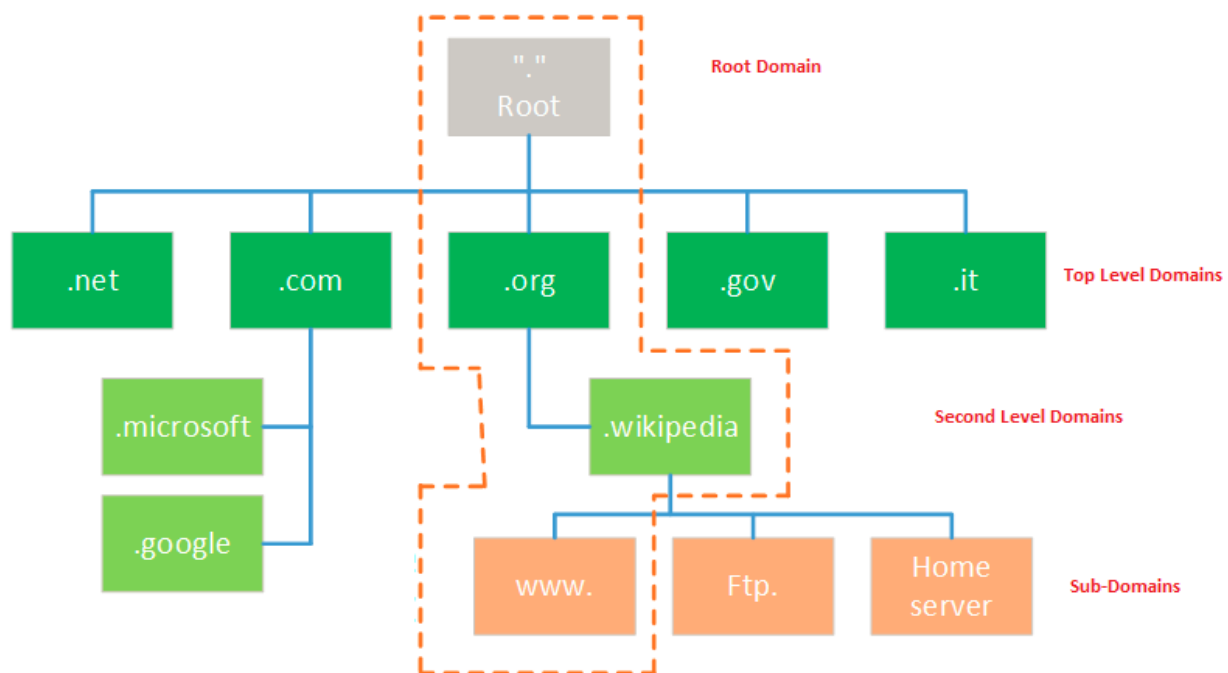


## DNS Server:

- o DNS Stands for Domain Name System or Domain Name Server.
- o DNS is a large database, which resides on various computers in world.
- o DNS contains names & IP addresses of hosts on Internet & various domains.
- o DNS servers match domain names to their associated IP addresses.
- o The Domain Name Systems (DNS) is the phonebook of the Internet.
- o DNS convert IP Address to domain name & domain name into IP address.
- o DNS names are assigned through the Internet Registries by the IANA.
- o There are 13 root name servers from [a.root-server.net](http://a.root-server.net) to [m.root-server.net](http://m.root-server.net).
- o 13 DNS root name servers can be check on this link <http://www.root-servers.org>.
- o DNS primarily uses User Datagram Protocol on port number 53 to serve requests.
- o Domain name system of the Internet works in an inverted tree structure.
- o The TLD is the letters immediately following the final dot in an Internet address.
- o In Internet address, <http://mail.google.com>, **com** is the top-level domain name.
- o **Google** is the second-level domain name and **mail** is a subdomain name.
- o Altogether, <http://mail.google.com> is fully qualified domain name (FQDN).
- o Addition of HTTP:// makes a fully qualified domain name FQDN complete URL.



