Infoblox
CONTROL YOUR NETWORK

WHITEPAPER

Are You Fully Prepared to Withstand DNS Attacks?

Fortifying Mission-Critical DNS Infrastructure

Are You Fully Prepared to Withstand DNS Attacks?

Fortifying Mission-Critical DNS Infrastructure

Since Q1 of 2012, the number of infrastructure attacks based on the Domain Name System (DNS) has increased by 200[1] percent. Why? Because by its very nature, DNS is easy to exploit.

- Most enterprise firewalls are configured to allow port 53 traffic to service DNS, giving attackers an easy way to evade your existing defense systems.
- Because DNS queries are asymmetrical, they can result in a response many times larger than the query, which means that your DNS system itself can be made to amplify an attack. Hackers can send one packet of data and cause a flurry that is amplified severalfold—effectively stopping your business in its tracks.
- Attackers can easily conceal their identities, because the DNS protocol is stateless.

Large IT organizations and service providers have little choice but to work around these weaknesses, because in the Internet age, DNS services are essential to almost every critical function of modern businesses. Without functioning DNS, smartphones don't work, an enterprise can't do business online, teams can't communicate effectively, productivity drops, customer satisfaction declines, revenue is reduced, and the company's reputation is at risk.

This whitepaper is about solving the problem of threats that target DNS. It reviews the functions of the DNS protocol, catalogs the various kinds of DNS-based attacks to give you a clear idea of the magnitude of the threat, and sets forth and explains the best available solution—Infoblox Advanced DNS Protection, the first DNS appliance that protects itself and plugs this gap in the overall security structure.

How DNS Functions, and What It Does

Before we get into threats and how you can prevent them, let's go over the basics of DNS. DNS is the address book for every destination on the internet. It transforms domain names such as infoblox.com into IP addresses such as 54.235.223.101. This means that DNS determines whether communications and requests get to the right addresses. Enterprises and service providers need fast and accurate DNS services for incoming and outgoing traffic to conduct business online. Communications with suppliers, customers, and company locations happen via email, web sites, and HTTP file transfer. A significant side effect of DNS processing is that DNS servers are a little like the main doors at a shopping mall: they let the shoplifters in as well as the customers.

There are two kinds of DNS name servers: authoritative and recursive.

- Authoritative DNS servers are the entry point to a company's services. They only answer queries about the domain names for which they have been configured or about names in a specific set of zones. DNS servers that connect to the Internet are usually configured in authoritative mode, and these are the target of external attacks such as amplification, reflection, and exploits.

- Recursive DNS servers, also called “caching servers,” answer queries by asking other name servers for the answer. Sometimes they draw the answers from a cache, hence the alternate name. If a recursive server doesn’t find the answer it needs in a cache, it traverses the namespace tree, repeating the query, following referrals from authoritative servers, until it finds a name server that gives the answer. In other words, recursive name servers depend on authoritative name servers. Recursive name servers are usually deployed internally to provide services to internal users. They are susceptible to attacks that originate from users inside the enterprise.

A Catalog of DNS Threats

The number of potential threats at the time of this writing is truly alarming. We’ve listed them here, and described them briefly.

Direct DNS amplification attacks are aimed at congesting DNS server outbound bandwidth. They start by sending a large number of DNS queries, specially crafted so that they result in a very large response that can reach up to 70 times the size of the request. Since DNS relies on the User Datagram Protocol (UDP), the attacker can use a small volume of outbound traffic to cause the DNS server to generate a much larger volume, resulting in congestion of the DNS server’s upload and eventually a denial of service (DoS).

Reflection attacks use a third-party DNS server (typically an open recursive name server) in the Internet to propagate a DoS or DDoS attack by sending queries to the recursive server. Recursive servers will process queries from any IP address, and they return responses. The attack spoofs the DNS queries it sends by including the victim’s IP address as the source IP in the query, so that the query has the victim’s server information rather than the attacker’s. So when the recursive name server receives the requests, it sends all the responses to the victim’s IP address. A high volume of such “reflected” traffic can bring down the victim’s site.

Distributed reflection DoS (DrDoS) attacks combine reflection and amplification that significantly increases the size of the response to the initial queries—and the likelihood that the victim’s server will be overwhelmed. Ironically, DNS Security Extensions (DNSSEC), designed to secure DNS responses through encryption and prevent cache poisoning, can make this type of attack even more effective because the cryptographic signatures DNSSEC uses result in larger DNS messages. The amplification can be as high as 100x, and attackers can use botnets—often utilizing thousands of servers—to greatly increase the number of queries sent.

