Infoblox
CONTROL YOUR NETWORK

WHITE PAPER

The New Standard in DNS Security

Understanding Threats and Using a Comprehensive Approach for Securing DNS

Overview

The Domain Name System (DNS) is mission-critical infrastructure that all organizations use and cannot function without. Yet DNS remains a vulnerable component in the network that is frequently used as an attack surface and inadequately protected by traditional security solutions. When critical DNS services are compromised, it can result in catastrophic network and system failure.

Your external (Internet-facing) DNS servers may be subject to cyberattacks such as DNS DDoS, exploits, and reconnaissance, leading to degraded performance and downtime. But threats are not always outside your firewalls. Today's targeted attacks pose risks to both data and infrastructure inside your enterprise. You could have an endpoint infected with malware or an advanced persistent threat (APT) trying to communicate with command-and-control (C&C) servers using DNS. You could have a malicious insider trying to steal sensitive information by opening a DNS tunnel or embedding data in DNS queries.

These security challenges mandate the need for DNS security solutions designed specifically for the two use cases—external and internal—and a solution that can offer protection for the DNS server itself while using the unique position of DNS in the network as an optimal enforcement point for protection and threat response.

This white paper gives you an overview of how you can secure external DNS from cyberattacks and secure internal DNS from malware that exploits DNS and prevent data exfiltration via DNS.

Threats to External DNS Infrastructure

External DNS servers are referred to as "authoritative" servers. Their job is to answer external queries from anyone trying to connect to your company network—for example, to send email or visit your website. Authoritative servers must be available 100 percent of the time, or your company will disappear off the Internet.

These external or Internet-facing DNS servers are subject to a variety of attacks, including DNS reflection, amplification, protocol anomalies, exploits, and reconnaissance. DNS is the number-one protocol used in reflection/amplification attacks (84 percent) according to Arbor Network's 2016 Worldwide Infrastructure Security report.

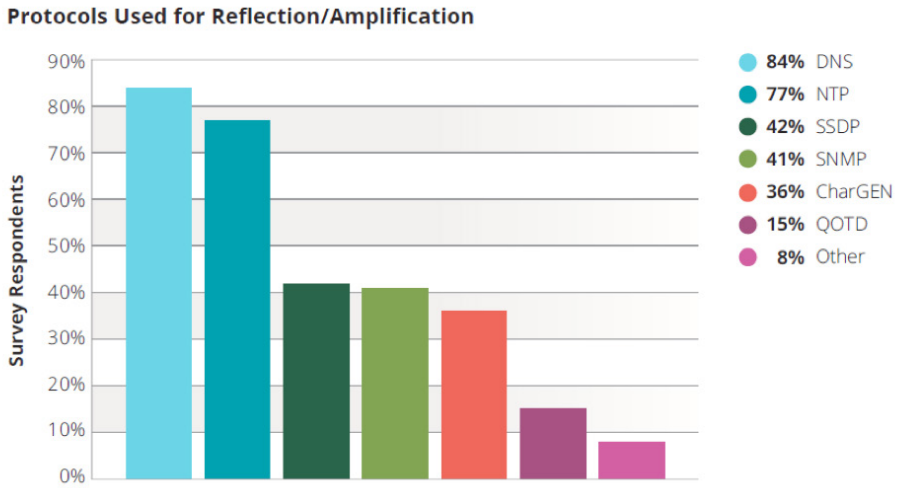

Figure 1: Protocols used for reflection/amplification

Source: Arbor Networks, Inc.

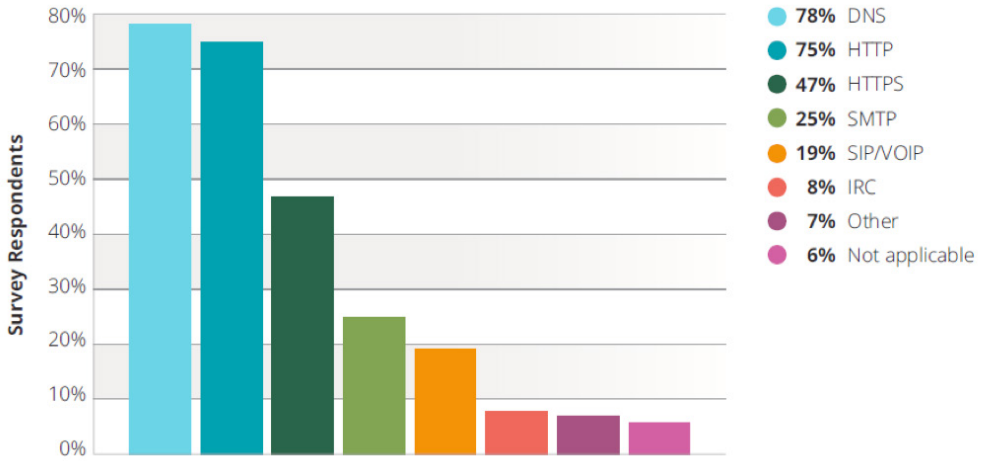

Figure 2: Targets of application-layer attacks
Source: Arbor Networks, Inc.

