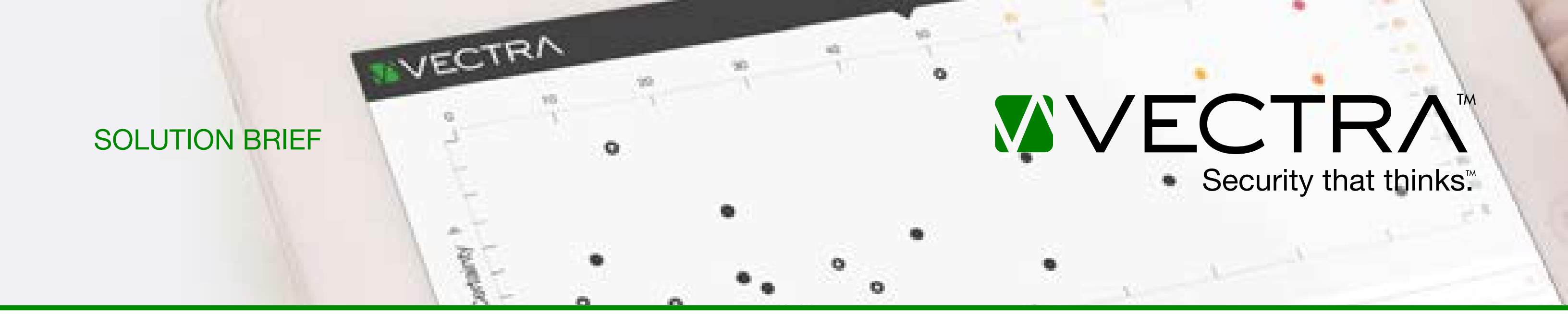


SOLUTION BRIEF

VECTRA™
Security that thinks.™

SSL Insight™ with Vectra Networks

The A10 Networks® Thunder Application Delivery Controller (ADC) product line delivers SSL Insight™ capability that enables inspection of encrypted flows, increasing the efficacy and accuracy of the Vectra X-series real-time breach detection platforms.

Executive Overview

Today's cyber security threat landscape is highly dynamic with attackers constantly morphing malware and attack vectors to evade detection, and persistently attack your information assets. One technique attackers use to evade detection is to encrypt communications with secure socket layer (SSL) encryption. Perimeter security systems like firewalls, intrusion detection systems/intrusion prevention systems (IDS/IPS) or sandboxes are unable to inspect the encrypted traffic payloads. Once a host is compromised, the perimeter defenses are blind to the malicious software and the attacker is free to begin their job.

To detect cyber attacks that have already bypassed the network perimeter, security professionals need automated real-time breach detection and reporting capabilities, providing defense in depth to stop the progression of a cyber attack. Automated breach detection can identify attacks in progress even when the payload is encrypted, but efficacy and accuracy increases when the packet flows are unencrypted.

The A10 Networks Thunder Application Delivery Controller (ADC) product line delivers an SSL Insight capability that enables inspection of encrypted flows, increasing the efficacy and accuracy of Vectra X-series real-time breach detection platforms.

Solutions that can inspect SSL traffic for cyber attacks will become a requirement as more enterprise traffic is encrypted. According to NSS Labs research, 25 – 35 percent of enterprise traffic is currently encrypted with SSL and, depending on the industry vertical, the percentage of SSL traffic can be as high as 70 percent.[1]

SSL Encryption — A Blessing and a Curse

Security and privacy is a top concern for organizations with the growing dependency on the Internet for business processes and customer interaction. As organizations move key applications like email, CRM, business intelligence, and file storage to the cloud, they need to monitor and protect these applications just as they would internally hosted applications.

In partnership with

A10®

[1] https://www.nsslabs.com/reports/ssl-performance-problems

SSL encryption helps address these concerns by providing client-server authentication and a private secure channel through which hosts can send and receive data. SSL encryption has become the ubiquitous de-facto standard for encrypting network connections to services such as email, instant messaging (IM) and cloud storage.

