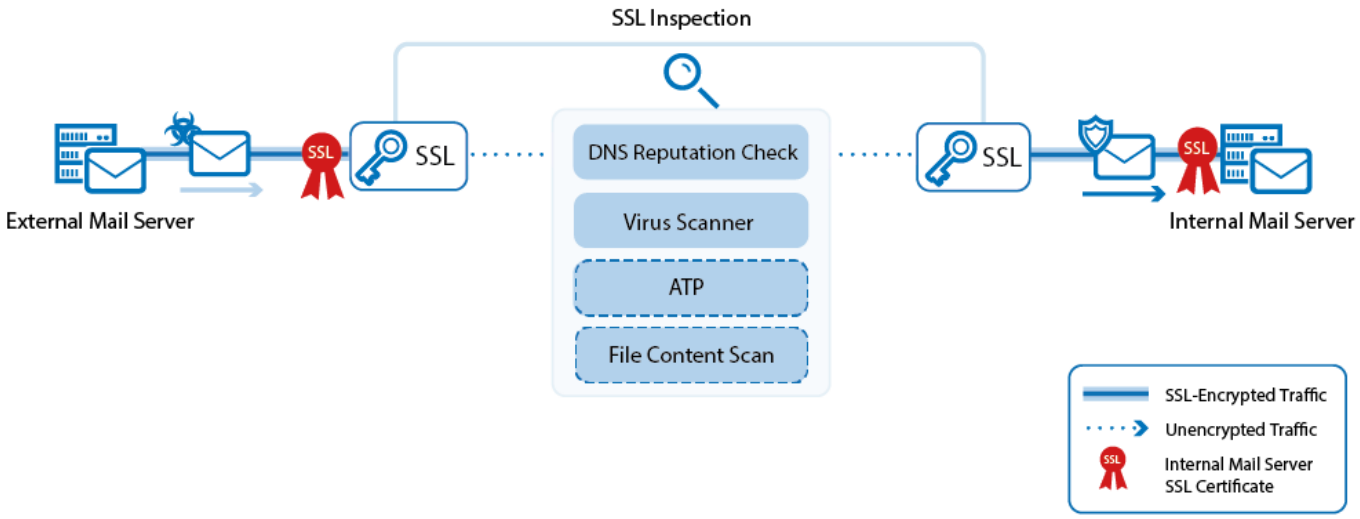
How to Configure Mail Security in the Firewall

https://campus.barracuda.com/doc/73719338/

The Barracuda CloudGen Firewall scans inbound SMTP and POP3 traffic in two steps:

1. SSL Inspection decrypts SMTP and POP3 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 Scanner service on the firewall. 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 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 and POP3.



Before You Begin

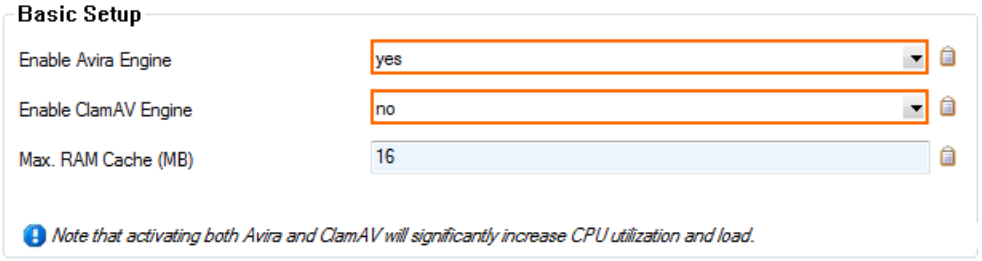
- The **Feature Level** of the Forwarding Firewall must be set to **7.2** or higher.
- Enable Application Control. For more information, see How to Enable Application Control.
- Configure SSL Inspection. For more information, see How to Configure Inbound SSL Inspection

and How to Configure Outbound SSL Inspection.
- 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 CloudGen Firewall 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 Inbound SSL Inspection

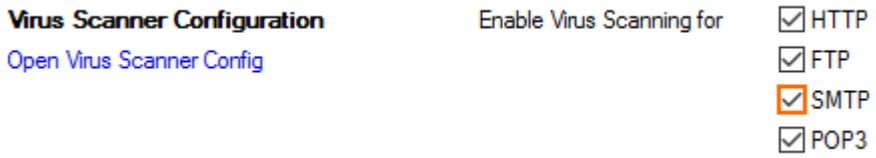
Upload the mail server certificate to the certificate store and configure Inbound SSL Inspection for the mail server. For more information, see How to Configure Inbound SSL Inspection.

