SOLUTION BRIEF

DNS Application Firewall

Thunder CFW and ADC Shield DNS Infrastructure from Attack and Optimize DNS Performance

Overview

Nearly every aspect of Internet communications — from browsing websites to sending email to transferring files — depends on domain name resolution from DNS servers. If an attacker disrupts access to a service provider's DNS servers, the attacker can essentially block the service provider's subscribers from accessing the Internet or completing voice over IP calls. Similarly, if an enterprise's DNS infrastructure fails, then Internet users will not be able to access the enterprise's web, mail and other critical services.

Besides knocking users offline, cybercriminals and hacktivists have discovered other nefarious uses for DNS servers. They can poison DNS servers' cache to redirect legitimate users to malicious sites. And they can exploit DNS servers to amplify the size of Distributed Denial of Service (DDoS) attacks. DNS amplification attacks can increase the size of DDoS attacks by orders of magnitude, providing an easy way for attackers to conduct large-scale DDoS assaults. Many of the largest DDoS attacks in recent years have been amplification attacks.

The A10 Networks® Thunder® Convergent Firewall (CFW) and Application Delivery Controller (ADC) provide a comprehensive and powerful defense against a multitude of DNS threats[1]. Thunder ADC and CFW are designed to handle process-intensive networking tasks, and with the Advanced Core Operating System (ACOS®), the solutions leverage a shared memory architecture and Flexible Traffic Accelerator (FTA) technology for exceptionally high performance.

[1] Licensing for Thunder CFW includes all functionality of Thunder ADC, including DNS Application Firewall.

Challenge

Attackers target DNS infrastructure to disrupt services and to transform DNS servers into weapons to unleash powerful DDoS attacks.

Solution

A10 Thunder ADC and CFW shield DNS infrastructure from attack with the powerful and comprehensive DNS Application Firewall.

Benefits

- Mitigate DDoS attacks targeting DNS servers
- Reduce the load on DNS servers up to 70% by dropping invalid traffic and caching DNS responses
- Maximize uptime with load balancing and high availability
- Scale to handle millions of DNS queries per second

The Challenge

Rising DNS Security Threats

DNS servers have gained the dubious distinction of becoming a top attack target for two reasons. First, taking DNS servers offline is an easy way for attackers to keep thousands or millions of Internet subscribers from accessing the Internet. If attackers incapacitate a service provider's DNS servers, they can prevent the service provider's 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. Both enterprise and service providers can suffer lost revenue and brand damage if an attacker disrupts access to DNS infrastructure and prevents users from accessing vital services.

Additionally, attackers can exploit DNS servers to amplify DDoS attacks. In the case of DNS reflection attacks, attackers spoof or impersonate the IP address of their real attack target. They send queries that instruct the DNS server to recursively query many DNS servers or to send large responses to the victim. As a result, powerful DNS servers drown the victim's network with DNS traffic.

Even when DNS servers are not the ultimate target of the attack, they can still suffer downtime and outages as the result of a DNS reflection attack. Organizations that host DNS servers must protect their DNS infrastructure.

