DNS

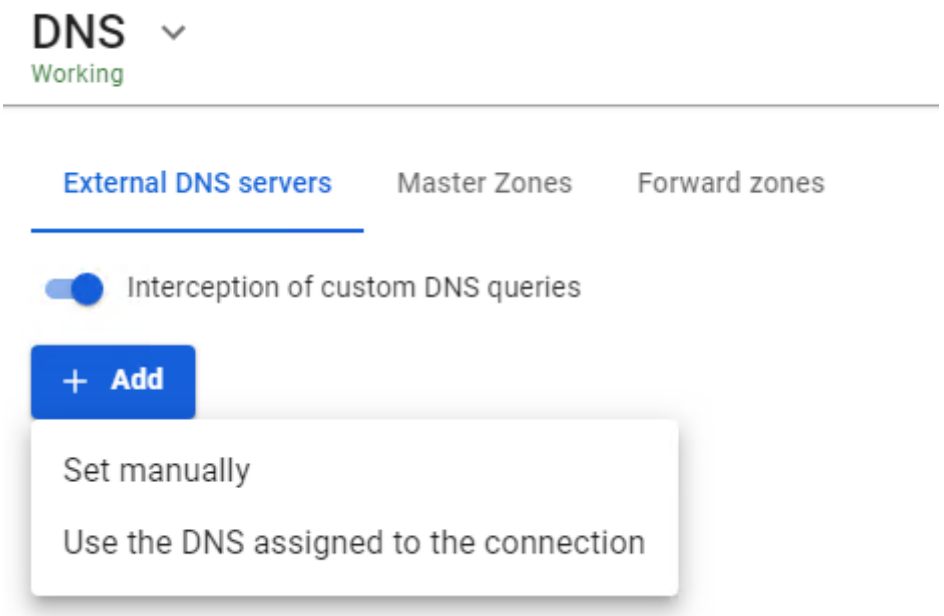
A DNS server converts human-readable server names into IP addresses. SafeUTM includes a DNS server that does not require additional configuration in most cases.

DNS service on the SafeUTM server is configured in **Services -> DNS**. The service allows you to specify DNS servers in external networks through which domain names will be resolved (**External DNS servers** tab) requested from LANs. It is possible to specify third-party DNS servers (in local or external networks relative to UTM) with an indication of the specific DNS zones that these servers serve (**Forward zones** tab). The listed DNS server features can be used simultaneously.
Also, in the **Master Zones** tab, you can configure a full-featured DNS server that resolves names to IP addresses of network devices in the LAN.

External DNS servers

For normal operation of name resolution on the Internet via SafeUTM, it is not necessary to specify DNS servers in this section. If DNS servers are not specified, the server will resolve names on the Internet using **root DNS servers** on the Internet. This configuration will not work if the upstream router intercepts DNS requests. In this case, we recommend:

- Specifying DNS servers manually (click **Add -> Set manually** and specify the IP address of the DNS server);
- Using **Use the DNS assigned to the connection** option, specifying the required connection;



