

How to Configure Virus Scanning in the Firewall for Outbound SMTP and POP3 Traffic

<https://campus.barracuda.com/doc/96026317/>

To scan SMTP and POP3 traffic from clients behind the firewall to SMTP and POP3 servers in the Internet, configure an access rule to match your web traffic and enable Application Control, TLS Inspection (optional, but mandatory for SMTPS and POP3S), and the Virus Scanner. If malware is detected, the file is discarded and the connection is reset. If ATP is enabled, files passed by the Virus Scanner are then uploaded to be analyzed in the Barracuda ATP Cloud.

Before You Begin

- Enable Application Control. For more information, see [How to Enable Application Control](#).
- Create a Virus Scanner service. For more information, see [Virus Scanner](#).
- (optional) Configure File Content Filtering in the Firewall. For more information, see [File Content Filtering in the Firewall](#).
- (optional) Configure ATP in the Firewall. For more information, see [How to Configure ATP in the Firewall](#).
- Configure TLS Inspection for FTPS traffic. For more information, see [How to Configure Outbound TLS Inspection](#)

Step 1. Configure the Virus Scanner Engine(s)

Select and configure a virus scanner engine. You can use Avira and ClamAV either separately or together. The CloudGen Firewall F100 and F101 can only use Avira.

Using both virus scanner engines significantly increases CPU utilization and load.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Virus-Scanner > Virus Scanner Settings**.
2. Click **Lock**.
3. Enable the virus scanner engines of your choice:
 - Enable the Avira AV engine by selecting **Yes** from the **Enable Avira Engine** list.
 - Enable the ClamAV engine by selecting **Yes** from the **Enable ClamAV** list.
4. Click **Send Changes** and **Activate**.

Step 2. Enable Virus Scanning for SMTP and POP3

Enable support for virus scanning SMTP and POP3 connections in the Firewall service.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Security Policy**.
2. Click **Lock**.
3. In the **Virus Scanner Configuration** section, select the **SMTP** and **POP3** check box.

Virus Scanner Configuration
[Open Virus Scanner Config](#)

Enable Virus Scanning for

- ☒ HTTP
- ☒ FTP
- ☒ SMTP
- ☒ POP3


4. (optional) Change the **Action if Virus Scanner is unavailable**.

