Technical Introduction

IPsec

Internet Protocol Security

About IPsec

IP Security (IPsec) is a framework of open standards defined by IETF to provide high-quality, cryptography-based security for IP communications. It is a Layer 3 VPN technology that transmits data in a secure channel established between participating peers. Such a secure channel is usually called an IPsec tunnel.

IPsec protocol framework

IPsec is not a single protocol. It is a security framework that contains security protocols (AH and ESP) and key exchange management protocols (IKE and IKEv2).

AH

Authentication Header (AH) can provide data origin authentication, data integrity, and anti-replay services to prevent data tampering, but it cannot encrypt data.

ESP

Encapsulating Security Payload (ESP) can provide data origin authentication, data integrity, and anti-replay services, and it also supports data encryption.

IKE

Internet Key Exchange (IKE) uses the Diffie-Hellman (DH) key exchange algorithm for securely exchanging keys over an insecure channel. IKE can provide automatic key exchange and SA setup services for IPsec, simplifying IPsec configuration and management.

IKEv2

Internet Key Exchange version 2 (IKEv2) is an enhanced version of IKEv1. IKEv2 provides stronger protection against attacks and higher key exchange ability and needs fewer message exchanges than IKEv1.

Benefits

Data confidentiality

IPsec uses symmetric encryption algorithms to encrypt data to ensure data confidentiality. The keys for encryption and decryption can be manually configured or automatically negotiated by IKE. Commonly used symmetric encryption algorithms include DES, 3DES, AES, and SM4.

Data origin authentication

IPsec uses authentication algorithms to ensure the integrity and source of data received from the sender. Symmetric authentication keys can be manually configured or automatically negotiated by IKE. Commonly used authentication algorithms include MD5, SHA1, and SM3.

Anti-replay

Replayed packets are duplicate packets that have been processed by IPsec. De-encapsulation of replayed packets is meaningless, and the de-encapsulation process consumes large amounts of resources. IPsec anti-replay can check and discard replayed packets before de-encapsulation by using a sliding window mechanism.

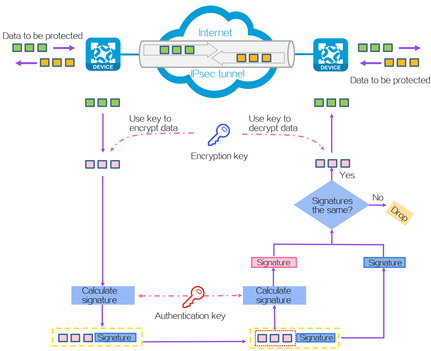
IPsec smart link selection

The smart link selection feature is to improve network stability and availability. When multiple links are available, IPsec can automatically select a link of high quality to establish the IPsec tunnel and reselect a link for the IPsec tunnel when the quality of the current decreases.

Operating mechanism

IPsec operates as follows:

1. The IPsec peers determine the data protection and authentication policy (including the security protocols, authentication and encryption algorithms, keys, and the key lifetime) and establish the IPsec tunnel accordingly, using one of the following methods:
   - **Manual configuration**: Configures all settings for the IPsec tunnel through commands. The IPsec tunnel is established immediately after the configuration is complete.
   - **IKE negotiation**: Uses IKE to negotiate an IPsec policy automatically. After IKE is configured, data flows from the sender can trigger the setup of the IPsec tunnel.
   - **Quantum encryption**: Obtains quantum keys from the quantum key server to negotiate an IPsec policy automatically. After the required configuration is complete, data flows from the sender can trigger the setup of the IPsec tunnel.
2. The IPsec peers use the security protocols to encrypt and authenticate the packets sent and received by the IPsec tunnel for secure transmission of the packets over the Internet.

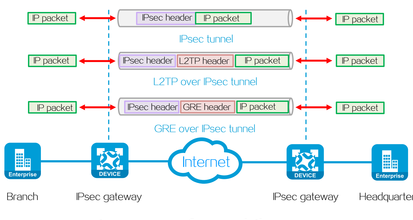


Application scenarios

Secure connections between LANs

A branch establishes an IPsec tunnel with the headquarters or with another branch for secure communication. Secure connections between LANs primarily fall into the following types:

- P2P VPN – IPsec tunnel: IPsec tunnel established between IPsec gateways to protect IP packets between LANs.
- P2P VPN – L2TP over IPsec tunnel: Packets are encapsulated by L2TP and then by IPsec to protect L2TP packets between LANs.
- P2P VPN – GRE over IPsec tunnel: Packets are encapsulated by GRE and then by IPsec to protect GRE packets between LANs.



Secure remote access for mobile users

Remote access refers to mobile users (such as traveling staff or partners) connecting to the core network through insecure networks to access internal resources on the core network. Mobile users can remotely access the headquarters through L2TP. L2TP communication is not secure because L2TP does not support encryption. To resolve this issue, you can deploy an L2TP over IPsec tunnel between the user and the IPsec gateway to secure the communication by using IPsec.