Protection against the
Widest Range of DNS Attacks

DNS: One of the Fastest Growing Attack Vectors

Security, availability, and integrity are the top three concerns regarding DNS infrastructure. Attackers seek weakest links and pressure points to harm or illegally exploit businesses, and by its very nature, the Domain Name System (DNS) protocol is easy to exploit. As a result, cyber attacks on DNS are on the rise.

DNS distributed denial of service (DDoS) attacks are designed to bring down DNS servers and consume network resources, thereby interfering with critical IT applications such as email, web sites, VoIP, and software as a service (SaaS). In the last year alone, DNS attacks have increased by more than 216 percent. The damage is costly, and Forrester Research estimates upward of $100,000 an hour as the cost resulting from a DDoS attack, not including customer defection and damage to brands.

DNS hijacking compromises the integrity of DNS and redirects users to a bogus site controlled by attackers, resulting in theft of sensitive information and loss of revenue. DNS-based attacks are also used as diversions in broader plans to steal data, a practice called “smoke screening.”

Mitigating the Problem with Infoblox External DNS Security

Infoblox External DNS Security provides defense against the widest range of DNS-based attacks such as volumetric attacks, exploits, NXDOMAIN, and DNS hijacking attacks. Unlike approaches that rely on infrastructure over-provisioning or simple response-rate limiting, External DNS Security intelligently detects and mitigates DNS attacks while responding only to legitimate queries. Moreover, it uses Infoblox Threat Adapt™ technology to automatically update its defense against new and evolving threats as they emerge, without the need for patching.

Key Features

- Protection against the widest range of attacks: Continuously monitor, detect, and drop all types of DNS attacks, including volumetric and exploit attacks, and maintain DNS integrity.
- Infoblox Threat Adapt™ technology: Automatically update protection against new and evolving threats using the latest threat intelligence, and morph protection to reflect changes in DNS configuration—all without downtime or patching.
- Global visibility of attacks: Stay on top of attack types and sources.
- Tunable traffic thresholds: Fine-tune protection parameters.
- Enhanced processing: Leverage next-generation programmable processors to provide dedicated compute for threat mitigation.
- An extensive family of hardened appliances: Choose the appliance that fits your network environment.
- POC/trial: Deploy in line in monitor mode to detect and monitor attacks without actually blocking, or deploy out of band using port mirroring to detect attacks.
- Patented Infoblox Grid: Automate all appliance configurations and updates, enabling rapid, automated security policy rollout to all Infoblox Advanced Appliances.
**Solution Components**
- **Infoblox Advanced Appliance**: A DNS server that is purpose built with security in mind.
- **Infoblox External DNS Security Service**: The software with Threat Adapt technology to provide ongoing protection against existing and new threats to the DNS server.

**The Fortified DNS Server: The Best Protection against DNS-based Attacks**

The Advanced Appliance is a fortified DNS server with security built in. It leverages dedicated compute to filter out attacks before they reach the DNS server or application.

**Protection against the Widest Range of Attacks**

External DNS Security continuously monitors, detects, and drops various types of DNS attacks—including volumetric attacks such as floods and NXDOMAIN and non-volumetric attacks such as exploits and anomalies—while responding to legitimate queries. It maintains DNS integrity, which can be compromised by DNS hijacking attacks.

**Infoblox Threat Adapt™ Technology**

External DNS Security uses Infoblox Threat Adapt technology to keep the protection updated automatically against new and evolving threats as they emerge. Threat Adapt uses independent analysis and research on evolving attack techniques, including what we have seen in customer networks, to update protection, and it automatically morphs protection to reflect DNS configuration changes.

**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.

**Quick Deployment**

External DNS Security is fast and easy to get up and running. Once installed, it starts blocking attacks immediately—even if an attack is already in progress.
## Summary of Attack Types Protected against by External DNS Security

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS reflection/DrDoS attacks</td>
<td>Volumetric</td>
<td>Using third-party DNS servers (open resolvers) to propagate a DoS or DDoS attack</td>
</tr>
<tr>
<td>DNS amplification</td>
<td>Volumetric</td>
<td>Using a specially crafted query to create an amplified response to flood the victim with traffic</td>
</tr>
<tr>
<td>TCP/UDP/ICMP floods</td>
<td>Volumetric</td>
<td>Denial of service on layer 3 by bringing a network or service down by flooding it with large amounts of traffic</td>
</tr>
<tr>
<td>NXDOMAIN</td>
<td>Volumetric</td>
<td>Flooding the DNS server with requests for non-existent domains, causing cache saturation and slower response time</td>
</tr>
<tr>
<td>Random sub-domain (slow drip attacks) Domain lock-up attacks Phantom domain attacks</td>
<td>Slow-volume stealth</td>
<td>Flooding the DNS server with requests for phantom or misbehaving domains that are set up as part of the attack, causing resource exhaustion, cache saturation, outbound query limit exhaustion, and degraded performance</td>
</tr>
<tr>
<td>DNS-based exploits</td>
<td>Exploits</td>
<td>Attacks that exploit vulnerabilities in the DNS software</td>
</tr>
<tr>
<td>DNS cache poisoning</td>
<td>Exploits</td>
<td>Corruption of the DNS cache data with a rogue address</td>
</tr>
<tr>
<td>Protocol anomalies</td>
<td>Exploits</td>
<td>Causing the server to crash by sending malformed packets and queries</td>
</tr>
<tr>
<td>Reconnaissance</td>
<td>Exploits</td>
<td>Attempts by hackers to get information on the network environment before launching a large DDoS or other type of attack</td>
</tr>
<tr>
<td>DNS hijacking</td>
<td>Exploits</td>
<td>Attacks that modify the parent/ registrar DNS records to point to a rogue DNS server</td>
</tr>
</tbody>
</table>
Infoblox External DNS Security

Infoblox Threat-rule Server

Automatic Updates (Threat Adapt)

Grid Master

Infoblox External DNS Security

Grid-wide rule distribution

Data for Reports

Reporting Server

Reports on attack types, severity
Delivery Options

Advanced Appliances Come in Three Physical Platforms

The Advanced Appliances have next-generation programmable processors that provide dedicated compute for threat mitigation. They offer both AC and DC power supply options. PT-4000 comes in 1-GigE and 10-GigE options.

PT-1400

PT-2200

PT-4000

About Infoblox

Infoblox (NYSE:BLOX), headquartered in Santa Clara, California, delivers network control solutions, the fundamental technology that connects end users, devices, and networks. These solutions enable more than 7,000 enterprises and service providers around the world to transform, secure, and scale complex networks. Infoblox (www.infoblox.com) helps take the burden of complex network control out of human hands, reduce costs, and increase security, accuracy, and uptime.

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