How to Configure DNS Zones

https://campus.barracuda.com/doc/73719070/

Configure DNS zones for use with the DNS service of the Barracuda CloudGen Firewall. Modify the DNS zone template by adding hosts, subdomains, mail exchangers, etc. You can also create new DNS zones. When adding new zones, they will inherit all the settings specified in the template zone. The procedure for creating and modifying zone template settings is identical to the procedure for creating and editing settings in a new zone. Each zone can be defined as forward or reverse lookup zone.

Before You Begin

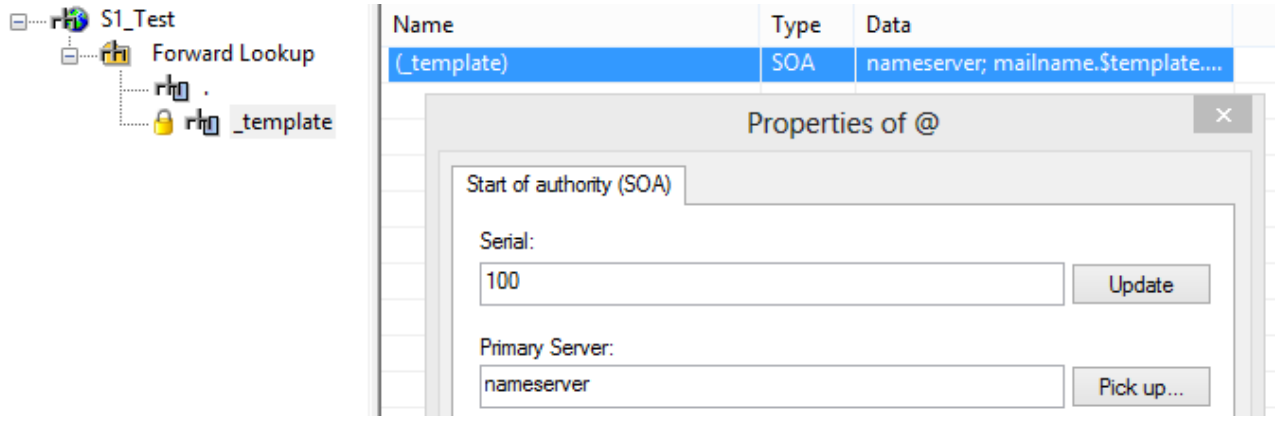
- Before starting the configuration, you must create a DNS service. For more information, see How to Configure Services.
- Make sure that you DNS server is properly configured. For more information, see How to Configure the DNS Service.

Configure a DNS Zone

Configure zone 1 (**_template**), by modifying the Start of Authority (SOA). Then, you can add and configure further zones that will inherit the template settings.

> Every DNS record has a Time to Live (TTL) value, which is the length of time that the DNS record can be cached. For most DNS records, two days is a typical and acceptable value. However, A records should have a very short TTL, such as 30 seconds.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > DNS-Service**.
2. Double-click **DNS Template Zone**.
3. Right-click the zone entry (e.g. **_template**) in the left navigation tree and select **Lock Zone**.
4. In the main table, double-click the zone entry (e.g. **_template**). The **Properties of** window opens.



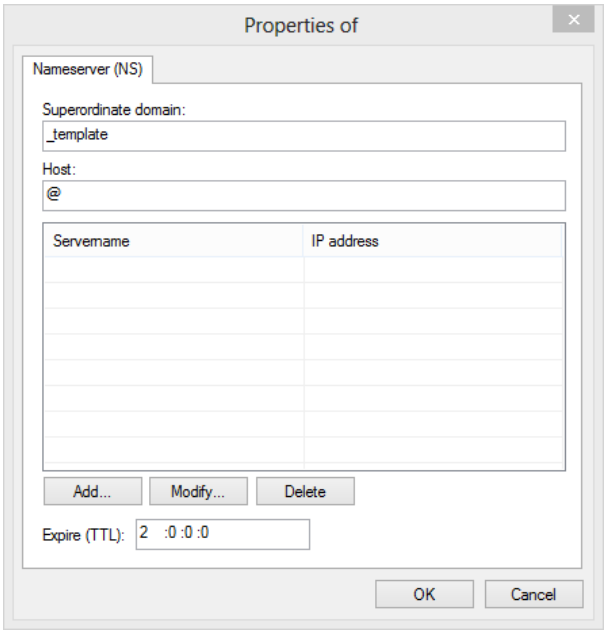
5. Define a **Serial** number. **Update** will increase the serial number by one.
   The serial number of the master has to be higher than the serial number saved on a slave, otherwise the slave will stop fetching information updates from its master.
6. In the **Primary Server** field, define the primary name server of the domain. Click **Pick up** to select already created entries.
7. In the **Responsible person** field, define a person responsible for this host/zone. The syntax that has to be used is username.domain (e.g. `ernestexample.test.org`.
8. Adjust the following settings according to your needs:
   - **Refresh after** – This interval tells the slave how often it has to check whether its data is up to date.
   - **Retry after** – When the slave fails to reach the master server after the refresh period (Refresh after), then it starts trying again after this set time interval.
   - **Expire after** – When the slave fails to contact the master server for the expire period, the slave expires its data. Expiring means that the slave stops giving out answers about the data because the data is too old to be useful.
   - **Minimum TTL** – (standard) This value sets the Time To Live of cached database entries of this zone (format:days:hours:minutes:seconds).
   - **Expire (TTL)** – This value sets the Time To Live of cached database entries of this zone until it is considered as expired.
9. Click **OK**.
10. Click **Send Changes** and **Activate**.

