SOLUTION NOTE

Secure DNS for Mobile Service Providers

SUMMARY

Security and speed are two of the top subscriber and enterprise selection criteria for choosing a mobile service provider, with most subscribers listing security as more important to them than access to the latest devices. Unsecured devices put mobile network assets at risk, and dissatisfied subscribers can damage a trusted, valuable brand and reputation. Excessive network delay or latency can have a profound effect on subscriber experience where subscribers expect close-to-instantaneous network response. Infoblox Secure DNS provides highly cost-efficient management and control, a superior subscriber experience, and deep protection from a wide range of DNS attacks and malicious domains.

Protect Subscribers from Growing Malware Threats

Malicious software is a real threat. Every year, millions of smartphone users experience undesired behavior on their phones, such as sending unauthorized text messages or accounts accessed without their permission—symptoms indicating the presence of malicious software.

Security has risen to the top of subscriber and enterprise criteria for choosing mobile service providers, with most consumers listing security as more important than access to the latest devices. Still, many consumers don't take even minimal security measures, such as using a screen lock, backing up data, or installing an application to locate a missing phone and remotely erase data from it. Subscribers are surprisingly lax in applying security solutions to their own devices, yet quick to place blame on mobile operators.

Significant Business Risks for Mobile Service Providers

Unprotected subscribers create high cost and reputation risks for mobile operators. Unwanted activities from applications, even those freely downloaded and accessed by the subscribers themselves, will negatively affect the brand reputation of the mobile operator, increasing churn and reducing upsell revenue opportunities. These risks include:

- **Customer dissatisfaction:** Unhappy subscribers with infected devices increase expensive trouble calls to customer care and cause subscribers to leave altogether.
- **Service disruption:** Malicious hackers can control infected devices and send traffic floods into the network. Hackers can even exfiltrate data from subscriber devices using a variety of techniques.
- **Unauthorized premium services:** Once discovered, the charges must often be credited back to the subscriber, adding costs for processing.
- **Negative revenue impact:** The use of imposter services replaces the use of legitimate, revenue-generating services. Potential upsell opportunities are lost as victimized subscribers might now be eager to purchase a premium service from another provider to prevent such breaches.

