How to Configure Avira Virus Scanning

https://campus.barracuda.com/doc/79463094/

To configure Avira virus scanning on the Barracuda CloudGen Firewall, import a legacy license and specify which threats the engine should scan for. You can define settings for the following features:

- **Archive Scanning** – Define the settings for compressed scanning archives.
- **Malware Detection** – In addition to detecting viruses, Avira can also detect malware, spyware, and bandwidth wasters. Specify which of these threats the engine should scan for.
- **Engine-Specific Options** – Import a legacy license, specify an email address to receive license notifications, and specify a quarantine directory for Avira.
- **HTTP Multimedia Streaming** – Because the Virus Scanner service downloads an entire file before scanning and delivering it, some audio or video streams cannot be accessed. Enable content streaming by disabling virus scanning for specific DNS domains.

Before You Begin

Before configuring Avira virus scanning, activate the Virus Scanner service. For more information, see How to Enable the Virus Scanner.

Configure Virus Scanning

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Virus-Scanner > Virus Scanner Settings**.
2. In the left menu, select **Avira**.
3. Set **Scan Archives** to **yes** to enable the archive scan.
4. In the **Avira Archive Scanning** section, define the following archive scanning settings:
   - **Max. Scan Size (MB)** – The maximum size for a file to be scanned. (default:1024). If an archive is scanned the largest uncompressed file in the archive may not exceed this limit. Set to 0 to disable this limit. Disabling the limit may result in high system load.
   - **Max. Nesting Depth** – The maximum nesting level for the archives (default: 20). If a limit is not required, enter 0 (zero).
   - **Max. Compression Ratio** – The maximum allowed decompression ratio for the archives (default: 150). Disabling the max compression rate limit removes protection from *ZIP bombs***.** *ZIP bombs* use very high compression ratios causing the virus scanner to run out of resources when it attempts to decompress it.
   - **Max. File Count** – The maximum number of files that can be stored in an archive (default: 10000). If a limit is not required, enter 0 (zero).
   - **Block Encrypted Archives** – To block encrypted archives, select **yes**.

     If the archive contains file types like .zip, .rar, .exe, .iso, .tar, .tgz, .cab, .msi, .btn,

etc. it is possible that one of these files is encrypted (virus scanner message: *Encrypted archives are blocked*). In this case, the virus scanner will block the whole archive. To disable blocking of encrypted archives, select *no*.

- **Block on Other Error** – As some services, such as Google Play updates, may deliver partial archives for updates to save bandwidth, set **Block on Other Error** to **No**. When enabled, the virus scanner blocks archives that cause errors while they are decompressing.
- **Block Unsupported Archives** – To block archives that cannot be decompressed because their formats are unsupported, select **yes**.

  The following archive types are supported: ZIP, ZIP-Sfx, ARJ, ARJ-Sfx, TAR, GZ, ZOO, UUEncode/XXEncode, TNEF, MIME, BinHex, MSCompress, MS CAB, LZH/LHA, LZH/LHA Sfx, RAR, RAR-Sfx, JAR, BZ2, ACE, ACESfx.

5. To configure malware detection, specify the types of malware that the engine should scan for in the **Avira Non-Virus Detection** section.
6. To configure engine-specific options, configure the following parameters in the **Avira Misc. Options** section:
   - **Legacy Avira license** – To import a legacy Avira license, click **Ex/Import** and select **Import from file**.
   - **Contact Email Address** – The email address to receive notifications on when the license will expire.
   - **Quarantine directory** – The path to the directory where infected files should be placed.

     The Virus Scanner service places files that are infected by a virus into the Quarantine directory. This directory is NOT cleaned up automatically. You must manually clean up the Quarantine directory.
7. Click **Send Changes** and **Activate**.

Configure HTTP Multimedia Streaming

To enable content streaming, disable virus scanning for specific DNS domains.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Virus-Scanner > Virus Scanner Settings**.
2. In the left menu, select **Content Scanning**.
3. Click **Lock**.
4. In the **Scan Exceptions** table, add an entry for each DNS domain that should not be scanned:
   1. Enter a name for the entry and click **OK**.
   2. In the **Allowed MIME types** table, add an entry for each MIME type that should not be scanned.

      To determine the MIME type for a file, enable the debug log and check the **cas** log files.
      To enable the debug log, go the **Virus Scanner Settings -Basic Setup** page. In the **Debug Log Level** field, enter *1*.
   3. In the **Domain** field, enter the domain name.

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

Avira Update

Updates of the Avira engine are done automatically. If a faulty Avira update is downloaded and activated, a rollback to the last working version is done. During this process, further updates will be blocked for 1 hour. A virscan/cas message will be created, stating "*Doing rollback. Disabling update for 60 min*."

To manually update the Avira pattern, complete the following steps:

1. Go to **CONTROL > Server**.
2. In the **Service Status** section, right-click the **virscan** service that should be updated with the most current pattern.
3. Click **Update Pattern** in the context menu.

If you must perform a manual rollback, create a file named */var/phion/run/virscan/dorollback*. During this process, any other updates will be blocked for 1 hour. The virscan/cas message will be created, stating "*Doing rollback. Disabling update for 60 min*."

After a successful update, Avira creates a backup that will be used for the next rollback. A log entry will be created, stating "*Creating backup for Rollback*".