SOLUTION NOTE

INFOBLOX ADVANCED DNS PROTECTION FOR BROADBAND PROVIDERS

Protect broadband networks from DNS-based attacks and disruptions

The Domain Name System (DNS) is critical in modern broadband provider networks. Without DNS, subscribers would be expected to remember and input complex IP addresses to access websites, applications, and services, significantly hindering the usability of the modern internet. Moreover, DNS enables essential network functions such as load balancing, traffic management, and fault tolerance, optimizing network performance and reliability. Ensuring DNS infrastructure availability, security, and efficiency is paramount for Service Providers to maintain seamless connectivity and deliver high-quality services to their customers. Operators must protect this vital asset—for their reputations and customers who rely on stable, always-on Internet connectivity. If the DNS service goes down, subscribers are cut off from the Internet. DNS disruption interferes with or shuts down critical IT applications like email, websites, VoIP, and software as a service (SaaS).

NETWORK OPERATOR CHALLENGES

Broadband service providers are witnessing a significant expansion in their operator networks, extending not only within their traditional infrastructure network boundaries but also penetrating deeper into the edge and public cloud environments. This shift brings forth many challenges, particularly in security, as operators navigate the complexities of safeguarding their expanded network infrastructure against evolving threats and vulnerabilities.

Threats range from disruptive DDoS to nefarious specially crafted and targeted DNS-application and protocol level attacks:

The telecommunications & broadband services sector faces severe and continuous threats from DDoS and application-level DNS-based attacks, including tunneling, which can disrupt network infrastructure and applications and pilfer subscriber and/or provider intellectual property. Recent statistics highlight the impact of these attacks:

- In the first half of 2023, cybercriminals launched approximately 7.9 million DDoS attacks, marking a 31% year-over-year increase.[1]
- In 2022, 78% of DDoS attacks targeted the application layer of the OSI model, 17% hit the network and transport layers, and 3% targeted DNS.[2] These statistics underscore the growing frequency, sophistication, and damage caused by DDoS and DNS-based attacks, posing a significant challenge for

1 https://www.darkreading.com/cyberattacks-data-breaches/netscout-identified-nearly-7-9m-ddos-attacks-in-the-first-half-of-2023

2 https://www.infosecurity-magazine.com/blogs/2022-ddos-yearinreview/

KEY FEATURES

Reduce Business Disruptions: Infoblox Advanced DNS Protection (ADP) continuously monitors, detects and stops all types of DNS attacks— including volumetric and non-volumetric types like exploits and hijacking. It ensures DNS integrity and offers a secure foundation for your network, guaranteeing high availability.

Adapt to Evolving Threats: Infoblox ADP uses Infoblox Threat Adapt™ technology to automatically update protection against emerging threats. It applies independent analysis and research to evolving attack techniques, including insights from customer networks, ensuring continuous adaptation of protection to reflect DNS configuration changes.

Gain Single-Pane-of-Glass Visibility: With Infoblox, your organization 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 points across the network and attack sources, supplying the intelligence necessary for threat management. It is integrated with our DNS solution.

telecom service providers to ensure their networks and services' resilience and reliability.

Non-Malicious Disruptions: Non-malicious DDoS attacks are rare occurrences in which a large amount of traffic is unintentionally directed to a target, causing a denial-of-service condition without malicious intent. These events can happen due to misconfigurations, software bugs, or unexpected events. For example:

- **Overwhelming Popularity:** Sometimes, websites experience an unexpected surge in legitimate traffic that can resemble a DDoS attack. For instance, when a small business gets featured on a popular TV show or a viral social media post, its website might receive more traffic than it can handle, leading to a temporary denial of service. In 2016, the popular game Pokémon Go experienced a non-malicious DDoS attack when millions of users tried to access the game servers simultaneously, overwhelming the capacity and causing outages.[3]
- **Misconfigured Devices:** There have been instances where poorly configured networked devices unintentionally sent out large amounts of network requests, which caused disruptions like a DDoS attack. An example of this could be a botched software update that triggers excessive communication between devices on a network, overwhelming the infrastructure.

