CoIP Cloud Ready Enclave

Product Overview

Enterprise applications are typically coupled with underlying network and security infrastructure. Both network and security infrastructure are static in nature and unable to flow application when it moves from enterprise datacenter to cloud. Additionally, cloud breaks enterprise security model based on perimeter and network infrastructure. Therefore, finding a right solution that allows enterprises to be cloud ready while maintaining security and compliance is challenging.

CoIP Cloud Ready Enclave™ enables enterprise workload migration into the cloud by decoupling enterprise workloads from their existing network and security infrastructures and makes the workloads dynamic and ready for cloud migration. Cloud Ready Enclave uses the CoIP® (Cloud over IP®) Platform, which secures workloads in the multicloud ecosystem by connecting them through a unified virtual overlay network. In addition to enabling enterprise workload migration, the Cloud Ready Enclave also migrates the enterprises' existing security policies, and offers micro-segmentation, encryption and application interlock, a feature that only permits specific applications to access the CoIP overlay network. Lastly, the Cloud Ready Enclave offers adaptive discovery, a feature that identifies applications on compute endpoints to automate the application interlock process. CoIP's security can be unified with its virtual network overlay. The combined CoIP platform shields production workloads and cloud endpoints.

CoIP Cloud Ready Enclave

The CoIP Cloud Ready Enclave (CCRE) solution allows enterprises to easily prepare workloads and make them ready to move to the public cloud. CCRE decouples applications from the underlying on-premise physical network and security infrastructures. Using the CoIP Network-in-Motion™ and CoIP Security-in-Motion™ capabilities, workloads can be simply moved between clouds or datacenters while maintaining and extending secure connectivity between the enterprise and the hybrid cloud.

CCRE consists of a CoIP Controller™, CoIP Endpoints™, CoIP Edge Gateway and Zentera Network Switch (ZNS). Endpoints can be VMs, servers, and containers.

Features

- Virtual hybrid network across multiple cloud domains
- Private routing plane and chamber firewall for application shield across outsourcing ecosystem
- CoIP endpoint security via OS environment protection and application interlock along with network setting monitoring and enforcement
- Cloud Connectors convert cloud APIs to mouse clicks
- Data encryption and automated synchronization across domains
- Secure remote terminal access without IP leakage

Benefits

- Ease of management with unified network console across enterprise and cloud
- Full enterprise control in any cloud datacenter
- Enterprise protection without altering corporate perimeter security & compliance
- Remotely shield hybrid cloud workloads in any cloud
- Unified security for cloud endpoints across cloud ecosystem
- Virtual network segregation for cloud applications on top of shared corporate networks
- Extremely fast deployment— within days, not months or years

Product Specifications

CoIP Controller

The CoIP Controller is the management portal for the CoIP platform. All policies and configurations are implemented centrally in the controller and pushed to the endpoints for enforcement. The CoIP controller enables and manages Application Profiles – which provision virtual infrastructures and security policies across the multicloud – to define the cloud ready enclave using mouse clicks and programmable cloud APIs. The Controller can be a physical appliance or VM running in public and private clouds, or running in the enterprise datacenter.

Table 1: CoIP Controller Specifications and Performance for Physical Appliance

Hardware Appliance	Specifications	Performance
ZCA-1000	x86 Server with 4-core, 2.1GHz and 8G RAM, 2 1G NIC and 500G Storage	1G throughput and 10k endpoints
ZCA-5000	x86 Server with 12-core, 2.4GHz and 16G RAM, 4 1G NIC and 500G Storage	5G throughput and 15k endpoints
ZCA-10000	x86 Server with 12-core, 2.4GHz, 16G RAM, 2 10G NIC and 500G storage	10G throughput and 30k endpoints

