Infoblox
CONTROL YOUR NETWORK

Elastic Scalability Provides Overload Protection

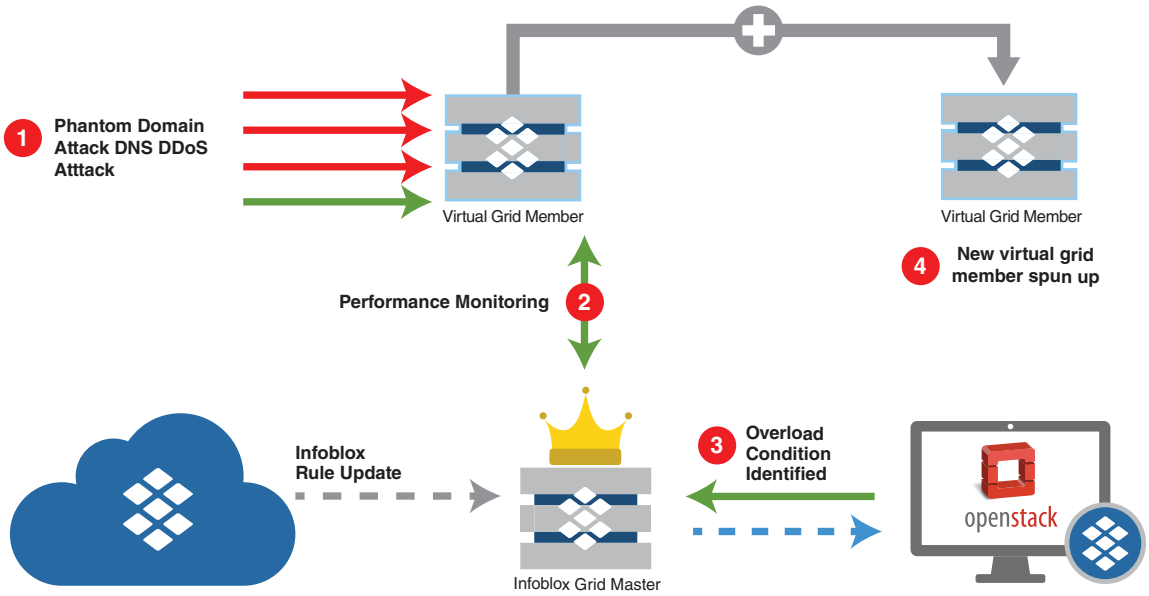
SOLUTION NOTE

Service providers have embraced network functions virtualization (NFV) and software-defined networking (SDN) as key technologies to promote service agility for fast roll-out, simplify network operations, provide cost-effective and elastic scalability, and reduce costs. This extensive network transformation, combined with new security and competitive challenges, requires a redefinition of the role of DNS, which was initially designed to provide simple mapping of application and service names to IP addresses. Infoblox has grown DNS into a robust technology, which supports new services, protects against escalating threats, and supports service-provider network strategies.

Today Infoblox Virtual Secure DNS solution includes enhanced capabilities that support existing physical and hybrid networks and a smooth network transition to NFV and SDN.

Infoblox Virtual Secure DNS Solution

The Infoblox Virtual Secure DNS solution for service providers is a hardened, proven solution that provides mission-critical functionality while reducing business and operational risk during the network transition to NFV and SDN. The Infoblox solution redefines DNS, once regarded simply as a rugged, scalable network utility, and incorporates the function into a strategic platform that supports next-generation operator services, network transformation strategies, and business goals.



Elastic Scalability

Infoblox Virtual Secure DNS provides the elastic scalability of DNS virtual network functions (VNFs) and the carrier-grade reliability, flexibility, and operational control required in virtualized networks. The solution ensures seamless, multi-service operations and delivers superior subscriber experience and new services in a timely manner—even under evolving market conditions.

Protection of often highly distributed DNS functions is a top priority. The solution allows you to quickly view and control all points in the DNS infrastructure network, pinpoint areas under attack or subject to other traffic surges, and then elastically scale up DNS instances in the specific local area where they are needed. This ability to prevent disruption or impairment of DNS functionality is fundamental to achieving the business advantages of NFV and SDN.

Infoblox
CONTROL YOUR NETWORK

Elastic Scalability Provides Overload Protection

SOLUTION NOTE

Elastic scalability in the Infoblox solution enables automatic instantiation of additional Secure DNS virtual machines upon detection of an overload condition or sudden spike in DNS traffic. With the Infoblox OpenStack Adapter, Infoblox Grid™ members are monitored and overload policies and thresholds are defined. Once an overload condition is identified, new members are provisioned and enabled to join the Grid.

Use Cases for Virtual Secure DNS

Virtual DNS Caching

Infoblox Virtual Secure DNS can be deployed as a subscriber-facing DNS caching server. The solution responds to queries made by subscribers either from its cache or via recursion.

Authoritative Virtual Secure DNS for Mobile Service Selection

Virtual Secure DNS can be deployed as the authoritative source for signaling and packet gateway selection in mobile networks (SGW/PGW). In a 4G environment, when a subscriber initiates a data connection, Virtual Secure DNS will send a list of configured gateways to the Mobile Management Entity (MME) in order to pick a gateway.

