How to Configure DNS Settings

https://campus.barracuda.com/doc/46209548/

The Barracuda NextGen Firewall F-Series can act as an authoritative DNS server, returning definitive answers to DNS queries about domain names installed in its configuration. With local DNS caching enabled, DNS queries will be forwarded to or cached from the specified DNS servers and DNS queries can be logged.

In this article:

Configure Basic DNS Settings

1. Go to **CONFIGURATION > Configuration Tree > Box > Administrative Settings**.
2. In the left menu, click **DNS Settings**.
3. From the **Configuration Mode** menu, select **Switch to Advanced View**.
4. Click **Lock**.
5. Enter the **Box DNS Domain** that the Barracuda NextGen Firewall F-Series belongs to.
6. In the **DNS Server IP** table, specify the DNS server's IPv4 and/or IPv6 addresses to be queried by the Barracuda NextGen Firewall F-Series.
7. Click **Send Changes** and **Activate**.

Configure Advanced DNS Settings

1. From the **Configuration Mode** menu, select **Switch to Advanced View**.
2. Click **Lock**.
3. In the **DNS Search Domains** table, add the names of the domains that should automatically be appended to an alias name when performing a DNS query. Separate multiple domains with spaces.
4. When using multiple DNS servers,
    1. Select if DNS queries should regularly rotate between the servers from the **DNS Query Rotation** list.
    2. Specify the **DNS Query Timeout** in seconds. When the timeout is exceeded, the next DNS server is queried.
5. To add local hosts,
    1. Click **+** in the **Known Hosts** section.
    2. Enter a **Name** for the local host and click **OK**.
    3. Enter the **Host IP** address.
    4. Enter Fully Qualified Domain Name (FQDN), with dots as namespace delimiter.

5. Add **Aliases** if applicable (no dots).
6. Click **OK**.

6. Click **Send Changes** and **Activate**.

The name and IPv4 addresses of local hosts are added to the system `/etc/hosts` file. By default, this file is consulted first for name resolution. It is useful to specify address/name pairs of locally known hosts for which no name resolution via DNS is available. The name and alias are used.

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 Slave DNS** list, activate a local slave DNS service if applicable. Configure the settings as described in **Configure Slave DNS Settings**.
7. From the **Query Source Address** list, select which IP address to use as source address when querying the DNS or Master 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 –** (For firewalls that are administered by a Barracuda NextGen Control Center) - Uses the system's Virtual Management 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 firewall rule.
9. Enable **Log DNS Queries** to log every DNS query.
10. Click **Send Changes** and **Activate**.

Configure Slave DNS Settings

When activated, configure the local slave DNS service. The slave DNS service gets its slave zone configurations from the entries in the **DNS Slave Zones** table and the configuration files from the servers specified in the **Default Master DNS** table. To allow zone transfers from the master DNS servers create an access rule to allow TCP 53 traffic.

1. Add the **Default Master DNS** servers that the slave can query for zone files. You can enter a single DNS server or a list of DNS servers (IPv4).
2. In the **DNS Slave Zones** table, click **+** to add an entry for the slave zone.
3. Enter the fully qualified domain name of the zone in the **Name** field and click **OK**. The **DNS Slave Zone** window opens.
4. Specify the DNS **Zone Type**. You can select:
   - **Forward (default) –** Provides IP addresses for known hostnames.
   - **Reverse –** Provides hostnames for known IP addresses.
     - Specify the network and netmask that the specified zone resides in in the **Reverse Lookup Net** and **Reverse Lookup Netmask** fields.
   - **Both –** Provides both.
     - Specify the network and netmask that the specified zone resides in in the **Reverse Lookup Net** and **Reverse Lookup Netmask** fields.
5. In the **DNS Master IP** table, add the DNS servers that the local slave DNS service queries for this zone. You can enter a single DNS server or a list of DNS servers (IPv4). If specified, this setting overrides the globally defined DNS Master IP address. If left empty, the field is ignored.
6. From the **Transfer Source Address** list, select which IPv4 address to use as source address when querying the master DNS servers. This IP address will override the globally defined value. You can select:
   - **Wildcard (default) –** IP address selection is accounted for dynamically according to definitions in the routing table.
   - **Query-Source –** Uses the IP address of the client that initiates the query.
   - **VIP –** (For firewalls that are administered by a Barracuda NextGen Control Center) Uses the system's virtual management IP address.
   - **MIP –** Uses the system's management IP address, which is the main box IP address.
   - **Other –** Select this check box to explicitly specify an IPv4 or IPv6 address.
7. Click **OK**.
8. Click **Send Changes** and **Activate**.