Step 3. Enable Virus Scanning

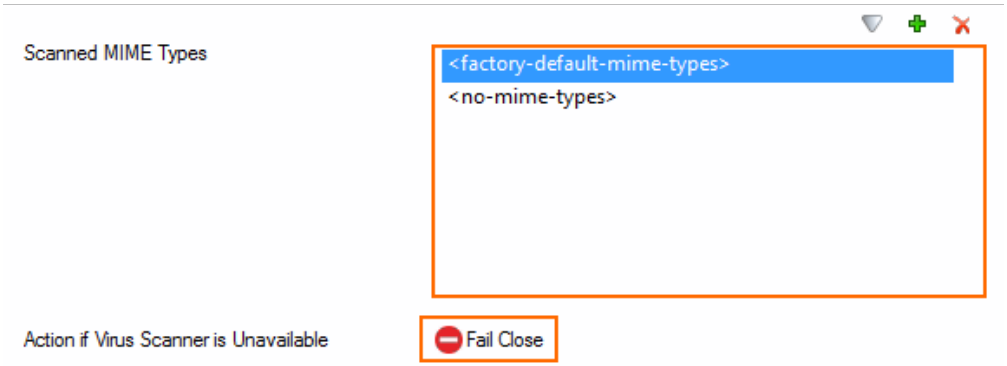
The firewall must use your internal mail server's SSL certificate to be able to pass identity checks carried out by some MTAs. You must also enable virus scanning and enter the IP address of the DNSBL server.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Security Policy**.
2. Click **Lock**.

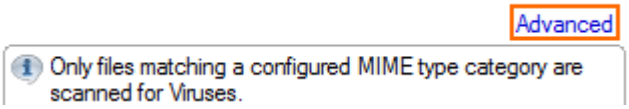
3. In the **Virus Scanner Configuration** section, select the checkbox for **SMTP** and/or **POP3**.



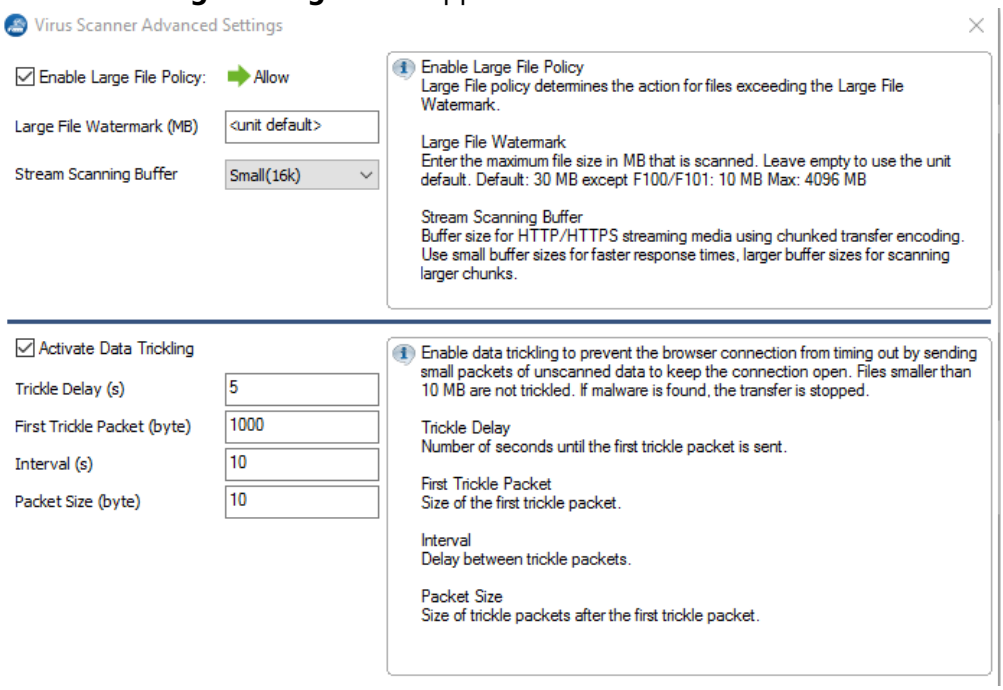
4. In the **Scanned MIME types** list, add the MIME types of the files that you want the virus scanner to scan. Default: `<factory-default-mime-types>` and `<no-mime-types>`. For more information, see Virus Scanning and ATP in the Firewall.



