



Solution Brief

AX Series New Generation Server Load Balancer

Importance of Server Responsiveness

Server availability to fulfill requests and responsiveness to clients are essential for computing transactions, especially for Web-based transactions. Outages are not tolerated and 99.999% uptime expectations are now normal.

Traffic spikes in the form of malicious attacks or legitimate traffic peaks are common. Solutions to ensure computing resources are available despite overwhelming traffic conditions are now viewed as essential to the network infrastructure.

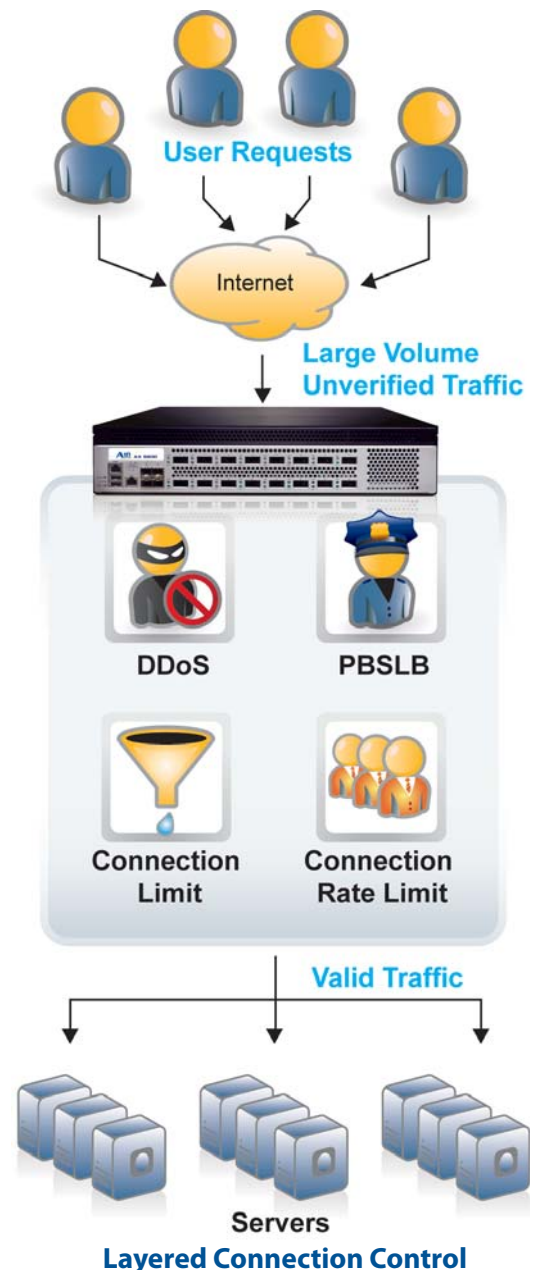
The AX Series new generation Application Delivery Controllers are designed to protect server farms by effectively controlling the total connection limit and the rate of new connections, despite overwhelming traffic or malicious attacks from users.

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 AX to ensure site availability and performance:

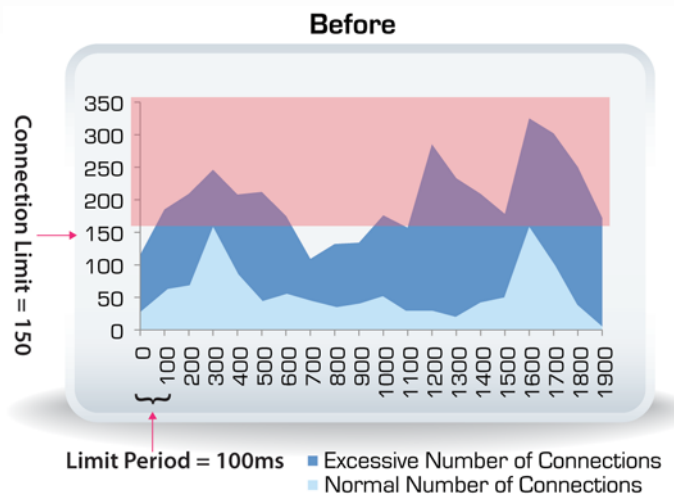
- ▶ DDoS: The AX Series protects against Distributed Denial of Service (DDoS) attacks at an industry leading data rate. An example of a DDoS attack is the SYN flood attack. The SYN flood attack sends half open TCP connection requests faster than a machine can process them, which can cripple a network.

To effectively stop these attacks, DDoS protection is built into the AX platform. The AX Series is designed to handle high volume DDoS attacks, allowing legitimate application traffic to be serviced without interruption. Several AX models include the Flexible Traffic ASIC that can handle millions of SYN flood attacks per second with 0% additional load on the CPU utilization.

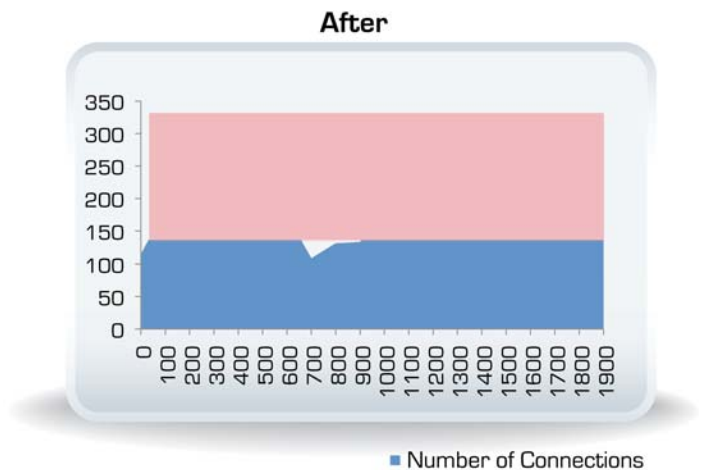


Solution Brief

- ▶ 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.
 - » 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 Limit: Set a maximum number of concurrent 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.
 - » 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.



Normal vs. Excessive Connection Requests



No Excessive Connection Requests With Source-IP Based Connection Rate Limit

AX Platform: Hardware and Software Synergy

A10's AX Series is specifically built for processor intensive high volume networking tasks. The AX Series includes the 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 AX Series deploys shared memory, together with ACOS technology to enable effective enforcement of rate limiting and connection limits. The AX architecture provides the flexibility to implement any future security enhancement without sacrificing performance.

To find out more, please contact A10 Networks.