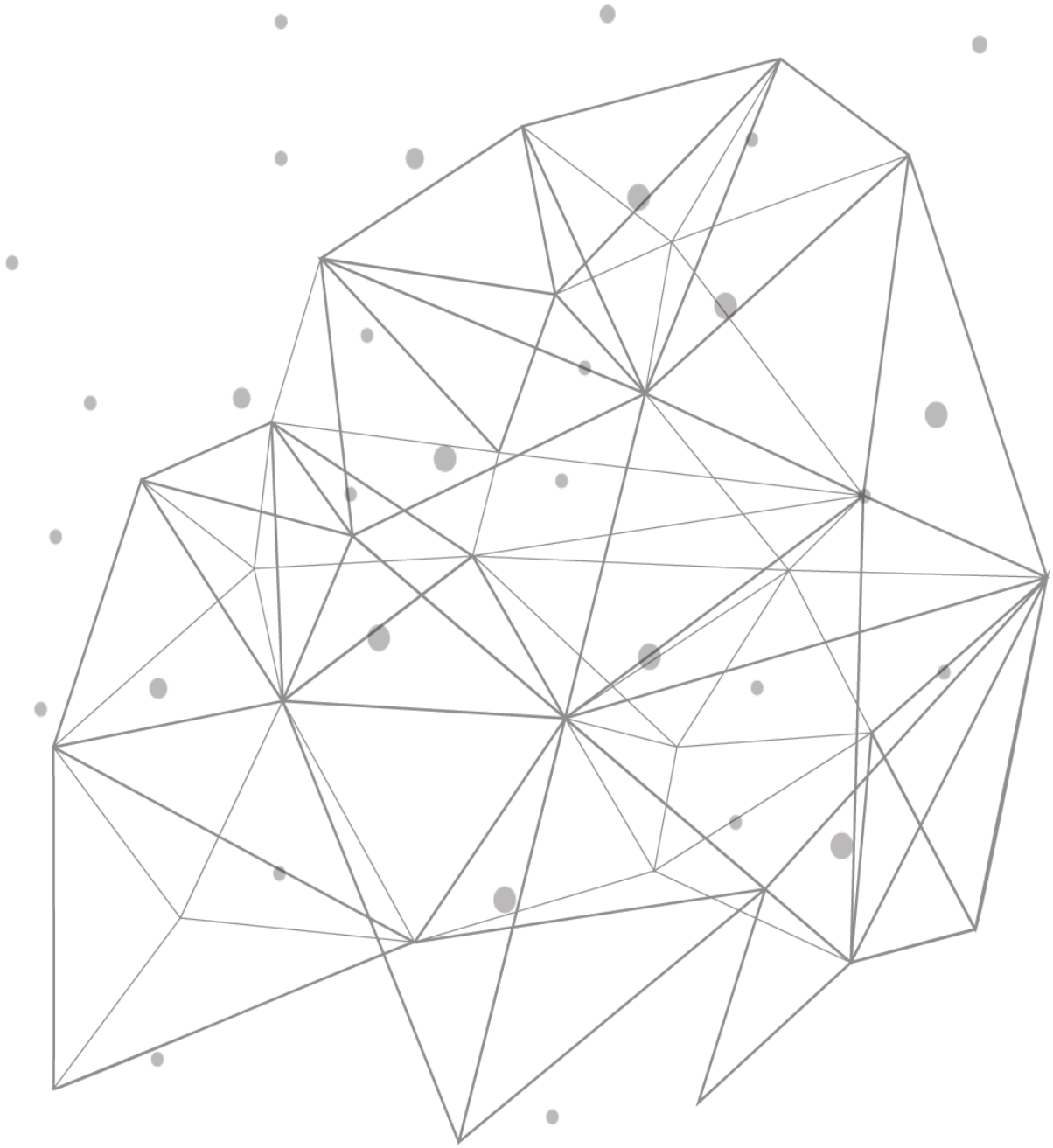
DNS Proxy: Enable Internal DNS Caching Servers to Query External DNS Servers



Introduction

Do you have internal DNS caching servers not connected to the internet that, ideally, could resolve queries for records in business partners' authoritative DNS servers on the internet? Perhaps this difficulty exists because there is not full connectivity from all areas of your company's intranet to the internet. One option that may come to mind for handling this case is to configure the internal DNS caching servers to send some queries to DNS forwarders that would query the partners' DNS servers. However, this would be problematic because the internal caching servers would eventually get query responses that contain records that the server would later attempt to use to directly contact partners' DNS servers. In specific, the caching servers would get and cache nameserver (NS) records in the Authority sections of query responses.