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.



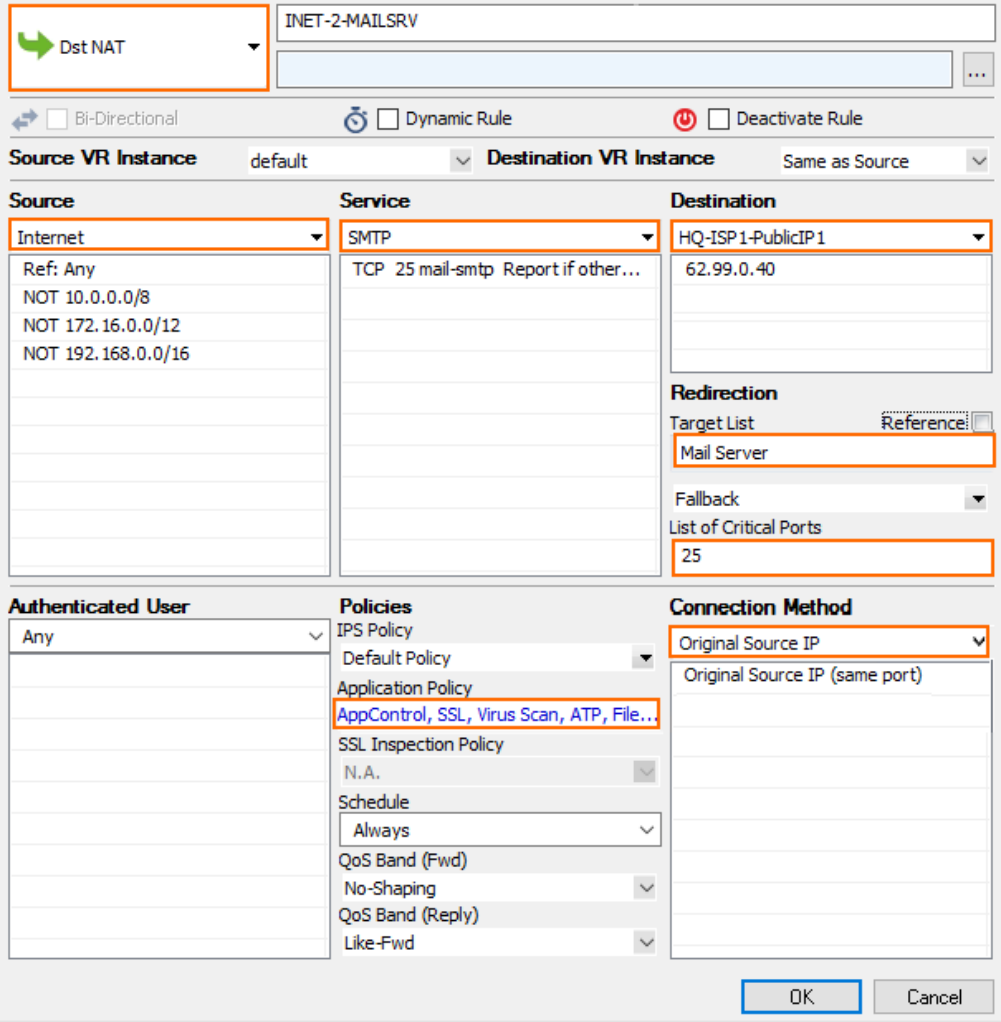
6. Click **Send Changes** and **Activate**.

