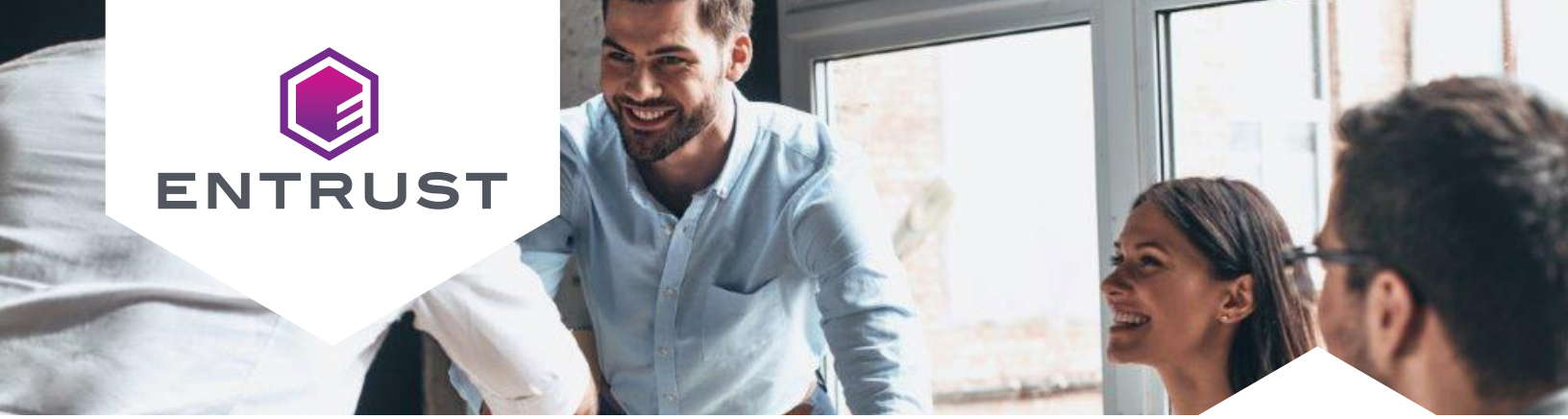

Entrust and Palo Alto Networks enhance encryption key security

Protecting your entire network security system's root of trust

HIGHLIGHTS

- Secure keys within carefully designed cryptographic boundaries using robust access control mechanisms so keys are only used for their authorized purpose
- Ensure key availability by using sophisticated management, storage and redundancy features to guarantee they are always accessible when needed by the firewall
- Offer a robust FIPS 140-2 Level 3 certified cryptographic platform
- Facilitate auditing and compliance with data security regulations
- Integrates with PA-3000 Series, PA-3200 Series, PA-4000 Series, PA-5000 Series, PA-5200 Series, PA-7000 Series, and VM-Series firewalls and on Panorama (virtual appliance and M-Series appliance)

The problem: increasingly interconnected organizations are vulnerable to attacks

Organizations today are increasingly interconnected and depend on this interconnectivity and the cloud to conduct business. While this concept of the interconnected enterprise has taken off and improved business acceleration and agility, it has also surfaced increased exposure to data security risks. To reduce these risks, next-generation firewalls have emerged as a must-have for today's organizations.

The challenge: delivering interconnectivity and the cloud while protecting sensitive data

Next-generation firewalls can block, detect and prevent attack. Often, they also include the encryption of content to ensure validated connections and protect the data's confidentiality and integrity. While encryption is a great start, storing encryption keys outside of a cryptographic boundary can leave an organization vulnerable to attacks. To ensure the security of valuable cryptographic keys in an auditable and proven way, hardware security modules (HSMs) should be used. An HSM will provide an unassailable root of trust that greatly enhances network security.

The Solution: Palo Alto networks and Entrust nShield HSMs

Palo Alto Networks® Next-Generation Firewall integrates with Entrust nShield® Connect hardware security modules (HSMs) to enhance the security of the master key used to encrypt all private keys and

Entrust and Palo Alto Networks enhance encryption key security

passwords. Deployed on-premises or as a service, nShield HSMs also safeguard and manage private keys used in the SSL/TLS decryption process – providing a root of trust that enhances the complete network security posture. Encryption keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromising of critical keys. HSMs are the only proven and auditable way to secure valuable cryptographic material. The combination delivers an auditable method for enforcing security policies that underpin critical components of an enterprise's network security system. By providing a mechanism to enforce security policies, and a secure tamper-resistant environment for the encryption and decryption of passwords and keys, customers can protect the root of trust of their entire network security system.

Why use Entrust nShield HSMs with Palo Alto networks next-generation firewall?

Entrust nShield HSMs protect privileged account keys and passwords in a dedicated hardened environment. Keys handled outside the cryptographic boundary of certified HSMs are significantly more vulnerable to attacks, which can lead to disclosure of confidential information. HSMs are the only proven and auditable way to secure valuable cryptographic material. HSMs:

- Secure keys and certificates within carefully designed cryptographic boundaries that use robust access control mechanisms so keys are only used for their authorized purpose
- Ensure availability by using sophisticated key management, storage and redundancy features to guarantee keys are always accessible when needed
- Deliver high performance to support increasingly demanding transaction rates
- Comply with regulatory requirements for public sector, financial services, and enterprises

nShield Connect is a high performance, network-attached HSM for high-availability data center environments. nShield as a Service is a subscription-based, high-performance option that offers greater flexibility and cost-effectiveness.

Palo Alto networks

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets.

www.paloaltonetworks.com

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com