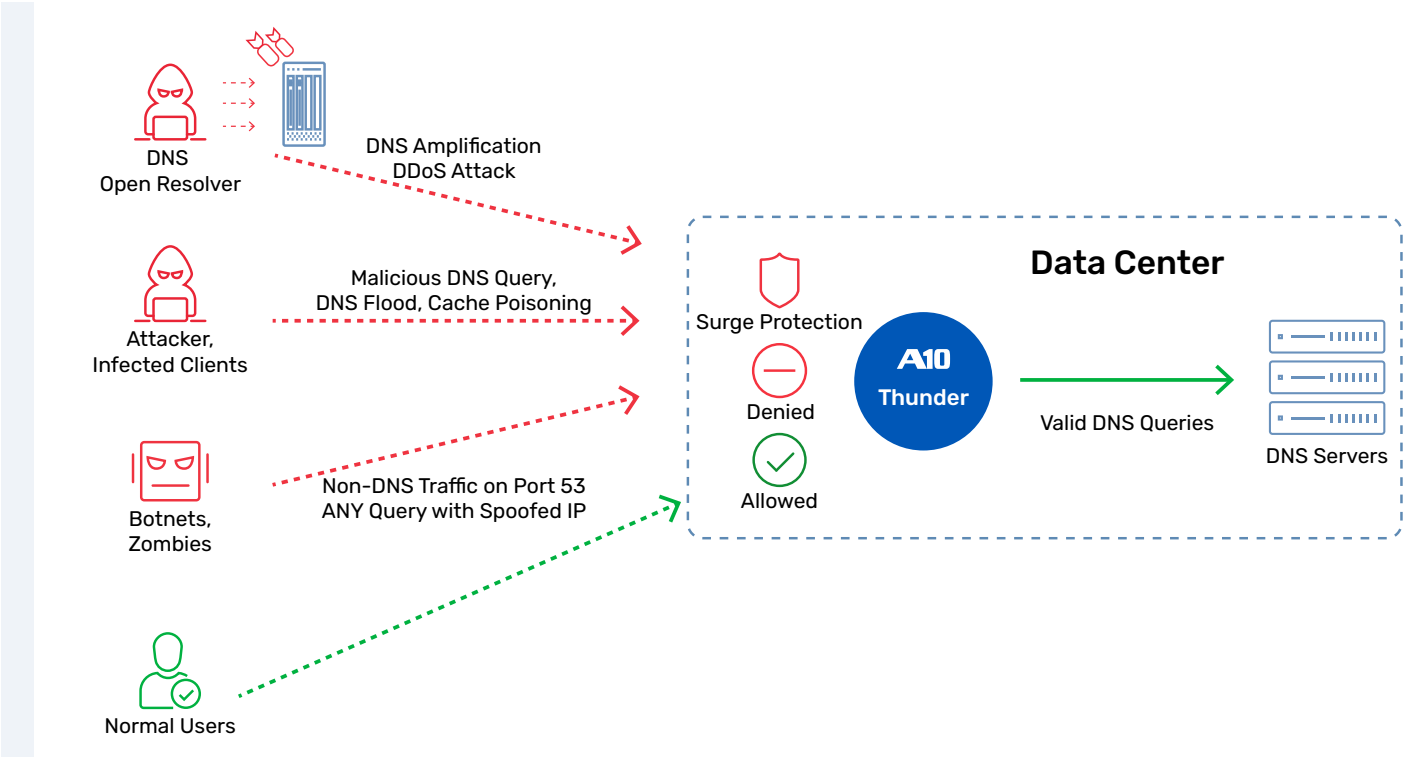

Figure 2: With a built-in DNS Application Firewall, Thunder CFW or ADC can detect attacks, non-DNS traffic and DNS queries from known malicious clients

The A10 Networks Thunder Solution

Whether the direct target of attack, the conduit for amplification attacks, or the inadvertent recipient of malformed requests, DNS servers are under fire. Few organizations have implemented security measures at the level needed to monitor or protect DNS servers from today's most sophisticated attacks, leaving DNS infrastructure wide open to attack.

To protect DNS servers, organizations need to deploy a DNS Application Firewall (DAF) that can mitigate a multitude of threat vectors and still deliver unmatched application performance. A10 Thunder ADC and CFW do just that: leveraging a Shared Memory Architecture and 64-bit scalability to provide ironclad protection at high speed.

As part of Thunder CFW and ADC, A10 Networks provides an integrated and powerful DNS Application Firewall. It stops buffer overflow, malformed requests and Denial of Service (DoS) attacks, shielding DNS servers from attack. In addition, because Thunder ADC can load balance multiple DNS servers and cache DNS responses, it also provides scale, enabling DNS servers to handle heavy loads and massive attacks.

Features and Benefits

With Thunder DNS Application Firewall, organizations can:

