

**SOPHOS**

Security made simple.

# Workflow Guide

## Protect Internal Email Server

For Customers with Sophos Firewall

Product version: Beta

Document Date: September 2015



Contents

Scenario ..... 2

Prerequisites ..... 3

Configuration ..... 3

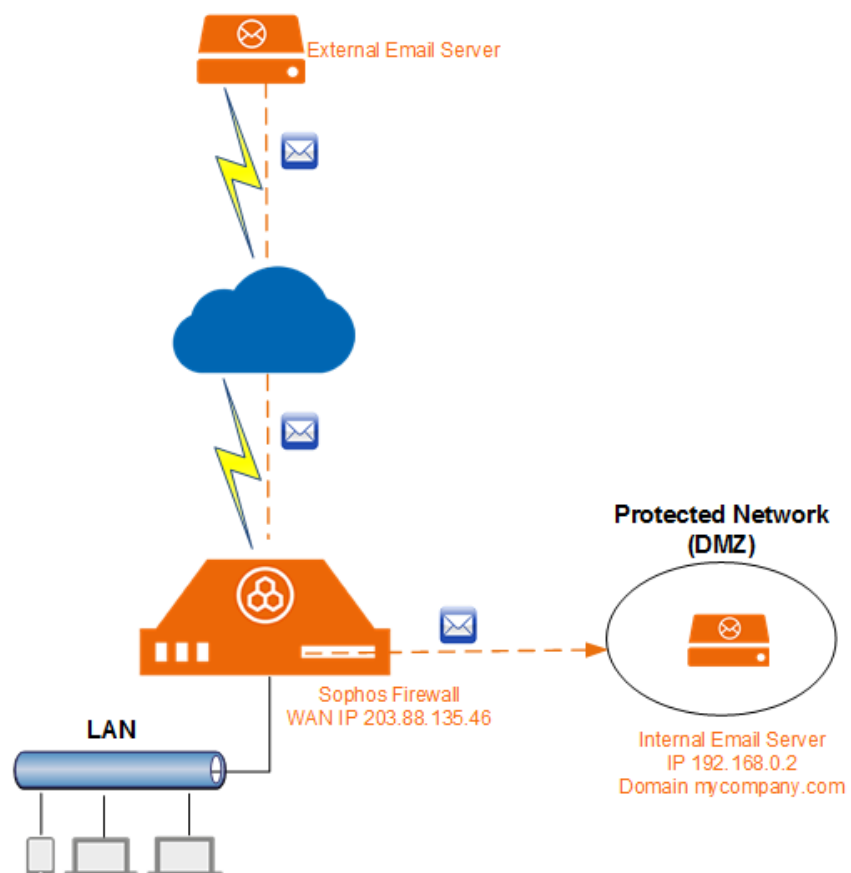
Test Configuration ..... 16

## Scenario

Configure Sophos Firewall (SF) to route Emails from the Internet to an Internal Email server and set Anti-virus, RBL, IP Reputation, Anti-spam and DLP scanning policies for the Email traffic.

Consider the hypothetical network example as shown in the below network diagram, where SF is placed at the gateway and an Email server with domain as mycompany.com and with IP Address 192.168.0.2 is hosted in DMZ. Follow the below given configuration steps to scan email traffic destined for the internal Email server:

1. Create Business Application Policy to Route Internet Emails to Internal Email Server
2. Create Network Policy to allow all traffic to and from Protected Network
3. Configure Global Email Settings - Settings may include configuring file size restriction for scanning, action to be taken for oversized mail, IP Reputation, bypass scanning of mails from authenticated connections
4. Create Malware Scanning Rule - Rule may include configuration to block attachment of specific File Type based on MIME Whitelist, whether to quarantine mail, and how to deliver mail to the recipient if malware is identified.
5. Create Content Scanning Rules



## Prerequisites

- Email Protection Module should be subscribed and activated. Check subscription status from System > Maintenance > Licensing.