### Root Servers

A B C D E F G H I J K L M

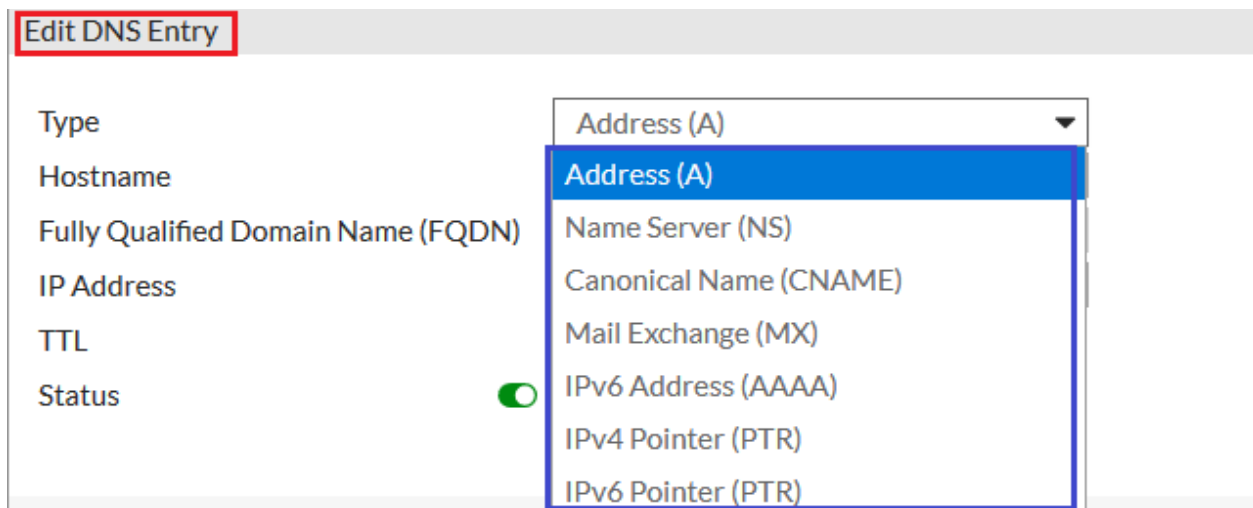
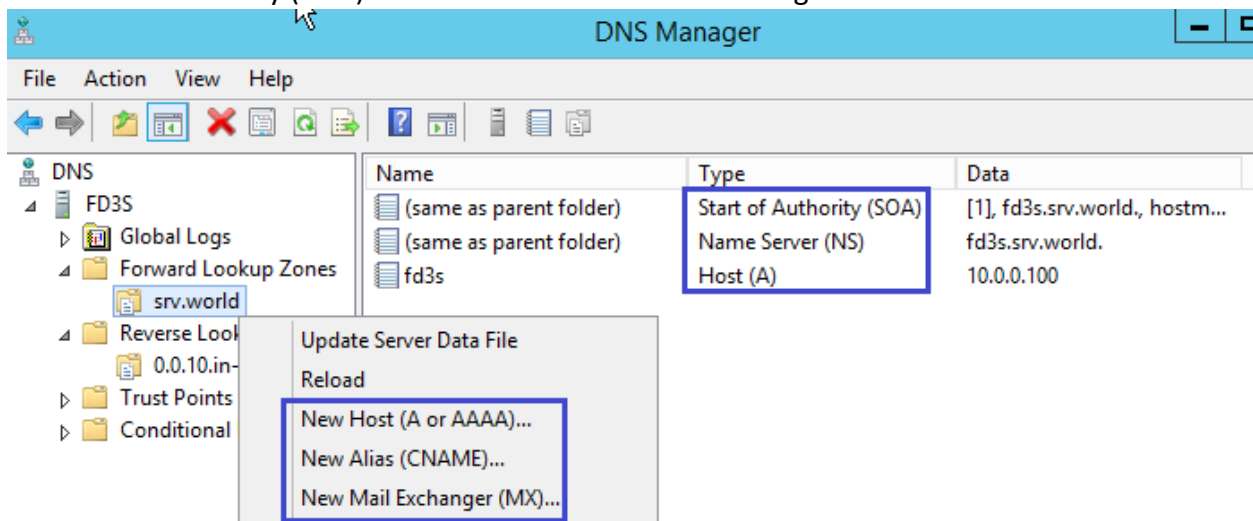
Operator: Verisign, Inc. [Homepage](#) [Statistics](#) [Contact Email](#)

