DNS

https://campus.barracuda.com/doc/73719068/

The Barracuda CloudGen Firewall can act as an authoritative DNS server, returning definitive answers to DNS queries about domain names specified in its configuration. The CloudGen Firewall DNS service specifies DNS zones such as hosts, domains, mail-exchangers etc. Each of the available zones can be defined as forward or reverse lookup zone. You can use the the same namespace internally and externally. You can return different IP addresses based on the source IP address of the DNS query (split DNS).

Configure the DNS Service

The DNS service provides the following configuration instances:

- **DNS Hint Lookup Zone** – The hint zone contains information on the initial set of root servers.
- **DNS Template Zone** – Use the template zone to build templates for the creation of new zones.
- **DNS Configuration** – This node contains the **Forward Lookup** configuration area. Sub-items of **Forward Lookup** are the already existing zones, including the hint and template zones.

For more information, see How to Configure the DNS Service.

DNS Zones

The DNS server stores information about parts of the domain name space in so-called zones. All names in a given zone share the same domain suffix. For example, if barracuda.com is the domain suffix, mail.barracuda.com and eng.barracuda.com are possible subdomains. These can all be served by one domain name server or some of the subdomains can be delegated to other domain name servers. Every domain or subdomain is in exactly one zone. Rather than make a distinction between a zone and a domain, the CloudGen Firewall offers the possibility to create a domain.

The CloudGen Firewall DNS configuration contains two predefined zones:

- **Zone 1: _template** – This zone contains the general template, which is used as model for all newly created zones. Here, you can create or modify settings for Start Of Authority (SOA), primary server, Name Server (NS), etc.
- **Zone 2: '.'**– The initial set of root-servers is defined using a hint zone. When the server starts up, it uses the hint zone file to find a root name server and get the most recent list of root name servers. The "." zone is short for this root zone and means any zone for which there is no locally defined zone (slave or master) or cached answer.

> Do NOT modify the root server settings in zone 2 ('.') unless you know exactly what you are doing.

When creating additional zones, you can configure the following zone types:

- **Master** – Every domain configuration change takes place on the master. From here, the information is propagated to the secondary servers. A master zone requires at least a Start of Authority (SOA) record and a Name Server (NS) record.
- **Slave** – A slave zone is a replica of a master zone. The masters list specifies one or more IP addresses that the slave contacts to update its copy of the zone. DNS slave zones do not require much configuration; just enter the IP addresses of the master server (or servers) and examine the security settings.
- **Forward** – A forward zone is used to direct all queries in it to other servers. The specification of options in such a zone will override any global options declared in the options statement. A forward zone does not need a transfer-source-IP.
- **Hint** – The initial set of root name servers is specified using a hint zone. When the server starts up, it uses the root hints to find a root name server and get the most recent list of root name servers. The CloudGen Firewall DNS server already has a hint zone (Zone ".") preconfigured, so normally there is no need to introduce another hint zone.

For information on how to configure DNS zones, see How to Configure DNS Zones.

DNS Interception

DNS Interception allows redirection or blocking of DNS queries for specific domains. This is achieved by applying policies. When creating a policy, you can also specify whitelisting for certain domains.

For more information, see How to Configure DNS Interception.

Debug Logging

You can also enable debug logging for the DNS service via the Command-Line Interface.

When you enable debug logging for DNS:

- The log file may increase, depending on the number of requests.
- With every change in the service configuration, the debug-logging is disabled.

For information on how to enable debug logging, see How to Configure DNS Zones.