Security Solutions

White Paper

neustar

Master Your Domain:

Why DNS Matters in the Connected World

Table of Contents

Master Your Domain: Why DNS Matters in the Connected World

If you read the news—and more than likely, you read it online—you know that the Internet can be a dangerous place. Seemingly harmless emails in our inboxes can serve as the perfect Trojan horse, waiting to infect our computers with malicious malware or simply hijack our identities. Once-innocuous locations like libraries and local restaurants are becoming havens for scammers and hackers who can steal your personal information via public Wi-Fi. Even the websites posing as legitimate news sources may, in fact, be nothing more than a means to install malware on our devices.

Unfortunately, security threats like these are not just an individual problem. Organizations also need to worry about them, in addition to "big" threats such as massive Distributed Denial of Service (DDoS) attacks and data theft. As many organizations are learning, employee actions on the Internet can have a significant impact on profits, public image, and the ability to protect customer data.

Make DNS Your First Line of Defense and Not an Afterthought

Organizations spend a significant amount of time and treasure thinking about security. But misplaced priorities and the false assumption that today's threats can be quelled with yesterday's defenses can quickly doom an organization. It's time to be more aggressive about infrastructure safety. The first step to doing so lies in the Domain Name System (DNS).

DNS is more than a directory of Internet Protocol (IP) addresses; it can be the first line of defense for Internet communications entering and leaving your network. By filtering the traffic that goes in and out of the network at the DNS level, organizations can stop the vast majority of malware, viruses, and unwanted content before it enters their networks.

In this paper, we'll examine four key DNS-related problems that affect organizations and identify how a DNS solution provider can best address them.

Every organization that has a website also has at least two DNS servers: an authoritative server that directs external traffic to its website, and a recursive server that directs internal users (i.e., anyone logged into your network) to online assets that reside inside and outside the network. There are accepted industry practices focused on how to best implement these servers, but the security requirements and operations management can be a headache if you host your own servers.

Using a hosted DNS provider will reduce the management burden, but using only one hosted DNS provider is risky because it represents a single point of failure in the event of a DDoS attack or outage. Industry analyst firm Gartner recommends that organizations use at least two different DNS hosts, preferably in different locations, for better redundancy and resiliency.

When choosing a DNS provider, organizations need to look at more than just the provider name. For example, choosing a provider that offers a DNS security solution on top of basic name resolution can reduce cost and complexity while providing an improved security barrier.

1 You've Got a Performance Problem

Last year, three out of four organizations were affected by DDoS attacks—many of them more than once.* DDoS attacks are often used to overload the authoritative DNS server, blocking visitors from accessing an organization's website. But DDoS attacks can also be directed at your recursive DNS server, blocking your internal network users from accessing the Internet or internal assets. A successful DDoS attack can impact employee productivity (on the recursive side) and negatively affect revenue (on the authoritative side), costing enterprises $100,000 or more per hour during peak periods.[1]

Internet access issues can occur for reasons other than DDoS attacks. There may be too many users on the network. There may be too much latency between "hops" in the network. A DNS hosting provider can exacerbate or mitigate these problems, depending on how their solution is architected.

Neustar's integrated UltraRecursive and UltraDNS solutions are designed to improve network performance issues by providing:

- **Near-zero latency and Instant cache updates** between Neustar's DNS servers through colocation (i.e., the recursive and authoritative servers are located in the same physical facility)
- **Rapid deployment and scale using a hosted model**—add nearly unlimited capacity with no appliances to install or manage
- **Built-in DDoS protection** using the world's largest DDoS mitigation network

To get the whole story on DDoS, download your free copy of Neustar's "Worldwide DDoS Attacks & Protection Report: A Steady State of Threats in the Connected World."

[1] Neustar, "Worldwide DDoS Attacks & Protection Report: A Steady State of Threats in the Connected World," October 2016.

2 You've Got a People Problem

You can devise hundreds of security policies, but you can't ensure that people are always doing the right thing. One problem could be employees who consume an inordinate volume of network bandwidth by watching videos on their lunch break. Another could be customers who access inappropriate content in your restaurants over lunch. Accessing inappropriate or unauthorized content can hurt your network's performance, harm your devices, and expose your network to new threats. The best way to stop internal users from bringing bad things inside your corporate network is to stop them at the source using recursive DNS servers.

Neustar's UltraRecursive solution is an advanced recursive DNS service that enables enterprises to filter a variety of content types from being accessed or downloaded over the network.

ULTRARECURSIVE INCLUDES

- **20 pre-defined categories** for content blocking
- **Blacklists and whitelists** that support endless customization
- **Consistent Acceptable Use Policy enforcement** at the user level and across thousands of remote locations
- **A simple point-and-protect platform:** bad traffic is blocked automatically with no additional hardware needed

> The best way to stop internal users from bringing bad things inside your corporate network is to stop them at the source using recursive DNS servers.