Locations: Sites: 28

- Amsterdam, NL
- Ashburn, US
- Atlanta, US
- Chicago, US
- Frankfurt, DE
- Hong Kong, HK
- London, GB
- Los Angeles, US
- Los Angeles
- Miami, US
- New York, US
- Paris, FR
- Plano, US
- Plano, US
- San Jose, US
- Seattle, US
- Tokyo, JP

## DNS Records:

- o There are several different types of resource records used by DNS.
- o The **A** record specifies IP address Internet Protocol (IPv4) for given host.
- o **A**, records are used for conversion of domain names to correspond IP addresses.
- o The **AAAA** record specifies Internet Protocol (IPv6) address for given host name.
- o Domain name system also allows us to name single device but give it multiple names.
- o Give it nickname or secondary name it has called Canonical Name record, or **CNAME**.
- o **CNAME** records in the DNS Server are used for creating aliases of domain names.
- o **CNAME** records are truly useful when want to alias domain to an external domain.
- o The **MX** resource record specifies a Mail Exchange server for a DNS domain name.
- o SMTP use MX resource record to route emails to proper hosts uses the information.
- o PTR stand for Pointer Record, this is opposite of an address record (A or AAAA).
- o An address record took a name and provided you with an IP address IPV4 or IPV6.
- o A Pointer record in DNS Server took IP address and come up with a name.
- o Name Server (**NS**) The NS record specifies who the DNS servers are for the zone.
- o Start of Authority (**SOA**) The SOA record stores the settings for the DNS zone.



## DNS Configuration:

Go to **Network > DNS** by default, using Fortinet's FortiGuard servers are select.

The screenshot shows the FortiGate DNS Settings page. The left sidebar has 'Network' and 'DNS' highlighted. The main content area shows 'DNS Settings' with a 'DNS servers' section where 'Use FortiGuard Servers' is selected. Below this, the 'Primary DNS server' is 96.45.45.45 and the 'Secondary DNS server' is 96.45.46.46, both marked as 'Unreachable'. The 'Local domain name' field is empty. Below the DNS servers section is the 'DNS Protocols' section with 'DNS (UDP/53)' checked, 'TLS (TCP/853)' unchecked, and 'HTTPS (TCP/443)' unchecked. At the bottom is the 'Dynamically Obtained DNS Servers' table:

Interface	DNS Server	Response Time
MGMT (port1)	192.168.114.2	730 ms
WAN (port2)	8.8.8.8	Unreachable

It is possible to specify using different DNS server, click on **Specify** and enter in primary / secondary DNS servers. In Primary DNS Server, type the IP address of the **primary DNS server 8.8.8.8**. In Secondary DNS Server, type the IP address of the **secondary DNS server 8.8.4.4**. Click **Apply** button to save the changes.

The screenshot shows the FortiGate DNS Settings page with 'Specify' selected. The 'Primary DNS server' is 8.8.8.8 and the 'Secondary DNS server' is 8.8.4.4, both marked as 'Unreachable'. The 'Local domain name' field is 'test.local'. The 'DNS servers' section has 'Specify' selected. The 'DNS Protocols' section is the same as in the previous screenshot.

In the **Local Domain Name** field, enter the first domain such as test. local etc. Click the **+** to add more domains You can enter up to **eight** domains names.




## DNS Over TLS:

DNS over TLS (DoT) is a security protocol for encrypting and encapsulating DNS queries and responses over the TLS protocol. DoT increases user privacy and security by preventing eavesdropping and manipulation of DNS data via man-in-the-middle attacks. Disabling DoT and DoH is recommended when they are not supported by the DNS servers.



## DNS Over HTTPS:

DNS over HTTPS (DoH) provides a method of performing DNS resolution over a secure HTTPS connection. DoT and DoH are supported in explicit mode where the FortiGate acts as an explicit DNS server that listens for DoT and DoH requests. Local-out DNS traffic over TLS and HTTPS is also supported. Before enabling DoT or DoH, ensure that they are supported by DNS servers.

