



DNS Protection: DNS Amplification Mitigation



Solution Brief

AX Series New Generation Server Load Balancer

Attacks on Critical Services

As the Internet has evolved, so have the attacks on its infrastructure. Each piece of critical infrastructure used by a typical user must be secured. Sporadic outages of key services can damage reputations and consumer confidence, and are thus not tolerated. Outage of the critical DNS (Domain Name System), used to resolve friendly domain names to IP addresses, is no exception.

Exploits take many forms, from Denial of Service to DNS Cache Poisoning. Recent DDoS (Distributed Denial of Service) attacks demonstrate the protocol-specific nature of the issue and ever evolving techniques. For example, a large provider recently experienced an unusually sustained variant of the DNS Amplification attack as follows:

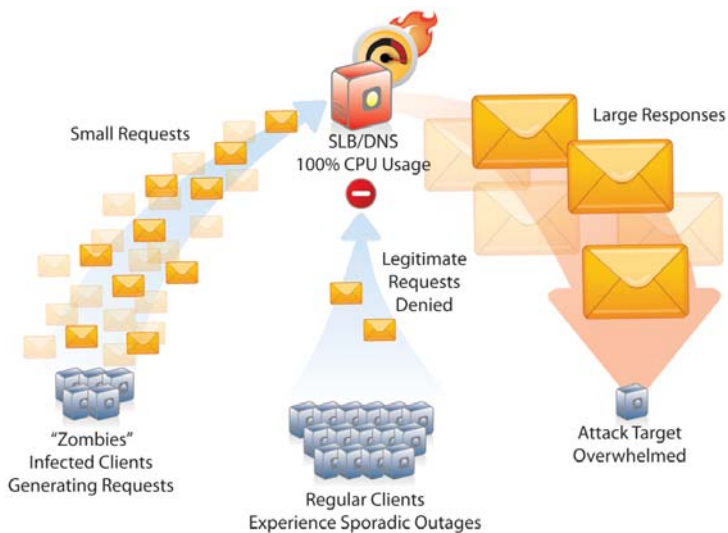
- ▶ DNS using UDP (typically port 53/UDP)
- ▶ NS (Name Server) query for "." (a single dot)
- ▶ Spoofed IP address (to redirect to an intended target)

As the attack was targeted at DNS, which is almost exclusively a UDP based protocol, it evaded typical DDoS SYN flood protection, making seemingly valid requests of the DNS server. However, the result of this had potentially two targets: The unsuspecting holder of the IP address being spoofed, as well as the provider's DNS infrastructure.

First, the real IP address holder of the spoofed IP address can be overwhelmed, as the "hijacked" machines acting as traffic generators for the DNS queries inform the DNS server that the spoofed machine is the requester. Second, and potentially more importantly, the DNS server itself is vulnerable to an outage. With the high volume of requests for data, the DNS server CPU and the server load balancers that precede it can become over taxed, as well as the network itself.

This is known as a DNS Amplification attack, as a small request is sent to the server and a larger set of data is sent out. For a generic example, if a hacker sends a 5 k request, and is able to generate a 20 k return, he or she has amplified the initial packet by 4 times.

This, multiplied by many hijacked machines acting as "zombies" (also known as a botnet), can create outages of major consequence. The latest attack draws upon previous attacks from a few years ago,



DNS Amplification Attack

but differs in a critical aspect, as DNS servers allowing non-recursive queries are now vulnerable.

A10 offers a range of mitigation technologies to deal with DNS Amplification attacks, and other similar attack types, ensuring availability of service for legitimate users. This allows whole classes of attacks to be mitigated, not just the current attack of the day.

