

High Integrity DNS for Service Providers



Service Provider Quote

“The Infoblox solution performs approximately 20 times faster than the existing solution, I have thousands of clients and the system is so plug-and-play that it is practically running itself. We also have delegated administration to several customers without jeopardizing visibility into other DNS (client) records, allowing us to reduce administration overhead and further optimize our resources.”

Jared Martin,
Executive VP of Operations,
BigCity Networks

New Applications and Services are Driving DNS Loads Higher

DNS traffic has increased tremendously with the advent of Web 2.0. The complexity of web applications and mash-ups necessitates 10-50 times more DNS lookups per page than before. In addition, content delivery networks (CDNs) and load balancing technologies depend on DNS to redirect clients to the best content location and therefore expire clients' DNS caches frequently, resulting in more DNS lookups. Email and anti-spam solutions use DNS lookups heavily. New IP applications including IPTV, VoIP and others have increased the use of DNS. In addition, DNS is increasingly a target for distributed denial-of-service (DDoS) and other types of cyber attacks, which can generate huge DNS loads. As a result, service providers must engineer their networks to scale with ever increasing DNS loads in order to maintain adequate performance and security for their subscribers.

DNS appliances have emerged as the solution of choice for large enterprise networks to provide highly resilient, high performance DNS solutions. However, a lack of carrier grade DNS appliances has forced service providers to look for software based solutions that can be installed on high performance servers to achieve the required DNS performance criteria at an acceptable cost.

Software solutions running on high performance hardware may help achieve high DNS performance numbers but network operators have to compromise on the resilience, security, ease of management and lower TCO offered by appliance based solutions.

The Infoblox 4030 DNS Caching appliance provides a new level of DNS price/performance and provides an extremely resilient, automated, high-performance solution optimized for service provider networks.

Issues with Software-based DNS

Software based DNS solutions pose several operational challenges when implemented in service provider networks. Service provider networks must operate nonstop and providers are often subject to penalties if they fail to meet contracted SLAs. Additionally, service providers are under pressure to deliver more services to more subscribers with fewer people. And with an increasingly hostile security environment, service providers must be prepared to patch their DNS systems, on very short notice, without introducing downtime.

Against these requirements, software-based DNS solutions pose the following challenges:

- Frequent hardware refreshes may be required to satisfy increasing DNS loads using commodity hardware;
- Servers need to be hardened for security vulnerabilities (both at the OS and application level) and must be front-ended with load balancers, IDP devices and other systems;
- Patching or upgrading the software is a manual process that can require hours per server and introduces downtime;
- No single point for accountability for the hardware, OS, DNS software/application, reporting systems and other utilities;
- No easy way to provide centralized system and data management with delegation and automation, backup and restore, auditing, maintenance, automated disaster recovery, etc.

High Integrity DNS for Service Providers



Solution Benefits

- DNS throughput of over 1 million queries per second (QPS) enables operators to scale their networks easily.
- Automated centralized management using Infoblox Grid technology enables fewer people to manage more systems, reliably and securely.
- One click patching and upgrades eliminate downtime, security issues and administrative effort.
- Security hardened appliances and cache poisoning attack monitoring and mitigation features provide protection against attacks.
- Multiple resilience technologies including hardware based high availability, DNS Anycast and automated disaster recovery ensure nonstop operation, even during software upgrades.
- Supports numerous applications including authoritative DNS and DNS caching.

Business Impacts of Staying with Conventional Software Infrastructure

Maintaining the status quo is risky and can impact business in the following ways:

- **High TCO:** Software solutions running on general purpose servers have high TCO due to costs of software licensing, high server count, deployment complexity, maintenance, patching, the need for additional security products, etc.
- **Security:** General purpose server based solutions are not inherently secure and must be hardened. Patching is time consuming and error prone and requires unscheduled downtime to react to a zero-day attack.
- **Resilience:** High-availability at the hardware, OS, protocol, and system level are rarely if ever found in software solutions and therefore need to be custom fitted on top of the basic DNS service, resulting in additional capital and operating costs and risk.



Infoblox IB-4010/4030 Carrier-Grade Appliance Family: High Performance DNS Services with Built-in Security, Resilience, and Automation

The Infoblox 4030 DNS Caching appliance was designed to meet the needs of service providers and large enterprises who need the highest possible DNS performance at the lowest possible cost of ownership.

The Infoblox 4030 DNS Caching appliance provides built-in, automated protection against DoS/DDoS attacks, using embedded hardware-based detection of common attack types. This combined with high computing capacity enables the Infoblox 4030 to withstand traffic levels up to 1 million DNS queries per second without slowing response to users, and enabling service providers to protect their networks against attack while also managing growth and spikes in DNS traffic levels.

About Infoblox

Infoblox (NYSE:BLOX) helps customers control their networks. Infoblox solutions help businesses automate complex network control functions to reduce costs and increase security and uptime. Our technology enables automatic discovery, real-time configuration and change management and compliance for network infrastructure, as well as critical network control functions such as DNS, DHCP, and IP Address Management (IPAM) for applications and endpoint devices. Infoblox solutions help over 7,100 enterprises and service providers in 25 countries control their networks.