SSL INSIGHT AND LOAD BALANCING FOR CHECK POINT

Improve SSL Visibility and Scale Network Security

Challenge:

To gain full visibility into threats, Check Point Next Generation Firewalls must scale to protect the largest networks in the world and inspect all traffic, including encrypted traffic.

Solution:

A10 Thunder ADC empowers Check Point customers to inspect and block threats in SSL traffic, increase aggregate performance and maximize uptime using A10's SSL Insight and load balancing capabilities.

Benefits:

- Uncover threats concealed in encrypted traffic by decrypting SSL traffic at high speeds
- Maximize uptime and scale using best-in-class load balancing and clustering
- Protect applications and network resources with the world's most proven firewall
- Provide granular security policies at a per user, per group or per machine level

Check Point® SOFTWARE TECHNOLOGIES LTD.

Uncompromising Security and Availability

To stop dangerous threats like advanced persistent threats and intrusions, organizations need a flexible, high-performance and laser-accurate security solution. Check Point Software's Next Generation Firewall provides all of this – plus the management, monitoring and reporting that established Check Point as the leader in network security two decades ago.

Over the past twenty years, security and networking requirements have transformed. Now, large enterprises need to inspect tens or hundreds of gigabits of throughput, not just with the deep packet inspection (DPI) that made Check Point famous, but with URL filtering, data leak prevention, antivirus, threat emulation and more. While these defenses ratchet up security, they also impact performance.

In addition, Check Point customers must also contend with growing SSL bandwidth usage. To prevent snooping and theft, an increasing number of applications encrypt all communications. Online search engines, social media, banking sites and retailers alike use SSL or TLS to encrypt traffic. In fact, according to NSS research, 25-35% of enterprise traffic is encrypted and, depending on the industry vertical, the percentage of encrypted traffic can approach 70%[1] of all traffic.

To protect applications and data, Check Point customers should inspect all traffic, including encrypted data. Furthermore, customers with demanding bandwidth requirements should maximize uptime and increase overall inspection capacity by load balancing Check Point firewall deployments.

A10 Thunder ADC and Check Point Next Generation Firewall

A10 Networks has partnered with Check Point Software to uncover malicious activity hidden in SSL traffic and to load balance Check Point firewall appliances. The A10 Networks® Thunder™ ADC line of high-performance application delivery controllers, with its integrated SSL Insight™ technology, terminates and decrypts SSL traffic. Thunder ADC then sends decrypted traffic to Check Point Next Generation Firewall for inspection and analysis.

Thunder ADC functions as an SSL forward proxy in order to intercept SSL traffic. In a Check Point Next Generation Firewall and Thunder ADC deployment, a pair of Thunder ADC appliances[2] is installed between internal clients and Check Point Next Generation Firewalls. An additional pair of Thunder ADC appliances is installed between the Check Point Next Generation Firewalls and the Internet. As shown in Figure 1, for each SSL session:

- A Thunder ADC appliance deployed between end users and the Check Point appliance intercepts outgoing SSL traffic and sends the traffic unencrypted to a Check Point appliance.

[1] NSS Labs, SSL Performance Problems, https://www.nsslabs.com/system/files/public-report/files/SSL%20Performance%20Problems.pdf

[2] One or more Thunder ADC appliances can be deployed between network clients and Check Point appliances. However, most organizations prefer to deploy two Thunder ADC appliances for redundancy.

- The Check Point appliance inspects the traffic for malicious activity and, if the traffic does not violate any security policies, forwards it on.
- A second Thunder ADC appliance deployed between the Check Point appliances and the Internet receives traffic from the Check Point appliance, encrypts the data, and sends it to the intended server.

