SOLUTION BRIEF

Protect Critical DNS for Low Latency, Highly Available Broadband Networks

The A10 DNS Solution Portfolio Protects and Scales DNS for a Better Subscriber Experience

Overview

Domain Name System (DNS) provides the critical IP look-up function that directs every network connection request through the internet to its destination. Overloaded, malfunctioning, compromised or inadequate DNS infrastructure will cripple the subscriber experience, causing slow page loads, sluggish response or may deny service altogether. High performing DNS is essential for maintaining the experience of speed and availability in service provider networks – mobile, fixed or wireless. A10 Networks provides solutions that secure and scale DNS, allowing service providers to offer a faster, safer, more resilient subscriber experience.

Security Challenges

DNS Is a Favorite Target for Cybercrimnals

DNS services have gained the dubious distinction of becoming a top attack target. First, taking DNS servers offline is an easy way for attackers to keep thousands or millions of internet users from accessing the network, services, or applications. If attackers incapacitate a service provider's DNS servers, they can prevent subscribers from resolving domain names, visiting websites, sending email, and using other vital internet services. DNS attacks have brought down service providers' DNS services for hours, even days, and in extreme cases have led to class action lawsuits by subscribers. Organizations can suffer lost revenue and brand damage if an attacker disrupts access to DNS infrastructure and prevents users from accessing vital services.

Challenge

DNS is critical to maintaining the subscriber experience for speed, security, and resilience, but is highly vulnerable to malicious attacks and traffic overload that disrupt service availability. Service providers and enterprises must protect brand and reputation with high-performing solutions.

Solution

The A10 DNS portfolio shields DNS infrastructure from DDoS attacks and exploits while augmenting capacity for recursive and authoritative functions.

Benefits

DNS solutions from A10 add scalability and resilience to existing DNS infrastructure, protecting network and service availability and subscriber confidentiality.

©2023 A10 Networks, Inc. All rights reserved.

The A10 DNS solution portfolio includes security solutions optimized for DNS, including DNS application firewall, DDoS mitigation and protection and DNS over HTTPS/TLS. These solutions provide added security against malicious exploits and prevent service disruption from DDoS attacks

DNS Application Firewall (DAF)

A10 Thunder® CFW and Thunder ADC provide an integrated and powerful DNS application firewall, which stops buffer overflow, malformed queries, and Denial of Service (DoS) attacks, shielding DNS servers from attack. A DAF can be integrated with DNS load balancing to enable DNS to withstand heavy loads and massive attacks.

DDoS Detection and Mitigation

A10 Thunder TPS detects and mitigates multi-vector DDoS attacks at the network edge and scales to defend against the DDoS of Things and traditional zombie botnets. It does this by tracking 27+ traffic behavioral indicators to detect anomalous behavior against learned peacetime traffic to surgically distinguish legitimate users from attacking bots. Multiple layers of protection are provided for DNS services which include source-based rate limiting, authentication challenges, block abusive requests, ML-powered zero-day attack patten recognition and more. This gives defenders the ability to create customized defenses to ensure DNS services are resilient to targeted multi-vector DDoS attacks.

Privacy through Encryption

Security of the DNS infrastructure has never been more critical for service providers and for their enterprise customers. Many DDoS, ransomware and data theft attacks are carried out by targeting DNS. This is largely possible because the DNS query— the request between the DNS client and the local DNS server that provides the internet address— is transmitted in clear text, that is, unencrypted. To overcome this vulnerability, DNS over HTTPS (DoH) and DNS over TLS (DoT) have been proposed by the IETF, providing the DNS query encryption protection.

With the DoH/DoT features in A10 Thunder CFW, service providers can offer their subscribers the option of higher security and enhanced privacy protection through end-to-end encryption for DNS queries. Service providers can protect their ability to offer value-added services that depend upon DNS information, such as anti-malware tools, localized video content delivery, filters such as parental controls and responses to law enforcement. This can further strengthen their subscriber relationship and prevent accidentally “breaking” offered services from subscribers using alternative DNS providers.

