SOLUTION NOTE

INFOBLOX SOLUTIONS FOR MULTI-ACCESS EDGE COMPUTING

Solving scalability and security challenges for 5G and edge computing

SUMMARY

As the demand for new and innovative digital services increases, the momentum for communications service provider (CSP) digital transformation is escalating rapidly.

While 5G and edge computing promise to bring considerable benefits to enterprises and consumers, these same trends pressure CSPs as they strive to modernize their businesses and their network architectures. Today's networks are more decentralized, clouddriven and dependent on the network edge. In response, CSPs will need new platforms and architectures that can keep pace with the rising demand for edge-centric networking and security.

DNS, DHCP and IPAM (DDI) continue to play a critical role in CSP networks for scalable, secure resource allocation and agile control of virtualized services as they expand their 5G and edge portfolios. Infoblox DDI solutions help solve edge computing challenges with capabilities that address critical aspects of scale, performance, and security that CSPs need to keep pace with the rising demand for edge-centric networking.

This solution note will help you understand the importance of DDI in 5G and edge computing and how Infoblox solves common challenges with capabilities that address critical aspects of scale, performance and security.

OVERVIEW

Multi-access Edge Computing (MEC) is an edge-computing standard that moves cloud architecture capabilities such as compute, storage and networking resources closer to end-users and subscribers at the network edge. With MEC, CSPs can provide near real-time cloudcomputing capabilities to power next-generation services requiring high-bandwidth and low-latency access. It's important to note that MEC is not infrastructure; instead, it is a function or paradigm. While sharing similarities with 5G, edge computing will represent a set of capabilities that is a piece of service provider edge networks. It deploys cloud computing capabilities at the mobile network's edge by integrating application platforms and MEC applications with virtualized network infrastructure.

HIDDEN IMPORTANCE OF DDI IN 5G AND EDGE COMPUTING

Operator networks leverage various advanced technologies, including Network Functions Virtualization (NFV), containers, virtualized RAN (vRAN) and software-defined networking (SDN). Still, the lack of required infrastructure, deployment and management capabilities is a major factor restraining the buildout of MEC. While CSPs actively adopt this technology to fulfill subscribers' bandwidth demand, they require better deployment capabilities that include automation and security.

To deliver, realize, and maximize investments in 5G and edge deployments, operators must quickly and dramatically evolve their existing legacy DNS, DHCP and IP Address Management (DDI) management processes. Virtualized and containerized MEC solutions will have pre-deployment and lifecycle requirements, which necessitate the use of DNS and IP Address Management (IPAM) procedures. But often, operators are leveraging traditional IPAM and DNS management processes using spreadsheets and databases to enable deployment of cloud functions or track device inventory limits. These legacy approaches often delay business-critical 5G and MEC deployments, and place vital product initiatives at risk.

- **Visibility and discovery.**
  Without a consistent DNS andIPAM solution across the telco cloud, operators often mustrely on multiple tools to access DNS and IP address data–increasing inconsistencies in the network-wide management of the DNS and IP address space. This also leads to longertroubleshooting times, reduces the ability to performnetwork planning, and increases security risks.
- **Automation.**
  While service delivery today is delivered bya static infrastructure—for example, a packet data networkgateway (PGW) will rarely change once installed and inoperation—the 5G world will be much more dynamic, andprovisioning must adapt. Tens of thousands of containersand virtual network functions (VNFs) will be instantiatedand terminated on demand. Containers and VNFs will rely on DNS more than ever. But how can operators ensure thatinstances are automatically put into service and in sync withthe workload lifecycle?
- **Security.**
  Continually evolving threats and increased attacksurfaces demand a foundational approach to security thatis ubiquitous, scalable and automated. Rapidlya evolvingcyberthreats require CSPs to invest ever greater resourcesin threat intelligence to stay a step ahead of cybercriminals. Today, threat intelligence is hampered by information silos,lack of actionable context, and an inability to prioritize bythreat category. With more resources being deployed at thefar edge, operator IT and server admin teams must managesignificantly more pods, VMs—sometimes hundreds at atime, and potentially thousands of containers—in their virtualand cloud environments. With thousands of containersspread across multiple platforms and regions, carefulplanning and monitoring is essential. With many more virtualservers, containers, and services, the network becomeseven more massive—increasing the overall attack surface,making security even more critical.

Today, there are many clouds, technologies, service models and deployment approaches for operators to deploy microservices for 5G and MEC networks. Each operator will approach and solve this differently. Operators need platform tools and solutions that afford them the flexibility to employ zero-touch provisioning capabilities to deploy, track, send and secure these microservices with full lifecycle automation.

INFOBLOX SOLUTIONS FOR MEC

Infoblox supports service provider MEC platforms with cloud orchestration technologies that simplify and streamline provisioning and de-provisioning IP addresses to newly created VMs and containers, update DNS records, and release IP addresses when the VMs are taken down—all in a matter of seconds instead of hours or days.

