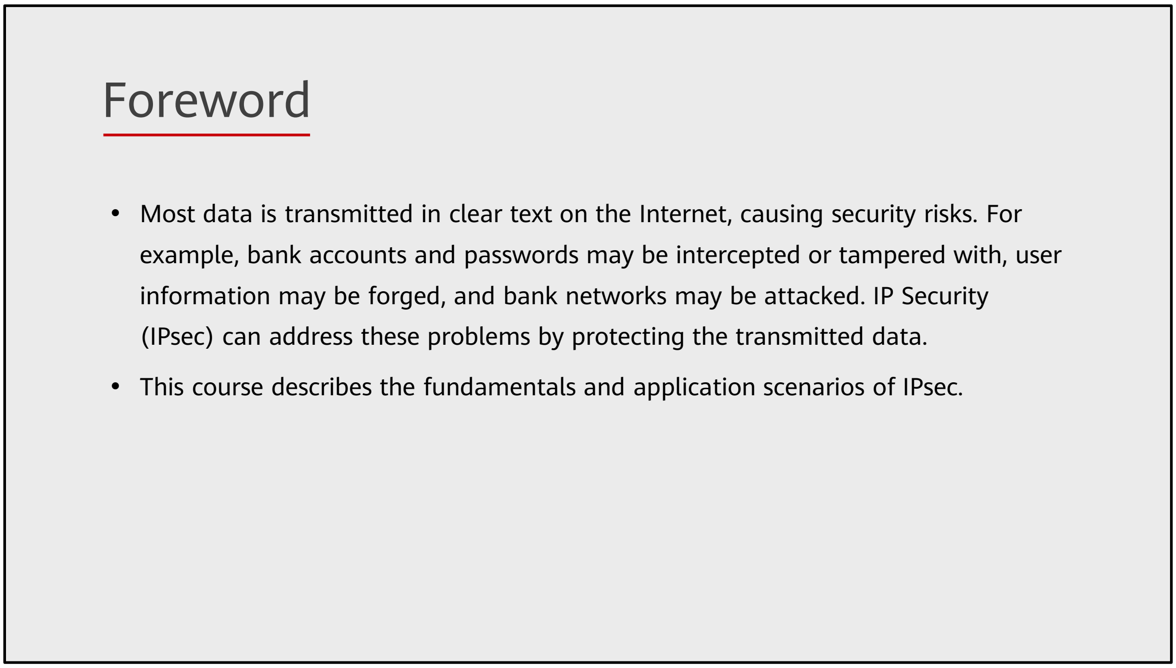
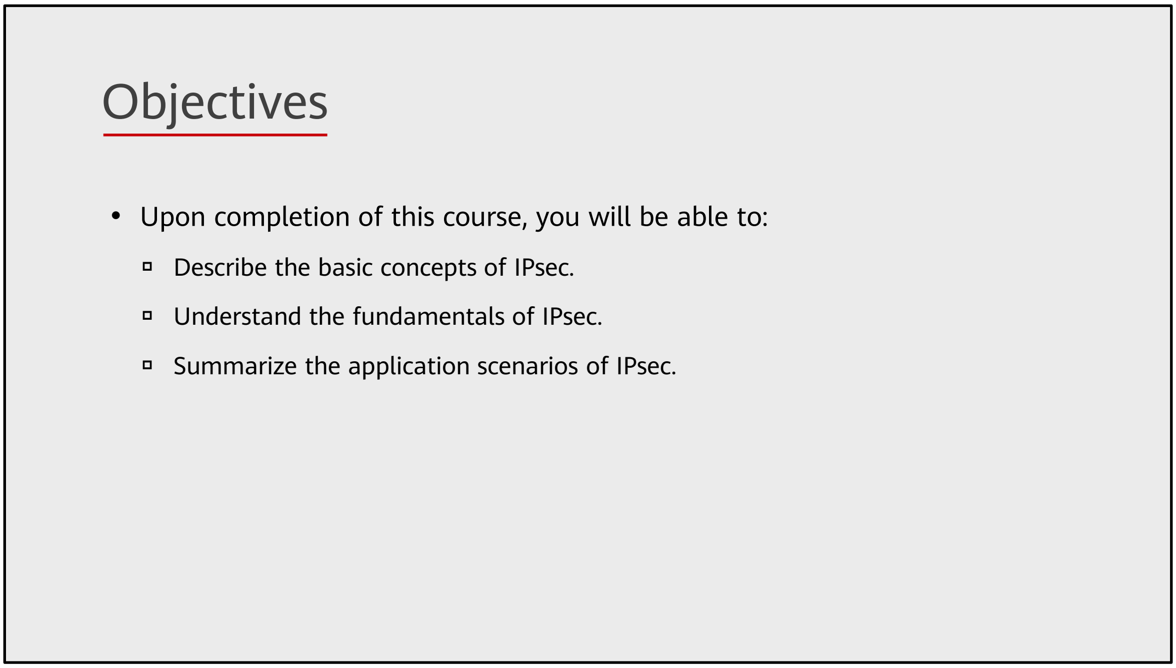
IPsec VPN Technology



