DATASHEET

cCEP

Cloud Certes Enforcement Point (cCEP)

The Cloud Certes Enforcement Point (cCEP) is a cloud-native evolution of the Certes Enforcement Point (CEP), purpose-built for platforms like Amazon Web Services (AWS). Unlike traditional CEPs, cCEP integrates directly with AWS services such as Gateway Load Balancer (GWLB), delivering scalable, high-performance data protection and application segmentation.

FEATURES AND BENEFITS

- Interoperable with CryptoFlow ® Net Creator (CFNC) software
- Up to 1 Gbps encrypted throughput (AWS t3.xlarge, Layer 4 AES-256-GCM)
- Seamless integration with AWS GWLB
- Scale up or down based on traffic demands
- High availability and disaster recovery capabilities
- Visibility of data in transit
- Easy installation and management
- Per-frame/packet authentication

COMPREHENSIVE DATA PROTECTION

- Amazon Virtual Private Clouds (VPCs)
- Hybrid cloud architectures (On-prem to AWS)
- Cloud-based backup and disaster recovery networks
- Secures traffic to and from AWS storage services over protected network paths
- VPC-to-VPC and inter-region traffic protection
- Cloud-hosted VMware backup environments

PRODUCT OVERVIEW

The Cloud CEP (cCEP) represents a significant evolution in data security and content encryption, bridging traditional security with cloud flexibility. Unlike on-premises or virtual appliances, the cCEP integrates directly with cloud-native constructs like AWS Gateway Load Balancer (GWLB), delivering elastic, high-availability encryption and policy enforcement. Designed from the ground up to integrate with cloud services, cCEP leverages the scalability, flexibility, and distributed nature of cloud computing while delivering the proven encryption capabilities of CEPs.

The cCEPs are interoperable with our key management software, CryptoFlow® Net Creator (CFNC), and are easy to install, scalable for any size infrastructure, and simple to manage. With dedicated cCEP deployments, customers experience high encryption throughput without impacting performance.

Scalable and Secure Group Protection

The cCEP uses scalable group protection to provide encrypted, authenticated, low-latency, any-to-any connectivity. Group encryption reduces deployment complexity. It provides multiple logical policy support including point-to-point and hub-and-spoke that is easy to manage. Group protection is used to provide compatibility with highly available network designs, QoS, and support is provided to network monitoring tools.

IP Packet Protection

The cCEP provides full data protection for Certes patented Layer 4 protection to protect the IP packet payload while preserving the original IP header and original TCP/UDP headers including QOS. By preserving the original header and encrypting only the payload, the cCEP protects your data over any IP network. This includes any multi-carrier, load-balanced, or high availability network, and allows Class of Service (CoS) based traffic shaping, to be maintained throughout the network.

Policy Limitations

cCEP supports only Layer 4 policies due to its single-interface cloud deployment model (e.g., via AWS GWLB). Easy Mesh, overlapping subnets, and wildcard networks are not supported. These constraints are enforced by CFNC to ensure accurate policy definition and traffic handling.

Central Policy Management

CFNC is a centralized Quantum-safe key management system using Quantum Key Distribution and Quantum Random Numbers that organizes and streamlines operations while providing you with full control of your security posture. With a user-friendly GUI and drag-and-drop tool, you can define and deploy policies with ease from one central point of control.

Certes Data Protection and Risk Mitigation (DPRM) is

100% data focused, Crypto Agile and Quantum Safe

cCEP

Cloud Certes Enforcement Point (cCEP)

PERFORMANCE

- Supports over 10,000 encryption policies
- *Up to 1 Gbps **
  ** Dependent on packet size of 512 or larger*

ENCRYPTION ALGORITHMS

- AES-256-GCM
- AES-256-CBC

MESSAGE AUTHENTICATION & INTEGRITY ALGORITHMS

- HMAC-SHA2-256
- HMAC-SHA2-512

CLOUD PROVIDER

- Amazon Web Services

COMMUNICATIONS AND MANAGEMENT PROTOCOLS

- Management: HTTPS (via CFNC), SSH2, SNMP v2c/v3, Syslog, CLI, NTP
- Data Plane Support: Protocol-agnostic Layer 4 encryption (TCP/UDP)

INSTALLATION SOFTWARE

- AMI for AWS

DEVICE MANAGEMENT

- CryptoFlow Net Creator
- Command Line Interface
- Out-of-band management
- Supports both SNMPv2c and SNMPv3 (SNMPv3 recommended for secure monitoring and traps)
- Trap support for CPU usage, disk space, policy mismatch
- Hardware-specific alarms do not apply to virtual cCEP deployments
- Alarm reporting for high CPU usage, low disk space, and policy mismatch
- Syslog support for system events
- Health checks via HTTPS
- Auto-scaling support via Target Group configuration
- Integration with AWS GWLB using Geneve

Certes Networks Global Headquarters
300 Corporate Center Drive, Suite 140
Pittsburgh, PA. 15108
Tel: +1 (888) 833-1142
Fax: +1 (412) 262-2574
Certes.ai

To learn more visit Certes.ai

For product enquiries:
info@certes.ai