SOLVES CHALLENGES WITH MEC APPLICATION GROWTH

As the shift toward microservices continues to take off, edge computing is expected to drive a tremendous increase in the number of dynamic applications deployed as microservices. With the ability to reside at the network edge, microservices will make it simple to push services and tools as close as possible to subscribers, increasing the ability to scale based on demand. These small microservice instances will be extremely dynamic as they will spin up or spin down in micro-seconds. Edge platforms must provide access to DNS. Also, the number of simultaneous network and service function instances that require IP Address Management (IPAM) is projected to increase by one or even two orders of magnitude.

Infoblox solutions help provide guaranteed performance at the edge, plus streamlined and automated DNS and IPAM for MEC applications.

- **Supports high-bandwidth, ultra-reliable low latency communications (URLLC).** Infoblox DNS Cache Acceleration provides low latency, high-performance DNS critical for URLLC applications and the increased scale of application and containerized DNS traffic.
- **Kubernetes integration supports service provider flexibility and adaptability requirements.** Infoblox provides highly available critical network services by extending the DNS, DHCP, and IP address management (IPAM) capabilitiesto virtualized and containerized MEC environments and provides a Kubernetes plugin that provides IPAM services for the Kubernetes pods. Kubernetes integration offers automated provisioning and de-provisioning of IP addresses and DNS records for containers as they are created and destroyed.
- **Integration with CoreDNS and ExternalDNS.** CoreDNS is a fast, flexible and modern DNS server that also provides service discovery in cloud-native deployments. While CoreDNS has become a popular DNS server for cloud-native implementations, it may be challenging to gain unified visibility of the microservices running on clusters—especially as scale increases. Infoblox's integration with CoreDNS provides unified visibility of the Kubernetes microservices running on the MEC clusters within NIOS. Since native Kubernetes commands are cumbersome to execute and their results challenging to view, Infoblox simplifies network management of containers, services and pods running within a cluster and provides a better tool that accommodates the management of dynamic clusters at scale.

Likewise, External DNS makes Kubernetes services discoverable via external DNS servers like Infoblox. Similar to our leadership with CoreDNS development efforts, Infoblox has assumed complete ownership of the integration code for ExternalDNS.

SUPPORTS EDGE COMPUTING GROWTH AND EXPANSION

MEC is expected to expand the numbers of edge computing sites dramatically. This expansion creates management challenges not found with a data center or conventional cloud computing. Spreading mission-critical applications and data to the edge introduces scale and performance challenges, which demand edge environments function efficiently and reliably no matter how many instances are introduced.

Infoblox's centralized IPAM capabilities help streamline management and improve visibility as edge sites grow in large numbers.

- **Enables CSPs to unify DDI across existing centralized mobile edge compute locations.** While storage and compute workload processes are considered commodities in centralized data center management structures, MEC demands IT to reconsider its views to effectively push storage and workload into virtual environments at the edge. Infoblox delivers unified DDI across centralized and mobile edge environments. This enables a uniform policy of DNS naming and IP address provisioning across clouds. The IPAM system understands the network's actual state and knows what IP addresses are used and aren't. When virtual resources are decommissioned, IP addresses and DNS records are automatically reclaimed.
- **Provides centralized management and visibility.** Infoblox delivers unified IPAM management of physical, virtual and cloud environments, providing centralized management across multiple data centers, multiple cloud management platforms and different networks. This approach helps support teams identify problems quickly and reduces time to repair, providing greater visibility of VMs and networks.
- **Enables faster MEC site provisioning.** Infoblox helps dramatically shorten the time needed to spin up new MEC sites and workload instances, decreasing the estimated time to provision sites, improving agility and accelerating time to service. Administrative overhead is reduced by eliminating handoffs between cloud and network teams in the provisioning process.

