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.

**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

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 cost-predictable and higher performing options are available.

Ultimately, if your network is deployed using traditional DDI models and you’ve already adopted Office 365 or will soon, its 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
Infoblox enables next-level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world’s most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

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

© 2020 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).