Also according to the same report, DNS is the top targeted service of application-layer DDoS attacks.

Reflection and amplification attacks are the top threats to external DNS. These attacks leverage inherent weaknesses in the DNS protocol (for example, its use of connectionless UDP) to inundate a server with unexpected responses it must process. Top industries targeted include gaming, software, technology, telecommunications, media, and financial services.

These attacks can also be part of a smoke-screening effort—a common tactic used by malicious actors who try to distract the organization with a DDoS attack on external DNS while data theft and deeper infiltration are happening elsewhere on the network. Attacks such as these are often launched by someone with an ax to grind—such as hacktivists, unscrupulous competitors, or hostile governments.

Business impact: If your Internet-facing DNS inadvertently takes part in a reflection/amplification attack, you could end up with unwanted publicity and brand damage. If your Internet-facing DNS is the target of volumetric attacks or protocol exploits or anomalies, it could cause your server to slow down and eventually crash—effectively disconnecting your business from the Internet and resulting in service disruption, direct loss of revenue, and expenses for bringing the servers back up.

DNS Hijacking

DNS hijacking compromises the integrity of DNS and redirects users who are trying to access a website to a bogus site controlled by the hijackers, which may look like the real thing. The hackers can then acquire user names, passwords, and other sensitive information. For businesses, DNS hijacking could again mean direct loss of revenue and negative brand impact. According to a recent article in *SC Magazine,* a DNS security survey of 300 IT decision-makers in the U.S. and U.K. in November 2014 showed that 33 percent had been targets of DNS hijacking.

Threats to Data and Internal DNS Infrastructure

Threats to internal DNS are manifold:

- DNS-exploiting malware can communicate with C&C servers.
- Data exfiltration via DNS can result in loss of sensitive data such as credit-card information, social-security information, or company financials.

Malware Exploiting DNS

According to the Cisco 2016 Security Report, 91% of malware uses DNS to carry out campaigns. Malware is increasingly becoming more sophisticated and using DNS to communicate with C&C servers, making it harder to detect with traditional tools. Proliferation of BYOD devices and mobile users means that threats can be inside the firewall, not just outside.

Techniques such as fast flux—in which malicious domains rapidly change their identity and IP addresses to avoid detection by traditional security solutions—and domain-generation algorithm (DGA)—in which malware randomly generates a large number of domain names and attempts communications to some of these domains to receive updates or commands—are much harder to detect and take down. In addition, threat response time is often too long, and finding infected devices can be challenging.