The Start of Authority (SOA) for the zone is now configured and you can add Name Server (NS), host, Mail-Exchanger and sub-domains, depending on your requirements. Each added entry generates an additional tab in the **Properties of** window for the SOA from where you can edit the settings.

Add a New Name Server

Introduce a Name Server (NS) to the zone.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > DNS-Service**.
2. Double-click **DNS Template Zone**.
3. Right-click the zone entry (e.g.: **_template**) in the left navigation tree and select **Lock Zone**.
4. Right-click in the table and select **New Name Server (NS)**.



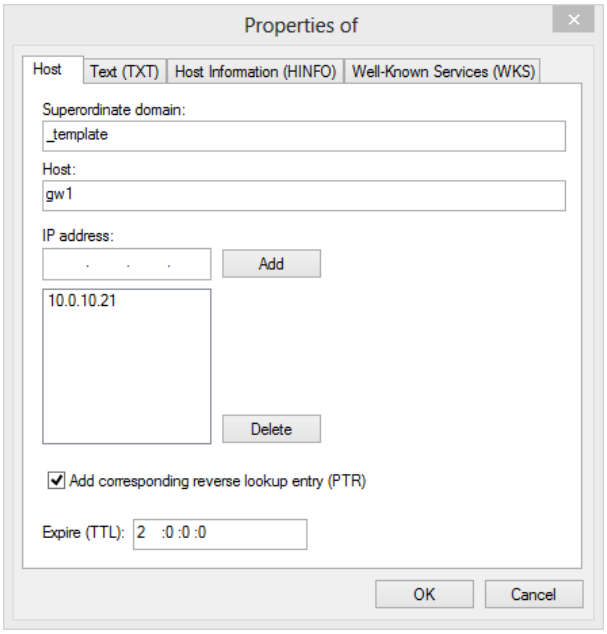
5. Click **Add**. The **Properties of** window opens.
6. Enter the **Servername**. To select existing entries, click **Pick up**.
7. Enter the IPv4 or IPv6 address of the name server and click **Add**.
8. In the **Expire (TTL)** field, set the globally defined length of life, future name server records are expected to have (format: days:hours:minutes:seconds), and click **OK**.
9. Click **OK**.
10. Click **Send Changes** and **Activate**.

An entry for the new name server is now displayed in a separate row within the main table and can be selected for further modification.

Add a New Host

Introduce a host to the zone (e.g.: **_template**.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > DNS-Service**.
2. Double-click **DNS Template Zone**.
3. Right-click the zone entry (e.g.:**_template**) in the left navigation tree and select **Lock Zone**.
4. Right-click in the table and select **New Host** .



5. In the **Host** field, enter the name of the host.
6. Enter the host IPv4 address and click **Add**.
7. Define the **Expire (TTL)** (format:days:hours:minutes:seconds).
8. Select **Add corresponding reverse lookup entry (PTR)** to automatically create a pointer record when creating the A-Record.

   Entries made in the individual tabs will be saved in separate rows of type A, TXT, HINFO and WKS within the main configuration window. Each configuration tab allows specification of the **Expire (TTL)** format:days:hours:minutes:seconds).
9. Open the **Text (TXT)** tab.
10. In the **Text** field, enter an optional description of the system to simplify maintenance of the DNS database.
11. Under the **Host Information (HINFO)** tab, add information on the hardware and operating system of the host if applicable.
12. Under the **Well-Known Services (WKS)** tab, specify the IPv4 address and the used protocol in the appropriate fields. The services must be entered in plain text and separated with blanks (e.g. `telnet ssh smtp ftp`.
13. Click **OK**.
14. Click **Send Changes** and **Activate**.

