DATASHEET

# Infoblox advanced DNS protection for service providers

## CHALLENGE: SERVICE DISRUPTIONS

CSPs, mobile operators and cloud providers all rely heavily on DNS, partly as an essential connectivity component and partly as a service they offer their customers, either implicitly or explicitly. CSPs must protect this vital asset—for their reputations and for their customers who rely on stable, always-on Internet connectivity. If the DNS servers go down, your subscribers are 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 affected 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 subscriber defection and damage to brands. Attackers look for the weakest links—attack vectors—in your network, and the DNS protocol is easy to exploit for DDoS or DNS hijacking; such attacks compromise the integrity of DNS.

## A PLETHORA OF DEFENSES–BUT STILL FLYING BLIND

Many CSP networks adopt an array of tools, including intrusion-prevention systems (IPSs), firewalls and loadbalancing systems, which are adept at protecting various aspects of the provider's infrastructure. However, these tools are ineffective when applied to DNS since they are not integrated with DNS servers and don't have DNS understanding or visibility.

Despite deploying these tools extensively, many CSPs still complain that the first they know about attacks on DNS is when they hear from customers about slow network performance or other degradations. Most organizations have little or no early warning of attacks on DNS systems. Many operations teams even resort to manual parsing of DNS server log data to determine whether traffic levels have risen and whether servers have become stressed or compromised.

## CRITICAL AREAS REQUIRING PROTECTION

Two critical areas that require protection inside the provider's network are authoritative DNS servers and the DNS caching servers. Authoritative DNS servers in various locations inside the provider's network respond to DNS queries and connectivity requests from their subscriber base. Authoritative DNS servers enable web presence, e-commerce functions, and the location of multiple network components for mobile IP connectivity, especially roaming

## BENEFITS AND FEATURES

**Reduce Business Disruptions:** Infoblox Advanced DNS Protection (ADP) continuously monitors, detects and stops all types of DNS attacks—including volumetric attacks 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 provides a solid foundation for security, enabling five-nines availability for your network.

**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 Infoblox threat specialists have seen in customer networks, to update protection. It automatically adapts protection to reflect DNS configuration changes.

and gateway location in LTE and 5G networks. To ensure a smooth subscriber Internet experience, the DNS caching layer is key to establishing a rapid response to DNS queries. Therefore, it is critical to hold cached query responses for commonly accessed websites and other URLs to achieve acceptable response times.

## A NEW VARIABLE: ENCRYPTED DNS

New encrypted DNS standards have emerged that, while protecting the privacy of DNS requests and the integrity of responses, CSPs can lose some of the control needed to govern DNS usage within their networks unless they provide their encrypted DNS services. DNS over TLS (transport layer security) or DoT, and DNS over HTTPS or DoH, work by encrypting the DNS communication between your operating system's stub resolver or a local application and your recursive DNS resolver. Both technologies ensure data privacy and authentication by encrypting communications between DNS clients and servers. However, in doing so, many solutions are changed to point to external DNS resolvers, allowing client devices to access DNS services outside of the provider's control and exposing the subscriber to potential security risks and negative customer experiences. Providers should take steps now to reduce the risks these technologies pose. Implementing encryption through the DNS resolver on your network allows you to remain in control of your subscriber's network experience. It will enable providers to continue to provide security, content filtering and other critical on-net services.

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

With Infoblox Advanced DNS Protection (ADP), your business is always up and running, even under a DNS-based attack. Infoblox blocks the broadest range of attacks, such as volumetric attacks, NXDOMAIN attacks, exploits and DNS hijacking. Unlike approaches that rely on infrastructure overprovisioning or simple response-rate limiting, ADP intelligently detects and mitigates DNS attacks while responding only to legitimate queries by using constantly updated threat intelligence without the need to deploy security patches. With Infoblox, you can take network reliability to the next level by ensuring that your critical network infrastructure—and your business—keep working at all times.

