Thunder CFW IPsec site-to-site VPN

Massive Scale and Throughput Traffic Encryption

Challenge:

To protect communications, businesses and service providers need to encrypt data at high speed and scale VPN tunnel capacity on-demand.

Solution:

A10 Networks empowers businesses and service providers to reduce their data center footprint and ensure data privacy with a high-performance IPsec VPN solution, which is integrated with other key security and application delivery components.

Benefits:

- High performance IPsec VPN, traffic inspection, and stateful firewall functionality
- Encrypt data at unparalleled speeds
- Reduce rack space and power requirements
- Scale capacity by launching new VPN gateways on-demand
- Securely interconnect remote sites over the Internet using high performance hardware-based IPsec cryptographic security

Data Privacy Challenges

Organizations of all sizes rely on IPsec VPNs to prevent snooping and data theft and to address compliance. IPsec provides a cost-effective and secure way to transfer data over IP networks.

While IPsec is a mature and well understood technology, new networking paradigms like cloud computing, as well as escalating bandwidth requirements, are compelling enterprises and service providers to rethink their VPN strategies. As a result, there is a requirement to develop VPN architectures that can:

- Support unprecedented IPsec throughput levels
- Leverage BGP routing for high availability and rapid scaling
- Spin up new IPsec tunnels and gateways on-demand in cloud environments
- Minimize power consumption and rack space requirements for data center efficiency

Organizations need a solution they can trust to deliver reliable IPsec connectivity, and one that can interoperate with their existing routers and IPsec VPN gateways.

The Need to Protect Data

Organizations typically transfer sensitive data between remote sites and now increasingly to public and private clouds. The need to protect data from eavesdropping and hijacking is a requirement for most businesses, government agencies and service providers. In order to protect the transfer of sensitive data, a site-to-site VPN solution should be implemented.

Using IPsec, IP packets can be secured between sites by providing data origin authentication, access control, protection against data replays and confidentiality using strong encryption. Using A10 Networks Thunder® Convergent Firewall (CFW), a high-performance IPsec solution can be deployed and easily integrated into an existing network infrastructure and centrally managed along with other critical security features, such as SSL Insight® and a firewall to protect data center applications.

A10's IPsec Solution

A10 Thunder CFW includes IPsec encryption capabilities that enable enterprises and service providers to build out large-scale VPN deployments. By supporting up to 20,000 VPN tunnels per Thunder CFW platform and a broad array of encryption algorithms and data integrity methods, organizations can deploy Thunder CFW alongside their existing VPN equipment or build out new VPN networks with Thunder CFW appliances.

ICSA labs CERTIFIED IPSEC - IKEV2 BASIC

The A10 Thunder CFW IPsec solution has achieved the IPsec IKEv2 certification from ICSA Labs. ICSA Labs testing and certification ensures that A10 Thunder CFW performs as intended and provides interoperable, cryptographically-based security services for IP layer environments.

Thunder CFW supports a comprehensive set of features in addition to IPsec VPN, including advanced server load balancing, Network Address Translation (NAT), IPv4 and IPv6 routing, data center and Gi/SGi firewalls, SSL Insight, secure Web gateway and many other traffic security features. By delivering a wide range of networking features, organizations can support complex network designs and granularly control access to remote resources without needing to deploy and manage numerous appliances. All of these features, in addition to IPsec, are provided standard with Thunder CFW.

High Availability and Rapid Scaling

For many organizations, VPNs serve business critical functions such as data migration, disaster recovery, remote user access, and connecting data centers to cloud networks. Regardless of the use case, organizations depend on VPNs to run their business and these VPNs must always be available.

Thunder CFW supports an array of clustering, high availability and dynamic routing features that maximize uptime, not just for IPsec VPN routes, but also to ensure connectivity to servers and applications. High availability and scaling features include:

- **Route monitoring and failover** – Using A10 Networks enhanced Virtual Router Redundancy Protocol implementation (VRRP-A), Thunder CFW can monitor route and VPN gateway failures and rapidly failover traffic to a passive Thunder CFW appliance. Supporting up to eight appliances in a cluster, VRRP-A can detect unresponsive services, servers and applications and identify infrastructure failures. With A10 Networks Virtual Chassis System (aVCS®), multiple A10 devices can function as a single virtual chassis, with a single point of control and centralized statistics.
- **Intelligent routing to increase VPN capacity** – Thunder CFW supports Border Gateway Protocol (BGP) routing, which not only allows BGP routers to communicate across IPsec VPN tunnels, but also enables organizations to boost IPsec capacity simply by deploying more Thunder CFW appliances. Using BGP, Thunder CFW deployments can scale to support terabit bandwidth requirements without complicated network designs or forklift hardware upgrades, and they can deploy more Thunder CFW appliances to increase IPsec throughput. VRRP-A integrates with BGP to inject routes and ensure smooth route failovers. Thunder CFW also supports Bidirectional Forwarding Detection (BFD) for fast path failure detection and route convergence.
- **Bandwidth aggregation by load balancing traffic over multiple paths** – Thunder CFW leverages Equal-Cost Multipath (ECMP) routing to increase total IPsec VPN bandwidth. ECMP, combined with BGP, allows routers to support multiple network routes simultaneously, allowing Thunder CFW to load balance traffic across multiple paths to boost overall VPN capacity.

High-Performance Architecture

Thunder CFW leverages unique software and hardware design advantages to deliver exceptional IPsec performance. The A10 Networks Advanced Core Operating System (ACOS®) powers Thunder CFW appliances. Built from the ground up to maximize the performance of multicore CPU architectures, ACOS can linearly scale compute processing as more CPU cores are added, providing unparalleled performance in a compact form factor.

