Infoblox
CONTROL YOUR NETWORK

Infoblox Advanced DNS Protection

DATASHEET

Key Features

- **Protection against the widest range of attacks:** Continuously monitor, detect, and drop all types of DNS attacks, including DNS DDoS, NXDOMAIN, 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.

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, cyberattacks 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). 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 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 bogus sites 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 Advanced DNS Protection

Infoblox Advanced DNS Protection provides defense against the widest range of DNS-based attacks such as DNS DDoS, exploits, NXDOMAIN, DNS tunneling, and DNS hijacking attacks. 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, it uses Infoblox Threat Adapt™ technology to automatically update its defense against new and evolving threats as they emerge, without the need for patching.

Solution Components

- **Infoblox Advanced Appliance:** A DNS server that is purpose built with security in mind
- **Infoblox Advanced DNS Protection Service:** The software plus 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

Advanced DNS Protection 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.

Benefits

- Achieve resilient, reliable, and trustworthy DNS services by identifying and blocking DNS based attacks.
- Continuously protect against new and evolving DNS-related attacks as they happen and automatically morph protection with DNS configuration changes—without downtime or patching.
- Start blocking attacks immediately.
- Protect your business from revenue loss and brand damage caused by network downtime.
- See attacks across your network as they happen, and take action based on detailed intelligence.
- Tailor your DNS protection based on your business's unique DNS traffic patterns.
- Keep your DNS services functioning even when under attack.

Infoblox Threat Adapt™ Technology

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 it automatically morphs protection to reflect DNS configuration changes.

Global Visibility of Attacks with Reporting

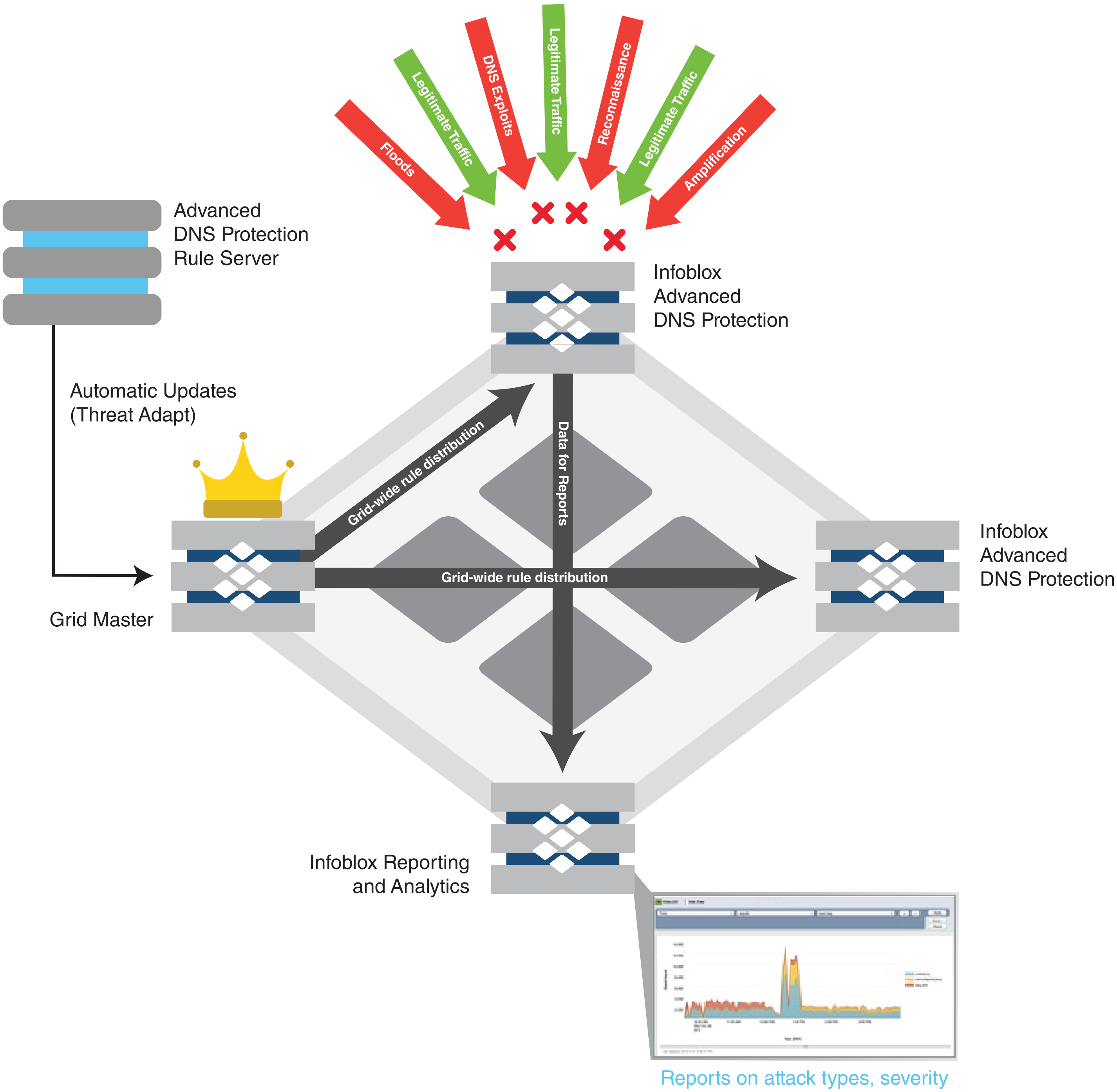
Through comprehensive reports and alerts, Advanced DNS Protection provides detailed views on attack points across the network and attack sources, providing the intelligence needed to take action. The reports can be accessed through the Infoblox Reporting and Analytics server.