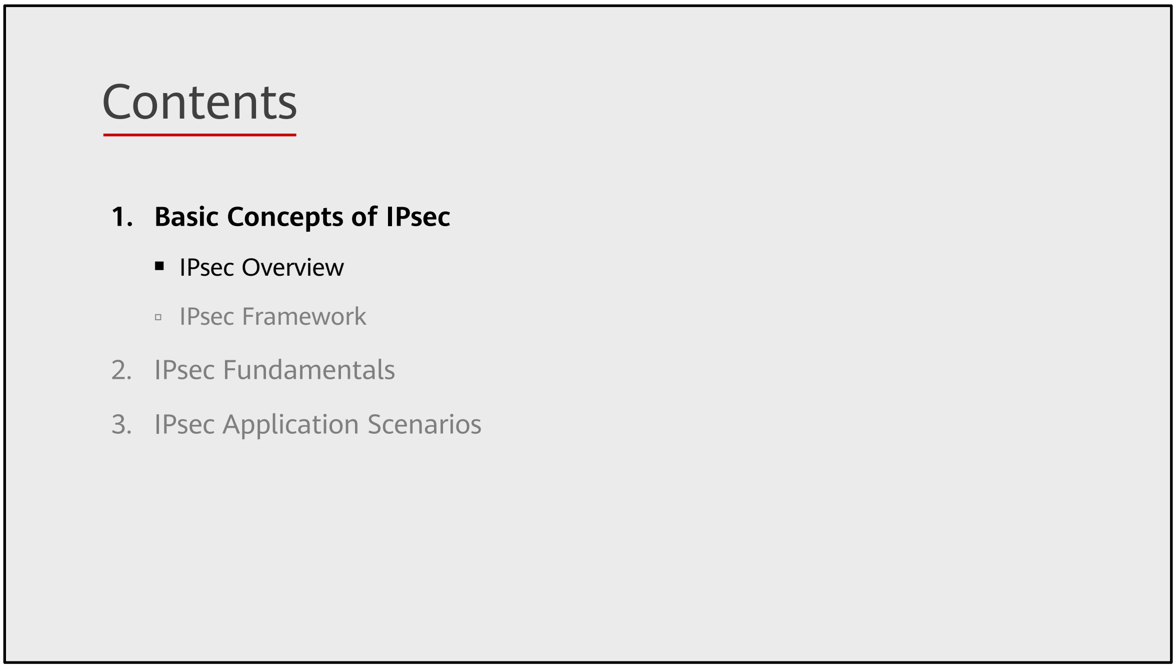
Foreword

- Most data is transmitted in clear text on the Internet, causing security risks. For example, bank accounts and passwords may be intercepted or tampered with, user information may be forged, and bank networks may be attacked. IP Security (IPsec) can address these problems by protecting the transmitted data.
- This course describes the fundamentals and application scenarios of IPsec.



Objectives

- Upon completion of this course, you will be able to:
  - Describe the basic concepts of IPsec.
  - Understand the fundamentals of IPsec.
  - Summarize the application scenarios of IPsec.

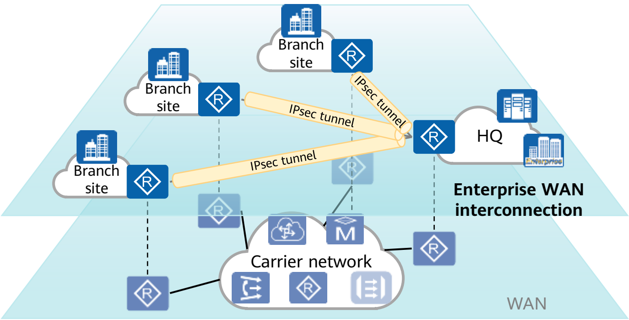


Contents

1. **Basic Concepts of IPsec**
   - IPsec Overview
   - IPsec Framework
2. IPsec Fundamentals
3. IPsec Application Scenarios

IPsec Background

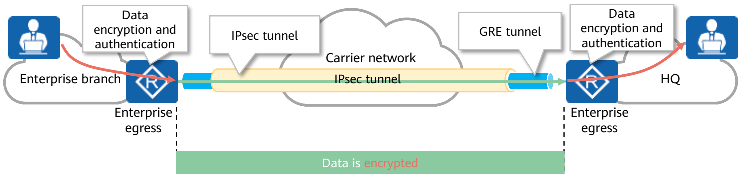
- Enterprise branches often need to communicate with each other. They can communicate using many methods, for example, using private lines or Internet links.
- Considering costs and requirements, some enterprises choose to use Internet links for interconnection. However, data may be intercepted when being transmitted on the Internet, posing security risks.
- IPsec technology encrypts data packets to secure enterprise interconnections.



