

Solution Brief

Load Balancing to Provide Scalable, Reliable, Secure Access Solutions

September 2008



Mobile Users Require Secure Always-On Network Access

Secure Sockets Layer (SSL) virtual private networks (VPNs) have become the de facto standard technology for remote access to enterprise network resources. SSL VPN has attained widespread adoption as a low-cost, more easily configured and managed alternative to cumbersome, cost-inefficient IPsec solutions.

With SSL VPN, employees, partners, and vendors can easily and securely access the enterprise network from remote locations, without the need to install or maintain special software. Evolution of the technology over the last several years has yielded mature, highly configurable solutions such as Juniper Networks Secure Access.

Success Brings New Challenges

The success of SSL VPN has created its own challenges. As organizations continue to deploy the technology, the user base accordingly continues to grow. Organizations are faced with the need to scale deployed SSL VPN solutions to meet ever increasing demand, while at the same time maintaining the availability, robustness, and ease of use of the solution. Similar scalability and reliability challenges confront organizations wishing to deploy new SSL VPN solutions. To address the challenges facing legacy and greenfield global SSL VPN deployments, robust, reliable, high performance load balancing is required.

Juniper Networks Secure Access and A10 Networks AX Series Provide a Robust, Scalable Solution

A combined solution using Juniper Networks Secure Access and A10 Networks AX Series provides optimal SSL VPN service. The access and security features of Secure Access are easily extended to a quickly expanding mobile workforce by deploying AX Series server load balancers.

AX Series load balancers add the following benefits to a Secure Access solution:

- Intelligent, flexible load balancing algorithms to select the best Secure Access node for each session
- Industry leading connection speed, supporting greater than 500,000 new TCP connections per second¹
- Customizable health monitors to ensure service availability
- Stickiness options, such as persistence based on client source IP address
- Hardware-based protection against Distributed Denial-of-Service (DDoS) attacks
- One virtual VPN server to provide a single point of access for all users in all locations
- High Availability AX redundancy with session synchronization to eliminate single point of failure

Protect Return on Investment

Organizations with existing Secure Access deployments can protect return on investment and meet increasing demand by adding A10 Networks AX Series server load balancers. Likewise, organizations deploying new SSL VPN solutions can take advantage of the many benefits of the combined solution to meet present needs, with assurance that the solution will scale to meet tomorrow's needs.

AX Series devices can be inserted into the network as Layer 2 "transparent" switches or Layer 3 routers that can support RIP and OSPF. In either case, Layer 4-7 features are supported.

Combine Ease of Use with Scalability and Reliability

Users benefit from ease of use while network administrators benefit from increased robustness and availability of SSL VPN access. Regardless of the location or size of Secure Access clusters, users can access the enterprise network using a common URL. The URL maps to a virtual IP address managed by AX Series server load balancers.

¹ The actual number is 541,000 new TCP connections per second on model AX 3200, as independently verified by A10's January 08 Tolly Test.

AX load balancing uses health checks to ensure the availability of Secure Access nodes before sending user traffic. If a Secure Access node is unavailable, the AX selects another Secure Access node to serve the user's connection. All this is transparent to the user. The user simply experiences fast, reliable access.

AX Series devices deployed in High Availability sets provide an added layer of reliability. In the event an AX device or links become unavailable, the other AX device in the set takes over to provide continued service. Session synchronization ensures that existing client sessions continue uninterrupted.

Global SSL VPN Load Balancing for Anywhere, Anytime Access

Today's highly mobile, geographically dispersed workforce requires consistent, uncomplicated network access. A superior SSL VPN solution relieves users of the burden of remembering multiple URLs. Users should be able to log in from anywhere using a single, easily remembered (or cached) URL.

Global server load balancing (GSLB) enables a seamless access solution. Users can request network access using the same URL from any geographic location. An AX Series device running GSLB selects the best site for the request and modifies the DNS to direct the user the chosen site.

