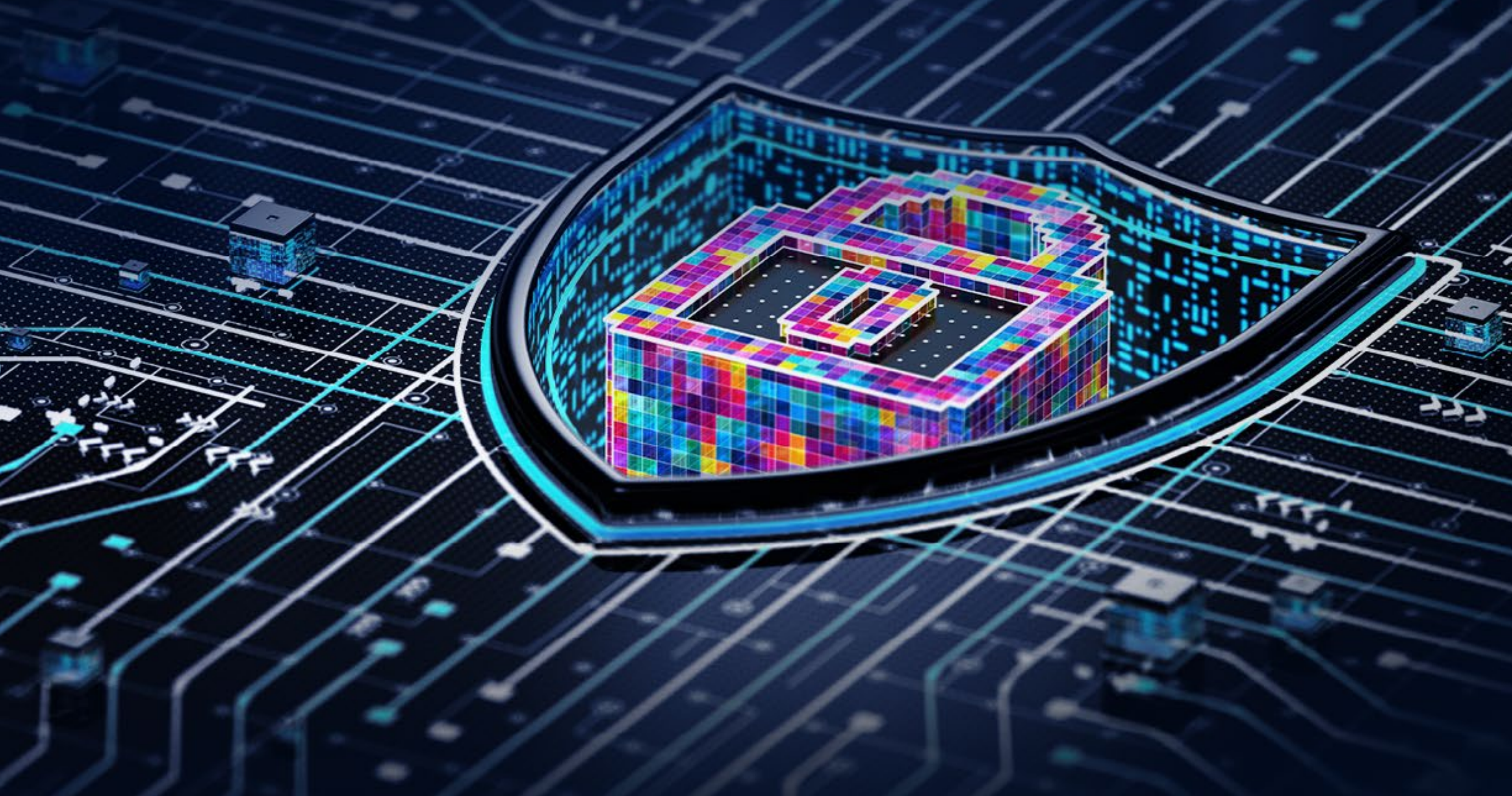
WHITE PAPER

Converging Performance, Security and Resilience with A10 Networks' Advanced DNS Solutions



Executive Summary

Organizations are increasingly adopting DNS solutions that integrate performance, security, and resilience to ensure fast, reliable, and secure access to applications—all while streamlining operational complexity. High performance is essential for delivering low-latency, globally optimized name resolution and intelligent traffic steering, which enhances user experience and application uptime. Security is the primary driver, as DNS serves as a frontline defense against threats such as phishing, malware, and DNS tunneling. It also supports Zero Trust architectures and compliance needs through features like DNSSEC and encrypted DNS. Resilience plays a vital role in maintaining business continuity during outages or DDoS attacks, leveraging distributed architectures and automated failover.

This document explores how A10's DNS solutions directly support these key drivers—helping organizations reduce risk, minimize downtime, and simplify operations—making DNS a strategic control point for both IT and security teams.

