Engage Communication

Black•DoorGIG

GIG Encryptor

AES Encryptor for Gigabit Ethernet

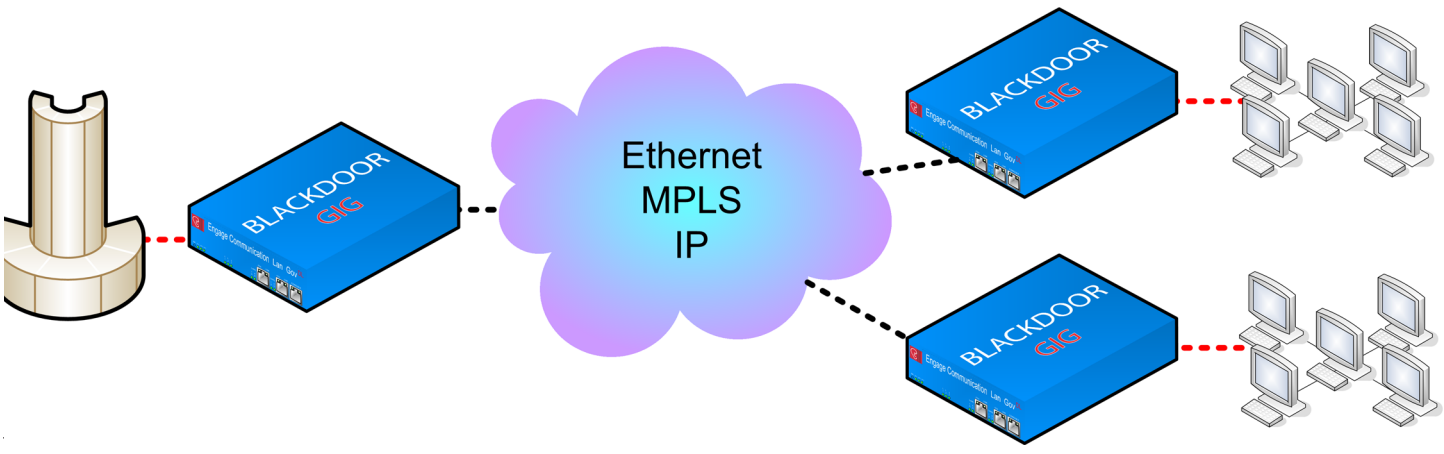
- **Encrypt Layer 2/3/MPLS Payloads**
- **Secure Proprietary Information**
- **Point-to-Point or MultiPoint Architecture**

Encrypt Voice, Video, & Data At Gigabit Speeds

The Black•Door GIG Encryptor supports Point to Point and Multipoint information assurance configurations with unique dynamic keys. The Black•Door GIG Encryptor is designed for gigabit wireline or wireless backbone configurations. The Black•Door meets stringent security requirements while reducing overall network complexity in applications including:

- Department of Defense
- Telecommunications Providers
- Oil and Gas Companies
- Transportation Agencies
- Homeland Security
- Natural Gas & Electric Power Utility Companies
- Banking & Financial Services Institutions
- Public Safety Networks

The Black•Door GIG Encryptor transparently encrypts Ethernet Voice, Video or Data packets, that are destined for a device located on a remote network or a different local network segment. Data packets are AES encrypted at the Link, Network or Transport Layer and then tunneled, bridged or routed to the destination network. At the destination network the packets are decrypted and the original Ethernet packets are securely delivered to the destination Ethernet device.



Engage Communication • 9565 Soquel Drive, Aptos, CA 95003 • Tel: (831) 688-1021 • Fax: (831) 688-1421 • www.engageinc.com

Engage Communication

Black•DoorGIG

Black·Door GIG Standard Features

OSI Layer Encryption

It is important for an external encryption device to be able to handle encryption at multiple layers of the OSI model. The Black•Door GIG Encryptor can interface to all layers with an internal bridge and router and provides secure data encryption at Gigabit throughput levels.

Bridge

Interfaces at Layer 2, non-local packets are encrypted above the MAC layer and then directed to the appropriate destination address by the internal bridge.

Router

Interfaces at Layer 3, packets are encrypted above the Network Layer and then can be dynamically or statically routed to the destination network by the internal router.

Tunnel

Many times network to network security requires an encrypted 'tunnel' carrying Ethernet packets over a pre-defined network path. The Black•Door GIG Encryptor permits user creation of a destination table, encrypts the entire incoming packet, and adds the appropriate destination address for correct network transport.

MPLS

The Black•Door GIG Encryptor can provide "payload only" encryption for MPLS data packets, maintaining the MPLS labels but encrypting the data. It is flexible enough to provide an encrypted 'tunnel' for point-to-point MPLS connections or can encrypt at Layer 2 or Layer 3 or both, easy to configure without any down time for network access equipment.

Advanced Encryption Standard

FIPS approved symmetric encryption algorithm that may be used by U.S. Government organizations (and others) to protect sensitive information.

Management

Key

Automated 256 bit key management configurations ensure timely key transitions and eliminate the operational and maintenance costs of managing an encrypted network with manual key distribution.

SNMP

The Black•Door GIG Encryptor is manageable with SNMP via standard and private MIBs. Large scale deployments of encryption devices with centralized management have made SNMP support a priority.

Technical Specifications

Encryption Algorithm:

- AES 256-bit
- Fully Automatic key management
  - 1 minute to 42 day rekey interval without interruption
- Hardware Random Number Generator
- Full Duplex real time encryption

LAN Network Interface:

- Two 10/100/GB Full/Half Ethernet
- Auto negotiation or Configured Speed and Duplex

LAN Network Protocols Supported:

- IP, TCP, UDP, ICMP
- SSH

System Architecture:

- Point-to-Point
- Point-to-Multipoint

Performance:

- JUMBO Ethernet Packet capability (9KB MTU)
- Full Duplex
- Low latency
- n Process Key Updates

Regulatory:

- CE • Safety -IEC60950 • EMC - CFR 47 Part 15 Sub Part B:2002, EN55022:1994+A1&A2, EN55024, ICES-003 1997, CISPR 22 Level A

Management:

- Console Port for Out of Band Management
- SNMP support (MIB I, MIB II) with configured traps
- Remote config., monitoring, & reset
- SSH

Power:

- 12-30 VDC, 1.0A. • Locking Connector
- Optional -48V 0.25 Amp • Hot Standby

Dimensions:

- Dimensions: 9" (L) x 7.3" (W) x 1.50" (H)
- Optional Medeco Case

TFTP Online Upgrade Capable (FLASH ROMs)

- Fully operational during upgrade

Environmental:

- 0° to 132° F (-10° to 50°C) operating temperature
- Up to 90% operating humidity (non-condensing)
- Optional Extended Temperature Range available