| Module                | Status       | Expiration Date |
|-----------------------|--------------|-----------------|
| Base Firewall         | Active       | Tue 31 Dec 2999 |
| Network Protection    | Active       | Sun 01 Nov 2015 |
| Web Protection        | Active       | Sun 01 Nov 2015 |
| Email Protection      | Active       | Sun 01 Nov 2015 |
| Webserver Protection  | Active       | Sun 01 Nov 2015 |
| Enhanced Support      | Active       | Sun 01 Nov 2015 |
| Enhanced Plus Support | Unsubscribed | -               |

- Interfaces connected to WAN (Internet) and DMZ (containing Email Server) zones should be plugged in and connected, as shown in example below. Check from System > Network > Interfaces.

| Interface                    | Status/Interface Speed                                 | IP Address                            | Misc |
|------------------------------|--|---------------------------------------|------|
| PortE0<br>LAN , Physical     | Connected<br>100 Mbps - Full Duplex<br>Auto-negotiated | 172.16.16.20/255.255.255.0<br>Static  |      |
| PortE1<br>WAN , Physical     | Connected<br>100 Mbps - Full Duplex<br>Auto-negotiated | 203.88.135.46/255.255.192.0<br>Static |      |
| PortE2<br>DMZ , Physical     | Connected<br>Auto-negotiated                           | 192.168.0.5/255.255.255.0<br>Static   |      |
| PortE3<br>Unbound , Physical | Disabled<br>Auto-negotiated                            | N/A                                   |      |

## Configuration

You must be logged on to the Admin Console using Device Access Profile which has read/write administrative rights over relevant features.

### Step 1: Create Business Application Policy to Route Internet Emails to Internal Email Server

Go to Policies page and click +Add New Rule followed by Business Application Rule. Create policy as per parameters given below.

| Parameters                      | Value                          | Description  |
|---------------------------------|--------------------------------|--|
| About This Rule                 |                                |  |
| Template                        | EmailServer(SMTP)              | Select EmailServer(SMTP) template to define business application rule for internal Email Server.                             |
| Rule Name                       | ProtectEmailServer             | Specify a name to identify the business application rule.  |
| Source                          |                                |  |
| Host                            | Any                            | Select the source host from which SF would accept traffic. In this example, SF would accept traffic from all hosts.          |
| Hosted Server                   |                                |  |
| Source Zone                     | WAN                            | Click to select Source Zone from which SF would accept traffic. In this example, SF would accept traffic from WAN Zone,      |
| Hosted Address                  | #PortE1-203.88.135.46          | Specify the public IP address of the Email Server. Here, the Email Server is mapped with the IP address of SF WAN Interface. |
| Scan SMTP/SMTPS                 | Enable                         | Click the switch to Enable/Disable scanning of SMTP and SMTPS.   |
| Protected Application Server    |                                |  |
| Protected Zone                  | DMZ                            | Select the zone in which Email Server is placed.   |
| Protected Application Server(s) | InternalMailServer-192.168.0.2 | Specify the internal IP address of the Email Server.   |
| Forward all ports               | Disable                        | Click to enable/disable the service of port forwarding. When enabled, all ports are forwarded.                               |
| Port Forwarding                 |                                |  |

|                       |              |   |
|-----------------------|--------------|---|
| Protocol              | TCP          | Select the protocol TCP or UDP that you want the forwarded packets to use.  |
| External Port Type    | Port List    | Select the type of external port from the available options. Here, we select Port List.   |
| External Port         | 25, 587, 465 | Specify standard ports for SMTP and SMTPS to ensure port forwarding.  |
| Mapped Port Type      | Port List    | Select the type of mapped port from the available options. Here, we select Port List.   |
| Mapped Port           | 25, 587, 465 | Specify standard ports for SMTP and SMTPS to ensure port forwarding.  |
| Reflexive Rule        |              |   |
| Create Reflexive Rule | Enable       | <p>Enable to automatically create a reflexive rule. This ensures that the Email traffic originating from the protected Email Server is also scanned.</p> <p>Reflexive rule has the same policies as those configured for the hosted server but instead of source zone to destination zone, this rule is applicable on traffic from destination zone to source zone.</p> <p>By default, the reflexive rule is not created.</p> |

Note:

EmailServer(SMTP) applies only to SMTP/S traffic. To enable scanning of POP/S-IMAP/S traffic, use application template EmailClients(POP & IMAP).

