securosys

Fortinet FortiGate and Securosys Primus HSM

Enhanced security for FortiGate SSL/TLS Inspection with Securosys Primus HSM on-premises or in the cloud

Fortinet and Securosys have collaborated to deliver enhanced security using the industry-leading Fortinet FortiGate Next-Generation Firewall (NGFW). With native support for Securosys Primus HSM and CloudHSM, FortiGate ensures that sensitive key material is securely offloaded and protected within tamper-resistant hardware security modules. The high-availability capability as well as the FIPS and Common Criteria compliance of the Securosys Primus HSM make it an ideal choice for network environments of all sizes. This integration enables robust security for cryptographic keys with the FortiGate's security architecture.

Challenge

Fortinet FortiGate provides robust, multi-layered network security by inspecting and securing all traffic. To thoroughly inspect SSL/TLS encrypted traffic, firewalls must decrypt and re-encrypt it. However, if the private keys used in this process are not adequately protected, the security framework could be comprimised. As a result, safeguarding these private keys is essential to maintaining the integrity and security of your network.

Solution Benefits

Unmatched SSL/TLS Proxy Performance: Optimized for mission-critical enterprise applications with high-availability support.

Robust Key Protection: Primus HSM ensures that keys remain secure within the HSM and are never exposed externally.

Advanced Security Standards: Compliant with FIPS 140-2 Level 3 and Common Criteria EAL4+, providing also tamper protection and security assurance.

Seamless Integration: Fully integrated with FortiGate for a streamlined setup and simplified management.

Flexible Deployment: Multiple deployment options, including hardware and virtual appliances, with support for on-premises or CloudHSM.

Get started

Solution Integration

The integration of Securosys Primus HSM with FortiGate enhances security by offloading critical cryptographic key data to a tamper-resistant environment. The HSM securely generates, stores, and manages private keys.

During SSL/TLS inspection, short-lived server certificates are issued using protected keys on the HSM to decrypt SSL/TLS encrypted traffic. After inspection — and any necessary security remediation by FortiGate — the traffic is re-encrypted before being transmitted to its destination. This approach ensures that private keys remain secure and are never exposed outside the HSM, thereby significantly reducing the risk of key compromise and bolstering the overall integrity of the security architecture.
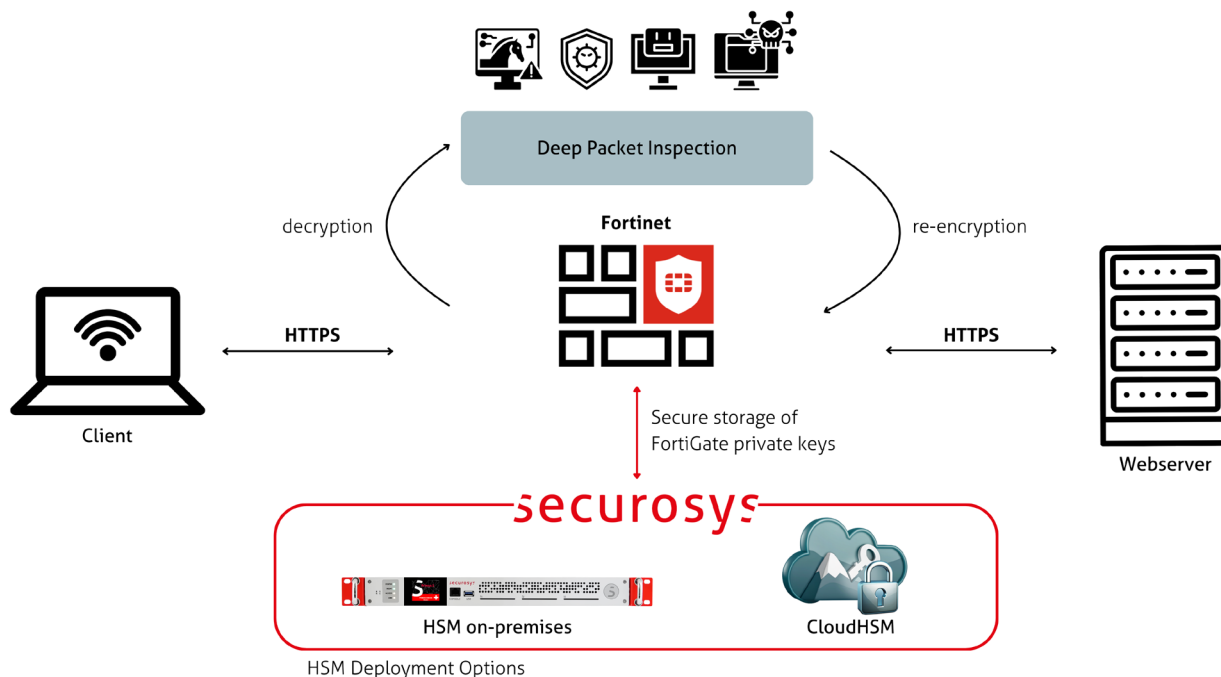
Use Cases

Secure Key Generation and Storage

Ensuring the security of cryptographic keys is critical for any organization. Securosys Primus HSM and CloudHSM provide high-entropy, hardware-based true random number generation and a tamper-resistant environment. While FortiGate has built-in key generation and storage capabilities, offloading this task to Securosys HSMs significantly enhances the security of the SSL/TLS inspection process.

Compliance with Security Standards

Compliant with regulatory requirements such as PCI-DSS, HIPAA, and GDPR demands rigourous control over cryptographic key management. Integrating FortiGate with Securosys Primus HSM or CloudHSM enables centralized management of keys and certificates on FIPS 140-2 Level 3 and Common Criteria EAL4+ certified hardware. This integration helps mitigate risks associated with key compromise and mismanagement, ensuring adherence to these stringent regulations.

About Fortinet

About Securosys