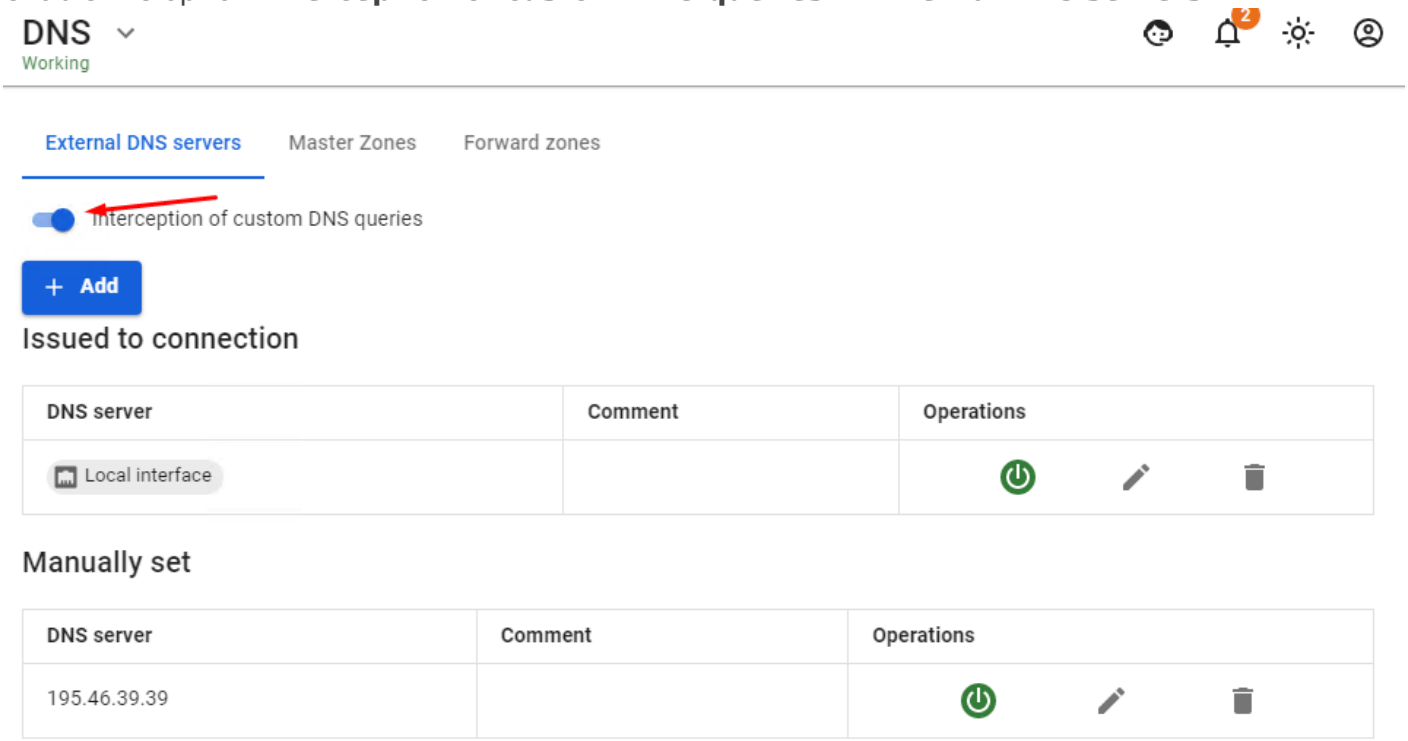
Recommendations:

1. The DNS server embedded in SafeUTM is a caching one. It is highly recommended to use it as a DNS server for your local network.
2. Do not enter `8.8.8.8`, `1.1.1.1` or similar ones unless absolutely necessary. SafeUTM will handle the resolution on its own without any intermediaries.
3. Do not specify a DNS server from your internal Active Directory server, even if it can resolve domain names on the Internet on its own. This, as a rule, is meaningless. When integrated with AD, SafeUTM will automatically configure everything necessary (forward zone) for AD operation and resolve the internal names of your domain. To resolve some special zones not related to AD, create a forward zone.
4. Do not use DNS provided by your Internet provider unless absolutely necessary (do not specify either manually or through the interface selection option). SafeUTM will automatically configure everything you need to connect to PPTP/L2TP via a domain name. In practice, provider DNS exceeds TTL, and also takes a long time to respond. The only case when this is needed is the provider's special internal domain zones. In this case, create a forward zone.
5. You can specify DNS servers engaged in filtering if necessary (SafeDNS).
6. If all DNS servers are disabled or deleted, DNS will work fine - SafeUTM will resolve the names on its own.
7. If the ISP or upstream device is intercepting DNS requests, then using the standard configuration with root servers is not possible, and you must either set the servers manually or use the DNS servers assigned to the connection.

Interception of DNS Requests

> Enabling interception of DNS requests blocks the use of DNS-over-TLS (DoT), DNS-over-QUIC (DoQ), and DNS-over-HTTPS (DoH).