ACOS uses scalable symmetric multiprocessing (SSMP) to leverage supercomputing techniques for parallel processing and to maximize the performance of multicore architectures. Due to its highly scalable 64-bit operating system optimized for multicore architectures, Thunder CFW appliances deliver unmatched IPsec VPN performance.

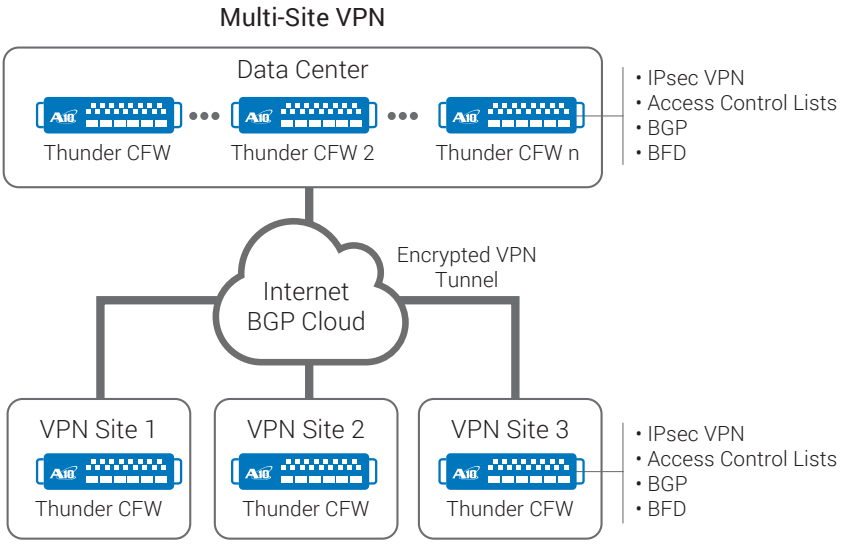

Figure 1: Thunder CFW can connect to multiple VPN sites over a BGP cloud

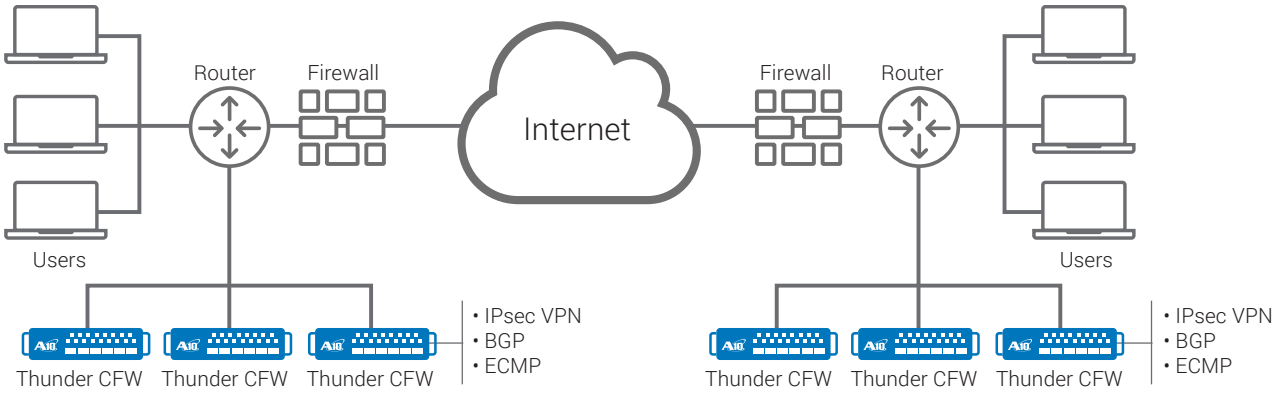

Figure 2: Users can forward traffic destined for the remote VPN site through the Thunder CFW appliance and send all other traffic directly to the Internet

Select Thunder CFW hardware models include dedicated security processors that accelerate IPsec encryption speed. Supporting multiple security processors on a rack-mountable appliance, Thunder CFW provides fast IPsec encryption without forcing organizations to deploy cumbersome and inefficient chassis-based systems.

Because of Thunder CFW's high-performance and data center optimized design, organizations can reduce the number of appliances they need to provision, lowering capital and operating expenses as well as reducing data center rack space and power costs.

Summary

Organizations need a solution they can trust to deliver reliable IPsec connectivity, and they also need one that can interoperate with their existing routers and IPsec VPN gateways. Thunder CFW's IPsec VPN capability enables organizations to encrypt traffic at high speed and support BGP routing and on-demand VPN provisioning. Using Thunder CFW's IPsec VPN technology, organizations can:

- Meet growing IPsec throughput requirements by leveraging A10's 64-bit ACOS platform and specialized security processors
- Consolidate IPsec VPN, data center and Gi/SGi firewalls, Network Address Translation (NAT), IPv4 and IPv6 routing, SSL Insight, secure Web gateway, server load balancing and additional security functionality on a single device
- Lower hardware, operating and maintenance costs with Thunder CFW's data center efficient design
- Support public, private and hybrid cloud provisioning and BGP networking requirements

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-19153-EN-02
Jan 2017

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
Hong Kong
hongkong@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
South Asia
southasia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To discover how A10 Networks products will enhance, accelerate and secure your business, contact us at **a10networks.com/contact** or call to speak with an A10 sales representative.

©2017 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, Thunder and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and 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. For the full list of trademarks, visit: www.a10networks.com/a10-trademarks.