Table 2: CoIP Controller Specifications and Performance for Virtual Appliance

VM Configuration	Cloud Platform	VM Details	CoIP Endpoint Support
C3.xlarge	AWS	4 cores, 7.5G RAM, 2 x 40G SSD	Up to 5,000
C3.2xlarge	AWS	8 cores, 15G RAM, 2x 80G SSD	Up to 10,000
C3.4xlarge	AWS	16 cores, 30G RAM, 2 x 160G SSD	Up to 20,000
Basic A3	Azure	4 cores, 7G RAM, 120G Storage	Up to 5,000
Basic A4	Azure	8 cores, 14G RAM, 240G Storage	Up to 10,000
D14	Azure	16 cores, 112G RAM, 800G Storage	Up to 20,000

CoIP Endpoints

CoIP endpoints are the computing resources which sit on the cloud enclave and are part of a common network plane and security policy. Endpoints can be VM, physical sever or containers. zLink is an agent of CoIP controller which runs on endpoints and registers with CoIP controller to be part of CoIP enclave.

Table 3: CoIP Endpoint support Matrix

OS Type	Supported Version
Microsoft Windows	Windows 7, 8 and 10 Windows Servers 2008, 2012,2016
Canonical Linux	Ubuntu Servers 16.04, 14.04, 12.04
Red Hat Enterprise Linux	RHEL 4, 5, 6 and 7
CentOS	CentOS 6 and 7
SUSE Enterprise Linux	SELS 10.3, 10.4 and 11.2
Open SUSE Linux	Open SUSE 10.3 and 12.2
Amazon Linux	Amazon Linux AMI 2016.09, 2017.03

CoIP Edge Gateway

The CoIP Edge Gateway acts as a gateway to non-CoIP networks. It is a layer 5 device that performs NAT and forwarding functions. The gateway does not provide routing functionality. Edge Gateway can be physical appliance or VM.

Table 4: CoIP Edge Gateway Specifications and Performance

Form Factor	Specifications	Performance
Physical	x86 Server with 6-core, 2.4GHz and 12G RAM, 2 1G NIC and 200G Storage	Unlimited connections with 1G throughput
VM	Linux VM(CentOS/Red Hat recommended) with 2 vCPU, 4G RAM and 10G Storage	10 concurrent connection
VM	Linux VM(CentOS/Red Hat recommended) with 4 vCPU, 6G RAM and 20G Storage	30 concurrent connection
VM	Linux VM(CentOS/Red Hat recommended) with 6 vCPU, 8G RAM and 30G Storage	100 concurrent connection

Zentera Network Switch (ZNS)

The CoIP Switch Node performs switching functionality for CoIP packets when CoIP is used for WANs. ZNS supports clustering for scale, performance and high availability. ZNS can be physical appliance or VM running in public and private clouds or in enterprise datacenter.

Table 5: CoIP ZNS Specifications and Performance

Form Factor	Specifications	Performance
Physical	x86 Server with 6-core, 2.4GHz and 12G RAM, 2 1G NIC and 200G Storage	Up to 10k endpoints and 1G throughput
Physical	x86 Server with 12-core, 2.4GHz and 16G RAM, 4 1G NIC and 500G Storage	Up to 10k endpoints and 5G throughput
VM	Linux VM (CentOS/Red Hat recommended), with 6 vCPU, 8G RAM and 30G Storage	Up to 100 endpoints
VM	Linux VM (CentOS/Red Hat recommended), with 12 vCPU, 16G RAM and 50G Storage	Up to 500 endpoints
VM	Linux VM (CentOS/Red Hat recommended), with 24 vCPU, 32G RAM and 60G Storage	Up to 1k endpoints

About Zentera

Zentera Systems, Inc., enables companies to extend production datacenter operations to public, private and managed hosted network domains. The CoIP™ (Cloud over IP™) cross-cloud session solution offers enterprise-grade networking and security for the emerging cloud ecosystem, protecting the new attack surface exposed by remote cloud endpoints. CoIP creates a unified overlay network plane across multiple private and cloud domains that connects dispersed computers, virtual machines and containers. Its agnostic network virtualization can be provisioned in hours over existing IP infrastructure. Based in Silicon Valley, Zentera offers CoIP through select regional channel partners, managed cloud service providers and Ingram Micro.

For More Information

To learn more about Zentera CoIP platform, please contact your local account representative, or visit http://zentera.net