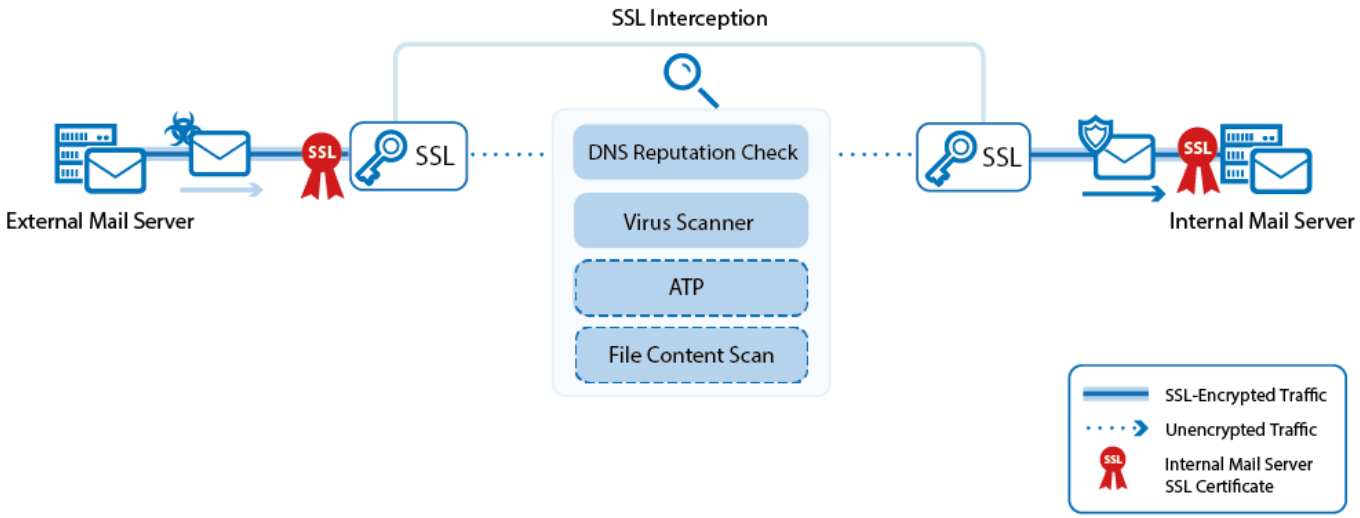
How to Configure Mail Security in the Firewall

https://campus.barracuda.com/doc/48203038/

The Barracuda NextGen Firewall F-Series scans SMTP traffic in two steps:

1. SSL Interception decrypts SSL-encrypted SMTP connections. For incoming connections, your mail server's SSL certificates are used.
2. The DNSBL base is queried via a DNS lookup using the sender's IP address. If the DNS reputation database is not available, the email is not modified. If the domain or IP address is blacklisted, the emails subject line is modified to start with **[SPAM]** and the following non-configurable MIME type headers are set:
   - X-Spam-Prev-Subject: Your email subject without the [SPAM] tag.
   - X-Spam-Flag: YES
   - X-Spam-Status: Yes
   - X-Spam-Level: ***
3. Email attachments are scanned by the Virus Scanning service on F-Series Firewalls. If malware is found, the attachment is stripped from the email and replaced by a customizable text informing the user that the malicious attachment has been removed. For F-Series Firewalls using ATP, the email attachments can also be checked via ATP using the **deliver first, then scan** mode. Scan results must be monitored by the admin because quarantining is not supported for SMTP.



Before You Begin

- The **Feature Level** of the Forwarding Firewall must be set to **6.2** or higher.
- Enable Application Control. For more information, see How to Enable Application Control.
- Enable SSL Interception. For more information, see How to Configure SSL Interception in the