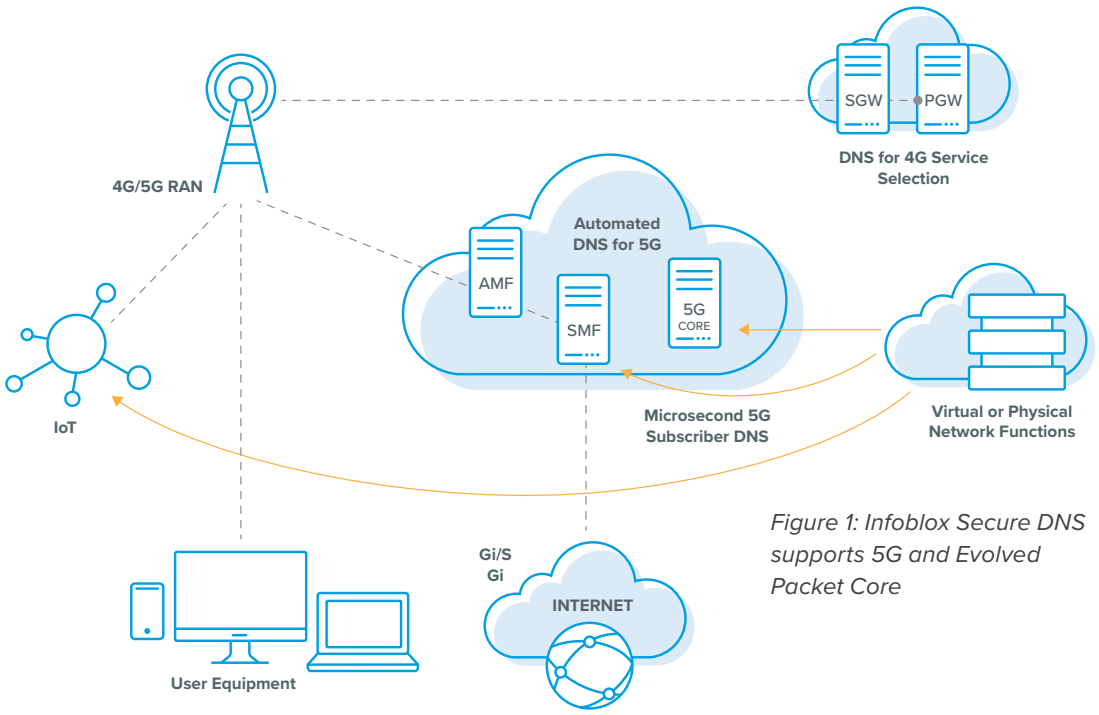

Figure 1: Infoblox Secure DNS supports 5G and Evolved Packet Core

With 5G—Latency Matters More Than Ever

In addition to security, speed matters enormously. At 5 milliseconds, current DNS latency is too high to support many 5G applications. For example, in 5G deployments, AR/VR, gaming, connected cars, and telesurgery will require end-to-end latency of 1-10 milliseconds. Current DNS latency is unacceptable. The pervasive connectivity of 5G will increase reliance on edge computing, which brings cloud resources—compute, storage, and networking—closer to applications, devices, and users. 5G implementations will require greater use of small cell stations at the very edge of the network, so data need not travel long distances to a cloud or data center. To ensure unhindered traffic flow at the edge, Secure DNS services must also be positioned at the edge.

Infoblox Secure DNS Protects Brand Reputation

Infoblox Secure DNS for service providers protects subscribers through global threat intelligence and automated protection packages. The solution maintains critical DNS service availability in rapidly evolving networks with growing traffic and even keeps traffic moving during a distributed denial of service (DDoS) attack. When combined with patented Infoblox Grid™ technology, the solution further ensures optimal operator visibility and control across all DNS infrastructure, including automated kill chain during security incidents. This enables quick detection of any service- threatening attacks while easing operational costs and increasing manageability.

DNS Firewall Keeps Subscribers Safe and Reinforces Brand Integrity

Infoblox DNS Firewall protects against advanced persistent threats and malware by identifying infected devices and preventing them from accessing known malicious domains. Infoblox DNS Firewall leverages multiple monitoring feeds for timely updates on the global threat landscape, providing fast and comprehensive protection for subscribers.

If subscribers, applications, or devices attempt to access a known malicious domain, they are blocked and presented with an operator-designed notification screen or redirected to an alternative site. This maintains subscriber confidence and reinforces the operator's reputation for high protection. Operatorsretain maximum flexibility and can include local, operator-specific threat feeds and customized whitelists and blacklists as desired to prevent erroneous blocking of non-malicious sites.

Advanced DNS Protection for Service Providers Maintains Service Availability

Service degradations and outages are a significant cause of subscriber churn. Denial of service (DoS) attacks and volumetric floods or DDoS attacks targeting DNS infrastructure can cause service degradation, slow down DNS response, or impede subscriber ability to access favorite domains. Infoblox Advanced DNS Protection for Service Providers maintains service availability, critical DNS functionality, and performance during an attack or unexpected traffic spikes generated by rapidly evolving networks, misconfigured devices or applications, emergencies, and network outages.

Rapid Detection Reduces Subscriber Complaints

The growing sophistication of DNS attacks makes it easier for them to remain undetected by large organizations, and many operators still report limited visibility into attacks. Without a DNS-specific protection plan that includes monitoring, central visibility, and continuous threat updates, service providers might remain unaware of DDoS attacks until subscribers complain. Infoblox Secure DNS with Grid management provides full visibility of DNS elements across the network, allowing operators to reduce detection time to minutes. This centralized management and control provides timely updates of threat heuristics to all DNS elements simultaneously and allows any needed configuration changes to be quickly administered.

Automated Kill Chain Enables Protection to Keep Pace against New Threats

Automated threat mitigation removes limitations of manual updates, significantly improving protection levels. The sheer volume of attacks has exceeded the ability of administrators to keep up with the changing landscape. Petabytes of data need to be combed through 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.

Robust and Cost-Effective DNS Cache Acceleration to Maximize the Subscriber Experience

Excessive network delay or latency can have a profound effect on subscriber experience where both Internet-based businesses and subscribers expect close-to-instantaneous network response. Response delays have been shown to negatively impact revenue for service providers' enterprise customers such as web-services companies and financial institutions; and slow-responding legacy DNS cache servers can cause significant latency in a network connection.

Infoblox DNS Cache Acceleration solutions are designed to handle the "perfect storm" of future 5G and edge-based applications that require ultra-low latency—supporting DNS query rates up to five million queries per second as a stand-alone appliance. Through centralized management, network operators can quickly instantiate, implement, and auto-scale network services and manage those services more efficiently through a unified family of devices. Infoblox virtual appliance software leverages x86 hardware virtualization technology to provide ultra-low latency of 50 microseconds on average.