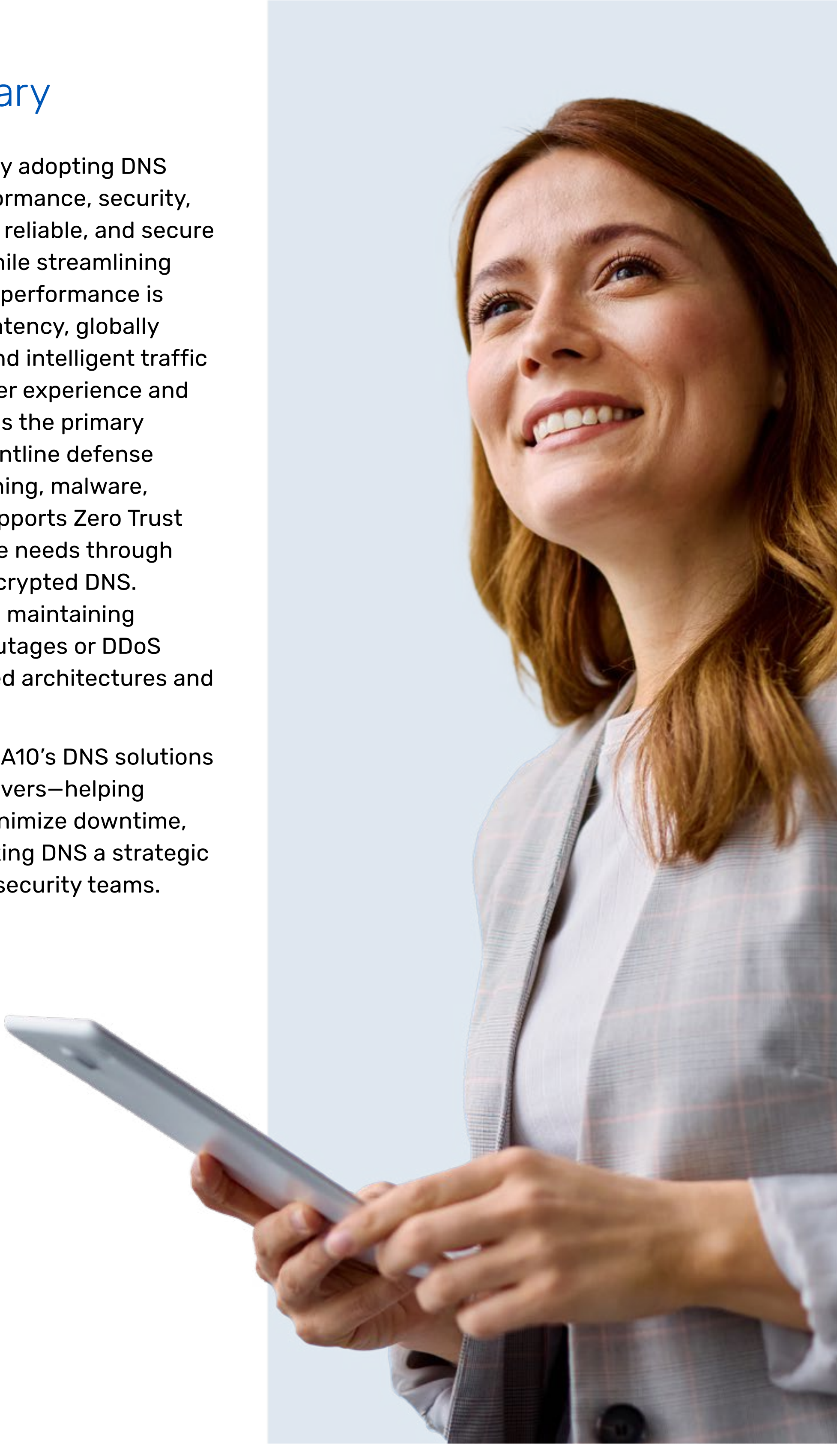


Table of Contents

Introduction

DNS is critically important for large service providers and enterprises. For organizations such as cloud platforms, telecom companies, or content delivery networks, DNS is a foundational component of their infrastructure. Efficient DNS traffic management ensures low latency, high availability, and seamless user experiences across global distributed networks. DNS facilitates traffic routing, ensuring users are directed to optimal server based on geo-location, latency and availability of services, which are essential for maintaining performance at scale. A10's application delivery controller (ADC) (Figure 1) is built with robust support for DNS. Ensure high performance, reliability and security for your DNS infrastructure.

