Infoblox
CONTROL YOUR NETWORK

Protect Against the Widest Range of External and Internal DNS Attacks

SOLUTION NOTE

Summary

Infoblox Advanced DNS Protection defends against the widest range of external and internal DNS-based threats such as volumetric attacks, NXDOMAIN, exploits, and DNS hijacking. Unlike approaches that rely on infrastructure over-provisioning or simple response-rate limiting, Advanced DNS Protection intelligently detects and mitigates DNS attacks while responding only to legitimate queries. Moreover, Infoblox ADP is the only solution that is fully integrated with DDI that can automatically protect the DNS server against new and evolving threats with a set of threat protection rules without the need for patching.

Continuously Block New and Evolving DNS Attacks While Responding to Legitimate Requests

DNS servers are mission-critical infrastructure, and they have to continue to respond to queries even when they are under attack. If your external DNS server goes down, your entire network is shut off from the Internet. DNS is now the number one targeted service for application-layer attacks and is the number one protocol used in reflection/amplification attacks according to leading security reports. The damage is costly, and Neustar estimates upward of $100,000 an hour as the cost resulting from a DDoS attack, not including customer defection and damage to brands.

Attackers look for the weakest links in your network, and the Domain Name System (DNS) protocol is easy to exploit. As a result, attacks designed to bring down DNS servers and consume network bandwidth—and to interfere with or shut down critical IT applications such as email, web sites, VoIP, and software as a service (SaaS)—are on the rise. Another common threat is DNS hijacking, which compromises the integrity of DNS.

As the leader in DNS, Infoblox delivers the widest range of protection on the market for guarding your mission-critical DNS services from attack.

The Threat Landscape

To underscore the seriousness of the danger DNS attacks present to your business, we'd like to highlight a few of the most common threats.

DNS reflection/DDos attacks use third-party DNS servers (open resolvers) to propagate a DoS or DDoS attack.
DNS amplification attacks use specially crafted queries to create amplified responses to flood their victims with traffic.
TCP, UDP, and ICMP floods deny service on layer 3, bringing a network or service down by flooding with large volumes of traffic.
DNS-based exploits exploit vulnerabilities in the DNS software as data exfiltration through known tunnels.
Protocol anomalies cause servers to crash by sending malformed packets and queries.
Reconnaissance probes are attempts to get information on the network environment before launching a large DDoS or other type of attack.
DNS hijacking attacks override a domain's registration information, usually at the domain's registrar, to point to a rogue DNS server.
NXDOMAIN attacks send a flood of queries to a DNS server to resolve non-existent domain names, causing the server's cache to fill up with NXDOMAIN results and slowing response time for legitimate requests.

Many IT organizations today use load-balancers, IPS and firewall devices, generic DDoS protection solutions, and cloud-based solutions to try to counter DNS-based attacks. But all of these approaches are limited in what they can and cannot protect. Most of them are external solutions that are "bolted on" rather than built from the ground up to secure DNS against attacks. None of them can compare to the effectiveness of a purpose-built, DNS-specific defense solution.

Infoblox
CONTROL YOUR NETWORK

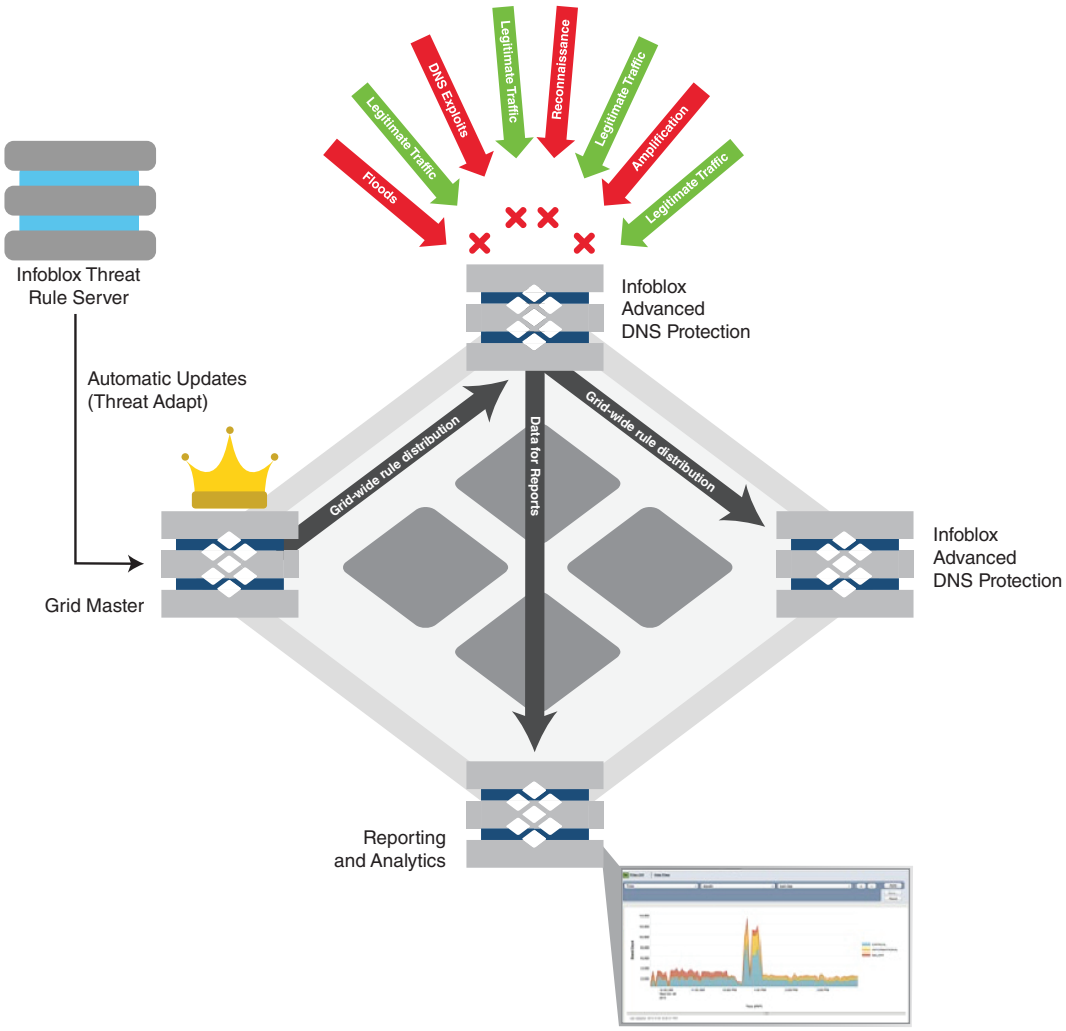
Protect Against the Widest Range of External and Internal DNS Attacks

