How to Configure POP3 Scanning

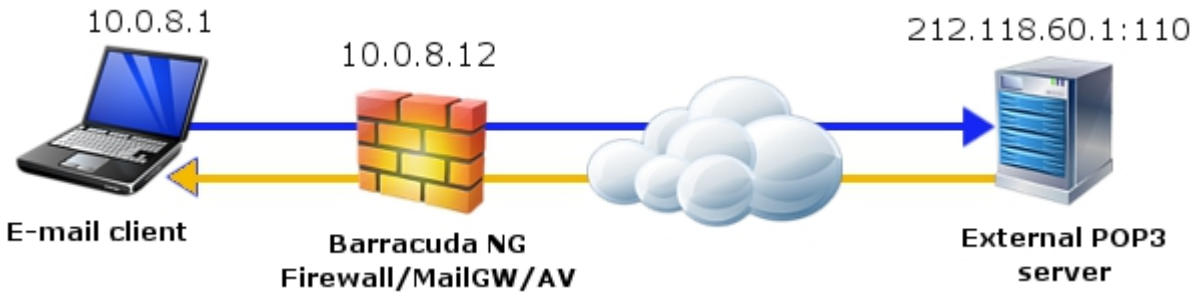
https://campus.barracuda.com/doc/43847207/

This article does not provide information on setting up a POP3 mail server; it provides instructions on how to configure the scanning of traffic between an email client and an external POP3 server.

Email clients use POP3 to retrieve mail from a remote server over a TCP/IP connection. Mail traffic is sometimes limited to fetching and forwarding emails to an externally hosted POP3 mail server, especially in small companies which do not operate an internal mail server. To enhance security when collecting emails, configure the Barracuda NG Firewall to scan data streams processed over POP3 for viruses and spam.

In this article:

POP3 Scanning - Example Setup



Requirements

Before configuring POP3 scanning, make sure that you have properly configured the following settings:

- **Firewall configuration –** A firewall rule must be configured to allow communication on the POP3 port (default: *110*).
- **Virus Scanner settings –** The Avira Virus Scanner service must be installed. The use of an external virus scanner is not possible.
- **Mail scanning settings –** Mail scanning must be activated. Settings apply to POP3 scanning.

- **Spam Filter settings –** If spam checking is required, install the Spam Filter service.
- **Email client configuration –** User specific login data must be entered into the email client that collects mail from the POP3 server. This login data has to be adapted so that the email client addresses the Barracuda NG Firewall instead of addressing the POP3 server directly. For the example setup that is illustrated in the figure above, configure the email client as follows:

Field	Value	Example
Username	username#POP3serverIP:port	cuda#212.118.60.1:110
Password	POP3 account password	*******
POP3 server	Listening IP of the POP3 scanning service	10.0.8.12

Configure POP3 Scanning

To configure the POP3 scanning service, complete the following steps:

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Mail-Gateway > Mail Gateway Settings**.
2. In the left menu, select **POP3 Setup**.
3. Click **Lock**.
4. You can configure the following settings:

Setting	Description
Use POP3	To enable the scanning of data processed over POP3, select **yes**. Virus scanning is also automatically enabled.
Listen on / Listen on IPv6	The IP address on which the mail gateway listens for POP3 requests. You can select **First-IP** and/or **Second-IP**. To explicitly specify IP addresses, select the **Other** check box. You can enter a comma-delimited list of IP addresses. If you explicitly specify the listen IP addresses, make sure that you also add them as virtual server addresses in the **Additional IP** table on the **Server Properties** page for your virtual server. For more information, see How to Configure Virtual Servers.
Maximum Children	The maximum number of concurrent connections that the mail gateway accepts for POP3 sessions (default: 10). Any connection attempts exceeding this limit are dropped.
Timeout (s)	The connection timeout between the email client and mail gateway. This value is of importance because long processing times caused by communication or connectivity problems between the mail gateway and POP3 server can lead to connection loss between the mail gateway and email client. You may leave the default setting at 30 seconds if you are not experiencing any problems.
Check Spam	To check emails retrieved via POP3 for spam, select **yes**. You must also make sure that the Spam Filter service has been properly created and installed.

Template	When the virus scanner finds a virus in an email, it immediately drops the email and attempts to send a new email informing the intended recipient about the infected message. In the **Template** field, enter a global template for these notifications. You can use the following variables in your template: ◦ %USERNAME% – Name of the user. ◦ %VIRUSNAME% – Virus information. ◦ %MAILFROM% – Sender email address. ◦ %MAILTO% – Recipient email address. ◦ %MAILDATE% – Date of the email. ◦ %SUBJECT% – Mail subject.
Subject	The subject header for the email informing the intended recipient about the infected message (default value: [VIRUS found]).
Delete Infected Mails	To delete infected emails immediately and not store them on the Barracuda NG Firewall, select **yes** (default: **no**). Emails are saved at `/var/phion/run/mailgw/<servername>_<servicename>/root/virus-rejected`.
Use HTML Tag Removal	To remove HTML tags from the email, select **yes** (default: **no**).

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

Continue with How to Configure Advanced Mail Gateway Settings.

Figures

1. mailgw_pop3.jpg