NCIPHER

www.ncipher.com

Scalable, automatic visibility and management of SSL/TLS traffic

- Help preserve data privacy compliance with policy-based selective decryption using whitelists, blacklists and URL categories
- Fully integrated with nCipher nShield Connect Hardware Security Module to ensure secure, efficient key storage
- Expose hidden threats, malware, and data exfiltration, with support for modern cryptographic applications
- Enhance security tools by centralizing SSL/TLS decryption and re-encryption – creating a “decryption zone”
- Scale by decrypting once and delivering traffic to multiple inline and out-of-band tools simultaneously
- Increase performance with additional GigaSMART® modules

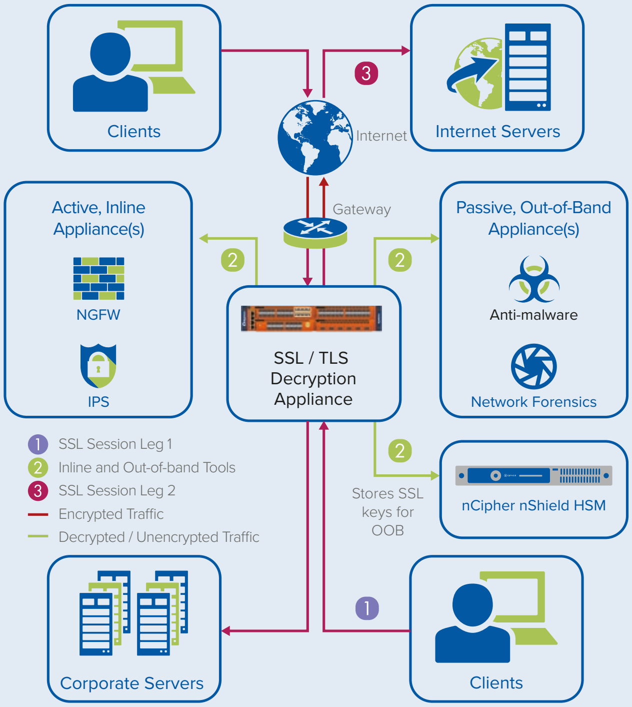
Gigamon GigaSMART and nCipher nShield; efficient and cost effective web security

THE PROBLEM: MALWARE COULD BE HIDING AND INVISIBLE

Email, e-commerce, voice-over-IP (VoIP), online banking, file storage and countless other applications are secured with Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption. The very technology that makes the Internet secure can become a significant threat vector by hiding malware and hindering network visibility. Enterprises need a way to ensure their security tools can inspect everything flowing into and over their networks.

THE CHALLENGE: TRADITIONAL APPROACHES TO DECRYPTION CAN BE COSTLY

The common approach to decrypt traffic is either to license decryption on each security tool you use – which increases both cost and the delay caused through multiple decrypt/encrypt cycles – or run a stand-alone SSL tool and then use a packet broker to distribute the decrypted traffic to the tools before routing it back to the decryption tool for re-encryption. By embedding purpose-built decryption capabilities as an option within its next generation packet broker, Gigamon provides a better solution.



Gigamon and nCipher secure SSL traffic

THE SOLUTION: GIGAMON GIGASMART AND NCIPHER SECURITY nSHIELD HARDWARE SECURITY MODULE

GigaSMART SSL/TLS Decryption enables SecOps teams to obtain automatic visibility into SSL traffic regardless of TCP port or application. As an integral feature within the GigaSECURE Security Delivery Platform – a next generation packet broker – customers can easily share this decrypted traffic to monitor application performance, analyze usage patterns and secure their networks against data breaches and hidden malware in encrypted networks.

- **Improve analytics efficiency.** By decrypting once, and then efficiently distributing the traffic to any tool that needs to inspect it, customers minimize latency and expense while ensuring the security of their enterprise.
- **Scale as your needs increase.** One instance of SSL/TLS Decryption in a Gigamon cluster is sufficient for any traffic in that node to take advantage of the functionality. Increase SSL/TLS decryption throughput by adding more GigaSMART modules.
- **Help protect data privacy and compliance.** Selectively decrypt traffic based on your own policies using a variety of parameters to help ensure that sensitive data remains encrypted.
- **Simplify your auditing process.** Fields within the payload can be masked to hide them from identification. In out-of-band mode, decrypted packets can be sliced to remove irrelevant or private payload data so that private data is never stored, read, or analyzed.
- **Increase the resiliency of your security and monitoring capability.** In the event of a tool failure, traffic can be redistributed to the remaining healthy tools.
- **Strengthen your organization's security posture.** Validate server certificates against certificate trust stores and check for invalid certificates with Certificate Revocation Lists (CRL) and the Online Certificate Status Protocol (OCSP).
- **Limit visibility of your organization's keys.** Integration with the nCipher nShield Connect HSM allows for secure use and storage of encryption keys, even while in use by the GigaSECURE platform.

WHY USE NCIHPER NSHIELD HSM WITH GIGAMON GIGASMART?

Store your decryption keys centrally and securely. The GigaSMART out-of-band decryption capability can access SSL decryption keys that your organization has stored centrally in a nCipher HSM removing the need to load your private keys into the Gigamon devices.

NCIPHER

Today's fast moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency. It also multiplies the security risks. nCipher Security, a leader in the general purpose hardware security module (HSM) market, empowers world-leading organizations by delivering trust, integrity and control to their business critical information and applications.

Our cryptographic solutions secure emerging technologies—cloud, IoT, blockchain, digital payments—and help meet new compliance mandates, using the same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensuring the integrity of your data and putting you in complete control – today, tomorrow, at all times. www.ncipher.com

GIGAMON

Gigamon is leading the convergence of network and security operations to reduce complexity and increase efficiency of the security stack. Gigamon's GigaSECURE® Security Delivery Platform is a next generation network packet broker purpose-built for security that helps organizations make threats more visible – across cloud, hybrid and on-premises environments, deploy resources faster and maximize the performance of security tools. Global 2000 companies and government agencies rely on Gigamon solutions to stop tool sprawl and save costs.

For more detailed technical specifications, please visit www.ncipher.com or www.gigamon.com