This is a particularly deadly and hard-to-counter threat. There are about 33 million open recursive DNS servers[2], and 28 million of them don’t have access controls and can be used in DrDoS attacks.

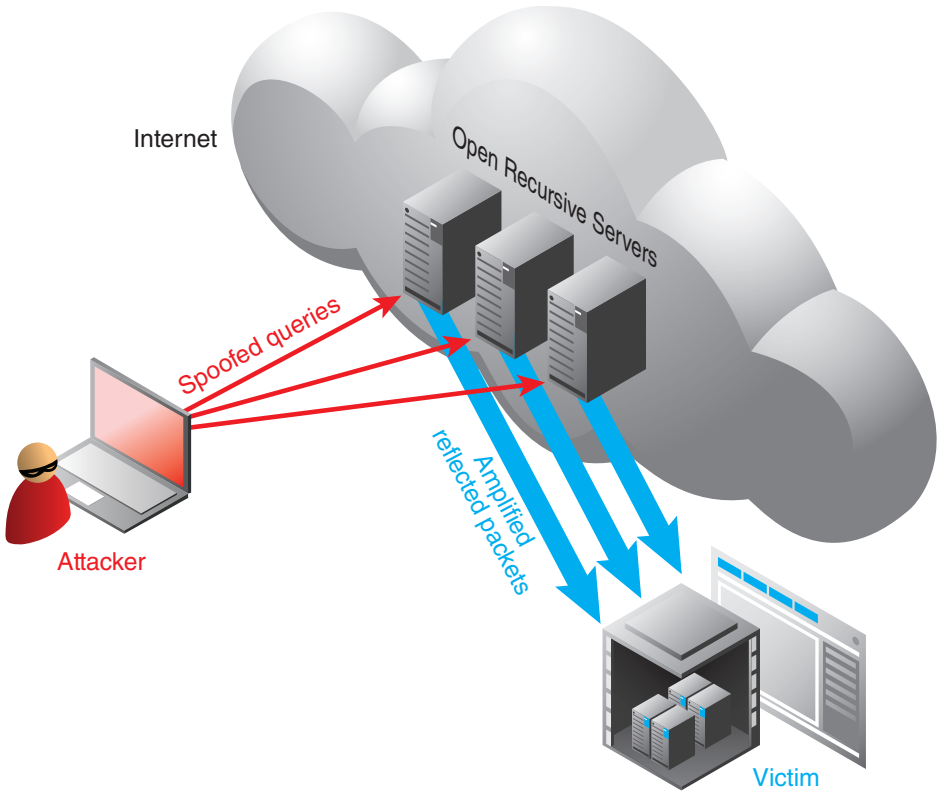

Figure 1: A distributed reflection DoS attack

TCP/UDP/ICMP flood attacks are volumetric attacks with massive numbers of packets that consume a network's bandwidth and resources. They exploit the Transfer Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

UDP floods send large numbers of UDP packets to random ports on a remote server, which checks for applications listening to the port but doesn't find them. The remote server is then forced to return a large number of ICMP Destination Unreachable packets to the attacker saying that the destination is unreachable. The attacker can also spoof the return IP address so that the replies don't go to the attacker's servers. Sending the replies exhausts the victim server's resources and causes it to become unreachable.

TCP SYN floods consist of large volumes of half-opened TCP connections that cause servers to stop responding to other requests from clients to open new connections. This attack takes advantage of the way TCP establishes connections. Each time a client such as a browser attempts to open a connection, information is stored on the server. Since this takes up memory and operating system resources, the number of in-progress connections allowed is limited, usually fewer than ten. The server then sends a response to the client, which sends an acknowledgement back, and the connection is established. At this point the queued resources are freed to accept other connections.

During an attack, the attacking software generates spoofed packets that appear to the server to be valid new connections. These packets enter the queue, but the connection is never completed—leaving false connections in the queue until they time out. The system under attack quits responding to new connections until after the attack stops.

ICMP attacks use network devices like routers to send error messages when a requested service is not available or the remote server cannot be reached. Examples of ICMP attacks include ping floods, ping-of-death attacks, and smurf attacks.

Ping floods send ICMP packets rapidly without waiting for replies, overwhelming their victims with the ICMP echo reply packets they are sending back.

Ping-of-death attacks are oversized ICMP packets sent in a fragmented fashion. When the targeted server reassembles these fragments, the packets become larger than the maximum allowed packet size and cause the server to crash due to overflow of memory buffers.

Smurf attacks involve spoofing ICMP packets with the victim's source address and broadcasting to a computer network. All the devices on the network respond to these packets and the responses flood the victim server.