## SUPPORTS ENCRYPTED DNS STANDARDS

Infoblox Network Identity Operating System (NIOS) is the OS that powers Infoblox core network services, ensuring the network infrastructure's continuous operation. Infoblox Encrypted DNS for Service Providers is a NIOS feature that provides efficient encryption while delivering Infoblox best-inclass DNS and value-added subscriber services. With support for DoT and DoH, Infoblox Encrypted DNS delivers a unique approach to encrypting your DNS traffic. Unlike methods that rely on load balancers or over-provisioning, Infoblox Encrypted DNS runs as a single service for all of your DNS needs. Available through virtualized instances of ADP, Infoblox Encrypted DNS enables Infoblox to encrypt last-mile DNS communications between their endpoints and DNS servers regardless of which protocol the endpoint supports. It supports this capability while also solving performance concerns associated with the additional overhead related to encrypted DNS communications. From the same service, we allow CSPs to accommodate encrypted DNS with microsecond latency when the connection is already established while all other DNS features are running.

## BENEFITS AND FEATURES

**Gain Single-Pane-of-Glass Visibility:** With Infoblox, Communications Service Providers (CSPs) can easily view prior or current DNS attacks and improve operational efficiency through our rapid threat remediation. Infoblox Advanced DNS Protection also provides a single view of attack vectors across the network and attack sources, supplying the intelligence necessary for threat management. It is integrated with our DNS solution.

**Deploy Flexibly:** Carriers may deploy on Infoblox Trinzic Flex virtual appliances, which enable carriers to add specific capabilities across their entire Infoblox footprint while leveraging elastic scaling capabilities and service provider-specific, capacitybased pricing.

**Lower Your Costs:** Infoblox Software ADP leverages existing hardware, which means customers only need to upgrade software that runs on the hardware resulting in minimal incremental upgrade costs.

## FLEXIBLE DEPLOYMENT OPTIONS

Infoblox Advanced DNS Protection is designed for CSP environments requiring scalable edge deployments. It is available in multiple carrier-grade options, including orchestrated Virtualized Network Function (VNF) and cloudnative solutions.

- Infoblox Trinzic Flex: a scalable virtual platform based on the resources allocated to the virtual machine. The Infoblox Network Identity Operating System (NIOS) automatically detects the virtual machine's capacity and scales it to the appropriate platform. Additionally, Trinzic Flex appliances are covered under the Service Provider License Agreement Program (SPLA).
- Available on Physical and Virtual Platforms: Software ADP is a software subscription add-on to Trinzic TE-815/825/1415/1425/ 2215/2225/4015/4025 appliances.

| Attack Name | Type | How It Works |
|---|---|---|
| DNS reflection/DDoS attacks | Volumetric | Using third-party DNS servers (open resolvers) two 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 |

*Table 1: Summary of Attack Types That Advanced DNS Protection (ADP) Defends Against*

## PROTECTING SUBSCRIBERS AND BRAND

Infoblox carrier-grade solutions for service providers protect subscribers by using global threat intelligence and automated protection packages. The solutions maintain critical DNS service availability in rapidly evolving networks, growing traffic, and even during a malicious DDoS attack.

- Infoblox Advanced DNS Protection is the industry's most comprehensive and integrated DNS protection solution for service-provider DNS infrastructure.
- Advanced, automated detection and mitigation capability for DNS-based attacks like amplification, reflection, protocol anomalies, and tunneling—all built into the DNS server.
- Carrier-grade and available in multiple form factors including orchestrated Virtualized Network Function (VNF) and cloudnative solutions, featuring the world's fastest DNS caching server and support for DNS caching and authoritative DNS deployments.
- Threat intelligence and mitigation rules with automatic updates from Infoblox.
- Patented Infoblox Grid technology provides extensive control, automation and distribution of updates, to reduce operational support costs and eliminate the risk of outages caused by manual configuration errors.
- Supports encrypted DNS protocols, including DNS over TLS (DoT) and DNS over HTTPS (DoH).

To learn more, visit www.infoblox.com/sp or contact your local Infoblox representative today.

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

© 2023 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc.
All other marks are the property of their respective owner(s).