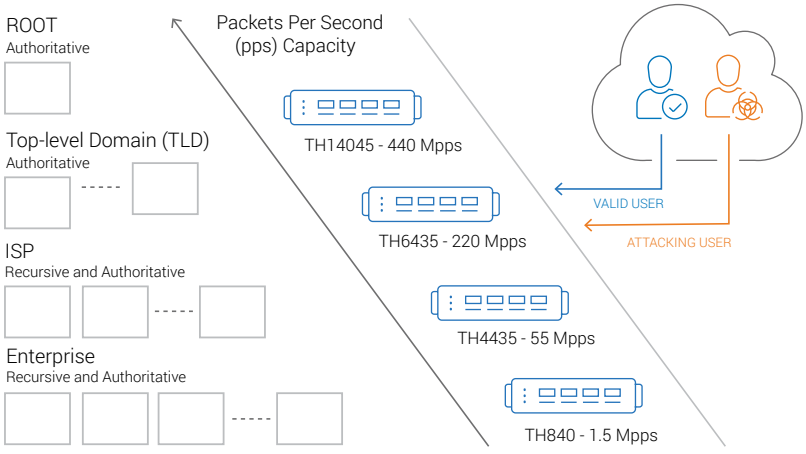
SOLUTION BRIEF

ENSURE DNS RESILIENCE AGAINST MULTI-VECTOR DDOS ATTACKS

PROTECT CRITICAL DNS INFRASTRUCTURE

The Domain Name System (DNS) is the critical infrastructure that service providers and enterprises depend on for their users to smoothly navigate the internet. Recent headlines of crushing distributed denial of service (DDoS) attacks targeting websites and infrastructure are creating greater awareness around the criticality of DNS for reliable internet services and the catastrophic effects of DNS outages. Network operators must take an active role in applying adequate defenses to build DDoS resilience into their DNS infrastructure or suffer the inevitable consequences.

THUNDER TPS SCALES TO PROTECT DNS INFRASTRUCTURE AT ANY SCALE



CHALLENGE

DNS is the critical infrastructure that all users depend on to navigate the internet. DNS is one of the most common targets of nefarious actors to interrupt business operations.

SOLUTION

A10 Thunder® TPS® is a surgical multi-vector DDoS protection solution that ensures availability of business services at any scale. It's available in a wide range of form factors that make economic sense for businesses.

BENEFITS

- Ensure DNS resilience with surgical precision against multi-vector DDoS attacks
- Scale to terabit defenses to protect the most challenging DNS environments
- Automatically learn peacetime traffic behavior
- Increase effectiveness of frontline defenders with automated mitigation escalation during wartime
- Simplify integration into SecOps orchestration with an open API

THE DNS THREAT LANDSCAPE

Generating DDoS attacks against DNS infrastructure is remarkably simple. Just like a legitimate user, the attackers send queries to name servers across the internet and those name servers return responses. The trouble begins when the attackers apply scale utilizing sprawling botnets to overwhelm DNS services.

The challenge for DNS defenses in distinguishing legitimate users from attacking agents to block nefarious activity and ensure smooth operation.

- DNS servers are subject to general network flooding and resource-exhaustion protocol attacks
- Attackers exploit DNS-specific functionality and vulnerabilities
- Attackers can easily spoof source IPs due to UDP-based transport mechanisms
- Complexity of DNS response creates opportunities for attackers
- Attackers leverage amplification attacks due to significant disparity in DNS query-to-response sizes
- DNS is subject to reflection attacks utilizing millions of unsecured open DNS resolvers

ATTACK STRATEGIES

FLOOD

DNS services are run on servers with networking functionality and, as a result, are subject to general network flooding attacks like malformed packets, User Datagram Protocol (UDP) packets to random ports, Transmission Control Protocol (TCP) SYN floods and other resource-exhaustion attacks. Attackers leverage botnets to create large scale of irrelevant network functions or high rates of malicious DNS queries that tie up the server from servicing legitimate users.

SPOOFING

Spoofing DNS queries is particularly easy because they are usually carried over connectionless UDP. Instead of sending the queries from their own IP addresses, attacking agents send DNS queries from arbitrary IP addresses to help hide the attack and make it more effective and scalable.

THE DDOS OF THINGS

As a result of weaponized vulnerable and persistent Internet of Things (IoT) devices, attacks can now originate from an even broader base of distributed agents. Attacking IoT agents flood DNS servers with bogus traffic, causing the server to exhaust all of its resources serving attacker requests and degrades its ability to service legitimate users recursion and authoritative functions.

DNS REFLECTION AMPLIFICATION

Reflection leverages spoofing the target's IP address. Attackers make numerous spoofed requests to globally distributed open DNS resolver servers on the internet to flood the victim's authoritative servers. To maximize the impact, reflection attacks leverage DNS protocol amplification capabilities to create very large responses.

