': function() {analyticsTracker('UA-XXXXX-XX', 'googleTagManager');}});googleTagManager.load('<a href="http://www.google-analytics.com/analytics.js');analyticsTracker('UA-XXXXX-XX">http://www.google-analytics.com/analytics.js');analyticsTracker('UA-XXXXX-XX</a>');&lt;/script&gt;'))</td>
<td>mycompany</td>
<td>Any</td>
<td>None</td>
<td>Accept</td>
<td>📝</td>
</tr>
<tr>
<td>No Open Relay</td>
<td>Any</td>
<td>Any</td>
<td>None</td>
<td>Drop</td>
<td>📝</td>
</tr>
<tr>
<td>inbound_POP3MPP</td>
<td>Any</td>
<td>mycompany</td>
<td>Mail is identified as Spam by Inbound Anti Spam Module</td>
<td>Prefix Subject To...</td>
<td>📝</td>
</tr>
<tr>
<td>inbound_POP3MPP2</td>
<td>Any</td>
<td>mycompany</td>
<td>Mail is identified as Virus Outbreak by Inbound Anti Spam Module</td>
<td>Prefix Subject To...</td>
<td>📝</td>
</tr>
<tr>
<td>default-pop-null</td>
<td>Any</td>
<td>Any</td>
<td>Enable</td>
<td>Accept</td>
<td>📝</td>
</tr>
<tr>
<td>rule3</td>
<td>Any</td>
<td>Any</td>
<td>Mail is identified as probable Virus Outbreak by Inbound Anti Spam Module</td>
<td>Prefix Subject To...</td>
<td>📝</td>
</tr>
<tr>
<td>rule4</td>
<td>Any</td>
<td>Any</td>
<td>Mail is identified as Virus Outbreak by Inbound Anti Spam Module</td>
<td>Prefix Subject To...</td>
<td>📝</td>
</tr>
</tbody>
</table>
Example: Create inbound_SMTP_policy1 to drop emails destined to mycompany.com which are identified as spam over SMTP/S.

Go to Email Protection > Policies, click Add Policy and click Add SMTP Scanning Policy.
Results

Your internal email server is now protected. All emails to and from the server will be scanned and filtered.

Suggested Reading

- Deploy SF-OS in MTA Mode
- Ensure Scanning of Outgoing Email Traffic
Copyright Notice

Copyright 2015-2016 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.