

# LOAD BALANCING PULSE SECURE SSL VPN DEPLOYMENTS

Provide Scalable, Reliable and Secure Remote Access

## Challenge:

Remote users require secure and uninterrupted access to corporate resources.

## Solution:

A10 Thunder ADC load balances Pulse Connect Secure deployments for High Availability and to increase overall SSL VPN capacity.

## Benefits:

- Maximize uptime and scale with best-in-class load balancing and clustering
- Detect network or service failures with advanced health monitoring
- Extend secure remote access to a wide array of PC and smart device OS platforms
- Lower total cost of ownership (TCO) by using a single SSL VPN client across various desktops and mobile devices



## Mobile Users Require Secure Always-On Network Access

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

With SSL VPN deployments, 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 Pulse Connect Secure (formerly 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 continues to grow accordingly. Organizations are faced with the need to scale SSL VPN deployments 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.

## Pulse Connect Secure SSL VPN and A10 Thunder Series Provide a Robust, Scalable Solution

A combined solution using Pulse Connect Secure and A10 Networks® Thunder™ ADC line of high-performance, next-generation application delivery controllers provides optimal SSL VPN service. The access and security features of Pulse Connect Secure are easily extended to a quickly expanding mobile workforce by deploying Thunder ADC.

Thunder ADC adds the following benefits to a Pulse Connect Secure solution:

- Intelligent, flexible load-balancing algorithms to select the best Pulse Connect Secure node for each session
- Industry-leading connection speed
- 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 (HA) with session synchronization to eliminate single point of failure

## Protect Return on Investment

Organizations with existing Connect Secure deployments can protect return on investment and meet increasing demand by adding Thunder ADC. 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 as well.

Thunder ADC devices can be inserted into the network as Layer 2 “transparent” switches or Layer 3 routers that can support RIP and OSPF routing. 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 Connect Secure clusters, users can access the enterprise network using a common URL. This URL maps to a virtual IP address managed by Thunder ADCs.

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

Thunder ADC devices deployed as a high availability pair provide an added layer of reliability. In the event a Thunder ADC device or links become unavailable, the other Thunder ADC 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.

## SSL VPN Solution Architecture

To manage multiple Pulse Connect Secure clusters, deploy a set of Thunder ADCs configured for Global Server Load Balancing (GSLB).

### A10 Thunder ADC and Pulse Connect Secure Cluster

Thunder ADC can intelligently balance traffic among multiple Pulse Connect Secure nodes while presenting a single, virtual URL to users.

Mobile users can access the VPN from anywhere with a single URL, such as myvpn.corp.com, mapped to a single virtual IP (VIP) address. To service a connection request, ADCs assess the health and session load on each Connect Secure node, then select a Connect Secure 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 Connect Secure node, even across multiple sessions, so long as that node is available.

Robust hardware-driven Thunder ADC security features such as hardware-based SYN cookies can supplement the advanced security features of Pulse Connect Secure, easily dismissing up to 200 million TCP-SYN packets per second.

## Global Thunder ADC Deployments

GSLB enables seamless access and disaster recovery, maintaining business continuity even in the event of a site outage or a natural disaster. With GSLB, users in all geographic locations can request network access using the same URL. A Thunder ADC device running GSLB selects the best site for the request and modifies the DNS to direct the user to the chosen site.

When Thunder ADC is configured for GSLB, it manipulates DNS replies to choose the best site for each user. The ADC 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 Connect Secure nodes.

## Summary

An SSL VPN deployment consisting of Pulse Connect Secure and A10 Networks Thunder ADC provides the industry’s most reliable and scalable secure remote access solution. New and existing SSL VPN deployments alike can benefit from Thunder ADC features such as configurable health monitors, flexible load balancing, persistence (“stickiness”) options and HA. Hardware-based DDoS protection detects and drops unfriendly TCP traffic while allowing legitimate user traffic to the Pulse Connect Secure nodes. High Availability eliminates service interruption due to Thunder ADC or link unavailability. GSLB provides additional flexibility and ease of use, enabling a single user

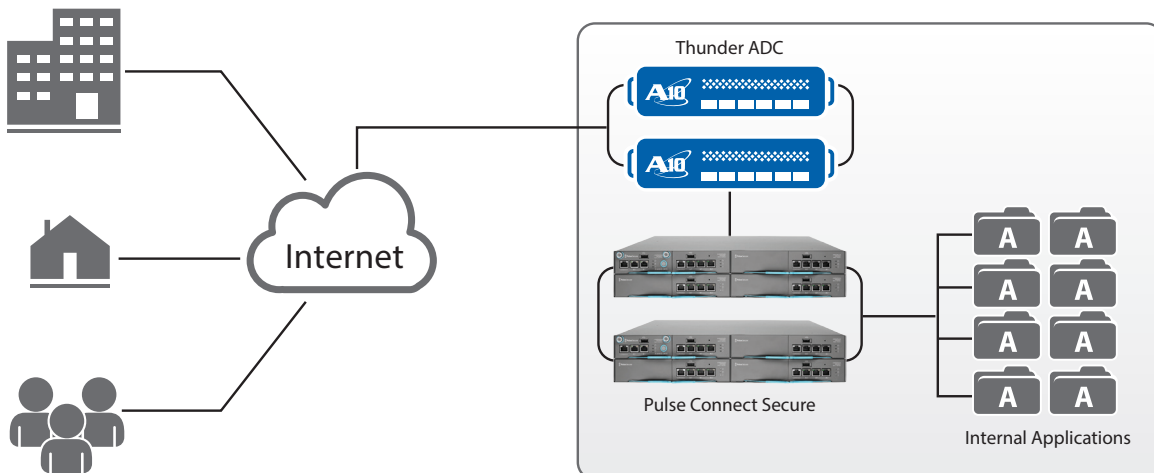


Figure 1: A10 Thunder ADC and Pulse Connect Secure SSL VPN architecture

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.

