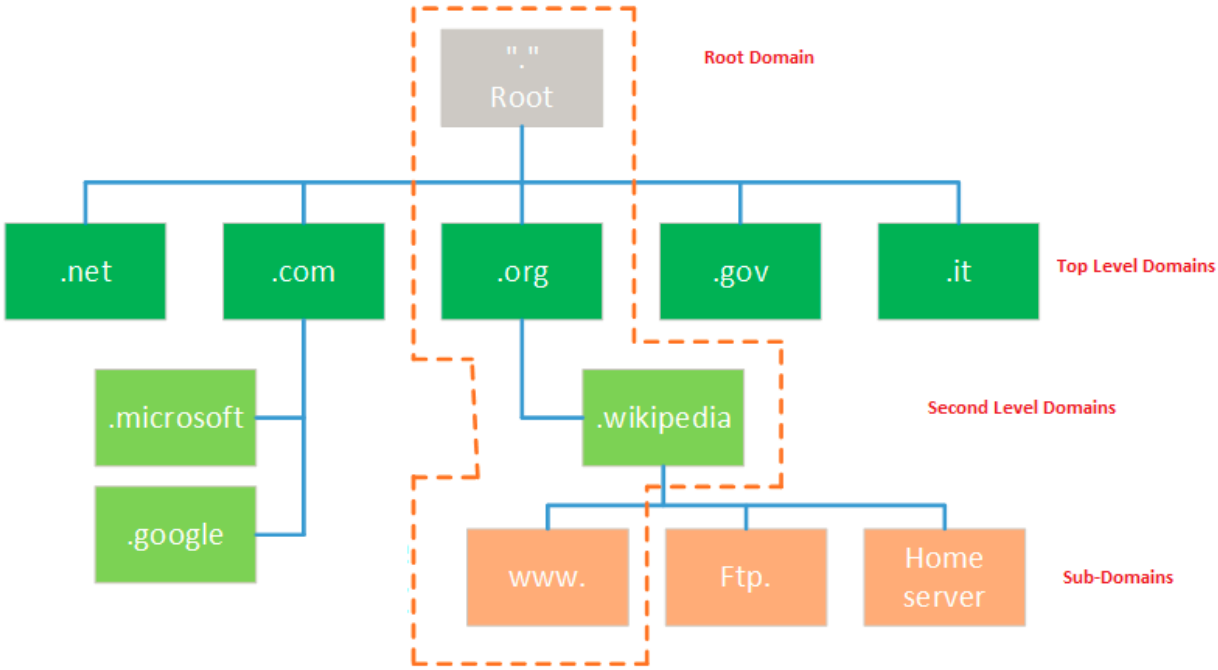
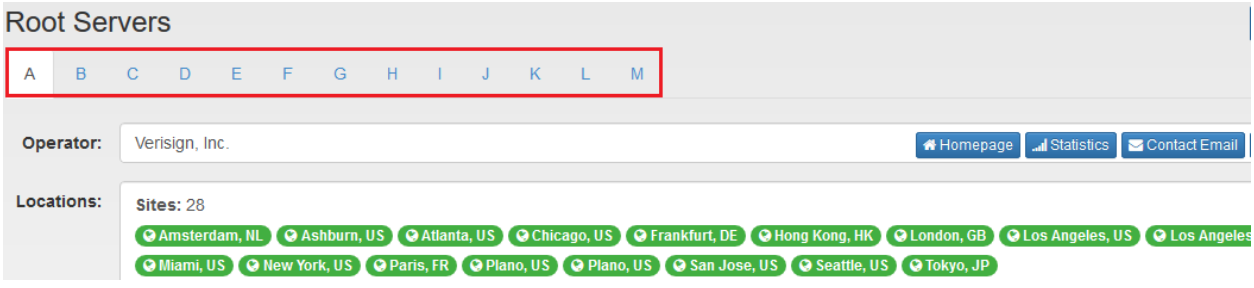
DNS Server:

