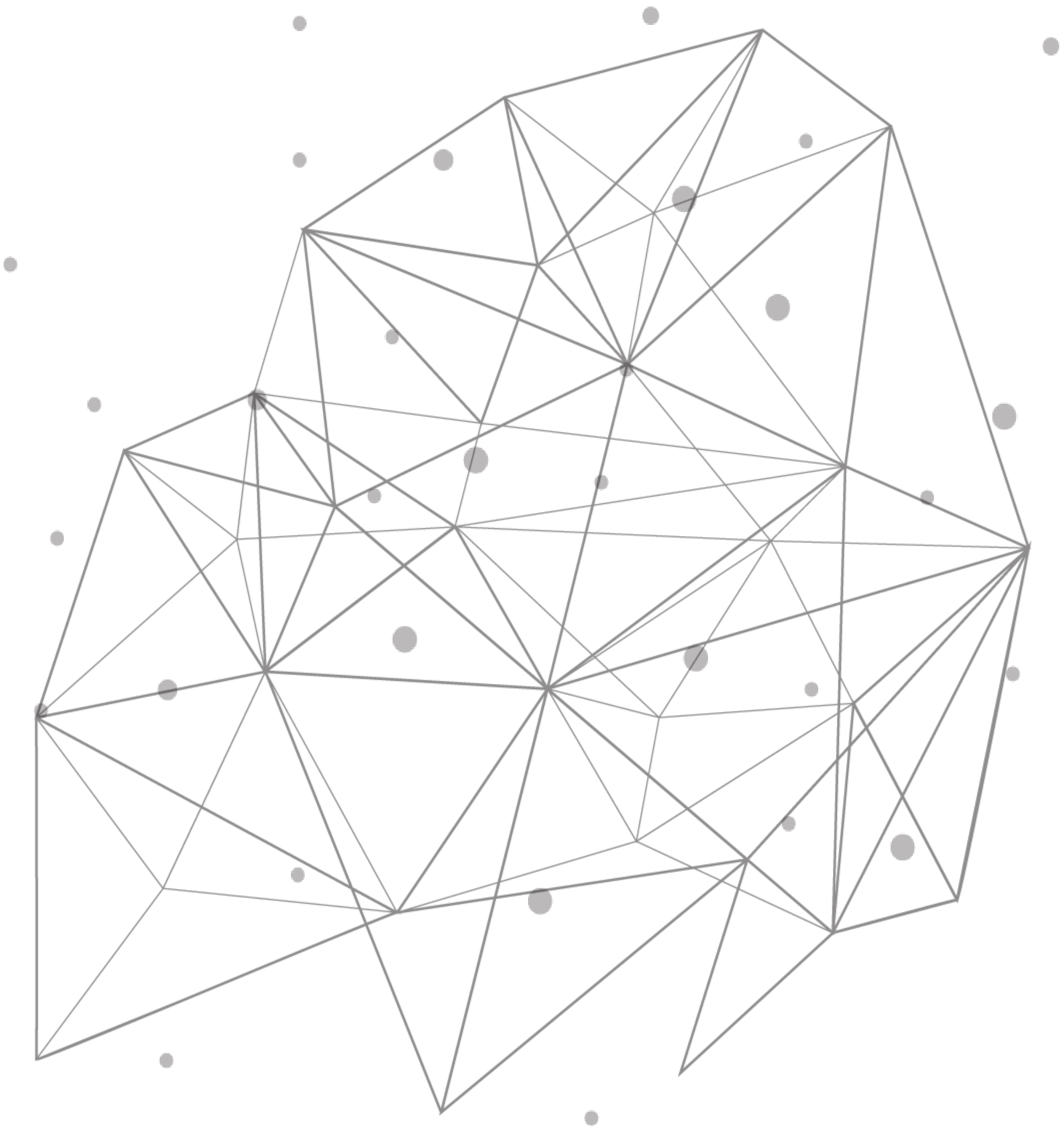
TCPWave DDI - DNS Over TLS



Introduction

When the DNS was created and started using it for the functionality of the internet, security was not given serious consideration in the system architecture. All transactions were happening in cleartext, and anyone who could read the packets on the wire could see what domain was being queried. For this reason, the DNS server is vulnerable to malicious attacks such as DNS spoofing/cache poisoning, DNS tunneling, Distributed Denial of Services, DNS hijacking, DNS flood attacks, and subtypes of these attacks. This has costed billions of dollars each year all over the world. When the internet became public and popular in the ’90s, the need for improving the DNS was given serious consideration. After identifying several security flaws in the DNS system, IETF published several RFEs to address those issues. A few of them are as follows:

DNSSEC (Domain Name System Security Extensions) was created and published to improve DNS security. DNSSEC signs all the data sent on DNS records so resolvers can verify its authenticity. This makes sure that you are connecting to the DNS records that belong to the actual domain name you are trying to connect. To know more about how DNSSEC works in TCPWave IPAM, please visit https://www.tcpwave.in/dnssec_tcpwave/

Response Policy Zones (RPZ) / DNS Firewall was developed by the Internet Systems Consortium led by Paul Vixie as a BIND Domain Name Server (DNS) component. A DNS firewall selectively intercepts DNS resolution for known-malicious network assets, including domain names, IP addresses, and name servers.

Introducing Additional Protocol Enhancement

Since the DNSSEC has a meager adoption rate because the DNS communication was still handled in cleartext thought, there was cryptography involved in ensuring the integrity of resource records in the DNS domain. As we live in a world that entirely depends on technology, digital privacy has become an integral part of customers and businesses due to concerns about government surveillance and the use of data for unethical business practices. To resolve these issues adoption of DNS over TLS (DoT) and DNS over HTTPS (DoH) has been explored and adopted by several organizations which provide public DNS services.

DNS over TLS

As we understand already, the normal DNS traffic sent over UDP or TCP port 53 is not encrypted and prone to attacks and vulnerabilities. To address the issues related to DNS resolution, TCPWave offers DNS over TLS over TCP connections encrypted with TLS as specified in RFC 7858. Encryption provided by TLS eradicates chances for snooping and on-path interfering with DNS queries in the network. Setting up DNS over TLS is very simple. By creating a connection over a well-known port, clients and servers expect and agree to negotiate a TLS session to secure the channel. RFC 7858 specifies the following method for using DNS over TLS to establish secure sessions:

Session Initiation: The DNS client using DNS over TLS must establish a TCP connection to port 853 on the server unless it has a mutual agreement with the server to use a port other than port 853 for DoT. The cleartext DNS messages should not be sent over port 853, and encrypted DNS messages over TLS should not be sent over port 53 either.

TLS Handshake: Once the DNS client succeeds TCP connection on the well-known port for DNS over TLS, it proceeds with the TLS handshake.

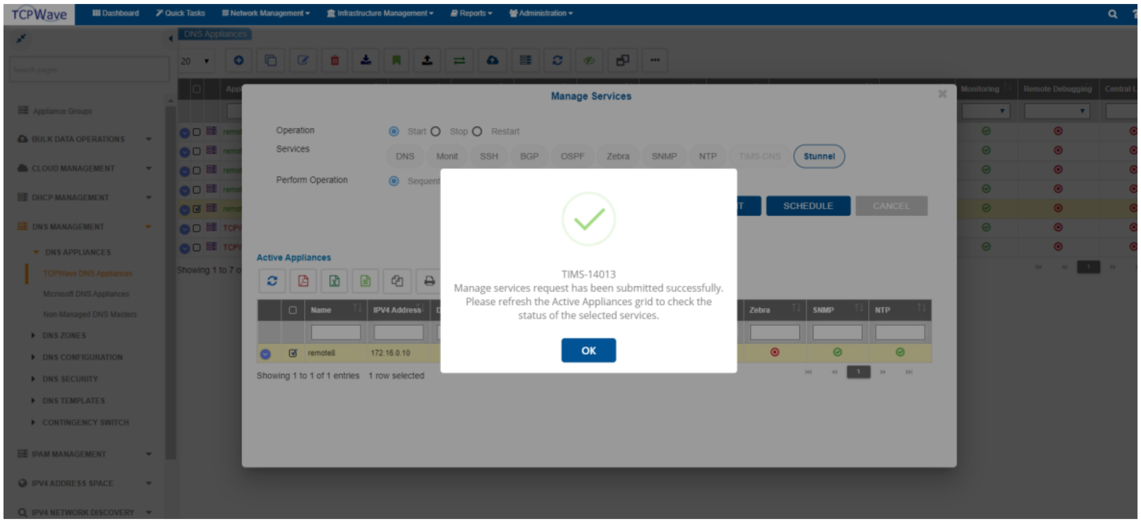
TLS Authentication: The client then authenticates the server if required. The DNS client might choose not to require authentication of the server, or it might use the trusted Subject Public Key Info (SPKI) fingerprint pin set. After the TLS negotiation completes, the connection is encrypted and protected from eavesdropping.

