How to Configure Antivirus Mail Gateway Integration

https://campus.barracuda.com/doc/46209198/

Scanning of SMTP emails is based on standard SMTP communication between the Barracuda NextGen Firewall F-Series mail gateway and Virus Scanner MailGate. The following procedure describes how email is handled by the Barracuda NextGen Firewall F-Series virus scanning service:

1. Mail approaches the mail gateway.
2. Mail is redirected to virus scanner.
3. (Optional) Infected mail is deleted.
4. Mail is returned for delivery.
5. Mail is delivered.

For antivirus integration, you can configure either advanced virus protection options or an external scan engine.

In this article:

Configure Advanced Virus Protection Options

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 **Content Adaptations**.
3. Click **Lock**.
4. In the **Virus Detection** section, select **yes** from the **Enable Virus Detection** list.
5. Next to **Advanced Virus Protection Option**, click **Set** or **Edit**.
6. In the **Advanced Virus Protection Option** window, you can configure the settings in the following sections:

Section	Setting	Description
Scanner Location	**Scanner Location**	Specifies if a local or remote Virus Scanner Service is used. You can select: ◦ **Local** – The Virus Scanner service is running on the local Barracuda NextGen Firewall F-Series. ◦ **Remote** – The Virus Scanner service is running on a remote Barracuda NextGen Firewall F-Series. In the **Scanner IP** field, enter the IP address of the SMTP scan engine. If multiple virus scanners are used, the first available scanner will be used for virus scanning. If the connection to the active virus scanner breaks, the next available virus scanner is contacted.

Notification	**Expose Sender Alerts**	Specifies if warnings are sent to the sender of emails containing viruses and malicious software. You can select: ◦ **no** – Warnings are never sent to the sender. ◦ **yes** – Warning are always sent to the sender. ◦ **Local** – Warnings are sent only if the sender is a local domain user. Local domain users belong to domains that are defined as *internal* and *strictly_internal* in the **Protection Profile** setting of the Extended Domain Setup of the Mail Gateway service.
	Expose Postmaster Alerts	To send warnings to the postmaster about emails containing viruses and malicious software, select **yes**.
	Silently Drop Phishing Mail	To drop a phishing email without sending a DSN delay message to the sender, select **yes**. The phishing email is then automatically moved to the give-up folder and no further attempts are made to forward it.
Adaptions	**Add Status in Body**	To add the virus status to the mail body, select **yes**.
	Add X-Status in Header	To add the virus status to the mail header, select **yes**.
	Add Body to Notice	To add the original body of the infected mail to the postmaster notice mail, select **yes**.
No Scan Exceptions	**NoScan For (Recipients) | No Scan For (Sender)**	In the **NoScan For (Recipients)** and **No Scan For (Sender)** tables, add the email address or domain of recipients and senders whose emails should be not scanned. For example, enter the following to exclude a domain from scanning: `*.exampledomain.com` For example, enter the following to exclude a specific email address from scanning: `foo@exampledomain.com`

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

Configure an External Scan Engine

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 **Content Adaptations**.
3. Click **Lock**.
4. In the **Virtual Detection** section, select **external** from the **Enable Virus Detection** list.
5. Next to **External Scan Engine**, click **Set** or **Edit**.
6. In the **External Scan Engine** window, you can configure the following settings:

Setting	Description

Scan Engine IPs	In this table, add the IP addresses of the external SMTP scan engines. If multiple virus scanners are used, the first available scanner is used for virus scanning. If the active virus scanner is disconnected, the next available virus scanner is contacted.
Scan Engine Port	The ports that are used to contact the external SMTP scan engine.
Listen IP	The IP address on which the Mail Gateway service listens to and awaits virus scan engine replies. Make sure that the listen IP address is listed as a virtual server address in the **Additional IP** table on the **Server Properties** page for your virtual server. For more information, see How to Configure Virtual Servers.

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

Continue with How to Configure Content Stripping, Grey Listing, and Blacklists.