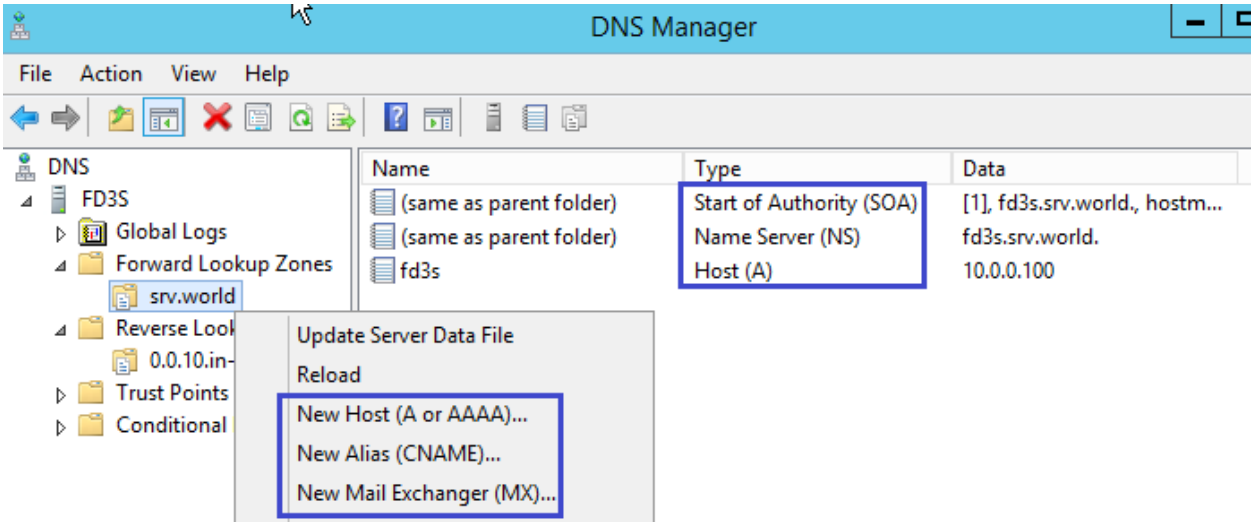
- DNS Stands for Domain Name System or Domain Name Server.
- DNS is a large database, which resides on various computers in world.
- DNS contains names & IP addresses of hosts on Internet & various domains.
- DNS servers match domain names to their associated IP addresses.
- The Domain Name Systems (DNS)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

