Detect DNS Attacks with Advanced DNS Protection POC

Infoblox
CONTROL YOUR NETWORK

Product Summary: Infoblox Advanced DNS Protection provides defense against the widest range of DNS-based attacks such as floods, NXDOMAIN, tunneling, 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, DNS Tunneling, and Much More

DNS DDoS attacks are constantly on the rise as attackers seek weakest links in an infrastructure 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 or your internal recursive server, you can deploy Advanced DNS Protection, a DNS server with intelligence built in to detect attacks, in a couple of ways that are non-disruptive to your production traffic.

POC Option 1: Monitor Mode

Replace your external or internal DNS server with Advanced DNS Protection in monitor mode. This allows the server to detect incoming attacks likes DNS DDoS, exploits, tunneling, etc. Deploying in monitor mode will not block the attack traffic, giving you an option to review the attacks before taking action.

For internal DNS, you can also deploy the Advanced DNS Protection in a forwarding layer to your existing DNS servers (e.g. Microsoft).

To block attacks, you can turn off the 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 also be attached to the span port of the incumbent external or internal 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, tunneling etc. 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 the monitor mode is turned off.

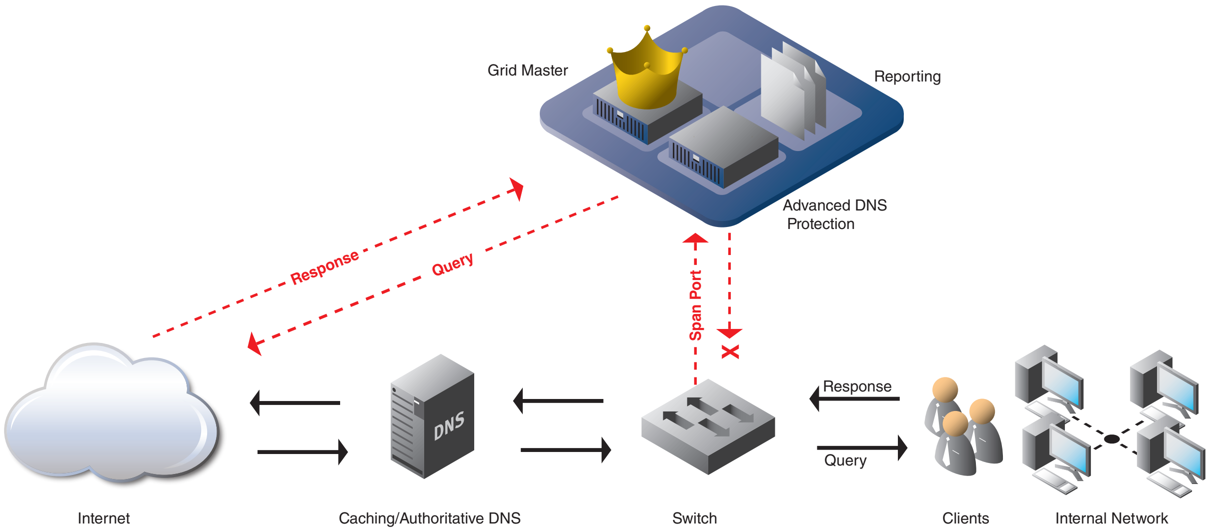


Figure 1: Advanced DNS Protection deployed in port mirroring mode on internal DNS

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.

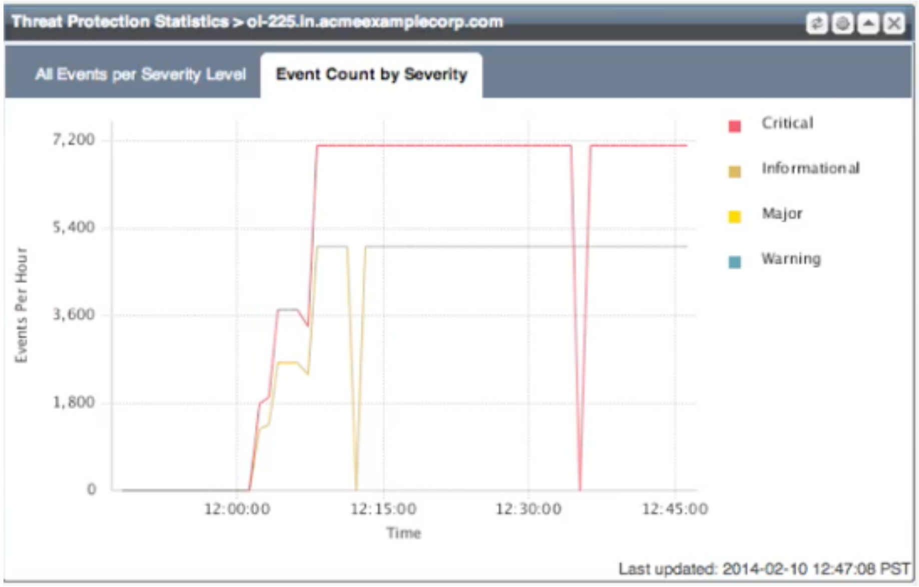
Threat Adapt Technology

Advanced DNS Protection Threat Adapt™ technology provides ongoing protection against new and evolving attacks.

