Hewlett Packard Enterprise

Check if the document is available in the language of your choice.

HPE PROLIANT SECURITY—DATA IN MOTION WITH PENSANDO

Data is the new currency and when it comes to security, customer information and other sensitive data are those that keep most CSO's up at night. Hewlett Packard Enterprise is providing a set of solutions to address data security at various stages: data at rest, data in motion, and data in execution. In this document, we cover HPE solution for when the data is transferred from data at rest (in a storage or local server) to another node within WAN. This solution consists of a robust HPE ProLiant server and the Pensando card (from here on, referred to as the solution or our solution).

BACKGROUND

Connected devices are reaching 35 billion by end of 2021 and produce enormous amounts of data at the edge.[1] Traditionally, this data would be transferred to servers in the data center. This data could include sensitive information such as credit card transactions, patient healthcare records, government data, and so on that must be protected from intruders.

The previously mentioned paradigm is shifting from edge to core where most of the processing is occurring at the edge instead of centralized data centers. Therefore, the traditional approach based on appliances and point solutions is no longer effective. The traditional approach of centralized data centers adds latency and represents a single point of failure in server-to-server interactions. It adds cost to the data centers and creates complexity to scale-given massive data growth; however, managing policies implemented in the appliances are difficult. In addition, a significant part of the servers' CPU power is used for network services management purposes instead of serving the business.

These new, distributed, compute-at-the-edge architectures deploy microservices in containers and virtual machines. Therefore, the traditional perimeter security (firewall between the data center and the internet) is often inadequate. With a majority of network traffic now taking place within the data centers (east-west), the granular security inside the data center is to isolate specific hosts from each other. Security breaches now happen increasingly inside the data center, where the traditional security solutions are less effective, and breaches take a long time and high cost to detect. This lack of agility to detect a security breach could result in damage to the brand, bad publicity, data recovery, and outages or downtime.

HPE has been partnering with Pensando to help address these problems. Our solution uses a Distributed Service Platform (DSP), which is essentially a programmable edge computing accelerator, based on Distributed Services Card (DSC). DSC, with its pre-installed software, implements the security and network services with the centralized Policy and Services Manager (PSM) software through which security policies are defined and provisioned. The PSM is also the dashboard for network monitoring.

[1] "How Many IoT Devices Are There in 2021? [All You Need To Know]," TechJury, 2021

In summary, the benefits of our solution are listed as follows:

- It protects the smallest entity such as a single VM or a single container and isolates it from the rest of the network. It can be moved across servers without impact via microsegmentation.
- It provides for secure, high-speed, east-west traffic protection.
- It lowers TCO: compute resources are freed from running network security (that is, DSP software runs on DSC's silicon).
- There is no need for dedicated appliances for running security functions.
- It provides high visibility over network and security services through always-on telemetry, deep observability, and centralized management. This contributes to reducing the time to detect a security breach and Mean Time To Recover (MTTR).
- It allows to manage and control policies centrally.
- It provides advanced network services such as Load balancer and Encryption Offloading as described next.

ENCRYPTION OFFLOADING CAPABILITY

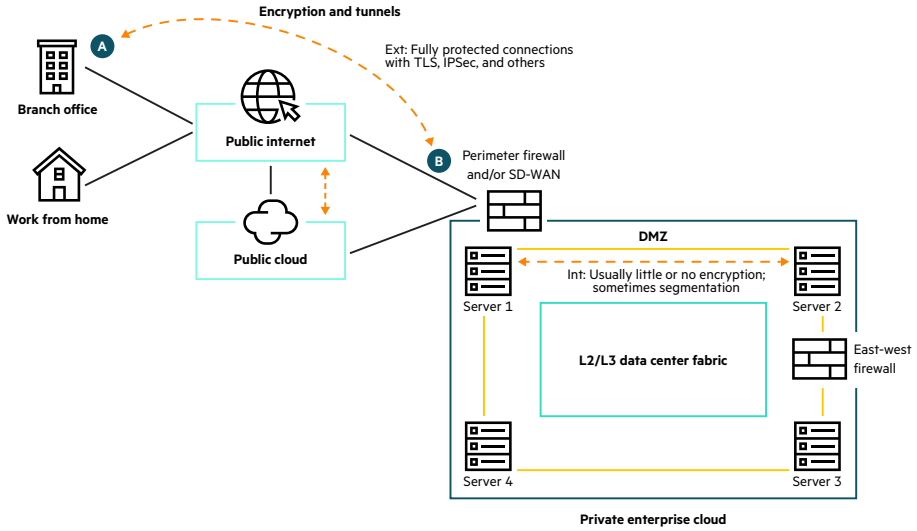


FIGURE 1. Typical network encryption in today's environment

We are all very familiar with encryption of flows over the public internet or when accessing or communicating between workloads within the public cloud. We rarely run a browser without the lock symbol showing the connection is secure over a TLS encrypted link. Unfortunately, the same cannot be said for connectivity inside a modern enterprise network or hybrid cloud. Rarely is the traffic encrypted when moving from one server to another either across or within the data center. The problem is exacerbated as today's private clouds are exhibiting more the characteristics of a public rather than a private cloud. Illegal access to enterprise clouds has become rampant. For example, the majority of the time, credentials to gain access are phished from end users working outside the Data Center (DC) in ransomware attacks. The result is that the third-party foreign entities gaining access and residing within the private data center. It is difficult to detect that an intrusion has occurred. One or two malevolent users are dormant among thousands of other legitimate users.