If you have this need for internal DNS caching servers to resolve queries for records in business partners' DNS servers on the internet, then TCPWave enables you to meet it with a solution unique among vendors of DNS-related products. With this solution, TCPWave DNS Proxy Appliances are placed between internal DNS caching servers and the internet and remove the troublesome Authority sections and NS records in them from query responses. Consequently, internal caching servers are able to resolve the needed queries but do not attempt to use cached NS records to directly contact external DNS servers.

Also, in cases in which partners use daisy chains of canonical name (CNAME) records, DNS Proxy Appliances can flatten them. In these cases, DNS Proxy Appliances retrieve and then store the final Address record at the end of each chain. One benefit of this is that when DNS clients query flattened domain names, query resolution times are much faster, since DNS Proxy appliances already have the needed Address records.

To enable those interested in these capabilities to understand and take advantage of TCPWave DNS Proxy Appliances, information on the following topics on them is presented below:

- Query flow without CNAME flattening
- Query flow with CNAME flattening
- Configuration

Query Flow Without CNAME Flattening

A query flow diagram for the TCPWave DNS Proxy Appliance is presented below in Figure 1 and provides an overview of its operation for the typical case in which the DNS Flatten service is not used.

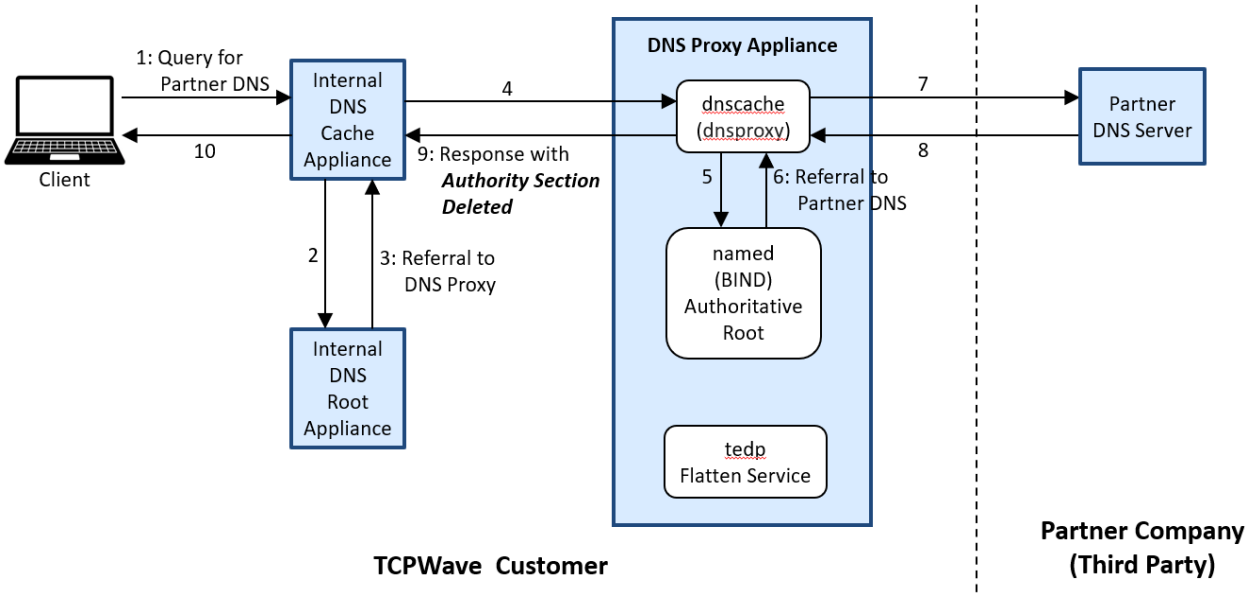


Figure 1: Query Flow for DNS Proxy Appliance Without Flatten Feature

A summary of the DNS queries and responses in this diagram is as follows:

1. A DNS client sends a query to a company's internal DNS caching appliance, which is not connected to the internet, that needs to be resolved by an authoritative DNS server on the internet that is operated by a business partner.
2. The internal DNS caching appliance queries an internal DNS root appliance.
3. The internal DNS root appliance contains a nameserver (NS) record for the queried domain that points to the DNS Proxy Appliance, so it responds with a referral to it.
4. The internal DNS caching appliance queries the DNS Proxy Appliance.
5. In the DNS Proxy Appliance, the caching service checks if the query is an iterative one, and if so, converts it into a recursive query. Then the caching service queries the authoritative root service in the DNS Proxy Appliance.
6. In the DNS Proxy Appliance, the authoritative root service contains an NS record for the queried domain that points to the partner's DNS server and contains an associated glue Address record. Consequently, the root service responds with a referral to the partner's server.
7. The caching service in the DNS Proxy Appliance queries the partner's DNS server.
8. The business partner's authoritative DNS server returns the query response.
9. In the DNS Proxy Appliance, the caching service deletes the Authority section in the query response if it is present. When present, the Authority section contains NS records, each of which specifies a DNS server that is authoritative for a domain. Then the caching service returns the modified response to the internal DNS caching appliance.
10. Finally, the internal DNS caching appliance returns the query response to the DNS client that initiated the query.

