IP address management with security at its core

When it comes securing IP networks, it all starts – and ends – at the DNS layer. We can help you better secure your business with our DNS Security solutions. Our DNS firewall service can protect your network from the inception of malware communications and prevent infected devices obtaining attack instructions. In addition, DNS Security Extensions (DNSSEC) technology can automate complex initialisation and maintenance of keys and signing processes – all seamlessly integrated into your Diamond IP IPAM solutions.

DNS firewall

Most enterprise networks freely permit DNS traffic through firewalls because DNS is the essential first step in Internet communications for every device. Most infected devices use DNS to lookup the IP address of the malware controller's command centre. The malware then essentially serves as a remote "bot" implanted within your enterprise network to execute commands from the attacker's command centre.

Actionable intelligence

The BT DNS Firewall protects your network from the inception of malware communications attempts. It enables you to block or redirect queries for known malware and other undesirable domains to prevent infected devices from obtaining software or attack instructions. We provide a continually updated firewall feed for your recursive DNS servers to enable you to protect your network and to identify and mitigate infected devices.

Multi-faceted filters

You can protect your users from access to known malware domains and those of ill-repute – and also customize rules to filter DNS responses for queries to other undesirable sites, such as those known to contain adult, political or radical content. You have control for network protection and acceptable use policy governance.

Firewall policies

We provide a variety of triggers based on known bad actor domains and IP addresses from which you can enable or disable policies. You can select firewall policies to apply for each category you enable including:

- drop the response to the client
- respond with "not found" (NXDOMAIN)
- respond with "no data received" (NODATA)
- redirect to a given IP address, e.g., a captive portal
- respond with the "truncated" header bit to trigger TCP
- pass-through ("whitelist")

A simple subscription service that stops malware in its tracks

- enhance your overall network security implementation – DNS is the first step in communications
- timely firewall updates – our firewall feed provides updates several times daily to keep your policies fresh
- prevent malware callbacks – with over 91% of malware using DNS, controlling access at the DNS layer can inhibit the effectiveness of such malware
- identify infected devices – with policy logging and reporting you can quickly identify devices issuing queries.

Actionable reporting

Should a device querying your DNS server request a domain for which a policy exists, logging and alerts notify you of the querier IP address. This enables you to track down the offending device to investigate malware infestation and to apply remediation tactics.

Secure your DNS namespace

DNS Security Extensions (DNSSEC) technology enables organisations to digitally sign DNS data so resolvers can be assured of the validity of the publisher of the data and of the integrity 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 appliances are secure DNSSEC appliances that provide automated key generation, zone signing, and key rollover based on user-defined policies. The Sx models provide "set and forget" policy operation to automate the setup and ongoing management tasks associated with signed zones.

Multi-master redundancy

They 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-cut key rollovers.

Seamless IPAM integration

DNSSEC policies can be defined using a dedicated secure Sapphire DNSSEC administrator account. The IPControl 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.

Our IPControl software 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 Sx20 and Sx10D appliances for automated 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.

Key features

The Sapphire Sx20 is a highly redundant, highly scalable DNSSEC appliance while the Sx10D supports mid-tier deployments. Both models provide substantial cost savings by automating and simplifying your DNSSEC implementation. These savings can be realised through the following critical automation features.

Simple DNSSEC configuration

- 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 or notification to contact parent zone administrators
- use existing BIND servers or use Sapphire appliances as secure zone slaves.

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 operating system
- 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 as well as IPControl corroboration of master peer status for reliable failovers
- dual hot-swappable power supplies
- RAID-5 hard disk redundancy on the Sx20
- IPMI lights-out interface
- OS, kernel, and services upgrades can be deployed from the centralised IPControl interface
- signed and unsigned DNS zone management
- IPControl
- Static and dynamic zones support
- Centralised monitoring and control via EX or IPControl appliance dashboard.

Why choose BT?

Diamond IP from BT offers the most flexible and scalable solutions for today's complex IP networks. Our solutions help you reduce costs, enhance productivity and gain efficiencies while improving the management and security of your IP infrastructure devices and services.

Our products adhere to open standards, providing maximum interoperability within your existing network, including cloud and hybrid networks.

What could IPAM DNS security services do for you?

Visit globalservices.bt.com/en/solutions/products/diamond-ip

Offices worldwide.

Issued: December 2018