RANDOM QUERY NAMES

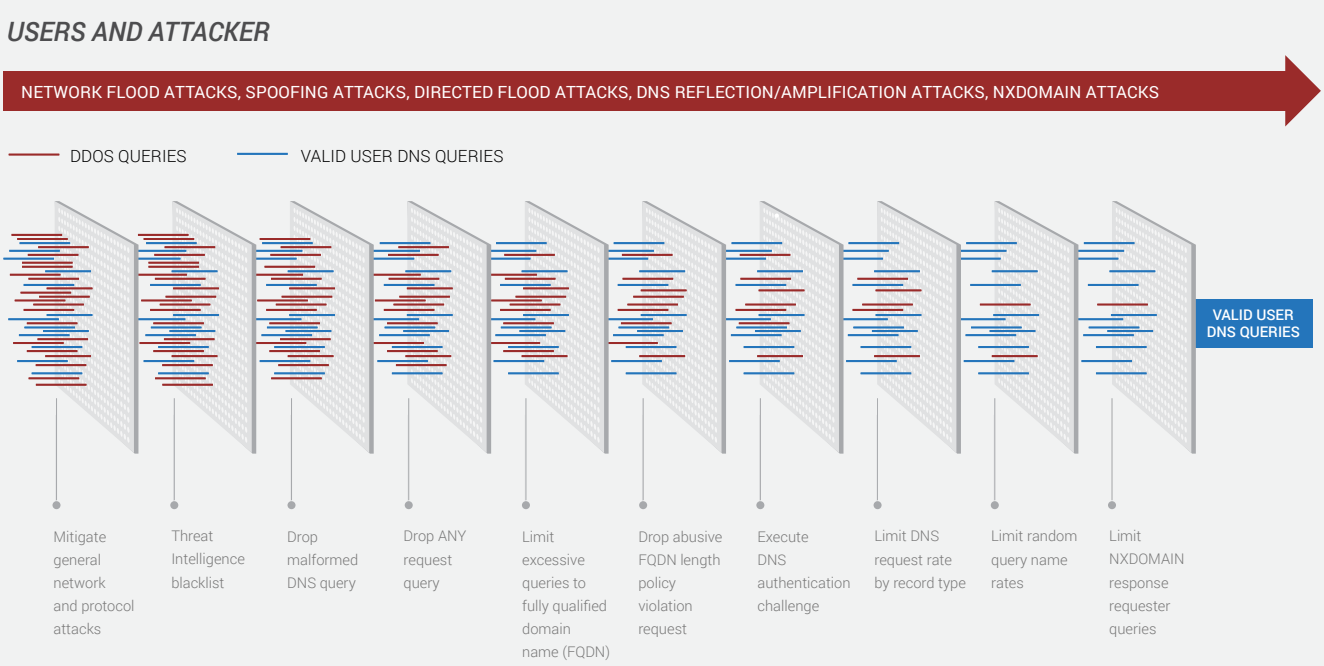
Random query name attacks make DNS queries to invalid or non-existing domains. The DNS server spends significant resources searching for records that don't exist, rather than leveraging fast-access cached responses. Additionally, performance is degraded as the cache is filled with useless data.

HOW IT WORKS

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 that include source based rate limiting, authentication challenges, block abusive requests, blacklisting and more.

Thunder TPS provides extensive customization capabilities from the graphical user interface, command line interface (CLI) or over open API. This gives defenders the ability to create customized defenses to ensure DNS services are resilient to targeted multi-vector DDoS attacks.

THUNDER TPS DNS DDOS DEFENSES



THUNDER TPS DNS DEFENSE COMPONENTS

A10 Thunder TPS provides detection and mitigation for both general network attacks and DNS-specific attack vectors.

GENERAL DNS SERVER MITIGATION

- General counter measures to protect DNS server farms
- L3/L4 packet anomaly detetion
- Source based filtering and limits
- Invalid and malformed packet detection
- TCP/UDP/DNS authentication challenges
- Destination-based filtering and limits
- Peacetime behavioral learning and baselining
- Five-level programmatic automatic mitigation escalation against learned baseline thresholds
- Integrated threat intelligence to block known malicious sources

DNS-SPECIFIC MITIGATION

- Drop malformed query
  - Basic
  - Extended
- Drop ANY request query
  - Restrict costly queries with limited practical utility
- Drop abusive FQDN length policy violation requests
  - At any suffix position
  - Beginning at specific suffix position
- Limit excessive queries to fully qualified domain name (FQDN)
  - Per source IP
  - Specify how many labels of the FQDN to evaluate (up to ten labels)
- Limit DNS request rate by record type
  - Defends against sophisticated attacks
- Limit NXDOMAIN response requester queries
- Limit destination query rate
  - Prevent overwhelming the server
- Execute DNS query authentication challenges per source IP
  - Force retry with time limit
  - Truncated reply with force to TCP

These mitigation capabilities thwart DNS DDoS attacks including amplification, Land, Water Torture and Phantom Domain attacks. These are among the most common and problematic types of DNS attacks. They are particularly effective against DNS services.