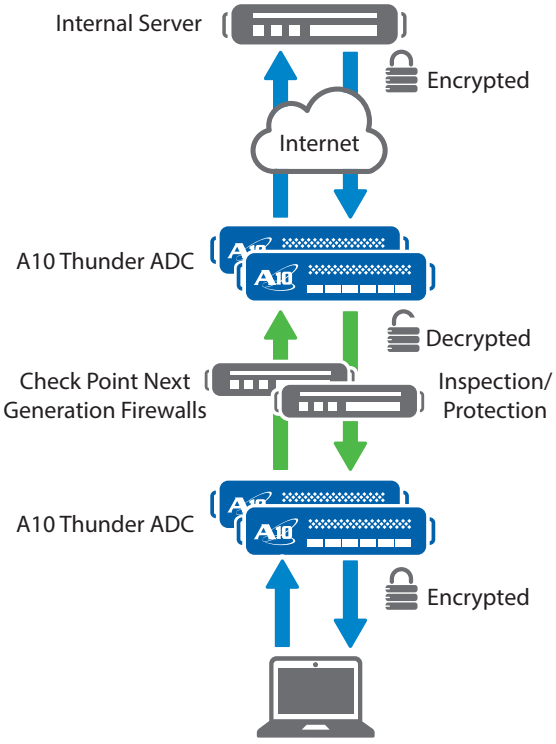

Figure 1: Thunder ADC decrypts and forwards traffic to Check Point Next Generation Firewalls.

From both the client's and the server's point of view, there still is an end-to-end encrypted session that is only decrypted within the client's network, in a contained environment. Customers can have peace of mind knowing that security blind spots created by SSL are eliminated. SSL Insight ensures that connections between internal clients and servers are encrypted to prevent unwanted snooping and data theft.

Using A10's SSL Insight technology, Check Point firewalls can inspect all inbound and outbound network traffic without needing to perform computationally intensive SSL encryption and decryption processes. SSL Insight ensures that all inbound and outbound network traffic can be properly analyzed to detect and mitigate threats.

High Performance Security Processors

SSL termination, which involves encrypting and decrypting many sessions simultaneously, is an extremely CPU-intensive task. Increasing security strength calls for an exponential increase in CPU power.

Encryption strength is determined in part by SSL key length. 2048-bit SSL certificates require approximately 3.4 times more processing power to encrypt and 6.3 times more processing power to decrypt than 1024-bit certificates,[3] while 4096-bit certificates require roughly 25 times more processing power than 1024-bit certificates to decrypt. Because of growing concern over government snooping and NIST Special Publication 800-131A, which deprecated the use of 1024-bit certificates, more applications than ever use 2048- and 4096-bit SSL keys.

A10 Thunder ADC has been designed from the ground up to deliver exceptional SSL performance, even with 4096-bit SSL keys. Powered by A10 Networks' 64-bit Advanced Core Operating System (ACOS®), Thunder ADC provides linear scalability and offers the maximum performance available from dedicated security processors and switching and routing processors. All Thunder ADC models can support SSL offloading, but select models include dedicated high-performance security processors that can handle up to 174,000 SSL connections per second and 1.55 million SSL transactions per second[4] with 2048-bit SSL keys.

When using conventional CPU resources for establishing SSL connections, performance degrades drastically as SSL key sizes increase. With its next-generation security processors, Thunder ADC delivers near parity performance between 1024- and 2048-bit key sizes, and has the extreme power needed to handle 4096-bit keys at high-rate production levels.

Scale Security Deployments with Load Balancing

With its load-balancing capabilities, Thunder ADC also provides high availability and scale, enabling organizations to deploy multiple Check Point Next Generation Firewalls and, in the event of a hardware or network failure, to route around failed devices. Supporting a wide range of load-balancing algorithms, including round robin, weighted round robin, least connections and fastest response, Thunder ADC can also scale Check Point deployments.

Advanced health monitoring ensures that servers and applications are responding as expected and routes traffic to available firewall appliances. With scriptable health checks, Thunder ADC can evaluate the responsiveness of multiple firewall appliances based on a wide set of criteria and direct traffic to the best firewall appliance to meet performance and latency goals.

Granularly Control Traffic

Using Thunder ADC's fine-grained policies, customers can control which secure sessions to intercept and which to leave encrypted. Organizations can use these policies to bypass traffic to trusted sites, such as banking and healthcare applications. Supporting an optional URL classification subscription which can categorize traffic to over 460 million domains, as well as manual URL bypass lists, Thunder ADC can bypass sensitive traffic to satisfy privacy and compliance requirements.

[3] On commodity hardware, 2048-bit Check Point certificates require 6.3x and 3.4x more computational effort, to decrypt and encrypt respectively, than 1024-bit Check Point certificates according to a StackExchange analysis.
[4] 1.55 million TPS with unlimited requests per connection for SSL offload.

