CHECK POINT + FUTUREX
PROTECT THE KEYS TO YOUR KINGDOM

PROTECT THE KEYS TO YOUR SECURE KINGDOM

Solution Benefits

- Detect threats hiding in encrypted traffic
- Securely store private keys essential to inspecting HTTPS channels
- Secure allowed encrypted channels
- Block malicious encrypted channels or internet use not allowed by policy

INSIGHTS

Industry experts believe over 70% of web malware will be carried by encrypted traffic in 2020. That's a huge blind spot for enterprise security systems, which may not have threat detection or protection against these attacks. With the widespread adoption of SSL/TLS encryption, the ability to ensure every key and certificate is available to decrypt and then inspect SSL/TLS traffic in real time, is more important than ever.

JOINT SOLUTION

Together, Check Point and Futurex enable your organization to detect threats hiding in encrypted traffic. Check Point, a leading provider of cyber security solutions globally, has integrated with Futurex's complete line of hardware security modules (HSMs). Check Point's Next Generation Security Gateway solution integration with Futurex's HSMs adds a powerful layer of security for enterprises to securely manage certificates.

Futurex's HSMs are universally compatible, FIPS 140-2 Level 3 and PCI HSM validated solutions for the highest security level of certificate management, data encryption, fraud protection, and financial and general-purpose encryption. With this integration, Futurex HSMs, either on-premises or through Futurex's VirtuCrypt cloud HSM service, are used to store and serve the certificates used for outbound HTTPS inspection via Check Point Security Gateways.

WHAT HSMS DO

A hardware security module, or HSM, is a dedicated, standards-compliant cryptographic appliance designed to protect sensitive data in transit, in use, and at rest through the use of physical security measures, logical security controls, and strong encryption.

An HSM's core functionality is centered around encryption: the process by which sensitive data is rendered indecipherable to all except authorized recipients. HSMs also offer a secure way to decrypt data to ensure message confidentiality and authenticity. Encryption is made possible through the use of encryption keys—randomly generated values that must be kept secret in order to protect the encrypted data. Because knowledge of the encryption key aids in decrypting information, it is vital that these keys are secured in a private environment.

Hardware security modules generate and store the keys used for encrypted communication among devices within a Secure Cryptographic Device (SCD), which is a far more secure method than solely using software. When information is sent to the HSM via a trusted connection, the HSM allows for the quick and safe encryption or decryption of that information using the appropriate key.

WHY DO FIREWALLS DECRYPT HTTPS CONNECTIONS?

The short answer is the need to do deep packet inspection to see if there is malicious content hidden in the encrypted HTTPS session. Firewalls essentially act as a proxy for the web server, decrypting the browser connection and, if needed, encrypting it again from the firewall to the web server. Check Point Next Gen Firewalls tightly integrate multiple security functions, providing significant cost savings over multiple point solutions.

PREVENT ZERO-DAY THREATS

Unlike other solutions that only detect threats, Check Point Next-Gen Firewalls prevent threats. Check Point SandBlast Zero-Day Protection is a cloud-hosted sandboxing technology where files are quickly quarantined and inspected, running in a virtual sandbox to discover malicious behavior before it enters the network. The Check Point solution also includes Application Control and URL Filtering to enforce safe web use. IPS, Anti-Bot and Antivirus protect customers from known threats. HTTPS inspection safeguards companies from threats trying to hide inside encrypted HTTPS channels.

Furthermore, Check Point is a fully consolidated and connected cyber security architecture protecting on premises, cloud and branch networks as well as endpoint and mobile devices from advanced persistent threats. Threats identified on one device can be automatically propagated as an IoC (Indicator of Compromise) to protect branch, mobile and cloud-hosted assets from the same zero-day threat.

CONCLUSION

While SSL/TLS provides a secure, authenticated encrypted channel, it also can create blind spots for enterprise security. Cybercriminals can use encryption to hide malicious activity from an organization's security controls, in order to evade detection and hide attacks. Together, Check Point and Futurex help to solve that problem by securing critical certificate keys in use by organizations protected with Check Point NGFWs.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

ABOUT FUTUREX

For more than 40 years, Futurex has been a trusted provider of hardened, enterprise-class data security solutions. More than 15,000 organizations worldwide, including financial services providers and corporate enterprises, have used Futurex's innovative hardware security modules, key management servers, and enterprise-class cloud solutions to address their mission-critical systems, data security, and cryptographic needs. This includes the secure encryption, storage, transmission, and certification of sensitive data.

CONTACT US

Worldwide Headquarters | 5 Shlomo Kaplan Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-628-2117 | www.checkpoint.com