Virus Checking and Notifications

https://campus.barracuda.com/doc/3866666/

Virus scanning is automatically enabled on the Barracuda Email Security Gateway and the system checks for definition updates on a regular basis (hourly by default). Virus Scanning takes precedence over all other mail scanning techniques and is applied even when mail passes through the Connection Management layers. As such, even email coming from “whitelisted” IP addresses, sender domains, sender email addresses or recipients are scanned for viruses and blocked if a virus is detected.

Use the **BASIC > Virus Checking** page in the web interface to enable or disable virus checking. If you enable Barracuda Real-Time Protection, the Barracuda Email Security Gateway will check unrecognized spam and virus fingerprints against the latest virus threats logged at Barracuda Central that have not yet been downloaded by the Barracuda Email Security Gateway Energize Updates. See the online help on the **BASIC > Virus Checking** page for more details about this setting.

Advanced Threat Protection

The subscription-based Advanced Threat Protection (ATP) service analyzes inbound email attachments in a separate, secured cloud environment, detecting new threats and determining whether to block such messages. ATP offers protection against advanced malware, zero-day exploits, and targeted attacks not detected by the Barracuda Email Security Gateway virus scanning features. ATP is available with the Cloud Protection Layer (CPL). For more information about CPL, see Cloud Protection Layer and How to Set Up Your Cloud Protection Layer.

Internal Virus Scanning For Your Microsoft Exchange Mail Server

The Barracuda Email Security Gateway offers an add-in that you can download from the web interface and install on your Microsoft Exchange Server to provide internal virus scanning within your network. The **Barracuda Exchange Antivirus Agent** runs as a Windows service on your 2003, 2007 or 2010 MS Exchange Server and works together with MS Exchange to scan internal mail traffic for viruses. Scanning is based on constantly updated virus signatures from the Barracuda Email Security Gateway.

Any time a new virus signature is released, the Barracuda Exchange Antivirus Agent will scan all internal mail traffic for that virus as well as mail previously stored on the server, depending on how you configure settings for the agent. See the **ADVANCED > Exchange Antivirus** page on the Barracuda Email Security Gateway web interface or see How to Get and Configure the Barracuda Exchange Antivirus Agent 6.0.x for instructions on downloading and configuring the add-in for your organization’s needs.

Attachment Block Notifications

You can enable or disable notification emails to senders of messages that are blocked due to file attachment content filters. Configure these notifications for inbound and outbound mail from the **ADVANCED > Bounce/NDR Settings** page in the web interface. From this page you can also enter custom message text to insert in the notifications. Attachment content filters are configured in the Attachment Content Filters section of the **BLOCK/ACCEPT > Content Filters** page.

Spam and Quarantine Notifications

Separate non-delivery notifications (NDR) can be configured to alert the sender when a message is blocked or quarantined due to spam scoring or policy (content filtering). See Non-Delivery Reports (NDRs) for more information.