

SOLUTION NOTE

Security Implementation

Infoblox core network services appliances provide critical infrastructure for over 4,000 enterprises world-wide. Recognizing the key role played by our products, Infoblox devotes significant attention to security across all phases of product design and deployment, addressing security at the physical layer, in the operating system, in applications, in distributed appliance deployments, and in ongoing support operations, as described below.

Physical Security

Infoblox appliances are dedicated, task-specific devices. Infoblox hardware is designed to meet the strict security requirements of the global government and military organizations. There are no unnecessary physical ports and connections, such as keyboard, mouse, monitor, CD ROM and floppy disk—as are found on general purpose server or “pseudo-appliance” platforms. The LCD panel can be disabled or placed into display only mode. Any network port that has not been configured is disabled.

NIOS Operating System

The NIOS operating system is a hardened version of Fedora distribution. The OS has been optimized by Infoblox to address today’s most stringent security and performance requirements. Such optimization allows Infoblox to achieve superior DNS and DHCP performance over other open source and commercial solutions in the market. Another benefit of adopting Fedora distribution is its openness. This distribution is widely deployed and the source code undergoes an extensive review by multiple solution providers, resulting in a high degree of confidence that the code is free of embedded exploits.

The Infoblox software architecture is similar in key security aspects to that used by the industry’s leading firewall and security appliances. Key elements include:

- TCP/IP stack randomization
- Socket binding restriction in the kernel
- Hardened IP stack
- Program executable pages are read and execute only
- All kernel data structures and memory are not accessible from user (administration) mode
- Shared library text and data is mapped private, which means copy-on-write is enforced
- Denial of Service and malformed packet detection/prevention
- All drivers and executable code is digitally signed by Infoblox and is verified cryptographically by the appliance platforms before it is able to install and run

SOLUTION NOTE

In addition to tuning the Linux kernel for performance and stability, any OS components that are not required for the Infoblox application are removed. Utilities and tools commonly found on Linux distributions are also removed from the Infoblox NIOS operating system. Ptrace, debuggers, compilers and other developer-oriented tools and administrative functions common to mainstream Linux implementations are removed. This means that many security vulnerabilities are simply not present in the Infoblox code and therefore Infoblox appliances are not vulnerable to many exploits. For example, while there have been approximately 8 CERT security advisories related since January 1st, 2006, Infoblox has only been vulnerable to 2 of these. In both cases, Infoblox issued patched software in less than 24 hours. Thanks to the one-button software update capability of Infoblox appliances, Infoblox customers were able to patch their systems with a single, simple operation.

Core Services

Infoblox appliances only enable core network services per the package ordered and installed on each appliance. All non-essential services, such as Telnet, SMTP, etc. have been completely removed from the NIOS base operating system. Any standard Infoblox supported service (DNS, DHCP, TFTP, NTP, etc.) that is not configured is disabled.

Management Security

There are several security features that enhance the management and security of the NIOS appliance:

- No root/shell access is allowed. This greatly reduces the risk of software exploits and also prevents administrators from making configuration changes that are not logged or preserved on upgrades.
- If enabled, all management traffic must traverse through the management port enabling out-of-band management on dedicated VLANs or subnets for added security. SSH access is allowed, but must be specifically enabled. SSH access can be permanently disabled and completely removed from the system.
- Administrators can authenticate via an internal database or through a RADIUS or AD server. Authorization rights are applied on a granular zone or network basis in addition to granular access control to DNS resource record types (a, PTR, MX, NS, etc.).
- Routing between interfaces has been disabled, BIND process runs as the 'nobody' user.

Grid Security

All grid communications are encrypted using 128 bit AES and authenticated using shared secret exchange. Both third-party and server-generated certificates are supported. Appliances that are configured into a grid cannot be exploited via local administrative actions—all configuration changes must be performed at the grid master and replicated to the members, which ensures security and also guarantees a full audit trail.

SOLUTION NOTE
Patches, Security Updates and Vulnerability Assessment

Infoblox employs a 16 member Security Alert Response Team (with representation from Engineering, Technical Support and Product Management) which continuously monitors various sources for potential vulnerabilities. The Security Response Team is included on private security alerts distributed from key contributors to BIND, ISC DHCP, NTP and other core protocols. Every reported vulnerability alert is reviewed the Infoblox Security Alert Response Team with members on-call 24x7x365. All discovered vulnerabilities are patched or fixed prior to release. All security patches and fixes are generally made available in monthly patch releases. Serious vulnerabilities, such as the recent DNS cache poisoning vulnerability, are patched immediately, customers are alerted and patches to multiple releases are made available on the Infoblox Support Portal. We also update the CERT Vulnerability Knowledgebase website with remediation information. Every product release is scanned with two commercial vulnerability assessment scanners before posting to the web or manufacturing.

Summary

By employing rigorous design practices for hardware and software, selecting the most secure elements, proactively eliminating vulnerabilities, locking down systems, vigilantly monitoring security alerts and responding quickly and proactively, Infoblox ensures that its customers' core network services infrastructure is presents the minimum possible attack surface and is robust against a wide ranges of exploits.

For more information contact your Infoblox representative.

Infoblox Product Warranty and Services

The standard hardware warranty is for a period of one year. The system software has a 90-day warranty that will meet published specifications. Optional service products are also available that extend the hardware and software warranty. These products are recommended to ensure the appliance is kept updated with the latest software enhancements and to ensure the security and availability of the system. Professional services and training courses are also available from Infoblox. Information in this document is subject to change without notice. Infoblox Inc. assumes no responsibility for errors that appear in this document.