Trusted Cyber Technologies

THALES
Building a future we can all trust

Quantum Resistant High Speed Network Encryption

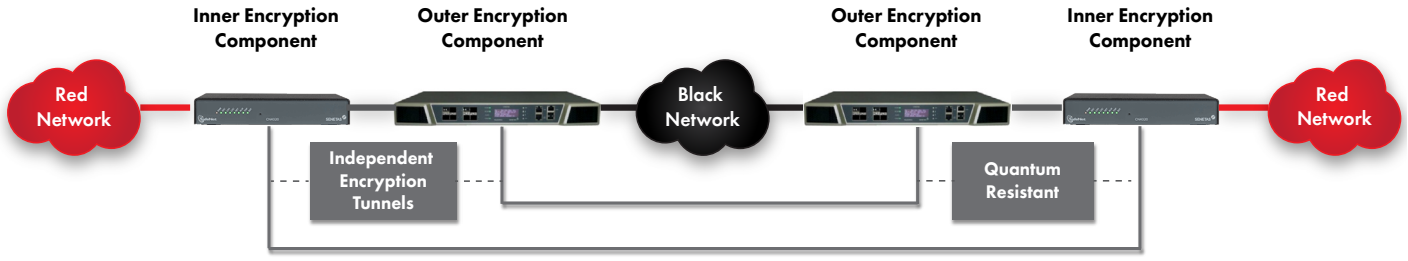
Nested Encryption Configuration for Multi-Site Connectivity

There is an emerging network encryption strategy that uses a defense-in-depth approach implemented using two nested, independent encryption tunnels to protect the confidentiality and integrity of data as it transits an untrusted network. These nested encryption solutions reduce the risk of data exposure in the event that one of the encryption layers is compromised.

Additionally, using two independent encryption layers helps to protect against certain types of attacks that may target a single encryption layer such as replay attacks, man-in-the-middle attacks, or quantum attacks. This strategy has been adopted by the Commercial Solutions for Classified (CSfC) Multi-Site Connectivity (MSC) solution. CSfC MSC solutions use a combination of IPsec and MACsec to protect the data in transit. However, many existing CSfC solutions are complex to configure and use protocols that negatively impact performance and efficiency.

Thales High Speed Encryptors (HSE) offer an MSC solution that not only provides the multiple layers of encryption, but does so while providing significant performance benefits over typical IPsec / MACsec solutions. HSE delivers deterministic wire speed encryption with microsecond latency and supports up to 100 Gbps throughput per device. Furthermore, the HSE is also quantum safe and is FIPS 140 certified to operate in a hybrid classic/quantum mode of operation.

Nested Encryption Configuration for Multi-Site Connectivity



Thales HSE Key Features

Independent Modes of Operation

The nested configuration consists of two HSE devices at each site, one acting as the inner encryption component and the other as the outer encryption component. HSE can encrypt data on the inner and outer components using two independently implemented policy and key management engines. The devices are configured to use different modes of operation: layer 2 mode and Transport Independent Mode (TIM). In layer 2 mode of operation all network traffic is encrypted at the Ethernet layer and the encryptors can be deployed in point-point, hub-spoke or full mesh topologies. In this mode the HSE uses X.509 certificate based authentication to authenticate peer devices and establish a secure connection. Layer 2 mode also supports hybrid quantum safe key establishment using dual X.509 certificates.

In Transport Independent Mode, the HSE uses an independent policy engine and key management design. The TIM policy engine allows network traffic to be encrypted using highly efficient tunnel-free encryption at either layer 2, 3 or 4. The encryptor can be deployed in point-point, hub-spoke or full mesh topologies across any underlying network (e.g. MPLS, public internet, satellite, etc.). A NIST approved Key Derivation Function (KDF) is used to generate strong encryption keys that are resistant to brute-force attacks, rotated regularly, provide perfect forward and backward secrecy and that are also quantum safe. The use of a KDF in a network encryption system can provide significant benefits over traditional pairwise key agreement protocols. It improves security by removing the vulnerability of an attacker eavesdropping on the key exchange, increases scalability by reducing the number of key exchanges needed, and provides a practical way to generate encryption keys.

With its NIST approval and efficiency, a KDF is a strong choice for securing network communications. The use of a 5-tuple policy provides granular control over network traffic and can be used to enforce security policies that are specific to an organization's needs. It can also be used to prevent malicious traffic from entering the network, as well as prevent sensitive data from leaving the network. As part of a quantum safe architecture, the encryptors can optionally be initialized with keys from an approved Key Generation Solution (KGS) such as Thales CipherTrust Manager.

High Performance, Drop-In Encryption Solution

Not all encryption solutions are created equal. There are different protocols and modes of operation that affect the performance, efficiency, and security of network encryption. Thales HSE uses a tunnel-free mode that encrypts only the data portion of the packet with minimal overhead and changes to the packet structure. This approach delivers higher performance and lower latency than IPsec. Thales HSE security appliances include a wire speed hardware encryption engine that operates at full line rate up to 100 Gbps with no performance ceiling. Cut-through packet processing means that the encryptor only needs to receive a few bytes of the header to look up policy and start encrypting data without waiting for the rest of the packet to arrive. Thales HSE is also vendor-agnostic and can work with any network device or protocol without requiring any changes to the existing infrastructure.

Flexible Configuration Options

The HSE nested encryption solution consists of two components: the inner component and the outer component. Both components operate in a FIPS approved mode and use AES256 encryption to provide full data confidentiality with optional authentication (using GCM). To provide the benefits of independence in the nested configuration the components should be configured in different modes of operation. Multiple combinations of layer 2 mode and Transport Independent Mode can be used to satisfy the specific security requirements of a deployment and network architecture. The flexible configuration options allow system integrators to use a common family of HSE security appliances that adapt to a multitude of different network configurations. The HSE appliances and policy can be securely configured using the Thales Secure Management Console (SMC) or CM7 element manager, both managers have built-in Certificate Authorities (CA) or any external CA may be used. The HSE solution can be deployed in various scenarios, such as point-to-point, point-to-multipoint, or mesh networks. The encryptors can be configured as endpoints or intermediaries depending on the network topology and requirements.

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