Infoblox
CONTROL YOUR NETWORK

Infoblox Advanced DNS Protection

DATASHEET

Key Features

- **Signature based detection of DNS attacks:** Continuously monitors, detects, and drops various types of DNS attacks, including volumetric and exploit attacks, and maintains DNS integrity.
- **Threat Adapt:** Uses Threat Adapt™ technology to deliver the latest threat intelligence and morph protection to reflect changes in DNS configuration. Threat Adapt uses independent analysis and research on evolving attack techniques, including what's seen in customer networks, to update protection.
- **Reporting and Analytics:** Provides detailed central view of attack points and patterns across the entire network, query Logging with access to raw DNS data for security forensics, integrated dashboards and pre-built & customized reports for faster threat investigation.
- **Enhanced processing for threat mitigation (hardware option only):** Features a dedicated compute (dedicated network packet inspection hardware) for threat mitigation; blocks attacks before they reach the DNS server application.

Protection Against the Widest Range of External and Internal DNS Attacks

Challenges/Problems with DNS: One of the Fastest Growing Attack Vectors

Security, availability, and integrity are the top three concerns regarding DNS infrastructure. Attackers seek weakest links to illegally exploit businesses, and since the Domain Name System (DNS) protocol is not protected by legacy security systems, it is easy to exploit. As a result, cyberattacks on DNS are on the rise. 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.

DNS distributed denial of service (DDoS) attacks are designed to bring down external and internal DNS servers and consume network resources, affecting the availability of critical IT applications such as email, web sites, VoIP, and software as a service (SaaS). 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. It is important to preserve the integrity and availability of the DNS to ensure pre-processing of DNS traffic to filter out attacks while responding to legitimate DNS requests in parallel.

Solution: 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 data exfiltration (through known tunnels), 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 to deliver Actionable Network Intelligence.

Solution Components

- **Infoblox Appliances [Appendix 2]**
  - Advanced PT Appliance: Special-purpose appliance that has dedicated processing power for the Advanced DNS Protection Service. The PT 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. These are DNS appliances only; they do not include DHCP and IPAM.
  - Infoblox Trinzic Hardware and Virtual Appliances: Consists of existing Trinzic TE-1410/1420/2210/2220 appliances as well as newer Trinzic TE-815/825/1415/1425/2215/2225/4015/4025 appliances with ADP software subscription add-on. Virtual appliances are supported on VMWare and KVM.
- **Advanced DNS Protection Service:** The software plus Threat Adapt technology provides ongoing protection against existing and new threats to the DNS server.

Infoblox
CONTROL YOUR NETWORK

Infoblox Advanced DNS Protection

DATASHEET

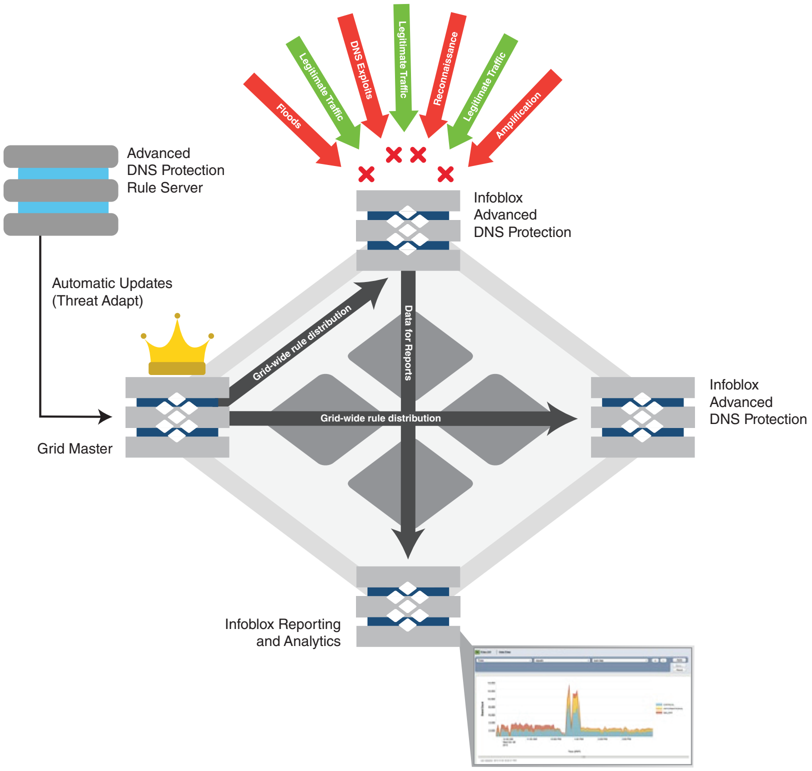
Benefits

Prevent DNS Service Disruption: Advanced DNS Protection protects against widest range of internal and external DNS attacks [Appendix 1] to increase application and service availability. It maintains DNS integrity, which can be compromised by DNS hijacking attacks.

Protection against Evolving Threats: Advanced DNS Protection uses Infoblox Threat Adapt technology to keep the protection updated automatically against new and evolving threats as they emerge, without downtime or patching.

Threat Management with centralized visibility: Through comprehensive reports and alerts, Advanced DNS Protection features central and detailed views of attack points across the network and attack sources, providing the intelligence needed to take action.

Flexible Deployment Options: It provides flexible deployment options as a subscription add-on to virtual and physical Trinzic appliances or as specialized advanced appliances.


Floods
Legitimate Traffic
DNS Exploits
Legitimate Traffic
Reconnaissance
Legitimate Traffic
Amplification
Advanced DNS Protection Rule Server
Infoblox Advanced DNS Protection
Automatic Updates (Threat Adapt)
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

Get Started on Evaluation

30-day free software ADP evaluation with temporary license for customers will be made available through your Account Managers/SEs.

What customers our say

> Service incidents from DDoS attacks have been cut in half, and customer complaints about lengthy page load times have been significantly reduced.
>
> *— VP of Customer Support, Large Service Provider*

> I've been using Infoblox for DNS, DHCP, and IP address management for four years. It's a solid product. We've moved resources around because the product works so well. Our global footprint is managed by 1.5 FTE—and that's 65 devices.
>
> *— Manager of Global Infrastructure, Adobe*

Appendix 1: Summary of Attack Types protected by Advanced DNS Protection(ADP)

DNS reflection/DDoS 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
NS hijacking	Exploits	Attacks that override domain registration information to point to a rogue DNS server
Data Exfiltration (using known tunnels)	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

Appendix 2: Delivery Options

PT Appliances Ship in Three Physical Platforms

The PT Appliances have next-generation programmable processors that provide dedicated compute for threat mitigation. They offer AC and DC power supply options.

PT - 1405

PT - 2205

PT - 4000

Software ADP: Available on Physical and Virtual Platforms

It is a software add-on to Trinzic TE 1410/1420/1415/825/815 appliances.

TE - 4015/4025

TE - 2215/2225

TE - 1415/1425

TE - 2210/2220

TE - 1410/1420

TE - 815/TE 825

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