Use Case: Defense in Depth

CoIP Enables Defense-in-Depth

The CoIP™ (Cloud over IP) platform offers numerous advanced security capabilities through a software defined Enclave. These are separate and independent security features that can be deployed as standalone or together to protect application workloads in any cloud. CoIP defense-in-depth includes end-to-end encryption, security access broker for network access, micro-segmentation, application interlock, adaptive learning and end-to-end network encryption. The following diagram depicts defense-in-depth deployment typically used in enterprise on-prem.

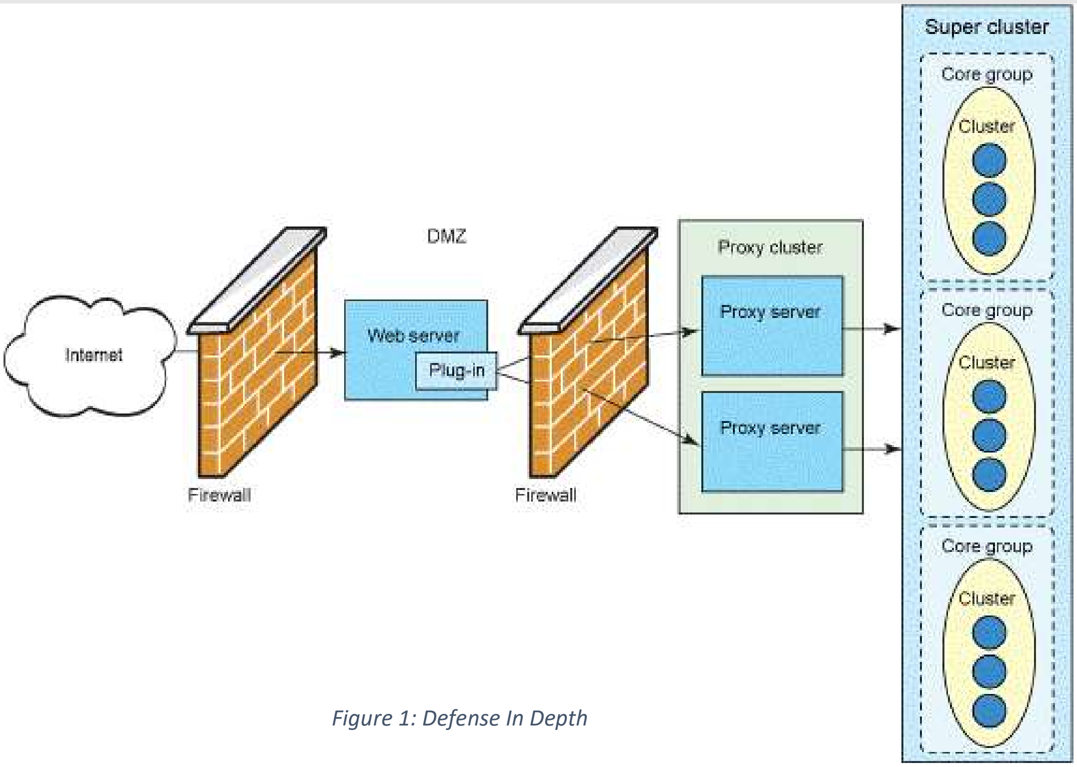

Figure 1: Defense In Depth

CoIP Defense-in-Depth solution provides various advanced infrastructure security capabilities as part of the CoIP Enclave. Together, a CoIP Enclave with these security capabilities provides an orthogonal protection vector around the application workloads in any cloud. The infrastructure security capabilities in the defense-in-depth solution include security broker for network access, micro-segmentation, Application Interlock, and Adaptive Learning and end-to-end network encryption. Micro-segmentation automatically generates security rules for the endpoints in the enclave based on the unified security policy specified in the central CoIP Controller for a specific Enclave. The automatic rule generation works seamlessly with the cloud orchestration layer for elastic security.

Application Interlock allows users to specify a list of software applications that are allowed to access CoIP Enclave which is an overlay enclave for isolated applications across enterprise networks and multiclouds. Any application that is not included in the list, including any malicious software or cybersecurity attacking tools or even the popular OS commands used by hackers are blocked and notification messages are sent for warning and investigation.

Adaptive Learning allows InfoSec teams to learn security rules automatically and recursively to protect applications that are already in production without disruption. This capability bridges the enterprise operations and the InfoSec requirements in a cloud automation environment. This capability also helps InfoSec team to insert security policy to the DevOps flows.

Key Features of CoIP Defense-in-depth

- Security Broker for Network Access
- Micro-segmentation
- Adaptive Learning for security policy automation
- Application Interlock
- End-to-end Network Encryption

Key Benefits of Defense-in-depth

- Lowers barrier to cloud adoption
- Empowers InfoSec to take control of security in cloud
- Easy and quick deployment
- Consistent security policy across any cloud
- Avoid cloud provider lock-in
- Help enterprise to achieve security compliance