With A10 Networks' aFleX® scripting, Thunder ADC can programmatically control application traffic. aFleX scripts can manipulate all aspects of traffic, even sanitizing sensitive content before sending it to the intended destination.

The A10 Thunder ADC product line of high-performance, next-generation application delivery controllers enables customers' applications to be highly available, accelerated and secure. As an added benefit, all features, including SSL Insight, are included without licensing fees.

Offload and Inspect Inbound SSL Traffic

Besides decrypting outbound traffic with SSL Insight, A10 Thunder ADC can also proxy and decrypt inbound traffic with its SSL Offload feature. When deployed as a reverse proxy, Thunder ADC can terminate traffic sent from external users to corporate-owned web, mail, or other servers. Thunder ADC can then direct it to an inline Check Point Firewall for inspection before encrypting the traffic again and forwarding it on to intended destination.

In addition, Thunder ADC can send unencrypted traffic to non-inline Check Point appliances, such as a DLP, IPS, or Threat Emulation appliances, through a TAP or mirror port. Then Thunder ADC can either encrypt the traffic and forward it to corporate-owned servers or it can send the traffic unencrypted to the servers, offloading SSL processing from the servers.

Thunder ADC's SSL Offload capability enables Check Point appliances to inspect encrypted traffic and detect attacks such as web attacks targeting web servers hosted in internal data centers. With SSL Offload, Thunder ADC provides 360 degree visibility into traffic, including SSL traffic, without burdening network firewalls. It also enables organizations to protect critical servers like web servers from attacks hidden in SSL traffic.

Check Point Next Generation Firewall

Check Point Next Generation Firewall extends the power of the firewall beyond stopping unauthorized access by adding intrusion prevention system (IPS) and application control. Next Generation Firewalls come in many sizes and offer throughput of up to 110 Gbps.

With the Check Point Next Generation Firewall, network administrators can securely control access to clients, servers and applications. Based on the industry's most advanced identity awareness, the Check Point software provides robust authentication capabilities to confirm the identity of all users and establish their rights and privileges. Integrated intrusion prevention detects known attacks, infiltration attempts and vulnerability exploits.

Conclusion

Since SSL traffic accounts for a large – and growing – percentage of all network traffic, SSL exposes dangerous blind spots in corporate defenses. A10 Thunder ADC offers Check Point customers an easy-to-deploy, high-performance solution for decrypting SSL communications and maximizing the availability and scale of Check Point deployments. A10 Networks has successfully tested and validated interoperability between A10 Thunder ADC and the Check Point Next Generation Firewall. Using A10's SSL Insight technology, organizations can:

- Improve application performance, availability and scalability using A10's 64-bit Advanced Core Operating System and specialized security processors
- Integrate with Check Point Next Generation Firewall to stop unauthorized access, control access to applications and stop network intrusions
- Gain unified security management to streamline monitoring, configuration and reporting for multiple Check Point gateways

A10's powerful SSL Insight capability, included as a standard feature of Thunder ADC, enables businesses to:

- Gain complete visibility into network activity, including encrypted traffic, to prevent attacks and infiltrations
- Use Thunder ADC as a centralized point for load balancing and decryption, intercepting SSL traffic and sending it to multiple security devices, such as Check Point Firewall, Data Loss Prevention (DLP), Threat Emulation and IPS gateways, for inspection and protection
- Optionally bypass traffic to sensitive websites, such as communications to banking and healthcare sites, to prevent confidential data from being decrypted
- Future-proof their investment as SSL usage expands and encryption key lengths increase

About Check Point Software Technologies

Check Point Software Technologies Ltd., the worldwide leader in securing the Internet, provides customers with uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented stateful inspection technology. Today, Check Point continues to develop new innovations based on the Software Blade Architecture, providing customers with flexible and simple solutions that can be fully customized to meet the exact security needs of any organization. Check Point is the only vendor to go beyond technology and define security as a business process. Check Point 3D Security uniquely combines policy, people and enforcement for greater protection of information assets and helps organizations implement a blueprint for security that aligns with business needs.

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-19126-EN-01
Jan 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.