SOLUTION NOTE

INFOBLOX TRINZIC FLEX FOR SERVICE PROVIDERS

PROVIDING DYNAMIC AND ALWAYS-ON SECURE DNS FOR CARRIER NETWORKS

Service Providers are experiencing business transformations with new trends such as the Internet of Things (IoT), smart devices, mobile connectivity, and transient users that put more stress on carriers in terms of competition, cost control, and revenue per user.

With new technologies like Network Functions Virtualization (NFV) to improve service delivery and minimize risks for current and future investments, the legacy underlying infrastructure often has limited functionality and security and relies on manual processes.

Infoblox Actionable Network Intelligence empowers Service Provider infrastructure transformation initiatives, including NFV, to enable new services and provide additional revenue and upsell monetization opportunities. The Service Provider-grade platform for DNS, DHCP, and IP address management controls, secures and provides visibility to cloud administrators with direct integration, intelligent correlation, and discovery of virtual and legacy physical infrastructure.

ENABLING SUCCESSFUL NFV DEPLOYMENTS

As service providers migrate from physical to virtual to NFV, a common oversight is assuming legacy core network services like DNS and DHCP will handle the new requirements. With deep integration into NFV, and OpenStack and VMware technologies, Infoblox optimizes Service Provider resources by eliminating manual processes and custom scripts and speeds delivery time with integration into provisioning, operations, security, fault, and performance management.

SECURING THE CHALLENGING DNS-BASED THREAT RISKS

An often-overlooked security vulnerability revolves around DNS-based exploits that bypass traditional security approaches. Infoblox Secure DNS protects subscribers through global threat intelligence and automated protection packages. The high-performance solution maintains critical DNS service availability in rapidly evolving networks and even during malicious attacks. Sub-millisecond response and advanced threat protection maintains a low latency and a secure subscriber experience.

SCALING TO MEET CARRIER-CLASS REQUIREMENTS

Carrier deployments require a flexible and scalable infrastructure to handle the dynamic requirements of NFV. Infoblox auto-scaling capabilities allow service providers to optimize investments while having the ability to grow without replacing infrastructure enabling profitable monetization of services. Infoblox Trinzic Flex virtual appliances enable carriers to add specific capabilities across their entire deployment leveraging topology-independent pricing, so carriers experience true workload mobility. Deployments can be a single node or widely distributed with high availability with Trinzic Flex virtual appliances.

ENSURING NFV MANAGEMENT AND ORCHESTRATION (MANO)

One of the fundamental challenges in NFV deployments revolves around interoperability across different vendors and standards compliance. Infoblox is fully ETSI NFV MANO compliant, so carriers can easily leverage Infoblox with other NFV vendors. Infoblox has achieved certifications from multiple vendors including VMware's Telco NFV Ready certification and NFV interoperability testing through independent New IP Agency (NIA).

FLEXIBLE CAPABILITIES AND DEPLOYMENT OPTIONS

With Infoblox Trinzic Flex, service provides can select specific capabilities to be deployed across their infrastructure. Infoblox provides the ability for value-based pricing across the entire deployment and allowing one or more feature capabilities to be leveraged across NFV deployments.

DNS—Authoritative and Recursive

Service providers can enable authoritative and recursive DNS with Trinzic Flex. With Infoblox DNS, you can centrally manage and automate all aspects of DNS using a purposebuilt platform to achieve the high availability, efficiency, security, and application response times you need to thrive in a digitally connected world.

DNS Traffic Control

Instead of deploying costly global server load balancers (GSLB) to ensure availability, Infoblox DNS Traffic Control eliminates costly delays in application response times and allows you to uniquely combine advanced load balancing functionality with DNS management within a single, unified platform.

BloxOne® Threat DefenseSecurity organizations are under tremendous pressure to protect their infrastructure and data from existing and emerging cyberthreats and hazards. A lack of effective threat intelligence leads to poor incident response and slows remediation. Infoblox provides a single solution that collects, aggregates, and manages threat data from internal sources and multiple third-party vendors. In addition, Infoblox enables the selective dissemination of threat data to your existing security infrastructure such as the Infoblox DNS Firewall, SIEMs, next-generation firewalls, vulnerability management systems, endpoint security solutions.

Advanced DNS Protection

Distributed denial of service (DDoS) and other DNS-based threats can flood your DNS servers with malicious requests, bringing down your network. These attacks can redirect users to harmful Internet destinations, exfiltrate data, and expose your customers and business to additional risks. With Infoblox Advanced DNS Protection, you can comprehensively defend your DNS server from the widest range of DNS-based attacks, while maintaining service availability and business continuity.

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

© 2024 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).

Version: 20240226v1