Secure DNS for Mobile Service Providers

Infoblox
CONTROL YOUR NETWORK

Summary: Security is one 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. 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

Most consumers list security as more important to them than access to the latest devices, yet according to *Consumer Reports*, almost 40 percent of consumers surveyed 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 or remotely erase data from it. Mobile subscribers are surprisingly lax in applying security solutions to their own devices, yet quick to place blame on service providers.

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, negatively impact the brand reputation of the mobile operator, increasing churn and reducing upsell revenue opportunities.

- **Customer dissatisfaction**: Unhappy subscribers with infected devices increase expensive trouble calls to customer care or 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 usage**: Once discovered, the charges must often be credited back to the subscriber, adding costs for processing.
- **Negative revenue impact**: Use of imposter services replaces use of legitimate, revenue-generating services. Potential upsell opportunities are lost as subscriber victims might now be eager to purchase a premium service that could prevent such breaches from another provider.

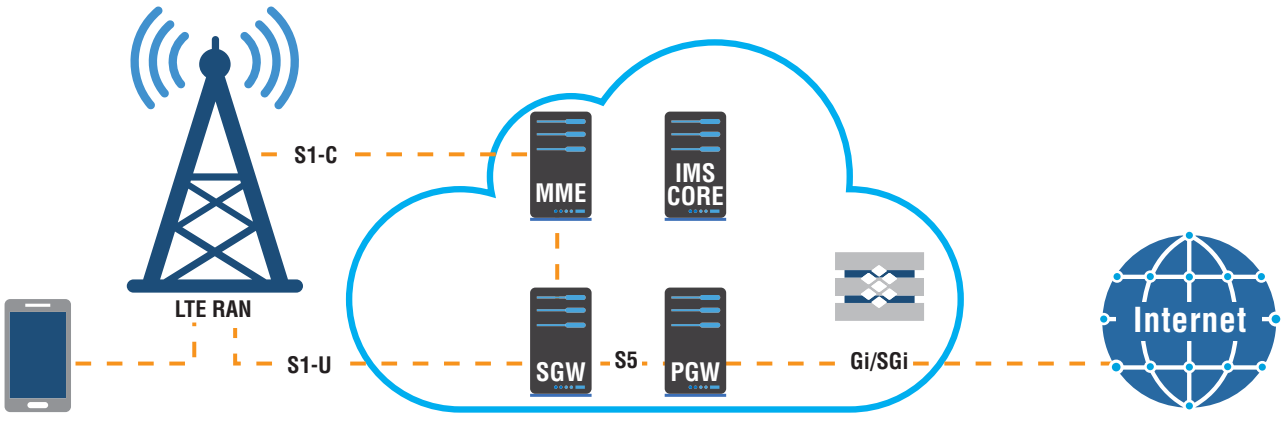

Figure 1: Infoblox Secure DNS supports the Evolved Packet Core.

Secure DNS for Mobile Service Providers

Infoblox
CONTROL YOUR NETWORK

Infoblox Secure DNS Protects Brand and Reputation

Infoblox Secure DNS for mobile network operators protects subscribers through use of global threat intelligence and automated protection packages. The solution maintains critical DNS service availability in rapidly evolving networks, growing traffic, and even during a malicious DDoS attack. When combined with patented Infoblox Grid™ technology, the solution further ensures optimal operator visibility and control across all Infoblox DNS infrastructure. The solution enables quick detection of any service-threatening attacks while easing operational costs and increasing manageability.

Infoblox DNS Firewall Keeps Subscribers Safe and Reinforces Brand Integrity

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 to the global threat landscape, providing fast and comprehensive protection for subscribers.

If subscribers, applications, or devices attempt to access a malicious domain, they are blocked and presented with an operator-designed notification screen or redirected to an alternate site. This maintains subscriber confidence and reinforces the operator reputation for high protection. Operators retain 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 degradation and outages are a significant cause of subscriber churn. Denial of service (DoS) attacks and volumetric floods or distributed denial of service attacks (DDoS) targeting mobile network DNS infrastructure can cause service degradation, slow DNS response, or impede subscriber access to domains over the mobile network. Advanced DNS Protection for Service Providers maintains service availability, critical DNS functionality, and performance during volumetric DDoS attacks or unexpected traffic spikes generated by rapidly evolving networks, misconfigured devices or applications, emergency situations, or network outages.

Rapid Detection Reduces Subscriber Complaints

The growing sophistication of DNS attacks makes it easier for them to remain undetected by large service provider organizations, and many operators still report limited visibility to attacks. Without a DNS-specific protection plan that includes monitoring, central visibility, and continuous threat updates, service providers may 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 updating of new threats to all DNS elements simultaneously and allows needed configuration changes to be quickly administered.

Automated Kill Chain Provides Protection to Keep Pace against New Threats

Automated threat mitigation removes the limitations of manual updates, significantly improving protection levels. The sheer volume 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.

Why Infoblox?

Advanced DNS Protection for Service Providers

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

- Built-in intelligent attack protection keeps track of source IP addresses of DNS requests, as well as the DNS records requested.
- Excessive DNS requests from the same IP address are dropped intelligently, saving resources 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.
- Infoblox actively monitors the latest DNS-based vulnerabilities and ensures that the solution provides protection against attacks out of the box.
- Automatic rule set updates provide protection against new and evolving attacks without the need for downtime or patching.

Secure DNS for Mobile Service Providers

Infoblox
CONTROL YOUR NETWORK

Infoblox DNS Firewall

With the Infoblox DNS Firewall, mobile network operators can now protect subscribers against DNS-based malware. DNS Firewall protects subscriber devices from becoming infected via 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 a combination of local and subscription-based threat feeds
- **Notification**: A mechanism for in-browser notification or redirect, or walled garden implementation
- **Analytics**: Insightful reporting on malicious DNS queries including threat severity and impact and pinpointing of infected devices

Infoblox Carrier-grade DNS Appliances

Infoblox builds hardware-based DNS attack detection and protection into the Infoblox 4030 and PT-series appliances. This specialized hardware drops attack traffic and passes legitimate traffic, offloading the DNS server engine from DDoS protection and from processing malicious DNS traffic and preserving a low-latency web experience for subscribers. The IB-4030 is one of several classes of appliances for service providers. For a full listing of Infoblox appliances, see the *Infoblox Appliance Guide.*

Protect the Subscriber—Protect Your Brand

The Infoblox Secure DNS solution for mobile service providers delivers the intelligence, performance, and proactive protection 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 brand stays intact.

In addition, 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; and provides a single centralized view of the entire network, with advanced reporting visibility for planners and operations teams.

Contact us today to find out more about Secure DNS for mobile 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