SOLUTION NOTE

SUPERCHARGED DNS INFRASTRUCTURE FOR BROADBAND NETWORKS

Accelerate and protect DNS from core to cloud

The telecommunications industry is undergoing a profound transformation fueled by rapid advancements in mobile and broadband technologies. Innovations like augmented reality, virtual reality, the metaverse, and Industry 4.0 further accelerate this evolution, pushing operator functions further to the edge of the network than ever before.

These advancements are not just about surpassing current standards; they promise to revolutionize connectivity, offering high speed, low latency, and extensive network coverage. Many broadband operators are adept at leveraging cloud technology, adopting cloud-like architectures to meet the evolving demands of modern digital infrastructure. By virtualizing network functions, they can dynamically allocate resources and deploy services faster, ensuring agility in adapting to market conditions and customer needs.

BROADBAND OPERATOR CHALLENGES

Transitioning to cloud-based environments introduces complexities necessitating new network designs and security protocols. Tomorrow's operator networks must be highly resilient, facilitating fast, low-latency performance and robust protection against cyber threats such as hacking, malware, and denial-of-service attacks. These resilient foundations give network administrators with the visibility, context, and control required to navigate complexity, safeguard subscribers and customers, and ensure network resilience in a dynamic environment. As broadband providers modernize to support the network demands of the future — with diverse systems and siloed management — their traditional network infrastructures are being choked by challenges and increasingly attacked by cyber threats.

THE OPPORTUNITY

Broadband networks are expanding – both within their existing network footprint and increasingly into the edge and public cloud. This transition and accompanying industry impact creates numerous challenges for operators. A perpetual priority is ensuring high performance while managing the challenge of cost-effectiveness and scalability in delivering network services at wire speeds anywhere on the network across various physical and virtual form factors. With increasing resource deployments at the network edge and on different cloud platforms, security teams face the difficult task of managing numerous pods, virtual machines (VMs), and containers across physical, virtual, and cloud environments.

Networking and Security Priorities

- **Ultra-low DNS latency.** Operators need to accommodate real-time applications that require fast and smooth communication between users and servers. To achieve this, they need to deploy DNS servers closer to users and optimize the DNS query process.
- **Achieving High Throughput.** Operators face the challenge of delivering high-performance network services anywhere in a cost-effective and scalable way. Wire-line speed, the peak data transfer rate a physical wire or cable can handle, is crucial for virtualized network functions in telecommunications. Maximizing this speed minimizes latency, boosts performance, and unlocks opportunities for bandwidth-intensive, low-latency applications and services.

- **Low-Overhead DNS Logging:** DNS is critical to any CSP, and operators must clearly understand how their DNS functions to ensure the reliability, security, and performance of their networks while aiding in regulatory compliance and optimizing resource utilization. However, using methods like packet capture and syslog is highly inefficient and complex, especially in today's increasingly distributed operator networks.
- **Auto-scaling DDI.** For mobile providers, private and public 5G network slicing allows network operators to create multiple virtual networks on the same physical infrastructure, each with different characteristics and requirements. To support this, network operators need flexible and scalable DDI services that can adapt to the changing needs of each network slice.
- **Delivering DDI Services at the Edge.** This is beneficial as operators increasingly leverage public clouds to support deploying and managing networks and multi-access edge computing (MEC) closer to subscribers and devices. To enable this, network operators need to have distributed DDI services that can support the dynamic and heterogeneous nature of the edge network.
- **Diversity and complexity of attacks.** DDoS attacks pose a significant threat to the telecommunications sector, capable of severely disrupting network, service, and server traffic and potentially inflicting substantial financial losses. Broadband operators face a myriad of attack vectors, including volumetric, protocol, and application layer attacks, each necessitating unique detection and mitigation strategies. DNS disruption interferes with or shuts down critical IT applications like email, websites, VoIP and Software-as-a-Service (SaaS).
- **Manual intervention.** Operators often rely on manual processes to identify and respond to DDoS attacks, which can be slow, error-prone, and resource-intensive.
- **Cost and scalability.** Operators have typically invested in expensive hardware or software solutions to protect their networks from DDoS attacks, which may not be able to scale up or down as needed. As operators expand beyond their traditional network architectures, using different DDoS solutions for operator networks and public clouds can make things more complex because of their varying features, interfaces, and capabilities.