Network Availability and Fast Response

Underperforming DNS technology will slow DNS resolution and add latency to query responses, causing slow web page downloads, timeout of applications and other problems that can impact the subscriber experience. Continually adding DNS capacity increases capital costs. By incorporating high-performance DNS technology, DNS servers can scale to process higher volumes of DNS queries and response times can be improved.

The A10 DNS portfolio includes high-performance Thunder TPS, Thunder ADC and Thunder CFW that provide added protection and processing capability including authoritative caching, load balancing and recursive functions to offload or replace existing DNS servers.

Authoritative DNS Cache

Thunder TPS can be used as a high-performance authoritative DNS cache. The solution’s non-stop DNS operational mode can cache millions of DNS records and respond to queries at millions of queries-per-second during a DNS DDoS attack. Through periodic DNS cache updates with one of the authoritative DNS servers, DNS queries are forwarded and responded to by Thunder TPS. Non-stop DNS can also work in conjunction with Thunder TPS DDoS defenses to create a highly resilient and a “non-stop” DNS service where the Thunder TPS mitigator scrubs all incoming DNS queries before sending them to the Thunder TPS authoritative DNS cache.

©2023 A10 Networks, Inc. All rights reserved.

Recursive DNS

DNS servers can be consolidated or eliminated with Thunder ADC or Thunder CFW, providing high-speed resolver and cache support while coexisting with current DNS features.

When used as DNS cache, Thunder ADC and Thunder CFW correctly identify and route DNS traffic, preventing other types of traffic from ever reaching DNS infrastructure. This shields DNS servers from attacks and reduces the number of DNS servers that need to be provisioned, lowering capital expenses.

Both Thunder ADC and Thunder CFW can also replace all or part of existing recursive DNS infrastructure.

DNS Load Balancing

Thunder ADC and Thunder CFW can load-balance multiple DNS servers and cache DNS responses, providing scale and enabling DNS servers to handle heavy loads and massive attacks. A10 Thunder can be deployed as an active standby high availability (HA) pair using A10's high-availability feature, VRRP-A. Moreover, with A10's DNS cache synchronization feature, DNS cache entries are synchronized between active and standby DNS load balancing nodes, further minimizing the impact on existing DNS sessions.