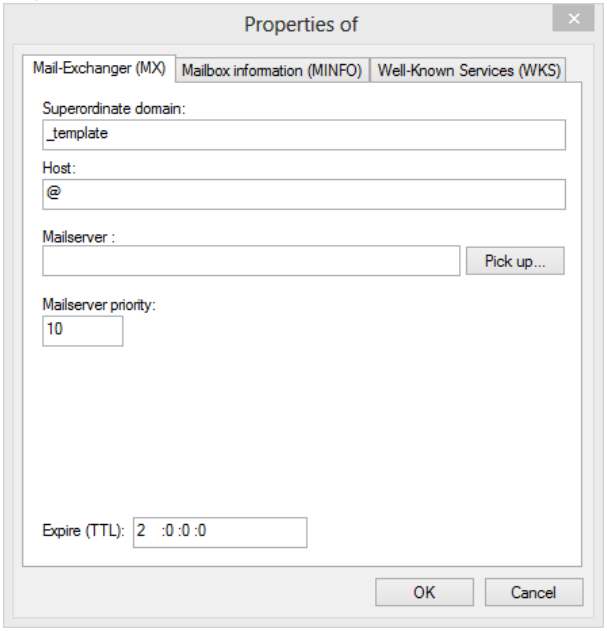
An entry for the new host is now displayed in a separate row within the main table and can be selected for further modification.

Add a New Mail Exchanger

Introduce a mail exchanger to handle mail traffic for the domain.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > DNS-Service**.
2. Double-click **DNS Template Zone**.

3. Right-click the zone entry **(_template)** in the left navigation tree and select **Lock Zone**.
4. Right-click in the table and select **New Mail-Exchanger**.



5. In the **Host** field, specify the following values according to your needs:
   - Mail-exchanger is responsible for `@domain.com any_text`
   - Mail-exchanger is responsible for `@any_text.domain.com`
6. Specify the **Mailserver** name. To select existing entries, click **Pick up**.
7. If required, set the values for **Mailserver priority** and **Expire (TTL)** (format: days:hours:minutes:seconds).
8. Open the **Mailbox information (MINFO)** tab.
9. Specify the name of the **Mailbox (MB)**. To select existing entries, click **Pick up**.
10. Specify the name of the **Error Mailbox (MB)** and **Expire (TTL)** (format:days:hours:minutes:seconds).
11. Under the **Well-Known Services** (WKS) tab, enter the IPv4 address and the used protocol in the appropriate fields.
12. Enter the services (e.g. `telnet ssh smtp ftp`. The services must be entered in plain text and separated with blanks.
13. Click **OK**.
14. Click **Send Changes** and **Activate**.

An entry for the mail exchanger is now displayed in a separate row within the main table and can be selected for further modification.

Add a New Domain

Introduce a new subdomain to the zone (e.g.: **_template**.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > DNS-Service**.
2. Double-click **DNS Template Zone**.

3. Right-click the zone entry **(_template)** in the left navigation tree and select **Lock Zone**.
4. Right-click in the table and select **New Domain**.
5. Enter a name for the new sub-domain and click **OK**.
   After clicking **OK** , the new subdomain displays in the DNS tree. Within the new sub-domain, you can perform the same operations as described above.
   > Completely set up new subdomains before clicking **Send Changes** and **Activate**. Otherwise, incompletely configured subdomains are deleted.
6. Click **Send Changes** and **Activate**.

Add New Others

There are several other objects you can add to your DNS configuration. These objects can be introduced by right clicking in the DNS config table and selecting **New Others**. The following objects can be added to the DNS configuration:

