Infoblox
CONTROL YOUR NETWORK

Authoritative Domain Name Server

SOLUTION NOTE

Summary

Unseen and little-noticed, domain name servers are vital to the commercial and network infrastructure of most organizations. If they are impaired, inbound Internet access to all network-based functions will be at risk. This solution note explains the role of authoritative domain name servers, the threats they face, and how Infoblox delivers best-of-breed authoritative DNS to organizations and service providers.

Background: Domain Name Services

DNS translates or "resolves" Internet domain names into IP addresses. People use domain names, such as www.google.com, but the Internet needs IP addresses to route traffic to the proper destination. Because DNS performs a domain-to-address resolution it is frequently characterized as a "phonebook" for the Internet. The maps of domain names and IP addresses are stored on DNS servers distributed across the Internet. Most DNS servers are software running on a computer, software running on purpose-built hardware or running within a cloud.

To resolve an address, DNS is navigated using an inverted tree. Inputting a domain name into a browser causes the first DNS server in its configuration, often a DNS resolver, to search its cache for that domain's IP addresses. If an IP address is not found in cache, the resolver processes a set of queries over the Internet through the hierarchy of DNS servers—first to a root-name server, then to a top-level domain server, and finally to an external authoritative domain name server that contains the IP addresses of the destination domain.

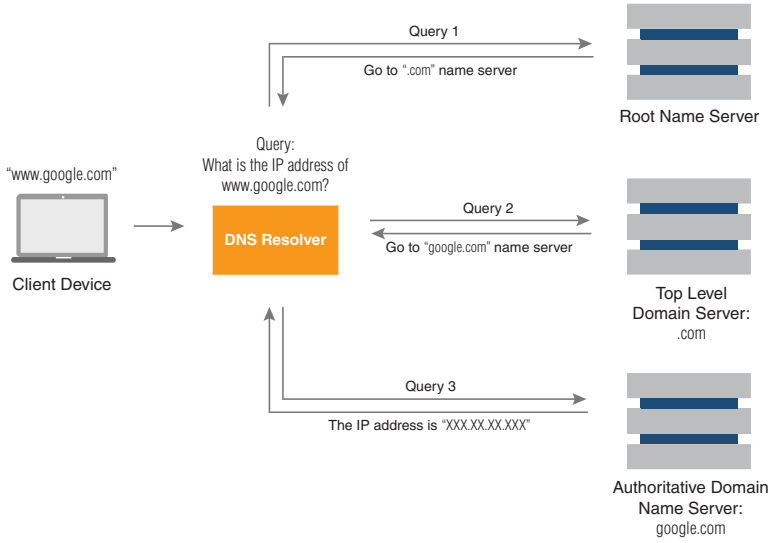

Figure 1: Acquiring an IP address through DNS recursion

The resolver repeatedly obtains destination IP addresses and updates its cache. It is called a "recursive DNS server" because it uses recursion to perform the resolution process. Once the resolver obtains the IP address requested by the client device, that client can begin communicating with the intended domain.

Despite the first-glance complexity, DNS protocols make the recursion process rapid and transparent. A detailed look at the inner workings of DNS can be found here.

The Importance of an Authoritative DNS Server

Authoritative DNS servers are managed by or on behalf of the domain owner. Internet service providers often host the service. Because they have complete and up-to-date information about their zones these servers are the authoritative source for IP addresses. That fact makes authoritative DNS servers crucial to an organization's availability on the Internet.

Constant change is the nature of a network. Traffic growth, re-allocation of capacity, and the evolution of web-based services are frequent drivers. Since each network element requires an accurate IP address, every change requires a corresponding and timely update to the authoritative DNS server. This ups the ante for authoritative DNS servers because not only must they be reliable; they must also be well-managed and secure.

The Risks to DNS

The DNS protocols were optimized for speed and efficiency, but not security. This makes DNS a common vehicle for network attacks. The pivotal roles of DNS and the authoritative DNS server make it easy see how a successful DNS-based attack could wreak havoc on an organization's services, as well as its reputation.

There are numerous variants of DNS attacks but three chief categories are:

Distributed Denial of Service (DDoS). This is the most infamous type of DNS attack and has many sub-variants. In a DDoS attack authoritative DNS servers are overwhelmed with messages, queries, zone transfers, TCP, UDP, and other traffic. This traffic may be amplified in packet size and query volume for greater effect. If a DDoS attack is successful, the authoritative DNS server resources are consumed responding to attack traffic, thereby ignoring legitimate access to services. This amounts to a "denial of service" to valid users and their traffic.

Cache poisoning. A cache poisoning attacker sends bogus IP addresses in a forged DNS response to a recursive DNS server and if the attack is successful, that server caches and maps a bogus IP address to a domain. Once the bogus address is cached, that DNS server will respond to a legitimate DNS query with the false IP address. An unsuspecting client could then transact information with the attacker rather than the intended web service.

Man-in-the-middle attack (MITM). This is often a means to perform another attack, such as DNS spoofing. A MITM attack uses a machine that compromises the network to intercept traffic. It then spoofs DNS transactions and delivers counterfeit IP addresses to clients, similar to cache poisoning. Here again unsuspecting traffic is routed to a host controlled by the attacker rather than the intended service.

Other types of DNS-based attacks target authoritative DNS servers, such as floods, DNS hijacking, and botnet-based attacks. But irrespective of the type of attack, the ramifications of a compromised authoritative DNS server can be profound. Among them are:

- Poorly performing services, unavailable services, and/or long recovery times
- Dissatisfied customers, clients, prospects, partners, and job candidates
- Lost revenue
- The appearance of being technically inept, a commercial laggard, or indifferent

Brand-name organizations have suffered embarrassing and costly service failures because of DNS-based attacks. No one wants to join that hall of shame.