The use of SSL encryption ensures privacy of network application traffic, but it can enable cyber attackers to obfuscate the identity and behavior. Attackers are already using SSL to bypass perimeter network security.

Gartner believes that, in 2017, more than half of the network attacks targeting enterprises will use encrypted traffic to bypass controls, up from less than 5% today[2]. For example, the Zeus botnet uses SSL communication to upgrade after the initial email infection.

Reverse the Curse

To protect users, data and applications, enterprises must inspect all traffic, including encrypted traffic. SSL encrypted traffic prevents network security devices from performing deep packet inspection, creating a blind spot. To address this problem, perimeter security systems like firewalls and IDS/IPS have incorporated the ability to decrypt SSL traffic for deep packet inspection. Decrypting SSL traffic on these perimeter security systems is CPU-intensive, resulting in performance degradation.

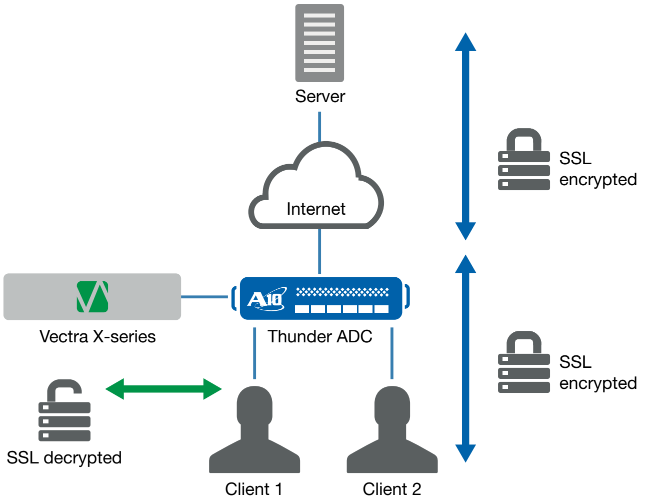
A study by NSS Labs[3] found that the leading next-generation firewall vendors experienced an average of 81% degradation in performance when decrypting SSL traffic. This led NSS Labs to assert that it had "concerns for the viability of SSL inspection in enterprise networks without the use of dedicated SSL decryption devices."

A solution is available in the form of purpose-built SSL decryption devices to address the performance degradation problem. These devices, transparent to the end user can decrypt the SSL traffic for deep packet inspection and re-encrypt the traffic before sending it to destination.

Automated Breach Detection via Performance-optimized SSL Intercept

The Thunder ADC product line's SSL Insight feature combined with the Vectra Networks X-series platform eliminates the blind spot imposed by SSL encryption. As a natural function of optimizing application delivery, the Thunder ADC product offloads CPU-intensive SSL decryption functions enabling security devices to inspect encrypted traffic while maintaining application performance levels.

The Thunder ADC functions as a SSL forward proxy to intercept SSL encrypted traffic between internal clients and the Internet.



Vectra X-series deployed with the Thunder ADC and SSL Insight.

The sequence below outlines the role of the Thunder ADC SSL Insight with Vectra Networks X-series real-time breach detection in a round-trip SSL-encrypted session between a user and a Web server.

1. The Thunder ADC decrypts outbound SSL encrypted HTTP traffic and sends a copy of the unencrypted traffic to the Vectra X-series platform for real-time breach detection.
2. The Thunder ADC re-encrypts the HTTP traffic and forwards it onto the external Web server.
3. The Web server sends an encrypted reply to the Thunder ADC.
4. The Thunder ADC decrypts the reply and forwards a copy of the unencrypted traffic to the Vectra X-series platform for inspection.
5. The Thunder ADC re-encrypts the reply from the Web server and sends it to the client.