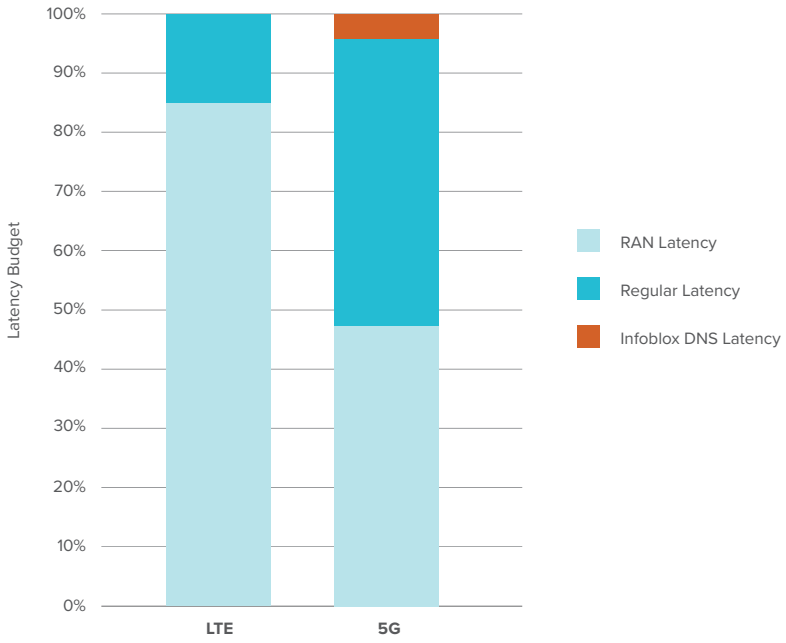

Figure 2: The Infoblox Advantage—Ultra-Low Latency for 5G

Why Infoblox

Advanced DNS Protection for Service Providers

Infoblox Advanced DNS Protection for Service Providers provides intelligent detection and mitigation of malicious attacks that can impair service quality and availability to subscribers. Advanced capabilities include:

- Built-in intelligent attack protection keeps track of source IP addresses of DNS requests, and the DNS records requested.
- Intelligent dropping of excessive DNS requests from the same IP address conserves resources needed to respond to legitimate requests.
- Dedicated network packet inspection hardware and automated threat intelligence rules stop protocol-based attacks such as DNS amplification, reflection, and cache poisoning.
- Active monitoring of the latest DNS-based vulnerabilities ensures that the solution protects against attacks out of the box.
- Automatic rule set updates protect against new and evolving attacks without the need for downtime or patching.

Infoblox DNS Firewall

With the Infoblox DNS Firewall, service providers can now provide broad protection against DNS-based malware. DNS

Firewall protects subscriber devices from becoming infected by accessing malicious domains and identifies infected clients for cleanup. DNS Firewall 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.

Specific features provide:

- **Flexible threat feeds:** Optimal customization for local operator environments via local and subscription-based threat feeds
- **Notification:** A mechanism for in-browser notification or redirect for a walled-garden implementation
- **Analytics:** Insightful reporting on malicious DNS queries, including threat severity and impact, and pinpointing of infected devices

Infoblox DNS Cache Acceleration

With Infoblox DNS Cache Acceleration, service providers can deliver subscribers unprecedented low levels of DNS query latency. This enables traffic from the latest applications such as Internet gaming, virtual reality/augmented reality, content sharing, and social media to be handled, providing a rapid Internet response time that ultimately ensures a high level of user satisfaction. Infoblox offers the most robust and cost-effective DNS caching infrastructure solutions:

- Available is an easy software subscription add-on to the latest generation of our IB-FLEX and Trinzic appliances, providing ultra-low latency of 50 microseconds on average for a superior subscriber experience
- Reduces the cost of ownership—do more with the same headcount by eliminating repetitive and labor-intensive server administrative tasks and eliminating generic server support costs
- Leverages existing hardware, which means that providers only need to upgrade software that runs on the hardware resulting in minimal incremental cost for upgrades

Protect the Subscriber—Protect Your Brand

The Infoblox Secure DNS solution for mobile service providers delivers the intelligence, performance, and proactive protection that service providers need to safeguard their networks, subscribers, and brand.

This carrier-grade solution can detect and mitigate attacks, block malware communications, and keep services running—even while under attack. Subscribers and enterprise customers stay up and running, and the operator brand stays intact.

Also, Infoblox automated network control solutions can free key network operations staff from labor-intensive, costly, and error-prone administrative tasks. Patented Infoblox Grid technology automates routine tasks such as updates, patches, and configuration changes. It provides a single centralized view of the entire network, with advanced reporting visibility for planners and operations teams.

Contact us today to discover more about Secure DNS for Mobile Service Providers.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com