Source: <http://www.a10networks.com/products/axseries-SSL_Intercept.php>

**SSL Intercept: Securing Encrypted Traffic**

**Securing Encrypted Traffic**

The security industry has shifted its focus to the client side. Malware and other malicious programs are increasingly being installed unknowingly on client computers where they can replicate to other clients, and relay information to malicious entities.

Security vendors provide tools to detect and mitigate these problems by inspecting the traffic between client and the untrusted side of the network (the Internet). At the same time, most online web services or cloud applications now use TLS/SSL to secure the session with the client. TLS is the IETF-standardized successor of SSL; both are very similar in that they provide encrypted communications for web applications. In common usage, SSL is used to describe both, as will we in this document. While this is a good strategy for many reasons, it introduces a problem for active traffic inspection tools—the information is encrypted and thus, unreadable.

A10's SSL Intercept feature addresses this problem by decrypting traffic and forwarding it through a 3rd party security device (for example, a firewall) for deep packet inspection and then securely forwarding on to its destination.

**SSL Intercept Solution: Challenges and Requirements**

SSL Intercept, also known as SSL forward proxy, is a technology consisting of two SSL termination devices that have separate secured sessions between server and client. The adjacent diagram explains the flow. The encrypted traffic from the client (1) is decrypted by the AX on the client side and sends the unencrypted data (2) to the security appliance of choice. After inspection, the AX device on the server side receives the data from the security device, encrypts the data again and sends it to the server (3). The same process takes place for the encrypted traffic from the server (4); it is decrypted (5), inspected and forwarded to the client, but now encrypted (6).

From the client and the server's point of view, there still is an end-to-end encrypted session. The traffic between the two [AX devices](http://www.a10networks.com/products/axseries.php) is not encrypted, so a 3rd party security device can do in-depth traffic analysis, which would not have been possible without the SSL Intercept feature.

SSL termination—setting up and tearing down many secure sessions, encrypting and decrypting many sessions simultaneously—is an extremely CPU-intensive task. Increasing security strength calls for an exponential increase in CPU power. The encryption strength is determined in part by the key length. When upgrading from 1024-bit to 2048-bit key sizes, the CPU usage can increase 4 – 7 times. When more secure 4096-bit keys are used, regular server CPUs will be taxed beyond their limits.

SSL sessions encrypted with 1024-bit keys are not deemed secure enough. The US National Institute of Standards and Technology (NIST) recommended that the minimum key length should be changed from 1024-bit to 2048-bit. For more sensitive information, stronger encryption increases security. Certificate Authorities (CAs) no longer provide certificates with key sizes less than 2048-bit.

A device that is used for SSL intercept therefore must possess a lot of computing power to manage multiple sessions simultaneously, be able to establish many SSL Connections per Second (CPS) and be able to handle larger SSL keys.

Many security solutions such as:

* Unified Threat Management (UTM)
* Data Loss Prevention (DLP)
* Intrusion Detection Systems (IDS)
* Other content filters/inspection devices

These devices are built to deal with traffic analysis; verifying traffic behavior utilizing their internal policy engine, which already consumes a lot of computing power. In many cases, even if these devices provide SSL Intercept functionality, they can only manage low volumes of secured web traffic. The AX Series solution allows for any security device to inspect any SSL content. Using all-in-one security devices and stacking SSL Intercept responsibility on top of their regular tasks, results in poor scaling and poor end-user experience. A powerful, dedicated SSL Intercept solution is therefore recommended. The AX Series takes a fully transparent approach to allow full flexibility and freedom of choice for traffic inspection.

**AX Series with SSL Acceleration Hardware**

The setup of a secure connection is the most CPU demanding part of an SSL connection. Encrypting/decrypting the bulk data of a session is still CPU intensive but to a lesser degree. Managing many secure connections simultaneously is a perfect task for the AX Series. The AX Series—the first ADC solution to introduce SSL Intercept— provides exceptional SSL CPS rates and is a powerful, feature-rich platform with all-inclusive pricing. The AX Series are powered by A10's 64-bit [Advanced Operation System (ACOS)](http://www.a10networks.com/products/axseries-acos-architecture.php), which provides linear scalability and is designed to get maximum performance. All models have powerful CPUs and support the [SSL offloading feature](http://www.a10networks.com/products/axseries-ssl_acceleration.php), but select models are available with a wide range of high-performance, multi-chip SSL acceleration modules. The AX Series is exceptionally well suited for managing many SSL sessions simultaneously.

When using conventional CPU resources for establishing SSL connections, the performance hit is significant when SSL key sizes increase. With the new SSL acceleration hardware, the AX device has near-parity performance for the upgrade to 2048-bit key sizes, and has the extreme power needed to handle 4096-bit keys at high performance production levels.

ACOS' SSL Intercept feature allows the user to make the decision apply only to select secure sessions, and to leave other sessions encrypted.

**Conclusion**

The AX Series is the right solution for deploying SSL Intercept solutions:

* The 64-bit ACOS operating system leverages specialized SSL acceleration hardware for maximum performance and scalability.
* Enables analysis of all network data.
* Transparent approach allows freedom of choice and best-of breed content inspection solutions.

With the AX Series, A10 offers extremely powerful SSL offloading solutions, providing many business benefits:

* Future-proof investment for expanding TLS/SSL usage, and higher encryption standards.
* The power of the AX Series allows the leverage of existing security devices, significantly reducing CAPEX.
* Eliminates blind spots in corporate defenses.

The AX Series provides a wide range of options in CPU performance and hardware acceleration so customers can choose the right model for their environment. The AX Series offers unprecedented features, performance, flexibility and cost-efficiency.