CASE STUDY

Tier-1 Cable Provider Protects Subscriber Privacy with Encrypted DNS at Scale with A10 Networks Thunder CFW

Industry | Service Provider

DNS is one of the most essential functions of the internet, but until recently, DNS queries have been largely unprotected. If the queries are left unencrypted, the websites that users visit are visible to anyone with a little technological know-how. With DNS traffic vulnerable to spoofing, interception, and hijacking by bad actors, internet users are at risk of malware, ransomware, and data theft. Lack of protection is why DNS resolvers are one of the top-five DDoS weapons and DNS service ports are one of the most prominent UDP targets, according to the latest State of DDoS Weapons Report.

> *As encrypted DNS grows in usage, the cable operator can assure privacy and security for tens of millions of subscribers without impacting the user experience.*
>
> – Tier-1 Cable Operator

Network Solution

A10 Thunder® CFW

Critical Issues

- Rapidly support the new encrypted DNS protocol to protect subscriber privacy and security while maintaining service continuity

Results

- Meet the performance and scalability requirements of encrypted DNS queries from potentially tens of millions of subscribers
- Able to support up to 600 million encrypted DNS queries per day
- Gain enhanced security and visibility to protect its DNS infrastructure from multiple attack vectors
- Protect key services such as parental controls and content delivery

The Challenge: Subscriber Privacy and Security

This prominent Tier-1 cable operator recognized the importance of protecting its subscribers' DNS activity to assure their privacy and security. The company, with tens of millions of customers, wanted to deploy the new encrypted DNS protocol, DNS over HTTPS (DoH), into its production network as quickly as possible.

In short, DoH ensures end-to-end encryption for DNS queries. DoH, in RFC 8484, is a proposed standard from the Internet Engineering Task Force (IETF) that enables the encryption of DNS lookups between a user's device and its DNS resolver to protect user privacy and security.

Rolling out DoH quickly would enable the cable operator to assure the user experience and maintain continuity for services that depend on DNS query data, such as content delivery, parental controls, and law enforcement requests. If DNS queries were resolved beyond the provider's infrastructure, it would lose visibility and control over key services.

Selection Criteria

With Firefox and Chrome supporting the new encrypted DNS protocol, the provider wanted to move rapidly to protect subscriber privacy and maintain service continuity. How many subscribers will adopt browsers with the new encrypted DNS was an unknown.

The company needed a high-performance, scalable DoH solution that it could rapidly deploy into production. It undertook a "build versus buy" evaluation for the new encrypted DNS functionality.

The Solution

The cable operator ultimately partnered with A10 Networks for a DoH solution that would enhance its user privacy and scale efficiency. A10 Networks worked swiftly to add DoH as a native capability to its Thunder® Convergent Firewall (CFW).

Thunder CFW combines a highly scalable and high-performance firewall, IPsec VPN, secure web gateway, application device controller (ADC), DNS over HTTPS (DoH), carrier-grade NAT with integrated DDoS protection traffic steering, and other functions in a single, standalone product.

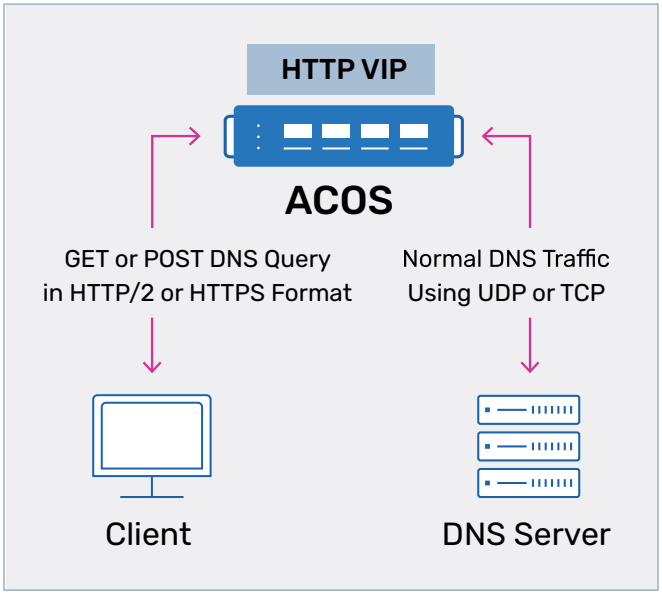

Figure 1: DNS over HTTPS

Quantifiable Results

As encrypted DNS grows in usage, the provider can assure subscriber privacy and security without sacrificing performance or impacting the user experience. And with Thunder CFW, it was able to deploy a DoH solution in weeks, rather than months.

End-to-end DNS encryption is enabled by TLS and requires additional processing capability. Thunder CFW is designed to deliver the scale and performance needed for high volumes of DoH traffic, as its advanced hardware capabilities are designed specifically to deal with encrypted sessions. The operator currently handles 600 billion DNS queries per day.

By deploying Thunder CFW, the cable operator protected its investment in its DNS infrastructure. Its existing DNS infrastructure components remain unchanged, while Thunder CFW natively handles secure connectivity and protocol translation.

With Thunder CFW, the provider can ensure continuity for services that depend on DNS query data. Beyond name resolution, DNS query data is used to deliver content and advertising based on geographical location.

Parental controls leverage DNS query information to keep children from accessing inappropriate websites at home. In the workplace, organizations can block access to gambling or other not-safe-for-work sites. The provider can also comply with law enforcement requests for users' internet activity. Without Thunder CFW, DNS requests would be resolved outside of the provider's infrastructure, and it would lose essential visibility and potentially impair subscriber experience.

Success and Next Steps

As browsers with encrypted DNS grow in popularity, the cable operator is prepared to protect its subscribers privacy as well as maintain service continuity. With a high-performance, scalable solution for DNS encryption, the provider is ready for widespread customer adoption.

The success of encrypted DNS depends on the collaboration of all organizations that provide DNS resolution services. The cable operator is committed to testing and deploying encrypted DNS to assure its subscribers' privacy and ensure continuity of important services like parental controls as the industry upgrades to the new, more secure DNS.

About This Tier-1 Cable Company

This Tier-1 cable company provides video, high-speed internet, and voice services to tens of millions of residential customers. It also offers a full suite of Ethernet, internet, Wi-Fi, video, and voice services to businesses.

The State of DDoS Weapons Report

Download Report

Request a live demo and experience the A10 Networks Difference

Schedule a Demo

About A10 Networks

A10 Networks (NYSE: ATEN) provides secure application services for on-premises, multi-cloud and edge-cloud environments at hyperscale. Our mission is to enable service providers and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness. We deliver better business outcomes that support investment protection, new business models and help future-proof infrastructures, empowering our customers to provide the most secure and available digital experience. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally.

For more information, visit A10networks.com and follow us @A10Networks.

Learn More

About A10 Networks

Contact Us

A10networks.com/contact

Part Number: A10-CS-80203-EN-01 APR 2020