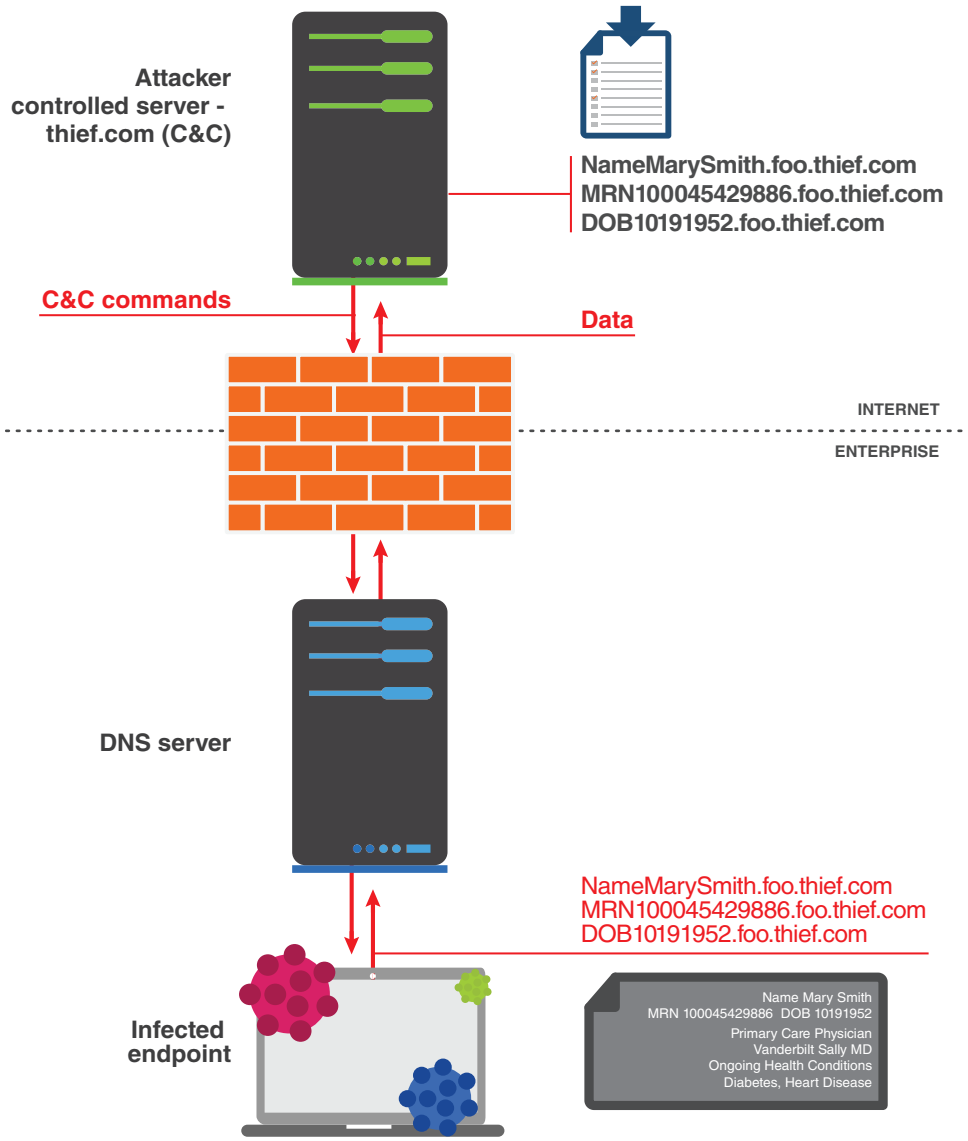

Figure 3: Data exfiltration via DNS using host and subdomain records

Business impact: If malware spreads inside the network, sensitive data can be stolen, which could even lead to the theft of millions of dollars, if the organization is a financial institution. As a case in point on the financial impact of ransomware, the FBI, quoted in the *Financial Times,* reported that organizations payed out over $209 million USD in ransom just in the first quarter of calendar year 2016 to get back their data, as compared to $24 million USD in all of 2015. Another example is a botnet that was responsible for theft of hundreds of millions of dollars in 2014—GameOver Zeus (GOZ).

Data Exfiltration via DNS

DNS is increasingly being used as a pathway for data exfiltration either unwittingly by malware-infected devices or intentionally by malicious insiders. DNS tunneling involves tunneling IP protocol traffic through DNS port 53—which is often not even inspected by firewalls, even next-generation ones—for the purposes of data exfiltration. A freeware tunneling application released under the ISC license for forwarding IPv4 traffic through DNS servers is one example of the software used in this kind of attack.

Sensitive information such as credit-card numbers, company financials, or SSNs is being stolen either by establishing a DNS tunnel from within the network or by encrypting and embedding chunks of that data in DNS queries. Data can be decrypted at the other end and put back together to get the valuable information.

According to the same DNS security survey mentioned in *SC Magazine*, 46 percent of respondents experienced DNS exfiltration and 45 percent experienced DNS tunneling.

Infoblox Advanced DNS Protection for Comprehensive Protection of External DNS

Some security solutions claim to offer protection for DNS, but the truth is that they are limited in what they can 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 most effective way to address these threats to DNS is to have intelligent detection capabilities built into the DNS servers themselves.

Addressing Availability of External (Internet-facing) DNS

Infoblox Advanced DNS Protection is a purpose-built external DNS server that provides defense against the widest range of DNS-based cyberattacks such as volumetric, exploits, and reconnaissance attacks. It continuously monitors, detects, and mitigates DNS attacks while responding only to legitimate queries. Moreover, it uses Infoblox Threat Adapt™ technology (threat feeds) to automatically update its defense against new and evolving threats as they emerge, without the need for patching. Hardware-accelerated DNS DDoS mitigation maintains system integrity and availability even under extreme attack.

Methods for protection:

- **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 normal rates associated with them.
  - **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.