## Edit Business Application Rule

[Help](#) [admin](#)

[Security Policies](#) > [Business Application Rule](#)

### About This Rule

|                      |                                |
|----------------------|--------------------------------|
| Rule Position        | <div>Top</div>                 |
| Application Template | <div>Email Servers(SMTP)</div> |
| Rule Name *          | <div>ProtectEmailServer</div>  |
| Description          | <div>Description</div>         |

### Source

|            |  |
|------------|--|
| Host *     | <div>Any</div> <div>Add New Item</div> |
| Exceptions | <div></div> <div>Add New Item</div>    |

### Hosted Server

|                  |  |
|------------------|--|
| Source Zone *    | <div>WAN</div> <div>Add New Item</div> |
| Hosted Address * | <div>#PortE1-203.88.135.46</div>       |
| Scan SMTP        | <div>ON</div>                          |
| Scan SMTPS       | <div>ON</div>                          |

### Protected Application Server(s)

|                                   |  |
|-----------------------------------|--|
| Protected Zone *                  | <div>DMZ</div>                             |
| Protected Application Server(s) * | <div>InternalMailserver-192.168.0...</div> |
| Forward all ports                 | <div>OFF</div>                             |

Port Forwarding

|                    |  |
|--------------------|--|
| Protocol           | <input checked="" type="radio"/> TCP <input type="radio"/> UDP   |
| External Port Type | <input type="radio"/> Port <input type="radio"/> Port Range <input checked="" type="radio"/> Port List |
| External Port *    | <input type="text" value="25,587,465"/> - <input type="text"/>   |
| Mapped Port Type   | <input type="radio"/> Port <input type="radio"/> Port Range <input checked="" type="radio"/> Port List |
| Mapped Port *      | <input type="text" value="25,587,465"/> - <input type="text"/>   |

Routing

|                                       |                              |
|---------------------------------------|------------------------------|
| Rewrite source address (Masquerading) | <input type="checkbox"/> OFF |
|---------------------------------------|------------------------------|

Policies for Business Applications

|                      |                                   |
|----------------------|-----------------------------------|
| Intrusion Prevention | <input type="text" value="None"/> |
| Traffic Shaping      | <input type="text" value="None"/> |

Log Traffic

|                                       |                              |
|---------------------------------------|------------------------------|
| Rewrite source address (Masquerading) | <input type="checkbox"/> OFF |
|---------------------------------------|------------------------------|

Policies for Business Applications

|                      |                                   |
|----------------------|-----------------------------------|
| Intrusion Prevention | <input type="text" value="None"/> |
| Traffic Shaping      | <input type="text" value="None"/> |

Log Traffic

|                      |                              |
|----------------------|------------------------------|
| Log Firewall Traffic | <input type="checkbox"/> OFF |
|----------------------|------------------------------|

Reflexive Rule

|                       |  |
|-----------------------|--|
| Create Reflexive Rule | <input checked="" type="checkbox"/> ON |
|-----------------------|--|

Security Heartbeat

|                             |  |
|-----------------------------|--|
| Require Security Heartbeat  | <input type="checkbox"/> OFF   |
| Minimum Heartbeat Permitted | <input type="radio"/> GREEN <input type="radio"/> YELLOW <input checked="" type="radio"/> No Restriction |

## Step 2: Create Network Policy to allow all traffic to and from Protected Network (DMZ)

Create Network policies to allow traffic, other than Email traffic, to and from the protected network. In other words, create rules to allow traffic DMZ-WAN and WAN-DMZ traffic. Here, we have created the DMZ-WAN rule. You can create the WAN-DMZ rule in similar manner.