Strategies for Superior Authoritative DNS

There are three areas of focus to make authoritative DNS servers more reliable and more secure.

Architecture. The external DNS server infrastructure should be designed to avoid any single point of failure. A good way to do this is by running a primary DNS server in concert with two (or more) authoritative DNS servers that are topologically dispersed and have their own, dedicated links to the Internet. The primary DNS server provides external zone records to the secondary authoritative DNS servers, which in turn resolve non-recursive queries from the Internet.

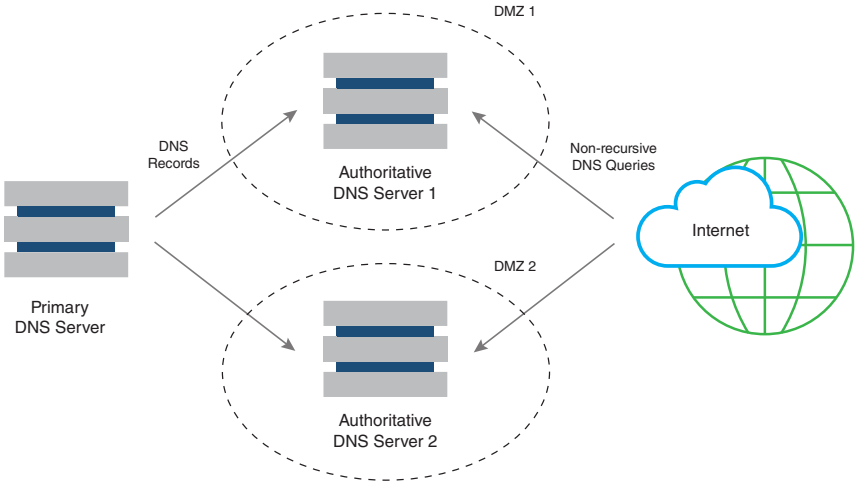

Figure 2: Well-architected external DNS servers

This architecture isolates the primary source of DNS records from potentially dangerous Internet traffic. Using multiple authoritative DNS servers, each with its own Internet link, creates redundancy that prevents the failure of one server or one link from interrupting access to services.

Server Configuration. Since the authoritative DNS servers are linked to the Internet, they should be configured to resist attacks. The most crucial action to take it to disable the DNS recursion function. That prevents these servers from responding to traffic types commonly used in DDoS and other DNS-based attacks. In addition, the DNS zone transfer function (replicating the DNS database to other DNS servers) should be turned off because a hacker who can transfer your zones can mount a DDoS attack or scour that zone data for the names and addresses of name servers, mail servers, domain controllers, and other assets.

Server Hardening. Using authoritative servers that are designed to resist attacks are as important as fortifying architectures and configurations. Using purpose-built hardware is an advisable first step. With a hardened kernel, a focused set of network interfaces, and password protection, a DNS server appliance prevents errant root access.

Dedicated DNS server appliances will have added security features. DDoS detection, rate limiting, blacklisting and NXDOMAIN redirection, DNSSEC, out-of-band management, and encrypted communication protect Internet accessibility from all manner of DNS-based attacks.

Finally, a dedicated appliance can enhance the performance of authoritative DNS services with advanced caching, multi-gigabit network interfaces, and scalable compute power to handle the demands of an enterprise or service provider.

Conclusion

Infoblox is the expert on authoritative DNS servers. Our authoritative DNS meets the expectations for high speed and responsiveness while reducing the administrative burden of updating and maintaining records. Infoblox solutions also improve service continuity by providing robust protection against common DNS-based attacks.

Attack	Description	Infoblox Protection
TCP SYN Flood	TCP SYN requests go to a server which responds with ACKs. Attackers do not reply to ACKs leaving "hung" connections.	Tracks SYN requests per second. If requests exceed a threshold client ACKs are examined. Requests are dropped if there are no client ACKs.
UDP Flood	A flood of UDP packets go to a port on a server, requiring ICMP replies. Reply processing causes the port to become unavailable.	Detects a high number of packets with small payload for one or a small number of clients. Uses prioritized packet discard to throttle incoming traffic.
Spoofed Source Address	TCP/UDP packets are sent to server using the server's address as the source and destination address in the packets. The server continuously replies to itself, causing overload and denial of service.	Validates the source address of all incoming packets. If source address on a packet is the server's address, the packet is discarded.
Cache Poisoning	A poisoned DNS cache redirects legitimate traffic to the attacker's website.	Uses VPN, encrypted communication, HTTPS, and out-of-band management.
MITM	A compromised machine on the network hijacks DNS infrastructure to redirect legitimate traffic to an attacker's website.	Uses VPN, encrypted communication, HTTPS, and out-of-band management.

Authoritative DNS servers are essential to any organization that must be accessible via the Internet. If these services are compromised, the ramifications are potentially broad, painful, and long-lasting. Best-practice implementations of authoritative DNS will become more critical, and thought-leading organizations are hardening authoritative DNS servers today as standard work, rather than as a reaction to the consequences of successful attacks.

About Infoblox

Infoblox delivers Actionable Network Intelligence to enterprises, government agencies, and service providers around the world. As the industry leader in DNS, DHCP, and IP address management (DDI), Infoblox provides control and security from the core—empowering thousands of organizations to increase efficiency and visibility, reduce risk, and improve customer experience.

Corporate Headquarters: +1.408.986.4000 1.866.463.6256 (toll-free, U.S. and Canada) info@infoblox.com www.infoblox.com