THE SOLUTION: ADVANCED SOLUTIONS BRINGING NETWORKING AND SECURITY TOGETHER

Infoblox, an industry leader in networking and security services, offers best-of-breed Core Network Services with comprehensive security to provide a single end-to-end solution for centralized management of secure, distributed environments. Both solutions are designed for CSP environments requiring scalable edge deployments. DNS Cache Acceleration and Advanced DNS Protection are available in a variety of carrier-grade options, including orchestrated Virtualized Network Function (VNF) and cloud-native solutions, including public clouds.

INFOBLOX DNS CACHE ACCELERATION

DNS Cache Acceleration enhances the speed and scalability of DNS caching, which is the process of storing DNS query results in memory for faster retrieval. DNS caching reduces the latency and bandwidth consumption of DNS queries and the load on authoritative DNS servers, reducing the latency and load on the network. DNS Cache Acceleration can handle millions of queries per second and deliver sub-millisecond response times, even during peak traffic periods. This enhances the user experience and reduces the bandwidth and operational costs.

Features That Matter:

- Designed to handle the "perfect storm" of future mobile and edge-based applications that require ultra-low latency, it supports DNS query rates up to five million queries per second and ultra-low latency of 50 microseconds on average.
- Supports DNSTap, a log format for DNS software that allows operators to monitor and analyses DNS infrastructure performance and security by providing detailed data on queries and responses, including latency, error rates, and source/destination addresses. This data aids in troubleshooting, performance optimization, anomaly detection, and generating reports. DNSTap simplifies logging by eliminating the

need for packet capture or additional software on DNS servers.

- Supports encrypted DNS protocols, including DNS over HTTPS (DoH) and DNS over TLS (DoT), enabling broadband operators to encrypt last-mile DNS communications between their endpoints and DNS servers regardless of which protocol the endpoint supports.
- Supports Type 64 (HTTPS Binding) and Type 65 (SVCB) DNS Resource Records, helping reduce the latency and bandwidth consumption of HTTPS connections, as well as enhance the privacy and security of users. By using Type 64 and Type 65 records, clients can avoid unnecessary DNS queries, TCP connections, and TLS handshakes, and instead connect directly to the optimal server with the desired protocol and encryption settings.
- Provides wire speeds without the overhead and boosts network performance anywhere operators require, even at the edge and on the public cloud, by leveraging technologies such as DPDK and SR-IOV that can optimize packet processing and bypass the overhead of the operating system kernel. These features enable operators to improve network performance, reduce latency, increase throughput, and enhance security.
- Expands DNS efficiency by supporting TCP and UDP protocols to handle different types of DNS queries and scenarios, enabling larger response sizes and greater network compatibility. It also allows for increased flexibility in working with Authoritative and Recursive DNS, enabling operators to streamline their networks for improved efficiency.

