DATASHEET

Infoblox DNS Infrastructure Protection

Minimize business disruptions caused by DNS-based attacks

CHALLENGE: SERVICE DISRUPTIONS

DNS is the hidden backbone of digital operations. Every website, app and user relies on it to stay connected. If DNS services go down, it can cost millions in lost revenues and lost customer trust. That is especially true for the external DNS services that keep your websites, email and other public-facing applications online. At the same time, external DNS servers must be exposed to the public internet, making them a constant target of cyberattacks, including:

- **DDoS attacks**, which overwhelm servers with massive traffic from multiple sources, causing websites to crash
- **DNS hijacking**, where attackers tamper with DNS records to redirect traffic to a malicious site
- **Cache poisoning**, where attackers inject malicious or invalid data into a network's cache, either to serve malicious content or redirect users to malicious sites
- **NXDOMAIN exploits**, which flood DNS servers with queries for non-existent domains, causing service disruption

Additionally, external authoritative DNS records get distributed across internet servers worldwide. So if an attacker is able to alter them, it can take hours, even days to correct all that bad data, during which your websites and other online apps may be totally unreachable.

Infoblox DNS Infrastructure Protection (formerly Advanced DNS Protection) stops DDoS and other attacks targeting DNS servers. This NIOS software add-on keeps your mission-critical internet-connected applications up and running—even when DNS infrastructure is under heavy attack.

SOLUTION: SAFEGUARD YOUR BUSINESS FROM DISRUPTIONS CAUSED BY DNS-BASED ATTACKS

DNS Infrastructure Protection continually detects and blocks a wide range of threats targeting critical DNS services and prevents attackers from manipulating DNS integrity. It blocks both volumetric attacks, like DDoS and NXDOMAIN, and non-volumetric exploits, like DNS hijacking, cache poisoning and other threats targeting external and internal DNS servers.

Unlike one-size-fits-all approaches that can block legitimate traffic, DNS Infrastructure Protection uses continually updated intelligence to identify genuine threats. Meanwhile, it keeps real traffic flowing so your business stays up and running, even while DNS infrastructure is under attack.

KEY FEATURES

Reduce Business Disruptions: Infoblox DNS Infrastructure Protection continuously monitors, detects and stops all types of DNS attacks—including volumetric attacks and non-volumetric attacks, such as DNS exploits and DNS hijacking—while responding to legitimate queries. It also maintains DNS integrity, which DNS hijacking attacks can compromise. Infoblox helps ensure that mission-critical websites and apps stay online and available.

Adapt to Evolving Threats: Infoblox DNS Infrastructure Protection 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 Infoblox threat specialists have seen in customer networks, to update protection. It automatically adapts protection to reflect DNS configuration changes.

ENABLING ENCRYPTED DNS (DoH AND DoT)

Communication between the DNS client (stub) resolver and local DNS server (recursive resolver) is unencrypted. Unencrypted communications are subject to data snooping, interception and exfiltration—otherwise known as DNS's "last mile" security problem. In response, the industry initiated DNS over TLS (DoT) and DNS over HTTPS (DoH) to provide privacy and encryption between DNS clients and external internet DNS servers. Implementing encryption through the DNS resolver on your network allows you to remain in control of your user's network experience while providing security and content filtering per your security policy requirements. DNS Infrastructure Protection optimizes DNS encryption so you can terminate encrypted DoT and DoH connections on your network.