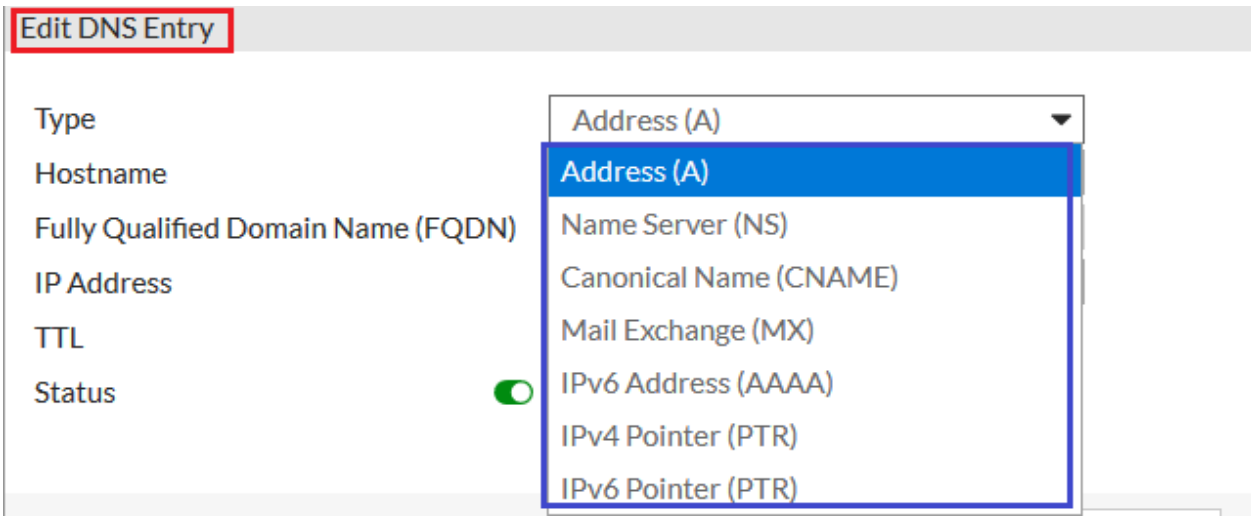




DNS Records:

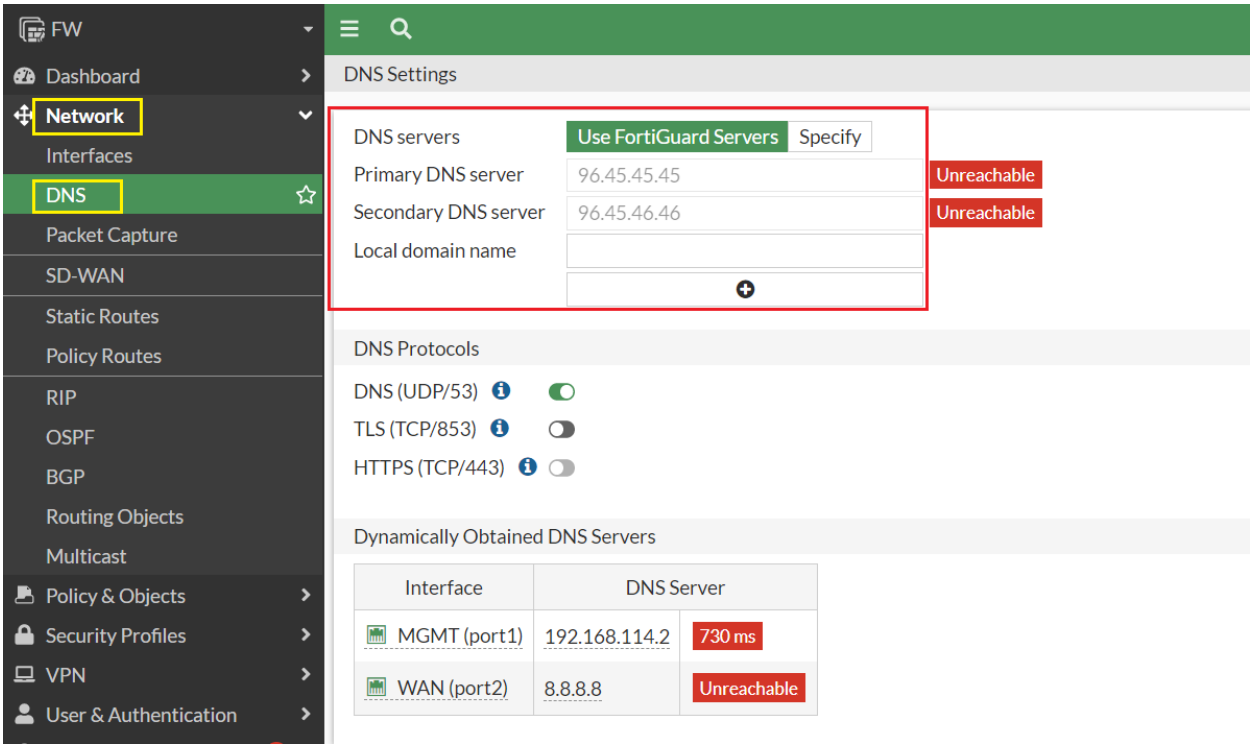
- There are several different types of resource records used by DNS.
- The **A** record specifies IP address Internet Protocol (IPv4) for given host.
- **A**, records are used for conversion of domain names to correspond IP addresses.
- The **AAAA** record specifies Internet Protocol (IPv6) address for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



