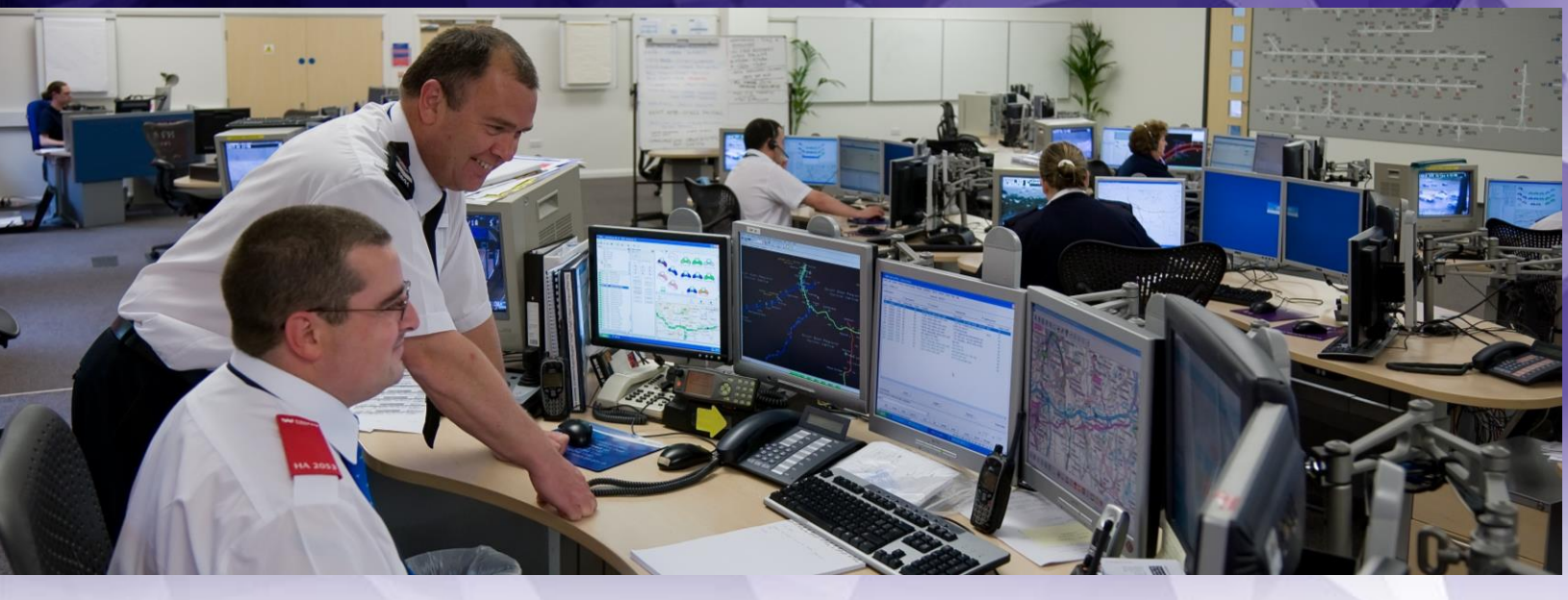
Datasheet.

Diamond IP 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. 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.

IPControl™ software and Sapphire appliances from BT Diamond IP facilitate 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. BT Diamond IP natively supports mitigation for these within its solution set without requiring extra licenses and appliances.

- Denial of service attacks. Extensive access control lists are definable for port access as well as by DNS transaction type; 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. Sapphire DNS appliances natively support randomized port and transaction identifiers.
- Malware command and control (C&C) access. Sapphire DNS appliances support configuration of multiple response policy feeds to enable firewalling of DNS queries from reaching C&C domain servers.
- Server attacks. Protect your DNS servers from hacks with secure, purpose-built Sapphire appliances with jailed network services.

Datasheet.

Diamond IP DNS Security Solutions.

Secure your Authoritative DNS Servers.

Authoritative servers are responsible for responding to queries relevant to your published namespace. Attackers may attempt to manipulate resolution information to repoint resolution data to their websites for nefarious purposes.

BT Diamond IP supports mitigation of the following attacks to help you protect the integrity of your namespace, which is your very identity on the Internet

- Denial of service attacks. Extensive access control lists are definable for port access as well as by DNS transaction type; rate limiting provides thresholding of incoming packets to mitigate DOS/DDOS floods.
- Man in the middle attacks. Signing your namespace using DNSSEC enables you to authenticate your zone data to prevent attackers from falsifying responses.
- Authoritative data attacks. Protect updates to DNS zone data with access controls on updates and transfers, the control channel, as well as on system shell access.
- Reflector and amplification attacks. Configure response rate limiting using IPControl's web interface and deploy policies to your Sapphire DNS appliances 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 Sapphire and BIND recursive DNS servers. The Sapphire Sx20 is an automated signing authoritative DNSSEC appliance enabling these features.

- 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.
- Multi-master replication
- NSEC and NSEC3 support.
- Automated DS record generation and publication for managed zones or notification to contact parent zone administrators.
- Use existing BIND servers or use Sapphire appliances as secure zone slaves.
- Support of PKCS#11 API for optional secure private key storage on an external hardware security module (HSM).
- Secure purpose-built hardened

DNS Security Summary

Diamond IP solutions can help you secure your DNS and therefore secure your network.

- DNS firewall with support of multiple response policy feeds
- Query/response rate limiting to mitigate D/DOS and reflector/amplification attacks
- Queries per client and query depth to reduce impacts of bogus query attacks
- Transaction signatures for DNS transactions
- Anycast support for D/DOS resiliency
- DNSSEC signing of zone data
- DNSSEC validation of signed responses
- DNS service access control lists
- DNS update policy to granularly control dynamic updates
- Control and statistics channels ACLs
- Appliance port access controls and packet rate limiting
- Hardened Sapphire appliance operating system
- Query logging support for SIEM and log aggregators
- BT Assure services in conjunction with DNS logging analysis and controls

Find out more at:

+1 610 321 9000 www.diamondipam.com