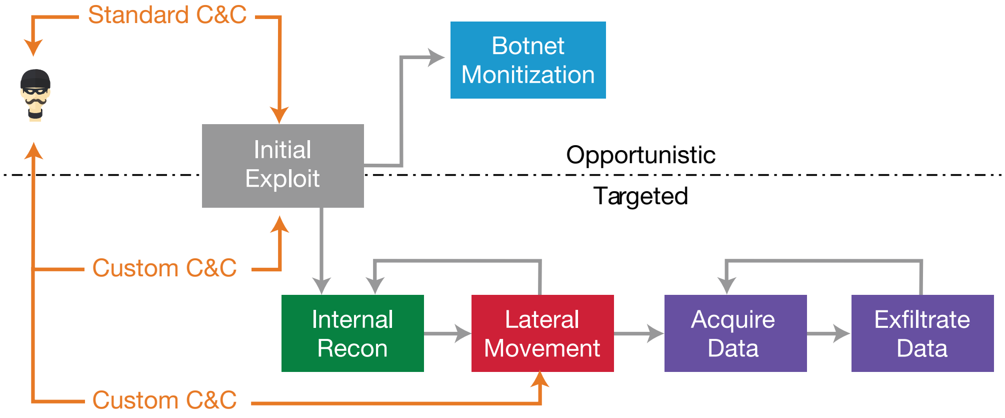
[2] "Security Leaders Must Address Threats From Rising SSL Traffic," by Jeremy D'Hoinne, Adam Hils, Gartner, 9 December 2013, ID G00258176, https://www.gartner.com/doc/2635018/security-leaders-address-threats-rising

[3] https://www.nsslabs.com/reports/ssl-performance-problems

The Vectra X-series platform combines security research, data science and machine learning to automate the detection of an ongoing cyber attack. Vectra Network's algorithms detect the behavior of the malware without using signatures or reputation lists. Vectra listens continuously to all traffic — user to internet, user to data center and user to user — to detect any phase of the attack amid the chatter of your network. The Vectra X-series correlates detections over days, weeks or months to tell a story about what the attacker is doing and the lifecycle of the attack. The intuitive reporting prioritizes the highest-risk attacks, enabling you to stop it or mitigate loss.

The Vectra X-series detects attacks on any device running any operating system or application. Vectra provides multiple opportunities to stop an ongoing cyber attack whereas perimeter security only detects the initial exploit of the attack and sometimes the command and control callback.

The infographic to the right shows the Vectra Kill Chain.



Benefits of the Thunder ADC and Vectra X-series platform

The tables below outline the key benefits of the Thunder ADC and Vectra X-series Platform.

Thunder ADC SSL Insight Benefits
Inline deployment with passive, non-inline third-party device
Inline deployment with active, inline third-party devices
SSL Intercept Bypass based on hostname; bypass list scales up to 1 million Server Name Indication (SNI) value
Extensive Cipher and Protocol Support • TLS 1.0, TLS 1.1, TLS 1.2,SSL v3 • RSA, DHE, ECDHE ciphers with PFS support • MD5, SHA, SHA-2
URL classification powered by Webroot (available in ACOS version 4.0.1) to selectively bypass specific websites

Vectra X-series Platform Benefits
Passive network deployment
Detects attacks regardless of methods and location of initial delivery
Detects zero-day threats using a combination of data science and machine learning
Identifies attacks on all operating systems, applications and devices
Delivers clear, intuitive reports with all supporting data one click away
Reports anomalous behaviors during multiple phases of an advanced targeted attack

Conclusion

With SSL encrypted traffic increasing to more than half of an organization's network traffic, dangerous blind spots will be created in security defenses. Combining the SSL Insight capability of the A10 Thunder ADC with the automated breach detection of the Vectra Networks X-series platform will provide traffic visibility and enable detection of any phase of a cyber attack that is attempting to remain obfuscated in encrypted SSL network traffic.

VECTRA™
Security that thinks.®