Domain Aliasing

https://campus.barracuda.com/doc/96022983/

> If you make setting changes, allow a few minutes for the changes to take effect.

You can alias a domain to another domain already added and configured on the **Domains > Domain Settings** page. When you make a domain an alias, it inherits the settings created on the parent domain.

> Users
>
> - When using domain aliasing, all users *must* be a member of the parent domain.
> - Barracuda Networks does NOT recommend using domain aliasing and user aliasing at the same time, especially if the mail server is doing recipient verification. This includes LDAP, AZURE, or manually-created user aliases.

Once you alias a domain to one or more domains already added and configured in the service, the number of configured domain aliases displays in the **Domains Manager** table on the **Domains** page. Click on the domain name to toggle the alias names. Click on a domain alias to view the inherited domain settings.

> **Important**
>
> When using aliases, keep the following rules in mind:
>
> - An aliased domain only uses the parent *policy* settings.
> - An aliased domain cannot access its per domain policy settings.
> - An aliased domain uses its own *configuration* settings.
> - If the aliased domain has per domain settings, these settings are ignored if the domain is an alias.
> - If you un-alias a domain, any per-domain settings will then work normally.
> - Un-alias child domains before deleting a parent domain.
> - Barracuda Networks does NOT recommend using domain aliasing and user aliasing at the same time, especially if the mail server is doing recipient verification. This includes LDAP, AZURE, or manually-created user aliases.

If you use domain aliasing and user aliasing at the same time, Email Gateway Defense will always check the *username@primary_domain* against the mail server to verify its validity. If the mail server is doing recipient verification and returns a "550 Invalid User" error when making the request, the error is returned to the sender and the mail will fail even though the address is in the user list.

If you use domain aliasing, all users in all aliased domains must exist in the primary domain. If they do

not exist and the mail server returns a "550 Invalid User" error for *username@primary_domain*, then mail to that user will fail even if the *username@alias_domain* is valid.

Use Case Examples

Example 1. Using Domain Aliasing

When domain aliasing is used, all users and domains use the settings of the *primary_domain*. All usernames (eg: bob.smith) must exist in the *primary_domain*.

For example, we have three different domains with the following users:

Domain-one.com (primary_domain)
bob.smith@Domain-one.com

Domain-two.com (alias of Domain-one.com)
bob.smith@Domain-two.com
bob.jones@Domain-two.com

Domain-three.com (alias_of Domain-one.com)
sam.jones@Domain-three.com
bob.smith@Domain-three.com

As a result, the following are allowed/blocked:

- bob.smith@Domain-one.com is allowed because bob.smith is in Domain-one.com.
- bob.smith@Domain-two.com is allowed because bob.smith is in Domain-one.com.
- bob.smith@Domain-three.com is allowed because bob.smith is in Domain-one.com.
- bob.jones@Domain-two.com is blocked because bob.jones is NOT in Domain-one.com.
- sam.jones@Domain-three.com is blocked because sam.jones is NOT in Domain-one.com.

NOTE : If the mail server is NOT doing recipient verification, then it will accept mail for all of the above users. This, however, leaves the domains open to Denial Of Service attacks. It is essential to create a valid user list in Email Gateway Defense and ensure unmanaged users are set to BLOCK.

Example 2. Using User Aliasing (manual, LDAP, or Azure)

This example assumes no domain aliasing is enabled.

Sample user list:

PARENT / ALIASES
bob.smith@Domain-one.com / bob.smith@Domain-two.com / bob.smith@Domain-three.com
bob.jones@Domain-two.com / bobbyJ@Domain-two.com
sam.jones@Domain-three.com / sjones@Domain-three.com

Email Gateway Defense will accept mail for all of the above users.