Action if Virus Scanner is Unavailable

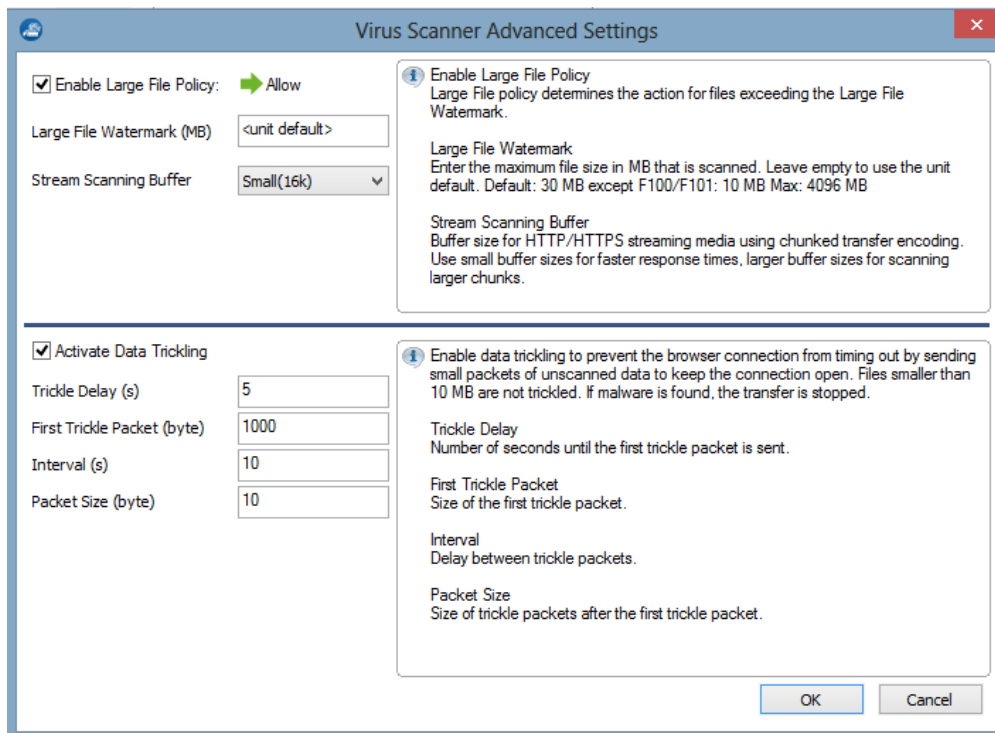
- ☒ Fail Open
- ☐ Fail Close

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

Advanced

 Only files matching a configured MIME type category are scanned for Viruses.


- **Large File Policy** – Action taken if the file exceeds the size set as the **Large File Watermark**. Select **Allow** to forward the files unscanned; select **Block** to discard files that are too big to be scanned.
- **Large File Watermark (MB)** – The large file watermark is set to a sensible value for your appliance. The maximum value is 4096 MB.
- **Stream Scanning Buffer** – Select the buffer size for HTTP/HTTPS streaming media using chunked transfer encoding. Select **Small** for faster response times, **Big** to scan larger chunks before forwarding the stream to the client.
- **Data Trickling Settings** – Change how fast and how much data is transmitted. Change these settings if your browser times out while waiting for the file to be scanned.

