CYGNA LABS

Data Sheet

Sapphire DNSSEC Appliances

Redundant, fully automated DNSSEC zone signing

Secure your DNS namespace

DNS Security Extensions (DNSSEC) technology enables organizations to digitally sign DNS data so resolvers can be assured of the validity of the publisher of the data and of the DNS data itself.

Automation with control

DNSSEC is the only definitive solution identified for dangerous cache poisoning attacks. Unfortunately, DNSSEC configuration and operation requires strong technical expertise not only for initial configuration but for ongoing monitoring and maintenance of signed zone data. Among these tasks are creation of key signing and zone signing keys, signing zone information and rolling keys.

The Sapphire Sx20 and Sx10D hardware and virtual appliances from Cygna Labs are secure DNSSEC appliances that automate key generation, zone signing, and key rollover based on your policies. The Sx models provide “set and forget” policy operation to automate the setup and ongoing management tasks associated with signed zones.

DNSSEC helps DNS administrators assure the integrity of their published DNS namespace. The Sapphire Sx line of DNS appliances streamlines and automates complex DNSSEC implementation and lifecycle management.

Multi-master redundancy

The Sapphire Sx-series appliances can be deployed as standalone authoritative DNS appliances or in a multi-master pair. This intra- or inter-site redundancy enables seamless transitioning of signed zone integrity in the event of a failure of an Sx appliance or its corresponding site. Our unique dual corroboration technology facilitates reliable failover while minimizing flapping and flash key rollovers.

Seamless IPAM integration

DNSSEC policies can be defined using a dedicated secure Sapphire DNSSEC administrator account. The IPControl IPAM system enables comprehensive management of your IPv4 and IPv6 address space, your DNS domain space, which zones to sign and your DNS and DHCP server configurations.

IPControl software from Cygna Labs provides comprehensive DNS management for your signed and unsigned zones with support of all BIND option parameters, views, all resource record types and much more. Zones can be deployed to the Sapphire hardware or virtual Sx appliances for automated key and signature maintenance. IPControl also enables configuration of DNSSEC validation parameters for your stock BIND servers or Sapphire appliances serving as validating resolvers on behalf of your clients.

Features

The Sapphire Sx20 is a highly redundant, highly scalable DNSSEC hardware appliance while the Sx10D supports mid-tier deployments. Both models provide substantial cost savings by automating and simplifying your DNSSEC implementation. And both models are available in network function virtualization (NFV) format. These appliances can greatly reduce administration costs with support of the following critical automation features.

Simple, Resilient DNSSEC deployment

- Deploy DNSSEC signing appliances as hardware or as virtual appliances for AWS, Azure, OCI, GCP, VMware, KVM, Hyper-V and Xen.
- Deploy Sx pairs for primary/secondary multi-master resiliency to obviate flash re-signings upon appliance failure.
- Automate DNSSEC management with policies for:
  - Number of keys per zone.
  - Key algorithms and sizes per type.
  - Key generation and lifetimes.
  - Key rollover cycles per key type.
  - Signature expiration intervals.
- Automated zone signing, key generation and rollovers.
- NSEC and NSEC3 support.
- Automated DS record generation and publication for managed zones.
- Optional publication of CDS or CDNSKEY records for parent zone notification of a KSK rollover.
- Use existing BIND servers or deploy Sapphire appliances as secure zone secondaries.

Extensive security

- Support of PKCS#11 API for optional secure private key storage on an external hardware security module (HSM).
- Secure purpose-built hardened Sapphire OS.
- Configure additional security-oriented options such as BIND and port ACLs, rate limiting, views, update-policy and TSIG keys.

Flexible redundancy and manageability

- Multi-master authoritative server deployments.
- Direct and IPControl corroboration of master peer status for reliable failovers.
- Dual hot-swappable power supplies.
- RAID-5 hard disk redundancy.
- IPMI lights-out interface.
- Centrally manage and deploy both signed and unsigned DNS zones to Sx-series appliances with IPControl.
- Static and dynamic zones support.
- Centralized monitoring and control via EX or
- IPControl appliance dashboard.
- SNMP MIBs and traps facilitate performance reporting and management integration.
- OS, kernel, and services upgrades can be deployed from the centralized IPControl interface.

Unsurpassed lifecycle support

- Email notification of DS record update when the Key Signing Key is staged to rollover.
- Automated DS provisioning when parent and child are both managed on the appliance.
- No three-year support expiration unlike competitive appliance offerings.
- Attractive refresh and sparing pricing available.
- Optional managed services offer proactive monitoring, troubleshooting and repair.

About Cygna Labs

Cygna Labs is a software developer and one of the top three global DDI vendors. Many Fortune 100 customers rely on Cygna Labs' DDI products and services, in addition to its industry-leading security and compliance solutions to detect and proactively mitigate data security threats, affordably pass compliance audits, and increase the productivity of their IT departments.

Cygna Labs Corp

sales@cygnalabs.com
Toll Free: 844.442.9462
Intl: +1 (305) 501-2430
www.cygnalabs.com