Trusted Cyber Technologies

THALES

# Network Independent Encryption

## Flexible, policy-based network encryption security for today's high performance network architectures.

White Paper

## Introduction

First introduced to the CV Series virtualized encryption range in 2018, Thales Transport Independent Mode (TIM) is now available for the CN Series of hardware encryption devices. It enables concurrent, policy-based multi-layer encryption for modern Ethernet and Internet protocol architecture.

Developed specifically for today's multi-layer networks, TIM provides end-to-end encryption security without the typical performance and bandwidth costs associated with IPSec encryption solutions.

Historically, different network types have required different encryption solutions. As network architecture has evolved to comprise multiple transport layers, this has implications for network security, performance and cost.

In the case of Internet protocols, the most common encryption solution, IPSec, is more than 20 years old. IPSec was not developed with wide area networking and cloud applications in mind; it incurs additional bandwidth costs and can impact significantly on network performance.

## Network Independence

The introduction of TIM to the CN Series hardware encryptors will help customers meet the increasing demand to protect data flows across multiple network types. The most common network protocols in use today are Ethernet (Layer 2) and Internet (Layer 3).

CN Series hardware encryptors have been used to protect Ethernet networks and their data for the past twenty years. The addition of Network Independent Encryption expands their use to protect Internet protocol networks.

Customers choose different network types for different data flows. With Network Independent Encryption, customers may choose a single, best-of-breed solution. One that provides high-assurance, end-toend encryption across multiple network types, without compromising bandwidth and performance.

| | Data | | Layer | | |
|---|---|---|---|---|---|
| Host | Data | 7 | Application | Http, Ftp, Rc, Ssh Dns | |
| Host | Data | 6 | Presentation | Ssl, Ssh, Imap, Ftp, Mplg, Jplg | |
| Host | Data | 5 | Session | Api, Sockets, Winsock | |
| | Segments | 4 | Transport | E2e Connections, Tcp, Udp | Thales encryption solutions |
| Media | Packets | 3 | Network | Ip Kmp, Ipsec, Igmp | |
| Media | Frames | 2 | Data Link | Ethernet, Ppp, Wsitch, Bridge | |
| | Bits | 1 | Physical | Coax, Fibre, Wifi, Hubs, Repeaters | |

## Customer Solutions

CN Series high-assurance hardware encryptors using firmware v5.01 or above feature TIM (Layer 2 and Layer 3).

- CN4000 10Mbps-1Gbps
- CN6000 1Gbps single and multi-port

CV Series virtualized encryption provides even greater flexibility for wide-area network architectures, supporting concurrent, policy-based encryption across Layers 2, 3 and 4.

**Features & Benefits**

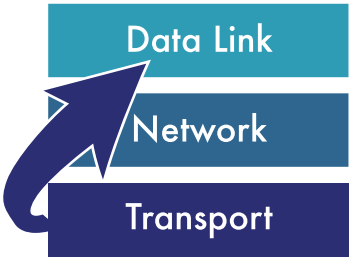
TIM delivers flexibility through the use of a single solution to encrypt multiple data flows. Both CN Series hardware encryption and CV Series virtualized encryption provide policy-based, concurrent encryption across Ethernet and Internet network topologies.

Key benefits include:

- High-performance, end-to-end encryption
- A single solution for both Ethernet and Internet networks
- Flexibility and ease of use, derived from independence from the underlying carrier network
- Destination and security policy-based encryption
- Tunnel-free, data flow encryption efficiencies
- Reduced management and bandwidth costs
- Near zero latency and data overheads

**Policy-Based Concurrent Encryption**

The cornerstone of TIM technology is policy-based, concurrent Encryption. This allows customers to define simple policies to concurrently encrypt different traffic flows at either Layer 2 or Layer 3, depending on the underlying network type and the assurance needs of the data.




The encryption of multiple network type data is concurrent IE. It occurs in conjunction with each other and having equal security protection while transported to pre-determined destinations.

Policy-based concurrent encryption matches the flexibility of security decisions with the flexibility of the network architecture employed.

