WHITE PAPER

PENSANDO

Pensando IPsec Solutions

Overview

Virtually every poll of IT executives reveals that security is one of the top three concerns in their data center planning and operations. While there are a dizzying array of security tools and products on the market, encryption is widely regarded as one of the most powerful weapons against unauthorised information disclosure, access or alteration. Client-server encryption using SSL/TLS has become ubiquitous across the Internet, but the rollout of encryption *inside* the data center has been slow. This paper describes the challenges associated with adopting East-West encryption, and how Pensando has addressed them with the **Distributed Services Platform**.

Security Challenges

The threat landscape for computing infrastructure has changed rapidly over the last decade. When it comes to data center security, the assumption that it is a "walled castle" with all threats coming from the outside is no longer viable. Malicious software on the inside of the data center or forged credential attacks can allow attackers to search for - and copy - valuable information, such as intellectual property, credit card numbers and Personally Identifiable Information (PII). The 'Best Practices' mitigation strategy is to always encrypt sensitive data before it leaves the server, so that it becomes harder for malicious attackers to access the information.

However, several challenges have limited workable solutions in today's data centers:

- Data encryption functions are CPU and memory intensive. It takes considerable host server resources to encrypt sensitive data. According to one study[1], it takes 7 CPU cores to encrypt a 100 Gbps stream. Doing so in a generic CPU also introduces higher latency for data transmission, which can be impractical for delay-sensitive business applications.
- There can be tens of thousands of workloads in a large enterprise data center. Determining which application is talking to which resource, and structuring the right encryption policy across the entire data center, is a daunting challenge for administrators. Many encryption solutions have no way to integrate with orchestration tools that assign and re-locate workloads.
- Encryption across the data center fabric interferes with traditional network monitoring approaches, rendering packet contents opaque, which limits many troubleshooting tasks. Historically, data centers have relied on analytics from the Top of Rack (TOR) switch or other "Collector" appliances in the network. With encrypted traffic, these tools have limited visibility beyond the outer header, impacting among other tasks the ability to track application vs. storage traffic, or identify congestion points.
- Application environments for enterprise data centers have also become more diversified, using approaches such as hypervisors versus bare metal, or Kubernetes Containers versus VMs. Finding a single encryption solution that fits all of these environments is very difficult.

Pensando's Solution

To solve all of these challenges, the Pensando Distributed Services Platform delivers high-performance encryption services at the server edge for any traffic entering and leaving the server. Crypto functions are implemented entirely on the Pensando Distributed Services Card (DSC) residing in each server, so enabling encryption on all traffic has no impact on the server CPU and—unlike fixed appliances—encryption resources scale naturally as your data center footprint grows.

[1] "AES-NI SSL Performance", https://calomel.org/aesni_ssl_performance.html

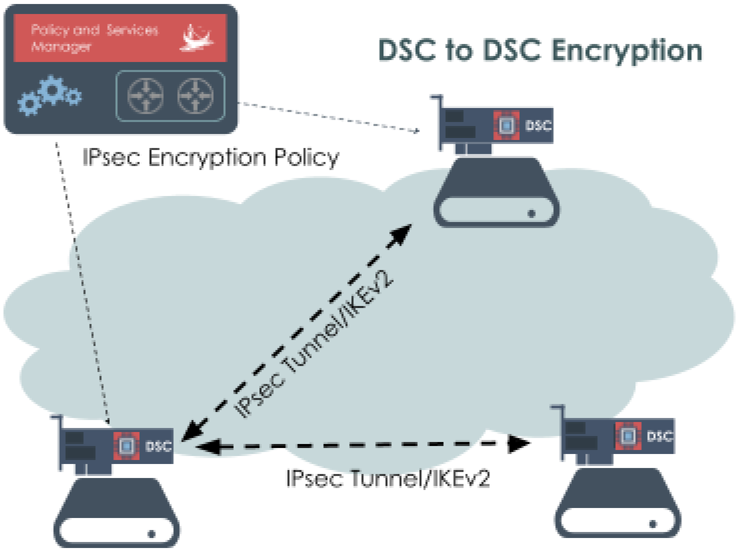
Solution Benefits

- All network traffic encryption/decryption, handshaking and key management is fully implemented in the DSC, requiring no crypto awareness on the x86 compute platform and creating a clean separation between server workloads and network encryption
- The DSC's integrated hardware acceleration engines deliver line-rate encryption; in addition, the DSC can provide other advanced services "chained" before or after the encryption processing.
- The ability to determine which flows need to be encrypted can be dynamically controlled via the Pensando Policy and Services Manager (PSM) for the entire data center—and since the PSM includes northbound REST APIs, any number of third-party tools can be used to easily configure these encrypted paths.
- In the DSC, since telemetry (both flow statistics as well as flow TAP/Mirror capability) takes place on the plaintext data *before* flows are encrypted, full visibility for any flow can be achieved when needed, even while the flow privacy remains protected across the data center fabric.
- Because the encryption functions are provided on the DSC completely independent of the host server, the solution works seamlessly across bare metal, virtualized, containerized or other non-standard operating environments.

