BLACK BOX®
NETWORK SERVICES

EncrypTight ™ WAN Encryption

Secure WAN links without tunnels!

- Strong WAN encryption without IPsec VPN tunnels.
- Multilayer encryption.
- Transparent operation without latency.

EncrypTight™

BLACK BOX WAN ENCRYPTION

0118 965 6150 | www.blackbox.co.uk/goto/EncrypTight

Solid security with versatility and scalability.

- Encrypts at OSI Layer 2, 3, or 4.
- Works with all kinds of network traffic, including VoIP.
- Works on the Internet or on private WANs.
- No need for VPN tunnels.
- No delays, no jitter, no latency.
- Transparent to network operation and applications.
- **WARRANTY** — 1 Year

ET1000A

ET0010A

More and more organisations are using the Internet to send data to branch offices. But because the Internet is a public network, security is an issue, so sensitive data must be encrypted.

EncrypTight™ is an encryption solution that overcomes the limitations associated with IPsec VPN tunnels. It brings you air-tight encryption across any WAN —even the Internet—without the hassle of setting up a VPN tunnel for each connection. Layer 4 encryption capability leaves packet headers intact, making encrypted data far more compatible with network operations. Plus, EncrypTight doesn't add latency to bog down network operations —it's totally transparent.

The not-so-private MPLS WAN

Many organisations don't encrypt their data because it's traveling on a "safe" MPLS network. Although MPLS networks provide more reliable connections than the Internet and aren't as public, they cannot be counted upon to be private —they're still vulnerable to attack.

MPLS is technically a VPN that mimics privacy by logically separating data with labels. Although the data traffic is kept separate from other traffic, it can still be easily intercepted at any node.

When vendors say MPLS is secure, what they mean is that the traffic is kept separate from other traffic, that they have processes in place to prevent unauthorised data snooping, and that their employees probably aren't going to snoop either. In fact, your data probably won't be stolen on an MPLS network, but you have no way of being sure and no way to tell if your data has been breached.

In fact, the only way to ensure data security over an MPLS network is by encrypting data as it travels across the WAN.

Breaking out of the tunnel

Although IPsec VPN tunnels are fairly simple to set up between only two points, when remote sites multiply, the number of tunnels increases exponentially. A tunnel is needed between each pair of sites, leading to administrative hassles every time a remote site is added.

EncrypTight eliminates the need to establish point-to-point tunnels between each pair of remote sites, freeing network administrators for other tasks. With EncrypTight, every network on your WAN can establish an instant encrypted connection to every other network equipped with an EncrypTight appliance.

Layer 4 encryption

In addition to Layer 2 Ethernet frame encryptions and Layer 3 IP packet encryption, EncrypTight offers a Layer 4 payload-only encryption option. Layer 4 encryption offers many advantages, including:

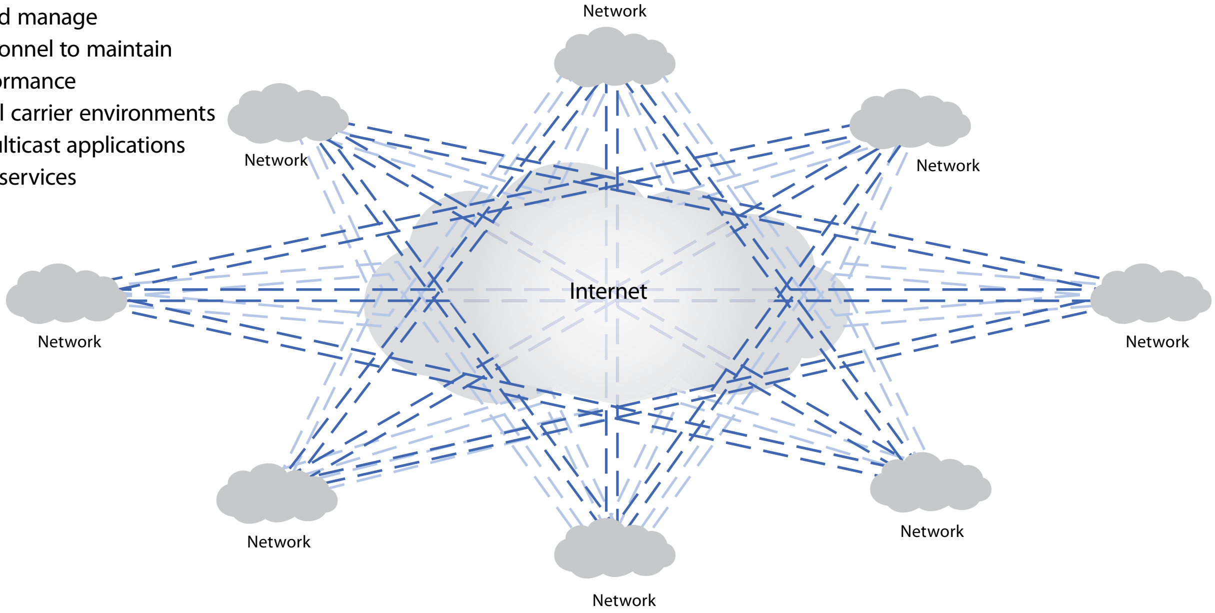
- Ability to pass encrypted data through NAT devices. VPN tunnels, which encapsulate the Layer 3 address, often don't work with NAT.
- Compatibility with policy-based routing and load balancing that require Layer 3 addresses to be intact.
- Layer 4 encryption leaves Layer 3 headers intact, making it possible to troubleshoot a network without turning off encryption.
- Because headers are intact, data looks unencrypted, making it possible to use within countries that restrict encrypted data.