One of the proposals is to encrypt data in-flight between servers. Encryption prevents visibility to critical data moving between servers. Distributed firewalling and segmentation could be required for a full networking solution.

To implement the proposal, IPSec could be utilized. IPSec is a security technology that allows encryption of data between two endpoints thus obfuscating the communication to third parties. Our solution supports IPSec between two DSCs. The aspects of the tunnel between the two endpoints are automated. Asymmetric keys are generated between endpoints using the IKEv2 protocol (Diffie-Hellman) and data entering the IPSec tunnel is automatically encrypted and decrypted on both sides with generated symmetric keys. These keys are automatically rotated periodically to enhance security. The tunnel is additionally secure because the seed keys (private keys) are generated from unique silicon (on the chip), and it only operates when that unique card is present. This obviates the risk of stealing credentials.

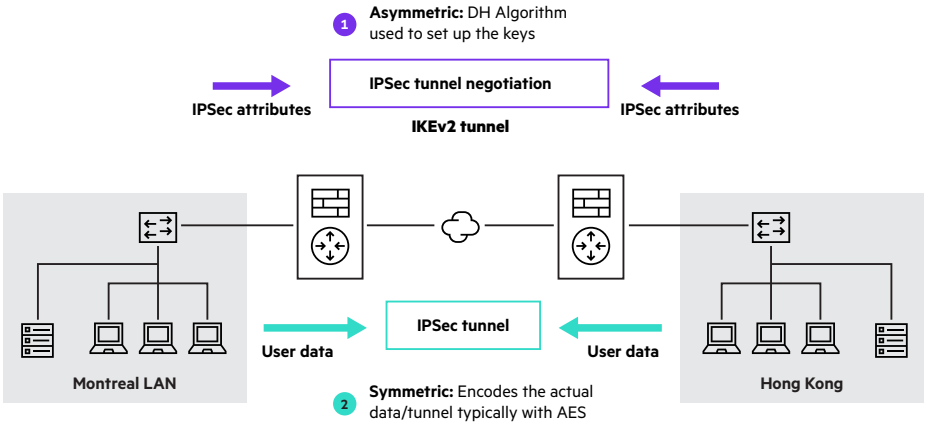


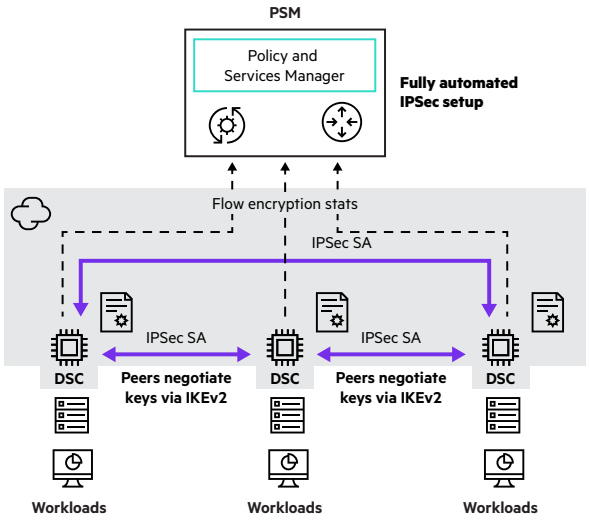
FIGURE 2. IPSec: Symmetric and asymmetric keys

Our solution currently supports AES-256 GCM and ECDSA-P384. We plan to support SHA-1, SHA-2 (SHA224, SHA256, SHA384, and SHA512) and AES variants such as GCM, CCM, and CBC as well as elliptic curve encryption based on P-521 and Curve25519 in the future releases of our solution.

The advantage of this solution is mainly offloading CPU encryption/decryption functions from the rack server CPUs. Therefore, there is no impact on the server CPU as the offloading card contains its host RISC cores with encryption datapath. Furthermore, our solution can capture both encrypted and unencrypted data from the link since DSC sits on the encryption path. As a result, it has direct access to the unencrypted data, so data monitoring tools such as Packet Capture can be easily run in parallel and solving the problem of diagnosing data issues which have been a major reason for not implementing data-in-motion in-flight encryption.

Today, data-in-motion flows are book-ended between two HPE servers, which truly provide workflow security across geographically separated locations.

Since the encryption protocols are open standard, encryption from one end, HPE server running VM or container, to a distant container or VM on a public cloud or a branch office server is possible.



Admin creates the workload-specific IPSec policy. After that, the IPSec setup is fully automated:

- DSCs authenticate to each other using the DSC certificate based on the IKEv2 protocol
- AES-GCM keys are negotiated directly between DSCs using IKEv2
- Flow encryption stats are reported back to PSM
- Supports CNSA cipher suite
  - AES-GCM 256, ECDSA-P384
  - Ready for FIPS 140-2, Level 2

FIGURE 3. Security and encryption

CONCLUSION

HPE ProLiant servers DL325, DL365, DL360, and DL380 have qualified Pensando card, which provides data in motion security solutions with a host of other advanced features with virtually zero impact on the host server CPU. Furthermore, this HPE solution is available as a capital expenditure (CAPEX) as well as an operational expenditure (OPEX) deployment model through HPE GreenLake. It provides business agility, IT simplification, and a lower TCO.

LEARN MORE AT

hpe.com/servers

Contact
For more information, email computesecurity@hpe.com

a50004732ENW, August 2021