

CipherEngine Policy & Key Manager

Global Security Policy, Encryption Key, and Device Management

Product Overview

CipherEngine is a global policy and key management solution for network encryption. This easy to use solution scales seamlessly and provides global security management, encryption key generation and distribution, and enforcement point configuration for any Ethernet or IP encryption deployment. CipherEngine offers simplified encryption management without requiring costly changes to your existing network infrastructure.

With CipherEngine you can:

- Centrally manage your encryption deployments over any network
- Monitor and manage encryptors from a single interface
- Make real time changes to security policies
- Generate and dynamically distribute encryption keys based on group policies
- Securely push encryption keys and policies to appliances throughout the network

CipherEngine is three powerful security applications, MAP, KAP, and Appliance Manager, in one easy-to-use solution. This unique combination allows you to easily configure and manage encryption appliances, define the security policies that will be enforced, and then generate and securely distribute the encryption keys and policies to the encryptors. CipherEngine also includes log and audit reporting mechanisms, which allow you to collect and monitor important criteria such as enforcement point status, as well as policy, password and device configuration changes.

CipherEngine Management Authority Point (MAP)

The Management Authority Point, or MAP, is CipherEngine's policy services interface, which provides centralized creation, monitoring and management of network encryption policies.

Policies defined within CipherEngine specify what traffic to protect and how to protect it. As part of the policy definition process, Certes Networks' encryption appliances are assigned to groups, called Network Sets. Each encryptor in a Network Set is given permissions and policies to mirror the logic of network architectures and application flows.

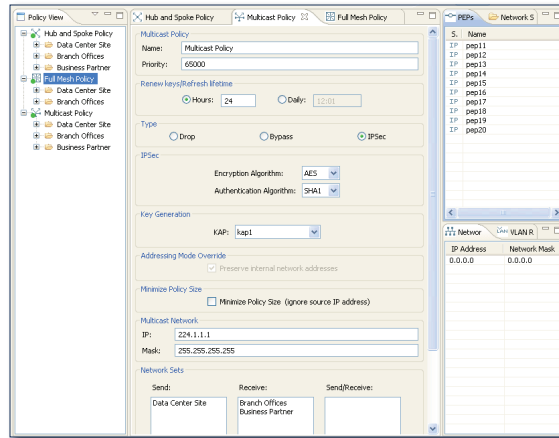
This grouping capability greatly reduces the complexity of large-scale encryption deployments, allows greater deployment flexibility, and enables fully meshed, any-to-any encryption for all network traffic. Policies can use a variety of encryption selectors, such as source or destination IP addresses, source or destination port numbers, protocol ID or VLAN tag ID.

CipherEngine Key Authority Point (KAP)

The Key Authority Point, or KAP, is CipherEngine's key generation and distribution mechanism. The KAP receives the policies from the MAP and then generates and distributes the encryption keys and the MAP policies to the CEPs.

CipherView Appliance Manager

CipherView is CipherEngine's device management application, which controls all configuration aspects of the CEPs, including network configuration, SNMP hosts and syslog servers.



Encryption policies can be deployed and centrally managed from CipherEngine.

PRODUCT SNAPSHOT

- Global security policy control
- Simplified encryption management
- Easy security policy deployment
- Simplified operation and reduced complexity

FEATURES AND BENEFITS

- Security policies for any network
 - Layer 2 Ethernet encryption
 - Layer 3 IP encryption
 - Layer 4 payload only encryption
- Global management
 - Encryption policy enforcement
 - Dynamic encryption key creation and distribution

COMPREHENSIVE DATA PROTECTION

- IPsec site-to-site networks
- MPLS meshed networks
- Metro Ethernet and VPLS networks
- Voice over IP
- Video and Multicast applications
- Support for Public Network Group Encryption

CipherEngine Policy & Key Manager

Global Security Policy, Encryption Key, and Device Management

Policy Generation

- Mesh topologies
- Hub and spoke topologies
- Multicast networks
- Point-to-point connections
- IPsec site-to-site connections

Key Services

- Generates encryption keys associated with policies
- Distributes encryption keys to enforcement points
- Re-key management by period (hours) or daily at a pre-determined time

Distribution Services

- All communications involving policies and keys are secured using TLS and transmitted through the management ports of the enforcement points
- Communications authenticated using X.509 certificates

System Synchronization

- Time synchronization via Network Time Protocol (NTP) version 3, RFC 1035

Minimum System Requirements

- Intel 3.0 GHz Pentium 4
- 140MB available disk space
- 512MB RAM
- Windows Server 2003, Windows XP
- Microsoft Internet Explorer 6 or greater

Supported Encryption Devices

- CEP10 VSE, CEP100 VSE, CEP1000 VSE, and CEP10G VSE
- CEP10, CEP10-R, CEP100, CEP100-XSA, CEP1000
- SG100, SG1002
- ESG100, ESG1002

Device Configuration Services

- Import and export CEP configurations
- Save CEP configurations
- Compare saved configuration with running configuration
- Secure CEP firmware upgrades
- Control user roles and passwords
- Monitor CEP status

Optional Hardened Key Server

Processor

- Quad Core Intel Xeon X3440, 2.53GHz, 8MB Cache Memory
- 8GB (4x2GB) 1333MHz Dual Ranked UDIMM

Dimensions

- Form Factor: 1U Rack
- Height: 1.67" (4.24 cm)
- Width: 17.10" (43.40 cm)
- Depth: 24.00" (61.00 cm)
- Weight: ~ 30 lbs. (13.61kg)

Power

- Redundant power supply (400W)

Ports

- On-Board Dual Gigabit NIC

Internal Storage

- Two 80GB 7200RPM SATA Hard Drives
- Internal slim-line optical drive

Environmental

- Operating Temperature: 10° to 35°C (50° to 95°F) with a maximum humidity gradation of 10° per hour
- Operating Relative Humidity: 8% to 85% (non-condensing) with a maximum humidity gradation of 10% per hour
- Operating Maximum Vibration: 0.25 G at 3-200 Hz for 15 minutes
- Operating Maximum Shock: 31 G for 2.6ms
- Operating Altitude: -16 to 3048 m (-50 to 10,000 ft)

Regulatory

- FCC Part 15 Class A