SSL VPN Solution Architecture

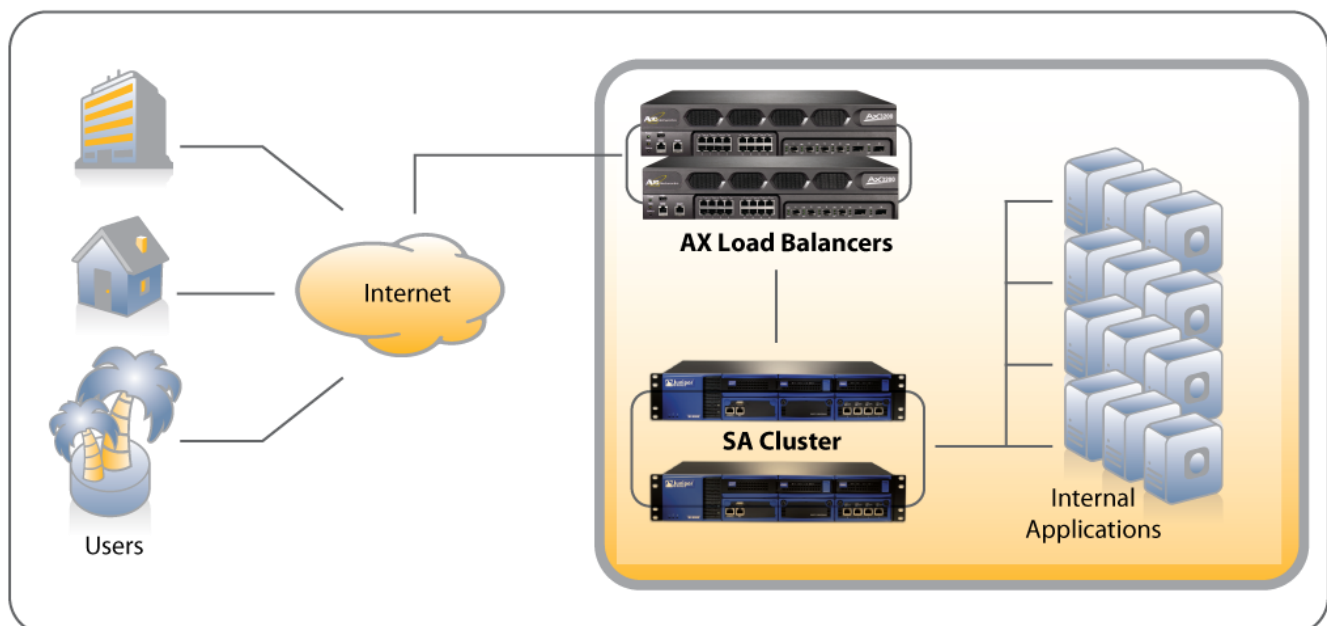
To manage multiple Secure Access clusters, deploy a set of AX Series server load balancers configured for GSLB.

AX Series and Secure Access Cluster

AX Series server load balancers can intelligently balance traffic among multiple Secure Access nodes while presenting a single, virtual URL to users. Mobile users can access the VPN from anywhere with a single URL (for example, vpn.corp.com) mapped to a single virtual IP (VIP). To service a connection request, AX Series load balancers assess the health and session load on each Secure Access node, then select a Secure Access node for the user session based on this information.

