

[HOME](#) | [CURRENT ISSUE](#)

Hot Pick

http://informationsecurity.techtarget.com/magItem/0,291266,sid42_gci1191319,00.html

Issue: [Jun 2006](#)

DNS/DHCP

Adonis 1000

[BlueCat Networks](#)

Price: Starts at \$9,995

BlueCat Networks' Adonis 1000 appliance bundles DNS and DHCP into an enterprise-class appliance for the centralized secure operation of network addressing. Featuring rock-solid security and terrific management capabilities, this device quickly tames networks' ragtag patchwork of DNS and DHCP services, regardless of enterprise size.

Placing DNS and DHCP services on a single hardened appliance minimizes maintenance and centralizes administration. Instead of having to keep track of new threats associated with the OS, BIND and DHCP, it's all amalgamated into a single system.

A skilled attacker can easily exploit flaws in DNS software and the OS on which it runs through cache poisoning, DoS attacks and buffer overflows. Adonis is highly resistant to these kinds of attacks. It runs on a Debian Linux kernel (with an option for a solid-state flash drive) that is completely hardened, so any application that might pose a security risk, such as ping, telnet or ftp, is stripped off. Only two ports are left open by default: 53 for DNS, and 10042 for the SSL communication between the appliance and the client. An attacker querying Adonis gets no information about the system at all.




BIND, patch, kernel, client and security vulnerability updates all take place through the client, so the appliance is never at risk by communicating with an external server. Native BIND 9.3.1 runs under the hood for DNS, and DHCP is based on ISC 3.0.2.

Flooding a DNS server with spoofed SYN packets can fill up all available TCP ports, thereby preventing communication to the server via TCP. Because Adonis can handle queries well above normal levels, it can mitigate or thwart DoS attacks. It's capable of supporting 23,000 queries per second--most large organizations' servers top out at a couple hundred per second.

Setup and management are a pleasure through the richly featured Adonis Management Console, a cross-platform Java client that runs on Windows, UNIX, Linux, Solaris and Mac. An intuitive wizard walked us through setting up the appliance for both DNS and DHCP, determining first what type of architecture will ultimately be configured, then issuing a domain name and internal address. A single click automatically generates host records, reverse pointers, glue records and ACLs.

Automatic data population saves network administrators time and cuts down on errors. For example, when we added a Web server by choosing "New Host" and filled in a name and IP address, the server was instantly listed in the architecture tree, complete with the extensions, reverse zones and

Exec Summary

-  Solid security
-  Richly featured console
-  High performance and scalability

reverse pointers. The Adonis 1000 has comprehensive data checkers that analyze the configuration for logical and syntax errors.

Recognizing that most network administrators have existing DNS/DHCP installations, Adonis offers the ability to import old BIND, DHCP configuration and Windows 2000 DHCP dump files.

A master/master configuration using a virtual IP address provides high availability--a real problem with distributed DHCP servers--mirroring configuration data from one appliance to another.

The Adonis 1000 makes good business sense, increasing security and reducing the management overhead of multiple DNS/DHCP servers in large, complex organizations.

--SANDRA KAY MILLER

Information Security magazine is a part of the [TechTarget](#) portfolio of enterprise IT-focused media. Copyright 2001-2004, TechTarget. All Rights Reserved.