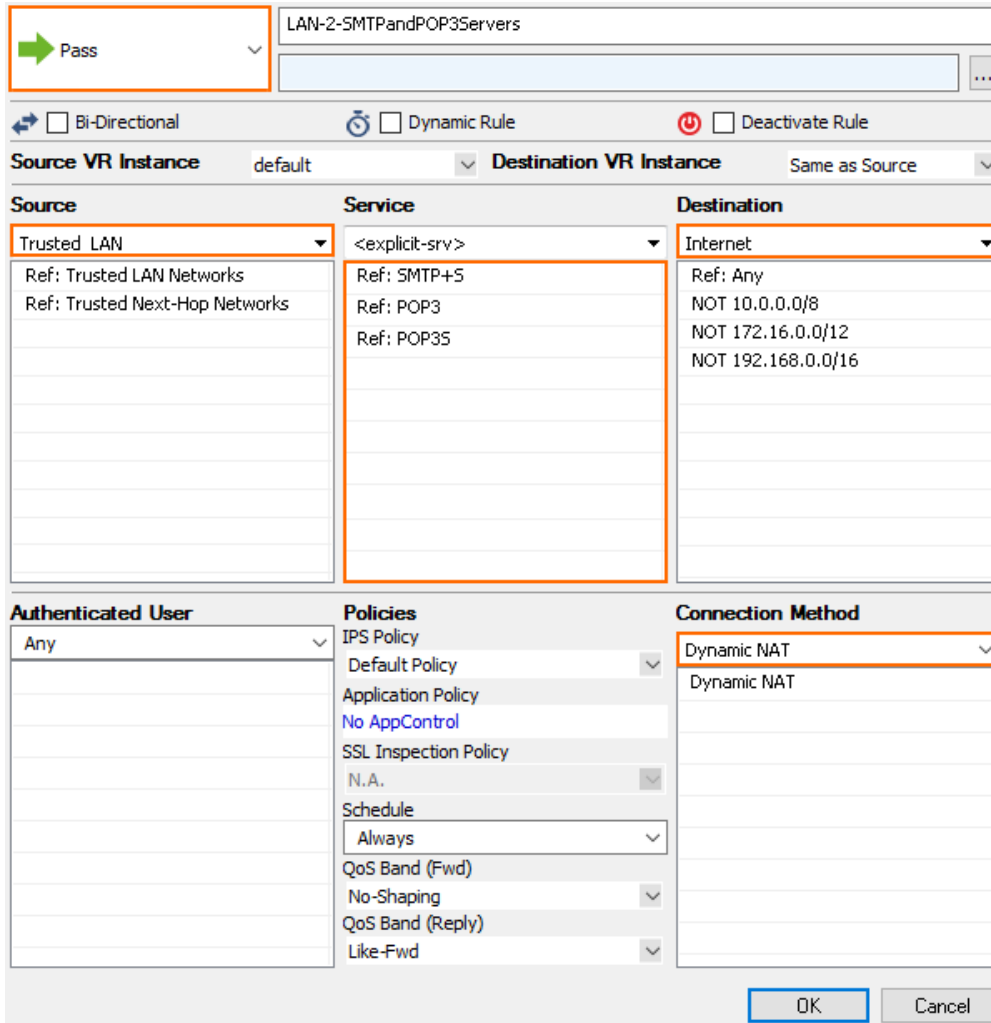


6. Click **Send Changes** and **Activate**.

Step 4. Create Access Rule for SMTP and POP3 Client Downloads

To scan connections to external SMTP, SMTPS, POP3, and POP3S servers, configure a Pass access rule and enable Application Control, TLS Inspection, Virus Scanning, and (optional) ATP.

1. Go to **CONFIGURATION > Configuration Tree > Box > 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 outbound SMTP and POP3 connections:
 - o **Action** – Select **Pass**.
 - o **Source** – Select **Trusted Networks**.
 - o **Destination** – Select **Internet**.
 - o **Service** – Select **SMTP+ S, POP3, and POP3S**.
 - o **Connection Method** – Select **Dynamic NAT**.



Pass

LAN-2-SMTPandPOP3Servers

☐ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

Source VR Instance: default Destination VR Instance: Same as Source

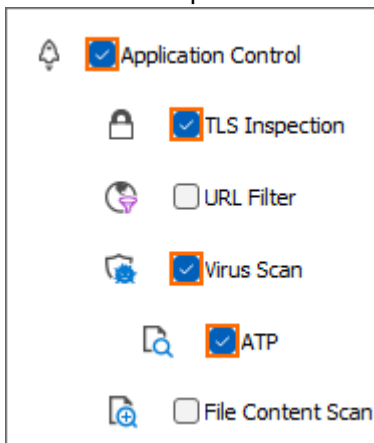
Source	Service	Destination
Trusted LAN	<explicit-srv>	Internet
Ref: Trusted LAN Networks	Ref: SMTP+S	Ref: Any
Ref: Trusted Next-Hop Networks	Ref: POP3	NOT 10.0.0.0/8
	Ref: POP3S	NOT 172.16.0.0/12
		NOT 192.168.0.0/16

Authenticated User	Policies	Connection Method
Any	IPS Policy	Dynamic NAT
	Default Policy	Dynamic NAT
	Application Policy	
	No AppControl	
	SSL Inspection Policy	
	N.A.	
	Schedule	
	Always	
	QoS Band (Fwd)	
	No-Shaping	
	QoS Band (Reply)	
	Like-Fwd	

OK Cancel

7. Click on the **Application Policy** link and select:

- **Application Control** – required.
- **TLS Inspection** – required.
- **Virus Scan** – required.
- **ATP** – optional.



☒ Application Control

☒ TLS Inspection

☐ URL Filter

☒ Virus Scan

☒ ATP

☐ File Content Scan

8. Select a policy for outbound TLS Inspection from the **TLS Inspection Policy** drop-down list. For more information, see [How to Configure a TLS Inspection Policy for Outbound TLS Inspection](#).

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

Next Steps

- To combine ATP with virus scanning, see [Advanced Threat Protection \(ATP\)](#) and [How to Configure ATP in the Firewall](#).
- To combine virus scanning with file content filtering, see [File Content Filtering in the Firewall](#).

Figures

1. AV SMTP_08.png
2. AV_FTP_06.png
3. AV SMTP_02.png
4. FW_virus_scan_advanced.png
5. FW_Rule_Add01.png
6. SMTP_AV_02.png
7. SMTP_AV_activated.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.