Virtual Secure DNS for Managed Service Providers (MSP)

The solution can also be deployed in the MSP cloud, where enterprises typically point all their recursive DNS data to Virtual Secure DNS servers located in the cloud. Virtual Secure DNS serves all recursive queries and uses Infoblox DNS Firewall to protect the organizations from malware, DNS data exfiltration, and phishing attacks.

Centralized Visibility and Control

Many legacy DNS systems, for example, have multiple disconnected, individually managed DNS services running in the network, making coordinated software updates, configuration changes, and other system-wide changes both labor intensive and prone to error. A single view of the entire network is essential to reduce administrative time, eliminate the risk of service-impacting configuration errors, and identify threats, overload conditions, or other traffic anomalies that need to be addressed in real time.

Infoblox provides a streamlined and efficient method of centrally managing all virtual and physical DNS machines. The Infoblox Grid manages a geographically dispersed, virtualized, or hybrid NFV system as one system. DNS data, including software updates, configuration changes, and threat feeds is replicated throughout the system in real time where necessary. Adding newly spun-up DNS members to the Grid is simple and can be easily automated through an orchestrator, and then added to the DNS pool—and everything can be centrally managed and visible from the easy-to-use user interface.

DNS servers that are deployed in different parts of the network, offering services to service zones (Gi, Gn, and Gx), are configured and managed centrally at the Grid Master. Using multi-tenancy and DNS views, the entire IP address management (IPAM) and DNS deployment is behind a single role-based, audited interface.

Operational Efficiency

Operators expect NFV and SDN to simplify operational processes when they deploy common automation and provisioning to commodity hardware. As operators fully implement NFV and SDN strategies, orders-of-magnitude greater management efficiencies (10x – 100x) are expected with the use of hypervisors and orchestration systems. Deployment is less complex and risky, since commodity servers can be used for multiple capabilities and can be quickly scaled up, changed, or moved as the network evolves or service requirements change.

The Infoblox Virtual Secure DNS solution supports these efficiency goals, easing the complexity of network transition. With Infoblox Virtual Secure DNS, service providers can quickly and effectively manage their entire platforms, across all networks—physical, hybrid, and virtual—based on the same familiar Infoblox GUI and processes. This decreases deployment time and complexity for network transition and reduces the burden of operational and administrator skill limitations often encountered when new technologies are implemented.

Infoblox
CONTROL YOUR NETWORK

Elastic Scalability Provides Overload Protection

SOLUTION NOTE

Improve Subscriber and Network Protection

Infoblox specializes in DNS-specific attack prevention and visibility. Virtual Secure DNS provides broad protection against DNS-based malware and other DNS-specific attacks including DNS tunneling, data exfiltration, NXDOMAIN, and phantom domain. The solution also protects subscriber devices from becoming infected if they access malicious domains and identifies infected clients for cleanup. The solution takes a live reputation-feed service from the Infoblox global threat ecosystem to create a dynamically updated list of known malicious URLs and IP addresses. When a DNS query reaches an Infoblox DNS server appliance, any match to the reputation-feed list results in redirection or blocking according to the service provider's policy rules configured on the appliance. All actions are logged, and reports can be generated showing all malicious activity.

Automated Kill Chain

Automated threat mitigation removes limitations of manual updates, significantly improving protection levels. The volume and diversity of attacks has exceeded the ability for administrators to manually keep up with the changing landscape. Petabytes of data need to be examined in order to identify infected or rogue devices and mitigate individual security incidents. The Infoblox global security ecosystem provides early detection and automatic updates. The unique automated update of both reputational and identified threats enables an automated kill chain, effectively blocking zero-day threats and often mitigating attacks before they can cause any damage to subscribers or service availability.

Reduce Business and Operations Risk

Infoblox Virtual Secure DNS for service providers delivers the intelligence, performance, and proactive protection service providers need to safeguard their networks, subscribers, and brand as they transition from hardware-based to virtualized environments, providing operational efficiency at the same time.

In addition, the Infoblox solution provides automated network control through the Infoblox Grid, which can free key network operations staff from labor-intensive, costly, and error-prone administrative tasks. The technology automates routine tasks such as updates, patches, and configuration changes, provides a mechanism for automatic, real-time security updates, and provides a single centralized view of the entire network, including both physical and virtualized elements, with advanced reporting visibility for planners and operations teams.

Proven Integration with Standard Orchestrators and Hypervisors

Infoblox has been deployed in cloud and virtualized environments for a number of years. In addition to tight VMware integration, Infoblox also offers OpenStack support for Icehouse, Juno, and Kilo. In fact, Infoblox is included in the OpenStack Liberty platform. Supported hypervisors include VMware, KVM, Xen, and Hyper-V. All Infoblox OpenStack code is freely available to Infoblox customers looking for integration at the github site—where you can also find documentation.

Contact us today to find out more about Infoblox Virtual Secure DNS Solutions for service providers.

About Infoblox

Infoblox delivers critical network services that protect Domain Name System (DNS) infrastructure, automate cloud deployments, and increase the reliability of enterprise and service provider networks around the world. As the industry leader in DNS, DHCP, and IP address management, the category known as DDI, Infoblox (www.infoblox.com) reduces the risk and complexity of networking.

Corporate Headquarters: +1.408.986.4000 1.866.463.6256 (toll-free, U.S. and Canada) info@infoblox.com www.infoblox.com