thalestct.com

THALES

High Speed Encryption Solutions **Across MPLS Networks**

Thales High Speed Encryptors (HSEs) are certified Layer 2 encryption devices that provide confidentiality and optional authentication of information that is transmitted across communication networks.

HSEs provide the optimal, most efficient means of encrypting data across modern metro or wide area Ethernet networks. By encrypting the payload of Ethernet traffic, sensitive data (including all IP addresses) is kept completely private whilst the frame headers are left unencrypted so that traffic can still be switched across the network. Although HSEs are designed for use across layer 2 networks such as metro or carrier Ethernet services, they can also be effectively deployed across layer 3 MPLS or IP/VPN environments.

HSEs provide extremely high performance encrypted throughput and can operate at wire speed at rates up to 10 Gbps. By using a dedicated hardware encryption engine and a non-blocking architecture the encryption process adds additional latency of less than 10 microseconds ensuring that performance sensitive network applications such as video or voice traffic are not impacted.

HSEs provide strong authenticated key management using industry standard X.509 certificates that are installed in each encryptor from a trusted root Certificate Authority. The encryptors automatically exchange credentials across the network for authentication and to securely exchange the AES data encryption keys that are used to encrypt network traffic.

MPLS Network Encryption

HSEs are designed to be transparent across any layer 2 network such as point-point dark fiber, WDM links, metro Ethernet, VPLS or any layer 2 MPLS services. HSEs can also be used across a layer 3 MPLS network (one in which Ethernet headers are not preserved end-end) with the following two conditions:

- The encryptor must be configured to preserve MPLS labels and/or IP addresses in the clear so that they are visible across the core for network forwarding
  - This is a standard encryptor configuration item and can be enabled via the CLI or remotely using Thales Encryptor Manager CM7 (CM7) or Thales Security Management Center (SMC) as shown in Figure 1.
- The second condition is that a layer 2 broadcast domain must be available for the encryptor's key management traffic which is sent as Ethernet frames.
  - This can be provisioned as either a physically separate network or across the MPLS network itself depending upon its capabilities

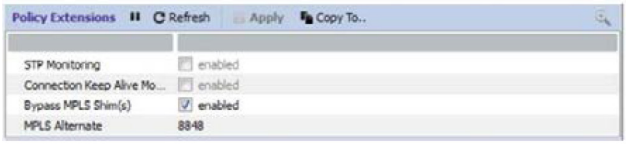

Figure 1 -Bypass of MPLS labels

Layer 2 domain provisioned across the MPLS network

This can be provisioned across the MPLS core itself.

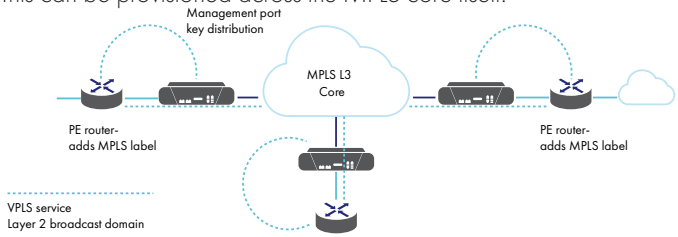

Figure 2 - Layer 2 Service across MPLS core

Figure 2 shows one way of achieving this. In this example the encryptors require out-of-band key management (a dedicated port on the encryptor) where the encryptor's management port is connected to a PE router on the protected side of the network. The network operator must configure a VPLS (layer 2 broadcast domain) service across the MPLS core that connects all the router ports that are connected to the encryptor's administration interface.

MPLS networks can generally be configured to pass either layer 2 or layer 3 traffic end-to-end. Provisioning the VPLS service where it is needed allows the encryptors to exchange keys and establish secure connections across the MPLS core.

Once a secure connection has been established, the HSEs will secure traffic at 100% line rate. The frame header can be left unencrypted ensuring that it can be switched across the network.

Physically separate key management network

Another option is to provision a separate layer 2 cloud for key management. Figure 3 shows HSEs sitting in an MPLS network. In this example the MPLS network operates at layer 3 and is incapable of delivering the broadcast Ethernet key management frames required by the encryptors to establish secure connections and distribute encryption keys.

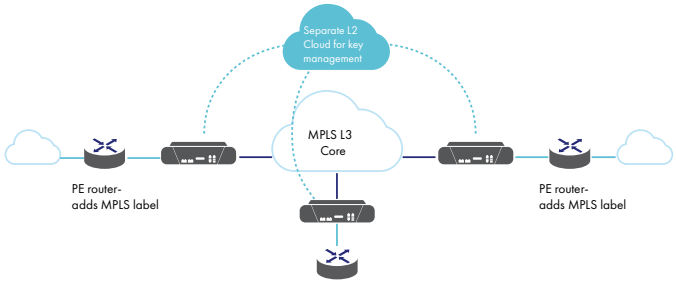

Figure 3 –Out-Of-Band Key Management

To bypass this issue, the HSEs have a standard mechanism to allow key management traffic to be sent out the administration (management) interface instead of out the normal network facing port; this is called out-of-band key management.

Figure 4 shows how this feature can be enabled using the Thales CM7 management platform. The feature functions similarly in SMC. Alternatively the CLI command to enable this is shown in Figure 5.

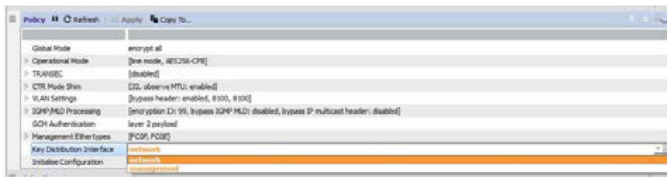

Figure 4 - Enabling management interface key distribution via CM7

Format:

controlplaneif<CR>	Display current status
[net|man]	Set key distribution port to Network port or Management port

Figure 5 - Enabling management interface distribution via CLI

In this topology, the encryptors will authenticate each other and exchange encryption keys across the separate layer 2 network. Once this is complete, data across the MPLS WAN will be fully encrypted and the MPLS/IP headers left in the clear to allow switching in the WAN. There is no degradation of performance or impact on the security of the network.

Summary

Thales High Speed Encryptors (HSEs) provide efficient, high throughput and low latency encryption of all traffic across a service provider network. Although HSEs are principally designed for use across layer 2 networks such as metro or carrier Ethernet services they can be deployed across layer 3 MPLS or IP/VPN environments as well using the configuration described in this document.

Thales High Speed Encryptors are available for sale to the U.S. Federal Government exclusively through Thales Trusted Cyber Technologies

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

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