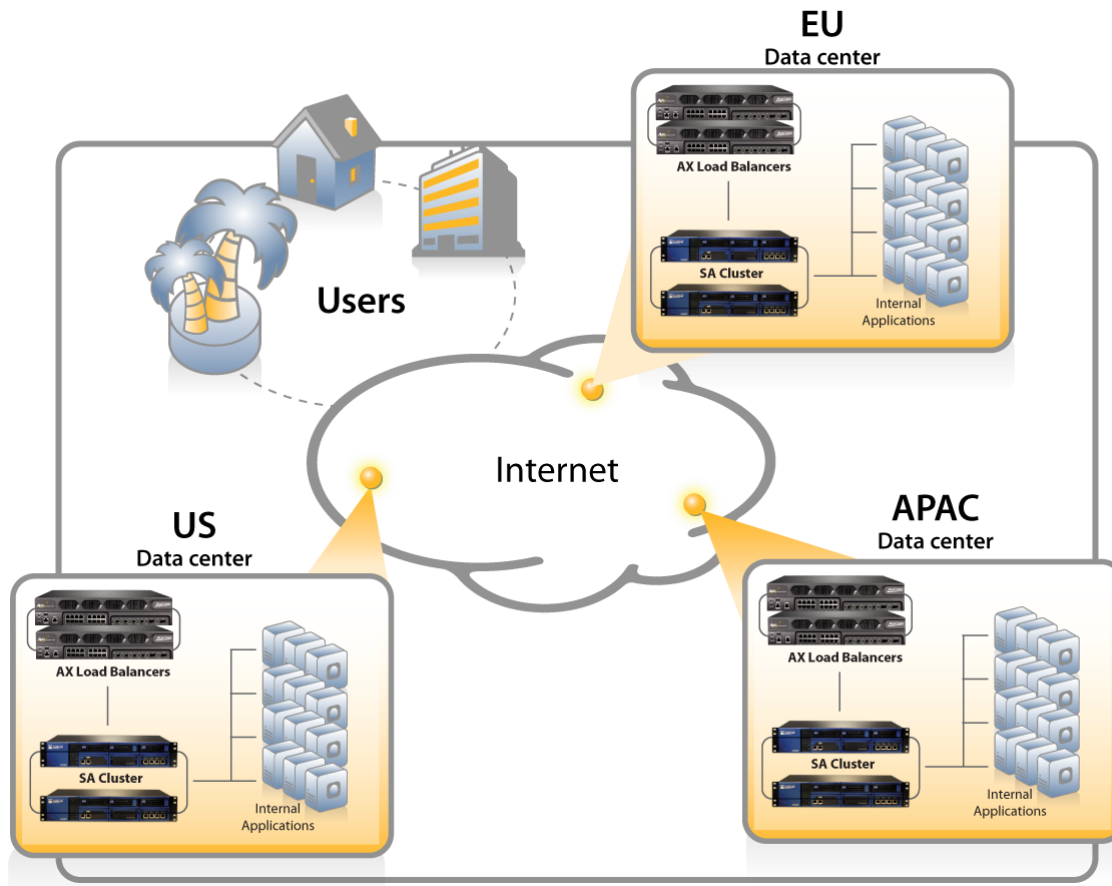
Stickiness features such as source-IP persistence can be used to keep a given user on the same Secure Access node, even across multiple sessions, so long as that node is available.

Robust hardware-driven AX security features such as hardware-based SYN cookies can supplement the advanced security features of Secure Access, easily dismissing up to 9 million TCP-SYN attacks per second.



Global AX Series Managing Multiple Secure Access Clusters

An AX Series server load balancer configured for GSLB manipulates DNS replies to choose the best site for each user. The AX Series device can determine the best site based on a set of configurable metrics, including the user's geographic location, capacity at each site, and the health of the Secure Access nodes.



Summary

The SSL VPN solution consisting of Juniper Networks Secure Access and A10 Networks AX Series provides the industry's most reliable and scalable Secure Access solution. New and existing SSL VPN deployments alike can benefit from AX Series features including configurable health monitors, flexible load balancing, persistence ("stickiness") options, and High Availability. Hardware-based DDoS protection detects and drops unfriendly TCP traffic while allowing legitimate user traffic to the Secure Access nodes. High Availability eliminates service interruption due to AX or link unavailability. GSLB provides additional flexibility and ease of use, enabling a single user access experience across multiple sites, regardless of user location, while transparently directing the user to the best site based on site health, user location, and other configurable metrics.

AX Series server load balancers allow Secure Access deployments to scale in support of today's mobile workforce. Tomorrow's ever-increasing numbers of users, running increasingly bandwidth intensive applications, continue to enjoy fast, reliable Secured Access without the need to manage and utilize multiple URLs due to user location or network load.



A10 Networks was founded in 2004 with a mission to provide innovative networking and security solutions. A10 Networks makes high-performance products that help organizations of all sizes accelerate, optimize and secure their applications. A10 Networks is a venture-funded, privately held, Silicon Valley-based technology company, with offices in the United States, Japan, China, Korea and Taiwan. For more information, visit www.a10networks.com.



Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high performance businesses. Additional information can be found at www.juniper.net.

Contact Information

Corporate Headquarters

A10 Networks, Inc.
2309 Bering Drive
San Jose, CA 95131
USA

Website

<http://www.a10networks.com>

A10 Sales

N. America: +1-888-A10-6363
sales@a10networks.com

International: +1-408-325-8616
sales@a10networks.com

China: +86 10 8515-0698
china_sales@a10networks.com

APAC: +886-2-2657-3198
apac_sales@a10networks.com