The product has the ability to intercept requests made through third-party DNS servers specified by users on workstations (in order to bypass locks, or due to incorrect configuration). To do this, enable the option **Interception of custom DNS queries** in **External DNS servers**.



The option is enabled globally for all hosts in the LAN that access the Internet via SafeUTM. This allows you to avoid possible substitution of the resource address when resolving its domain in order to bypass resource locks. Also, interception of all users' DNS requests will allow you to control the process of resolving domain names on the Internet exclusively by means of UTM.

The intercepted request will be redirected to the UTM DNS server, and the response will be generated by the UTM DNS server, not the original DNS server. Interception of DNS requests also blocks the possibility of tunneling through DNS (DNS tunneling). Enabling the interception of custom DNS requests also blocks the use of DNS-over-TLS.

You can use the following third-party DNS servers for additional traffic filtering:

- SafeDNS `195.46.39.39`, `195.46.39.40`
- Google DNS `8.8.8.8` , `8.8.4.4`
- Open DNS `208.67.222.222` , `208.67.220.220` , `208.67.222.220` , `208.67.220.222`
- Cloudflare DNS `1.1.1.1` , `1.0.0.1`

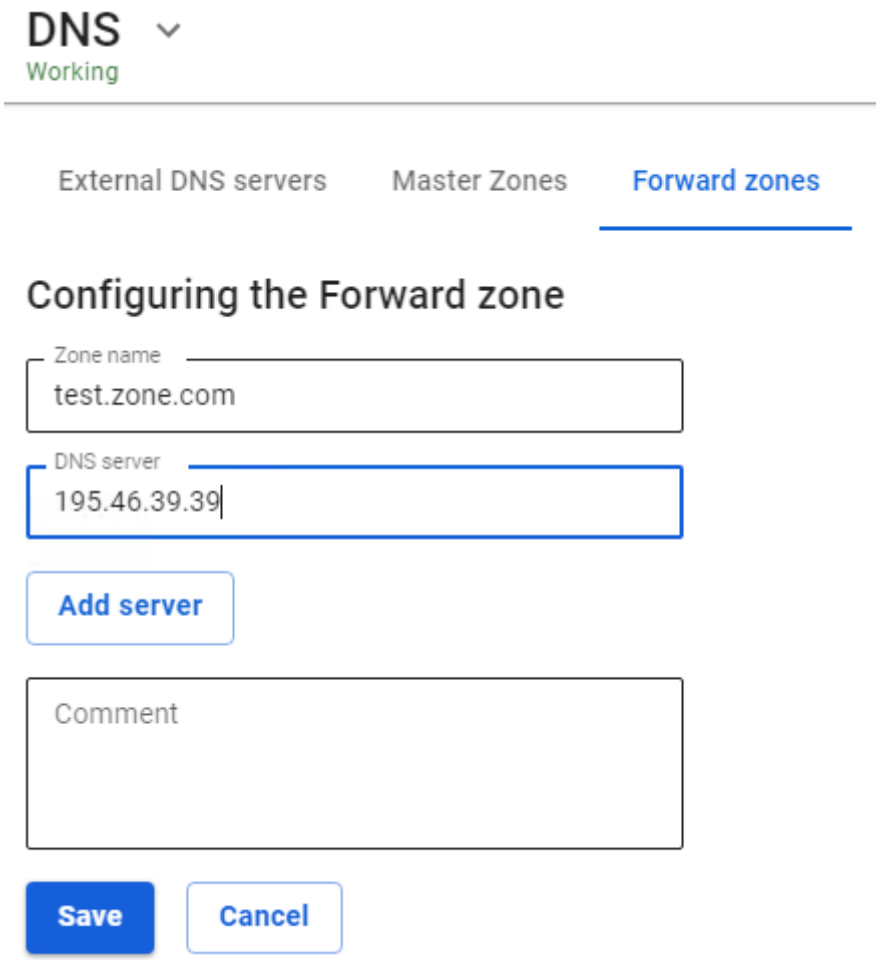
DNS Server Management

You can turn off/on, edit or delete DNS servers in column **Operations**.

