Next Generation DNS

Thunder NSI

Internet Optimization using Thunder DNS

The Evolving Role of DNS

The Internet continually finds new ways to improve our lives. Cloud adoption transforms businesses. Online retail changes the way we shop and mobile technology provides 24/7 connectivity. The Internet has evolved significantly and future technologies such as online currency, connected vehicles, and artificial intelligence will continue to transform our paradigm of the Internet Ecosystem.

Over the past four decades, one building block of the Internet that remains constant is the Domain Name System (DNS). During this period of change, DNS has quietly provided the primary means of navigating the Internet by offering a Domain to IP Address lookup service, essentially matching memorable domain names to seemingly random server IP addresses.

In fact, experts believe our reliance on Domains and the DNS service will increase exponentially as the Internet evolves. The three main reasons for this are, first, the adoption of Content Delivery Networks, meaning that content is provided by different servers in different locations. Second, on-browser construction of web pages requires that a single domain may need to lookup content from several different web servers. Third, universal compatibility makes DNS the technology of choice for the billions of new connected devices and cloud platforms.

Most interesting is the opportunity to re-purpose existing DNS service to optimize Service Provider Networks. DNS technology can now provide Cyber Security, enable a customized Internet experience, create brand loyalty, and enable machine-learning optimizations.

Integrated Cloud Firewall

Part of DNS's basic architecture is a failure mechanism originally designed to send an error message when a domain is no longer available. This mechanism can be leveraged to protect users and infrastructure from cyber threats.

Protecting Users

Due to constant, high profile security breaches, users demand protection against threats lurking on the Internet.

Malware poses two main challenges to end-users. One is the risk of subscriber information being stolen and exposed, i.e. financial fraud. The other is degraded Internet or network performance on infected devices. Users tend to blame their Internet or managed service provider regardless of whether or not they are at fault. Users also expect the service provider to resolve any degraded Internet service.

Thunder DNS provides a universal, network-based filtering capability that automatically blocks user access to malicious websites. Also, it has the ability to block automated botnet activity to maintain network uptime.

Protecting the end user against one of the primary sources of cyber attacks can significantly decrease end-user complaints, decrease customer support calls, and prevent the user from looking for alternative services. Additionally, DNS provides this protection for all devices including edge devices in Internet of Things (IoT) applications.

Protecting Network Infrastructure

DNS protects Network Infrastructure by constantly updating security definitions thereby preventing infected infrastructure from communicating with known malware servers.

One limited resource for providers is available public IP's they can assign to customers within their network. Many providers use a NAT to service multiple clients from a single IP public IP address. The challenge with this approach is that multiple customers sharing a single public IP address can be blacklisted if a single customer becomes infected.

Customizing the User Experience

Content & Timing Filters

In an increasingly competitive market, service providers innovate at a rapid pace with the goal of driving value through differentiated services. A focus on high quality services and network-level cyber security are important value-add services; however, there are additional opportunities using DNS to enable a personalized user experience.

Many users are looking to shield themselves from specific types of content, such as explicit violence, illegal drugs, or adult content. In addition, users may want to manage content availability by time. This DNS capability allows users to create unique filters and parental controls specific to their household.

Regulatory Compliance

Households are not the only group in need of DNS content filtering. In fact, many businesses use content filtering to protect their workplace. In the public sector, these requirements are typically mandated and many governments universally prohibit extreme content.

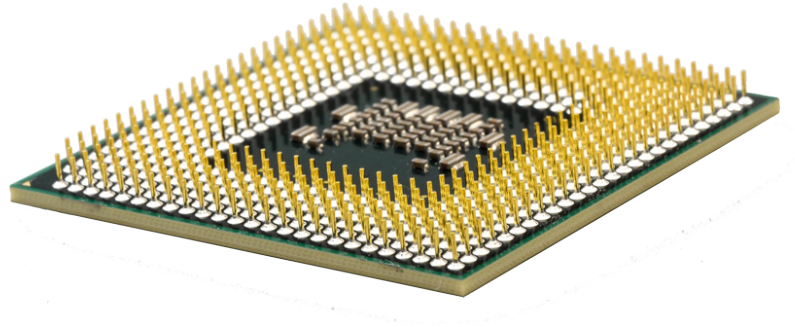
Leveraging DNS to Create New Value

Protecting and Redirecting Subscribers

Next generation DNS can re-direct subscribers from known cyber threats to a sponsored landing page. This landing URL builds customer loyalty by highlighting how the service provider is protecting their subscribers. In addition, this landing page can be used to cross sell the Service Provider's products and services to its customer base in an unobtrusive manner.

Machine Learning & Big Data

Machine Learning AI is poised to create huge value for service providers. It can be used to predict growth, identify opportunities for network optimization, anticipate which customers are likely to leave, and identify new customer demands. However, AI requires training using a huge dataset of relevant information.



Next generation DNS is ideal for creating that big data dataset by logging DNS queries. Each DNS query provides small pieces of meta-data that can be aggregated into a local "Big Data" database. Eventually, this database will train Machine Learning AI to create new value for users and service providers.

Next Generation DNS Summary

DNS has significant, untapped potential and will continue to be a cornerstone of the Internet infrastructure as the Internet grows. Next Generation DNS technologies leverage the ubiquitous nature of DNS to provide a significantly improved Internet experience. These improvements include, but are not limited to, integrated cyber security, custom filtering, and machine learning.

Unlike cloud-based DNS providers, Thunder DNS works with service providers and integrators to keep DNS services local. This local hosting enables partners to cost-effectively secure and optimize the user experience.

Thunder develops next generation Networking, Security, and Intelligence technologies. Originally founded in Silicon Valley, our company has since grown internationally with our headquarters in Las Vegas, USA. Our team includes world class engineering talent with experience from high growth telecommunications, security, and enterprise class product companies including Microsoft, Ubiquiti, Ericsson, Verisign, E-Bay, Telstra, and Syniverse. Our business approach is to empower Service Providers and Solution Integration partners with innovative technologies.