Parameter Overview

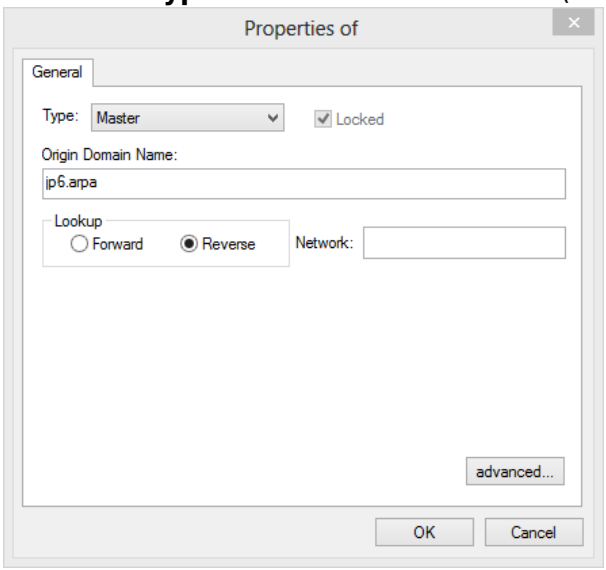
A	New host.
AAAA	IPv6 address.
AFSDB	AFSDB records specify the hosts that provide a style of distributed service advertised under this domain name. A subtype value (analogous to the preference value in the MX record) indicates which style of distributed service is provided with the given name. Subtype 1 indicates that the named host is an AFS® database server for the AFS cell of the given domain name. Subtype 2 indicates that the named host provides intra-cell name service for the DCE cell named by the given domain name.
CNAME	CNAME specifies an alias or nickname for the official or canonical name. An alias should be the only record associated with the alias; all other resource records should be associated with the canonical name and not with the alias. Any resource records that include a zone name as their value (for example, NS or MX) must list the canonical name, not the alias. This resource record is especially useful when changing machine names.
DNAME	DNAME specifies an alias for one or more subdomains of a domain. The effect of this is that the entire subtree of DNS identified by the domain name can be mapped onto the target domain.
HINFO	HINFO records contain host-specific data. They list the hardware and operating system that are running on the listed host. If you want to include a space in the machine name, you must quote the name. Host information is not specific to any address class, so ANY may be used for the address class. There should be one HINFO record for each host. For security reasons, many sites do not include the HINFO record, and no applications depend on this record.
ISDN	Representation of ISDN addresses.
MB	MB lists the machine where a user wants to receive mail. The "name" field is the user's login; the machine field denotes the machine to which mail is to be delivered. Mail box names should be unique to the zone.
MG	The mail group record (MG) lists members of a mail group.

MINFO	MINFO creates a mail group for a mailing list. This resource record is usually associated with a mail group, but it can be used with a mailbox record. The "name" specifies the name of the mailbox. The "requests" field is where mail such, as requests to be added to a mail group, should be sent. The "maintainer" is a mailbox that should receive error messages. This is particularly appropriate for mailing lists when errors in members' names should be reported to a person different to the sender.
MR	MR records lists aliases for a user. The "name" field lists the alias for the name listed in the fourth field, which should have a corresponding MB record.
MX	MX records specify a list of hosts that are configured to receive mail sent to this domain name. Every host that receives mail should have an MX record, since if one is not found at the time the mail is delivered, an MX value will be imputed with a cost of 0 and a destination of the host itself.
NAPTR	NAPTR records map between sets of URNs, URLs and plain domain names and suggest to clients what protocol should be used to talk to the mapped resource. For example NAPTR is used in SIP. The SIP URN for the US telephone number 1-800-555-1234 would be tel:+1-800-555-1234 and its domain name sipcalls.sip.com
NS	NS lists a name server responsible for a given zone. The first "name'' field lists the zone that is serviced by the listed name server. There should be one NS record for each name server of the zone, and every zone should have at least two name servers, preferably on separate networks.
PTR	PTR allows special names to point to some other location in the domain. The following example of a PTR record is used in setting up reverse pointers for the special in addr.arpa domain. This line is from the example mynet.rev file. In this record, the "name'' field is the network number of the host in reverse order. You only need to specify enough octets to make the name unique.
RP	RP identifies the name (or group name) of the responsible person(s) for a host. This information is useful in troubleshooting problems over the network.
RT	Route-through binding for hosts that do not have their own direct wide area network addresses (experimental).
SRV	Information on well known network services (replaces WKS).
TXT	A TXT record contains free-form textual data. The syntax of the text depends on the domain in which it appears; several systems use TXT records to encode user databases and other administrative data.
WKS	WKS records describe the well-known services supported by a particular protocol at a specified address. The list of services and port numbers comes from the list of services specified in /etc/services. There should be only one WKS record per protocol and address. Because the WKS record is not widely used throughout the Internet, applications should not rely on the existence of this record to recognize the presence or absence of a service. Instead, the application should simply attempt to use the service.
X25	Representation of X.25 network addresses (experimental).

Add a New Zone

Create an additional zone and configure the settings according to your requirements. This new zone will inherit the settings configured in the template zone. (Note that only template settings will be inherited that already existed before the zone was created.)