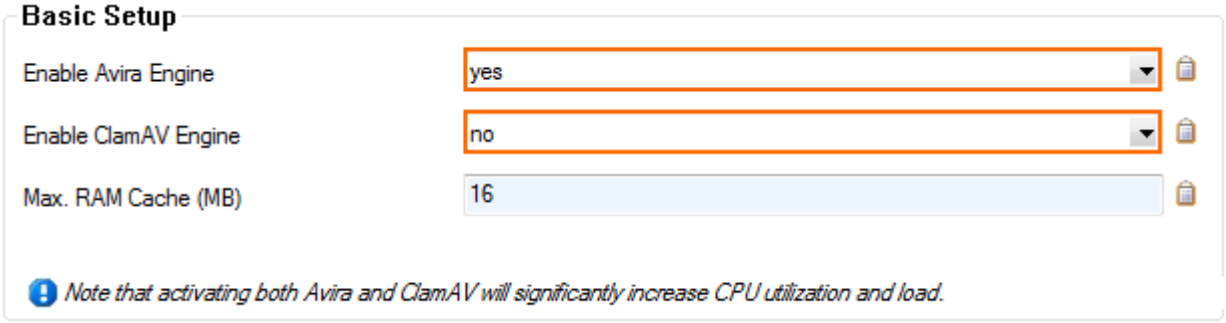
Firewall.

- Create a Virus Scanner service. For more information, see Virus Scanner.

Step 1. Configure the Virus Scanner Engine(s)

Select and configure a virus scanning engine. You can use Avira and ClamAV either separately or together. The F-Series F100 and F101 can only use the Avira virus scanning engine.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Virus-Scanner > Virus Scanner Settings**.
2. Click **Lock**.
3. Enable the virus scanner engines of your choice:
   Using both virus scanner engines significantly increases CPU utilization and load.
   - To enable the Avira AV engine, select **Yes** from the **Enable Avira Engine** drop-down.
   - To enable the ClamAV engine, select **Yes** from the **Enable ClamAV** drop-down.

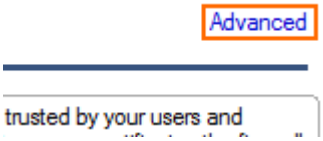


4. Click **Send Changes** and **Activate**.

Step 2. Configure SSL Interception

If needed, adjust the SSL Interception settings to support MTAs requiring SSLv2, SSLv3, or a specific cipher set. SSL-encrypted SMTP sessions cannot be scanned by an F-Series F100 or F101 because SSL Interception is not supported for those models.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Security Policy**.
2. Click **Lock**.
3. Verify the **Enable SSL Interception** check box is selected.
4. (optional) Click **Advanced** to enable support for SSLv2, SSLv3, and custom cipher string. For more information, see How to Configure SSL Interception in the Firewall.



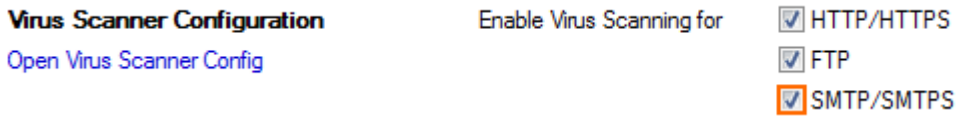
- **SSL version handling**
  - **Allow (obsolete) SSLv2** – Enable if you must support remote SSLv2-only MTAs.
  - **Allow (obsolete) SSLv3** – Enable if you must support remote SSLv3-only MTAs.
  - **OpenSSL cipher string** – You can set a custom cipher string. The firewall uses the following default cipher string:
    HIGH:!aECDH:!ADH:!3DES:!MD5:!DSS:!RC4:!EXP:!eNULL:!NULL:!aNULL

