
How to Configure the Mail Gateway Service

<https://campus.barracuda.com/doc/46209183/>

Before configuring the Mail Gateway service, you must create it. For more information, see [How to Configure Services](#). You must also have a server installed on the Barracuda NextGen Firewall F-Series.

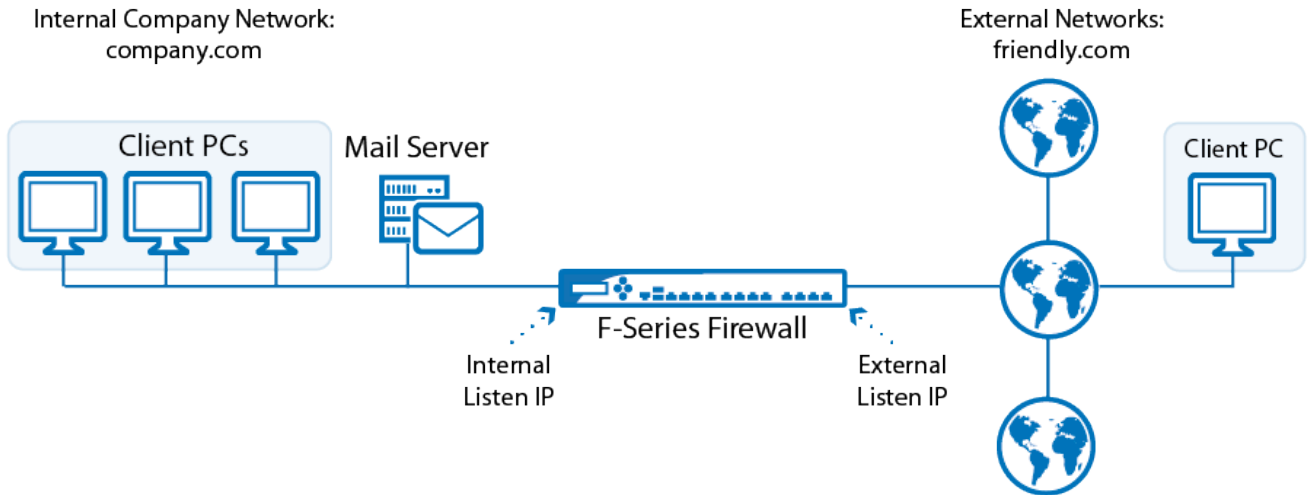
In this article:

Configure the Basic Mail Gateway Settings

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Mail-Gateway > Mail Gateway Settings**.
2. Click **Lock**.
3. On the **MailGW Settings - Basic Setup** page, configure the host, local domain, and global domain settings. For more information on these settings, see the following [Basic Mail Gateway Settings](#) section.
4. Click **Send Changes** and **Activate**.

Basic Mail Gateway Settings

For your server, configure more than one bind IP address that is reverse DNS resolvable. Otherwise, the mail gateway may not function correctly and the "Cannot bind to IP" error message displays in the system logs.



Host Configuration

The server uses the standard SMTP port 25 and the listen IP addresses to listen for requests. An inbound and outbound mail gateway must have at least two listening IP addresses. Inbound and outbound mail traffic are identified by the following listening IP types:

- **Internal** - Usually connects your LAN clients. If you are operating a mail server in your internal LAN, you can specify the mail gateway's internal listening IP address as a mail relaying address. If you do not have a dedicated mail server, clients may specify the gateway's internal listening IP address as an outgoing SMTP server address in the configuration of their email client programs.
- **External** - Connects your LAN to an external network.

The mail gateway determines the transportation direction by the email's incoming IP address. Mail rules are only interpretable when internal and external listening IPs are configured properly.

In the **Host Configuration** section, edit the following settings to specify your listen IP addresses and the email address of the postmaster:

Setting	Description
---------	-------------

<p>External Listen Address Internal Listen Address</p>	<p>In the External Listen Address and Internal Listen Address tables, add the listen IP addresses for the mail gateway. When adding a new IP address, specify the following settings:</p> <ul style="list-style-type: none"> • External Listen Address Internal Listen Address - The external and internal listen IP addresses (IPv4 or IPv6). From these lists, you can select <i>First-IP</i> or <i>Second-IP</i>. To explicitly specify the IP address, select the Other check box. Listen IP addresses must also be part of the server network configuration. If you enter a new IP address, you must also configure it as a virtual server address. • Greeting Name - The SMTP "helo / ehlo" greeting name that the mail server sends to the client after an SMTP connection has been established. Do not enter special characters, ciphers, ".", "-", and "_". For more information, see www.ietf.org/rfc/rfc2821.txt.
<p>Postmaster Mail-Address</p>	<p>The email address of the postmaster.</p>

Local Domain Settings

In this section, specify the mail server and trusted domains.

Setting	Description
<p>Internal Mail Server</p>	<p>The internal mail server. The mail gateway redirects incoming mail to this server. If you require another delivery policy setting, configure your mail gateway on the Extended Domains setup page.</p>
<p>My Domains List</p>	<p>In this table, add domains that are trusted by the mail gateway. The mail gateway will only accept mail relaying for these domains on its listening IP addresses. The security restrictions for these internal domains are identical to the formerly known Protection Profile. If you require more protection, configure your mail gateway on the Extended Domains setup page. When adding a domain, specify the following settings:</p> <ul style="list-style-type: none"> • My Domains List - The name of the internal trusted domain (for example, <i>barracuda.com</i>). You can enter wildcards to include multiple domains (for example, <i>barracuda.*</i>). However, entering a wildcard at the end of the domain name presents a potential security risk, as the top level domain might be interpreted as subdomain (for example, <i>barracuda.anyname.net</i>). Instead, create one entry per domain. • Include Subdomains - Specifies if the subdomains of the domain should also be trusted. If the subdomains should also be trusted, select yes. By default, <i>no</i> is selected and the subdomains are not trusted.

Global Domain Parameters

In this section, specify the database, authentication scheme, and group patterns for recipient verification. You can also specify email relay hosts.

Setting	Description
---------	-------------

Default Recipient DB	The relative path and name of the default database for recipient verification. If the configured server is unreachable or does not respond with the mail attribute, the email is not accepted.
Default Recipients	Click Ex/Import to export or import recipients in the default recipient database.
Default Recipients Lookup	<p>The authentication scheme used for an online mail recipient lookup in a meta directory for incoming mail. You can disable this setting, or you can select either <i>MSAD</i> or <i>LDAP</i>.</p> <p>The recipient email address is checked against the meta directory attribute named mail. If the meta directory server is unreachable or does not reply with the mail attribute, the email is not accepted.</p> <p>If you specify a Default Recipient DB and enable Default Recipients Lookup, the recipient email address must match both databases in order to be accepted.</p>
Recipients Lookup req. Groups	<p>The group patterns that must be matched by the recipient.</p> <p>If you selected <i>MSAD</i> or <i>LDAP</i> from the Default Recipients Lookup list, make sure that you also specify the group attribute in the authentication scheme configuration.</p>
Allow Relaying from	The hosts that are allowed to forward emails to be relayed on the internal listen IP address.

Figures

1. mail_gw_basic.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.