Step 4. Create a Dst NAT Access Rule for Incoming SMTP Traffic

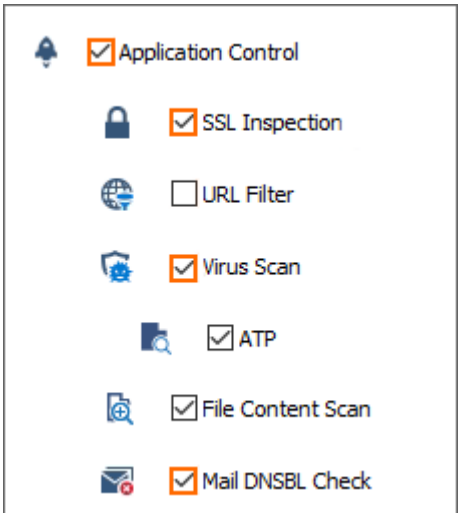
Enable Application Control, SSL Inspection, Virus Scanning, ATP (optional), and File Content Scanning (optional) in the access rule.

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** or **POP3**.
   - **Connection Method** – Select **Original Source IP**.



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



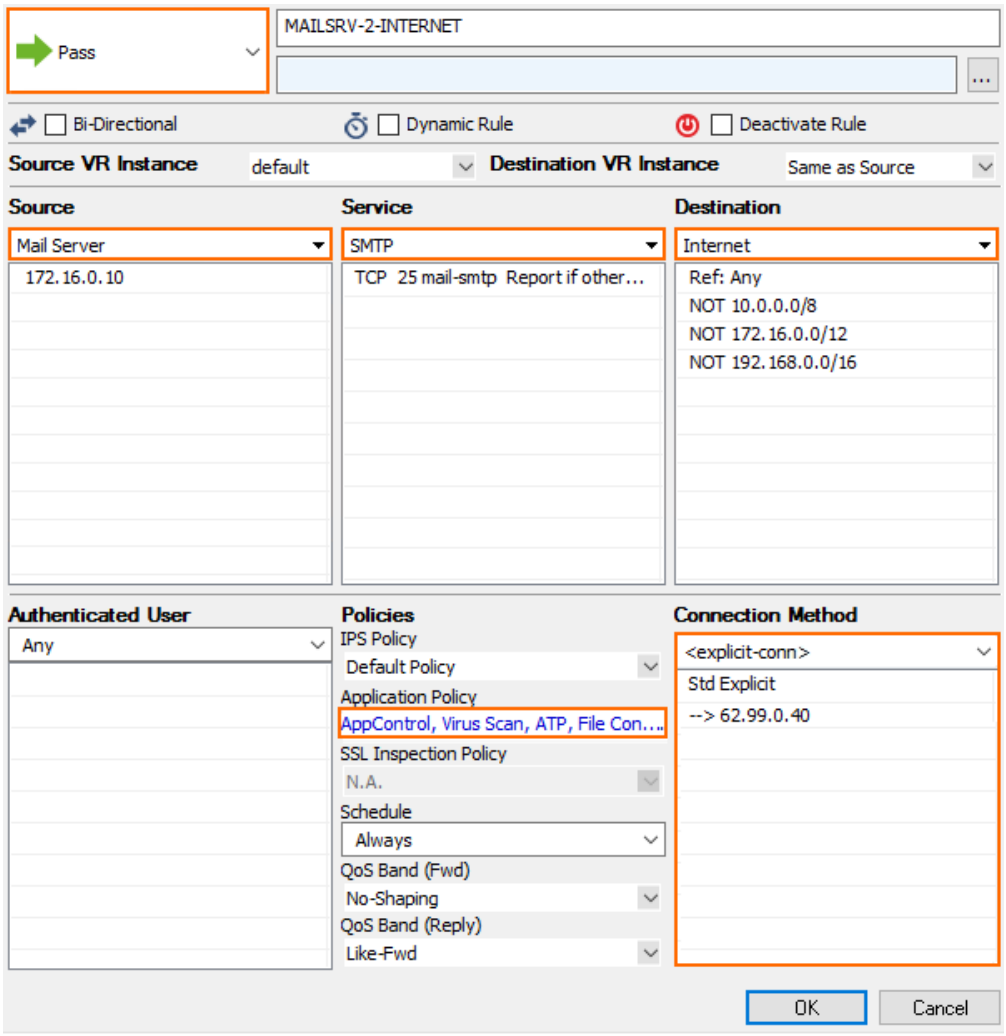
8. Select a policy from the **SSL Inspection Policy** drop-down list. For more information, see How to Configure Inbound SSL Inspection.
9. Click **OK**.
10. Click **Send Changes** and **Activate**.