Edge Forward Transformation: However, as telecoms embrace edge computing to bring resources closer to end-users, the traditional centralized approach to caching faces challenges. Deploying distributed caching mechanisms at the edge becomes imperative to ensure optimal performance and minimize latency.

Increasingly Dynamic Networks: Nevertheless, the dynamic nature of telecom networks, exacerbated by the rapid deployment of 5G technology and the proliferation of IoT devices, introduces complexities that traditional caching strategies may struggle to address. Providers must employ adaptive caching mechanisms capable of dynamically adjusting to changing network conditions and traffic patterns.

Navigating the Shift to Public Clouds: Operators increasingly embrace cloud computing to augment their infrastructure scalability, agility, and cost-effectiveness. However, this shift to public clouds necessitates rethinking DNS caching strategies to accommodate the distributed nature of cloud-based deployments. Traditional centralized caching architectures may prove inefficient or inadequate in cloud environments characterized by dynamic resource provisioning and geographically dispersed data centers. Telecoms must leverage cloud-native caching solutions that seamlessly integrate with cloud platforms, ensuring optimal performance and scalability while minimizing operational overhead.

Flexible and Scalable DNS Security: Infoblox ADP is adaptable to diverse deployment scenarios and operator needs and can be easily deployed as a subscription add-on to both virtual and physical Trinzic appliances–including public cloud platforms.

THE OPPORTUNITY

Operator networks are expanding – within their existing telco network footprint and increasingly into the edge and public cloud. This transition and accompanying industry impact creates numerous challenges for network 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.

3 https://www.engadget.com/2016-07-16-pokemon-go-expansion-and-ddos-attack.html

Networking and Security Priorities

- **Ultra-low DNS latency.** Telcos now need to accommodate real-time applications that require fast and smooth communication between users and servers. To achieve this, network operators need to deploy DNS servers closer to users and optimize the DNS query process.
- **Achieving High Throughout.** Telecoms 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.
- **Auto-Scaling.** Telcos often rely on manual processes or managing their DDoS protection. To support expanding networks supporting many more devices, network operators need flexible and scalable services that can automatically adapt to changing demands.
- **Delivering DDI Services at the Edge.** Delivering DDI Services to the Edge. This is beneficial as operators increasingly leverage public clouds to support deploying and managing private and public 5G network slices 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.
- **Reduced Manual Intervention.** Manual DNS caching management can be inefficient, unreliable, and insecure in modern telecom networks. It can also be resource-intensive, demanding significant memory, storage, and bandwidth to maintain DNS records. This manual intervention also introduces redundancy and inconsistency across cache servers, leading to potential data disparities. This can potentially slow down query responses, increase latency, and expose networks to vulnerabilities and attacks due to possible server failures or compromises.
- **Lower Costs and Increase Scalability.** Inefficient DNS caching can negatively impact telecom networks' costs and scalability. If the cached records are outdated or inaccurate, the DNS resolver may need to query other servers repeatedly, increasing the latency and bandwidth consumption for the clients. Also, if DNS caching is not managed correctly, DNS resolvers may need to refresh records more frequently, generating more network traffic and increasing the load on the authoritative name servers.

THE DNS THREAT LANDSCAPE

Here are some of the most common and severe DNS threats confronting your organization.

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

Attack Name	Type	How It Works
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 tunnelling 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

THE SOLUTION: INFOBLOX ADVANCED DNS PROTECTION

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 telecommunications networks.

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 subscribers—keep working at all times.

To safeguard DNS, operators may typically use various solutions like load balancers, IPS, firewalls, generic DDoS protection, and cloud-based options. However, these measures fall short against advanced threats, lacking specificity to address DNS vulnerabilities like cache poisoning, amplification, and hijacking, and adding complexity and cost to the infrastructure.

