Detect DNS Attacks with Advanced DNS Protection POC

Summary
Infoblox Advanced DNS Protection provides defense against the widest range of DNS-based attacks such as floods, reflection amplification, NXDOMAIN, DNS hijacking, and exploits. It intelligently detects and drops the attacks while responding only to the legitimate queries. The Infoblox Advanced DNS Protection Proof of Concept (POC) allows you to utilize and evaluate the attack detection capabilities for 60 days. For POCs, Advanced DNS Protection can be deployed either in monitor mode or out of band with port mirroring to detect attacks without actually blocking them.

Detect DNS DDoS, Exploits, and Much More
DNS DDoS attacks are constantly on the rise as attackers seek weakest links in IT infrastructures to cause damage. More than 75 percent of organizations in the U.S. and U.K. have experienced at least one DNS attack according to SC Magazine. 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.

To easily detect these attacks that could be targeting your external authoritative server, you can deploy Infoblox Advanced DNS Protection, a DNS server with intelligence built in to detect attacks, in two different modes, both of which are non-disruptive to your production traffic.

POC Option 1: Monitor Mode
Replace your external server with Advanced DNS Protection in monitor mode. This allows the server to detect incoming attacks such as DNS DDoS, NXDOMAIN, exploits, and reflection/amplification attacks. Deploying in monitor mode will not block the attack traffic, giving you the option to review the attacks before taking action.

To block attacks, you can turn off monitor mode.

POC Option 2: Port Mirroring Mode
If you don’t want to replace your existing DNS server just yet, Advanced DNS Protection can be attached to the span port of the incumbent external DNS server to analyze real-time DNS traffic without being in line with production traffic. This will again allow the server to detect incoming attacks such as DNS DDoS, exploits, and floods, without blocking them. Monitor mode is not required for this configuration.

To block attacks, you will have to deploy Advanced DNS Protection in line and make sure that monitor mode is turned off.
Temporary License

In both options, the Advanced DNS Protection POC hardware is shipped with a temporary license to enable the threat-protection features automatically. The license expires after 60 days.

Global Visibility of Attacks with Reports

Once the Advanced DNS Protection POC is deployed and the threat-rule parameters are fine-tuned, you can start seeing any attacks that hit the server through widgets, logs, and reports. The Threat Protection Statistics Widget on the Infoblox UI displays statistics about attack events by severity.

Figure 1: Infoblox Advanced DNS Protection provides unique protection against DNS-based attacks.
Reports provide intelligence on attacks that hit Advanced DNS Protection. They provide visibility into source, scope, and severity of attacks and allow for easy identification and isolation of issues for corrective action. These reports can be accessed using the Infoblox Reporting and Analytics server.

**Detect Malware and APTs with DNS Firewall**

According to the Cisco 2014 Security Report, 100 percent of business networks analyzed by Cisco have suspicious traffic going to websites that host malware. In spite of using the latest firewall and intrusion prevention devices, many organizations have malware or APTs in their networks and don't even know it.

Infoblox DNS Firewall can detect DNS-based malware and APTs inside the network and disrupt the ability of infected clients to communicate with botnets. You can evaluate DNS Firewall by installing the software on the Advanced DNS Protection POC hardware. The evaluation license is valid for 60 days and shows malware and APT activity through detailed logging and reports. The reports can be accessed through the same Infoblox Reporting and Analytics server that is used for the Advanced DNS Protection POC.

**Know if Your DNS Is Under Attack!**

The Advanced DNS Protection POC lets you easily detect any attacks that target your DNS server. With two non-disruptive options, easy-to-deploy hardware, and detailed logging and reports, you can proactively find out if your DNS is under attack and take corrective action.

**Figure 2: Threat Protection Statistics Widget**

**Figure 3: Threat Protection Event Count by Severity Trend Report**

**Figure 4: Threat Protection Top Rules Logged by IP**

---

**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.