Central management

Manage all your EncrypTight appliances with EncrypTight Management Software. The simple drag-and-drop interface scales seamlessly and enables you to set encryption policies based on IP addresses, port numbers, protocol IDs, or VLAN tags. You can quickly change policies across the entire WAN without interrupting network traffic. EncrypTight Management Software generates, and securely pushes, encryption keys and policies to appliances throughout the WAN. Logging and auditing functions enable you to collect and monitor important criteria such as enforcement point status, as well as policy, password, and device configuration changes.

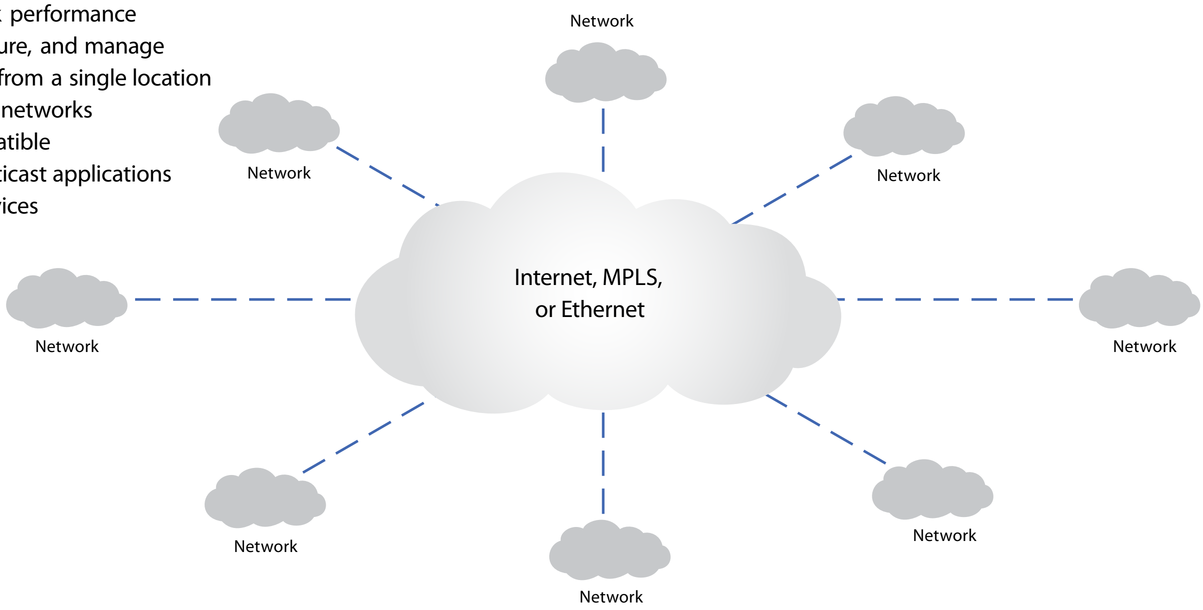
Traditional IPsec VPN

- Tunnel based
- Difficult to set up and manage
- Requires added personnel to maintain
- Slows network performance
- Doesn't support dual carrier environments
- Slows or disables multicast applications
- No Layer 4 network services



EncrypTight

- No tunnels!
- Doesn't slow network performance
- Easy to set up, configure, and manage
- Can be administered from a single location
- Supports dual-carrier networks
- VoIP and video compatible
- Compatible with multicast applications
- Preserves Layer 4 services



Compliance

EncrypTight helps you comply with HIPAA, HITECH, PCI, or other industry or government data-protection standards. EncrypTight offers AES 256-bit encryption. Plus, its logging and auditing functions help you save and organise the records required by many of these standards, reducing the scope of audits with thorough recordkeeping.

Seamless scalability

Because there are no tunnels to set up, it's easy to deploy EncrypTight across large WANs. For instance, an organisation with many sites around the world could add a new site to its WAN without having to establish a VPN tunnel to every other site.

