Summary

- SOLIDserver™ from EfficientIP helps you secure your business by hardening your DNS Server architecture.
- The SmartArchitecture features help you deploy the first line of defense by implementing very easily an effective DNS architecture following these best practices.
- Separate Authoritative DNS from Recursive DNS functions.
- Absorb DDoS volumetric attacks with a high performance DNS server. Always answer DNS queries.
- Mitigate zero day vulnerabilities by using an integrated Hybrid DNS architecture with 3 different DNS engines to harden Attackers work.
- Ensure performance and availability with a cloud deployment or mixed local and cloud DNS architecture integrating Amazon Web Services Route 53.

Enhanced DNS infrastructure Security

DNS servers deliver critical services to your company, such as internet visibility for your customers, partners and employees as well as access to network applications and other indispensable services such as email, CRM, VOIP, and the future IoT.

DNS technology allows you to type a name such as “efficientip.com” into your Web browser and your computer automatically finds that address on the Internet.

As a consequence of their fundamental role in Information Technology infrastructure, DNS servers are visible and vulnerable to everyone. Therefore, they must be secured to prevent catastrophic loss of business and brand damage resulting from DNS attacks.

There are two main types of DNS attacks:
- Attacks using DNS protocol flaws
- Attacks using bugs and/or flaws in DNS services or on machines running DNS services.

EfficientIP provides reliable and scalable solutions for hardening and securing not only your DNS servers but also your DNS service mechanisms and architecture.
Secure your business, secure your DNS

A Real Call to Action

An IDC DNS Security survey conducted in June 2014 shows that 72% of respondents said they had been targeted by a DNS attack in the last 12 months. As a result, their businesses reflected the following: 45% were impacted by downtime, 36% reported loss of business, and 40% had intellectual property stolen.

IDC concluded that “very little is being done about DNS security and companies feel that the basic protection offered by a firewall is enough. This is a real case of the wrong answer to a real problem. Firewalls are not the right technology to fight zero day vulnerabilities on DNS servers or when they are under DNS DDoS attack, as they will have no effect.”

(Read the full survey here: www.efficientip.com/idc-dns-security-survey-2014)

There are several DNS principles that must be followed to optimize the security and reliability of DNS architecture, but their complexity make them hard to deploy and maintain. EfficientIP’s solution dramatically simplifies the implementation of DNS best practices.

Apply DNS Best Practices through Smart Architecture™

The SmartArchitecture™ is a new approach to IPAM and DNS-DHCP services management to drastically simplify and secure deployment and administration of network services.

SmartArchitecture™ is a library of State-of-the-Art templates of DNS-DHCP architectures, applied on a group of Multi-Vendor servers (Microsoft®, Open source, SOLIDserver™) to automatically deploy and manage the architectures as a single entity.

The SOLIDServer™ centralized management platform will automatically configure all DNS servers according to their individual role within the selected template. It is no longer necessary to manually configure each server in order to build the architecture; the entire process is now carried out automatically. For example you can easily deploy a stealth architecture hiding the primary server to limit the risk of being attacked.

Update BIND as often as possible to limit bug problems:
EfficientIP releases security patches within 24 hours following the official publication of the update in order to ensure the highest level of security by running the latest version of BIND. These patches are available on EfficientIP’s web site and customers are also notified via EfficientIP’s customer mailing list.

SOLIDserver™ is a “one button” update technology, enabling top-tier security for your network and lower administration costs.

### Split authoritative name servers and recursive servers:

Authoritative name servers are assigned responsibility for specific domains and are reference points for DNS data validity. As such, it is critical to ensure the integrity of authoritative DNS servers. Splitting authoritative name servers from recursive servers and enabling modifications of authoritative DNS server configurations only directly from other authoritative servers or administrators eliminates all risk of corruption. Authoritative DNS servers are dedicated to only one function with strict policy access for modifications: an authoritative server will NOT cache. In the event of a DNS recursive server corruption, there will be no impact on the authoritative server.

Restrict recursive queries as much as possible to prevent spoofing: Limiting recursive queries is a fundamental rule when implementing the DNS architecture. This approach limits the risk of malicious requests that may corrupt DNS data or supply DNS architecture information to non-authorized DNS clients to steal for example personal data.

### DNS Blast Absorbs DDoS Attacks Up To 17 Million DNS Queries per Second

The world’s fastest DNS server

**Why is DNS Performance so Important?**

First: if your DNS servers crash and stop answering queries, your users will not be able to connect with their applications, nor will your customers be able to interact with you. In simple words, you lose money and your brand image will be dramatically impacted.
Second: the DNS protocol was designed to always answer every query. If for any reason there is latency or time out and some queries do not get resolved, this creates a major security hazard. Your DNS is now wide open for attackers to poison your DNS cache, which means that valid traffic will be easily redirected to malicious sites where private data can be intercepted and stolen.

