How to Configure Avira Virus Scanning

Configure Avira virus scanning on the Barracuda NextGen Firewall F-Series. Import a legacy license and and specify which threats that the engine should scan for. To configure Avira virus scanning, you can define settings for the following features:

- **Archive Scanning** – Define the settings for compressed scanning archives.
- **Malware Detection** – In addition to viruses, Avira can also detect malware, spyware, or bandwidth wasters. Specify which of these threats that 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.

In this article:

Before you Begin

- Before configuring Avira virus scanning, activate the Virus Scanner service. For more information, see How to Enable the Virus Scanner.
- The Avira scan engine requires an additional license (file extension: *.KEY). This license file must be imported with the **Avira License Button**.

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 amount of data to be scanned for each file (default:1024). Specifying a maximum size prevents the virus scanner from being overloaded.

      If a maximum scan size is not entered or the limit set too high, this may result in severe damage to the system.
    - **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 compression ratio for the archives (default: 150).

      If you use a very high compression ratio, a small archive can use a lot of working memory when it is decompressed and overload the virus scanner. Such an archive is often called a "ZIP bomb."
    - **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** – To block archives that cause errors while they are decompressing, select **yes**.
- **Block Unsupported Archives** – To block archives that cannot be decompressed because their formats are unsupported, select **yes**.

The Barracuda NextGen Firewall F-Series uses the SAVAPI scan engine from AVIRA. This engine supports following archive types: 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. Default: `/phion0/run/virscan/blocked`

   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 was 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 which will be used for the next rollback. A log entry will be created, stating "*Creating backup for Rollback*".