infoblox

CASE STUDY

# Infoblox network infrastructure refresh helps major Middle Eastern telecom operator modernize and position its network for growth

## OVERVIEW

### Today's 5G wireless technology will transform how we live, work and play.

More than just greater bandwidth or faster download speeds, 5G represents a revolution in wireless data throughput capabilities, especially for enterprises. It gives communication service providers the chance to become leading innovators in future technologies and play a foundational role in emerging business models. Meeting the demand, however, will take next-generation communication networks. That's why this service provider chose Infoblox solutions to refresh and modernize its core networking infrastructure—to support a virtualized, software-driven 5G and wireline broadband network. Infoblox features—such as automated DNS, DHCP and IP address management (DDI), microsecond DNS latency and protection against DDoS attacks—supply the technological underpinning this provider needed to build its 5G network and accommodate future wireless and wireline expansion.

## THE CUSTOMER

Headquartered in the Middle East, this award-winning telecommunications service provider serves approximately 9 million individual customers with mobile, fixed broadband Internet, and home services over its 4G LTE and 5G networks. As one of the fastest-growing operators in the region, the service provider holds a significant position in region with a goal of 5G coverage for 90 percent of the population. The company also provides services to over 100,000 businesses with its vast information and communication technologies and managed services range.

*Industry:* *Telecommunications*
*Location:* *Middle East*

**INITIATIVES:**

- Refresh and modernize core networking infrastructure
- Accommodate 5G and wireline broadband scalability and growth
- Improve speed, flexibility, efficiency and automation

**OUTCOMES:**

- Well-positioned to take advantage of future 5G and wireline business opportunities
- Simplified operations, effortless scalability, clearer financial predictability
- Built-in security for foundational protection security posture

**SOLUTIONS:**

- Infoblox NIOS
- Infoblox Grid technology
- DNS Cache Acceleration
- Authoritative and recursive DNS
- Advanced Reporting and Analytics
- Advanced DNS Protection
- Infoblox Trinzic Flex, Service Provider Licensing and Subscription Pricing
- BloxOne® Threat Defense

## THE CHALLENGE

### Modernizing networks to accommodate massive growth

A long-standing Infoblox customer, the company was highly pleased with Infoblox's proven reliability and existing architecture design. Thanks to the original resilient Infoblox implementation and design, the service provider has experienced high levels of dependability. How resilient? Since the company was using only approximately 40 percent of its capacity, it weathered the 2021 Facebook outage without the issues that forced many service providers worldwide to adjust their DNS infrastructure so they, too, would not experience downtime.

An upcoming tech refresh prompted IT decision makers at the company to consider an upgrade to Infoblox's next-generation telco data center solutions. From a business perspective, the priority was to continue to meet future capacity and efficiency requirements while maintaining the excellent performance its subscribers enjoy. The network had grown and expanded using physical network functions, making it difficult to scale for an unprecedented number of future subscriber devices across its wireless and wireline broadband networks. The service provider had also used older enterprise contracts requiring time to add licenses to expand, which meant that it needed to build out additional capacity to handle spikes in subscriber traffic. Newer service provider options based on usage-based pricing models would furnish financial predictability, lower operational costs and design flexibility. They would also enable the business to quickly expand the network without having to worry about contracting new licensing for individual virtual network functions or features.

## THE SITUATION

### A highly dynamic provider focused on the future

The service provider is based in a country that is a global trade, tourist and banking powerhouse. It's also predominantly a migrant-populated country; roughly 90 percent of its 10 million+ population are foreign born, most working on temporary employment contracts across white-collar, blue-collar and service industry jobs. On top of the citizen and foreign worker population, millions of tourists visit the country each year. While pre-pandemic figures topped 5 million visitors yearly, over 8 million visitors attended an international exposition in the capital city in 2020. The dynamic expansion and retraction of data traffic and network use set off by these factors point to how difficult traffic forecasting for network planning and dimensioning can be for today's providers. They also illustrate the need for flexible networks that can rapidly expand.

