

# DATA SHEET

## CipherEngine Network Encryption

### Global Security Policy, Encryption Key, and Configuration Management

#### PRODUCT SNAPSHOT

- Global security policy control for any network
- Simplified management of end-to-end data encryption without impacting network operations or application performance
- Organize endpoints into network groups
- Easy security policy deployment across the entire network
- Simplified operation and reduced complexity

#### SOLUTION FEATURES AND BENEFITS

- Security Policies for any network
  - Layer 2 Ethernet encryption
  - Layer 3 IP encryption
  - Layer 4 payload encryption
- Management and configuration
  - Global network security policy enforcement
  - Global encryption key creation and distribution

#### GLOBAL DATA PROTECTION

- IPsec site-to-site networks
- MPLS meshed networks
- Metro Ethernet and VPLS networks
- Voice and Video over IP applications

#### CONTACT INFORMATION

**CipherOptics, Inc.**  
701 Corporate Center Drive  
Raleigh, NC 27607  
Tel: +1.877.878.6655  
Fax: +1.919.233.9751  
info@cipheroptics.com

#### Product Overview

CipherEngine is a global security policy, encryption key and configuration management solution enabling comprehensive end-to-end data protection. Based on an open architecture for data security, CipherEngine takes a simplified approach to network and security management by providing an easy-to-use solution that controls all aspects of a CipherOptics IP, Ethernet or MPLS infrastructure encryption deployment. CipherEngine provides global security policy management, encryption key creation and distribution, as well as, CipherEngine Enforcement Point configuration within a single centralized solution.

#### Policy Services

CipherEngine's Policy Service is the policy management component that can be implemented to secure multiple data paths in redundant networks and complex mesh, hub and spoke, and multicast networks. Policy Services provide centralized creation, monitoring and management, and are used to create and manage the policies that are acted on by the Key Services.

A policy specifies what traffic to protect and how to protect it. Encryption is set by policy definition and can be based on source IP address, destination IP address, source and destination port number, protocol ID or VLAN tag ID. The Policy Service is the tool used to define the filtering criteria specified in the policy. Each policy specifies:

- The enforcement points utilized
- The networks the enforcement points will protect
- The networks in a group
- The action that is to be performed (encrypt, clear or drop)
- The type of traffic the policy affects - IP, Ethernet VLAN, Layer 4 payload policies

#### Key Services

CipherEngine's Key Service generates and then distributes the encryption keys and policies to the Enforcement Point Services, based on the policies generated from the Policy Service.

#### Configuration Services

All device configuration aspects of CipherEngine Enforcement Points, including network configuration, SNMP hosts and syslog servers, are controlled through the Configuration Service.

#### Enforcement Point Services

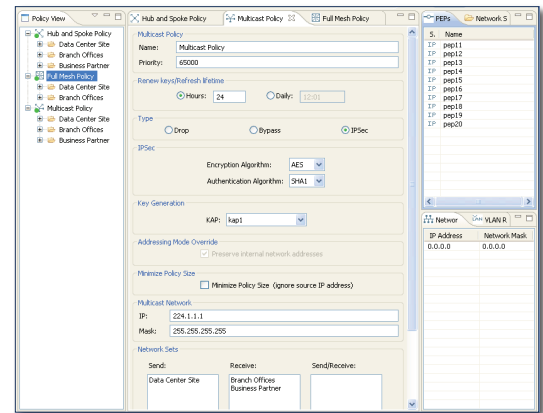
CipherEngine's Enforcement Point Services push the encryption keys and policy rules to the CEPs. The CEPs then encrypt the traffic, send it in the clear or drop it, depending on the policy rules it receives.

#### Monitoring and Reporting

CipherEngine includes log and audit reporting mechanisms, allowing you to collect and monitor key criteria such as enforcement point status, policy changes, device configuration changes, and password changes.

#### Administrative Roles and Users

CipherEngine allows appropriate levels of administrative access to specific users through the separation of roles. Enterprises can restrict or provide different levels of system privileges to specific individuals. CipherEngine provides two system level roles with change privileges (administrative user and operational user), and one monitoring role for read-only access. All user access is password-controlled.



Multiple policies can be deployed and managed centrally from CipherEngine.

### CipherEngine Features and Benefits

Feature	Feature Description	Benefit
Enforcement point configuration management	Quickly and easily configure and deploy enforcement points	Reduce overall configuration time for large or small network deployments
Flexible policy management	Create encryption rules per enforcement point or per network	Quickly and easily deploy network security policies
Single solution for global data protection	Encryption across different network layers	Flexible configuration and deployment
Monitoring	Actively monitor policies and enforcement point status	View overall status from one centralized location
High availability and scalability	Multiple CipherEngine servers can be deployed	Always on, always ready operations
Group policy creation	Group key distribution	Encryption for multicast, load balanced, or VLAN network topologies

### Technical Specifications

#### Policy Services

- Generates network security policies for:
  - Mesh networks
  - Hub and spoke networks
  - Multicast networks
  - Point-to-point connections
  - IPsec site-to-site connections
  - Ethernet frame encryption for Layer 2 networks
  - Payload encryption for MPLS Layer 3 networks.
  - Group policies

#### 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

#### 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

#### System Synchronization

- Time synchronization using Network Time Protocol (NTP) version 3, RFC 1035
- Time synchronization on enforcement points using Simple Network Time Protocol (SNTP), RFC 2030

#### Supported encryption devices

- CEP10, CEP100, CEP1000
- SG100, SG1002
- ESG100, ESG1002

#### Minimum System Requirements

##### Platform

- Intel 500MHz Pentium III
- 86MB available disk space

##### Operating System Support

- Microsoft Windows XP or greater

##### Client Browser

- Microsoft Internet Explorer 6 or greater

#### Optional CipherEngine Hardware Server

##### Processor and Memory

- Dual Core Intel Xeon 3100, 3.0GHz, 1333MHz FSB, 6MB L2 Cache
- 2GB DDR2 PC2 667MHz

##### Dimensions

- Form Factor: 1U Rack
- Height: 1.68" (4.27 cm)
- Width: 17.60" (44.70 cm)
- Depth: 21.50" (54.61 cm)
- Weight: ~ 26.0 lbs. (11.80kg)

##### Power

- Single power supply (345W)

##### Ports

- 2 embedded Gigabit NICs

##### Internal Storage

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

##### Environmental

- Operating Temperature: 10° to 35°C (50° to 95°F)
- Operating Relative Humidity: 20% to 80% (noncondensing) with a maximum humidity gradation of 10% per hour
- Operating Maximum Vibration: 0.25 G's 0-Peak, 3-200 HZ sweep @ 1/2 Octaves/minute
- Operating Maximum Shock: 31G, 2.6ms, 20inch/sec, bottom side
- Operating Altitude: -16 to 3048 m (-50 to 10,000 ft.)

##### Regulatory

- FCC Part 15 Class A, EN61000-3-2 (A1, A2), : EN61000-3-3, EN55022: 1998 and CISPR 22: 1997 Class A, VCCI Class 1, MIC Class A, BSMI, EN55024: 1998 and CISPR 24: 1997, IEC 61000-4-2
- IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-6, IEC 61000-4-8, IEC 61000-4-11

##### Safety

- EN60950-1, First Edition, IEC 60950 1, First Edition (2001), UL/CSA 60950-1, First Edition, EK1-ITB 2000:2003, ISO 9241,ZH1/618:GS-VW-SG7:1997, ISO 13406-2, ISO 7779, MsanPiN 001-96