Note that in step 9, the internal DNS caching appliance gets a query response that does not contain an Authority section and NS records in it. Consequently, this appliance will not cache NS records and later use them to attempt to contact the external partner DNS servers specified in them. This is desirable because the internal caching appliance does not have connectivity to the internet and external DNS servers on it.

Query Flow with CNAME Flattening

The DNS Proxy Appliance also contains a Flatten service, which can be used in cases in which a partner daisy-chains canonical name (CNAME) records. In these cases, a CNAME record points to another CNAME record or possibly a series of CNAME records, and the last CNAME record points to an Address record for a domain. Daisy-chaining CNAME records is not considered a best practice but is still sometimes done.

Before the Flatten service in a DNS Proxy Appliance functions, Flatten records for domain names to be flattened are entered in TCPWave. Then, before DNS queries are received, the Flatten service resolves daisy-chained CNAME records as summarized in the steps in Figure 2 below. Note that multiple queries to external DNS servers on the internet are done, although for simplicity only a single query and DNS server are depicted. After this, the Flatten service will periodically resolve Flatten records and update the authoritative root service in the DNS Proxy Appliance if needed.

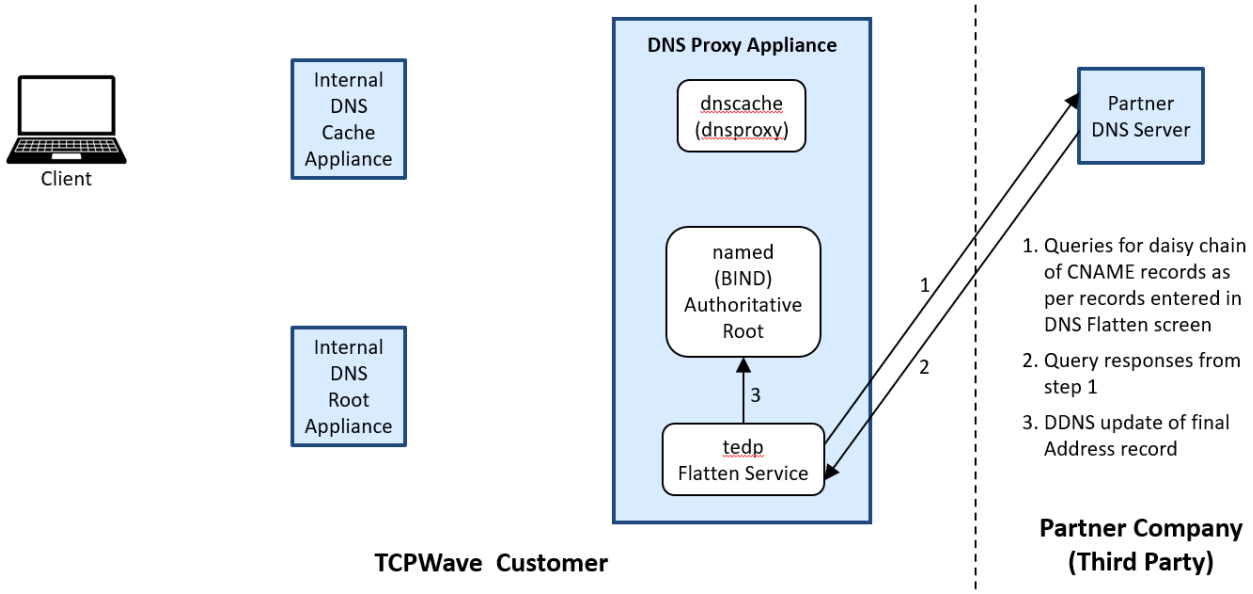


Figure 2: DNS Proxy Flatten Process

After the Flatten process has run, when DNS clients make queries, they are resolved as shown below in Figure 3. Most of the numbered steps in it are similar to the ones described in the section above for the case in which the Flatten service is not used. However, when the Flatten feature is used, the query response returned by the authoritative root service in a DNS Proxy Appliance in step 6 is different. With the Flatten feature, the response contains the Address record that the Flatten service found at the end of the CNAME chain, as summarized above in Figure 2. One benefit of the Flatten feature is that when DNS clients query flattened domain names, query resolution times are much faster, since multiple queries to external DNS servers on the internet have already been done.

