How to Configure Extended Domains

https://campus.barracuda.com/doc/73719390/To provide additional protection for your mail gateway, configure extended domain settings to create a complex and powerful rule feature that helps prevent fake email sender domains from abusing your mail gateway for relaying spam. Extended domain settings override local domain settings in the basic configurations for the Mail Gateway service.

Configure Extended Domain Settings

To configure the extended domain settings, complete the following steps:

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Mail-Gateway > Mail Gateway Settings**.
2. In the left menu, select **Extended Domain Setup**.
3. Click **Lock**.
4. From the **Enable Extended Domain Setup** list, select **yes**.
5. In the **Domains** table, add and configure domains. For more information about the settings that you can configure for each entry, see the following section.
6. In the **Default Internal MX** field, enter a default DNS-resolvable mail exchange server. Incoming mail will be redirected to this default MX. Usable for load balancing via DNS Round Robin.
7. In the **Default Internal Mail Server** table, add default internal mail servers to which incoming mail will be redirected. If you add multiple mail servers, the mail gateway subsequently tries each one until delivery is successful (for example, if the first default mail server is unreachable).
8. Click **Send Changes** and **Activate**.

Continue with How to Configure POP3 Scanning.

Domain Settings

Setting	Description
Additional Domain Pattern	If your trusted domain has additional patterns (for example, several top level domains such as *.com* or *.net*), you can add the additional patterns to the list. For the additional pattern, you can also enter wildcard characters such as * or ?.

<table>
<tr><td>Protection Profile</td><td>Protection profiles determine a mail domain's trust scope. Domains impersonating the highest trust level may only be forwarded by a gateway's internal listen IP address. Domains with the lowest trust level may be used to communicate outside the company LAN only. From the Protection Profile list, you can select one of the following rules to handle mail traffic:
<table>
<tr><th>Rule</th><th>Description</th><th>Allow as sender on internal</th><th>Allow as sender on external</th><th>Allow as recipient on internal</th><th>Allow as recipient on external</th></tr>
<tr><td>strictly_internal</td><td>Email senders using a domain defined as strictly internal are only accepted from within the company network at the mail gateway's internal listen IP address. This rule provides the highest protection level against fake email addresses, because emails cannot be forwarded through any external Internet-accessible mail relays.</td><td>pass</td><td>DENY</td><td>pass</td><td>pass</td></tr>
<tr><td>internal</td><td>Email senders using a domain defined as internal are accepted from within the company network at the mail gateway's internal listen IP address, as well from outside the company network at the mail gateway's external listen IP address. This rule is useful for mobile workers wishing to send emails with official company addresses when they are connected to the Internet via any ISP.</td><td>pass</td><td>pass</td><td>pass</td><td>pass</td></tr>
<tr><td>foreign</td><td>Email senders using a domain defined as foreign are accepted at both listening interfaces. Foreign domains can be defined if some of your clients want to use an external mail account (like a web mail account) company-wide and from the Internet. Because foreign domains are accepted as senders and recipients on both listening interfaces on the mail gateway, it makes sense to specify allowed clients explicitly (by selecting Explicit ACL from the Allow Relying from list). The foreign domain setting is only valid for these clients and not for the whole internal client network.</td><td>pass</td><td>pass</td><td>pass</td><td>DENY</td></tr>
<tr><td>strictly_foreign</td><td>Email senders using a domain defined as strictly foreign are only allowed at the mail gateway's external listening interface.</td><td>DENY</td><td>pass</td><td>pass</td><td>DENY</td></tr>
</table></td></tr>
<tr><td>Delivery Policy</td><td>Specifies how the mail gateway forwards incoming emails that are addressed to the specified recipient domain. You can select:
• MX – The mail gateway tries to resolve a DNS MX (mail exchange) record for the specific domain.
• Default_Internal – The mail gateway redirects incoming mail for a trusted domain to the respective default mail server that is listed in the Default Internal Mail Server table.
• Default_MX – The mail gateway redirects incoming mail for a trusted domain to an MX-resolvable domain that is specified in the Default Internal MX field.
• Explicit_Peer_IP – To explicitly specify IP addresses to which the mail gateway redirects matching incoming mail, select this option. In the following Delivery IPs table, enter the IP addresses.
• Explicit_MX_Domain – To explicitly specify the MX-resolvable domains to which the mail gateway redirects responsibility for email forwarding, select this option. Email distribution to the final recipients will then be handled by the other domains' mail servers. This option can be used when multiple internal mail servers are in use. In the following Delivery IPs table, enter the MX-resolvable domains.</td></tr>
<tr><td>Delivery IPs</td><td>If you selected either Explicit_Peer_IP or Explicit_MX_Domain from the Delivery Policy list, enter the delivery IP addresses or MX domains in this table.</td></tr>
<tr><td>Local Deliver IP</td><td>If you are using multiple listen IP addresses, add them to the Local Deliver IP table. One of the available IP addresses is selected as the binding IP address.</td></tr>
<tr><td>Allow Relaying from</td><td>Specifies which peers are allowed to use the specified domain as sender domains. You can select one of the following accept policies:
• Any_Peer – The specified domain can be used by any peer.
• Basic_Relaying_Setup – The specified domain can only be used by peers specified in the Allow Relaying from setting of the Basic Setup configuration.
• Explicit_ACL – The specified domain can be used by peers that are listed in the following ACL table.</td></tr>
<tr><td>ACL</td><td>If you selected Explicit_ACL from the ACL list, enter the IP addresses of the allowed peers in this table.</td></tr>
</table>