5. Click **OK**.
6. Click **Send Changes** and **Activate**.

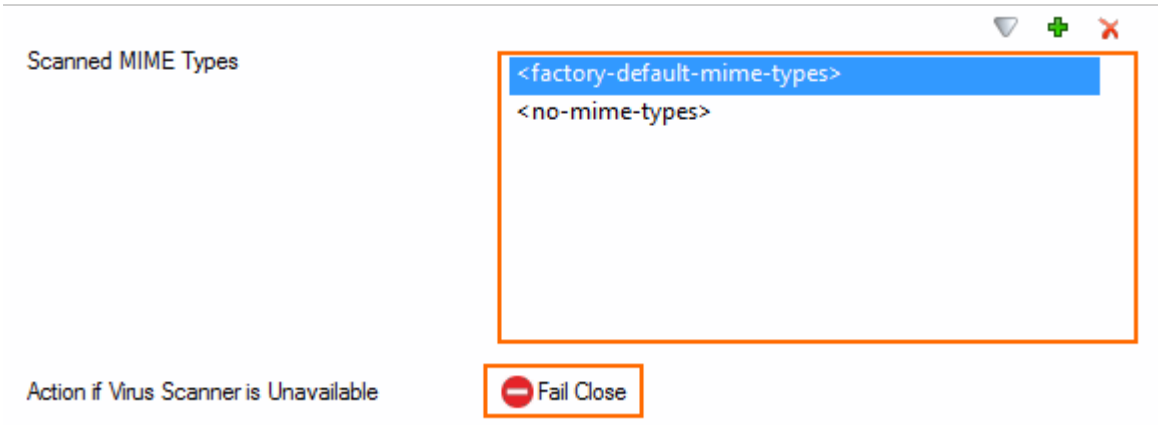
Step 3. Enable Virus Scanning

The firewall must use your internal mail server's SSL certificate to be able to pass identity checks carried out by some MTAs. You must also enable virus scanning and enter the IP address of the DNSBL server.

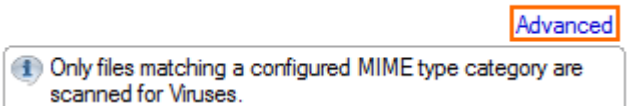
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Security Policy**.
2. Click **Lock**.
3. In the **Virus Scanner Configuration** section, select **SMTP/SMTPS**.



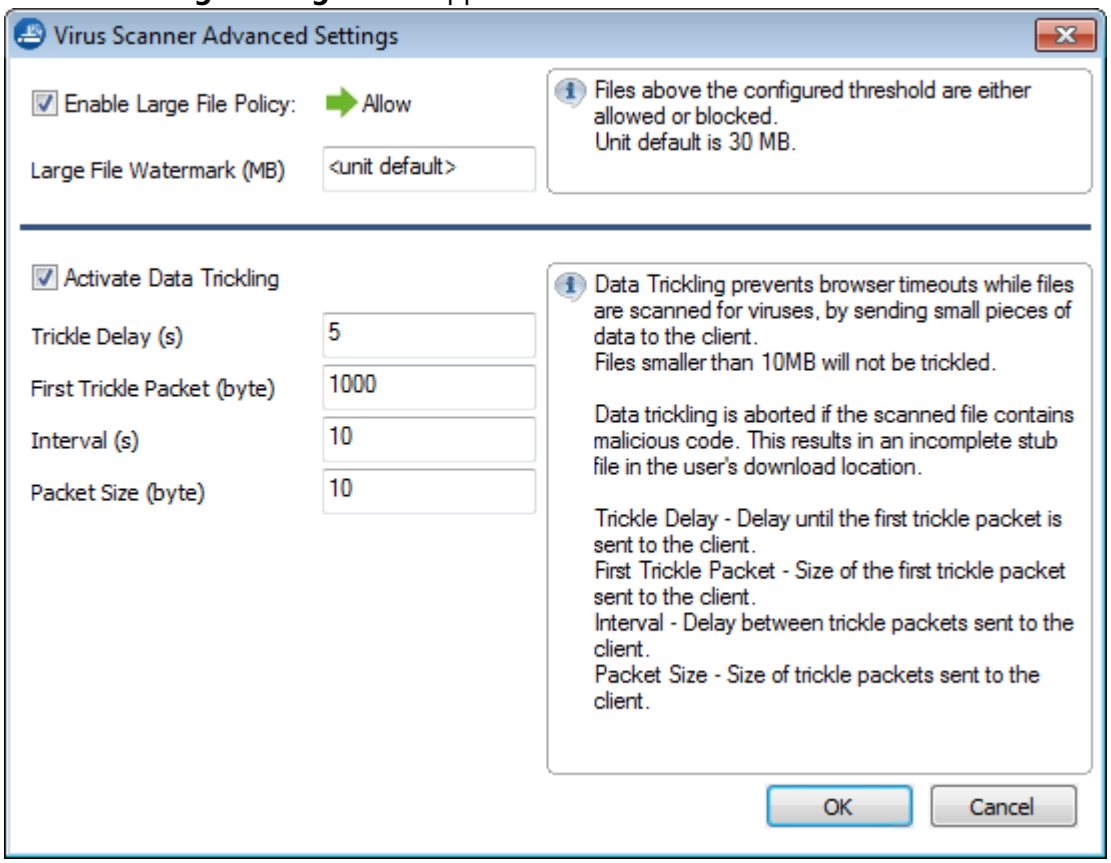
4. In the **Scanned MIME types** list, add the MIME types of the files that you want the virus scanner to scan. Default: and . For more information, see Virus Scanning and ATP in the Firewall.



