SOLUTION NOTE

INFOBLOX ADVANCED DNS PROTECTION

Minimize Business Disruptions Caused by DNS-based Attacks

SUMMARY

With Infoblox Advanced DNS Protection (ADP), your business is always up and running even during a DNS-based attack.

Infoblox blocks the widest range of attacks, such as volumetric attacks, NXDOMAIN, DNS exploits and DNS hijacking.Unlike approaches that rely on infrastructure overprovisioning or simple response-rate limiting, Advanced DNS Protection intelligently detects and mitigates DNS-based attacks while responding only to legitimate queries using constantly updated threat intelligence, without the need to deploy security patches. It provides single-pane-of-glass visibility into who is on the network, which devices they are on and details about the attack to ensure a rapid response. With Infoblox, you can take network reliability to the next level by ensuring that your critical infrastructure—and your business—keep working at all times.

> *"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**

CHALLENGES FROM SERVICE DISRUPTION

DNS is foundational to every organization because it provides the mission-critical connectivity necessary today to run a business. If your external DNS server goes down, your entire network is cut off from the Internet. DNS disruption interferes with or shuts down your critical IT applications, such as email, websites, VoIP and software as a service (SaaS). According to leading security reports, DNS is the second most targeted service for application-layer attacks, with 72 percent of enterprises impacted in 2018. Neustar estimates the cost resulting from a distributed denial of service (DDoS) attack carried out through DNS to be greater than $220,000 an hour, not including customer defection and damage to brands. Attackers look for the weakest links in your network, and the DNS protocol is easy to exploit for DDoS or DNS hijacking; such attacks compromise the integrity of DNS.

Infoblox delivers the widest range of protection on the market for guarding your mission-critical DNS services from attack, furnishing the five nines availability your organization depends on. It supplies centralized visibility into who is using the network, which devices they are on and details about the attack to ensure a rapid response.

THE DNS THREAT LANDSCAPE

Here are some of the most common and serious DNS threats confronting your organization:

Attack Name	Type	How it works
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
DNS 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

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 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 compares to the effectiveness of a purpose-built, DNS-specific defense solution. That solution is Infoblox ADP.

THE POWER OF INFOBLOX ADVANCED DNS PROTECTION

Infoblox Advanced DNS Protection solution components include:

Infoblox Appliances

- Advanced PT Appliance: special-purpose appliance that has dedicated processing power for Advanced DNSProtection. The PT Appliance is a fortified DNS server with security built in. It leverages dedicated compute resources to filter out attacks before they reach the DNS server or application. This is a DNS appliance only and does not include DHCP and IPAM.
- Infoblox Trinzic Hardware and Virtual Appliances: consist of existing Trinzic TE-410/1420/2210/2220 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 WThreat Adapt technology provides ongoing protection against existing and new threats to the DNS server.

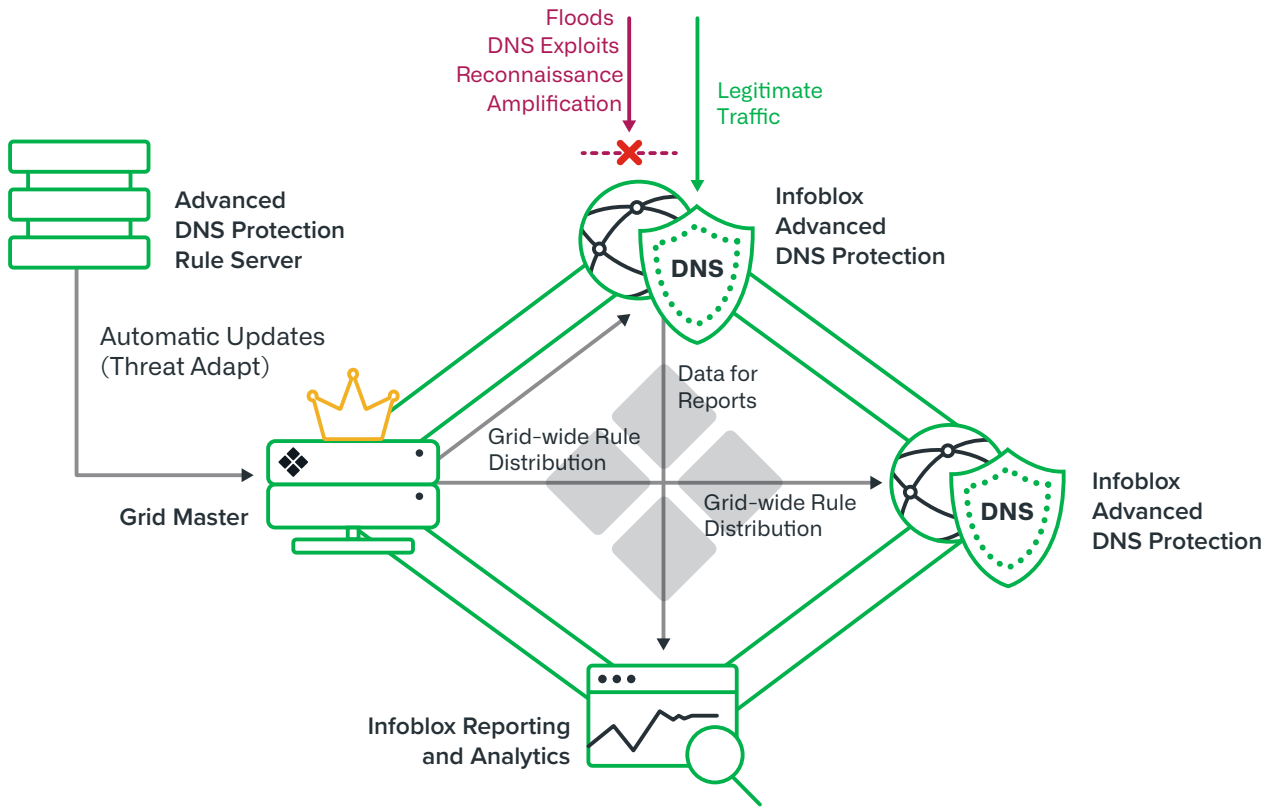

Figure 1: Infoblox Advanced DNS Protection provides a unique defense against DNS-based attacks

Reduce Business Disruption

Infoblox Advanced DNS Protection continuously monitors, detects, and stops all types of DNS-based 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 DNS hijacking attacks can compromise. Infoblox provides a solid foundation with five nines availability for next level reliability.

Adapt to Evolving Threats

Infoblox ADP uses Infoblox Threat Adapt™ technology to automatically update protection against new and evolving threats as they emerge. Threat Adapt applies independent analysis and research to evolving attack techniques, including what our threat specialists have seen in customer networks, to update protection. It automatically adapts protection to reflect DNS configuration changes.

Gain Single-Pane-of-Glass Visibility

With Infoblox, your organization can easily view prior or current DNS attacks and improve operational efficiency through our rapid threat remediation. Infoblox Advanced DNS Protection also furnishes a single view of attack points across the network and attack sources, supplying the intelligence necessary for threat management. It is already integrated with our DNS solution.

Deploy Flexibly

With Infoblox, you have the option of deploying as a subscription add-on to virtual and physical Trinzic appliances, or as specialized advanced appliances.

Lower Your Costs

With Infoblox, you have the option of deploying as a subscription add-on to virtual and physical Trinzic appliances, or as specialized advanced appliances.

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

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20230919v1