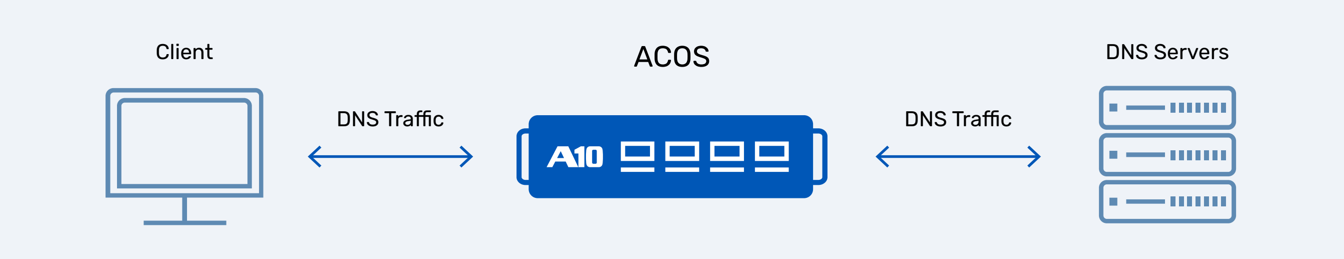


Figure 1. DNS Deployment and Feature Integration in A10 Thunder ADC

A10 Thunder ADC offers a comprehensive suite of DNS features

Advanced DNS protocol support:

A10 Thunder ADC supports DNS over UDP, TCP, TLS, HTTPS ensuring high performance, reliability, and security for DNS traffic.

Robust DNS protection:

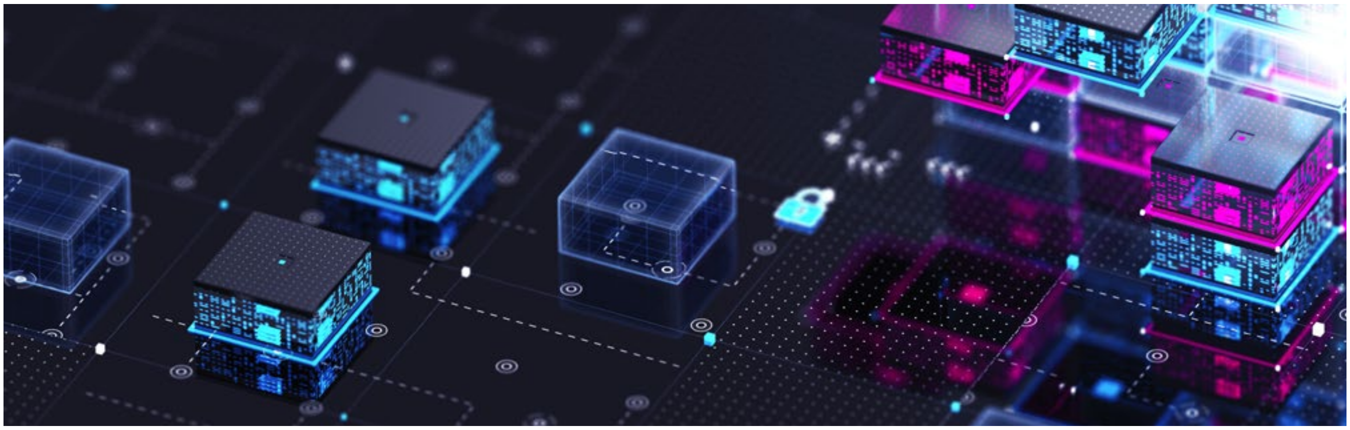
The integrated DNS firewall defends against DDoS attacks, cache poisoning, and malicious requests using rate limiting, DNS RPZ, DNS RRL, and deep packet inspection with aFleX scripting, supporting both IPv4 and IPv6.

Enhanced DNS caching and logging:

Thunder ADC provides intelligent DNS caching with TTL management, cache synchronization for failover, and detailed DNS logging for monitoring, security analysis, and compliance.

Traffic management:

Features like Layer 7 switching reduce DNS server load by up to 70 percent, while global server load balancing (GSLB) directs user traffic intelligently across data centers to enhance availability and performance without disrupting existing infrastructure.



1.0 – DNS Security

A10's DNS security features protect DNS infrastructure from a wide range of threats. They include a DNS firewall to block malicious queries, DNSSEC for response integrity, and response policy zones (RPZ) to prevent access to known malicious domains. Rate limiting, blacklisting, and protection against DNS amplification and reflection attacks ensure robust defense against both volumetric and stealthy threats. The following section looks in detail at the DNS security capabilities provided by A10 Thunder ADC.

1.1 – DNS Application Firewall

A10's DNS security features protect DNS infrastructure from a wide range of threats. They include a DNS firewall to block malicious queries, DNSSEC for response integrity, and response policy zones (RPZ) to prevent access to known malicious domains. Rate limiting, blacklisting, and protection against DNS amplification and reflection attacks ensure robust defense against both volumetric and stealthy threats. The following section looks in detail at the DNS security capabilities provided by A10 Thunder ADC.

Sanity Format Checks Thunder ADC inspects the syntax and format of incoming DNS queries and outgoing responses. It validates that DNS packets conform to protocol standards, preventing malformed or malicious requests from reaching backend DNS servers. This improves security posture by filtering out potentially harmful or non-compliant DNS traffic before it can cause disruption.