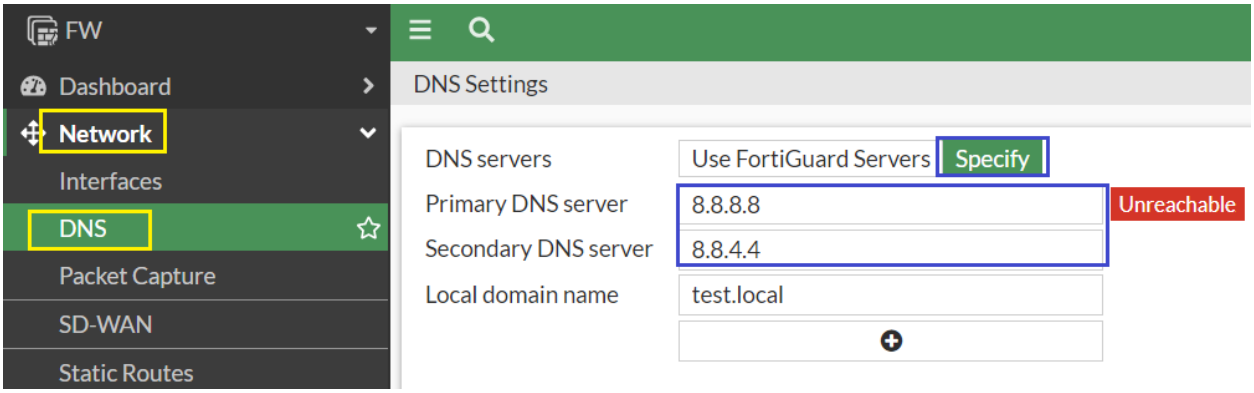


DNS Configuration:

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



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.



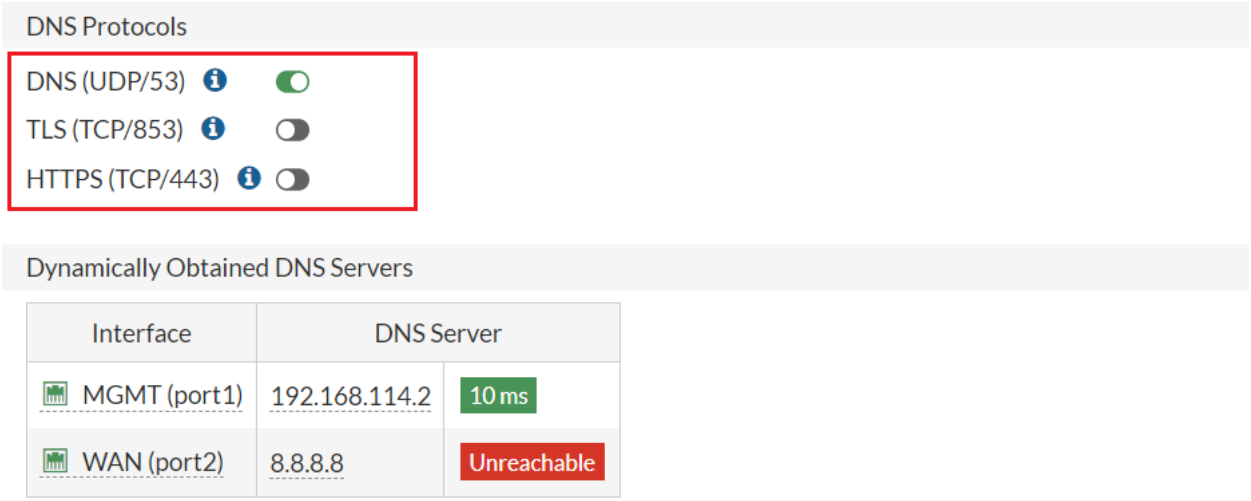
In the Local Domain Name field, enter the first domain such as test. local etc. Click the + to add more domains You can enter up to eight domains names.

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.



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:

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