# How to Configure DNS Interception

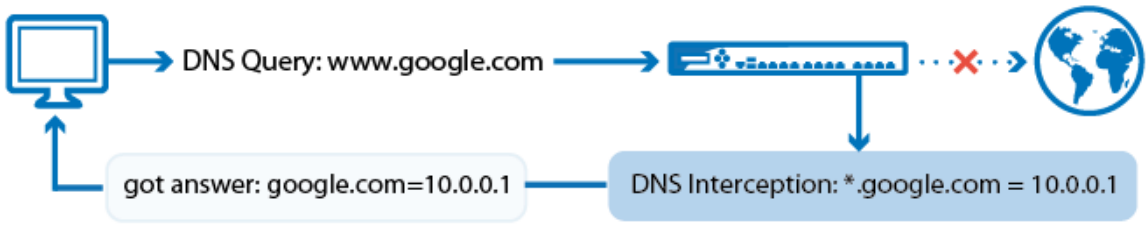
https://campus.barracuda.com/doc/46208959/

With the DNS Interception feature, you can configure a policy to redirect or block queries for specific domains. You can also configure a whitelist to create exceptions for queries to subdomains of the intercepted domains. Whitelisting always takes precedence over the DNS Interception policies. Follow the instructions in this article to add domains to the DNS Interception whitelist and policy. The DNS Interception feature requires a running Caching DNS.

**In this article:**

## DNS Interception Process

The DNS Interception feature handles DNS requests as follows:




1. A host behind the Barracuda NextGen Firewall F-Series sends a DNS query to the DNS server.
2. If the DNS request is for a domain that is in the DNS Interception whitelist, the request is not intercepted by the Barracuda NextGen Firewall F-Series, even if it is listed in the DNS Interception policy.
3. If the DNS request is for a domain that is listed in the DNS Interception policy, the Barracuda NextGen Firewall F-Series intercepts the request. According to the policy settings, the Barracuda NextGen Firewall F-Series then answers the request with one of the following actions:
   - **Blackhole (NXDOMAIN reply)** – Returns a non-existent domain message (NXDOMAIN) to the client indicating that the requested hostname does not exist.
   - **No Data** – Returns the information that, although the domain exists, there is no IP (no data) assigned to it.
   - **Return Other Domain (CNAME)** – Returns the hostname that is specified in the policy settings.
   - **Return IP Address** – Returns the IP address that is specified in the policy settings.

## Add Domains to the Whitelist

To add a domain to the DNS Interception whitelist:

1. Go to **CONFIGURATION > Configuration Tree > Box > Administrative Settings**.
2. From the left **Configuration** menu, select **DNS Interception**.
3. Click **Lock**.
4. In the **DNS Interception Exceptions** section, click the plus sign (**+**).
5. In the **Whitelisted Domains** window, enter the **Matched Domain** that must be allowed. For example, if you blocked the `google` domain but want to allow the Google mail service, enter `mail.google.com`.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

## Add Domains to the DNS Interception Policy

To add a domain to the DNS Interception policy:

1. Go to **CONFIGURATION > Configuration Tree > Box > Administrative Settings**.
2. From the left **Configuration** pane, select **DNS Interception**.
3. Click **Lock**.
4. In the **DNS Interception Policy** section, click the plus sign (**+**).
5. In the **Intercept Domains** window, specify the following settings:
   - **Matched Domain** – Enter the domain that must intercepted. You can use the asterisk (*****) or question mark (**?**) as wildcard characters. For example, if you want to intercept queries for the `www.google.com` domain, you can enter `*.google.com` or `*.google.?om`.
   - **Action** – Select how the intercepted queries are answered. Depending on which action you select, you might also have to specify these settings:
     - **Returned IP** – If you select the **Return IP Address** action, enter the IP address that is returned to the user.
     - **Returned Domain** – If you select the **Return Other Domain (CNAME)** action, enter the domain that the queries are redirected to.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

## Figures