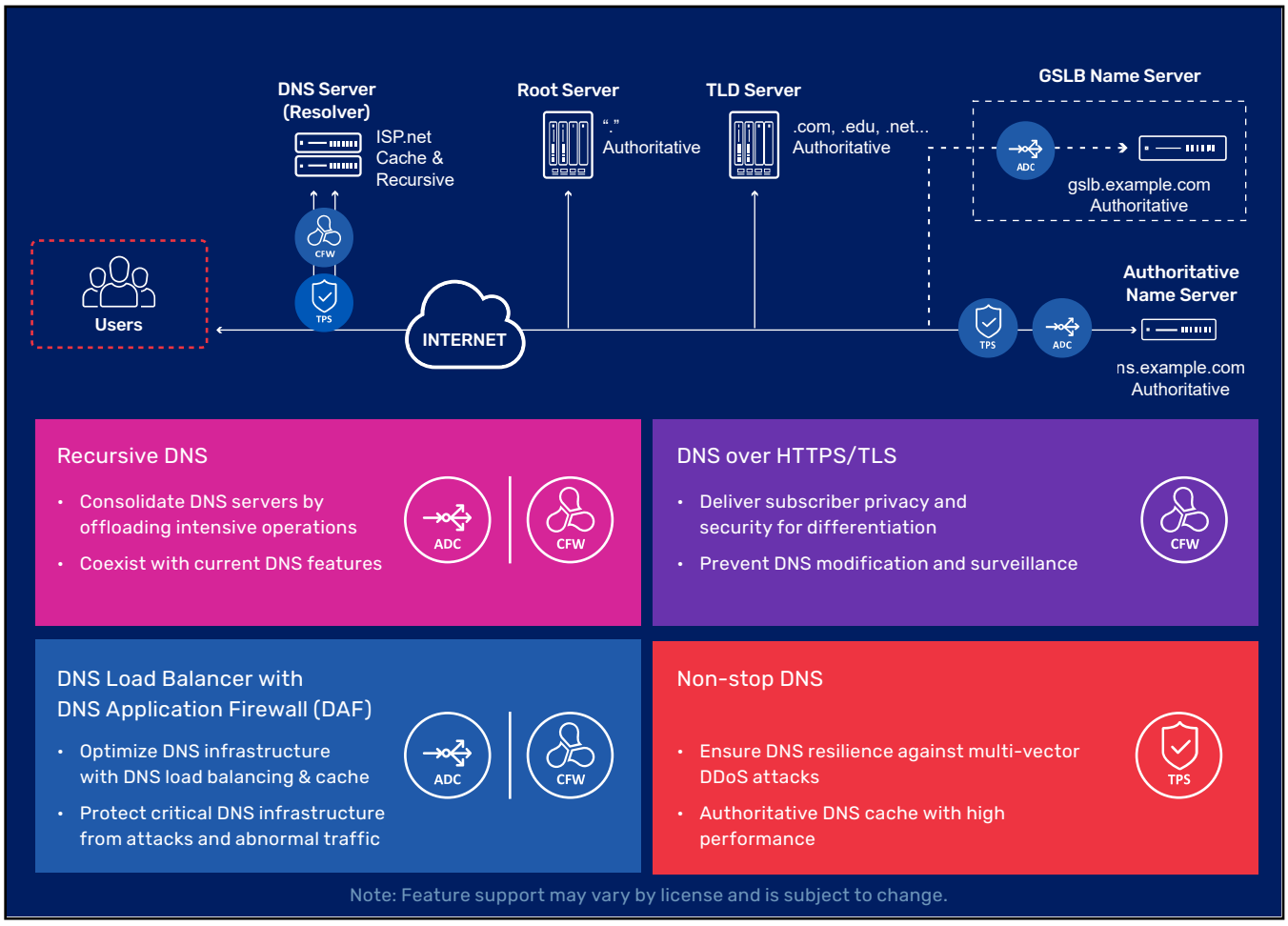

Figure 1: Comprehensive DNS protection with A10 DNS solution portfolio

©2023 A10 Networks, Inc. All rights reserved.

Features and Benefits of the A10 DNS Portfolio

The A10 DNS portfolio includes multiple solution components to enable enterprises and service providers to secure DNS infrastructure, protect network and service availability against DNS-related DDoS attacks and scale the DNS infrastructure more efficiently.

With the A10 DNS portfolio, service providers can:

- Prevent communication with C&C centers
- Shield critical DNS servers from direct DDoS attacks and exploits
- Avoid unwanted publicity and reputation damage by stopping DNS amplification attacks
- Shield critical DNS servers from direct DDoS attacks and exploits
- Avoid unwanted publicity and reputation damage by stopping DNS amplification attacks
- Outrun DNS attacks by scaling DNS infrastructure
- Reduce DNS server load for recursive look-up

Solution Components

Thunder CFW and Thunder ADC		Thunder TPS
DNS load balancing	DNS over HTTPS/TLS (DoH, DoT)	• Non-stop DNS - Authoritative DNS cache - DDoS mitigation and detection
DNS application firewall	DNS visibility in A10 Harmony® Controller	
Recursive DNS	Troubleshooting	

Comprehensive DNS Protection and High Availability

DNS is a critical component of the internet infrastructure, and thus it is important that DNS is always up and running to ensure normal network and business operations. DNS is, however, an inherently insecure protocol, and thereby vulnerable to a variety of attacks and vulnerabilities. As a result, an all-encompassing approach is required to secure DNS infrastructure and ensure constant availability and optimal performance.

The A10 DNS solution portfolio, including Thunder CFW, Thunder ADC, and Thunder TPS, with its comprehensive suite of DNS-related security features, provides such a solution. It enables service providers to upgrade and secure their DNS infrastructure while delivering a high-quality experience to the end users.

Next Steps

For more information, visit A10Networks.com or A10Networks.com/products/thunder-adc.

©2023 A10 Networks, Inc. All rights reserved.

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

©2023 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, Thunder, Harmony and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: **A10networks.com/a10trademarks**.

Part Number: A10-SB-19211-EN-01 July 2023