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 infrastructure attacks, APTs, and malware that exploit DNS, and from 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 (81 percent) according to Arbor Network’s 2015 Worldwide Infrastructure Security report.
Also according to the same report, DNS tied with HTTP for 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
Internal DNS Servers are typically recursive and are close to the endpoints inside the network, like laptops, mobile devices, servers etc. In some cases, internal DNS servers might be configured to be authoritative to queries from inside the network.

Threats to internal DNS are manifold:

- Infrastructure attacks can result in catastrophic network and system failure.
- DNS-exploiting APTs and malware can communicate with C&C servers.
- Data exfiltration via DNS can result in loss of sensitive data such as personally identifiable information (PII), regulated data, intellectual property, credit-card information, or company financials.

Internal Infrastructure Attacks
Your internal DNS servers are also potential victims of infrastructure attacks. The larger the enterprise, the more endpoints there are inside that may become compromised and be forced to participate in these attacks. Unfortunately, Internal DNS DDoS attacks have been on the rise. A big healthcare company recently experienced a flood attack on its internal DNS servers with a million queries per second. These volumetric floods can overwhelm an internal DNS server, causing slow performance and eventual failure. A large computer-storage company also had an internal DNS outage for four hours that caused its employees to be sent home.

Additionally, there are more sophisticated and stealthier attacks that stay under the radar and exhaust resources on recursive servers. Attackers are using advanced techniques ranging from simple NXDOMAIN attacks to highly sophisticated DDoS attacks involving botnets, chain reactions, and misbehaving domains. The impact on recursive servers includes resource exhaustion, cache saturation, and outbound bandwidth congestion. The external authoritative server of the target domain suffers DDoS.

Business Impact: Internal DNS attacks can lead to lost productivity, business downtime, and increased operational expenses.

APTs and Malware Exploiting DNS
According to the Cisco 2014 Security Report, 100 percent of business networks analyzed by Cisco had traffic going to websites that host malware. APTs are increasingly becoming more sophisticated and using DNS to communicate with C&C servers, making them 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.

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. One such example of a botnet that was responsible for theft of hundreds of millions of dollars last year is GameOver Zeus (GOZ).
Data Exfiltration via DNS

Theft of sensitive or regulated data and intellectual property is one of the most serious risks to an enterprise. DNS is increasingly being used as a pathway for data exfiltration either unwittingly by malware-infected devices or intentionally by malicious insiders. According to the same DNS security survey mentioned in SC Magazine, 46 percent of respondents experienced DNS exfiltration and 45 percent experienced DNS tunneling.

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. There are several popular tunneling toolkits such as Iodine, which is often considered the gold standard, OzymanDNS, SplitBrain, DNS2TCP, TCP-over-DNS, and others.

Sensitive information such as credit-card numbers, company financials, or SSNs can be stolen by one of two methods: by establishing a DNS tunnel from within the network using standard toolkits, or by encrypting and embedding chunks of sensitive data directly in DNS queries. In the second method, data can be decrypted at the other end and put back together to get the valuable information. This second method might not use well-established signatures and might be low and slow and harder to detect.

Figure 3: Data exfiltration via DNS using host and subdomain records
Infoblox External DNS Security 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 External DNS Security 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 External DNS Security’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 External DNS Security 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, External DNS Security 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 Server.
Infoblox Internal DNS Security for Securing Internal DNS and Leveraging DNS for Expanded Network Protection

Infoblox Internal DNS Security protects mission-critical DNS infrastructure from attacks, stops APTs and malware from exploiting DNS, and uses Infoblox DNS Threat Analytics to prevent data exfiltration—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.
Providing Resilient Network Infrastructure

Internal DNS Security provides defense against DNS/DHCP attacks to maximize service availability. It continuously monitors, detects, and drops DNS/DHCP attacks such as DNS DDoS, exploits, cache poisoning, DNS tunneling, and malformed DHCP requests. Hardware-accelerated attack mitigation maintains system integrity and availability even under extreme attack.

Protection against APT/Malware

Infoblox Internal DNS Security disrupts APT and 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. 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 Internal DNS Security also easily integrates and works with other security solutions such as FireEye NX series. It integrates with industry-standard ecosystems for information sharing and centralized threat mitigation.
Protection against Data Exfiltration
Internal DNS Security prevents the loss of sensitive information through DNS by detecting and stopping exfiltration of sensitive data tunneled via DNS. Most standard DNS tunneling toolkits (like Iodine) have well known signatures, which can be used to create protection rules. Internal DNS Security has 12 different threat protection rules that use these signatures to detect tunneling attempts. As new signatures become available, customers get automatic updates through the threat intelligence service.

In addition, Internal DNS Security uses the optional patented Infoblox DNS Threat Analytics module to automatically detect and block sophisticated data exfiltration attempts that encrypt and embed data directly in DNS queries. It uses real-time streaming analytics of live DNS queries and machine learning to accurately detect presence of data in DNS queries.

Methods for securing data and internal DNS infrastructure:

- **Deep inspection of DNS/DHCP traffic** to continuously monitor, detect, and drop DNS/DHCP attacks inside the network provides reliable and resilient internal DNS/DHCP services. It blocks DNS tunneling attempts. In addition, it prevents DNS from being used to attack other network components, turning DNS into an asset for expanded network protection.
- **Disruption of APT and malware communication channels** with C&C sites provides defense-in-depth against infections and stops propagation of malware inside the network.
- **Real-time streaming analytics of live DNS queries** detects data exfiltration by examining host.subdomain and TXT records in DNS queries.
- **Active blocking of data exfiltration attempts** is achieved by automatically adding destinations associated with data exfiltration to the blacklist and scaling protection through Grid-wide update.
- **Contextual reporting and visibility** provide detailed views of attack points and infected endpoints with Infoblox Identity Mapping and drill-down analytics. This helps to quickly identify endpoints and/or rogue employees trying to steal data.

Automating Threat Response through Integrations
While detection and blocking of malicious activity are critical, it is also important to ensure fast remediation of infected devices. This can be achieved by tighter integration between detection technologies and endpoint remediation solutions. Infoblox integrates with leading endpoint solutions such as Bit 9 + Carbon Black to provide indicators of compromise such as an endpoint trying to exfiltrate data. Using this intelligence, Carbon Black automatically bans the malicious processes from future execution and connection, thereby effectively quarantining the infected endpoint and preventing data from being exfiltrated, even if the device is outside the enterprise.

In addition, Infoblox exchanges valuable network and security event information with Cisco Identity Services Engine (ISE) to automate security response and timeliness. Infoblox sends “early warning” of compromised devices trying to exfiltrate data to Cisco ISE through Cisco pxGrid. That information can then be sent to the organization’s security architecture for quarantine.

Finally, Infoblox provides robust restful APIs, which can be used to enrich your SIEM or user behavior analytics tools with additional contextual data such as user name, MAC address, IPAM record, and more.
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.

About Infoblox

Infoblox delivers critical network services that protect Domain Name System (DNS) infrastructure, automate cloud deployments, and increase the reliability of enterprise and service provider networks around the world. As the industry leader in DNS, DHCP, and IP address management, the category known as DDI, Infoblox (www.infoblox.com) reduces the risk and complexity of networking.