Configuration of DoT in TCPWave IPAM

To configure DoT in TCPWave IPAM:

- Navigate to Network Management >> DNS Management >> DNS appliances >> TCPWave DNS Appliances >> select a DNS appliance >> Select Enable DNS over TLS checkbox.
- Click OK. Therefore, the system enables DNS over TLS on the appliance.
- Navigate to Network Management >> DNS Management >> DNS appliances >> TCPWave DNS Appliances >> select a DNS appliance >> Select Manage Services drop-down >> Select the operation as Start and select the Stunnel option in the service.

  Note: Stunnel is integrated within TCPWave IPAM application to provide TLS/SSL tunneling service.
- Click Submit.



Manage Services

Operation: ● Start ○ Stop ○ Restart

Services: DNS, Monit, SSH, BGP, OSPF, Zebra, SNMP, NTP, TIMS-DNS, Stunnel

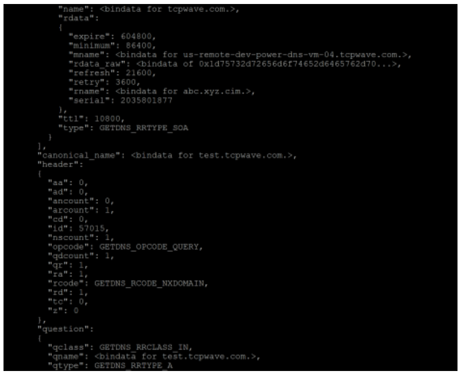
TIMS-14013
Manage services request has been submitted successfully. Please refresh the Active Appliances grid to check the status of the selected services.

Showing 1 to 1 of 1 entries 1 row selected

- Check the configuration of the Stunnel by executing the following command:
  - *cat /opt/tcpwave/stunnel/etc/stunnel.conf*

Note: The Stunnel uses TCP port 853.

- On one terminal, execute the following command:
  - *tcpdump -n -i any tcp port 853 -vv*
- On the other terminal, execute the dnsquery for any domain:
  - *getdns_query -s test.tcpwave.com. A @10.1.10.187 -l L*
- The traffic for the DNS query for the domain will be in the encrypted form as shown:



```
          "name": <bindata for tcpwave.com.>,
          "rdata":
          {
            "expire": 604800,
            "minimum": 86400,
            "mname": <bindata for us-remote-dev-power-dns-vm-04.tcpwave.com.>,
            "rdata_raw": <bindata of 0x1d75732d72656d6f74652d6465762d70...>,
            "refresh": 21600,
            "retry": 3600,
            "rname": <bindata for abc.xyz.cim.>,
            "serial": 2035801877
          },
          "ttl": 10800,
          "type": GETDNS_RRTYPE_SOA
        }
      ],
      "canonical_name": <bindata for test.tcpwave.com.>,
      "header":
      {
        "aa": 0,
        "ad": 0,
        "ancount": 0,
        "arcount": 1,
        "cd": 0,
        "id": 57015,
        "nscount": 1,
        "opcode": GETDNS_OPCODE_QUERY,
        "qdcount": 1,
        "qr": 1,
        "ra": 1,
        "rcode": GETDNS_RCODE_NXDOMAIN,
        "rd": 1,
        "tc": 0,
        "z": 0
      },
      "question":
      {
        "qclass": GETDNS_RRCLASS_IN,
        "qname": <bindata for test.tcpwave.com.>,
        "qtype": GETDNS_RRTYPE_A
```

Considerations

Performance: DNS over TLS incurs additional latency at session start-up due to establishing a secure TCP connection. It also requires a different state (memory) and increased processing (CPU) due to the usage of the TLS algorithms for encryption. To minimize this challenge, the clients should use a limited number of TCP connections.

Security: There are known attacks on TLS, such as man-in-the-middle and protocol downgrade, and it's not specifically for DoT. The DNS clients keeping track of servers known to support TLS enables clients to detect attacks. For servers with no support for TLS and no connection history, clients may choose to have the following based on the requirements:

- Try another server when available.
- Continue without TLS support.
- Refuse to forward the query.

Middleboxes [RFC3234] exist in some networks and are known to interfere with DNS resolution. Using a designated port for DNS over TLS should avoid such interference.

Conclusion

TCPWave DNS appliances support DNS over TLS. To understand and leverage the feature of TCPWave DNS appliances, contact the TCPWave Sales Team for a quick demo.