Connection Rate Limiting limits the rate of DNS queries based on the source IP address and DNS query name. Connection rate limiting will protect the DNS servers from being overwhelmed, ensuring service continuity and reducing the risk of volumetric attacks like DNS amplification.

Query Type and Class-based Filtering allow for filtering of DNS queries based on their type (e.g., A, AAAA, MX, ANY etc.) and class (e.g., IN for internet). This can be combined with aFlex scripting for advanced filtering and transformation of DNS traffic. Providing enhanced control over DNS traffic reduces exposure to attack vectors and ensures only relevant queries are processed.

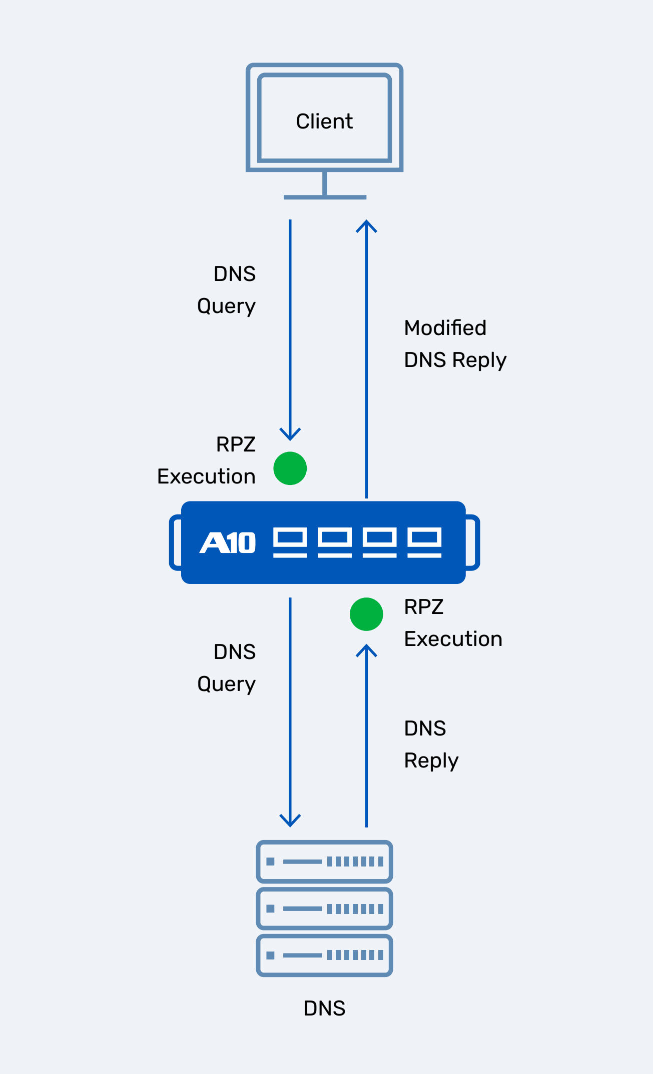


Figure 2. DNS Firewall Architecture with RPZ in A10 Thunder

Building on the foundational understanding of response policy zones and response rate limiting (RRL), this section explores, in detail, their internal workings, configuration options, and practical use cases. These features not only enhance DNS security but also provide administrators with fine-grained control over traffic behavior and threat mitigation.

1.2 – Response Policy Zone

The response policy zone is a DNS firewall mechanism originally developed for BIND and later standardized as an open specification. It enables DNS administrators to intervene in DNS resolution based on policy rules, allowing them to block, redirect or rewrite DNS responses to protect users from malicious or unwanted IP addresses or name servers. This feature helps to protect the recursive DNS servers, enterprise DNS resolvers and ISPs.

RPZ can perform several actions:

- **Protect clients:**
  prevents clients from resolving domain names known to host malware, phishing pages or botnet command-and-control servers.
- **Redirect to safe destination:**
  rewrite responses to point users to a safe landing page or warning site; prevents clients from accessing DNS information hosted by a known-bad name server.
- **Block known-bad clients:**
  RPZ can be configured to deny DNS service to clients identified as abusive or infected.

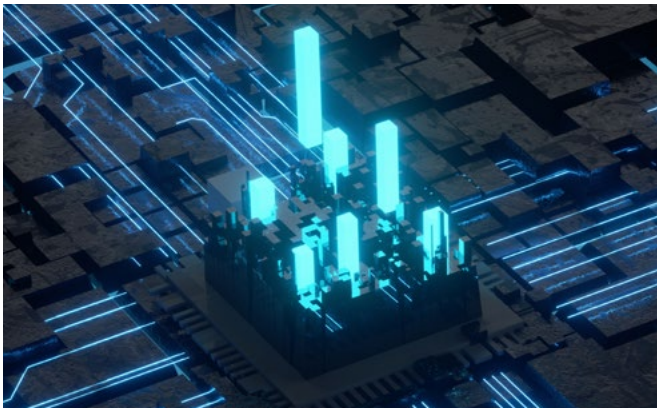
Administrators can import RPZ files from external sources or threat intelligence providers, with the option to securely transfer zone data using TSIG (Transaction Signature) to ensure integrity and authentication. Thunder ADC supports a range of response actions that includes DROP, MODIFY, RESPOND, NXDOMAIN etc., RPZ executions (Figure 2) are fully logged, enabling visibility into blocked or redirected queries and can be used for auditing, threat analysis and policy tuning. Thunder ADC supports up to 1.5 million RPZ entries, ensuring scalability for large enterprise and service providers.