The company's IT team realized that their network required a cloud focus to reach new levels of speed, flexibility, efficiency and automation. Specifically, the automation of DNS, DHCP and IP address management (DDI) would be central to this effort–and is critical in the rollout of 5G radios, and the next generation of 5G core and edge-based services. Like many other providers, the company will be deploying massive numbers of new radio sites and concentrating its mobile, fixed broadband and backhaul networks to handle enormous traffic growth. At the same time, security is increasingly becoming a top subscriber and enterprise concern. Unsecured devices put mobile network assets at risk, and dissatisfied subscribers can damage a trusted, valuable brand and reputation. As compute and storage at the edge based on the MEC architecture enables new types of service processing and delivery at thousands of new locations close to the UE, the potential for security threats from third-party applications at the edge or external attackers increases dramatically.

## THE SOLUTION

### Simplified operations, effortless scalability, financial predictability and an improved security posture

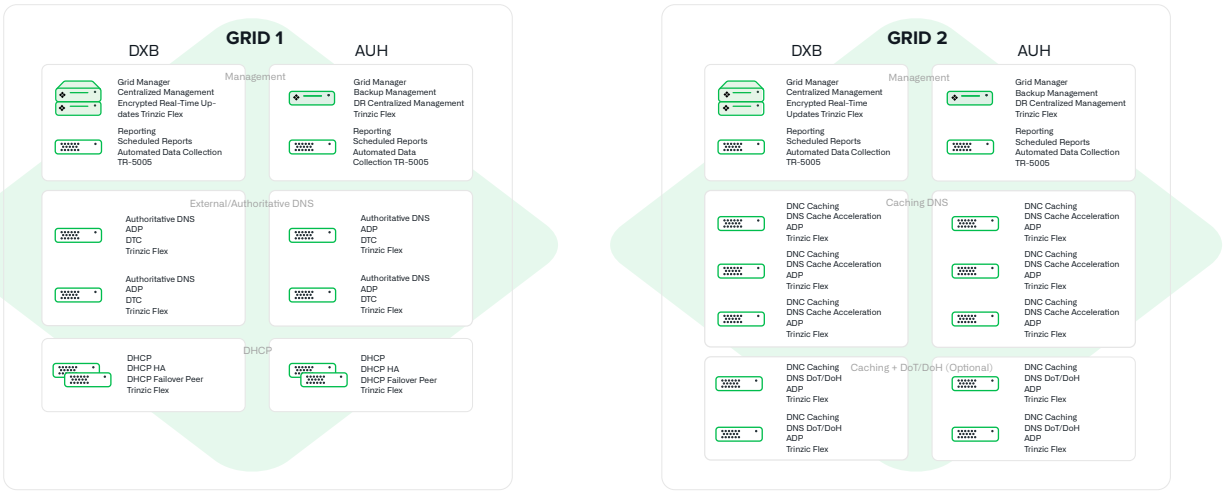
Infoblox's highly resilient DDI solution comprises physical Infoblox appliances running virtualized network functions (VNFs), including DNS caching, DNS cache acceleration, DHCP and IP address management (IPAM) within a single Infoblox Grid. Infoblox is a major embedded component of this provider's network. Additionally, the company's operations teams are so familiar with Infoblox solutions that they rarely submit trouble tickets and are comfortable fixing any issues that arise.

Despite the Infoblox team already working closely with the provider's operations manager and network design/implementation staff, its procurement team issued an RFP in spring 2021 soliciting other technology vendors to submit proposals for the DDI elements of the network refresh. Company decision makers wanted an end-to-end DDI solution from a single vendor based on their success with Infoblox. After several rounds of review with competing solutions providers, the team decided to move forward with an Infoblox solution that combined several key products.

## Infoblox Grid

Infoblox Grid technology empowers this provider with highly efficient management and control, freeing key technical and network operations staff from labor-intensive, costly and error-prone administrative tasks. Infoblox proposed two options:

- Migrate the existing production Grid to a new Grid but add greater reporting capabilities.
- Migrate DHCP and authoritative DNS instances in the existing production Grid to a new Grid, then migrate the current DNS cache in production to its new second Grid. Here, each Grid would have its own management and reporting indexing.