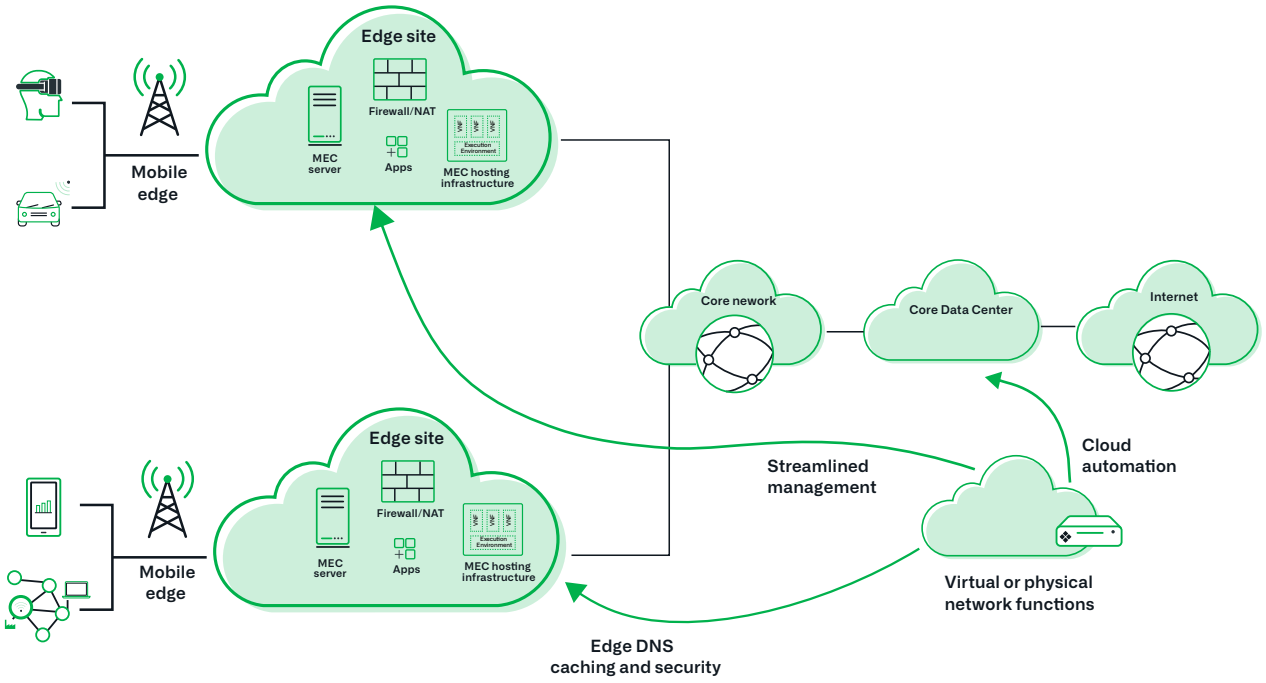

Figure 1: Infoblox multi-access Edge solutions

PROVIDES SECURITY FOR MEC AND SPECIALIZED NETWORKS

With tens of thousands of containers spread across multiple platforms and regions, careful planning and monitoring are required. Considering that many more virtual servers, containers and services are involved in MEC architectures, the network becomes even more massive, increasing the overall attack surface, making security even more critical. As service provider compute shifts from centralized to edge locations, Infoblox provides greater security by ensuring that subscriber data never leaves the provider network slice.

Infoblox provides security for 5G and edge-based telco cloud environments.

- **Secures the DNS services running on the edge instances.**
  Advanced DNS Protection provides DNS DDoS mitigation to protect the critical DNS infrastructure that is the "heartbeat" of operator networks. It automatically detects and stops the most extensive external/internal DNS-based attacks while maintaining DNS integrity and service availability.
- **Protects the edge services, consumers and applications from malware and advanced persistent threats.**
  BloxOne® Threat Defense maximizes brand protection by securing existing networks and subscriber imperatives like 5G, IoT, network edge, and the cloud enabling operators to transform DNS into their most valuable security asset. It empowers organizations to centrally and automatically secure every connection, regardless of device or location, across physical, virtual, containerized, and cloud infrastructure. By combining an up-to-date network inventory with Infoblox Threat Intelligence, operators gain current, conglomerated threat intelligence from multiple sources to identify threatening and threatened workloads—greatly simplifying at scale what it takes operators to shut down attacks early on before they spread and cause harm.
  - High-Quality Threat Intelligence mitigates the broadest range of DNS-based attacks, including Volumetric, Reflection, DDoS, NXDOMAIN, Amplification, TCP/UDP/ICMP floods, Data Exfiltration (through known Tunnels), Hijacking, Reconnaissance, Cache poisoning and Protocol anomalies.
  - Threat Insight enables security teams to get a jump on zero-day threats. Through analytics based on machine learning, inspects DNS traffic to detect patterns associated with data exfiltration and block DNS requests to those destinations.

- DNS Firewall proactively and automatically protects networks against fast-evolving, elusive malware threats that exploit DNS to communicate with C&C servers and botnets. The solution blocks connections to malicious destinations. Also, it enables security teams to rapidly pinpoint compromised devices, isolate them to prevent the spread of infection and trigger remediationc activities.

- **Supports encrypted DNS protocols.**
  Infoblox Encrypted DNS delivers a unique approach to encrypting DNS traffic using DNS over TLS (transport layer security) or DoT and DNS over HTTPS or DoH to host encrypted DNS resolvers locally. Unlike methods that rely on load balancers or overprovisioning, Infoblox Encrypted DNS runs as a single service for all of your DNS needs. Our standard features, including Advanced DNS protection and DNS Cache Acceleration, are all available from the same highly scalable DNS service.

CONCLUSION

As the number of edge data centers grows and spans a wider geographic region, CSP networks are becoming more decentralized, cloud-driven, and dependent on the network edge. Infoblox helps solve edge computing challenges with capabilities that address critical aspects of scale, performance and security. These are exactly the competencies CSPs need in order to keep pace with the rising demand for edge-centric networking.

To learn more, visit www.infoblox.com/sp or contact your local Infoblox representative today.

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

+1.408.986.4000
www.infoblox.com

Version: 20230919v1