Go to Policies page and click +Add New Rule followed by User/Network Rule. Create policy as per parameters given below.

| Parameters      | Value                       | Description  |
|-----------------|-----------------------------|--|
| About This Rule |                             |  |
| Rule Position   | Bottom                      | Specify position of the rule.  |
| Rule Name       | DMZ_WAN_Allow_Other_Traffic | Specify a name to identify the rule.   |
| Source          |                             |  |
| Zone            | DMZ                         | Select the source zone(s) of the network traffic.  |
| Destination     |                             |  |
| Zone            | WAN                         | Select the destination zone(s) of the network traffic.   |
| Action          |                             |  |
| Action          | Accept                      | Specify action for the rule traffic from the available options. <ul style="list-style-type: none"> <li>- Accept – Allow access</li> <li>- Drop – Silently discard</li> <li>- Reject – Deny access (“ICMP port unreachable” message is sent to the source)</li> </ul> |

# Add User / Network Rule

Help admin ▾

Security Policies > User / Network Rule

## About this Rule

|               |                              |
|---------------|------------------------------|
| Rule Position | Bottom ▾                     |
| Rule Name *   | DMZ_WAN_Allow_Other_Traffic  |
| Description   | <div>Enter Description</div> |

## Identity

Match rule-based on user identity ☒ OFF

## Source

|            |  |
|------------|--|
| Zone *     | <div>DMZ</div> <div>Add New Item</div> |
| Networks * | <div>Any</div> <div>Add New Item</div> |
| Services * | <div>Any</div> <div>Add New Item</div> |
| Schedule   | All The Time ▾                         |

## Destination

|            |  |
|------------|--|
| Zone *     | <div>WAN</div> <div>Add New Item</div> |
| Networks * | <div>Any</div> <div>Add New Item</div> |

## Action

Action ☒ Accept ☐ Drop ☐ Reject

## Routing

|   |  |
|---|--|
| Rewrite source address (Masquerading)   | <input checked="" type="checkbox"/>              |
| Use Gateway Specific Default NAT Policy | <input type="checkbox"/>                         |
| Use Outbound Address                    | <input type="text" value="MASQ"/>                |
| Primary Gateway                         | <input type="text" value="Load Balance"/>        |
| Backup Gateway                          | <input type="text" value="None"/>                |
| DSCP Marking                            | <input type="text" value="Select DSCP Marking"/> |

## Malware Scanning

|                      |                          |
|----------------------|--------------------------|
| Scan FTP             | <input type="checkbox"/> |
| Scan HTTP            | <input type="checkbox"/> |
| Decrypt & Scan HTTPS | <input type="checkbox"/> |

## Policy for User Applications

|                        |                                   |  |
|------------------------|-----------------------------------|--|
| Application Control    | <input type="text" value="None"/> | <input type="checkbox"/> Apply Application-based Traffic Shaping Policy  |
| Web Filter             | <input type="text" value="None"/> | <input type="checkbox"/> Apply Web Category based Traffic Shaping Policy |
| Intrusion Prevention   | <input type="text" value="None"/> |  |
| Traffic Shaping Policy | <input type="text" value="None"/> |  |

## Log Traffic

|                      |                          |
|----------------------|--------------------------|
| Log Firewall Traffic | <input type="checkbox"/> |
|----------------------|--------------------------|

## Security Heartbeat

|                             |  |
|-----------------------------|--|
| Require Security Heartbeat  | <input type="checkbox"/>   |
| Minimum Heartbeat Permitted | <input checked="" type="radio"/> GREEN <input type="radio"/> YELLOW <input type="radio"/> No Restriction |

Accept any service going to the "WAN" zone, when in the "DMZ" zone, and coming from any network

### Step 3: Configure Global Email Settings

Go to Protection > Email Protection > Configuration and configure the required global settings to be applied on Email traffic.

Example:

1. Enable IP Reputation
2. Set email size restriction for scanning to 2 MB (2048 KB)

Configuration
Help admin

Protection > Email Protection > Configuration

General Settings

Append Signature to All Outbound Messages ☐ OFF

Email Signature

SMTP/S Settings

Don't Scan Emails Greater Than \* 2048 KB Enter 0 for default size restriction of 51200 KB

Action for Oversize Emails \* ☐ Accept ☒ Reject ☐ Drop

Bypass Spam Check For SMTP/S Authenticated Connections ☐

Verify Sender's IP Reputation ☒ Enable

Confirm Spam Action Reject

Probable Spam Action Reject

SMTP/S DoS Settings ☐ Enable

POP/S and IMAP/S Settings

Don't Scan Emails Greater Than \* 2048 KB Enter 0 for default size restriction of 10240 KB