5. (optional) Click on **Advanced**:



- **Large File Policy** – The large file policy is set to a sensible value for your appliance. The maximum value is 4096 MB.
- **Data Trickling Settings** – Not applicable for SMTP traffic.

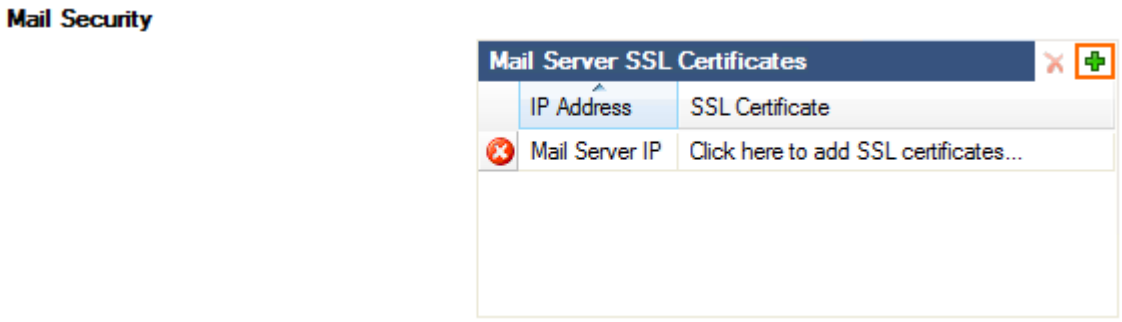


6. Click **Send Changes** and **Activate**.

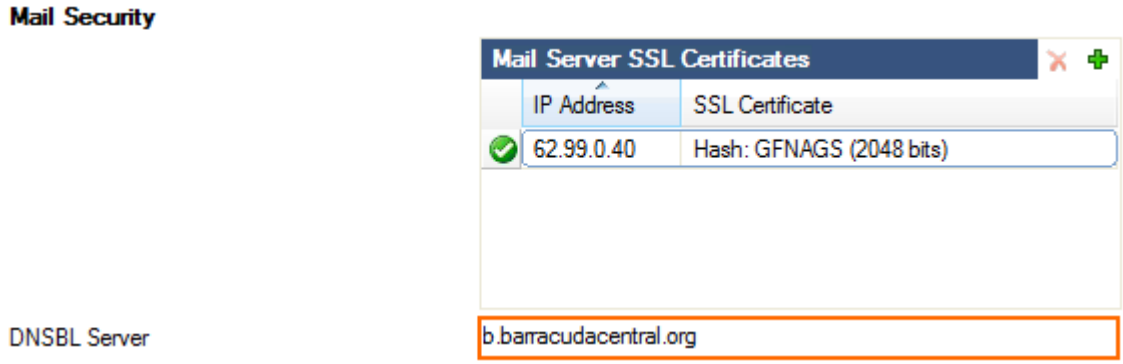
Step 4. Enable Mail Security in the Firewall and Upload the Mail Server SSL Certificate

Enable the DNSBL check and upload your mail servers SSL certificates.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Security Policy**.
2. Click **Lock**.
3. In the **Mail Security** section, click + to add your **Mail Server SSL Certificates**. An entry is added to the list.



4. In the **IP Address** column, click on **Mail Server IP** and enter the IP address that your mail server domain's MX record resolves to.
5. In the **SSL Certificate** column, click the **Click here to add SSL certificates** link and import the SSL certificates of your internal mail server:
   - **Import Key** – Select to import the private key from the clipboard or file in PEM format.
   - **Import Certificate** – Select to import the public key from the clipboard or file in PEM or PKCS12 format.
   - **Chain Certificate** – Select to import a certificate chain in PEM format.
6. Enter the **DNSBL Server** as a FQDN. Default: `b.barracudacentral.org`