3 You've Got a Malware & Phishing Problem

***Phishing* is a form of identity theft that looks to collect your personal information by posing as a legitimate email from a trusted company or organization. It may feel like a random crime because of its prevalence—for many people, phishing emails are a daily reoccurrence—but phishing can be the result of the sites we visit. Cybercriminals often use seemingly innocuous websites that may advertise celebrity news, downloadable movies or other content to "phish" for personal information and download malware onto computers and mobile devices.**

This is a particular problem at universities and school campuses. The proliferation of mobile devices among students combined with a school's limited resources can create a perfect storm for phishing, malware, and viruses. Here again, addressing the problem at the recursive DNS server level with strong blacklisting and threat intelligence can filter out the vast majority of bad agents and malware.

UltraRecursive further protects against site-specific phishing and malware attacks by blocking known malware and phishing categories and by cutting communications with the external command and control (C&C) servers that are used to activate and direct malware once it has breached network defenses. The sooner you can shut down the C&C connection, the less time and money a breach will cost you.

The proliferation of mobile devices among students combined with a school's limited resources can create a perfect storm for phishing, malware, and viruses.

4 You've Got a Public Problem

In the retail and hospitality industries, some customers are feeling too much at home, especially when it comes to what they're watching on public Wi-Fi connections. Several national "take out" restaurants, for example, have encountered high-profile problems because of what their customers are bringing in to their restaurants: adult and illicit content. In an industry where free Wi-Fi access is as expected as free ketchup packets, some customers have clearly taken advantage of the amenity. The problem of public online adult content has brought unwanted publicity to some businesses, eliciting a public backlash that demands businesses police the types of content that can be streamed on their network.

Filtering inappropriate content at the firewall level, while individually effective, presents a number of logistical challenges for a national chain that may have thousands of separate locations. By using a solution such as UltraRecursive, an organization can enforce consistent content filters at all of its locations simply by pointing the recursive DNS requests to Neustar's DNS network. In this way, all locations share the same blacklists with no additional configuration needed and no added latency to their network experience.

By using a solution such as UltraRecursive, an organization can enforce consistent content filters at all of its locations simply by pointing the recursive DNS requests to Neustar's DNS network.

Two Solutions for Better Protection

The right security intelligence is key in the fight against DDoS attacks, data theft, viruses and other forms of malware. DNS servers are an enterprise's first line of defense against these cyberattacks. Authoritative and recursive DNS servers have complementary but different roles to fill in that line of defense. An authoritative DNS server, for example, needs to protect your network against DDoS attacks and *ransomware*—a newer form of malware that is increasingly being launched in conjunction with DDoS attacks. Recursive DNS servers need to provide consistent and customizable policies that block threats and bad user behavior based on current, reliable threat intelligence.

Neustar's UltraRecursive (for recursive DNS) and UltraDNS (for authoritative DNS) deliver a powerful one-two punch that knocks out most malware before it reaches your firewalls or other lines of defense. By filtering out more first-line threats, Neustar's hosted DNS services ensure that enterprises can focus their security efforts (and security budget) on specific threats with better results. Neustar's DNS solutions employ a hosted "point-and-protect" model that delivers industry-leading DNS protection without the need to implement or maintain on-premises systems.

With UltraRecursive and UltraDNS, enterprises have a powerful DNS platform that blocks out the bad guys and bad content for a better, safer online experience. The Neustar platform features ultra-secure capabilities not found in other DNS solutions, such as:

- **Two Highly Reliable, Global DNS Infrastructures** that are engineered to deliver near-zero latency responses and instant cache updates
- **Advanced early detection capabilities** that block malware before it reaches your network
- **Customizable blacklists and filters** that block potentially harmful websites or inappropriate content from your network
- **DNS Shield Network:** a shadow network of privatized connections between DNS servers that dramatically reduces latency and enhances security for DNS requests
- **Built-in DDoS protection** through Neustar's global DDoS protection network—the world's most sophisticated DDoS protection network
- **A rapid, inexpensive ramp to world-class DNS services** with no upfront fees, no installation, and no configuration required

One Vendor to Trust

At Neustar, we take your security seriously. From fraud protection to IP reputation, DDoS to DNS, we build solutions that make the online world safer.

To learn more about **UltraRecursive**, **UltraDNS** and our complete portfolio of security solutions, visit us online at:

www.neustar.biz

About Neustar.

Every day, the world generates roughly 2.5 quadrillion bits of data. Neustar (NYSE: NSR) isolates certain elements and analyzes, simplifies and edits them to make precise and valuable decisions that drive results. As one of the few companies capable of knowing with certainty who is on the other end of every interaction, we're trusted by the world's great brands to make critical decisions some 20 billion times a day. We help marketers send timely and relevant messages to the right people. Because we can authoritatively tell a client exactly who is calling or connecting with them, we make critical real-time responses possible. And the same comprehensive information that enables our clients to direct and manage orders also stops attackers. We know when someone isn't who they claim to be, which helps stop fraud and denial of service before they're a problem. Because we're also an experienced manager of some of the world's most complex databases, we help clients control their online identity, registering and protecting their domain name, and routing traffic to the correct network address. By linking the most essential information with the people who depend on it, we provide more than 12,000 clients worldwide with decisions—not just data.

More information is available at

www.neustar.biz