Quick Deployment

Advanced DNS Protection 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 Advanced DNS Protection Protects Against

DNS reflection/DrDoS attacks	Volumetric	Using third-party DNS servers (open resolvers) to propagate a DoS or DDoS attack
DNS amplification	Volumetric	Using a specially crafted query to create an amplified response to flood the victim with traffic
TCP/UDP/ICMP floods	Volumetric	Denial of service on layer 3 by bringing a network or service down by flooding it with large amounts of traffic
NXDOMAIN	Volumetric	Flooding the DNS server with requests for non-existent domains, causing cache saturation and slower response time
Random sub-domain (slow drip attacks), Domain lock-up attacks, Phantom domain attacks	Low-volume stealth	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
DNS-based exploits	Exploits	Attacks that exploit vulnerabilities in the DNS software
DNS cache poisoning	Exploits	Corruption of the DNS cache data with a rogue address
Protocol anomalies	Exploits	Causing the server to crash by sending malformed packets and queries
Reconnaissance	Exploits	Attempts by hackers to get information on the network environment before launching a large DDoS or other type of attack
DNS hijacking	Exploits	Attacks that override domain registration information to point to a rogue DNS server
DNS tunneling	Exploits	Attack involves tunneling another protocol through DNS port 53—which is allowed if the firewall is configured to carry non-DNS traffic—for the purposes of data exfiltration


Floods
Legitimate Traffic
DNS Exploits
Legitimate Traffic
Reconnaissance
Legitimate Traffic
Amplification
Advanced DNS Protection Rule Server
Automatic Updates (Threat Adapt)
Infoblox Advanced DNS Protection
Grid-wide rule distribution
Data for Reports
Grid Master
Grid-wide rule distribution
Infoblox Advanced DNS Protection
Infoblox Reporting and Analytics
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, and 1-GigE and 10-GigE options.

PT - 1400

PT - 2200

PT - 4000

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.

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

© Infoblox, Inc. All rights reserved. Infoblox-DS-0200-00 1609 - Infoblox Advanced DNS Protection