7. Click **Send Changes** and **Activate**.

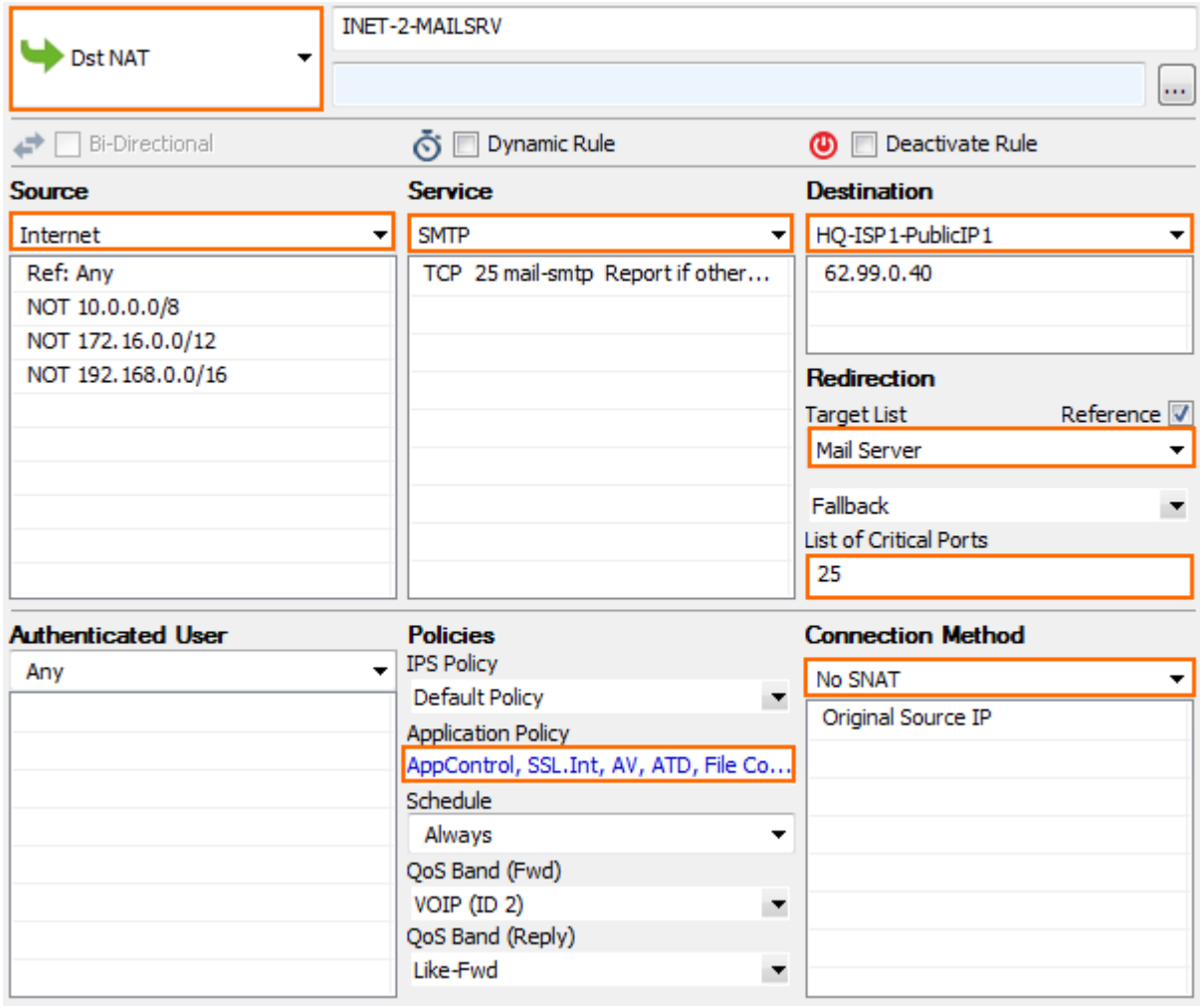
Step 5. Create a DNAT Access Rule for Incoming SMTP Traffic

Enable Application Control, SSL Interception, Virus Scanning, ATP (optional), and File Content Scanning (optional) in the access rule.

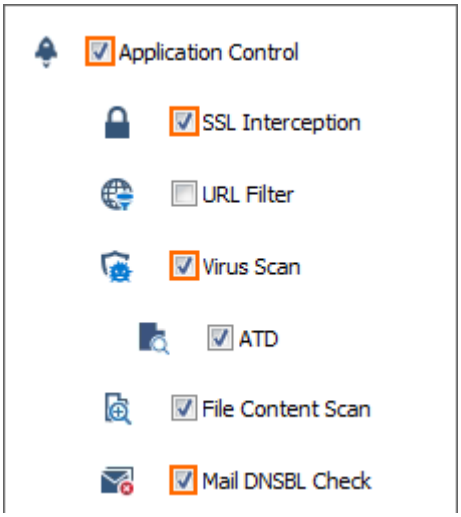
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Either click the plus icon (**+**) at the top right of the ruleset, or right-click the ruleset and select **New > Rule**.