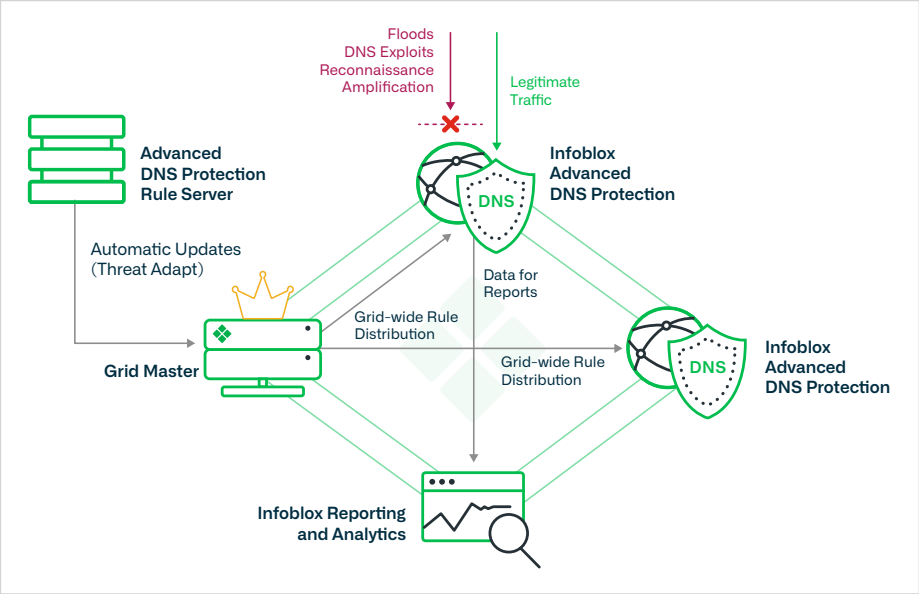

Figure 1: Infoblox Advanced DNS Protection provides a unique defense against DNS-based attacks.

Advanced DNS Protection is a purpose-built, DNS-specific solution offering comprehensive protection. It detects and thwarts attacks at the root, preventing spoofing and hijacking and enhancing performance and resilience. It seamlessly integrates with your existing DNS setup, eliminating the need for costly overhauls. DNS-specific defense solutions ensure robust security and reliability, mitigating the shortcomings and risks of generic alternatives.

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 telcos to encrypt last-mile DNS communications between their endpoints and DNS servers regardless of which protocol the endpoint supports.
- It allows deployment anywhere and scaling as needed, even at the far edge and on public cloud platforms. Network operators can efficiently instantiate, implement, and auto-scale network services through centralized management across a unified family of devices. Infoblox can be deployed as a subscription add-on to virtual and physical Trinzic appliances, including instances on popular public cloud platforms.

PROTECT DNS–FROM CORE TO EDGE TO CLOUD

Advanced DNS Protection Effective DDoS protection helps broadband providers maintain service continuity, protect their reputation, and ensure customer satisfaction in the increasingly complex and distributed network environments combining existing core networks, edge computing and public cloud platforms. It offers flexible and scalable DNS protection, tailored to various deployment scenarios and operator requirements, and is available in multiple carrier-grade options–including orchestrated Virtualized Network Function (VNF) and cloud-native solutions. 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:** Software Advanced DNS Protection is 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.

NETWORKING AND SECURITY: A POWERFUL COMBINATION

Infoblox unites networking and security by offering two complementary solutions that help broadband operators boost the security and performance of DNS resolution in their networks. In addition to Advanced DNS Protection, Infoblox DNS Cache Acceleration (DCA) 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, as well as the latency and load on the network. DCA 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.

Better Together

By combining Infoblox Advanced DNS Protection with DNS Cache Acceleration with, broadband operators gain a dual advantage. From network core to network edge, they can expect enhanced performance through efficient DNS response caching and robust security against diverse DNS threats. This synergy ensures a fast, reliable, secure network experience, instilling confidence in the operators about the improvements they can expect in their network operations.

