Overview: Distributed Denial of Service via DNS (DNS DDoS) is now a common network traffic attack used by various malicious actors to negatively impact business or agency operations. DNS DDoS attacks are designed to bring down DNS servers and consume network bandwidth thereby impacting critical IT applications (e.g. email, web transactions, VoIP, SaaS). For target businesses, there are two typical roles to a DNS DDoS attack: victim and accomplice. Using best practices for DNS configuration and operation, you reduce your risk of being impacted by a DNS DDoS attack or being used in one.

Avoid being a Victim

To avoid being a victim of a DNS DDoS attack, you must understand the components of the attack and have a plan to mitigate them. While you can never completely eliminate or mitigate DNS DDoS attacks, you can take measures to survive them and keep critical applications running. Below are some basic steps to temper the impact of a DNS DDoS attack on your IT infrastructure:

Over-provision DNS Servers
Simply having the capacity to handle a DNS DDoS attack is one of the easier steps to take in protecting your DNS services. Over-provisioning DNS servers provides cushion for both DNS DDoS but also internal business growth as well.

In order to have I/O and bandwidth and DNS query horsepower to address a DNS DDoS attack, a conservative factor of 10x of highest average DNS/Query Per Second (QPS) is recommended. Maintaining this 'headroom' requires periodic review (e.g. once per quarter or once every six months) of usage and equipment capacity.

Build-in High Availability
DNS is critical to business operations and thereby should be configured in an High Availability (HA) pair to ensure automatic fail-over. In the case of a DNS DDoS attack (or any other hardware/software issue), the sudden over-load can cause a DNS server to fail or slow responses to the point of impacting transactions. Having the DNS server automatically fail-over to a readily available stand-by server (equal capacity at minimum) will minimize disruption to business operations and trouble tickets to IT. High-availability best practices recommend documenting configuration and have a testing plan. Testing should validate the failing over from one server to another and back and what steps are needed when it does not perform as specified.

Set Response Rate Limit by Source IP Address
Rate limiting by IP address allows specifying how many DNS queries per time slot can be accepted from a particular IP or subnet, blocking any attack or misuse that sends DNS requests above the configured threshold. This throttling mechanism will require the attacker to have to spoof a much larger IP address range in order to reach the query rate necessary for the attack to succeed. Caution: before implementing this rule(s) on your network, it is recommended to do extensive testing where the offending requests are not actually dropped, only logged. This procedure will help identify the traffic patterns of your network and give confidence that the rate-limiting rules will not harm legitimate traffic.

Set Response Rate Limit by Destination IP Address
The destination IP address rate limit is useful when the operational load limit of a DNS server is known and you don’t want to reach this limit. By using this type of rate limiting you can specify the maximum number of queries that can reach each DNS server on the server farm, dropping any additional traffic above this threshold (which would be discarded anyway) and thus protecting the DNS server from being overwhelmed by receiving more queries than it can handle. Before implementing the rule(s) on your network it is recommended to do testing to determine the settings that will work both for both business and security purposes.

Use Cloud-based Anycast Secondary Servers
Spreading a DNS DDoS attack diffuses the impact and enables the targeted business's DNS infrastructure to continue operations. DNS query loads can easily be spread to geographically dispersed DNS servers via Anycast. There are a number of Internet-based ('cloud') companies that offer Anycast secondary services which can help mitigate the effect of DNS DDoS attacks.
Configuration of Anycast can be done in a number of ways to ensure proper operation:

- Configuration of Anycast IP address(es) into the routed network - This can be accomplished using either static routes or using routing protocols such as OSPF, or BGP.
- Host-based routing software that supports one of the major routing protocols.
- Clients should be configured to resolve DNS queries via the Anycast address(es)
- Name servers should listen to DNS requests on the Anycast IP addresses
- Name servers should be advertised at the Anycast address(es) in A and AAAA records
- Name servers should be configured with at least one Anycast IP address on a loopback interface. Additionally, the server should be configured with a management IP which can be either a physical or an additional loopback interface.
- At least one physical IP must be defined for the exchange of routing information, as well as, system access and maintenance in the absence of the routes to the Anycast IP address(es).
- Name servers should be configured to use the physical or management IP addresses for zone-transfers, zone updates, and/or query-source because replies might go to a different server than intended.

Don’t be an Accomplice

The flip side of a DNS DDoS attack is the accomplice who unwillingly amplifies the attack with their DNS infrastructure. Being an accomplice in a DNS DDoS attack, while not as devastating as being the target, still impacts DNS services, network bandwidth and leaves the door open to possible litigation due to weak IT control. Simple best-practices configuration will help reduce the chance of becoming an accomplice in a DNS DDoS attack and reduce potential litigation.

Close your ‘Open’ DNS Recursive Server

Many businesses have recursive servers that have not been configured to respond to DNS queries from internal resources only. Simply restricting the Recursive DNS servers to internal IP addresses only is the simplest way to avoid being an accomplice to a DNS DDoS attack. Most IT administrators know the range of IP addresses within their organization. Simply setting an access control list limiting queries to the range of internal IP addresses will prevent your recursive DNS servers from attacking an IP address outside of your network.

Rate Limit Responses from Authoritative Name Servers

Rate limiting can also be used for Authoritative DNS servers. Doing so can be tricky since the source IP address that can reach your DNS server is unknown. Again testing with various limits should be performed and documented to settle upon a configuration that delivers the desired results without impacting business operations.

Summary

Utilizing best practice configurations and polices will improve your DNS architecture to make it more resilient against DNS DDoS attacks. Employing most if not all of them will decrease the odds of having your DNS infrastructure taken down by an attack. Below is a quick list of best practices:

Avoid being the Victim

1. Over-provision your DNS servers
2. Build-in high-availability
3. Use DNS Rate limit feature to control flows
   - Rate limit by Source IP address
   - Rate limit by Destination IP address
4. Anycast to Cloud-based Service to distribute DNS queries

Don’t be the Accomplice

1. Close your ‘open’ DNS Recursive Server
2. Rate limit responses from Authoritative Name Servers

Testing and documenting configurations and processes will help you correctly set and maintain thresholds and meet compliance audits.