4. Select **Pass** as the action.
5. Enter a **Name** for the rule.
6. Specify the following settings to match your incoming SMTP traffic:

- **Action** – Select **Dst NAT**.
- **Source** – Select **Internet**.
- **Destination** – Enter the public IP address that your mail server domain's MX record resolves to.
- **Service** – Select **SMTP**.
- **Connection Method** – Select **No SNAT**.



7. Click on the **Application Policy** link and select**:**
   - **Application Control** – Required.
   - **SSL Interception** – Required.
   - **Virus Scan** – Required.
   - **ATD** – optional.
   - **File Content Scan** – optional. For more information, see File Content Filtering in the Firewall.
   - **Mail DNSBL Check** – Select to enable DNSBL check.



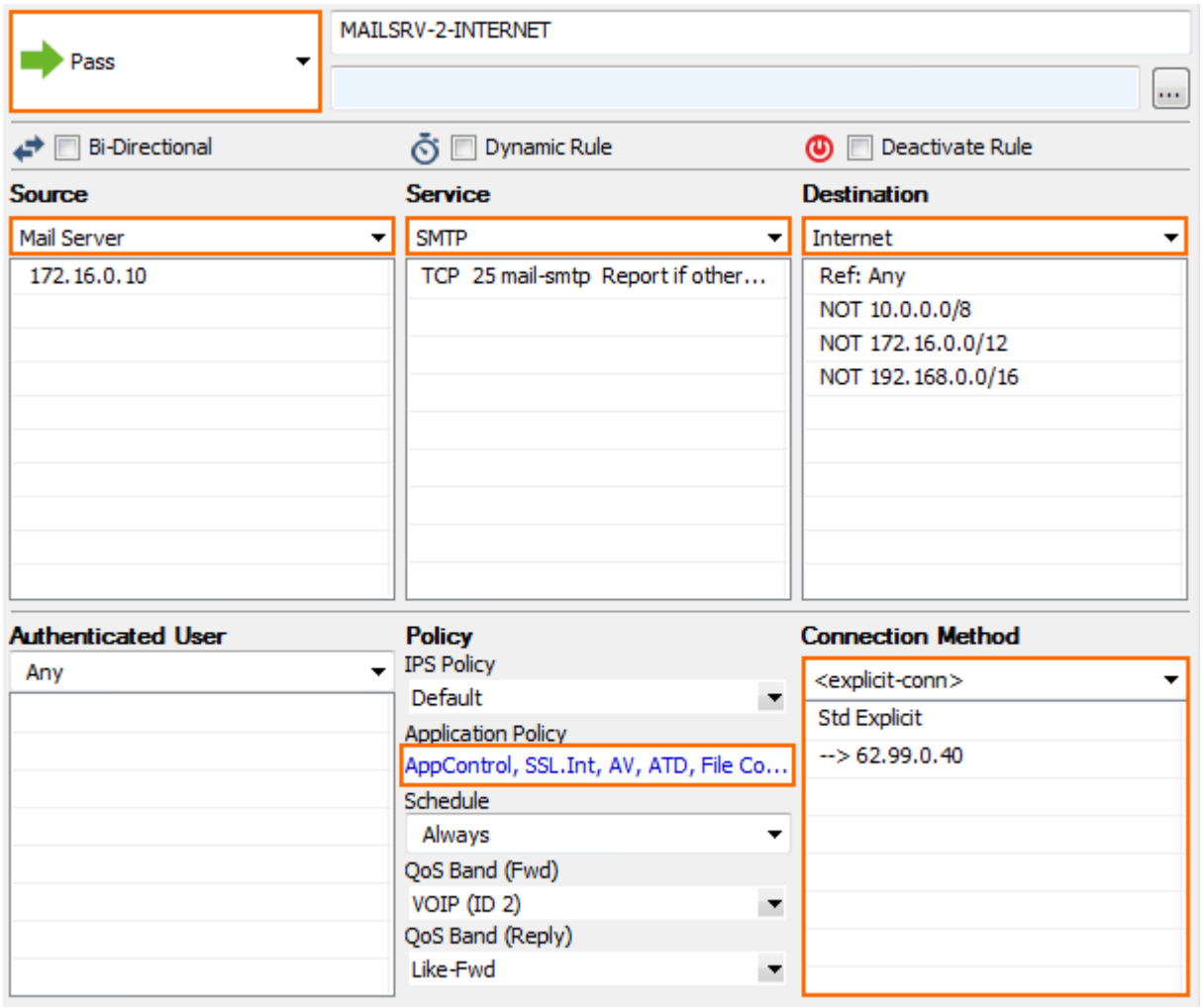
8. Click **OK**.
9. Click **Send Changes** and **Activate**.

