efficient iP®

White Paper

10 Best DNS Practices for Security and Service Continuity

Highlights

1. Keep your name server software up-to-date
2. Have alternative name server software ready to use
3. Use DNSSEC-compliant and TSIG-compliant name server software
4. Use IP Anycast routing to enhance DNS service reachability
5. Separate recursive from authoritative name servers
6. Place response time limits on recursive DNS queries
7. Hide your Primary DNS server from public view
8. Harden your name servers
9. Over-provision your name server environment
10. Establish physical security for your DNS servers

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

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

The Best Practices guidelines described in this document can thwart DNS DDoS and many other types of DNS-based cyber attacks. They will be helpful in order to keep hackers, cybercriminals and industrial spies from wreaking havoc in your organization.

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 Service Continuity 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.

1» Keep Your Name Server Software Up-to-Date

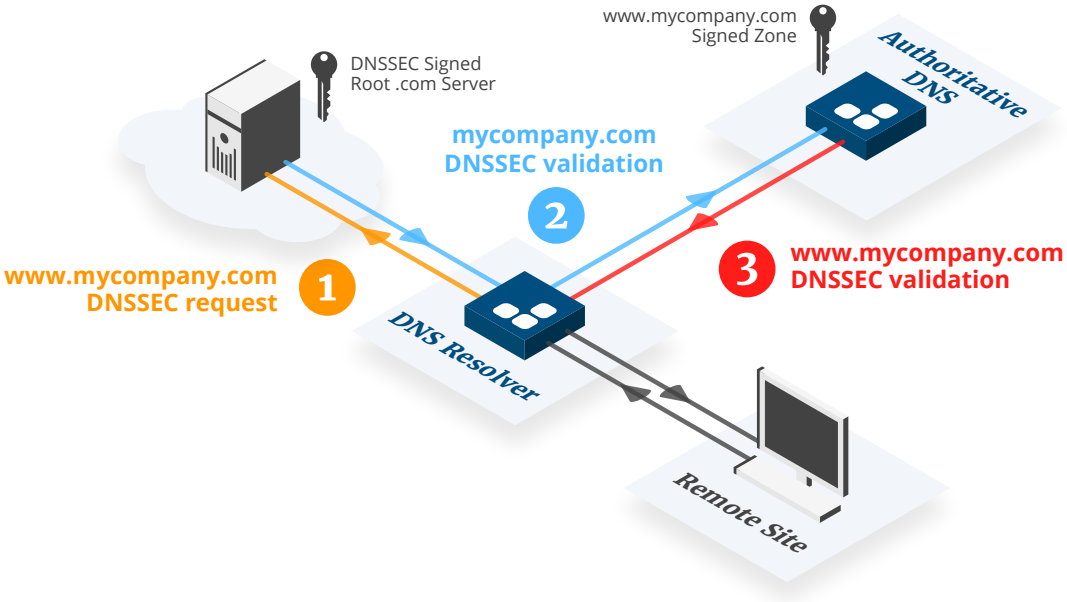
DNS software is a favorite target and whenever a security alert becomes known some may experiment exploiting it on any server on the planet. Within no more than 24 hours of the official release of an update or corrective patch to the name server software you're using, you should install the new name server software version on your name servers. This process is helped by the fact that the DNS service is the only one running in its appliance or virtual machine so avoids impact to other neighboring applications.

2» 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 on the one which is running, 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.

3» 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.



4» Use IP Anycast Routing to Enhance DNS Service Reachability

Routers use Anycast, which allows multiple servers to share the same IP address, to send network messages to the closest available 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
- Offer the service through an easy to remember address

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. This solution is designed for the Internet but is also suitable for private organizations' IP networks.

5» Separate Recursive from Authoritative Name Servers

Authoritative name servers search just a local datastore to find a name and its IP address and by extension any additional records that can be held in a zone. Recursive name servers search a local temporary cache plus a hierarchy of other name servers to find a specific record. You should use different authoritative and recursive name server machines to separate and isolate these roles according to a logical view of your network. In addition 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 make use of cache, fraudulent or corrupted database entries in a recursive name server will not affect the authoritative name servers.

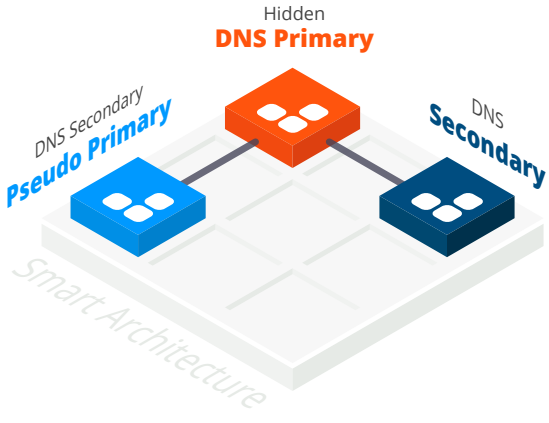
If you are installing only an authoritative DNS service, the Best Practices will tell you to install multiple servers, a primary and a secondary and they should be installed in two different data centers to ensure availability.

6» 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, 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.

7» Hide your Primary DNS Server from Public View

You should configure your publicly-visible DNS servers as secondary and designate your Primary DNS server to be a hidden primary name server. A hidden (stealth) primary name server is one for which no NS records exist in any publicly-accessible DNS database. Only the secondary name servers are known to the outside world. This secondary-and-stealthy-primary architecture prevents public interrogation of your hidden primary name servers (either by query or zone transfer). It also protects the integrity of the secondary name servers' DNS databases, because only the hidden primary server can update (via a push operation) the secondary servers.



8» 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.

At the operating system level, any unused services should be stopped, access control and credential validation should be set at the highest level possible for the organization and the administration team and audit log should be enabled.

9» 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. This can be adjusted with the level of response time limits set through the RRL (see §6).

10» 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 primary/secondary name server topologies.

efficient iP®

REV: C-210113

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752