CoIP Enclave™

Software-Defined Perimeter with Secure Remote Access

Connect vs. Protect – How Do Enterprises Balance Both?

In the new digital transformation era, enterprises increasingly need to grant access to security-sensitive applications and data to distributed parties, including employees, vendors, partners, and even customers. However, in order to defend against external as well as internal cybersecurity attacks, these sensitive applications and data are protected behind layers of firewalls in a secure zone. How can enterprises choose between securing these critical assets and providing access?

Conventional security methods rely on static network segmentation and isolation. Changing firewall, ACL, VLAN/VXLAN and routing rules to accommodate access requests is too time-consuming, resulting in project delays and loss of business agility.

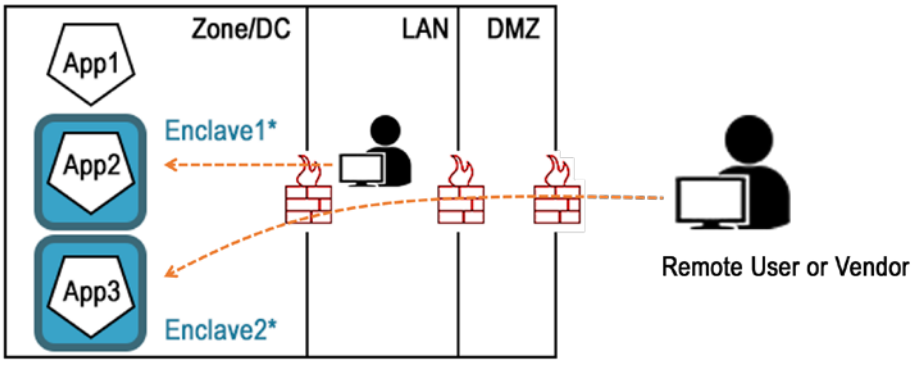
Enterprises need new security solutions that protect critical application and data elastically; capable of shielding assets without impacting user access.

Zentera's SDP Combines Flexible Segmentation with Granular User Access Control

Zentera's CoIP Enclave™ solution creates a Software-Defined Perimeter (SDP) that wraps authenticated endpoints (i.e. VMs, containers, bare metal servers etc.) into a single unified network. All machines inside the SDP are effectively isolated from the outside endpoints, even on the same subnet.

When the application development or operations environment is placed inside a CoIP Enclave in a secure zone behind firewalls, Zentera's patented CoIP® (Cloud over IP®) technology is able to render instant secure access without opening the corporate firewalls or changing the network routing. Applications and data can be effectively micro-segmented in the back end, away from other applications on the same network.

Given multiple applications deployed behind enterprise environments, multiple CoIP Enclaves can be dynamically deployed to protect and connect all applications to their respective users. Independent routing and security policies can be easily provisioned and implemented in each Enclave dynamically, on top of the complex physical environment. Using Zentera's CoIP Enclave, enterprises will be able to achieve their IP protection, security, and operational efficiency goals.



Enterprise On-Premises

CoIP Enclave Features

- Application-based workload isolation
- Micro-segmentation for network controls
- Network-level and VDI-based user access options
- CoIP overlay virtual addressing

CoIP Enclave Benefits

- Securing application workloads dramatically reduces security attack surface
- Installs without changes to legacy network and security infrastructure
- Enhanced operation productivity with elastic overlay fabric
- Avoids re-IPing of applications overlapping address ranges

 © 2018 Zentera Systems, Inc. All Rights Reserved.