DNS-based exploits make use of software bugs in protocol parsing and processing implementation to exploit vulnerabilities in DNS server software. By sending malformed DNS packets to the targeted DNS server, the attacker can cause the server to stop responding or crash.

DNS cache poisoning involves inserting a false address record for an Internet domain into the DNS query. If the DNS server accepts the record, subsequent requests for the address of the domain are answered with the address of a server controlled by the attacker. For as long as the false entry is cached, incoming web requests and emails will go to the attacker's address. New cache-poisoning attacks such as the "birthday paradox" use brute force, flooding DNS responses and queries at the same time, hoping to get a match on one of the responses and poison the cache.

Protocol anomalies send malformed DNS packets, including unexpected header and payload values, to the targeted server, causing it to stop responding or to crash by causing an infinite loop in server threads. These sometimes take the form of impersonation attacks.

Reconnaissance consists of attempts to get information on the network environment before launching a large DDoS or other type of attack. Techniques include port scanning and finding versions and authors. These attacks exhibit abnormal behavior patterns that, if identified, can provide early warning.

DNS tunneling involves tunneling another protocol through DNS port 53—which is allowed if the firewall is configured to carry non-DNS traffic—for the purposes of data exfiltration. A free ISC-licensed tunneling application for forwarding IPv4 traffic through DNS servers is widely used in this kind of attack.

The Inadequacies of Existing Security Measures

Some security solutions do exist that claim to offer protection for DNS, but the truth is that they are limited in what they can and cannot protect against. Most of them are external solutions that are "bolted on" as an afterthought rather than built from the ground up to secure DNS against attacks. The solutions use approaches such as overprovisioning, deep packet inspection, generic DDoS protection, simple rate limiting, and cloud delivery.

Approach 1: Overprovisioning.

Technologies like load-balancers can be made to respond to a DDoS attack by increasing the capacity of the network and hoping that the attack will stop at some point. This approach will not be able to keep up with the rapidly increasing size of DDoS attacks, and furthermore, it can't be used to monitor bad or malformed DNS traffic.

Approach 2: Deep Packet Inspection.

Next-generation firewalls and IPS devices offer some protection against common vulnerabilities and basic layer-3 DDoS. However, they do not have the ability to detect or mitigate DNS-specific protocol anomalies or DNS-based attacks. They require extremely high compute performance to accurately detect DNS-based attacks, making deep inspection an impractical approach in terms of cost and the number of distribution points that are needed.

Approach 3: Generic DDoS Protection.

These solutions cover a broad range of DDoS attacks, but contain no deep understanding of DNS-based attacks.

Approach 4: Cloud-based Solutions.

Cloud solutions focus on volumetric attacks only with no protection against malformed DNS and other types of attacks. They also raise privacy concerns[3], they can be bypassed[4], and they could result in latency issues.

Approach 5: Simple Response-Rate Limiting (RRL).

Simple RRL with no intelligence is a one-size-fits-all approach to setting a threshold that can lead to legitimate traffic being dropped. Different sources of DNS traffic might have different requirements. For example, a downstream DNS caching server might generate 100 times base traffic compared to a normal desktop source, and this traffic might be legitimate. An HTTP or email proxy server has a higher DNS traffic pattern. So simple rate limiting will generate too many false positives, which means employees and customers might not be able to access resources during a determined DDoS attack.

Closing the Gap with Comprehensive Threat Protection from Infoblox

There is currently only one effective way to address these DNS threats to your network security: directly from within the DNS servers themselves. Infoblox can help you do that because we have deep knowledge of the DNS protocol and our servers are the ones responding to the DNS requests.

Infoblox Advanced DNS Protection delivers a unique approach to protecting against DNS-based attacks. It intelligently distinguishes legitimate traffic from attack traffic and automatically drops malicious DNS traffic while responding to legitimate traffic. In addition, Advanced DNS Protection receives automatic updates based on threat analysis and research, delivering protection against new and emerging attacks. The capabilities of the solution are described below.

The Fortified DNS Server—the Best Protection Against DNS-based Attacks

The Infoblox Advanced Appliance is a fortified DNS server with security built in. It can be configured as an external authoritative server or a DNS recursive server to protect against external or internal attacks. The Advanced Appliance uses next-generation programmable processors to provide dedicated compute for threat mitigation. There is no better way to protect the network against DNS-based attacks than with a DNS server.