1.3 – Response Rate Limiting

The response rate limiting (RRL) is a DNS security initially introduced in BIND to combat DNS amplification attacks, a common form of DDoS. These attacks exploit DNS resolvers to flood a target with amplified traffic (Figure 3). RRL mitigates this by throttling excessive identical responses, especially those triggered by malicious or repetitive queries, thus protecting ADNS servers and public facing DNS infrastructures. A10 Networks has implemented RRL in its Thunder ADC, extending support to both UDP-based DNS and DNS over HTTPS (DoH) queries.

Key capabilities of A10's RRL include:

- **Query rate limiting** Limits the number of identical DNS responses sent to the same client IP address within a defined time window; prevents attackers from exploiting DNS servers to generate large volumes of traffic toward a victim, thus helping maintain service availability during attack scenarios.
- **Client-side tracking** Tracks query behavior per client's IP and FQDN pair, allowing precise control over response rates; optimizes resource usage by focusing on client-side patterns, rather than global traffic volumes. This helps in reducing false positives by distinguishing between legitimate high-frequency users and abusive sources.
- **DNS-based DoS attack protection** Shields custom DNS servers from being used as amplifiers in reflection attacks; prevents attackers from leveraging Thunder ADC as a vector for flooding third-party targets, ensuring DNS services remain responsive and secure under high load conditions.
- **Configuration options** Thunder ADC offers various rate limiting options (Table 1).



Option	Why It Matters
Response rate	Controls how many responses per second are allowed per client, helping mitigate abuse like DNS amplification attacks.
Window	Defines the time span over which the response rate is calculated. A shorter window reacts quickly to bursts, while a longer one smooths traffic patterns.
Src-ip-only	Simplifies rate limiting by applying it solely based on source IP, treating all queries from a client equally regardless of query type or name.
Slip / slip-rate	Allows a fraction of responses to bypass rate limiting, ensuring that legitimate clients still receive occasional responses during throttling.
Match-subnet	Groups clients by subnet (e.g., /24) for rate limiting, which is useful in NAT environments where multiple users share a single IP.
Enable-log	Enables logging of rate-limited events, aiding in monitoring, diagnostics, and identifying abuse patterns.
Action	Specifies what happens when the rate limit is exceeded (e.g., drop, slip, truncate), giving administrators control over traffic handling.
rrl-class-list	Targets specific response types (like ANY or NXDOMAIN) for rate limiting, allowing fine-grained control without affecting normal traffic.