**The Case for Network Independence**

Deployment of Thales encryption solutions is not carrier network dependent. Where Ethernet and Internet protocol networks are in place, Thales encryptors are easy to deploy, require very little management and provide uncompromising performance. In particular, the CN Series hardware encryptors offer:

- Near zero latency
- Minimal data overheads
- Predictable wire-speed performance

Proven ease of use and management have been a hallmark of Thales solutions used across Ethernet network types. Now Internet protocol network traffic can be protected by the same solution.

**Data-Flow Encryption**

The most efficient approach to concurrent encryption of Ethernet and IP traffic is tunnel-free encryption. This approach minimizes the encryption overhead and allows individual data flows to be natively encrypted at either Layer 2 or Layer 3.

A data-flow encryption approach ensures the optimal performance and security for transmitted data regardless of the underlying network type.

The performance and security benefits of Network Independent Encryption arise from:

- Lower data overheads minimizing the encryption overhead
- Minimizes data exposure on the network by encrypting at the most secure layer possible
- Network transparency, does not require network changes – unlike many tunnelling approaches

**Network Choices**

When it comes to encrypting and transporting data across network infrastructure, organizations naturally choose the service that best meets their needs. For example, high-bandwidth point-to-point networks are ideal for Ethernet Fiber.

However, where multiple office sites require a fully meshed network, but require more modest bandwidth, then a routed Internet protocol network may be sufficient.

In other cases, a switched Ethernet network may be a simpler solution. Then, of course, there will be cost and availability considerations.

**Fast-Moving Technologies**

For the past 20 years IPSec has been the encryption security "hammer" applied to Internet protocol network data, but in an era of fast-moving technologies, a more appropriate tool is required.

As network dependent application technologies, such as SaaS and Cloud services, demand more intelligent and efficient data networks, encryption security requirements have also changed. Carriers have offered more network types, enabling the direct flow of data. For example, SD-WAN network architectures allow data to be intelligently directed over the most appropriate transport network to meet the business intent e.g. direct to cloud or back to the data center.

Network Independent Encryption security enables a single solution for any customer's multiple network security use case. It matches network architecture flexibility with encryption flexibility by providing a single security solution for organizations' chosen network architecture.

## Thales Encryption Solutions

If your data is worth anything, it's worth encrypting. Thales is a global leader in the development of end-to-end encryption technologies. Our solutions protect sensitive data for a wide range of commercial, government, industrial and defense customers. From certified high-assurance hardware and virtualized encryption to secure file-sharing; all Thales solutions share a common high-performance encryption platform and are used to protect sensitive network data around the world.

Thales encryption solutions have been trusted to protect much of the world's most sensitive information for more than 20 years. They are used to protect everything from government and defense secrets to citizens' identity and intellectual property, financial transactions to real-time CCTV networks and critical national infrastructure control systems.

### Hardware Encryption

Thales Network Encryptors deliver high-assurance encryption for core network and IT infrastructure. Certified by leading independent authorities (DoDIN APL, Common Criteria, FIPS and NATO), Thales CN Series encryptors provide maximum security and data protection for public and private networks.

Operating from ultra-fast 100Gbps to modest 10Mbps bandwidths, they feature near-zero latency and overhead. Purpose built, secure and dedicated network encryption appliances; Thales CN encryptors provide maximum data protection and network security, without compromising network or application performance.

**Virtual Encryption**

The Thales CV1000 Virtual Encryptor (CV1000) delivers strong and flexible encryption security for virtual CPE and wide area networks. Scalable to thousands of endpoints, the CV1000 is a software application of the trusted Thales encryption platform. It delivers cost-effective, multi-Layer data protection at up to 5Gbps (with DPDK) bandwidth for Cloud, distributed and software-defined networks.

As a Virtual Network Function, the CV1000 is designed to meet the security and agility demands of virtualized data networks. It enables rapid encryption deployment to the virtual network edge.

## About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com

©2022 Thales 2.9.22