Use Case: Workload Shield

CoIP Enclave Enables Workload Shield

The CoIP™ (Cloud over IP) platform empowers enterprises to shield workloads with CoIP Enclave on demand across multicloud and enterprise datacenters. CoIP Enclave is the next-generation cloud security technology enabling enterprises to build their software defined perimeter for hybrid cloud and multilcloud in a completely different way without interfering, yet leveraging existing network and security infrastructure.

The CoIP Workload Shield solution hides and shields a computing environment for an application by closing all ports on the endpoints and encrypting all transport into and out of all endpoints. An application running in the Enclave using this solution can communicate with any public or private IP addresses in the CoIP Enclave, while the entire workload remains hidden on the Internet. The transport can be WAN or LAN connections which can be SSL encrypted. The following figure illustrates workload shield.

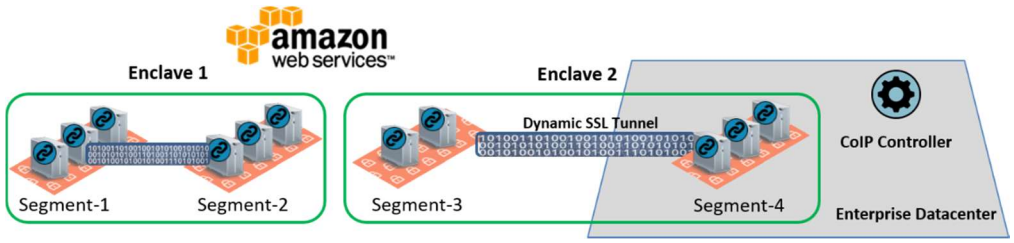

Figure 1: Workload Shield

The application running in a CoIP Enclave with the Workload Shield solution minimizes its cybersecurity attack surface in a global cloud environment. Additionally, other features like Application Interlock and End-to-end encryption can be deployed within Enclave for defense-in-depth.

Key Features of Workload Shield

- CoIP Enclave
- End-to-end Encryption

Key Benefits of Workload Shield

- Minimizes cyber security attack surface
- Helps enterprise to achieve security compliance
- Works in any cloud