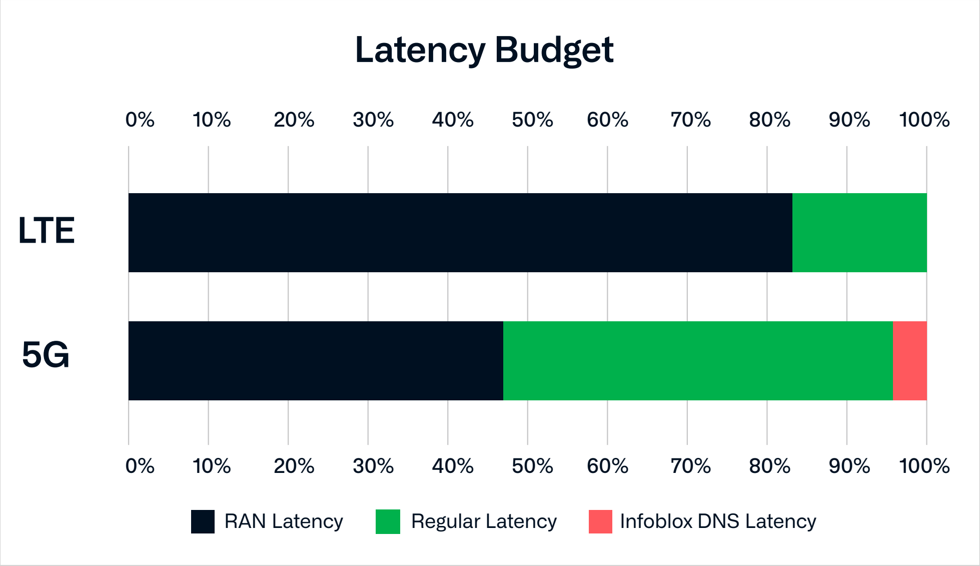

Figure 1: Infoblox DNS Cache Acceleration provides enhanced network performance and unprecedented low levels of DNS query latency

INFOBLOX ADVANCED DNS PROTECTION

With Infoblox Advanced DNS Protection (ADP), your network 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 at the network, protocol and application layers while responding only to legitimate queries by employing Infoblox adaptive threat intelligence. Without the cumbersome need to constantly apply software security patches and cause self-inflicted downtime, with Infoblox, you can take network reliability to the next level by ensuring that your critical network infrastructure — and your business — keeps working at all times.

Features That Matter:

- 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.
- Obtain comprehensive global visibility and reporting, revealing detailed attack points and patterns across your distributed network, alongside centralized insight into network users, device usage, and attack specifics for swift response.
- Utilizes Infoblox Threat Adapt™ technology to automatically update protection against emerging threats by applying independent analysis, research on evolving attack techniques, and insights from customer networks, while also adapting to DNS configuration changes.
- Leverages enhanced processing for threat mitigation by automatically blocking attacks before they reach DNS server applications, utilizing dedicated network packet inspection hardware.
- Supports encrypted DNS protocols, including DNS over HTTPS (DoH) and DNS over TLS (DoT), enabling broadband operators to encrypt last-mile DNS communications between their endpoints and DNS servers regardless of which protocol the endpoint supports.

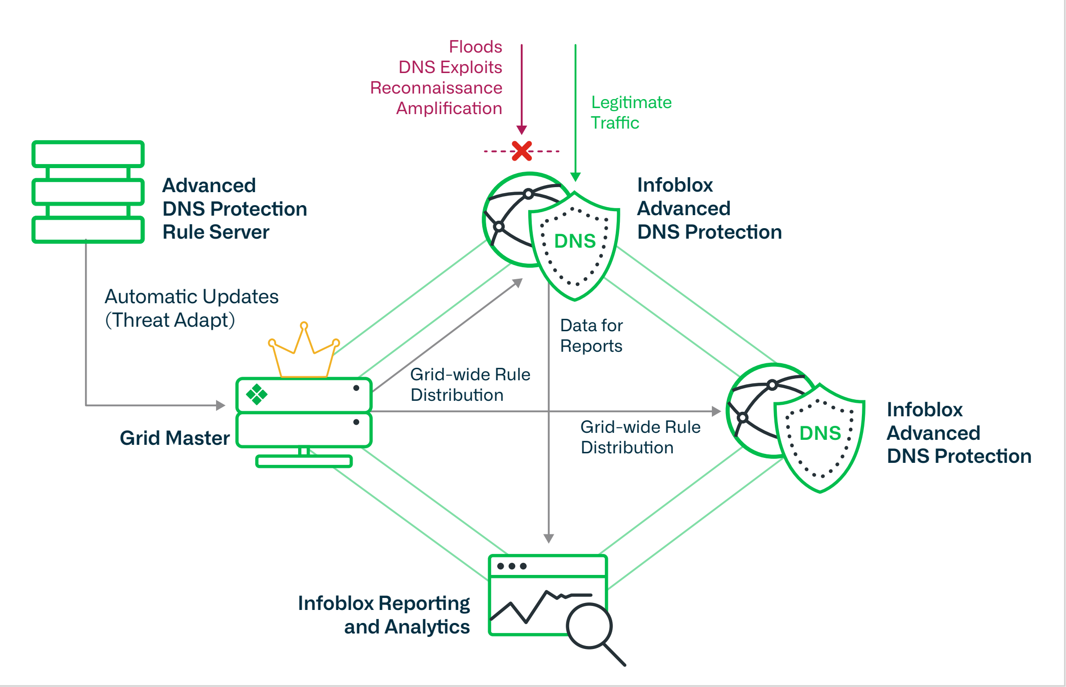
Floods
DNS Exploits
Reconnaissance
Amplification
Legitimate Traffic
Advanced DNS Protection Rule Server
Infoblox Advanced DNS Protection
DNS
Automatic Updates (Threat Adapt)
Data for Reports
Grid-wide Rule Distribution
Grid Master
Grid-wide Rule Distribution
Infoblox Advanced DNS Protection
DNS
Infoblox Reporting and Analytics

