SOLUTION NOTE

DELIVER BETTER OFFICE 365 EXPERIENCES WITH CLOUD-BASED DDI AND SECURITY

THE OFFICE 365 DILEMMA

The promise of Office 365 was exactly what you needed—a distributed cloud-based SaaS application that delivered improved collaboration and productivity.

So, you made the investment and deployed. But now you have a dilemma. Corporate Office 365 users are happy, but branch and remote users are complaining about access, reliability and performance.

When organizations plan their deployment of Office 365, how their branch and remote users connect to it and other SaaS-based applications is often overlooked. That's because enterprise networks were originally designed to centralize data and applications at the headquarters' datacenter, not provide direct Internet access from the branch. For branch and remote users, traditional network configurations can adversely impact Office 365 and SaaS access and performance. But before we explore that issue, let's take a brief look at the role that core network services play in providing access to cloud-based applications.

CORE NETWORK SERVICES

All network and cloud interactions depend on core network services, which include DNS, DHCP and IPAM (DDI). All play a foundational role in IP-based communications. For example, the Domain Name System (DNS) is the starting point for every network conversation. It's like the phone book of the Internet because it translates common, memorable alphabetic domain names into numeric Internet Protocol (IP) addresses used by web browsers to find unique devices, interact and exchange resources. Next, there's Dynamic Host Configuration Protocol (DHCP), the foundation of network identity and access. It provides quick, automatic, central management and distribution of IP addresses to connect devices to networks. Finally, IP Address Management (IPAM) refers to the planning, tracking and management of DNS and DHCP services that assign and resolve IP addresses for machines on the network. With accurate network endpoint discovery, IPAM becomes the authoritative source for all network-connected assets. For branch and remote users, these network services are essential for fast, reliable and resilient access to Office 365 and SaaS applications.

TRADITIONAL NETWORK CHALLENGE

When it comes performance issues with cloud-based applications in branch offices and remote sites, most of the problems arise because traditional DDI solutions do not provide direct-to-cloud access to these applications. A brief look at two prevailing configurations of conventional DDI shows why branch users are unhappy.

DNS Backhaul

The traditional DNS backhaul model involves having branch and remote traffic directed back through headquarters data centers before reaching the Internet (Fig. 1). As a result, workflows and routing to Office 365 and other cloud-based applications become inefficient and uncertain. Traffic from branch users must often travel longer network distances before reaching files and data, significantly impacting access, reliability and performance. Worse, there's no branch resiliency or local survivability as branch users are at the mercy of the headquarters datacenter being up and functional.

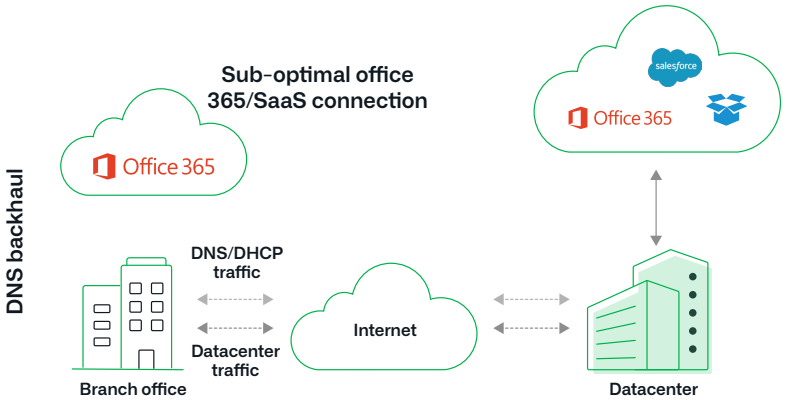

Figure 1: Routing of cloud-based DNS traffic to headquarters' datacenter introduces performance issues and latency.

Sub-optimal SaaS access & performance through datacenter

- Inefficient traffic flow
- Uncertain routing to SaaS application
- No local survivability

Server- and Router-Based DNS/DHCP

Utilizing servers and routers to manage DNS/DHCP is another network model that often results in adverse Office 365 user experiences. This approach involves labor-intensive, individual branch server- and router-management that can generate site-to-site inconsistencies. Server-based DNS/DHCP can experience performance degradation and process interruptions, while routers are often subject to limited administrative visibility.