Table 1. Configuration Parameters for DNS Response Rate Limiting in Thunder ADC

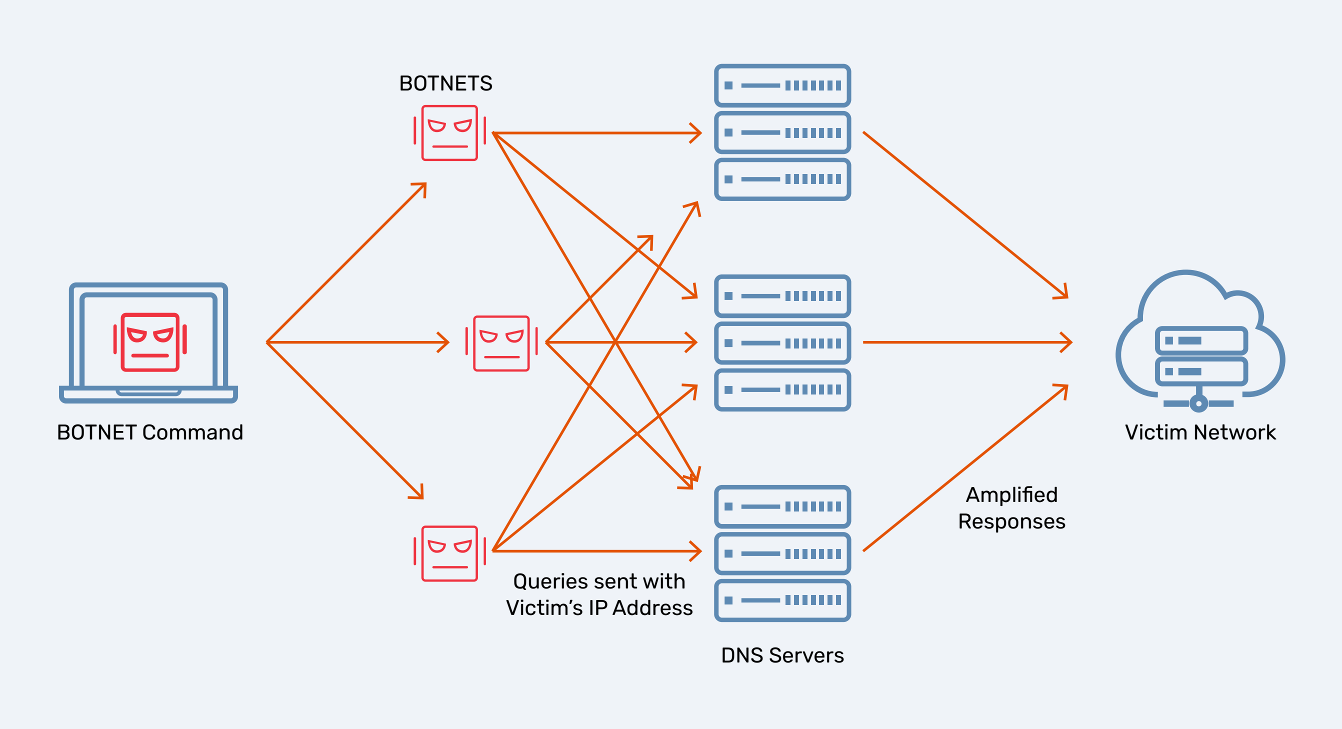


Figure 3. Operational Flow of DNS RRL

2.0 – Traffic Management

2.1 – Layer 7 Switching and Traffic Management

Layer 7 switching refers to traffic management at the application layer of the OSI model. In the context of DNS, A10 Thunder ADC uses Layer 7 intelligence to inspect and route DNS traffic based on specific query attributes, enabling fine-grained control, load balancing and security enforcement.

Here are the key aspects:

- **Query ID switching** distributes DNS traffic evenly across backend servers based on query ID/transaction ID included in DNS queries. Thunder ADC uses this ID to differentiate and distribute queries across service groups. This is effective for UDP traffic on port 53, where traditional load balancing based on source IP/port may be insufficient due to NAT or proxy behavior. Thus, it ensures balanced load distribution, prevents backend server overload and improves performance in high-volume DNS environment.
- **DNSSEC service group forwarding** ensures that DNSSEC queries are handled by servers capable of validating and signing DNSSEC responses. Thunder ADC checks if the request has OPT section and DO flags marked. These queries are forwarded to designated service groups configured for DNSSEC processing ensuring that DNSSEC validation is performed accurately and securely. This helps in maintaining DNS integrity and authenticity, compliance and prevents misrouting of DNSSEC traffic to non-compliant servers.
- **Malformed-query service group forwarding** helps to isolate and handle malformed or suspicious DNS queries without disrupting normal traffic. Thunder ADC inspects DNS queries for formatting anomalies, protocol violations or suspicious patterns. This helps enhance the security posture and helps support forensic analysis and threat detection.

2.2 – Global Server Load Balancing

Global server load balancing (GSLB) is a strategic feature in A10 Thunder ADC that enables intelligent traffic distribution across geographically dispersed data centers (Figure 4). It ensures high availability, performance, optimization and disaster recovery by dynamically directing user requests to the most appropriate data center based on real-time metrics.

Key features and functionalities of GSLB:

- **Data center failover and continuity** GSLB monitors the health and availability of data centers in the event of a failure (e.g., network outage, server downtime). Traffic is automatically redirected to a healthy site, ensuring uninterrupted service delivery and business continuity.
- **Optimization for multi-site deployments** GSLB uses geographic proximity and network performance metrics (e.g., latency, packet loss) to determine the best site for each user. This ensures users are connected to the nearest or fastest data center, improving web performance and user experience. Policy metrics include geo-location of client IP, network latency and availability, server load and response time.
- **Support for DNS proxy and DNS server modes** Thunder ADC acts as an intermediatory, forwarding DNS queries to backend DNS servers and applying GLSB logic. In the server mode, ADC functions as an authoritative DNS server, directly responding to queries with GSLB-optimized answers. This dual-mode support allows integration into diverse DNS architectures.
- **Synchronization of GSLB configuration and data** GSLB configurations and runtime data (e.g., health checks, metrics) are synchronized across controller groups deployed in different regions. This ensures consistency, redundancy and real-time decision-making across all sites.
- **Support for DNSSEC serving** When configured as an authoritative DNS server, Thunder ADC supports DNSSEC, ensuring authenticity of DNS responses, protection against cache poisoning and spoofing. The signing and validation of DNSSEC are integrated into GSLB responses for secure resolution.

The accompanying diagram illustrates the global distribution of data centers across Europe, the U.S., and the APAC region, highlighting the widespread implementation of GSLB.