Figure 2: Infoblox Advanced DNS Protection provides a unique defense against DNS-based attacks.

NETWORKING + SECURITY: A POWERFUL COMBINATION

Broadband operators gain a dual advantage by combining DNS Cache Acceleration and Advanced DNS Protection. They can expect enhanced performance from network core to network edge through efficient DNS response caching and robust security against diverse DNS threats. By integrating these solutions, Infoblox delivers a comprehensive approach to DNS services, enhancing speed, efficiency, security, and infrastructure resilience. This integration streamlines networking and security efforts, enabling customers to effectively achieve their business objectives.

For instance:

- Broadband operators can utilize Infoblox DNS Cache Acceleration instances as high-speed DNS caching-only name servers, supporting recursive UDP & TCP DNS queries from clients.
- Additionally, operators can deploy Infoblox Advanced DNS Protection as authoritative DNS servers, furnishing authoritative answers to DNS queries for managed domains. These instances can detect and halt DNS attacks through predefined and custom threat protection rules, dropping problematic packets and responding solely to legitimate traffic.
- Infoblox DNS Cache Acceleration instances can forward queries not in their cache to Infoblox Advanced DNS Protection instances, which resolve them by contacting other DNS servers. Responses are then sent back to the DNS Cache Acceleration instances, which cache and serve them to clients.