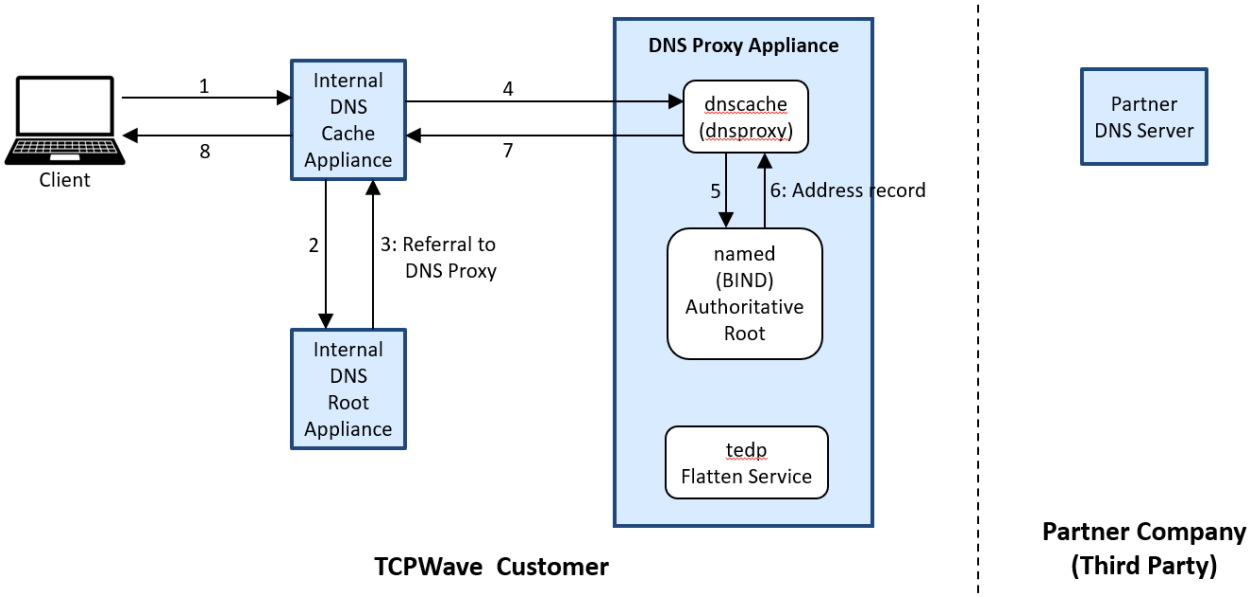


Figure 3: Query Flow for DNS Proxy Appliance with Flatten Feature

Configuration

Two main configuration steps are always needed for DNS Proxy Appliances to function, and a third step is needed only when a business partner uses CNAME daisy chaining. The two steps always needed are to configure one or more DNS (Internal) Root Zones and one or more DNS Proxy Root Zones. Both of these steps involve entering nameserver (NS) records, each of which specifies a DNS server that is authoritative for a domain. A summary of the configuration needed for these three items is provided below. Note that details on all the configuration steps needed are available in the *TCPWave IPAM Administrator Reference Guide*.

DNS (Internal) Root Zone: Each internal DNS root appliance uses an internal root zone. In this zone, enter NS records that delegate partners' domains to DNS Proxy appliances.

DNS Proxy Root Zone: The BIND authoritative root service in each DNS Proxy Appliance uses a proxy root zone. In this zone, enter NS records that delegate partners' domains to their authoritative DNS servers on the internet and enter associated glue Address records. (Alternatively, it is possible to delegate to DNS servers in a DMZ, which would contact the partners' DNS servers.)

DNS Flatten Zone: For each domain name to flatten, enter a TCPWave Flatten record that contains a domain name and an associated nameserver that the Flatten service will query first.

Solutions

If you need internal DNS caching servers to resolve queries for records in business partners' authoritative DNS servers on the internet, TCPWave DNS Proxy Appliances enable you to meet it with a solution unique among vendors of DNS-related products. Furthermore, in cases in which partners use daisy chains of canonical name (CNAME) records, DNS Proxy Appliances can flatten them. One benefit of this flattening is that when DNS clients query flattened domain names, query resolution times are much faster.

For more information on DNS Proxy Appliances and how other unique and beneficial features in TCPWave's DNS, DHCP, and IP address management (DDI) product can meet your needs, contact the TCPWave Sales Team.