CYGNA LABS

Data Sheet

Cygna Labs DNS Security Solutions

Secure the first link in IP communications

Secure your DNS infrastructure

DNS has proven extremely effective and scalable in practice and most people take DNS for granted given this and its proven reliability. However, its essential function and decentralized architecture serve to attract attackers seeking to exploit the architecture and rich data store for sinister activities.

Types of DNS Attacks

Attackers may target DNS servers in and of themselves in order to stifle communications or to steer unwitting end users to imposter web servers or other destinations. Alternatively, DNS may serve as a facilitator for use with the scope of a broader network attack, such as data exfiltration. Just as DNS enables users to connect to websites by resolving text-based destinations to IP addresses, it enables attacker malware to locate command and control centers or to tunnel information through firewalls. DNS by its nature also openly publishes potentially useful information about networks, host names and IP addresses for would-be attackers.

An attack that renders the DNS service unavailable or which manipulates the integrity of the data contained within DNS can effectively bring a network down.

Protect your Recursive DNS Servers

Cygna DDI software and appliances in conjunction with Cygna DDI Guard software secure DNS deployments. Recursive servers are responsible for resolving client DNS queries for internal and external Internet websites and destinations. These types of servers are subject to the following major attack forms. Cygna Labs natively supports mitigation for these within its solution set:

- Malware command and control (C2) access. Cygna DNS appliances support configuration of multiple response policy feeds to enable firewalling of DNS queries from reaching C2 domain servers.
- Domain Generation Algorithms (DGA) provide a means for malware miscreants to evade detection using algorithmic domain names. Cygna DDI Guard detects DGA queries via AI.
- DNS tunnelling enables attackers to stealthily exfiltrate sensitive data from your organization using the DNS protocol.
- Denial of service attacks. Anycast addressing, adaptive rate limiting, access controls and rate limiting provides thresholding of incoming packets to mitigate DOS/DDOS floods.
- Cache poisoning. Simple configuration of DNSSEC trust anchors and associated validation options enables you to secure DNSSEC-signed resolutions.
- Server attacks. Protect your DNS servers from hacks with secure, purpose-built Cygna DDI appliances with jailed network services.

Secure your DNS Servers

Cygna Labs supports mitigation of the following attacks to help you protect the integrity of your namespace, which is your very identity on the InternetDDI (DNS/DHCP/IPAM) vendors in terms of market share over the last several years by IDC, a leading analyst firm, who stated, “Cygna leveraged many years of IP resource management innovation while also being attuned to third platform trends.” We have indeed introduced numerous industry and product innovations over our two-plus decades of DDI experience and offer the following competitive advantages:

- **Denial of service attacks.** Adaptive rate limiting provides an automated mitigation mechanism to reduce the impacts of denial of service attacks; anycast addressing and extensive access controls are definable for port access as well as by DNS transaction type.
- **C2 DNS queries**. Identify and block or redirect clients querying malware command and control (C2) centers via our DNS firewall. Evasive DGA malware queries can be detected using AI technology by Cygna DDI Guard software.
- **Man in the middle attacks. Validating DNSSEC** - signed resource record data enables you to authenticate resolved zone data to prevent attackers from falsifying responses. DNS encryption via TLS (DoT) or HTTPS (DoH) reduce exposure of DNS query and response data to eavesdroppers.
- **Authoritative data attacks.** Protect updates to DNS zone data with controls on updates, transfers, the control channel, as well as on system shell access.
- **Reflector and amplification attacks**. Configure response rate limiting and deploy policies to your DNS servers to mitigate reflector style attacks.
- **Server attacks.** Protect your DNS servers from hacks with secure, purpose-built Sapphire appliances with jailed network services.

DNSSEC on Auto-Pilot

Configure DNSSEC validation natively on Cygna DDI and BIND recursive DNS servers. The Sapphire Sx20 is an automated signing authoritative DNSSEC appliance enabling these features.

- Automate DNSSEC management with policies for key algorithms, quantities, and lengths
- Automated zone signing, key generation and rollovers
- Multi-master redundancy
- NSEC and NSEC3 support
- Automated DS and CDS/CDNSKEY record generation and publication for parent zone notification.
- Use stock BIND servers or our appliances as secure secondaries.
- Supports PKCS#11 API for optional secure private key storage on an external hardware security module (HSM).

DNS transaction visibility

You can’t secure what you can’t see. Cygna DDI Guard provides DHCP and DNS transaction archiving with live traffic drill down to the packet level. Our Sapphire A30 IPAM Auditor appliance provides collection and aggregation of all Sapphire DNS query and response transactions as well as DNS firewall violations and detected DNS tunnels. Summary data and trending analysis are also provided for performance reporting.

DNS Security Summary

Cygna DDI solutions can help you secure your DNS and therefore secure your network.

- View, monitor, and audit DNS transaction data with Cygna DDI Guard software.
- Additionally view IPControl IPAM transactions with the Sapphire A30 IPAM Auditor appliance
- DNS firewall supports multiple response policy feeds and zones supporting block lists and allow lists
- DNS tunnelling detection and shutdown helps prevent sensitive data exfiltration and theft
- Adaptive rate limiting automatically mitigates DNS and DHCP denial of service attacks.
- Adaptive query throttling based on NXDOMAIN response frequency mitigates PRSD and DGA attacks
- Query/response rate limiting to mitigate D/DOS and reflector/amplification attacks
- Queries per client and query depth support reduces impacts of bogus query attacks
- Transaction signatures for DNS transfers, queries, notifies, etc.
- Anycast support for D/DOS resiliency
- DNSSEC signing and validation of zone data
- DNS service access control lists
- DNS update policy to granularly control dynamic updates
- Control and statistics channels ACLs
- Appliance port access and packet rate limiting
- Hardened appliance operating system reduces exposure to kernel or OS attacks

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