

## Best Practices Highlights

- Have alternative name server software ready to use
- Keep your name server software up-to-date
- Use DNSSEC-compliant and TSIG-compliant name server software
- Redirect DNS queries through forwarding routers (via Anycast)
- Separate recursive from authoritative name servers
- Place response time limits on recursive DNS queries
- Hide your Primary DNS server from public view
- Harden your name servers
- Over-provision your name server environment
- Establish physical security for your DNS servers

## Whitepaper

---

# DNS Security Best Practices

---

### Executive Summary

DNS cyber attacks exploit either the DNS protocol or the name server software's flaws and bugs.

By rigorously following a few simple, straightforward guidelines, you can mitigate and often even completely avoid the costs, downtime and headaches of DNS security breaches.

DNS (name server) protocols and software are subject to security breaches that can cripple your network, reveal confidential internal information about your company or turn your entire network into one huge botnet.

Use Best Practices guidelines to keep hackers, criminals and industrial spies from wreaking havoc in your organization.

The Best Practices guidelines discussed in this document can thwart DNS DDoS and many other types of DNS-based cyber attacks.

EfficientIP's SOLIDserver product implements these Best Practices to supply you with IPAM, DNS and DHCP services that minimize, mitigate and manage DNS-related (and other) security breaches.

## The Problem

DNS cyber attacks exploit either the DNS protocol or the name server software's flaws and bugs. In a simple form of Distributed Denial of Service (DDoS) attack, for example, a hacker queries your name server with a flood of small DNS request messages that causes your name server to transmit large response messages, with each response up to 70 times the size of the request. The resulting traffic jam can bring your network to its knees. Or a hacker causes a name server to become the apparent source of a DoS network packet flood by spoofing (altering) outgoing DNS network packets' source IP address to be the address of the actual target (victim) machine. The hacker inundates the name server with the spoofed DNS request packets. For each incoming DNS request, the name server returns its reply packets to the request packet's source IP address machine – which is the hacker's actual DoS target. In a third example, a hacker updates the DNS database with fraudulent entries that cause client computers to use hacker-substituted IP addresses instead of legitimate IP addresses.

The Best Practices guidelines discussed below can thwart these and many other types of DNS-based cyber attacks.

## Have alternative name server software ready to use

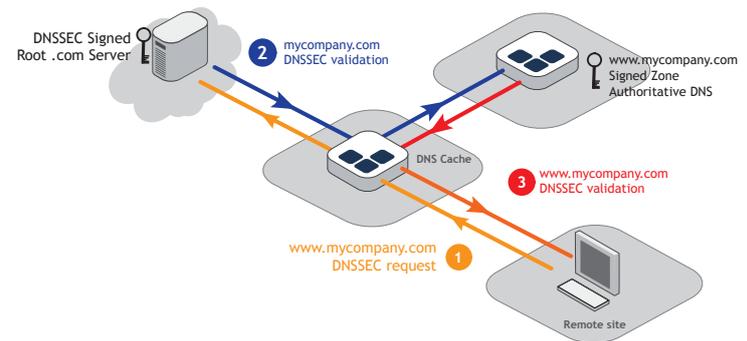
Network administrators should maintain – and be ready to switch between – at least two different name server software products. When a new security alert is issued, an administrator can switch to using name server software that is unaffected by the alert. The alternative name server software can remain in place while DNS programmers patch, test and validate a security upgrade to the vulnerable name server product. Additionally, this hybrid DNS approach confuses hackers by giving them different network message “footprints” to analyze because the different DNS engines use unique algorithms. Hackers' badly-formatted DNS probes will result in completely different, difficult-to-analyze responses.

## Keep your name server software up-to-date

Within no more than 24 hours of the official release of an update or corrective patch to the name server software you're using, you should install the new name server software version on your name servers.

## Use DNSSEC-compliant and TSIG-compliant name server software

Domain Name System Security Extensions (DNSSEC) uses digital certificates to authenticate DNS queries and responses. Transaction Signatures (TSIG) ensures that DNS database updates (new or changed URL-to-IP-address relationships) are valid and authentic. Together, DNSSEC and TSIG give you a high degree of confidence that your network's clients and servers are using correct IP addresses.



## Redirect DNS queries through forwarding routers (via Anycast)

Routers use Anycast, which allows multiple servers to share the same IP address, to send network messages to the most pertinent server rather than to a specific server. Name servers can use Anycast to

- Share the workload
- Exhibit resilience
- Mitigate a DDoS attack by diluting its effects

A network that uses Anycast is resilient because routers flexibly and dynamically send traffic to the nearest available server. If you remove a server (or data center) from the network, traffic flows to the next closest server (or data center).

Anycast helps mitigate a DDoS attack by “increasing a network's surface area” – i.e., that portion of the network exposed to attack. The effect of the DDoS attack is spread across multiple servers (or data centers), thus lessening the traffic flood that each server or center must absorb.

The Internet's root name servers have for many years made good use of Anycast.