Third: trying to filter malicious queries from valid queries is a very dangerous game and very difficult to achieve or administer operationally, in addition it could dramatically decrease the level of performance of the service. How do you correctly determine which query is valid from another? Always answering all queries eliminates the risk of Internet Exclusion due to DNS query filtering blocking clients access to your services.

According to a conference from ANSSI during the DNS OARC Fall Workshops conference in October 2013, the most secure solution is to answer all DNS queries. “DNS software that drops DNS messages is highly vulnerable to cache poisoning attacks since it will leave legitimate queries unanswered.”

Hybrid DNS Engine, the Ultimate Answer Against DNS Zero-Day Vulnerabilities

Hybrid DNS technology provides the highest-level of security for your name servers. When a security alert or actual cyber attack affects your currently-running name server software, Hybrid DNS technology gives you alternative name server software that you can switch to with a single click.

Your data center operations continue normally, and you revert to using the original name server software only after its vulnerability has been patched, tested and verified. The results are greater security, less risk, better performance (the alternative name server software is highly responsive), and easier administration.

EfficientIP is the only DDI vendor to provide state-of-the-art, high-quality, truly effective hybrid DNS security. The EfficientIP Hybrid Technology incorporates a second DNS engine, in addition to BIND, in a single DNS appliance. The alternate DNS engine is based on two different name server products, Unbound and NSD from NLnet Labs.

Unbound is a validating, recursive, and caching DNS resolver designed for high performance. NSD is an authoritative only, high performance name server.

At any given moment, one DNS engine is active (running) on a SOLIDserver™ DNS appliance and the other is in standby mode. EfficientIP’s SmartArchitecture™ automatically ensures that configuration changes are synchronized between the two DNS engines.

With a single click, you switch from running a Bind name server software that’s been hacked to alternate NSD or Unbound server software that’s been unaffected by a security breach. The alternative name server software can remain in place while DNS programmers patch, test and validate a security upgrade to the vulnerable name server product.

Hybrid Cloud Deployment

If you need more security and the best performance for your DNS infrastructure, you can choose to deploy a Hybrid Cloud DNS Infrastructure. You will centrally manage your in-house DNS server and your Domain Name in the Cloud. EfficientIP’s DNS Cloud is the only solution that integrates the Route 53 offering from Amazon Web Services, providing you with the ability to manage local and cloud DNS infrastructures from a single management console.
DNS Cloud includes all standard route 53 features through AWS APIs. DNS admins can manage domain names from this centralized console, which will automatically propagate the configuration to your DNS servers, locally and in the cloud. The DNS Anycast offers you the best performance and resilience that you can expect with a service level agreement of 100%. It is scalable, simple to deploy, cost effective, flexible and very secure.

DNS Firewall: Ensure Proactive and Efficient Protection against Malware

DNS-based malwares are particularly dangerous as they’re used to steal critical data, from you and from your customers.

EfficientIP’s DNS Firewall proactively protects SOLIDserver™ appliances and Linux-based DNS infrastructures by detecting and blocking malware activity, identifying infected devices and preventing new attacks.

Recursive DNS server response policy (DNS RPZ) is based upon domain data feeds created manually by the IT administration team and/or provided by an external service. SOLIDserver™ DNS Firewall offers a granular approach to RPZ zone management. Instead of blocking an entire domain, exceptions for subdomains are created and then for each individual subdomain response policies are defined.

Based on DNS query analysis, SOLIDserver™ DNS Firewall detects and isolates clients infected with malware, blocking all communication with external websites and then disrupting malware activity. SOLIDserver™ DNS Firewall identifies the IP of the client responsible for the query which, when combined with IPLocator™ network discovery, localizes where the IP is connected on the network enabling a quick device cleansing.

DNSSEC

With SOLIDserver™, EfficientIP automates and simplifies DNSSEC implementation by providing a centralized and unified approach to DNS service management.

SOLIDserver™ enables you to deploy Secure DNS (DNSSEC-RFC 2535: http://www.ietf.org/rfc/rfc2535.txt) cryptographic electronic signatures signed with a trusted public key certificate that will determine the authenticity of the data. It eliminates the risk of cache poisoning attacks. EfficientIP partners with Thales to provide a highly secure DNSSEC solution. Thales’ nShield appliances work with SOLIDserver™ appliances to secure the private keys used for DNSSEC signatures.

Authenticate DNS with TSIG

SOLIDserver™ allows using TSIG (Transaction Signatures) to cryptographically authenticate and verify zone data. The use of a key shared between several DNS servers guarantees the authenticity of queries, transfers and updates.

EfficientIP’s DNS management solution centralizes the management of TSIG shared keys across DNS servers and then instructs them to use the key to sign communications with each other. Although queries from a client to a DNS server may be made anonymously, queries or transfers from one DNS server to another one must be authenticated since they make lasting changes to the structure of the Internet naming system.

EfficientIP provides appliances with at least 2 Ethernet interfaces and up to 4 interfaces. This allows you to:

- Clearly separate productive flows (DNS/DHCP) from management flows
- Use a dedicated interface for backup tasks to avoid overloading the productive network.