SOLUTION NOTE

The Power of Infoblox Advanced DNS Protection

Advanced DNS Protection solution components include:

- Infoblox Advanced Appliance: Advanced special-purpose appliance that has dedicated processing power for the Advanced DNS Protection Service. These are DNS appliances only; they do not include DHCP and IPAM.
- Trinzic Hardware and Virtual Appliances: Consists of existing Trinzic TE-1410/1420 appliances as well as newer Trinzic TE 815/825/1415 appliances with ADP software subscription add-on. Virtual appliances are supported on VMWare and KVM only at this time.
- Infoblox Advanced DNS Protection Service: The software, in conjunction with Threat Adapt technology, to provide protection against existing and new threats to the DNS server.



Infoblox Advanced DNS Protection provides unique protection against DNS-based attacks.

Infoblox
CONTROL YOUR NETWORK

Protect Against the Widest Range of External and Internal DNS Attacks

SOLUTION NOTE

Reduce DNS Service Disruption

Infoblox Advanced DNS Protection continuously monitors, detects, and drops all types of DNS attacks—including volumetric attacks and non-volumetric attacks such as exploits and DNS hijacking—while responding to legitimate queries. It also maintains DNS integrity, which can be compromised by DNS hijacking attacks.

Adapt to Evolving Threats

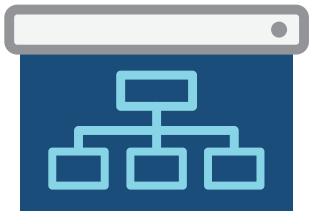
Infoblox Advanced DNS Protection uses Infoblox Threat Adapt technology to keep the protection updated automatically against new and evolving threats as they emerge. Threat Adapt uses independent analysis and research on evolving attack techniques, including what we have seen in customer networks, to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

Utilize Data for Threat Remediation

Easily view past DNS attacks or attacks in progress. Improve operational efficiency by providing visibility into threats and enabling rapid threat remediation. Infoblox Advanced DNS Protection also provides detailed views on attack points across the network and attack sources, providing the intelligence needed for threat management. It is integrated with our DNS solution, and hence no special integration is required.

Flexible Deployment Options

Take advantage of flexible deployment options by deploying the solution either as a subscription add-on to virtual and physical Trinzic appliances, or as specialized advanced appliances.



Note: Advanced DNS Protection can also be deployed in a trial or proof-of-concept mode, either in line in monitor mode to detect and monitor attacks without actually blocking them, or in out-of-band mode using port mirroring to detect attacks.

The Sooner You Act, the Safer Your Business Is

Security built in is better than security bolted on. There is no better place to defend against DNS-based attacks than from within the DNS servers they target. And the only solution built with this in mind is Infoblox Advanced DNS Protection.

Contact us today to find out more about the widest range of protection available for your external and internal DNS servers.

About Infoblox

Infoblox delivers Actionable Network Intelligence to enterprises, government agencies, and service providers around the world. As the industry leader in DNS, DHCP, and IP address management (DDI), Infoblox provides control and security from the core—empowering thousands of organizations to increase efficiency and visibility, reduce risk, and improve customer experience.

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