## Separate recursive from authoritative name servers

Authoritative name servers search just a local datastore to find a name and its IP address. Recursive name servers search a local datastore plus a hierarchy of other name servers to find a name and corresponding IP address. You should use different authoritative and recursive name server machines to separate and isolate these roles according to a logical view of your network, and you should configure the authoritative name servers to accept DNS database updates only from other authoritative name servers (or administrators). Because authoritative name servers do not cache, fraudulent or corrupted database entries in a recursive name server will not affect the authoritative name servers. Also note that the new BIND version 10 explicitly conforms to this guideline by separating recursive and authoritative name servers.

If you are just installing an authoritative DNS server, the Best Practices will tell you to install 2 servers, a master and a slave and they should be installed in two different data centers to ensure availability.

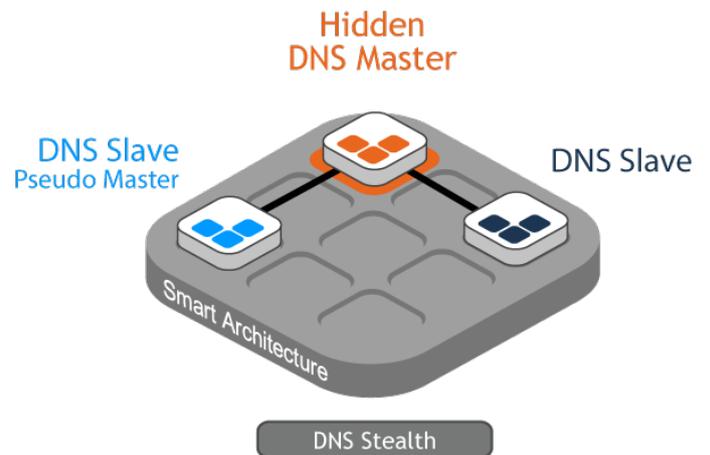
## Place response time limits on recursive DNS queries

You should use Response Rate Limiting (RRL) to throttle the speed at which an authoritative name server answers queries from a particular IP address. Many name server computer programs (such as BIND 9.9.4 or later, Knot and NSD) support RRL. With RRL, a name server remembers how many times it has sent the same response to the same querier. If this rate exceeds a threshold (that you configure), the name server waits for a time before sending a response (of course, the name server honors other queries from other computers in the meantime). As a result, the name server will never send responses to a querier any faster than specified by the threshold. The RRL-compliant name server becomes immune to many types of DDoS attack.

## Hide your Primary DNS server from public view

You should configure your publicly-visible DNS servers as slaves and designate your Primary DNS server to be a hidden master name server. A hidden (stealth) master name server is one for which no NS records exist in any publicly-accessible DNS database. Only the slave name servers are known to the outside world. This slave-and-stealthy-master architecture prevents public interrogation of your internal (master) name ser-

vers (either by query or zone transfer). It also protects the integrity of the slave name servers' DNS databases, because only the hidden master server can update (via a push operation) the slave servers.



## Harden your name servers

The only software running on your name server computers should be the name server software and the operating system, with the name server computer dedicated to its role of supporting your network. Any other software running on a name server invites hacking attempts. It can also degrade the name server's performance and even possibly crash the name server computer if bugs are encountered.

Similarly, a name server's only connection(s) to the outside world should consist of the network link(s) through which the name server gets updates and through which the name server answers DNS queries. Having additional open ports and/or additional attached network cables invites hacking attempts.

## Over-provision your name server environment

A successful DDoS attack overwhelms a name server's capacity to do its job. If you configure your name server environment to have excess computing speed, excess memory and excess disk access speed, by either over-provisioning a name server computer or by having multiple name server computers, you can mitigate the effects of what would otherwise be a highly successful DDoS attack.

## Establish physical security for your DNS servers

Attacks on your name servers might come from within your organization, not just from the outside world. You should set up a name server computing environment that prevents disgruntled or bribed employees from physically accessing your name server computers (not to mention, of course, your other mission-critical servers). Different data centers use different methods to establish the physical security of their servers and other critical infrastructure components. Make sure you have effective measures in place to physically secure your name servers.

## EfficientIP SOLIDserver and Best Practices

EfficientIP's SOLIDserver exhibits the highest levels of security by automating all the Best Practices enumerated here. For example, SOLIDserver contains three distinct name server software products (Bind, NSD, Unbound), automatically keeps name server software up-to-date, is DNSSEC- and TSIG-compliant, supports RRL, is hardened and easily (via a SmartArchitecture wizard) establishes master/slave name servers.

---

### ABOUT EFFICIENTIP

EfficientIP solutions address organizations' needs to drive business efficiency through the innovative use of IT. Its unified management framework for DNS-DHCP-IPAM, devices and network configurations enhances security, availability and agility of the IT infrastructure. EfficientIP's solutions have been chosen by hundreds of the most demanding organizations across all industries.

[www.efficientip.com](http://www.efficientip.com)

### EUROPE

EfficientIP SAS  
4 rue de l'abreuvoir  
92400 Courbevoie-France  
+33 1 75 84 88 98

### USA

EfficientIP Inc.  
14 West Chesnut, Street  
West Chester, PA 19380 USA  
+1 888.228.4655

Copyright © 2014 EfficientIP, SAS. All rights reserved. EfficientIP and SOLIDserver logo are trademarks or registered trademarks of EfficientIP SAS.

All registered trademarks are property of their respective owners. EfficientIP assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document.