PROGRAMMATIC AUTOMATIC MITIGATION ESCALATION

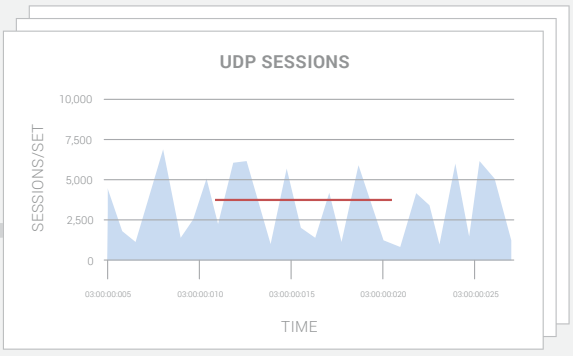
No organization has unlimited trained personnel or resources during the chaos of wartime under attack. Thunder TPS supports five levels of programmatic mitigation escalation and de-escalation against learned peacetime baselines per protected zone and service. Administrators can create custom policies for each protected service and Thunder TPS will automatically apply the required mitigations at each escalation level. This removes the need for frontline personnel to make time-consuming manual changes and improves response times during attacks.

Administrators have the option to manually intervene at any stage of an attack.

EXAMPLE DNS DEFENSE MITIGATION ESCALATION POLICY

	TRACKED INDICTORS	*MITIGATION APPLIED*	*ACTION*
LEVEL 4 – WARTIME Final Countermeasure	Continue tracking indicators Zone threshold 4	BGP black hole signaling Administrator manual intervention All level 3 mitigations	Create custom regular expression Create custom Berkley Packet Filter
LEVEL 3 – WARTIME Increase Countermeasures	Continue tracking indicators Zone threshold 3	DNS-udp-authentication-force-tcp Dst-rate-limit-request All level 2 mitigations	Challenge Drop Destination rate limit Blacklist source
LEVEL 2 – WARTIME Increase Countermeasures	Continue tracking indicators Zone threshold 2	DNS-udp-authentication-force-retry Malformed-DNS-query-check-extended Src-rate-limit-by-request-type All level 1 mitigations	Challenge Drop Source query type rate limit Blacklist source
LEVEL 1 – WARTIME Add Countermeasures	Continue tracking indicators Zone threshold 1	Malformed-DNS-query-check-basic DNS-any-check FQDN-label-length FQDN-rate-limit-domain-name-suffix FQDN-label-count All level 0 mitigations	Drop FQDN check Source rate limit Blacklist source
LEVEL 0 – PEACETIME Establish Baseline, Minimum Countermeasures	TCP-conn-miss-rate TCP-pkt-drop-ratio TCP-syn-rate TCP-src-threshold TCP-zone-threshold UDP-pkt-drop-ratio UDP-pkt-rate UDP-src-threshold UDP-zone-threshold	FTA L3/L4 packet anomaly check	Drop

TRACK 27+ INDICATORS FOR AUTOMATED ESCALATION AND DE-ESCALATION



Establish Protected Services Behavioral Baseline

FEATURES AND BENEFITS

- Multi-vector DDoS attack protection
- Surgical precision in differentiating real users from botnets by tracking 27-plus traffic behavioral indicators
- Granular source and destination pair per connection rate protection
- Fast response, down to 200 ms detection and mitigation interval
- Scales to 300 Gbps, 440 Mpps and 128 million concurrent tracked sessions in a single appliance
- 100 percent API programmable policy engine for easy automated orchestration integration
- Easy network integration for on-demand reactive deployments and L2/L3 proactive deployment with integrated BPG, OSPF, IS-IS routing.

NEXT STEPS

To learn more about the A10 Thunder TPS, please contact your A10 representative or visit: a10networks.com/products/thunder-series/ddos-detection-protection-mitigation

SUMMARY

New threat vectors have changed the breadth, intensity and complexity of options available to attackers. Established solutions, which rely on ineffective, signature-based IPS or only traffic rate-limiting, are no longer adequate. A10 Thunder TPS offers the scalability and precision to defeat the most challenging DNS-based attacks to make your DNS infrastructure resilient against DDoS attacks.

Unlike outdated DDoS products, Thunder TPS is built on A10's market-proven Advanced Core Operating System (ACOS®) platform, which delivers scalable form factors and cost structures that makes economic sense with a complete mitigation, detection and reporting solution.

A10 provides 24x7x365 support and includes the A10 DDoS Incident Security Response Team (DSIRT) to help you analyze and respond to DDoS incidents and attacks. The A10 Threat Intelligence Service leverages global knowledge to proactively stop known bad actors.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) is a Secure Application Services™ company, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com or tweet @a10Networks.

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19175-EN-02 SEP 2017