*Figures 1 and 2: Infoblox refresh supports the service provider's 5G buildout with increased flexibility, control and foundational security.*

Both options would include three new features that were not available when the service provider built out the original configuration: Trinzic Flex and Service Provider Licensing. IT team leaders wanted to increase the agility of their existing infrastructure to keep pace with changing business demands. Even when providers have leveraged virtualized network functions, many solutions rely on fixed resources that cannot be easily changed.

- **Infoblox Trinzic Flex:** The service provider gains elastic scaling capabilities that solve individual VM limitation issues, allowing tit to scale its solution as its capacity requirements increase. This flexibility will supply much-needed elasticity in the company's infrastructure, allowing it to initiate an unlimited number of instances within each Grid whenever it needs to upgrade. And it will only pay based on its capacity needs through flexible capacity-based pricing.
- **Service provider licensing:** Another plus: The solution is covered under the Infoblox Service Provider License Agreement (SPLA) program. This model is specifically designed for unique service provider requirements, such as meeting demand that can be difficult to predict accurately. With SPLA, the provider can increase capacity at any time and eliminate the painful task of procuring and provisioning new hardware.

- **Subscription pricing:** Older perpetual licensing models no longer fit in a cloud-first world. Subscription pricing works with SPLA and Trinzic Flex, providing a more flexible model that eliminates maintenance renewal refresh cycles. The service provider can plan for exact costs year over year without preparing for a refresh CapEx hit every four to six years with no more technology refreshes.

The customer chose the second option to add a second Infoblox Grid.

## High performance and secure DNS caching

Secure DNS caching protects subscribers from growing malware threats, service disruption and slow response through global threat intelligence and automated protection packages. It maintains critical DNS service availability in rapidly evolving networks, in situations where call volumes and data loads spike and even during a malicious DDoS attack. Advanced caching functions ensure that the best and most-used responses are always available for subscribers.

- **Infoblox Secure DNS Cache Acceleration (DCA):** This feature offers the most robust and cost-effective DNS caching infrastructure solution, combining sub-millisecond response and advanced threat protection, maintaining low latency and a secure subscriber experience.
- **Authoritative and recursive DNS:** With Infoblox DNS, the provider can enable and centrally manage and automate all aspects of authoritative and recursive DNS to achieve the high availability, efficiency, security and application response times subscribers need to thrive in a digitally connected world.
- **Infoblox IPAM and DHCP:** IT staff can now discover and capture all network assets in one authoritative IPAM database to establish a single source of truth for complete visibility. By automating DHCP and IPAM, Infoblox enables the provider to better manage the proliferation of mixed hybrid and multi-cloud infrastructure and mobile devices. It also sets the stage to transition to IPv6 provisioning smoothly.
- **Secure and centralized DNS and IPAM for OpenRAN:** Being a member of several Middle Eastern telecom operators comprising the Gulf OpenRAN initiative, the provider wanted to build out its 5G network using open interfaces, software and hardware that will allow it to diversify its supply chain. Infoblox can interface with whatever OpenRAN platform management systems that mobile operators choose, supplying vital and centralized DNS and IPAM. The Infoblox RESTful WAPI helps ensure the IP space perspective's overall integrity by interfacing across the different RAN management platforms, providing automated discovery and management across multiple data centers, cloud management platforms and networks.
- **Infoblox encrypted DNS for service providers:** This function furnishes efficient encryption for DNS over TLS (DoT) and DNS over HTTPS (DoH) while delivering Infoblox best-in-class DNS services. Infoblox has proposed an optional testbed that the IT team can leverage to test these new encrypted DNS technologies with DCA.

## Advanced reporting and analytics

Infoblox Reporting integrates with Infoblox Grid technology, enhancing real-time management with an extensive and customizable historical reporting engine. Infoblox Reporting delivers robust reporting capabilities within a single platform and interface. With their added reporting capacity, the team can quickly and efficiently manipulate reporting data in many formats to locate the exact information they are looking for by dates, locations, subscribers and other definable parameters.