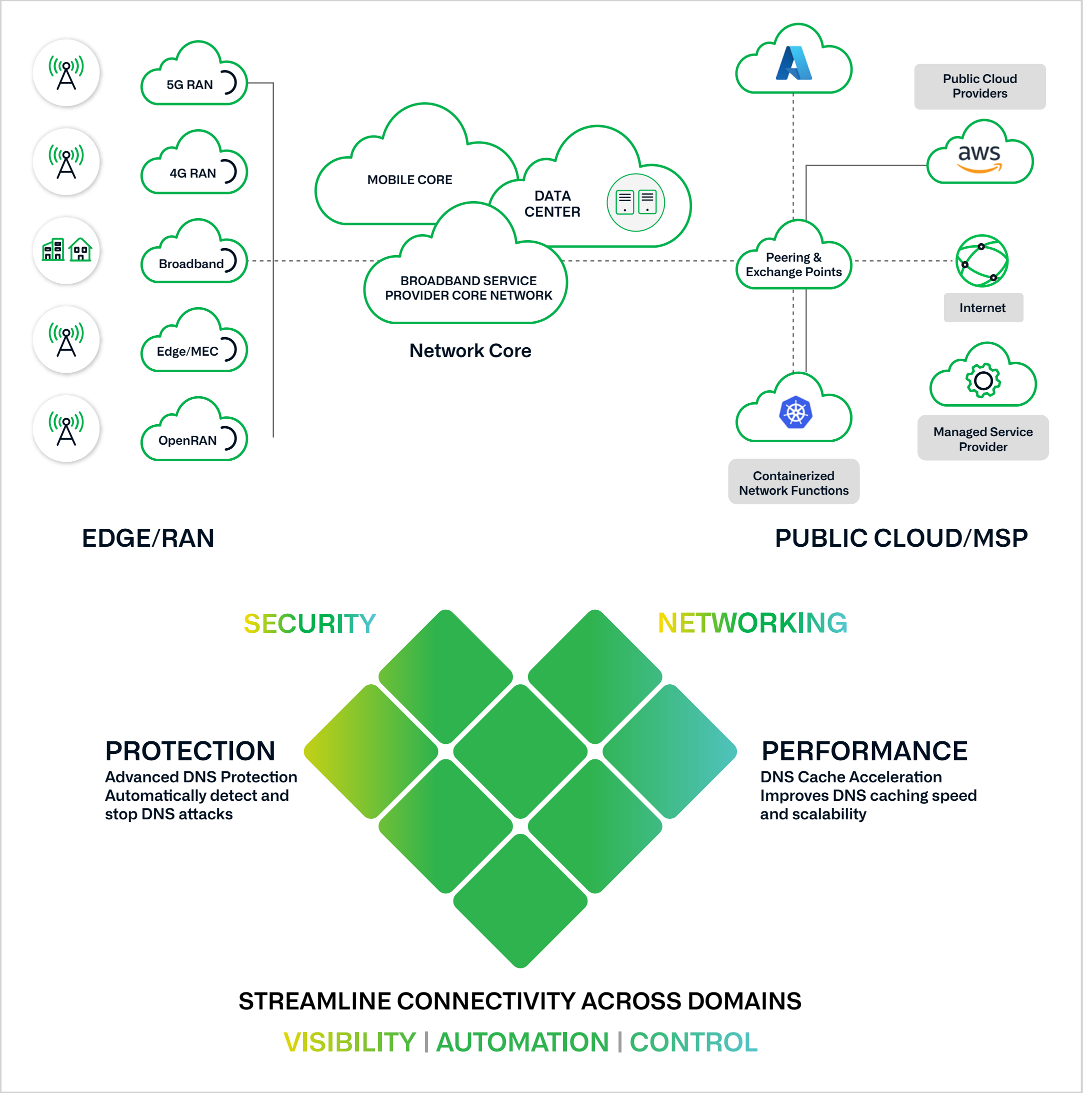
5G RAN
4G RAN
Broadband
Edge/MEC
OpenRAN
MOBILE CORE
DATA CENTER
BROADBAND SERVICE PROVIDER CORE NETWORK
Network Core
Public Cloud Providers
aws
Peering & Exchange Points
Internet
Containerized Network Functions
Managed Service Provider
EDGE/RAN
PUBLIC CLOUD/MSP
SECURITY
NETWORKING
PROTECTION
Advanced DNS Protection
Automatically detect and stop DNS attacks
PERFORMANCE
DNS Cache Acceleration
Improves DNS caching speed and scalability
STREAMLINE CONNECTIVITY ACROSS DOMAINS
VISIBILITY | AUTOMATION | CONTROL

Figure 3: Infoblox Advanced DNS Protection and DNS Cache Acceleration provide enhanced performance and robust security against diverse DNS threats.

UNLEASH YOUR DNS–FROM CORE TO CLOUD

Infoblox DNS Cache Acceleration and Advanced DNS Protection are designed for broadband environments requiring scalable edge and cloud deployments. Both are available in multiple carrier-grade options, including orchestrated Virtualized Network Function (VNF) and cloud-native solutions. Infoblox offers flexibility and scalability tailored to different broadband providers' operations to deploy where you want and scale when needed. And with centralized management, network operators can swiftly instantiate, implement, and auto-scale network services, efficiently managing them across a unified family of devices.

- **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 is covered under the Service Provider License Agreement Program (SPLA).
- **Available on Physical, Virtual and Cloud Platforms:** Both solutions are available as a software subscription add-on to a variety of Trinzic hardware and software appliances, enabling services to run on a common model and supporting on-prem, private and public cloud environments.

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

Version: 20240520v1