- **Automatic blacklisting of non-responsive and misbehaving servers and zones** helps avoid too many outstanding queries to misbehaving and dead domains.
- **Dynamic blocking of clients** that generate too many NXDOMAIN, NXRRset, or ServFail responses prevents misbehaving clients from bringing down the DNS server.
- **Next-generation programmable processors** provide high-performance filtering of traffic, making it possible to drop malicious traffic before it reaches the DNS server application.
- **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.

Addressing Integrity of External DNS

Infoblox Advanced DNS Protection maintains the integrity of DNS records by performing periodic integrity checks, ensuring that any compromise to the records by DNS hijacking is eliminated.

Global Visibility of Attacks with Reporting

Through comprehensive reports and alerts, Advanced DNS Protection provides detailed views on attack points across the network and attack sources, providing the intelligence needed to take action. The reports can be accessed through the Infoblox Reporting Analytics Server.

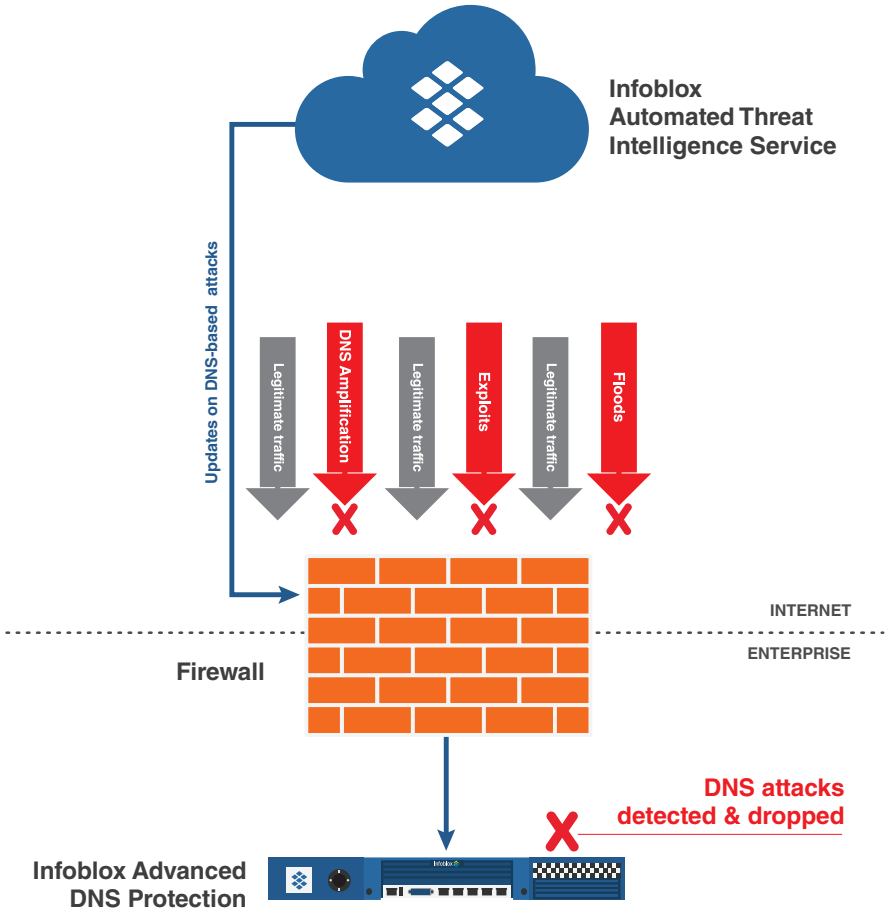

Figure 4: : Advanced DNS Protection with threat intelligence providing protection against attacks

Infoblox DNS Firewall for Malware Containment and Control and Data Exfiltration Prevention

Infoblox DNS Firewall stops malware from exploiting DNS and prevents data exfiltration, and protects mission-critical DNS infrastructure from attacks—all without the need for endpoint agents or changes to your network architecture. Unlike alternative solutions, it combines enterprise-grade DNS with the Infoblox automated threat intelligence feed to provide ongoing protection against new and evolving threats. The unique position of DNS in the network makes it the optimal enforcement point for protection and response.