IPsec Encryption Deployment

East-West encryption between servers (DSC to DSC) in the data center is one of the principal IPsec deployment use cases that the Pensando solution supports.

- IPsec key management is handled by the standard IKEv2 protocol running on each DSC. The IKE protocol authenticates DSC peers, negotiates keys and maintains the Security Associations (SAs), including rekeying on configurable time intervals.
- The Pensando PSM is responsible for authentication credential and encryption policy management, as well as distributing encryption rules to all DSCs. Rules can be configured down to workload-level granularity. For example, an Admin may specify that only traffic between certain workloads needs to be encrypted, while DNS and DHCP packets will be transferred to DNS/DHCP servers in clear text.
- The PSM's secure REST API provides partner integration points for Policy configuration/synchronization via 3rd party tools.



Encryption Services Architecture

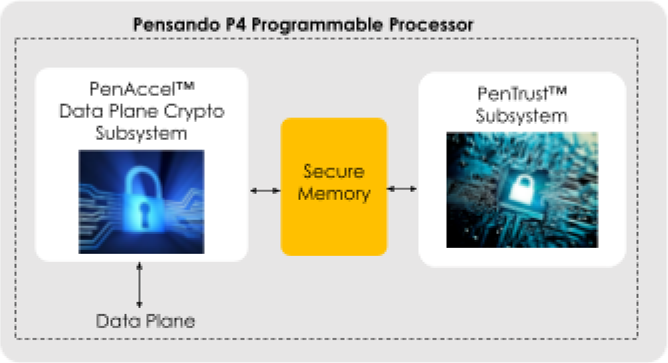
The IPsec data path as well as handshake and key management elements are implemented within the DSC, assuring an extremely high level of security, as both keys and sensitive encryption policies are maintained inside the secure perimeter of the DSC ASIC. The PenAccel™ subsystem implements high-performance hardware-based crypto acceleration in the DSC data path to provide IPsec encryption services at line speed (25Gbps or 100Gbps). The on-chip ARM subsystem runs the crypto handshake and key management control plane for the associated crypto protocol (e.g. TLS handshake or IKE for IPsec).

The default ciphersuite for IPsec ESP operation is AES-GCM-256, providing very high security, CNSA-compliant encryption and payload integrity and authentication.

In order to support very high crypto connection rates, hardware acceleration of both public key and symmetric encryption algorithms is available to the ARM subsystem, including RSA, Elliptic Curve, and Diffie Hellman. In addition, a high-grade entropy-based random number generator, compliant with NIST SP 800-90A/B, is used.

Platform Security

The *PenTrust* subsystem is the Root of Trust (RoT) for the Pensando Programmable Services Processor. PenTrust is the first subsystem to boot at power-on or hardware reset from an immutable embedded ROM, making it the first link in the Secure Boot Chain of Trust. The firmware for the PenTrust subsystem is burned in ROM during ASIC manufacturing and cannot be modified or tampered with once it is programmed. Together with a chip-unique key and identity, the PenTrust subsystem validates all code that runs on the DSC with a digital signature.


Pensando P4 Programmable Processor
PenAccel™ Data Plane Crypto Subsystem
Secure Memory
PenTrust™ Subsystem
Data Plane

Security Compliance and Certifications

The Pensando Distributed Services Platform is designed from the ground up with comprehensive security in mind… from the unique features in our silicon to the carefully designed and validated software. This enables Pensando's solution to be compliant with the toughest security certifications in the industry. These certifications are often baseline requirements for Federal government systems and highly regulated industries, such as financial services and healthcare.

- FIPS 140, level 2 compliance
- CNSA-compliant IPsec crypto suites for US Federal Government applications
- NIST SP 800-90A compliant hardware random number generator
- NIST CAVP (Cryptographic Algorithm Validation Program) certified crypto algorithms

Summary

The Pensando Distributed Services Platform delivers line speed encryption services with absolutely zero impact on the server CPU, enabling widespread deployment of East-West security throughout the data center. With its comprehensive secure platform architecture and integrated hardware root of trust, this solution enables enterprises to meet regulatory compliance requirements while reducing their management OpEx costs.

About Pensando

Founded in 2017, Pensando Systems is pioneering distributed computing designed for the New Edge, powering software-defined cloud, compute, networking, storage and security services to transform existing architectures into the secure, ultra-fast environments demanded by next generation applications. For more information, please visit pensando.io