DNS/DHCP management challenges through the datacenter

- Labor intensive, individually managed resources
- Limited administrative visibility
- Potential site-to-site inconsistencies

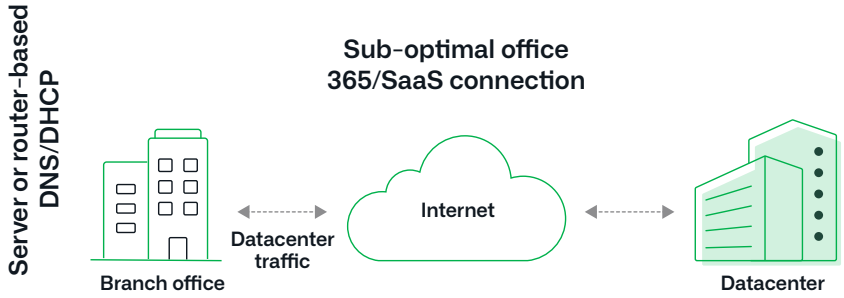

Figure 2: Server- or router-based DNS/DHCP can cause administrative conflicts and inefficiencies.

NETWORK TRANSFORMATION FOR OFFICE 365 AND SAAS

With the emergence of Office 365 and SaaS, technology forged ahead, pushing the network edge out to the branch and leaving traditional models in their wake. Because Office 365 is a globally distributed service, connectivity comes through Microsoft Global Network front doors scaled-out across hundreds of locations worldwide. From an architectural view, optimum user experience is achieved by deploying local DNS to access Office 365's local Internet breakouts. This enables branch and remote users to connect to the closest Office 365 cloud location for the best overall experience (Fig. 3). But it also means that DNS queries must be resolved locally, something that the DNS backhaul model cannot deliver.

So, you might ask, "What about local server- and router-based DNS/DHCP management models? By definition, don't they provide local service?" Yes, but it comes at considerable cost. Individual branch-located servers and routers can be expensive to deploy, maintain and refresh. They are also cumbersome, error-prone and inefficient to operate, especially for extensive, geo-diverse networks. Plus, servers can experience performance and service interruptions, impacting user experience. With constrained budgets, resources and cost reduction initiatives, the server- and router model may no longer be sustainable for many organizations, especially when lower-cost, more costpredictable and higher performing options are available.

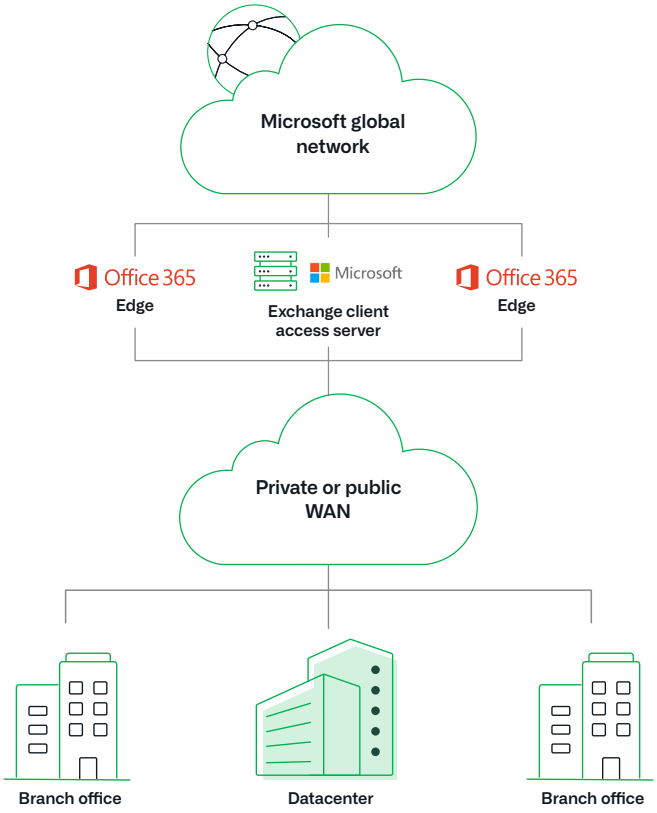

Figure 3: Deploy local DNS for local Internet breakout and optimum access

Ultimately, if your network is deployed using traditional DDI models and you've already adopted Office 365 or will soon, it's initial value and benefits could be at risk or already be costing you. So how do you resolve this dilemma? Move your core network services to the cloud.

DEPLOY LOCAL DNS AND LOCAL INTERNET BREAKOUT FOR OPTIMUM ACCESS

- Office 365 traffic routes to the closest Microsoft network edge location
- Exchange traffic routes to the closest Exchange Client Access Server
- Branch and remote users get best overall experience through local access

CLOUD DDI—OPTIMIZED OFFICE 365 ACCESS

BloxOne® DDI from Infoblox is the industry's first cloudmanaged DDI solution optimized for branch office networks. Unlike traditional network architectures, BloxOne DDI provides significant advantages over backhaul, server- and router-based delivery. By always connecting users to the nearest Office 365 entry point, BloxOne DDI optimizes user access to Office 365, SaaS and data center applications, improving reliability, performance and overall experience.