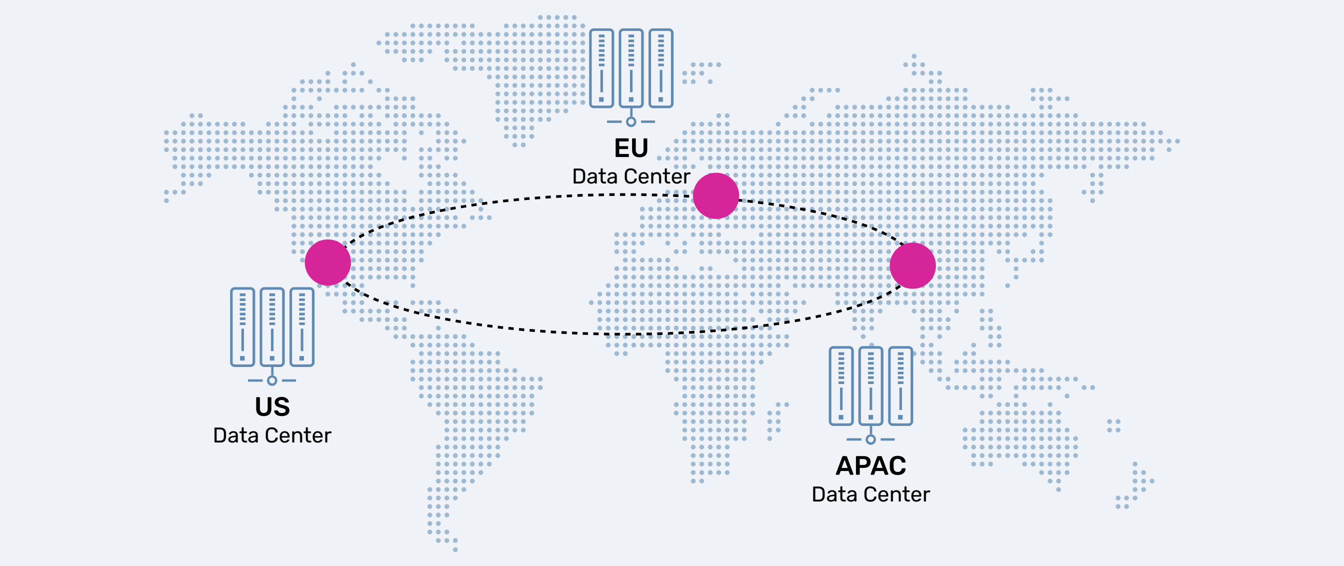


Figure 4. Global Server Load Balancing Across Distributed Data Centers

3.0 – DNS Infrastructure Optimization and Logging

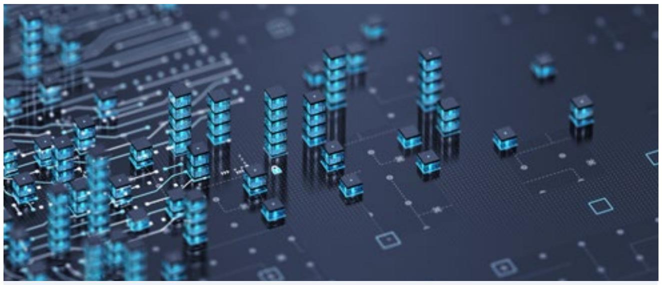
A10 optimizes DNS infrastructure by leveraging high-performance architecture and caching to reduce resource usage and costs for service providers using the recursive resolver solution. Additionally, A10 provides granular DNS logging and monitoring through customizable templates, protocol-specific logging (TCP/UDP), and integration with tools. Let's explore these topics in greater detail.

3.1 – DNS Recursive Resolver

The DNS recursive resolver is a fundamental component of DNS infrastructure that resolves domain names to IP address by querying a hierarchy of DNS servers. In A10 Thunder ADC, this resolver is enhanced with intelligent caching, adaptive forwarding and selective resolution policies to optimize performance and reliability.

- **Functionality**
  The resolver begins by querying public root DNS servers or other configured. It parses referral responses to identify the next authoritative name server in the resolution chain. This process is repeated until a final answer (IP address) is obtained for the queried domain. Responses are then cached to accelerate further queries and reduce upstream traffic.
- **Thunder ADC as a recursive resolver**
  Thunder ADC acts as a DNS recursive resolver especially in scenarios where none of the backend servers in the configured service groups are available and the response from a backend server lacks a valid or complete answer. In such cases, Thunder ADC initiates its own resolution process, starting from root servers or cached NS records.

  Customization and caching
  Administrators can replace default public root servers with custom IP addresses, such as internal DNS servers or private root zones. This allows for controlled resolution paths and integration with enterprise DNS architectures. Thunder ADC caches name server records, enabling it to identify and query name servers closer to the authoritative source. This reduces resolution latency and improves efficiency. The recursive resolution can also be applied selectively to specific domain names.
- **Adaptive query forwarding**
  Thunder ADC supports adaptive forwarding logic to optimize DNS traffic flow. By default, Thunder ADC performs recursive resolution to serve client queries efficiently. If a query matches a specified hostname or domain pattern, it can be forwarded to a designated service group. This enables policy-based routing of DNS queries for performance, security or compliance.