### DNS Protocols

DNS (UDP/53)		<input checked="" type="checkbox"/>
TLS (TCP/853)		<input type="checkbox"/>
HTTPS (TCP/443)		<input type="checkbox"/>

### Dynamically Obtained DNS Servers

Interface	DNS Server	
 MGMT (port1)	192.168.114.2	10 ms
 WAN (port2)	8.8.8.8	Unreachable

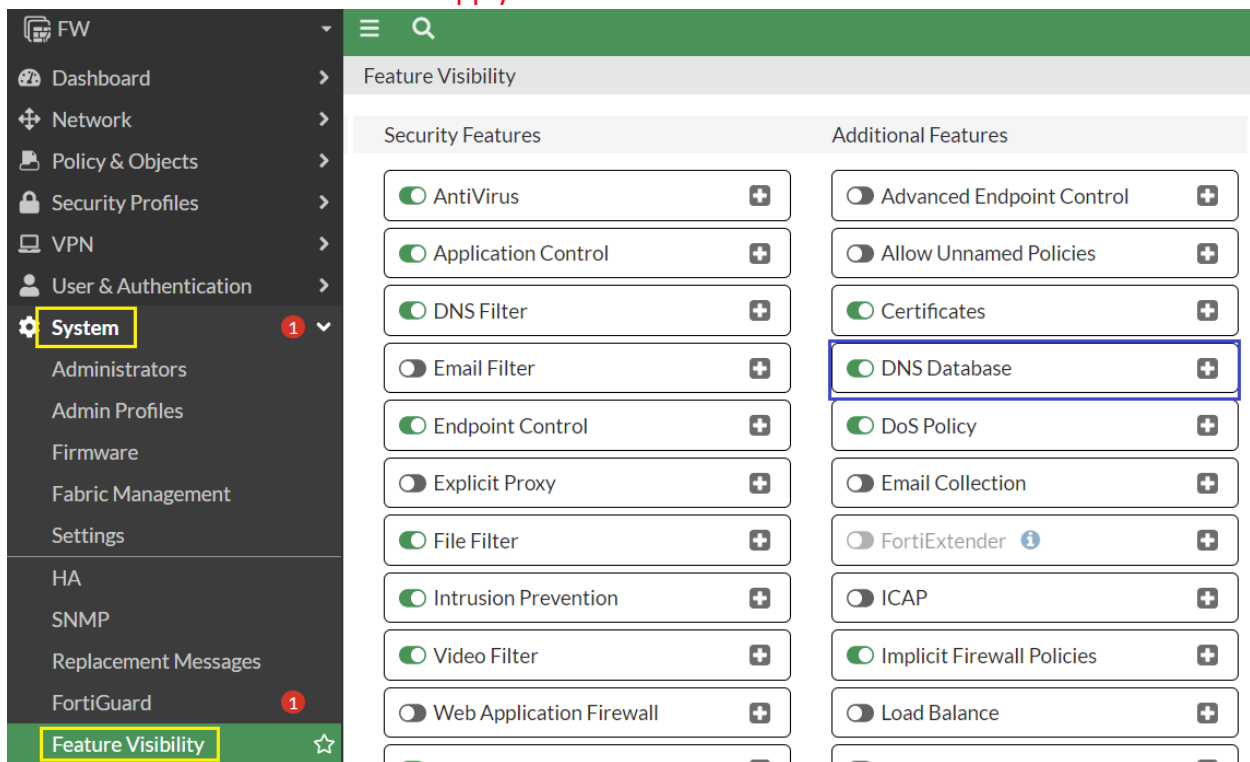
### Configure DNS domain List in CLI

```
config system dns
set primary 8.8.8.8
set secondary 8.8.4.4
set domain "test.com"
end
```