Thunder ADC allows Pulse Connect Secure deployments to scale to support today's mobile workforce. Tomorrow's ever increasing numbers of users, running increasingly bandwidth intensive applications, will continue to enjoy fast, reliable and secure access without the need to manage and utilize multiple URLs due to user location or network load.

## Pulse Secure

Pulse Secure is a "new" company born from the sale of Juniper Networks Junos Pulse product line to Siris Capital, a leading private equity firm. Pulse Secure is a leading provider of access and mobile security solutions to both enterprises and service providers. Enterprises from every vertical and of all sizes utilize the company's Pulse virtual

private network (VPN), network access control and mobile security products to enable end user mobility securely and seamlessly in their organizations. Pulse Secure's mission is to enable open, integrated enterprise system solutions that empower business productivity through seamless mobility. For more information, visit [www.pulsesecure.net](http://www.pulsesecure.net).

## 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](http://www.a10networks.com)

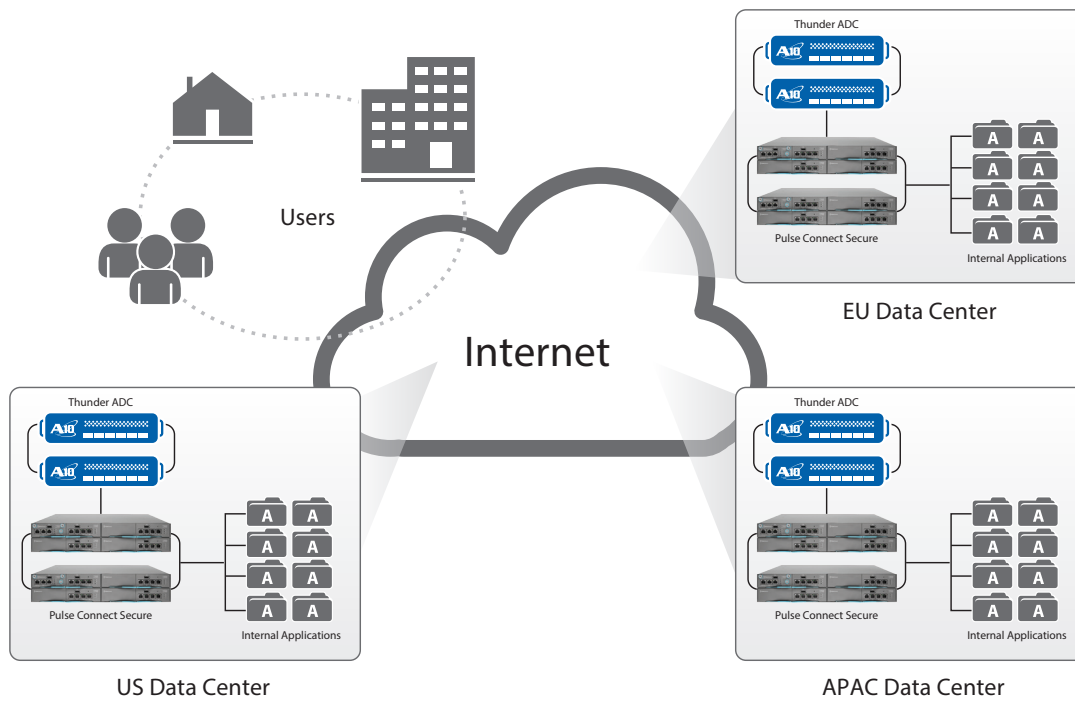


Figure 2: Global Thunder ADC and Pulse Connect Secure deployments

### 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](http://www.a10networks.com)

### Worldwide Offices

**North America**  
[sales@a10networks.com](mailto:sales@a10networks.com)  
**Europe**  
[emea\\_sales@a10networks.com](mailto:emea_sales@a10networks.com)  
**South America**  
[latam\\_sales@a10networks.com](mailto:latam_sales@a10networks.com)  
**Japan**  
[jinfo@a10networks.com](mailto:jinfo@a10networks.com)  
**China**  
[china\\_sales@a10networks.com](mailto:china_sales@a10networks.com)

**Taiwan**  
[taiwan@a10networks.com](mailto:taiwan@a10networks.com)  
**Korea**  
[korea@a10networks.com](mailto:korea@a10networks.com)  
**Hong Kong**  
[HongKong@a10networks.com](mailto:HongKong@a10networks.com)  
**South Asia**  
[SouthAsia@a10networks.com](mailto:SouthAsia@a10networks.com)  
**Australia/New Zealand**  
[anz\\_sales@a10networks.com](mailto: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](http://www.a10networks.com/contact) or call to talk to an A10 sales representative.

Part Number: A10-SB-19127-EN-01  
Oct 2014

©2014 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, A10 Thunder, Thunder, vThunder, aCloud, ACOS, and aGalaxy are trademarks or registered trademarks of A10 Networks, Inc. in the United States and in other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.