Recipient Headers

Headers

Delivered-To

Received

X-RCPT-TO

SMTP TLS Configuration

TLS Certificate \* SecurityAppliance\_SSL\_CA

Allow Invalid Certificate ☒ Enable

Require TLS Negotiation with Host/Net

Add New Item

Require TLS Negotiation with Sender Domain

Add New Item

Skip TLS Negotiation Hosts/Nets

Add New Item

POP and IMAP TLS Configuration

TLS Certificate \* SecurityAppliance\_SSL\_CA

Allow Invalid Certificate ☒ Enable

Apply

#### Step 4: Create Malware Scanning Rule

Go to Protection > Email Protection > Scanning Rules and click Add under Malware Scanning Rules.

Example:

1. Block all executable files
2. Enable Dual Anti-Virus scanning

| Parameters       | Value   | Description   |
|------------------|---|---|
| Name             | BlockExecutable   | Enter a unique name to identify the scanning rule.  |
| Sender           | Any   | <p>Select the sender name from the list of users.</p> <p>Select Any if the rule is to be applied on all the senders.</p> <p>You can also add a new Email address by clicking Create New link.</p>       |
| Recipient        | mycompany.com   | <p>Select the recipient name from the list of users.</p> <p>Select Any if the rule is to be applied on all the recipients.</p> <p>You can also add a new Email Address by clicking Create New link.</p> |
| Block File Types | Executable Files  | Select file types to be blocked as an attachment to remove all the files that are a potential threat and to prevent virus attacks.  |
| Scanning         | Dual Anti-Virus   | <p>Specify the type of scanning to be applied.</p> <p>Here, Traffic will be scanned by both Anti-Virus Engines.</p>   |
| Action           | Quarantine  | Quarantine infected Emails. Quarantined Emails can be viewed from System > Email > Malware Quarantine.  |
| Delivery Options |   |   |
| Recipient        | Infected Attachment:<br>Don't Deliver<br>Protected Attachment:<br>Deliver Original  | Select the action to be taken on the message that is detected to be Infected or includes a Protected Attachment.  |
| Administrator    | Infected Attachment:<br>Remove Attachment<br>Protected Attachment:<br>Send Original | Select the action to notify the Administrator for the message detected to be Infected or includes a Protected Attachment.   |

SMTP/S Malware Scanning Rules
Help admin

Protection > Email Protection > Scanning Rules

Name \*

Email Address/Domain Group

Sender \*

Recipient \*

Attachment Filter

Block File Types \*

None  
All  
Video Files  
Audio Files  
**Executable Files**  
Dynamic Files  
Image Files

MIME White List

None  
application/bat  
application/x-bat  
application/x-msdos-program  
application/textedit

Malware Filter

Scanning

Action
☒ Quarantine  
☐ Notify Sender

Delivery Option for

Infected Attachment
Protected Attachment

Recipient

Administrator

Save Cancel

Click Save to create the rule.

### Step 5: Create Content Scanning Rules

You can create a number of Content Scanning Rules to define the actions that SF should take if an Email is detected as Spam. Ideally, you will have to create all the rules mentioned in the below table to protect your network against any Spam from your Email Server. Content Scanning Rules are processed from the top down and the first suitable rule found is applied. Hence, while adding multiple rules, it is necessary to put specific rules before the general rules.

| Rule          | Purpose  |
|---------------|--|
| inbound_rule1 | Drops Emails destined to mycompany.com detected as SPAM over SMTP/S<br>Adds prefix "POPIMAPSpam:" to subject in Emails destined to mycompany.com detected as SPAM over POP/S-IMAP/S.                               |
| inbound_rule2 | Drops Emails destined to mycompany.com detected as Virus Outbreak over SMTP/S.<br>Adds prefix "POPIMAPVirusOutbreak:" to subject in Emails destined to mycompany.com detected as Virus Outbreak over POP/S-IMAP/S. |
| inbound_rule3 | Adds prefix "Spam(RBL):" to subject in Emails destined to mycompany.com that are detected as Spam by configured RBL(s).  |

|                       |   |
|-----------------------|---|
| DOMAIN_ACCEPT_inbound | Accept all Emails destined to mycompany.com.  |
| outbound_rule1        | Drops all Emails originating from mycompany.com detected as SPAM.   |
| outbound_rule2        | Drops all Emails originating from mycompany.com with content matching configured Data Protection Policy.          |
| OUTBOUND_ACCEPT_Rule  | Accept all Emails originating from mycompany.com.   |
| No_Open_Relay         | Drop All Emails over SMTP/S. This rule is necessary to protect the Email Server from being used as an open relay. |