## Infrastructure security

As providers simultaneously expand 4G capacity and migrate to 5G infrastructure for mobile and fixed wireless broadband coverage—especially in underserved and rural areas—network complexity and scalability demand new approaches. Widespread deployment of devices outside the data center also exposes many access points and creates a massive threat surface that attackers may be able to see. Constantly evolving threats and attack surfaces demand foundational security that is ubiquitous, scalable and automated.

Leveraging threat intelligence and AI/ML-based analytics on DNS supplies scalable protection against modern malware, command and control (C&C), data exfiltration, domain generation algorithms and more. In addition, traditional DNS open-source software and Internet-facing firewall appliances were not designed to address DNS-based attacks that could slow or crash a DNS server. Stopping these DNS attacks requires deep inspection with high compute performance to maintain network uptime during an attack.

- **BloxOne Threat Defense:** This product strengthens and optimizes a solution provider's security posture from the foundation, maximizing brand protection by securing existing networks and subscriber imperatives like 5G, IoT, the network edge and the cloud. It works with a service provider's existing defenses to stop malware from spreading inside a network–automatically detecting malware at the DNS layer, preventing devices from connecting with malicious destinations, isolating compromised devices and then triggering their remediation.
- **Advanced DNS protection (ADP) for service providers:** The Infoblox solution maintains service availability during malicious attacks. System administrators can use ADP to thwart attacks directed toward their DNS services that could otherwise cripple or compromise network communications. Unlike approaches that rely on infrastructure overprovisioning or simple response-rate limiting, ADP intelligently detects and mitigates DNS attacks while responding only to legitimate queries by using constantly updated threat intelligence, without the need to deploy security patches. These capabilities will help the provider ensure service availability during malicious or accidental attacks while supporting 5G service availability and critical DNS functions and performance.
- **Infoblox DNS Firewall:** The leading DNS-based network security solution, Infoblox DNS Firewall contains and controls malware that uses DNS to communicate with C&Cs and botnets. DNS Firewall employs DNS response policy zones (RPZs), actionable threat intelligence and the optional Infoblox Threat Insight to prevent data exfiltration. By collaborating with Infoblox DHCP for device fingerprinting, Infoblox IPAM and Infoblox Identity Mapping for capturing the username tied to an infected device, DNS Firewall provides actionable information to help pinpoint infected devices for remediation.
- **Infoblox Threat Intelligence:** Rapid detection reduces subscriber complaints, furnishing timely, coordinated threat intelligence from multiple sources. Access to up-to-the-minute threat data dramatically simplifies what it takes for service providers to shut down attacks early before they can spread and cause harm. Infoblox Threat Intelligence integrates with security solutions such as BloxOne Threat Defense and updates the service provider's cybersecurity ecosystem in real time on new and evolving malicious Internet destinations.
- **Infoblox ecosystem exchange:** This solution enables protection to keep pace against new threats, providing security professionals a highly interconnected set of integrations that enable them to eliminate silos and optimize their security orchestration, automation and response (SOAR) solutions. Ecosystem Exchange also improves the ROI of the provider's entire cybersecurity ecosystem, including third-party, multi-vendor assets.

## THE RESULT

### A strong foundation for the 5G future

The service provider reinforced its high confidence in the Infoblox solution through numerous consultations, road-map sessions and product testing with various Infoblox experts. In multiple phases, the provider will add a second Infoblox Grid, upgrade its Authoritative DNS and DHCP followed by DNS Cache Acceleration and add other features, including BloxOne Threat Defense. Best of all, the provider gained the flexibility to add virtualized functionality to its existing network wherever and whenever needed. Whether it requires Advanced DNS Protection to maintain service availability and critical DNS functionality during a volumetric DDoS attack or a quick increase in DNS Cache Acceleration capacity to accommodate additional network traffic temporarily, the service provider can leverage the platform's flexibility to support its future vision for 5G and beyond.



**Corporate Headquarters**
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com