Step 6. (optional) Create a Pass Access Rule for Outgoing SMTP Connections

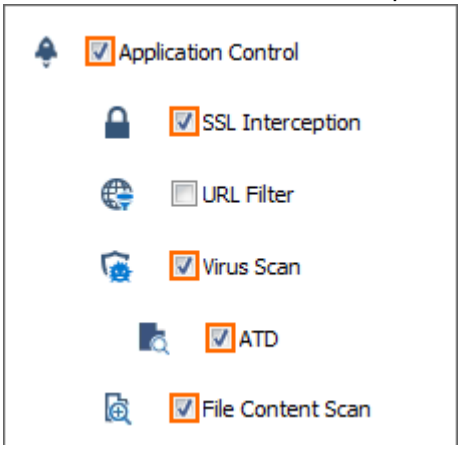
To also scan outgoing SMTP traffic from your internal mail server or mail clients for malware, create a PASS access rule.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Either click the plus icon (**+**) at the top right of the ruleset, or right-click the ruleset and select **New > Rule**.

4. Select **Pass** as the action.
5. Enter a **Name** for the rule.
6. Specify the following settings to match your incoming SMTP traffic:
   - **Action** – Select **PASS**.
   - **Source** – Select the network object containing your mail server IP addresses, or for SMTP client connections the network containing the SMTP clients.
   - **Destination** – Select **Internet**.
   - **Service** – Select **SMTP** for outgoing mail server traffic or create a service object for TCP port 587 for outgoing mail client traffic.
   - **Connection Method** – If used for an internal mail server, select a connection object using the public IP address that your mail server's MX record resolves to as the source IP address. If this rule applies to SMTP clients, select **Dyn SNAT**.



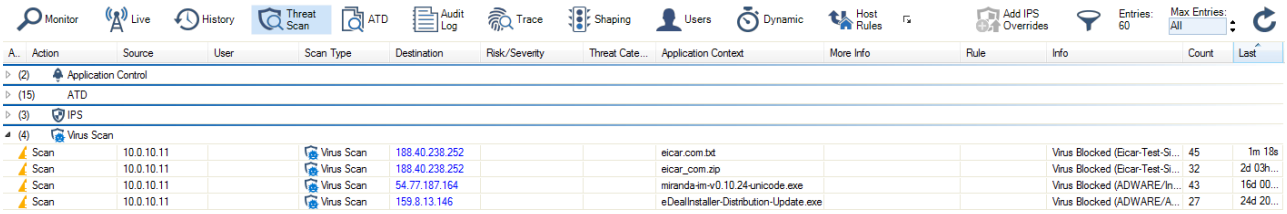
7. Click on the **Application Policy** link and select**:**
   - **Application Control** – Required.
   - **SSL Interception** – Required.
   - **Virus Scan** – Required.
   - **ATD** – optional.
   - **File Content Scan** – optional.



8. Click **OK**.
9. Click **Send Changes** and **Activate**.

Monitoring and Testing

- Test the virus scan setup by sending EICAR test files from http://www.eicar.com via email to a mail server located behind the firewall.
- To monitor detected viruses and malware, go to the **FIREWALL > Threat Scan** page.



Next Steps

- Customize the text used to replace removed email attachments. For more information, see How to Configure Custom Block Pages and Texts.
- To combine ATP with Mail Security in the Firewall, see Advanced Threat Protection (ATP).

Figures

1. virus_scanning_mail_traffic_atp-01.png
2. AV_SMTP_01.png
3. AV_SMTP_05.png
4. AV_SMTP_08.png
5. AV_SMTP_09.png
6. AV_SMTP_02.png
7. FW_virus_scanning_advanced.png
8. AV_SMTP_10.png
9. AV_SMTP_11.png
10. FW_Rule_Add01.png
11. AV_SMTP_04.png
12. file_content_fw_02.png
13. FW_Rule_Add01.png
14. AV_SMTP_07.png
15. AV_SMTP_12.png
16. avScanning02.png