Step 5. (optional) Create a Pass Access Rule for Outgoing SMTP Connections

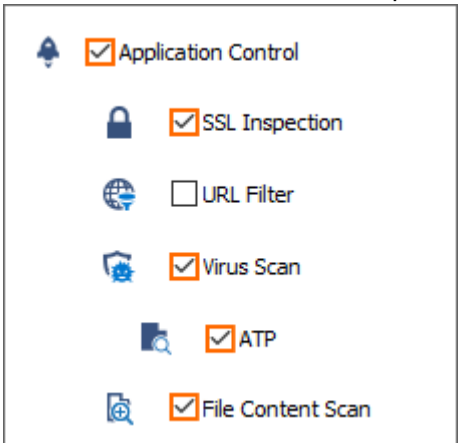
To also scan outgoing SMTP traffic from your internal mail server or mail clients for malware, create a PASS access rule.

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** or **POP3** for outgoing mail server traffic. You can also create a service object for TCP port 587 (SNMP) or 110 (POP3) for outgoing mail client traffic. For more information, see How to Create Service Objects.
   - **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 **Dynamic NAT**.



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

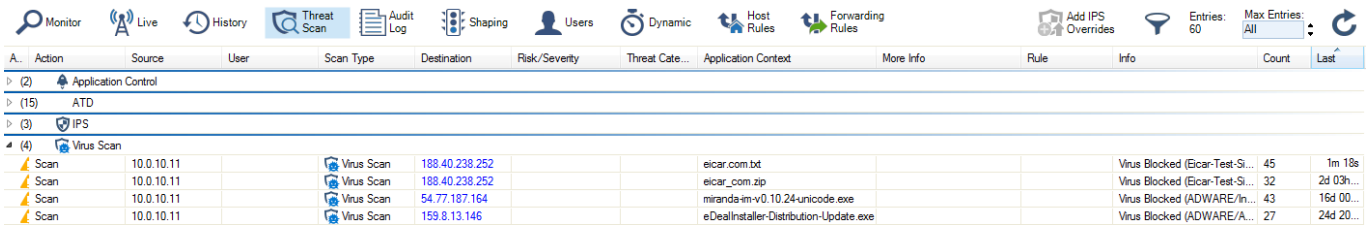


8. Select a policy from the **SSL Inspection Policy** drop-down list. For more information, see How to Configure Outbound SSL Inspection.

9. Click **OK**.
10. 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.
- All information about mail scanning in the firewall is logged to the **/firewall/virusscan.log** logfile.
- 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_atp1.png
2. AV_SMTP_01.png
3. AV_SMTP_08.png
4. AV_SMTP_09.png
5. AV_SMTP_02.png
6. FW_virus_scanning_advanced.png
7. FW_Rule_Add01.png
8. AV_SMTP_04.png
9. file_content_fw_02.png
10. FW_Rule_Add01.png
11. AV_SMTP_07.png
12. AV_SMTP_12.png
13. avScanning02.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.