Unique Detection and Mitigation

Advanced DNS Protection continuously monitors, detects, and drops packets of DNS-based attacks—including amplification, reflection, floods, exploits, tunneling, cache poisoning, and protocol anomalies—and mitigates them while responding to legitimate traffic. This provides critical DNS services even when under attack. The system also receives automatic updates based on threat analysis and research to provide protection against new and evolving DNS attacks as they emerge.

Centralized Visibility of Attacks

Through comprehensive reports, Advanced DNS Protection gives you a centralized view of attacks that have happened on your network and provides the intelligence you need to take action. These reports include details like number of events by category, rule, severity, member-trend analysis, and time-based analysis. They can be accessed through the Infoblox Reporting Server.

Tunable for Your Unique Needs

Every enterprise has different DNS traffic-flow patterns, and they can vary based on seasonality, time of day, or geography. For example, an online retail site can expect much higher levels of DNS traffic on Cyber Monday and during the holiday shopping season than a small bank might. An acceptable rate limit for the retail site might be an unusual rate limit for the bank. Advanced DNS Protection provides tunable traffic thresholds that you set, enabling you to fine-tune protection parameters based on your unique DNS traffic-flow patterns. This enables you to respond to good traffic without issues while blocking or dropping malicious traffic.

A Deep Dive into the Effectiveness of Infoblox Advanced DNS Protection

No single approach can protect against the many and varied techniques used to exploit DNS servers, so Infoblox Advanced DNS Protection combines a range of specific technological responses.

- **Smart rate thresholds** can put the brakes on DNS DDoS and flood attacks—without denying services to legitimate users. Smart rate thresholds use Advanced DNS Protection's ability to discriminate between different query types and rates associated with them. For example, a downstream DNS caching server might generate 100 times base traffic compared to a normal desktop source, and this traffic might be legitimate. An HTTP or email proxy server has a higher DNS traffic demand, which is legitimate.

  - **Source-based throttling** detects abnormal queries by source and causes brute-force methods to fail.
  - **Destination-based throttling** detects abnormal increases in traffic grouped by target domains.
- **Next-generation programmable processors** provide high-performance filtering of traffic, making it possible to drop malicious traffic and respond to legitimate queries.
- **Detecting reconnaissance activity and reporting it** can help identify attacks and allow network teams to prepare for them before they are even launched.
- **Analyzing packets for patterns of exploits that target specific vulnerabilities** makes it possible to stop some attacks before they reach the DNS software.
- **Centralized visibility and reporting** enable network teams to recognize attacks happening in different parts of the network. This provides a big-picture view and gives information on the scope and severity of the attacks so that appropriate action can be taken.
- **Ongoing protection through automatic updates from Infoblox** ensures that Advanced DNS Protection evolves to handle the changing threat landscape.
- **Advanced DNS Protection is a DNS server**, and it will NOT process bad traffic, unlike inline devices that do not have the intelligence or knowledge about DNS traffic.

All of these techniques contribute to the same outcome: continuing to provide resilient DNS services even when under attack.

Is It Time to Plug the DNS Security Hole in Your Network?

What we hope we've done with this white paper is raise your awareness of the seriousness of DNS vulnerability and convince you that the health and well-being of your network could very well depend on how soon you round out your security measures with DNS-specific protection.

Security built in is better than security bolted on. There is no better place to defend against DNS-exploiting techniques than within the DNS servers that are its targets. And the only solution built with these facts in mind is Infoblox Advanced DNS Protection. Contact us today to find out more about this critical shield against the most dangerous threats your network faces.

About Infoblox

Infoblox (NYSE:BLOX) helps customers control their networks. Infoblox solutions help businesses automate complex network control functions to reduce costs and increase security and uptime. Our technology enables automatic discovery, real-time configuration and change management and compliance for network infrastructure, as well as critical network control functions such as DNS, DHCP, and IP address management (IPAM) for applications and endpoint devices. Infoblox solutions help over 6,700 enterprises and service providers in 25 countries control their networks.

---

1 Prolexic Quarterly Global DDoS Attack Report , Q1 2013
2 http://openresolverproject.org/
3 http://www.renesys.com/2013/10/google-dns-departs-brazil-ahead-new-law/
4 http://www.crn.com/news/security/240159295/cloud-based-ddos-protection-is-easily-bypassed-says-researcher.htm

CORPORATE HEADQUARTERS:

+1.408.986.4000

+1.866.463.6256

(toll-free, U.S. and Canada)

info@infoblox.com

www.infoblox.com

EMEA HEADQUARTERS:

+32.3.259.04.30

info-emea@infoblox.com

APAC HEADQUARTERS:

+852.3793.3428

sales-apac@infoblox.com