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > DNS-Service**.
2. Double-click **DNS Template Zone**.
3. Right-click your DNS server and select **Lock Server**.
4. Right-click your DNS server and select **Add New Zone**. The **Properties** of window opens.
5. Select the **Type** of the zone from the list. (For more information, see DNS)



6. Enter the **Origin Domain Name** you wish to create here (e.g. barracuda.com).
7. Define whether the zone should perform DNS Forward or Reverse lookup:
   - **Forward** – Provides IP addresses for known host names.
   - **Reverse** – Provides host names for known IP addresses (provided only for 8-bit networks, e.g. `213.47.10.0/24`).
8. When type **Slave** is selected, add the master IP addresses.
9. When type **Forward** is selected, add the forward IP addresses.
10. Clicking **advanced** and configure the following settings in the **Interface** section:
    - **notify** – Allows the administrator to select whether the DNS server should notify slave DNS servers about zone changes. If **explicit** is selected, enter the explicit IP address in the **also notify** field.
    - **also notify** – Here you may enter a list of IPv4 or IPv6 hosts that should be notified about zone changes although these machines are not registered slaves of the DNS server. Separate multiple entries with a semicolon and space (e.g. `10.0.0.53; 10.0.0.67; 192.168.0.10; 2001:db8:85a3:0:0:8a2e:370:73341`.
    - **transfer-source-ip** – (only available for type **Slave**) The IP address the slave has to use when contacting its master DNS server.

      Be sure to set the transfer-source-IP when configuring a slave zone, otherwise the slave zone will not be accepted by the DNS server.
11. In the **Security** section, configure detailed security options for the DNS service (These settings are very important for type **Master** and **Forward**).:

- **allow notify** – (only available for type **Slave**). Defines if the slave accepts notifications about updates from its master.
- **allow query** – Lists the IPv4 or IPv6 hosts that are allowed to query the DNS server. By default all hosts are allowed.
- **allow update** – Lists the hosts that are allowed to update the database of the DNS server.
- **allow transfer** – Lists the hosts that are allowed to fetch the DNS database from the DNS server.

12. Click **OK**.
13. Click **Send Changes** and **Activate**.

The new zone is now displayed in the left configuration tree. Clicking on this entry displays the zone details in the main table, from where you can add Name Servers, hosts, subdomains, mail exchangers, etc.

Troubleshooting

Add a New Start Of Authority (SOA)

In case you have deleted the standard template that is automatically inherited by newly generated zones and have created a new zone afterwards, you must create a new Start of Authority (SOA).

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > DNS-Service**.
2. Double-click **DNS Template Zone**.
3. Right-click your DNS server and select **Lock Server**.
4. Locate the newly created domain lacking an **SOA** record in the tree view.
5. Right-click in the table and select **Add a New Start of Authority (SOA)**, or, if the SOA record already exists, double-click an existing entry with type NS or SOA and select the **Start of Authority (SOA)** tab.
6. Specify the settings as described in **Configure DNS Zones** .
7. Click **Send Changes** and **Activate**.

In order to function, the reverse zone as described in **Define Reverse Lookup Zones** must have already been created.

Enable Debug Logging

To enable debug logging for the DNS service, edit its named.conf file. Then restart the service.

1. Edit the named.conf file.

```
vi /opt/phion/config/active/servers/<servername>/services/<dns-
servicename>/named.conf
```

2. Replace these lines:

```
logging {
category "default" { "default_syslog"; };
};
```

3. with the following lines:

```
logging {
category "default" { "default_syslog"; };
category "general" { "default_syslog"; };
category "database" { "default_syslog"; };
category "security" { "default_syslog"; };
category "config" { "default_syslog"; };
category "resolver" { "default_syslog"; };
category "xfer-in" { "default_syslog"; };
category "xfer-out" { "default_syslog"; };
category "notify" { "default_syslog"; };
category "client" { "default_syslog"; };
category "unmatched" { "default_syslog"; };
category "network" { "default_syslog"; };
category "update" { "default_syslog"; };
category "queries" { "default_syslog"; };
category "dispatch" { "default_syslog"; };
category "dnssec" { "default_syslog"; };
category "lame-servers" { "default_syslog"; };
};
```

4. Restart the DNS service. Enter:

```
          phionctrl module restart dns
```

Figures

1. dns_prop.png
2. new_ns.png
3. host_config.png
4. mailex.png
5. rev_zone.png