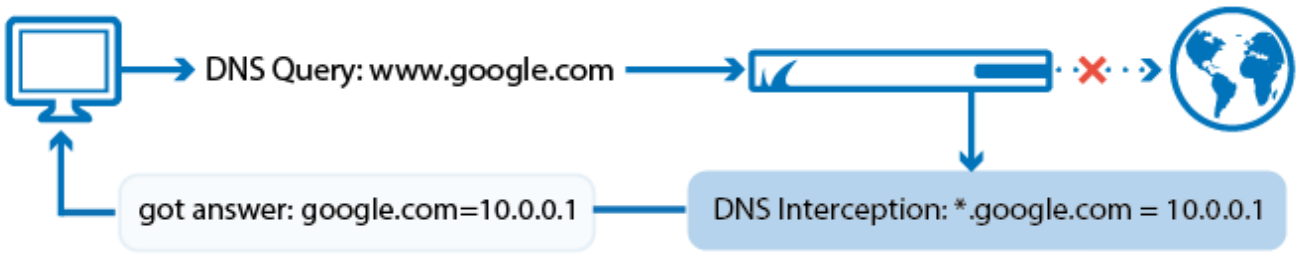
# How to Configure DNS Interception

The DNS Interception feature intercepts and replaces DNS queries matching the configured patterns. You can also whitelist domains. Whitelisted domains always take precedence over the DNS Interception policies. Subdomains of intercepted domains must be explicitly added. They are not intercepted automatically. You must run a caching DNS server to use DNS interception.

**DNS Interception Process**

The DNS Interception feature handles DNS requests as follows:

1. A host behind the firewall sends a DNS query to the DNS server.
2. If the DNS request is for a domain that is whitelisted, the request is forwarded.
3. If the DNS request is for a domain that is listed in the DNS Interception policy, the firewall sends one of the following replies depending on the configured policy:
   - **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.




**Before You Begin**

Enable and configure DNS Caching.

**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 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** to be allowed.
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 menu, 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 to be intercepted. E.g., `example.com` Wildcards or special characters are not allowed.
   - **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