BloxOne is the transformative, best-in-class platform that delivers both locally recursive DNS and locally hosted, high-availability DHCP with deep IPAM integration. BloxOne DDI is scalable to support thousands of sites and can increase capacity simply by adding site licenses. It offers the flexibility to deploy on an on-premises commodity hardware appliance, VM or in a container, significantly lowering hardware costs. It also lowers operating expense though a subscription-based, cloud-consumption model. The lightweight on-premises branch appliance provides resiliency and local survivability and guarantees geo-local access to cloud-based Office 365. It further improves workflows by centralizing visibility and automating core network services, allowing network administrators to manage more users and environment workloads in less time. Wherever users are, they can access and remain connected to Office 365 and SaaS applications regardless of network service interruptions at the corporate headquarters. This means superior reliability for thousands of remote offices, optimizing Office 365 access and improving user experience for performance and productivity (Fig. 4).

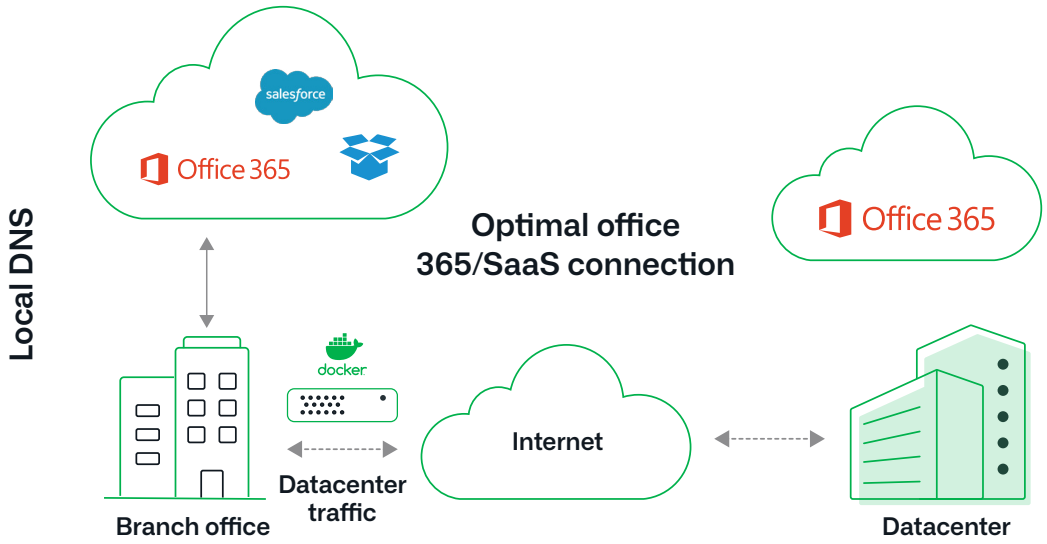

Figure 4: Local DNS queries resolve locally for closest Internet breakout.

LOCAL DNS QUERIES RESOLVED LOCALLY FOR CLOSEST INTERNET BREAKOUT

- Routing for nearest SaaS access and assured DNS/DHCP performance
- Local survivability and uniform policies and processes
- Central management and automated provisioning
- Deep visibility into network activity and history

Infoblox provides security protection at the DNS layer. This is a critical capability for Office 365 users in branch locations because they connect directly to the Internet to access the application, but without the full security controls available through the corporate network. BloxOne™ Threat Defense is the industry's first and only on-premises and cloud security solution that leverages DNS as the first line of defense. Tightly integrated with BloxOne DDI, BloxOne Threat Defense can protect branch locations and their direct Internet breakouts, providing secure Office 365 access. Emails with macros, unknown attachments, phishing links and links to lookalike domains are risky and could lead to malware downloads. BloxOne Threat Defense uses highly accurate threat intelligence and analytics based on artificial intelligence and machine learningto detect and block inadvertent connections from Office 365 users to domains hosting malware and command and control (C&C) servers, and to lookalike and destination domains designed to exfiltrate data.

LEARN MORE

If you're looking to improve branch user access, security, reliability and performance for Office 365, ask us more about BloxOne DDI—the first cloud-managed DDI solution for branch office networks and BloxOne Threat Defense—foundational security for branch offices. Because the network that works best is the network you never notice.

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

© 2023 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc.
All other marks are the property of their respective owner(s).

Version: 20230918v1