MITIGATE DDoS ATTACKS AND TRAFFIC SURGES WITH THUNDER ADC

Importance of Server Responsiveness

Application servers must be available all of the time. Customers will not tolerate slow and unresponsive websites. Application disruption and downtime can lead to lost revenues, brand damage, and customer turnover.

Traffic spikes can be caused by unusual events, such as product launches, or by malicious attacks. To successfully manage traffic spikes, organizations should deploy high-performance application networking equipment with built-in security and rate controls.

A10 Networks® Thunder® ADC line of Application Delivery Controllers are designed to protect server farms by effectively controlling the total connection limit and the rate of new connections, despite overwhelming traffic or malicious attacks from users.

Effective Connection Control

A tiered approach to session validation needs to be implemented with multiple check points and methods, all performing at high speeds. Valid connection requests may occur due to extraordinary traffic, such as huge spikes in Web traffic during the online holiday shopping season. In addition to huge legitimate traffic, there can be malicious attacks that make a website unreachable or unresponsive to legitimate traffic. Protections against malicious traffic are available in the Thunder ADC to ensure site availability and performance:

- **DDoS**: The Thunder ADC protects against Distributed Denial of Service (DDoS) attacks at an industry leading data rate. An example of a DDoS attack is the SYN flood attack. The SYN flood attack sends half open TCP connection requests faster than a machine can process them, which can cripple a network.

  To effectively stop these attacks, DDoS protection is built into the Thunder ADC platform. The Thunder ADC is designed to handle high volume DDoS attacks, allowing legitimate application traffic to be serviced without interruption. Several Thunder ADC models include the Flexible Traffic ASIC that can handle millions of SYN flood attacks per second with 0% additional load on the CPU utilization.
- **Policy Based Server Load Balancing (PBSLB):** Enables 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.

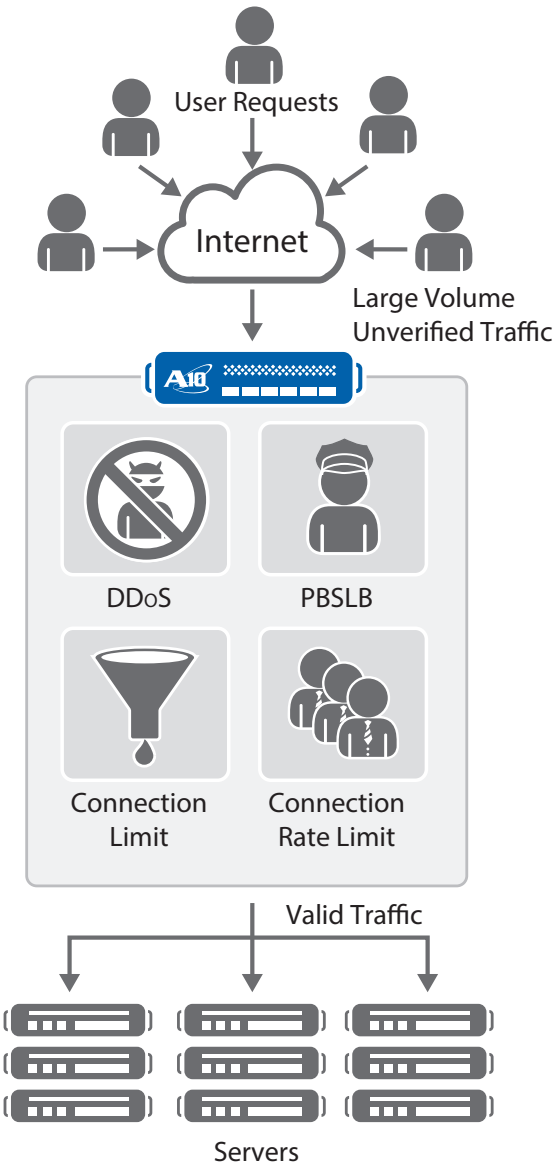

Figure 1: Thunder ADC uses multiple layers of defense to control traffic and block attacks

- 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.

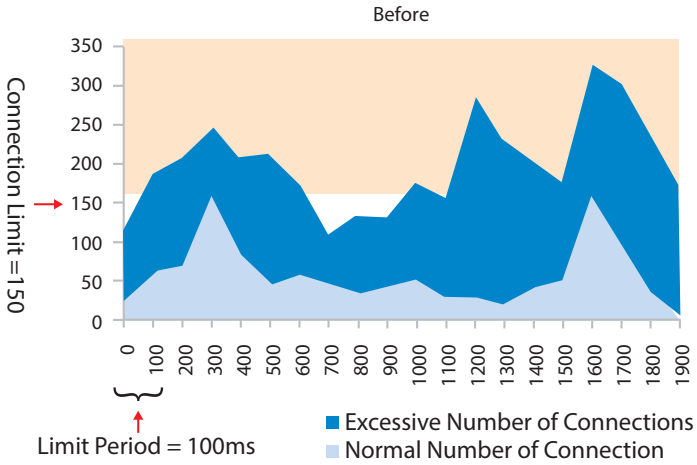

Figure 2: Normal vs. excessive connection requests

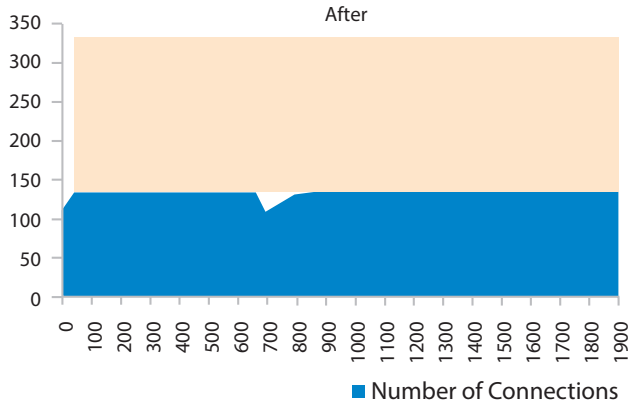

Figure 3: No excessive connection requests with source-IP based connection rate limit

- **Connection Limit:** Set a maximum number of concurrent connections allowed to the service port. If the connection limit is exceeded, the Thunder ADC device stops sending new connections to the service port. The Thunder ADC 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 Limit:** Sets the rate of new connections the Thunder ADC is allowed to send to servers during a time interval.
  - Source-IP Based Connection Rate Limit: Protects the system from excessive connection requests from individual clients. This feature can be enabled on a global basis. The feature applies only to SLB virtual ports.

A10 Thunder ADC Platform: Hardware and Software Synergy

A10 Thunder ADC is specifically built for processor intensive high volume networking tasks. The Thunder ADC is powered by A10's purpose-built Advanced Core Operating System (ACOS®), which integrates modern multi-core, multi-threaded software to provide significant performance advantages.

Typical multiprocessing appliances with distributed memory have significant challenges for any task that requires aggregation of data among multiple cores. The typical method to collect the data among multiple cores is Inter-Process Communication (IPC). IPC can introduce millisecond delays that prevent users from receiving real-time, accurate data. The more cores an appliance has, the longer the delays it will have with IPC data aggregation.

The Thunder ADC deploys shared memory, together with ACOS technology to enable effective enforcement of rate limiting and connection limits. Thunder ADC architecture provides the flexibility to implement any future security enhancement without sacrificing performance.

Next Steps

To learn more about A10 Networks products and solutions, please contact your A10 representative or visit www.a10networks.com.

About A10 Networks

A10 Networks is a leader in application networking, 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, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-SB-19143-EN-01
June 2015

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
Hong Kong
HongKong@a10networks.com
South Asia
SouthAsia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.