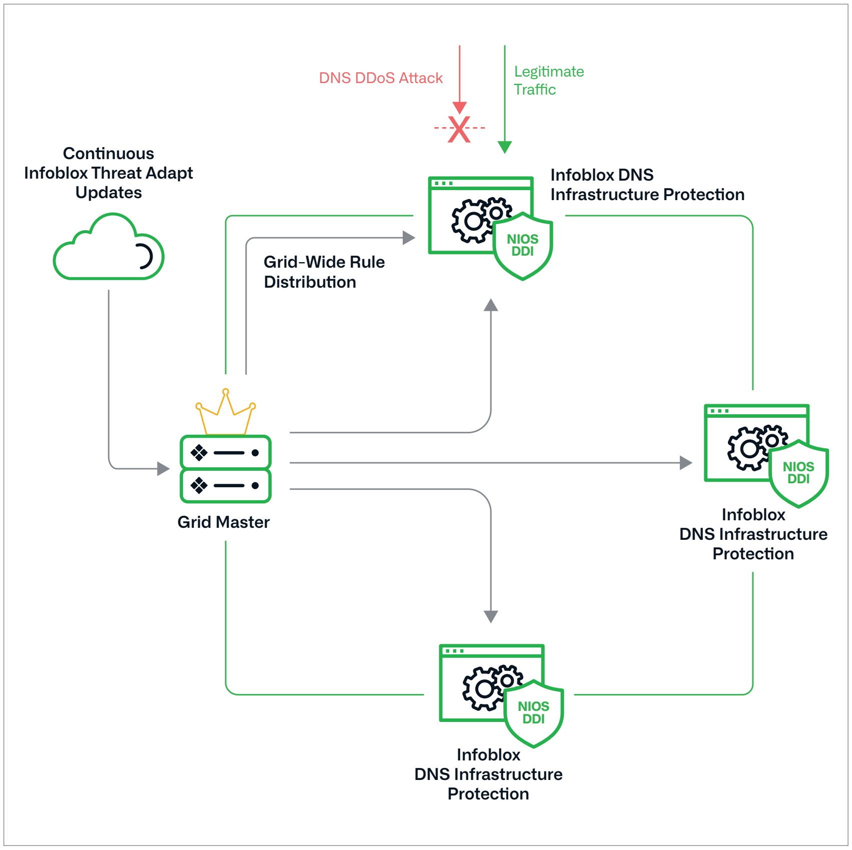
DNS DDoS Attack
Legitimate Traffic
Continuous Infoblox Threat Adapt Updates
Infoblox DNS Infrastructure Protection
NIOS DDI
Grid-Wide Rule Distribution
Grid Master
Infoblox DNS Infrastructure Protection
NIOS DDI
Infoblox DNS Infrastructure Protection
NIOS DDI

Figure 1. Infoblox DNS Infrastructure Protection provides a unique defense against DNS-based attacks

Gain Single-Pane-of-Glass Visibility: DNS Infrastructure Protection provides pervasive, centralized visibility into DNS attack patterns, both in real time and historically. NetOps and SecOps teams can track threat sources and view points of attack across the environment to accelerate mitigation and continually improve defenses.

Available on Physical, Virtual and Cloud Platforms: With Infoblox, you have the option of deploying as-a-software subscription add-on to virtual and physical Trinzic appliances, enabling services to run on a common model and supporting on-prem, private and public cloud environments.

WHAT OUR CUSTOMERS SAY

> *"Service incidents from DDoS attacks have been cut in half, and customer complaints about lengthy page load times have been significantly reduced."*

Vice President 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

TABLE 1:
SUMMARY OF ATTACK TYPES THAT DNS INFRASTRUCTURE PROTECTION DEFENDS AGAINST

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

APPLIANCE OPTIONS

DNS Infrastructure Protection: Available on Physical and Virtual Platforms

Infoblox DNS Infrastructure Protection defends against a broad spectrum of DNS DDoS attacks, ensuring uninterrupted service for your organization. It is a software subscription add-on to a variety of Trinzic hardware and software appliances, enabling you to safeguard DNS integrity and prevent both external and internal DNS DDoS attacks that could disrupt your business operations across on-prem, private and public cloud environments.

infoblox

Infoblox unites networking, security and cloud with a protective DDI platform that delivers enterprise resilience and agility. We integrate across hybrid and multi-cloud environments, automate critical network services and preemptively secure the business—providing the visibility and context needed to move fast without compromise.

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

+1.408.986.4000
www.infoblox.com

Version: 20251007v3