Forward zones

In this section, you can explicitly specify a DNS server to resolve the names of a specific DNS zone. By specifying the DNS server available on the network and the zone it serves, SafeUTM network clients are able to access the resources in this zone by the names of the domain it serves. For example, the IT department of an enterprise provides resources for employees in the zone `in.metacortex.com` under names `realm1.in.metacortex.com` , `sandbox.metacortex.com` and uses DNS server 10.10.10.10 for this.

To be able to access these resources by domain names, specify the provider's forward zone as an isp and then specify DNS server 10.10.10.10 in the Forward zone addition form.



Master zones

Master zones with configured DNS records will allow you to use UTM as a name server inside your network infrastructure to access the IP addresses of hosts on the network by domain names.

The DNS server in SafeUTM is not accessible from outside for security reasons. To support external DNS zones, we recommend using third-party DNS hostings.

Do not use master zones to block access to sites, there are other **means** in SafeUTM to do this. Blocking in this way works inefficiently and does not allow you to selectively prohibit access by users or subnets. It also leads to problems with excessive caching.

The records format for setting up the master zone corresponds to the records format of the BIND DNS server.

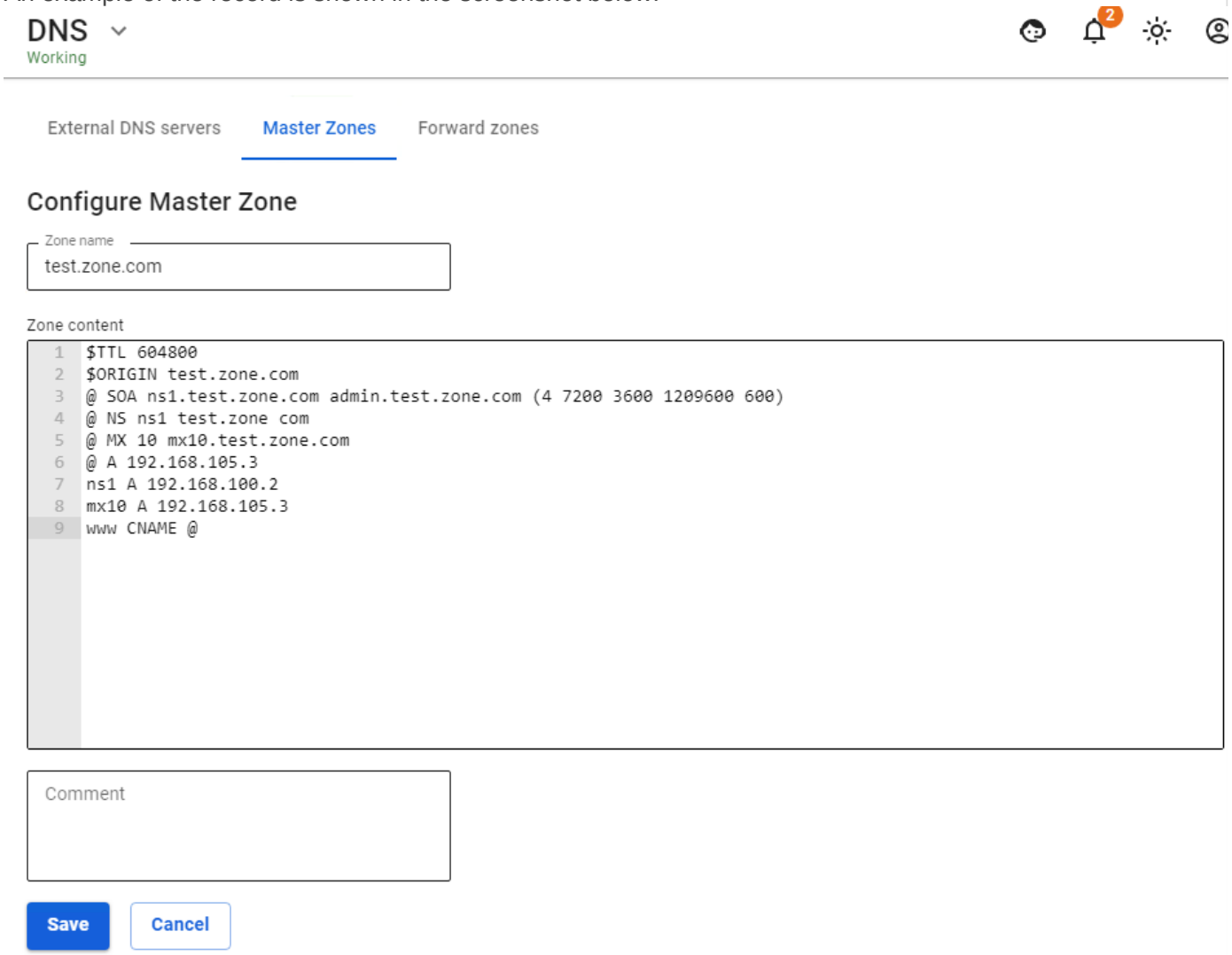
Description of record parameters:

