ML-Powered Next-Generation Firewalls and Entrust nShield

Protecting Your Encryption Keys with Hardware Security Modules

Key Benefits

- Enhances the security of encryption keys and signing certificates used in the SSL/TLS connections that a Palo Alto Networks NGFW establishes between itself and destination servers.
- Enables the ability to encrypt the main key used for all cryptographic operations performed on the Palo Alto Networks NGFW.
- Includes encryption of all private keys and passwords.
- Provides a FIPS 140-3 or 140-2 certified root of trust.

The Challenge

Managing the cryptographic keys that encrypt sensitive data while blocking, detecting, and preventing attacks on networks can be challenging. Encrypting sensitive data safeguards its confidentiality and integrity, ensuring that only validated connections with the right decryption key can access the content.

While encryption is a great start, storing encryption keys outside of a cryptographic boundary can leave an organization vulnerable to attacks, which can lead to the disclosure of confidential information.

The Solution

To ensure the security of valuable cryptographic keys in an auditable and proven way, your security team can use hardware security modules (HSMs). HSMs provide a strong root of trust that greatly enhances network security. They deliver an additional layer of protection to the main keys that firewalls use to encrypt private keys and passwords. Segregating key storage and management from the application ensures the underpinning security of the firewall. Cybersecurity professionals consider HSM deployment a best practice. Also, HSMs both enhance security and facilitate regulatory compliance.

Entrust nShield HSMs

Entrust nShield HSMs provide a hardened, tamper-resistant environment for protecting and managing keys and for performing secure cryptographic processing. Encryption keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack, which can lead to the compromise of critical keys and data. Entrust nShield HSMs enable the enforcement of key use policies, separating security functions from administrative tasks. The interface with supported applications uses industry-standard APIs for easy deployment.

Available for use on-premises or as a service, nShield HSMs provide a root of trust that enhances your network security posture. The nShield is a network-attached appliance for high availability data center environments. nShield as a Service is the subscription-based, high-performance option that offers greater flexibility, providing a dedicated nShield HSM in the cloud.

Palo Alto Networks ML-Powered Next-Generation Firewalls

Palo Alto Networks NGFWs offer a prevention-focused architecture that's easy to deploy and operate. The machine learning (ML)-powered NGFWs inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters most, and enforce consistent protection everywhere. The user, application, and content—the elements that run your business—become integral components of your enterprise security policy. As a result, you can align security with your business policies and write rules that are easy to understand and maintain.

Palo Alto Networks and Entrust

Palo Alto Networks NGFW integrates with Entrust nShield HSMs to enhance the security of the main key used to encrypt all private keys and passwords that the firewall uses. Deployed on-premises or as a service, nShield HSMs safeguard and manage the private keys used in the SSL/TLS decryption process. The integrated solution provides the secure software and hardware needed to ensure validated connections and decrypted inbound web traffic for inspection. The combination improves the security posture of the network with a FIPS 140 certified root of trust. By providing a mechanism to enforce security policies and a secure tamper-resistant environment for the encryption and decryption of passwords and keys, you can protect your entire network security system.

Use Case 1: Strengthen the Security Posture of Your Perimeter and Points of Ingress and Egress

Challenge

Reducing the attack surface requires protecting the credentials of all authenticated users, systems, and the network from malicious SSL/TLS encrypted inbound traffic.

Solution

By using the Entrust nShield HSM, you extend the boundaries protecting all the keys. This HSM allows decryption, review, and reencryption. The private key essential to SSL/TLS encryption never leaves the Palo Alto Networks NGFW, making it impossible for unauthorized users to steal the keys needed to decrypt secured traffic or masquerade as network servers. The nShield HSM appliance's tamper-proof design also provides significant physical security in addition to the logical security protecting the keys.

Use Case 2: Apply Strong Encryption and Certificate Signing for All Outbound Traffic

Challenge

Translating organizational policy into security rules and uniformly and consistently applying them to all outbound traffic takes time and expertise. Without security policy enforcement, the network depends on personnel and training to mitigate risk.

Solution

Secure the private key of the forward trust certificate that signs certificates in SSL/TLS forward proxy operations with Entrust nShield HSMs. The Palo Alto Networks NGFW will then send the certificates that it generates during such operations to the Entrust nShield HSM for signing before forwarding them to the clients.

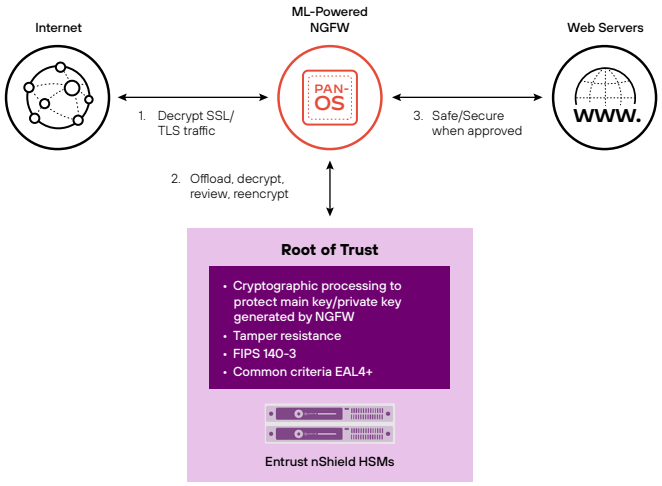

Figure 1. Entrust nShield HSM creates a certified root of trust to safeguard cryptographic keys that Palo Alto Networks NGFWs use

About Entrust

Entrust fights fraud and cyberthreats with comprehensive identity-centric security that protects people, devices, and data. Our solutions help enterprises and governments safeguard critical systems from every angle, enabling secure onboarding and issuance, providing everyday identity protection, and empowering them with 360-degree visibility and orchestration across keys, secrets, and certificates so they can transact and grow with confidence. Building on our decades as a pioneer and innovator in establishing trust, Entrust has a global partner network and supports customers in over 150 countries. For more information, visit www.entrust.com.

About Palo Alto Networks

As the global cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42®. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at www.paloaltonetworks.com.

paloalto® NETWORKS | ENTRUST SECURING A WORLD IN MOTION

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

parent_pb_entrust-nshield_102925