CSC

The Case for a Secondary DNS Service

Improved security strategies to protect your online assets

It can happen to you

On October 21, 2016, a well-known managed domain name system (DNS) provider was rocked by a massive distributed denial of service (DDoS) attack. The attack not only suspended the availability and services of the DNS provider, but the collateral damage was also spread to a number of well-known brands whose websites and applications also suffered intermittent outages.

In the aftermath of the attack came the sobering reality that no one is immune from DDoS threats, especially against their DNS. But of equal concern was the overwhelming notion that the affected companies hadn't done anything wrong. They did what many consultants recommended at the time—entrusted their DNS to a managed service. But their lack of a backup proved to be the fatal flaw.

The October 21 attack signaled a fundamental change in the way DDoS assaults would be assembled in the future. This attack was launched using the Mirai Botnet malware that is comprised of atypical internet-connected devices such as security cameras, DVRs, and home routers. Taken together, the hijacked devices formed a dangerously potent high-volume weapon. The Mirai Botnet unleashed a devastating DDoS attack on a scale previously unseen. And due to its effectiveness, the botnet would become a dangerous harbinger of things to come.

But most importantly, the attack provided an invaluable lesson on the new requirements for DNS. Specifically, that businesses shouldn't exclusively stake their entire online presence on just one DNS service. The organizations that solely relied on one DNS provider showed the real-world consequences of depending on a single point of failure. If those companies had split their DNS between multiple services, then their sites, apps, and other online assets would be less likely to have gone down—even during the height of the attack.

Compounding the problem is the pace of today's cyber crime. A solid strategy to limit cyber attacks can be rendered obsolete in less than six months. This is particularly true in cases of DNS attacks, as criminals realize the potential for disruption by taking aim at DNS vulnerabilities.

This document is based on "The Case for a Secondary DNS Service" by Neustar®.

Organizations can effectively update their DNS security posture with minimal cost and effort by incorporating new technology and revising their current security strategies.

Digging deeper into the DNS dilemma

In today's internet age, enterprise security has focused primarily on protecting the online perimeter (i.e., the network border). The rationale was, if you could block malware and bad agents from entering the network, then you could protect your data and your business. Cyber criminals, however, are persistent and adaptive. As one door closes, they discover a new, open window. And so, it wasn't long before cyber criminals found that they could impact and disrupt organizations by attacking the protocol responsible for their online presence—DNS.

Despite its importance, for many years DNS was something of a security afterthought. It was taken for granted as a public protocol that was used to route requests, but it wasn't seen as a security vulnerability per se. All of that changed with denials of service (DoS, and later, DDoS) attacks. By flooding a DNS server with requests, cyber criminals can indefinitely shut down an organization's website and applications. And since website and application availability are inextricably tied to DNS, security quickly went from an afterthought to front of mind.

To attack a DNS server, you first need its physical address. Hosting your own domain name system can expose your DNS address to anyone with even a modicum of internet skills. For example, a competent internet user can discover an unprotected DNS address in less than 30 seconds. Not surprisingly, security consultants began to advocate that organizations use an external DNS provider to handle their DNS requests in a more secure and efficient manner.

The proper security posture for authoritative DNS

The single most important thing that organizations can do to protect their authoritative DNS service is to implement both a primary and secondary DNS solution. In the wake of the Mirai Botnet, industry analysts (e.g., Gartner) recommend that organizations have a secondary DNS service for better performance and security.

A secondary DNS service shouldn't be confused with a redundant DNS provider. It's not about having a Plan B in case your Plan A fails. It's about having a smarter Plan A that effectively splits your DNS traffic between two trusted networks. This strategy not only prevents your brand against a single, take-down DDoS attack, but also improves your DNS redundancy by splitting the load between two networks.