- **$TTL** – determines the caching time of positive responses (response in the form of the found IP address). The time is set in seconds or using abbreviations: m — minutes, h — hours, d — days, and w — weeks.
- **$ORIGIN** – defines the current domain name. The current value of $ORIGIN replaces the @ symbol in the record. The current value of $ORIGIN is appended to any name that does not end with a "dot".
- **$SOA** – describes the basic/initial settings of the zone, or defines *this server's area of responsibility.* There should be only one SOA record for each zone and it should be the first one. The $SOA entry specifies the primary NS for the domain and the contact person's e-mail, and then in parentheses:
  - **Serial** – The serial number of the zone file. When changing data, you need to change the serial number, which updates the zone on all servers. Use the following format: YYYYMMDDnn (year, month, day, nn is the sequential number of the change for the day). If you are already making changes to the zone file for the second time in a day, specify "nn" equal to 01, the third one will be 02, etc.
  - **Refresh** – specifies how often secondary servers should poll the primary one to find out if the zone's serial number has increased.
  - **Retry** – waiting time after a failed polling attempt.
  - **Expiry** – the maximum time during which the secondary server can use the information about the received zone.
  - **TTL** – the minimum time during which data remains in the secondary server's cache.

- **$SRV** – indicates the servers providing operation of certain services in this domain (for example, Jabber and Active Directory).
- **$NS** –the DNS server servicing this domain. A minimum of two of them are needed, and they should be located in different subnets, or better yet, in different places geographically. Specify the primary server first.
- **$PTR** – displays the IP address in the domain name.
- **$MX** – describes mail gateways (usually one) to which all mail from this domain will be delivered. Priority is set for each gateway (by default it is 10). Usually, the domain name of the mail gateway looks like this: *example.com*. There must be corresponding A-records for MX hosts.
- **$A** – map the hostname (domain name) to an IPv4 address. One A**-record** must be made for each network interface of the machine.
- **$AAAA** – similar to record A, but for IPv6.
- **$CNAME** – displays the alias to the real name (for redirection to another name).

All resource records can be found **here**.

An example of the record is shown in the screenshot below:



A few examples of records in the master zone:

1. Zone name: ms

```
$ORIGIN ms.
$TTL 600
@ SOA ns1.ms. administrator.ms. ( 4 7200 3600 1209600 600 )
@ NS ns1.ms.
@ MX 10 mx10.ms.
@ A 192.168.0.250
ns1 A 192.168.0.250
mx10 A 192.168.0.250
www CNAME @
```

2. Zone name: example.com

```
$TTL 86400
@ SOA localhost. root.localhost. ( 991079290 28800 14400 3600000 86400 )
@ NS my-dns-server.example.com.
my-dns-server A 1.2.3.4
```

Revision #8
Created 2022-08-27 13:19:24 UTC by Val Redman
Updated 2022-10-13 15:29:12 UTC by Val Redman