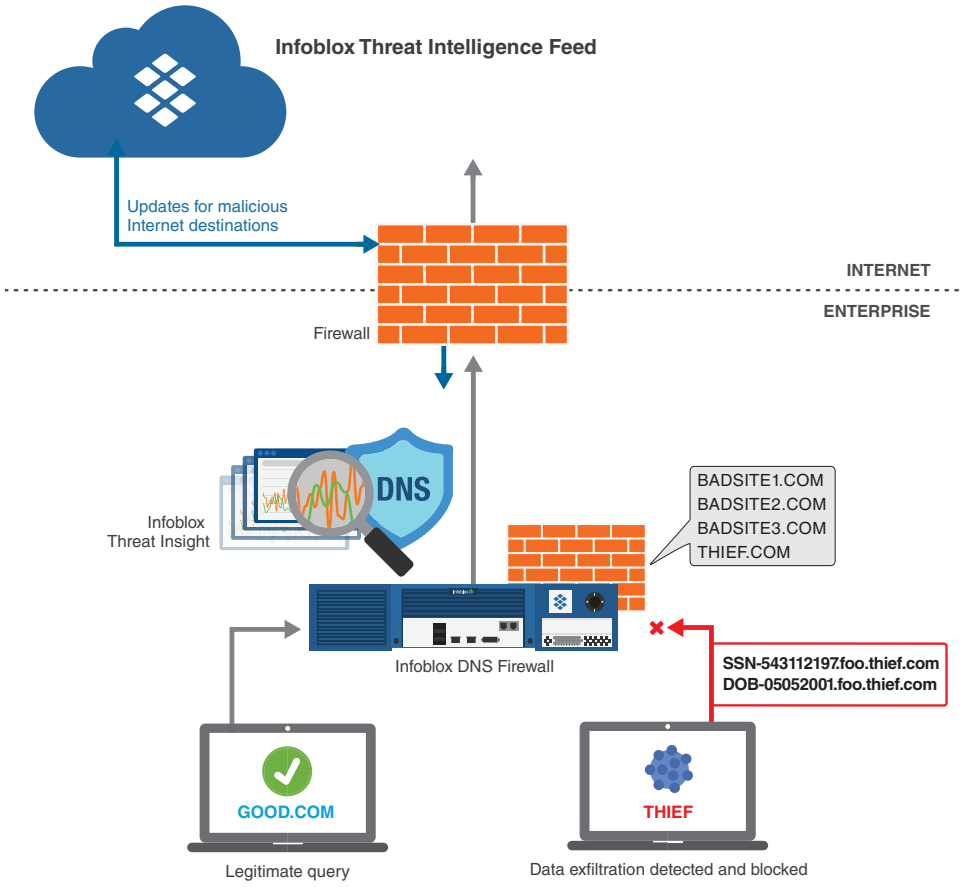

Figure 5: DNS Firewall helps prevent malware communications and data exfiltration using an automated threat intelligence feed and Infoblox Threat Insight.

Malware Containment and Control

Infoblox DNS Firewall contains and controls malware communication with external C&C servers and botnets by intercepting DNS queries associated with malware. It works by employing DNS Response Policy Zones (RPZs) and threat intelligence on known malicious destinations for effective protection. The Infoblox Threat Intelligence Feed constantly updates the blacklist of known malicious destinations. In addition it enables faster response by pinpointing the infected devices for remediation through collaboration with Infoblox DHCP for device fingerprinting.

Infoblox DNS Firewall also easily integrates and works with other security solutions such as from FireEye, Cisco and Carbon Black for enabling automated threat response and faster containment. Furthermore, Infoblox support for REST API, STIX™/TAXII™ and Cisco pxGrid simplifies integration with third-party technologies.

Data Exfiltration Prevention

DNS Firewall leverages the optional add-on Infoblox Threat Insight to help prevent data exfiltration. Threat Insight is a unique software technology that does streaming analytics on DNS queries to detect data exfiltration. The analytics model examines host.subdomain and TXT records in DNS queries, and uses entropy, lexical methods, time series, n-gram analysis and other proprietary factors to determine presence of data in queries. Once it classifies a request as data exfiltration, the destination associated with the data exfiltration is added to a special RPZ zone that contains the usual block, log, or redirect policy. It not only adds the special RPZ zone to the member running Threat Insight, but to all Infoblox Grid members running DNS Firewall, thereby scaling protection.

Methods for securing data and internal DNS infrastructure:

- **Disrupting malware communication channels** with C&C sites provides defense-in-depth against infections and stops propagation of malware inside the network.
- **Preventing loss of sensitive information via DNS through use of behavioral analysis** complements the reputation feed for defense-in-depth.
- **Contextual reporting** provides detailed views of attack points and endpoints infected by APTs and malware, using drill-down analytics to enable timely incident response.

Summary

DNS is critical network infrastructure that is too valuable to be vulnerable. Since DNS has not been adequately protected by organizations in the past, targeted attacks use it to their advantage. Infoblox has the most comprehensive DNS security portfolio in the market today. By implementing the right DNS security solutions, and by using the unique position of DNS in the network, you can convert your DNS servers from Achilles' heels to network security assets, thereby helping to improve your organization's security posture.

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