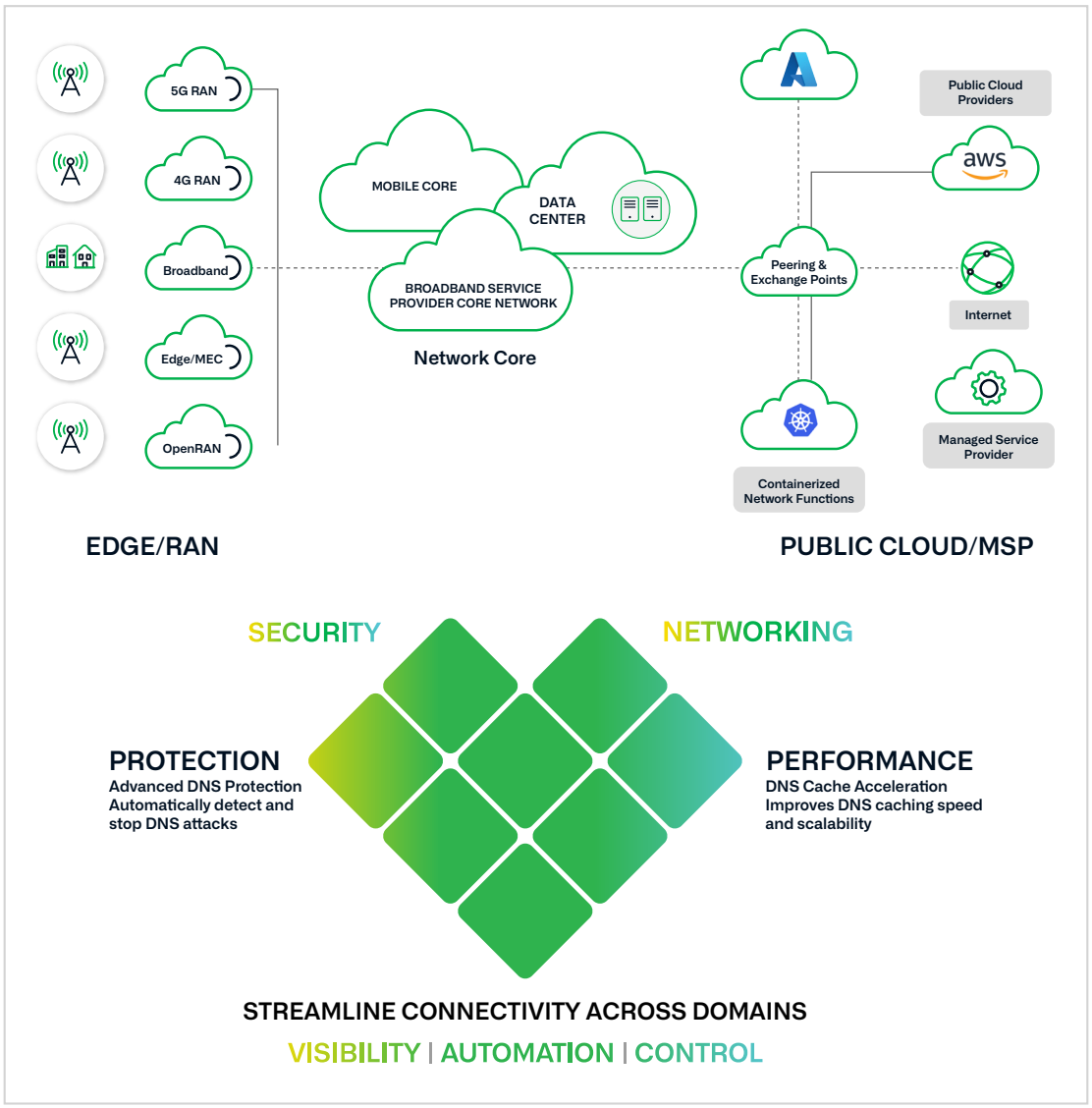

Figure 2: Infoblox Advanced DNS Protection, combined with DNS Cache Acceleration, provides enhanced performance and robust security against diverse DNS threats.

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