



Datacryptor® Gigabit



The Data Privacy Challenge

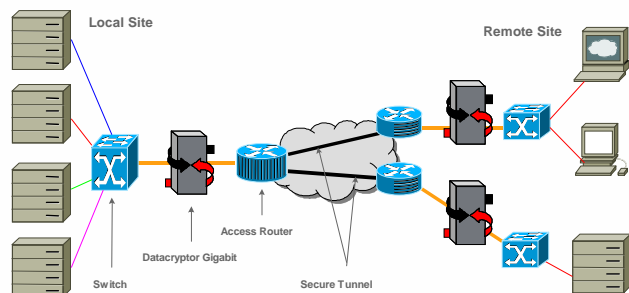
Data security is paramount in today's business environment. Corporate ideas and data – the lifeblood of any business – must be protected from unauthorized access. As enterprise networks migrate to gigabit Ethernet to transport critical applications, the challenges only increase. Transporting corporate intellectual property over a high speed digital infrastructure demands both digital security and high performance.

How do you protect the privacy of your data while it's in transit, without slowing the network to a crawl? The answer begins with Thales e-Security and IPsec.

Securing Data in Transit

Because hackers can easily defeat fiber and dedicated leased lines, a key component of today's security architecture is data privacy during transmission. IPsec is an IETF standard designed specifically to protect data while it is in transit across an untrusted network, providing three levels of security.

- Confidentiality: Keep your data private.**
 IPsec uses industry-standard encryption algorithms to keep data secret: AES, 3DES and DES.
- Authentication: Trust your sources.**
 While encryption is vital, it is equally important to verify the identity of the peer IP gateway that is the source of the data.



The Datacryptor's two gigabit Ethernet interfaces allow it to connect as a bump-in-the-wire. Commonly inserted between two or more trusted enterprise networks, The Datacryptor encrypts and protects data traffic flowing over an untrusted network.

- Integrity: Trust your data.**
 Once communication with a trusted source is established, IPsec prevents data from being altered as it traverses the network.

IPsec Encryption at Gigabit Speeds

The Thales e-Security Datacryptor Gigabit combines the best of breed in security and speed: robust AES or 3DES IPsec encryption processing with unparalleled full-duplex gigabit Ethernet wire-speed throughput. It eliminates costly processing bottlenecks in the network while affordably maximizing the efficiency of existing network resources.

Housed in a tamper-evident chassis, the Datacryptor Gigabit's breakthrough performance is achieved with a unique purpose-built architecture. Its low latency, high-speed encryption is ideal for bandwidth-intensive, latency intolerant applications such as IP-based storage area networking and site-to-site secure tunnels.

Wire-speed throughput

Full-duplex gigabit Ethernet wire-speed AES or 3DES IPsec encryption.

In-transit data security

Data authentication, integrity, and encryption.

Secure management

Remote configuration sessions and security policies are secured with IPsec.

Jumbo frame support

Encrypts jumbo frames without degrading network performance.

Network compatibility

Easily integrates into existing IP networks.

Streamlined IPsec policy definition

Single-screen policy configuration and centralized policy management.

Easy setup and installation

Maximum configuration flexibility combined with easy installation and management.

TECHNICAL SPECIFICATIONS

Device Management

Secure management interfaces (CLI and browser)
Out-of-band management
Secure download of software updates
SNMP v2c MIB managed object support
Optional certificate authentication
CryptoView Device Manager (optional)

Authentication and Key Management

Diffie-Hellman groups 1, 2, and 5
X.509 v3 digital certificates
Digital Signature Standard (DSS)
Internet Key Management (IKE)
Manual Keys

IPSec Modes

Tunnel mode
Encapsulated Security Payload (ESP)
Authentication Header (AH)

Performance

Throughput: Up to 1.8 Gbps full-duplex gigabit
Ethernet with AES or 3DES
current IPSec tunnels: 8000
Secure Associations: 16,000

Interfaces

Two full-duplex gigabit Ethernet ports with GBIC
interfaces (single mode or multimode fiber)
Management: 10/100 Ethernet and RS-232

Physical

Tamper-evident chassis
Footprint: 4" H x 17" W x 15" D
Rack mountable in standard 19" rack
Power: 115-240 VAC @ 50/60 Hz, auto-sensing
Weight: 10 lbs.

Network Support

IEEE 802.3
Jumbo frames
VLAN tags
MPLS labels
PMTU
VRRP for resiliency
Dead peer detection
Optical loss pass-through

Encryption and Integrity

DES: FIPS 46-2 (56 bit keys), Standard CBC mode
3DES: ANSI X.952 (168 bit keys), Standard CBC mode
AES: FIPS 197 (128, 192, 256 bit keys)
HMAC-MD5-96
HMAC-SHA-1-96

IKE Features

Pre-shared keys
DSS authentication
NIST FIPS PUB 186
Main and Aggressive modes

Environmental

Rating Temperature: 0° to 40° C (32° to 104° F)
Rating Humidity: Up to 90 % non-condensing
Operating Altitude: -200 to 10,000 feet AMSL operating
altitude

Certification

FIPS PUB 140-2 Level 2 compliant

Regulatory

Emissions: FCC Part 15 to Class B Specifications,
EN61000-3-2: 1995, EN61000-3-3: 1999, EN61000-4-2
through 4-6, 4-11: 1995
Safety: IEC 60950 (UL), CSA-C22.2 No. 60950-00,
EN 60950 for the participating European nations,
EN 60950 for all country deviations.

THALES

THALES e-SECURITY, INC.

2200 N. Commerce Parkway
Suite 200
Weston, Florida 33326, USA
Tel: +1 888 744 4976
or: +1 954 888 6200
Fax: +1 954 888 6211
e-mail: americas.sales@thales-esecurity.com

The Thales policy is one of continuous development and consequently the equipment may vary in detail from the description and specification in this publication.