How to Configure a Caching DNS Service

https://campus.barracuda.com/doc/98210585/

The caching DNS service is a box-level service that acts as a DNS proxy to speed up DNS queries. Do not run both the forwarding/caching DNS (bdns) service and a DNS service. The forwarding/caching DNS (bdns) configuration will collide with the DNS service. The caching DNS service listens on 127.0.0.1 and is accessed by the clients via an app redirect access rule in the forwarding ruleset. Depending on the rule, all DNS traffic can be routed over the DNS proxy, securing against misconfigured clients and servers attempting to use non-authorized external DNS servers.

In the DNS Query ACL table, add the IP range for the networks allowed to access the caching DNS server. Add 0.0.0.0/0 to allow everyone. Since the firewall services also use IP to communicate with the caching DNS service, these IP addresses must be added to the ACL to allow them to connect.
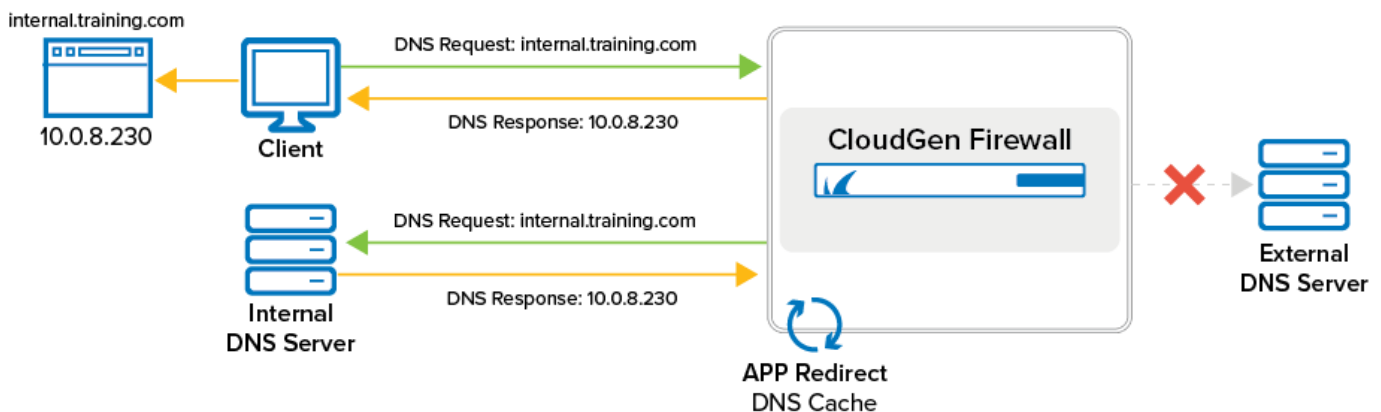
Step 1. Configure Caching DNS Settings

Do not install both the Forwarding/Caching DNS (bdns) service and a running DNS service. The Forwarding/Caching DNS (bdns) configuration will collide with the DNS service.
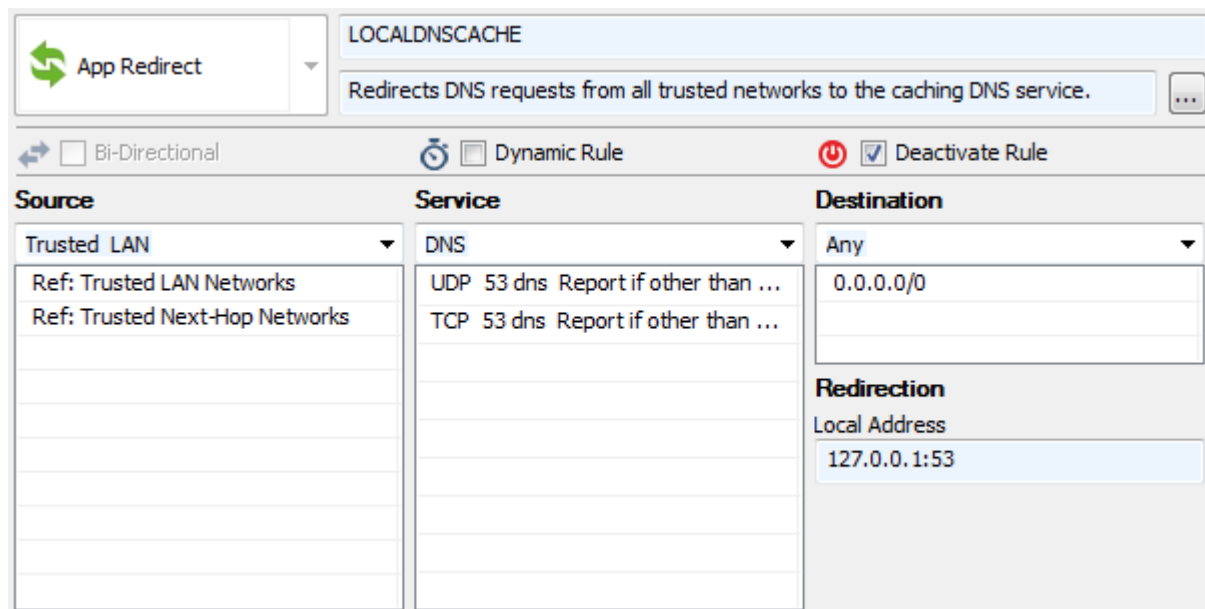
1. Go to **CONFIGURATION > Configuration Tree > Box > Administrative Settings** .
2. From the **Configuration Mode** menu, select **Switch to Advanced View**.
3. In the left menu, click **Caching DNS Service**.
4. Click **Lock**.
5. From the **Run Forwarding/Caching DNS** list, activate the local caching/forwarding DNS service.
6. From the **Run Secondary DNS** list, activate a local secondary DNS service if applicable. Configure the settings as described in How to Configure DNS Settings.
7. From the **Query Source Address** list, select which IP address to use as source address when querying the DNS or Primary DNS servers. You can select one of the following options:

- **Wildcard (default)** – IP selection is accounted for dynamically according to definitions in the routing table.
  - **VIP (managed firewalls only)** – Uses the firewall's VIP IP address.
  - **MIP** – Uses the system's management IP address, which is the **Main Box IP**.
  - **Other** – Select this check box to explicitly specify an IPv4 or IPv6 address.
8. In the **DNS Query ACL** table, add the single IPv4 / IPv6 addresses or netmasks that can access the DNS service via an App Redirect access rule.
9. Enable **Log DNS Queries** to log every DNS query.
10. Click **Send Changes** and **Activate**.

Step 2. Create an App Redirect Access Rule

Per default, access to the caching DNS service is handled by the LOCALDNSCACHE access rule. If this rule is not present on your firewall, add an **App Redirect** access rule to redirect DNS requests from the clients to the caching DNS service.

- **Action** – Select **App Redirect**.
- **Source** – Select the client network.
- **Service** – Select **DNS**.
- **Destination** – Select **Any**.
- **Redirection** – Enter the IP address and port the caching DNS service listens on.

Figures

1. dns_caching_83.png
2. DHCP_rule_01.png