Additionally, EncrypTight Management Software enables network administrators to centrally manage security across the entire WAN using a simple drag-and-drop interface.

EncrypTight Appliance Specifications

Item	Code	Available Speeds	Connectors	Power	Size	Weight

3–50 Mbps EncrypTight Appliance	ET0010A	3, 6, 10, 25, 50 Mbps	Local: (1) 10-/100-/1000-Mbps RJ-45 Ethernet;
			Remote: (1) 10-/100-/1000-Mbps RJ-45 Ethernet;
			Management: (1) 10-/100-Mbps RJ-45 Ethernet, (1) RJ-45 RS-232;
			For future use: (1) RJ-45
				Autosensing 100–240-VAC, 50/60 Hz External Power Supply	4 x 20.3 x 14.7 cm	Rackmount: 1.4 kg
						Desktop: 0.6 kg

100–250 Mbps EncrypTight Appliance	ET0100A	100, 155, 250 Mbps	Local: (1) 10-/100-/1000-Mbps RJ-45 Ethernet;
			Remote: (1) 10-/100-/1000-Mbps RJ-45 Ethernet;
			Management: (1) 10-/100-Mbps RJ-45 Ethernet, (1) RJ-45 RS-232
				Autosensing 100–240-VAC, 50/60 Hz Internal Power Supply	4.4 x 43.2 x 25.4 cm	2.7 kg

500–1000 Mbps EncrypTight Appliance	ET1000A	500, 650 Mbps
		1 Gbps
			Local: (1) SFP (1000-Mbps);
			Remote: (1) SFP (1000-Mbps);
			Management: (1) 10-/100-Mbps RJ-45 Ethernet; (1) RJ-45 RS-232;
			For future use: (1) RJ-45, (1) SFP
				Dual, Hot-Swappable, Autosensing 100–240-VAC, 50/60 Hz Internal Power Supply	8.9 x 43.2 x 38.1 cm	4.1 kg

An encryption solution for every network

EncrypTight Appliances come in three sizes to accommodate three different ranges of WAN interface speeds. Choose the appliance in the right range, then select a bandwidth license for your specific bandwidth. All appliances can be rackmounted. The 3–50 Mbps model can also be used as a desktop unit. Then choose the EncrypTight Bandwidth License that matches your WAN interface.

EncrypTight Management Software Package for Windows includes the Policy Manager (ETPM), Element Management System (ETEMS), and Key Management System Software for Windows on a CD to be installed on a customer-provided Windows XP platform. This software is included with the EncrypTight Appliance.

EncrypTight Management Software Package for Linux® (ETKMS) includes Key Management System Software for Linux and the Linux operating system. The software is an ISO image on a CD to be installed on a customer-provided x86 server and is recommended for installations of more than 15 EncrypTight Appliances.

Choose an EncrypTight Management Software License per EncrypTight appliance for up to 20, 21–50, or more than 50 appliances.

The EncrypTight Linux Server (ET-KSRV) is Key Management System Software for Linux (ETKMS) and documentation installed on an optimized and hardened Dell® server.

The EncrypTight Hardware Security Module (ET-HSM) works with the EncrypTight Linux Server (ET-KSRV) to provide secure storage of keys, true random number generation, and other advanced security features. Requires EncrypTight Server; order one Hardware Security Module for each EncrypTight Server.

Item	Code
First, select your appliance…	
EncrypTight™ Appliances	
3–50 Mbps	ET0010A
100–250 Mbps	ET0100A
500–1000 Mbps	ET1000A
…then, select a license for the desired bandwidth…	
EncrypTight Bandwidth Licenses	
ET0010A Licenses	
3-Mbps	ET-BWL-3MBPS
6-Mbps	ET-BWL-6MBPS
10-Mbps	ET-BWL-10MBPS
25-Mbps	ET-BWL-25MBPS
50-Mbps	ET-BWL-50MBPS
ET0100A Licenses	
100-Mbps	ET-BWL-100MBPS
155-Mbps	ET-BWL-155MBPS
250-Mbps	ET-BWL-250MBPS
ET1000A Licenses	
500-Mbps	ET-BWL-500MBPS
650-Mbps	ET-BWL-650MBPS
1000-Mbps (1 Gbps)	ET-BWL-1GBPS
…and management software…	
EncrypTight Management Software Package	
for Windows (Included with EncrypTight Appliance)	Included
for Linux	ETKMS
…then add a management software license.	
EncrypTight Management Software Licenses	
for 1 to 20 Appliances	EML-SMALL
for 21 to 50 Appliances	EML-MEDIUM
for More than 50 Appliances	EML-LARGE
For Key Management Software pre-loaded on a server, order…	
EncrypTight Linux Server	ET-KSRV
For increased security for the ET-KSRV, order…	
EncrypTight Hardware Security Module	ET-HSM