Recipient Lookup	Specifies if each mail recipient should be verified in a database. If the recipient cannot be found in the database, the mail is dropped. You can select any of the following options: • **Disabled** – No verification is performed. • **Default_DB** – Uses the database that is specified in the **Default Recipient DB** field of the **Global Domain Parameters** for the mail gateway. For more information on the **Default Recipient DB** field, see [How to Configure the Mail Gateway Service](). • **Explicit** – To explicitly specify the database that is used to verify mail recipients, select this option. If a large number of users must be verified, select this option and specify an individual recipient database for each domain.
Recipient DB	If you selected **Explicit** from the **Recipient Lookup** list, enter the relative path and name of the database to be used for recipient verification. A recipient database is always expected at `/var/phion/spool/mgw/*server*_*service*/` or a folder below it. You may enter the path and name of an existing database in this field. If the database does not yet exist, it will be created. For a database that has been or is expected to be created at `/var/phion/spool/mgw/*server*_*service*/`, enter *my_recipient.db* into this field. For a database that has been or is expected to be created at `/var/phion/spool/mgw/*server*_*service*/myfolder/,` enter *myfolder/my_recipient.db* into this field. If you wish to create a database in a subfolder of `/var/phion/spool/mgw/*server*_*service*/`, it will not be created automatically. If specified, the mail gateway is always going to query the recipient database before processing an email. Make sure that you immediately configure the contents of the recipients database after creation, because an empty recipient database will block all email traffic.
Recipients	To import recipients into the database that is specified in the **Recipient DB** field, click **Ex/Import** and then select the text file that contains the list of email addresses for the recipients. Each email address must be entered on its own separate line. If you must regularly update the recipient database, always use an up-to-date text file containing the total number of used email addresses. Only use the import routine when you have specified an existing database in the **Recipient DB** field. Do not use the import routine to update the recipient database with solitary users, because the contents of the recipient database are deleted before update. The contents of the recipient database are also not saved to the .par file when a backup of the system configuration is created. You must always keep the contents of your recipient database in a safe place in case it becomes necessary to restore your system configuration.
Default Recipients Lookup	Phibs scheme for lookup of a recipient email address in a meta-directory. You can only select either **MSAD** or **LDAP**.
Recipients Lookup req. Groups	In this table, add meta-directory group patterns to restrict allowed email addresses. Only persons which are assigned at least one of the here defined groups are allowed recipients. Patterns are allowed.