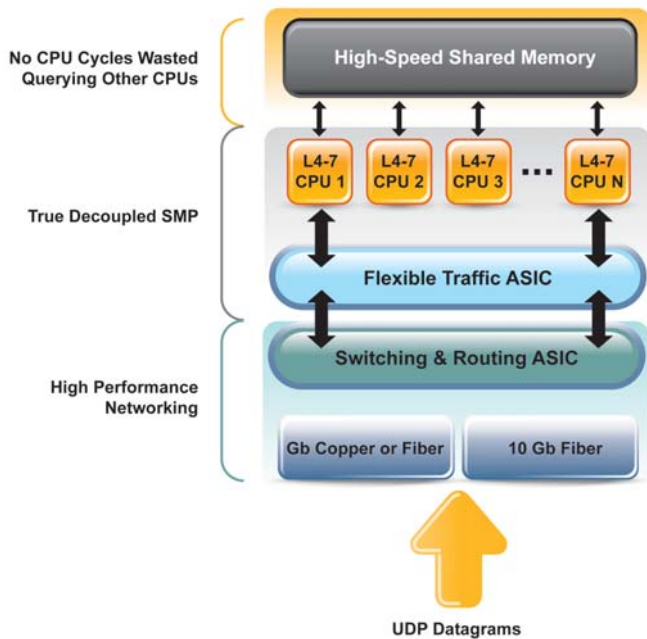
Mitigation Methods

Infrastructure changes, such as requiring all users to change DNS servers, are not options. Thus the ability to service requests as well as rate and connection limiting are critical.

- ▶ High Performance: In a recent DNS Amplification attack, a competitor's load balancer spiked from 12% to 100% load. Upon replacement with A10's AX Series, the average load on the AX CPUs was 4-5%, increasing to only 20% when under attack. This is due to A10's Advanced Core Operating System (ACOS) architecture that leverages a Flexible Traffic ASIC to intelligently manage and distribute traffic to multiple cores in a true decoupled architecture. ACOS also includes a high performance enabling shared memory architecture.
- ▶ Source-IP Based Connection Rate Limiting: Protects the system

Solution Brief

from excessive connection requests from individual clients. Importantly, the AX architecture employs shared memory for this task. Each CPU core can access any needed IP connection rate data instantly. This improves efficiency by eliminating the requirement to contact another processor for data, as some competitors' products do. This feature can be enabled on a global basis and applies to any server load balancer (SLB) virtual port.



AX Architecture

Optimized for High Volume Inspection Such as Source-IP Based Rate Limiting

- ▶ Policy Based Server Load Balancing (PBSLB): With black/white lists containing up to 8 million individual host addresses and up to 10,000 subnet addresses, PBSLB is highly scalable to block known bad or selected IP addresses or subnets.
 - » Sets connection threshold for the client address to drop excessive connection requests.
 - » Enables service group ID for specified client addresses that can be mapped to a service group, dropped, or reset.
- ▶ Connection Limiting: Sets a maximum number of connections allowed to the service port. If the connection limit is exceeded, the AX device stops sending new connections to the service port. The AX device resumes sending connections to the service port when the number of connections on the port is at or below the configurable Connection Resume threshold.

- ▶ Connection Rate Limiting: Limits the rate of new connections the AX device is allowed to send to ports. When a port reaches its connection rate limit, the AX device stops selecting the port for client requests. This limit is also configurable. For example, the threshold can be set to over a million connections and the sampling rate can be set to 100 milliseconds or 1 second.

Granular DNS rate limiting is implemented in A10's ACOS software to do per source IP rate limiting. This feature can apply to a single Virtual IP (VIP), or to all VIPs. Once exceeded, the available options are:

- ▶ Discard packet
- ▶ Log
- ▶ Lockout for "x" seconds
- ▶ Plus other policy options

In a subsequent release, A10 will add significant policy based enhancements.

AX Platform: Hardware and Software Synergy

A10's AX Series new generation server load balancers are specifically built for processor intensive high volume networking tasks. The AX Series includes the Advanced Core Operating System (ACOS), which integrates Symmetrical Multi Processing (SMP) with modern multi-core, multi-threaded software to provide significant performance advantages.

The use of hardware and software as appropriate are especially valuable for load balancing. For example, the Flexible Traffic ASIC exponentially optimizes multi-core systems (as well as completely off-loading the CPU from TCP based/SYN flood based DDoS attacks) so the load balanced servers are protected, and the server load balancer can still pass traffic as intended.

Another specific advantage for high speed DNS protection is the use of shared memory among all the processors within the AX platform. This ensures the CPUs are decoupled, and do not need to waste cycles querying each other, allowing the AX more CPU cycles to attend to more requests.

As attacks evolve, availability is critical, ensuring front end devices can handle traffic volume through a multi-layered approach of checks and balances. The end result is network availability so that business always runs smoothly.