- **Shield critical DNS servers from direct attacks and exploits** — The DNS Application Firewall blocks malformed DNS requests, protecting DNS infrastructure from buffer overflow and DoS. In addition, IP-based connection rate limiting and concurrent connection controls mitigate DDoS attacks. With policy-based server load balancing (PBSLB), A10 can block requests from known malicious sources; customers can import lists of up to 8 million IP addresses to blacklist users or to grant access only to known trusted sources.
- **Prevent communication with C&C centers with DNS RPZ** — Malware-infected hosts typically contact command & control servers (C&C). Thunder CFW supports DNS RPZ to block communication with known malicious domain names, such as C&C centers, by rewriting DNS responses for such domains. For example, DNS RPZ can be used to rewrite a response for a domain to be NXDOMAIN, thereby effectively blocking access to that domain.
- **Avoid unwanted publicity and reputation damage by stopping DNS amplification attacks** — With attackers exploiting DNS servers to amplify DDoS attacks, organizations need to ensure that their servers won't become conduits for attack against other organizations. A10's DNS Application Firewall not only offers connection rate limiting, it can also throttle based on source IP address. "Virtually patch" DNS configuration flaws with advanced scripting – A10 Networks aFleX® deep packet inspection (DPI) scripting technology policies can transform DNS queries and responses to prevent specific types of attacks like DNS recursion. In addition, aFleX rules can be written to force specific types of DNS queries to revert to TCP, preventing IP spoofing attacks for traditionally connectionless UDP traffic.
- **Outrun DNS attacks by scaling DNS infrastructure** — With advanced server load balancing, customers can deploy multiple DNS servers to maximize availability and to increase capacity to withstand large-scale attacks. A10's powerful ACOS platform and high-speed shared memory architecture provides exceptionally fast performance.

- **Reduce DNS server load by up to 70% with caching and protocol validation** — Often, DNS servers are bombarded by non-DNS traffic. Using protocol checking and enforcement, Thunder ADC correctly identifies and routes DNS traffic, preventing other types of traffic from ever reaching DNS infrastructure. Besides shielding DNS servers from attacks, caching also reduces the number of DNS servers that need to be provisioned, lowering capital expenses.
- **DNSSEC** — Defined as a set of security extensions to the original DNS protocol, hardens DNS by signing DNS response data. This is useful in preventing attacks such as DNS cache poisoning and DNS hijacking. When deployed as GSLB (global server load balancing) authoritative name server, Thunder ADC can sign DNS records, enabling the client or the local DNS resolver to verify that the records have come from an authentic source and have not been modified.
- **Linearly scale performance to maximize capacity** — Because Thunder DNS Application Firewall features a shared memory architecture, it can take full advantage of multi-core processors. Besides increasing performance, it also improves rate limiting accuracy because processor cores have full visibility into all connection counts in real time.
- **Secure IPv4 and IPv6 DNS traffic** — Thunder DNS Application Firewall provides the same level of protection for both IPv4 and IPv6 communications protocols. Since Thunder ADC and CFW support IPv6 transition technologies, organizations can easily serve DNS requests, regardless of what IP version is used.

With its integrated DNS Application Firewall, Thunder ADC and CFW provides best-of-breed and comprehensive protection against DNS threats while increasing DNS application performance.

DNS Application Firewall Specifications

DNS DDoS Attack Defenses and DNS Server Offloading

- Connection rate limiting
- Source IP-based connection rate limiting
- Policy-Based Server Load Balancing (PBSLB) with black and white lists millions of IP addresses and thousands of subnets
- DNS authentication
- DNS RPZ
- aFleX policies to prevent vulnerability exploits
- Throttling based on domain name for specific names
- Maximum query length protection
- DNS caching
- DNS traffic load balancing

DNS DDoS Attacks Mitigated by Thunder ADC

- DNS ANY attack
- Malformed DNS query
- DNS amplification attacks
- Volumetric Layer 3 DDoS attacks — SYN flood, ICMP flood, UDP flood, Ping of Death, Smurf attack, LAND attack, fragmented packets

Summary — Protecting Your DNS Infrastructure with a DNS Application Firewall from A10

With increasing data center security threats, organizations need a solution that can safeguard their DNS infrastructure from attacks. As attacks evolve, security solutions must adapt and provide the raw horsepower to handle surges of traffic and ensure that business always run smoothly.

Organizations can rely on A10 to protect their DNS servers. Thunder DNS Application Firewall delivers a powerful defense against DDoS attacks, DNS cache poisoning and custom exploits. With its integrated load balancing, protocol validation and DNS caching, Thunder ADC and CFW can increase the overall capacity of DNS infrastructure. Trusted by thousands of organizations around the world, A10 makes sure that DNS servers are highly available, accelerated and secure.

Next Steps

To learn more about A10 Networks Thunder Application Delivery Controller (ADC) and Thunder Convergent Firewall (CFW), please contact your A10 Networks representative.

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-SB-19136-EN-04 July 2023