How to Configure the FTP Gateway

https://campus.barracuda.com/doc/41116055/

The FTP Gateway service provides network users secure access to your company´s FTP server where they can perform actions such as up- and downloading files, etc., depending on their permissions. You can configure networking settings for the FTP Gateway and specify how the FTP Gateway service handles FTP commands and file transfers. You can also apply virus scanning and log settings according to your company´s requirements.

Before configuring the FTP Gateway service, make sure that you have properly created it. For more information, see How to Configure Services.

In this article:

Step 1. Configure Network Settings

To configure network settings for the FTP Gateway, complete the following steps:

1. Open the **FTP-GW Settings** page for the FTP Gateway service (**Config** > **Full Config** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **FTP-Gateway**).
2. Click **Lock**.
3. In the **Listening port** field, enter the TCP port that the gateway is listening on (default: *21*).
4. From the **NAT Policy** list, select the bind IP addresses. You can select:
   - **ProxyDyn** – The IP address is dynamically chosen according to the firewall routing tables.
   - **Server-First –** The first server IP is used for connections.
   - **Server-Second –** The second server IP is used for connections.
   - **Semi-Explicit –** The explicitly specified source IP address is used for connections. In the **Explicit NAT IP** field, enter the IP address.
   - **Explicit –** The explicitly specified listen and source IP address is used for connections. In the **Explicit NAT IP** field, enter the IP address.
5. If you select *Explicit* or *Semi-Explicit* from the **NAT Policy** list, enter the IP address in this field. This IP address is used by the FTP gateway on connection.
6. Proceed with the next step.

Step 2. Configure Data Transfer and FTP Commands

In the **FTP-GW Settings** node, you can configure how the FTP Gateway service handles FTP

commands and file transfer.

1. On the **Settings** page, select *yes* to **Deny active ftp-data transfer** if port commands should be denied and only passive data transfer should be allowed. When this setting is enabled, the server connects to the client.
2. To deny PASV commands and only allow active data transfer, select *yes* to **Deny passive ftp data-transfer**. When this setting is enabled, the client connects to the server.
3. To allow additional FTP commands that are not included in RFC 959 (such displaying the percentage of the file download in progress), select *no* to **Deny additional ftp- commands**.
4. To let the FTP Gateway service parse the protocol and check FTP commands for correctness, select *yes* to **FTP-command/protocol check**.
5. To configure buffer overflow protection, click **Set** or **Edit** next to **Buffer-overflow protection**. By default, all the buffer limits are enabled and set to *255*. You can enable and set the following limits:
   - **(Max.) Filename length –** The maximum length of file or directory names that are used with the following commands: RETR, STOR, SMNT, APPE, RNFR, RNTO, DELE, RMD, MKD, LIST, NLST, and STAT.
   - **(Max.) Username length –** The maximum length for usernames (USER).
   - **(Max.) Accountinfo length –** The maximum length for account information (ACCT).
   - **(Max.) Password length –** The maximum length for passwords (PASS).
   - **(Max.) String length –** The maximum length for strings that are used with the REST, SITE, and HELP commands.
   - **(Max.) Parameter length –** The maximum length for parameters that are used with all other FTP commands.
6. Proceed with the next step.

Step 3. Configure Virus Scanner Settings

In the **Virus Scanning** section, you can configure virus scanning of files that are retrieved via FTP. You can use a local virus scanner if configured on the Barracuda NG Firewall, such as Avira or ClamAV (requires a Barracuda NG Malware Protection license, see Virus Scanner), or you can use a remote virus scanner.

1. On the **Settings** page, select one of the following settings for **Use virus scanner** to enable virus scanning:
   - **local –** Enables the Barracuda NG Firewall virus scanner service.
   - **remote –** Enables a virus scanner service from a remote system.
     - **Scanner IP –** When using a remote virus scanner service, specify the IP address of the remote virus scanning system in this field.
2. Proceed with the next step.

Step 4. Configure Log Settings

In the **Logging** section, you can configure log settings for the FTP Gateway service. By default, all log settings are enabled.

1. On the **Settings** page, click **Edit** in the **Logging** section.
2. On the **Logging** page, configure the logging settings for FTP events by enabling/disabling logging of file downloads, uploads, appends, renaming, deleting, creation, etc.
3. Click **OK**.
4. Click **Send Changes** and **Activate**.