Global Visibility of Attacks with Reports

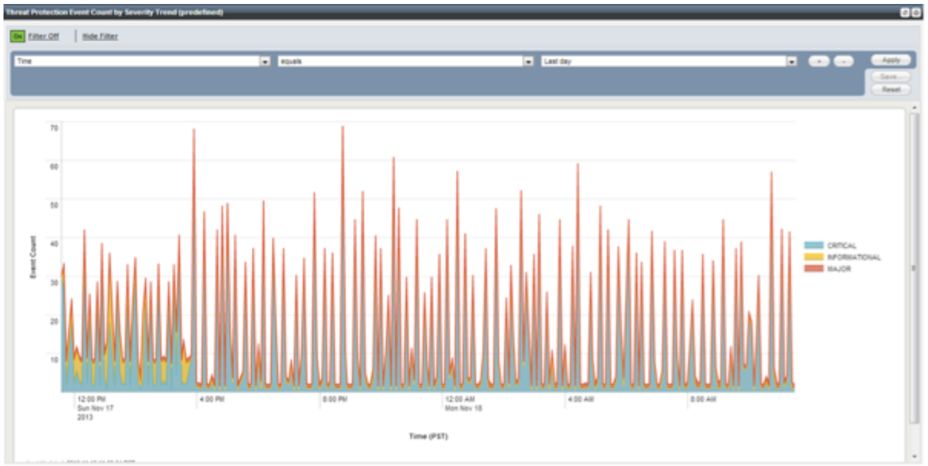
Once the Advanced DNS Protection POC is deployed and the threat rule parameters are fine-tuned, you can start seeing any attacks that may hit the server through widgets, logs, and reports.

The Threat Protection Statistics Widget on the Infoblox UI displays statistics about attack events by severity.



Last updated: 2014-02-10 12:47:08 PST

Figure 2: Threat Protection Statistics Widget



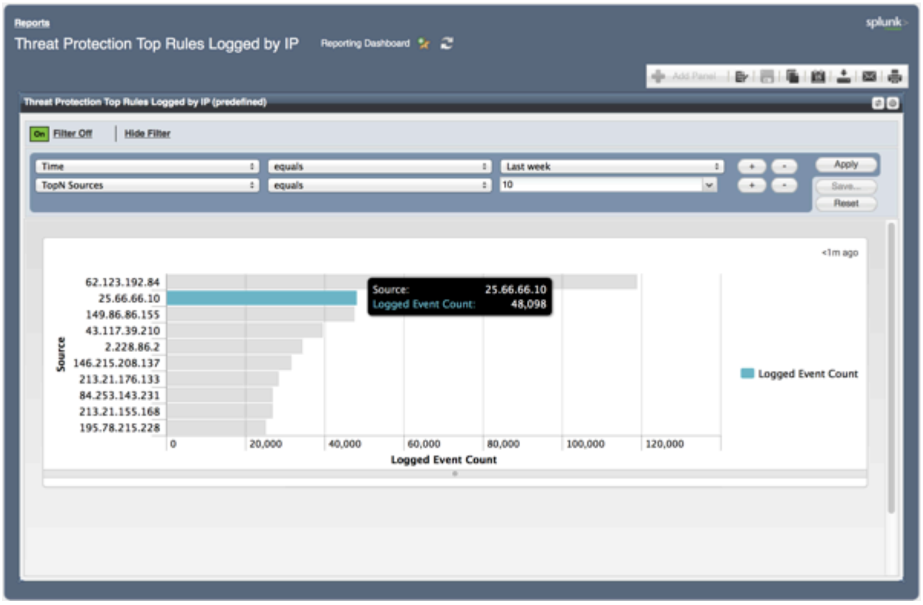
Threat Protection Event Count by Severity Trend (predefined)

On Filter Off | Hide Filter

Time | equals | Last day

Figure 3: Threat Protection Event Count by Severity Trend Report

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 Server.



Reports

Threat Protection Top Rules Logged by IP

Threat Protection Top Rules Logged by IP (predefined)

On Filter Off | Hide Filter

Time | equals | Last week

TopN Sources | equals | 10

Source: 25.66.66.10
Logged Event Count: 48,098

Figure 4: Threat Protection Top Rules Logged by IP

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 Server that is used for the Advanced DNS Protection POC.

Know if Your DNS is Under Attack!

Advanced DNS Protection POC lets you easily detect any attacks that target your DNS server (internal or external). 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.

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