THALES

Infoblox - Thales Solution for High Assurance DNSSEC

Infoblox

BENEFITS

- Up to 90% savings in IP management and monitoring
- Up to 50% reduction in network-related helpdesk calls
- Certified protection for DNSSEC signing keys and operations within tamper-resistant hardware
- Automation of burdensome and risk-prone key management tasks including key recovery and backup

DNS Vulnerabilities

The Domain Name System (DNS) is responsible for translating Internet and Intranet-based service names (e.g., web site addresses, email addresses, VoIP services, file transfer services and a range of cloud services) to IP addresses. Based on the vulnerability of DNS to illicit alteration of queries that seek to point end users or services to rogue IP addresses and route them to illegitimate servers for the purpose of data theft, DNS security has gained increased attention. DNSSEC provides a mechanism to mitigate DNS man-in-the-middle and DNS cache poisoning attacks by signing DNS records so that they can be validated by a DNS server or clients with appropriate software.

Any application or service that uses DNS and the Internet can benefit from DNSSEC. While it is possible to deploy DNSSEC in purely software-based systems, this introduces tangible risk of compromise of DNS signing keys. The use of hardware security modules (HSMs) provides proven and auditable security advantages, enabling proper generation and storage for signing keys to assure the integrity of the DNSSEC validation process.

DNSSEC Adoption

DNSSEC is an emerging technology that is seeing increased implementation in the Internet community. As a core technology, DNSSEC is applicable to multiple markets and industry sectors, with early adopters that include government online services and portals, financial services (online banking services), Internet service providers (domain registries, registrars, hosting providers), online retail, and large security-conscious enterprises. DNSSEC is a global initiative and early deployments are occurring in countries including Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Switzerland, Sweden, the United Kingdom and the United States.

Continuing attacks against the DNS infrastructure are an ongoing impediment to overall business continuity and therefore are likely to drive DNSSEC adoption. The adoption of cloud-based services is expected to further drive DNSSEC-enablement as the need for trust in the Internet grows. Just as secure socket layer (SSL) has become the de facto standard for encrypting sensitive data to protect privacy over the Internet, DNSSEC is expected to eventually become the default mechanism to verify the integrity of routing instructions.

Infoblox-Thales Solution

Together, Infoblox, a leading developer of network infrastructure automation and control solutions, and Thales deliver best-in-class IP address management integrated with FIPS 140-2 Level 3 certified HSMs for strong DNSSEC security and simplified key management. Thales nShield HSMs integrate with Infoblox IP Address Management (IPAM) appliances to provide a certified, tamper-resistant cryptographic platform to perform DNSSEC signing and signature validation, as well as employ secure DNSSEC key generation and lifecycle protection and key management techniques. These high assurance services assure the integrity of DNSSEC validation processes and provide robust access controls and event logging.

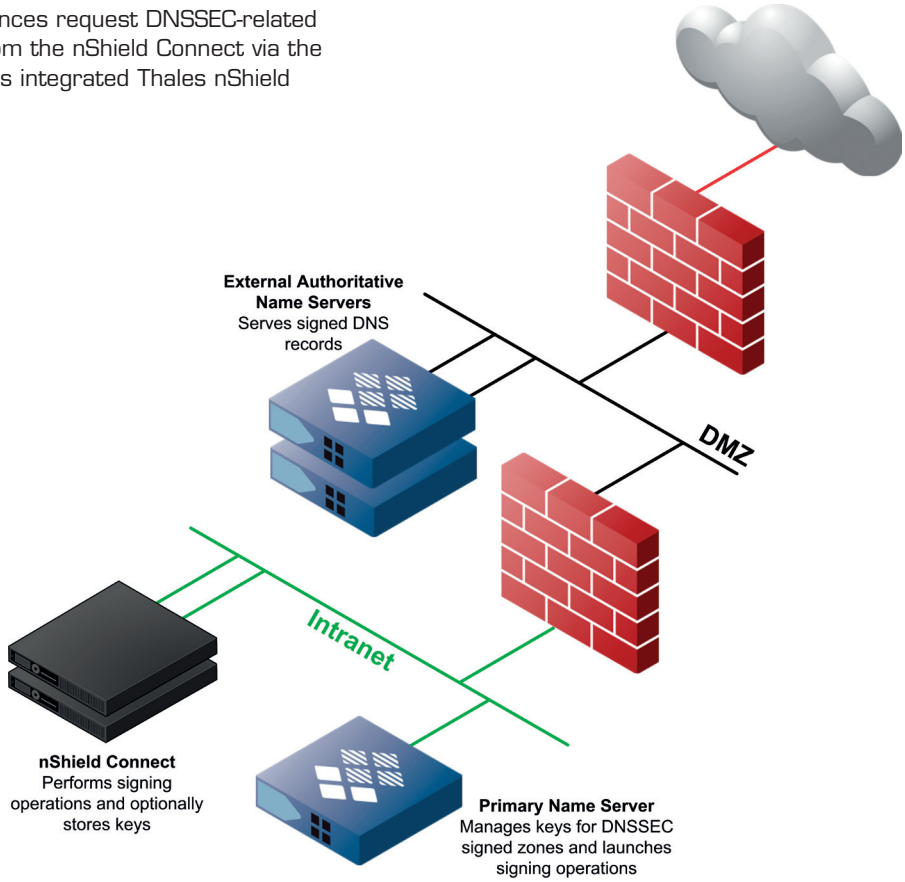
Infoblox IP Address Management appliances running NIOS 6.1 or later have integrated support for nShield Connect HSMs. Visit www.infoblox.com for a current and complete listing, including detailed descriptions and specifications, of all Infoblox IPAM appliance offerings.

A typical deployment of this solution will consist of:

- Two or more Infoblox appliances
- Two Thales nShield Connect 500 appliances

For high resilience, each Infoblox appliance can be configured as a client on each of the two nShield Connect appliances. Infoblox appliances request DNSSEC-related cryptographic services from the nShield Connect via the PKCS#11 API. Infoblox has integrated Thales nShield support software as well.

For users utilizing dynamic keys or signing a large number of zones, the nShield Connect 1500 or nShield Connect 6000 can provide increased performance. For more detail on the three nShield Connect performance options, visit www.thales-esecurity.com.



Infoblox®

Infoblox
4750 Patrick Henry Drive
Santa Clara, CA 95054

T: +1 408 625 4200
F: +1 408 625 4201