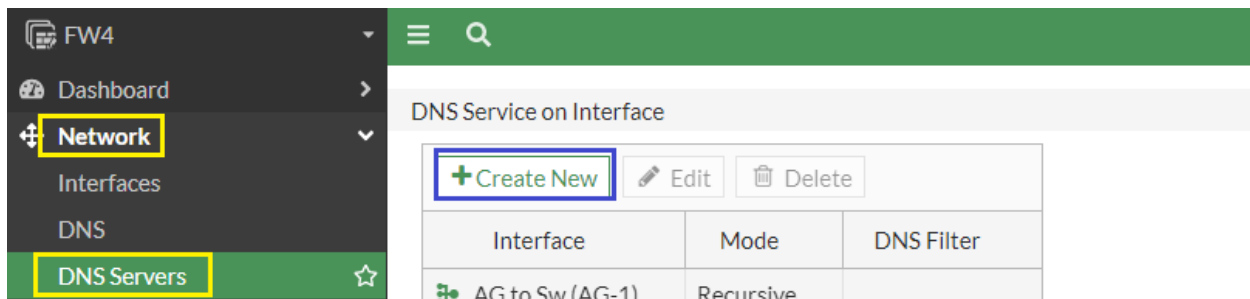
## FortiGate DNS Server:

- o FortiGate Unit Firewall can be created as a local DNS servers for your network.
- o Depending on requirements can either manually maintain entries master DNS server.
- o Or FortiGate Unit Firewall can use it to refer to an outside source Slave DNS server.
- o Local, master DNS server requires to manually add all URL and IP address combinations.
- o Using a master DNS server for local services can minimize inbound and outbound traffic.
- o Using a master DNS server for local services can also minimize the access time for traffic.
- o Slave DNS server refers to an alternate source to obtain URL and IP address combinations.
- o This is useful when there is a master DNS server where the entry list is maintained there.

To enable DNS server options Go to **System > Feature Visibility**, Enable **DNS Database** in the Additional Features section Click **Apply**.



The screenshot shows the FortiGate web interface. On the left, the 'System' menu item is highlighted with a yellow box. The main content area is titled 'Feature Visibility' and is divided into two columns: 'Security Features' and 'Additional Features'. In the 'Additional Features' column, the 'DNS Database' option is checked and highlighted with a blue box. Other options include AntiVirus, Application Control, DNS Filter, Email Filter, Endpoint Control, Explicit Proxy, File Filter, Intrusion Prevention, Video Filter, Web Application Firewall, Advanced Endpoint Control, Allow Unnamed Policies, Certificates, DoS Policy, Email Collection, FortiExtender, ICAP, Implicit Firewall Policies, and Load Balance.



The screenshot shows the 'DNS Service on Interface' page in the FortiGate web interface. The 'Network' menu item is highlighted with a yellow box, and the 'DNS Servers' sub-menu item is also highlighted with a yellow box. The main content area shows a table with columns for 'Interface', 'Mode', and 'DNS Filter'. A '+ Create New' button is highlighted with a blue box. The table contains one entry: 'AG to Sw (AG-1)' in the 'Interface' column, 'Recursive' in the 'Mode' column, and an empty 'DNS Filter' column.

FW4

Dashboard

**Network**

Interfaces

DNS

**DNS Servers**

Packet Capture

SD-WAN

Static Routes

Edit DNS Service

Interface: AG to Sw (AG-1)

Mode: Recursive Non-Recursive Forward to System DNS

DNS Filter:

DNS over HTTPS:

OK Cancel

Dashboard

**Network**

Interfaces

DNS

**DNS Servers**

Packet Capture

SD-WAN

Static Routes

Policy Routes

RIP

OSPF

BGP

Routing Objects

Multicast

Policy & Objects

DNS Service on Interface

+ Create New Edit Delete

Interface	Mode	DNS Filter
AG to Sw (AG-1)	Recursive	

DNS Database

+ Create New Edit Delete

DNS Zone	Domain Name	Type	View	TTL (seconds)	# of Entries
fgdns	test.local	Primary	Shadow	86,400	2

Dashboard

**Network**

Interfaces

DNS

**DNS Servers**

Packet Capture

SD-WAN

Static Routes

Policy Routes

RIP

OSPF

BGP

Routing Objects

Edit DNS Zone

Type: Primary Secondary

View: Shadow Public

DNS Zone: fgdns

Domain Name: test.local

Hostname of Primary DNS: dns

Contact Email Address: host

TTL (86400 seconds): 1 Day(s) 0 Hour(s) 0 Minute(s) 0 Second(s)

Authoritative:

DNS Forwarder: +