Note:

Since we have created Business Application Rule with template “EmailServer(SMTP)”, only SMTP/S traffic will be scanned via Content Scanning Rules.

| Content Scanning Rules   |                                       |           |           |  |                                 |   | <input type="button" value="Add"/> <input type="button" value="Delete"/> |  |
|--------------------------|---------------------------------------|-----------|-----------|--|---------------------------------|---|--|--|
| <input type="checkbox"/> | Name                                  | Sender    | Recipient | Rules  | SMTP/S Action                   | POP3/S-IMAP/S Action                      | Manage   |  |
| <input type="checkbox"/> | <a href="#">inbound_rule_1</a>        | Any       | mycompany | Mail is identified as Spam by Inbound Anti Spam Module           | Drop                            | Prefix Subject To "POPIMAPSpam:"          |  |  |
| <input type="checkbox"/> | <a href="#">inbound_rule2</a>         | Any       | mycompany | Mail is identified as Virus Outbreak by Inbound Anti Spam Module | Drop                            | Prefix Subject To "POPIMAPVirusOutbreak:" |  |  |
| <input type="checkbox"/> | <a href="#">inbound_rule3</a>         | Any       | mycompany | Sender IP Address Black Listed By Premium RBL Services           | Prefix Subject To "Spam(RBL) :" | NA  |  |  |
| <input type="checkbox"/> | <a href="#">DOMAIN_ACCEPT_inbound</a> | Any       | mycompany | None   | Accept                          | Accept                                    |  |  |
| <input type="checkbox"/> | <a href="#">outbound_rule1</a>        | mycompany | Any       | Mail is identified as Spam by Outbound Anti Spam Module          | Drop                            | NA  |  |  |
| <input type="checkbox"/> | <a href="#">outbound_rule2</a>        | mycompany | Any       | Data Protection Policy   | Reject                          | NA  |  |  |
| <input type="checkbox"/> | <a href="#">OUTBOUND_ACCEPT_RULE</a>  | mycompany | Any       | None   | Accept                          | Accept                                    |  |  |
| <input type="checkbox"/> | <a href="#">No_Open_relay</a>         | Any       | Any       | None   | Drop                            | Accept                                    |  |  |

Example: Create inbound\_rule1 to

1. Drop Emails destined to mycompany.com detected as SPAM over SMTP/S
2. Add prefix “POPIMAPSpam:” to subject in Emails destined to mycompany.com detected as SPAM over POP/S-IMAP/S.

Go to System > Email > Scanning Rules and click Add under Content Scanning Rules. Create rule as shown below.

Content Scanning Rules

[Help](#)
[admin](#)

Protection > Email Protection > Scanning Rules

Name \*

Email Address/Domain Group

Sender \*

Contains

Any

Recipient \*

Contains

mycompany

Filter Criteria

☒ Inbound Email is
 

Spam

☐ Outbound Email is
 

Spam

☐ Source IP/Network Address
 

Add New Item

☐ Destination IP/Network Address
 

Add New Item

☐ Sender Remote Blacklist
 

RBL Group

☐ Message Size
 

Greater Than

KB

☐ Message Header
 

Select Message Header

Contains

☐ Data Protection Policy
 

None

☐ None

Action

SMTP/S

Drop

To

SPX Templates

None

☒ Quarantine

POP3/S-IMAP/S

Prefix Subject

To

POPIMAPSpam:

Save

Cancel

Click Save to create the rule.

## Test Configuration

You can check how Emails sent to and from the Email Server are accepted or dropped from the Log Viewer. Access it from System > Diagnostics > Log Viewer.

