Infoblox

SOLUTION NOTE

NIOS Security Implementation

SUMMARY

Infoblox delivers foundational protection to embed security everywhere, automate responses and reduce SecOps workloads. Automatically detect and stop the widest range of DNS attacks—attacks that many other security providers often miss—to protect your network, minimize disruptions and maximize uptime. Gain visibility, enrich your data with contextual ecosystem insights, improve threat analyst productivity, speed remediation and lower costs. With Infoblox, you can leverage industry best security practices for hardware and software design, eliminate vulnerabilities, secure systems, monitor alerts, enhance threat intelligence and accelerate response for greater core network security visibility, control and automation.

With over two decades of expertise in delivering global, reliable, enterprise-grade DNS, DHCP and IPAM (DDI), Infoblox is the industry leader in core network and security services for the data center, hybrid multi-cloud and the network edge. Over 12,000 customers in every major industry and vertical, including 70 percent of the Fortune 500, trust Infoblox to power their core network, cybersecurity and cloud network automation services because company revenue, operations, employees, partners and—most of all, customers—depend on all of these things running reliably.

Infoblox delivers modern, cloud-first networking and security services from on-premises to cloud-native solutions so you can reliably automate and secure access to apps and services anytime, anywhere. For the data center and cloud, Infoblox provides Advanced DNS Protection to guard enterprise DNS infrastructure using best-in-class DoS signature and blocking capabilities, enabling maximum uptime and performance. Infoblox also offers extensive, market-leading cybersecurity ecosystem integrations with leading security vendors to automate SecOps response and efficiency.

For organizations with SaaS initiatives, BloxOne® Threat Defense quickly deploys hybrid DNS-layer security everywhere to protect the data and infrastructure of the distributed enterprise. Infoblox also supplies advanced threat intelligence for better DNS and contextual and multi-sourced threat intelligence to empower your entire security stack. By establishing foundational security throughout the network, Infoblox simplifies security administration, delivers unparalleled visibility and boosts the productivity of your security staff and resources.

Infoblox embeds security everywhere to automate responses and reduce the burdens on SecOps teams. Beginning with core DNS, DHCP and IPAM and extending throughout the operating system, physical and virtual layers, applications, distributed appliance deployments, security integrations, threat intelligence and ongoing support operations, Infoblox delivers foundational protection for anytime, anywhere defense.

Core Services

Infoblox enables core network services based on the package ordered and installed on each appliance. The Infoblox Network Identity Operating System (NIOS) completely removes all non-essential services from the base operating system and disables any standard Infoblox supported service (e.g., DNS, DHCP, TFTP and NTP) that is not configured by the customer.

Network Identity Operating System (NIOS)

The NIOS operating system is a hardened Linux distribution. Infoblox optimizes the OS 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.

The Infoblox software architecture uses industry best practices found in leading firewall and security solutions. Key elements include:

- TCP/IP stack randomization
- Socket binding restriction in the kernel
- Hardened IP stack
- Denial of service and malformed packet detection/prevention

In addition, program executable pages are read and execute only, and all kernel data structures and memory are not accessible from user (administration) mode. Shared library text and data are mapped as private, enforcing copy-on-write processes. All drivers and executable code are digitally signed by Infoblox and verified cryptographically by appliance platforms before they is able to install and run. The NIOS code base uses encryption to achieve obfuscation of code delivered as part of the product.

The Linux kernel is tuned for performance and stability. As noted above, NIOS removes any OS components not required for application functionality, including common Linux utilities, ptrace, debuggers, compilers and other developer-oriented tools and administrative functions common to mainstream Linux implementations. This configuration approach means that many security vulnerabilities are simply not present in the Infoblox code, keeping Infoblox appliances isolated and safe from threats and exploits. Further, Infoblox appliances provide single-click software updates, enabling customers to patch their systems if needed with a simple operation.

Physical Appliance Security

While hybrid and virtualization technologies are driving network transformation, many organizations continue to require physical appliances in the data center. The Infoblox platform enables you to see, secure, analyze and manage your network whether on-premises or in the hybrid, multi-cloud environment. This level of deployment flexibility begins with the latest generation of reliable, purpose-built appliances, which are security hardened with NIOS software designed to meet strict government security standards, including FIPS 140-2 (SL1 [software] and SL2 [hardware]) and Common Criteria EAL2+. NIOS is also listed in the Department of Defense Information Networks Approved Products List (DoDIN APL) and meets the DISA Security Technical Implementation Guide (DISA STIG) standards for configuring software to strengthen organizational security posture. Further, Infoblox continues ongoing testing and certification to meet these security standards and deliver the stringent network security solutions that today's market leaders require.

Management Security

Several security features harden security and enhance the management of NIOS appliances:

- **Access —** 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.
- **Management —** 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 can be allowed, but it must be specifically enabled. SSH access can be permanently disabled and completely removed from the system.
- **Authentication —** Administrators can authenticate users via an internal database or through a variety of remote AAA services. Authorization rights are applied on a granular zone or network basis in addition to granular access control to DNS resource record types.
- **Routing —** Routing between interfaces has been disabled and the BIND process runs as the "nobody" user.

Grid Security

The Grid communications used by Infoblox appliances are kept secure through VPN tunnels established between the Grid Manager and Grid Members. The VPN tunnels used for Grid communications are built using the OpenVPN protocol. The key exchange is done using TLS (using DHE-RSA-AES256-SHA) with device specific certificates (signed by an internal Infoblox Certificate Authority). The tunnel encryption in the VPN uses 128 bit AES encryption in cipher block chaining (CBC) mode. Both third-party and server-generated certificates are supported. Appliances that are configured into a Grid cannot be changed or misconfigured via local administrative actions. All configuration changes must be performed through the Grid Manager and replicated to the members, ensuring security and guaranteeing a full audit trail.

Patches, Security Updates and Vulnerability Assessment

Infoblox employs a Security Alert Response Team (with representation from engineering, technical support and product management) to continuously monitor 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.

With members on-call 24x7, the Infoblox Security Alert Response Team reviews every reported vulnerability alert. Critical vulnerabilities (e.g., BIND vulnerabilities) are patched immediately and customers are alerted so they can access multiple release patches on the Infoblox Support Portal. Infoblox also updates the CERT Vulnerability KnowledgeBase website with remediation information. Every NIOS product release is scanned with multiple leading vulnerability assessment scanners before posting to the web or manufacturing. A minimum of one internal and one third-party penetration test are done annually on this product—specifically to addresses NIOS security, including the NIOS Grid, DNS, DHCP and IPAM.

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

+1.408.986.4000 | info@infoblox.com | www.infoblox.com