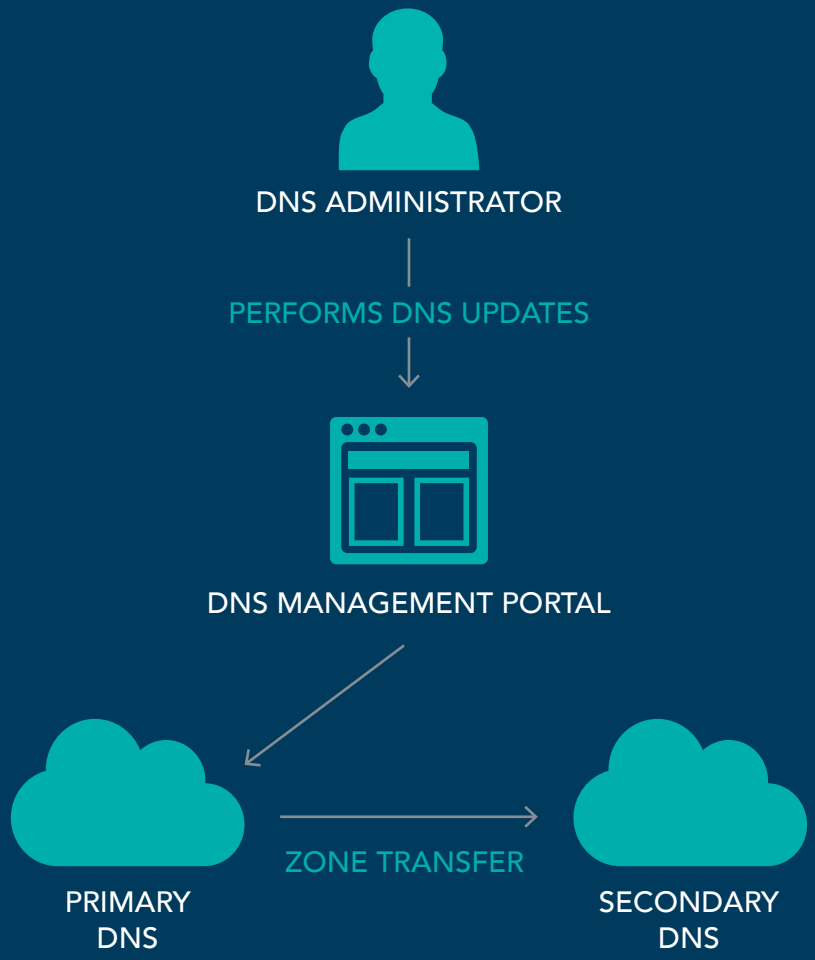
Finding a secondary managed DNS service is the first thing that you should do to shore up your DNS security. Second is select a DNS provider that offers a dedicated in-house DDoS mitigation service for its managed DNS networks. As more connected devices join the internet and create the potential for more and broader botnet armies, a separate layer for DDoS protection makes sound sense for organizations. Better still, if you can "hide" your DNS from direct exposure to the internet through an air-gapped network, you can dramatically reduce the number of attacks against your DNS.

A stronger security posture for authoritative DNS includes:

- A primary and secondary managed DNS service
- Choosing a provider that has a dedicated in-house DDoS mitigation service for its DNS network
- The ability to hide DNS systems from direct internet exposure

HOW PRIMARY AND SECONDARY DNS WORKS

1. DNS administrator logs into DNS management portal
2. DNS administrator updates a DNS record
3. Change propagates through DNS network
4. Secondary DNS will be notified there had been an update and performs a zone transfer to receive updated record



Double down on DNS attacks with trusted and secure partners

As the saying goes, "you are only as secure as your weakest link." Work with providers who offer you the security you need. CSC is the most security conscious enterprise-class provider of domains, DNS, and digital certificates in the market today. We enforce security policies to ensure our systems are secure, and our staff are aware of and trained to mitigate threats, so that we protect our clients' digital assets 24/7/365. An important part of our security posture is selecting and working with the right partners.

CSC partners with Neustar because it's an enterprise-class provider capable of delivering the availability, scalability, and security required to power DNS in today's digital climate. Neustar has invested heavily in building advanced DNS security solutions that protect organizations from all types of threats. Together with our domain and digital certificate management services, and CSC Security Center℠, CSC enables its clients to securely manage all their digital assets outside the firewall, which are at risk of attack from DNS cache poisoning, domain or DNS hijacking, domain shadowing, as well as DDoS, malware, and phishing.

Request more information on how CSC Security Center and our DNS Management services can help you mitigate cyber threats.

CSC supports companies that are making significant investments in their security posture by exposing blind spots that exist within fundamental internet assets such as domain names, DNS, and digital certificates. By leveraging our proprietary security solutions, CSC secures companies from cyber threats to their digital assets, helping them avoid devastating revenue loss, brand reputation damage, or significant financial penalties as a result of policies like GDPR. Along with internet assets, CSC protects online brands that are being exploited via counterfeit websites, fraud, and IP violations, and helps monitor and mitigate this, providing enforcement and advisory services to protect many of the world's largest brands. Learn more at cscdigitalbrand.services.

cscdigitalbrand.services