The Thunder ADC recursive resolver ensures DNS resolution even when a backend server fails. Caching and NS optimization reduce query latency to improve performance.

Custom root servers and selective recursion support diverse DNS architectures, thus providing flexibility. The adaptive forwarding enables intelligent routing of DNS queries having more traffic control.

3.2 – DNS Cache

The DNS cache feature in Thunder ADC (Advanced Core Operating System) is designed to enhance the performance and efficiency of DNS servers by caching DNS responses. Thunder ADC can serve repeated queries faster and more reliably.

Here are the key points:

- **Caching DNS responses** Thunder ADC stores DNS responses from backend servers in its local memory. When a client sends a query for a previously resolved domain (FQDN), the cached responses are served directly. This reduces latency for end users, the load on backend DNS servers and network traffic between ADC and upstream DNS infrastructure.
- **Time to live (TTL)** Each cached DNS entry includes a TTL value, which defines how long the entry remains valid. Thunder ADC allows customization of TTL values, enabling administrators to balance between freshness of DNS data and performance through longer caching. When the TTL expires, the entry is purged or refreshed via a new query. The TTL can be adjusted dynamically based on policy or traffic patterns.
- **Cache weighting** Thunder ADC supports cache weighting, a mechanism to prioritize cache entries. Lower-weighted entries are removed first when cache memory reaches capacity. This ensures that high-value or frequently accessed entries remain in cache longer.
- **Negative response caching** Thunder ADC also caches negative responses (e.g., NSDOMAIN, NODATA). This prevents repeated queries for non-existent domains, improving efficiency and reducing unnecessary backend load. This ensures faster response for invalid queries and reduce DNS traffic for typo or malicious domain.
- **Persistent storage** Cached DNS entries are stored persistently, meaning they survive device reboots. Upon restart, Thunder ADC reloads the cache, avoiding cold start delays and maintaining continuity. This provides consistent performance across maintenance cycles and reduces downtime impact on DNS resolutions.
- **Global DNS cache synchronization** In a high availability setup, DNS cache entries are synchronized to a standby device, ensuring that the standby device can immediately serve DNS queries from cache during failover, providing seamless continuity of DNS service without performance degradation during failover events.

3.3 – DNS Logging

The DNS logging feature in Thunder ADC (Advanced Core Operating System) provides comprehensive visibility into DNS traffic by capturing detailed logs for DNS queries and responses. This includes traffic processed by Thunder ADC itself – from DNS cache, GSLB, RPZ – making it a powerful tool for monitoring, troubleshooting and security auditing.

- **Logging support** Thunder ADC supports per query/response DNS logging. This includes client-originated queries, responses such as those from DNS cache responses, GSLB-optimized responses, and RPZ-filtered or rewritten responses, providing full visibility into how DNS queries are processed and resolved.
- **Remote log server** DNS logs are sent to a remote log server ensuring centralized log collection for compliance, security monitoring and performance analysis. The support protocol for log transmission is TCP, UDP or both.
- **Logging options** There are various options (Table 2) for logging, including:

Logging Option	Choices	Explanation
Type	Query, response, both	Choose whether to log incoming DNS queries, outgoing responses, or both.
Protocol	TCP, UDP, both	Select the transport protocol used to send logs to the remote log server.
Request Section	Header, question, all	Specify which parts of the DNS request to log: just the header, the question section, or the entire request.
Response Section	Header, answer, all	Specify which parts of the DNS response to log: just the header, the answer section, or the entire response.
RDATA Field Length Limiting	Applicable to TXT, RRSIG, DNSKEY	Limits the length of the RDATA field for specific record types to control log size and prevent excessive data.

Table 2. DNS Logging Configuration Options in Thunder ADC

Conclusion

Customers can leverage A10's comprehensive DNS features to enhance scalability, performance, and security across enterprise and service provider environments.

A10 remains committed to expanding its DNS offerings, delivering a unified solution that combines robust DNS management, intelligent traffic handling, and advanced security.

A10 Thunder ADC DNS solution simplifies operations, strengthens security, and improves application delivery. To learn more about how A10's DNS solution can be a cost-effective alternative to complex or fragmented DNS systems, contact sales.

About A10 Networks

A10 Networks provides security and infrastructure solutions for on-premises, hybrid cloud, and edge-cloud environments. Our 7000+ customers span global large enterprises and communications, cloud and web service providers who must provide business-critical applications and networks that are secure, available, and efficient. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally.

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

About A10

A10Networks.com

Contact Us
A10Networks.com/contact

Part Number: A10-WP-21173-EN-01 Oct 2025