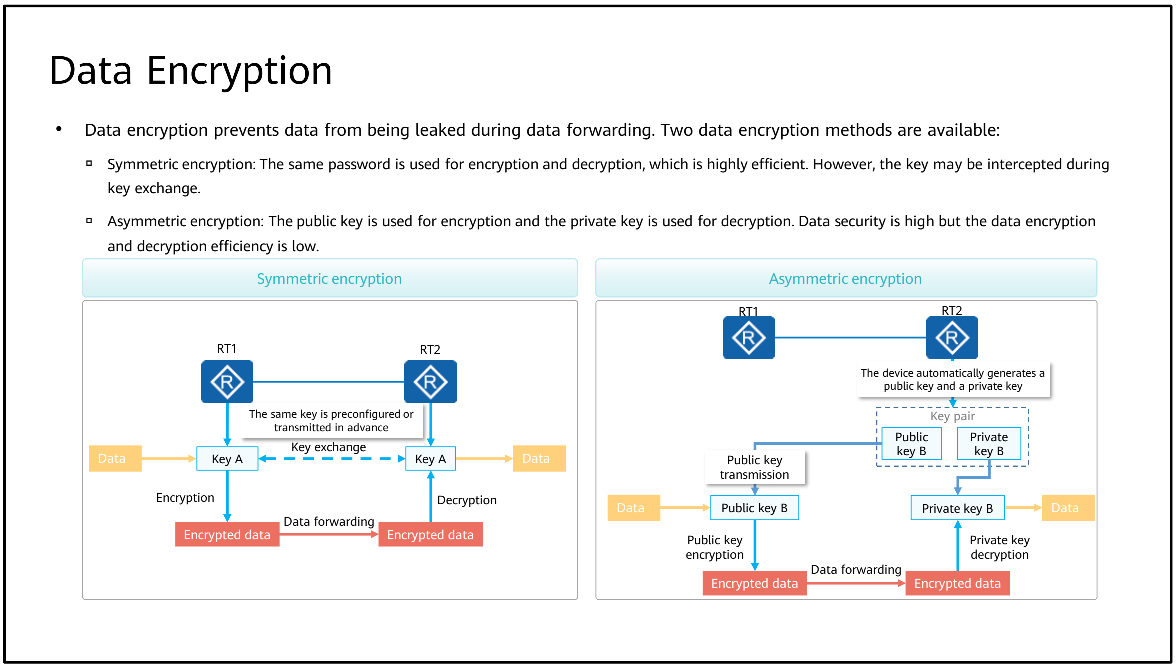
IPsec Overview

- The IPsec protocol suite is a series of security protocols developed by the Internet Engineering Task Force (IETF). It provides a cryptology-based, interoperable, and high-quality security protection mechanism for end-to-end IP packet exchange.
- IPsec encrypts and authenticates data to ensure secure data transmission on the Internet.
- IPsec VPN technology can be used with multiple VPN technologies to provide flexible and secure enterprise interconnections.

GRE over IPsec



- On the live network, GRE over IPsec technology is typically used for interconnection between branch sites. IPsec technology ensures secure data transmission, and GRE technology ensures interconnection between enterprise intranets.



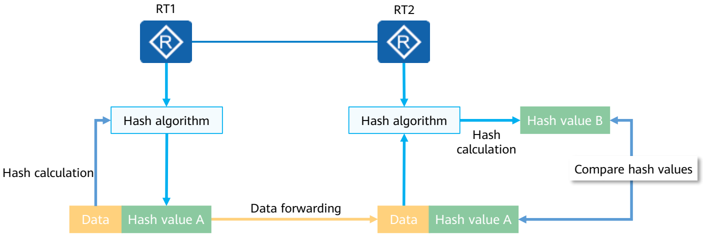
Data Encryption

- Data encryption prevents data from being leaked during data forwarding. Two data encryption methods are available:
  - Symmetric encryption: The same password is used for encryption and decryption, which is highly efficient. However, the key may be intercepted during key exchange.
  - Asymmetric encryption: The public key is used for encryption and the private key is used for decryption. Data security is high but the data encryption and decryption efficiency is low.

- The symmetric encryption algorithm is also called traditional cryptographic algorithm, in which the encryption key can be calculated from the decryption key. The sender and receiver share the same key, which is used for both encryption and decryption. Symmetric key encryption is an effective method for encrypting a large amount of data. There are many algorithms for symmetric key encryption, and all of them aim to convert between cleartext (unencrypted data) and ciphertext. Because symmetric key encryption uses the same key for data encryption and decryption, data security depends on whether unauthorized users obtain the symmetric key. If two communicating parties want to use the symmetric key to encrypt data, they must exchange the key securely before exchanging the encrypted data.
- An asymmetric algorithm is also called public key algorithm, in which a public key is used for encryption and a private key for decryption. The two keys are mathematically related. In public key encryption, the public key can be publicly transmitted between two communicating parties or released in the public repository, but the private key is confidential. The data encrypted using the public key can be decrypted only using the private key. The data encrypted using the private key can be decrypted only using the public key.

Data Authentication

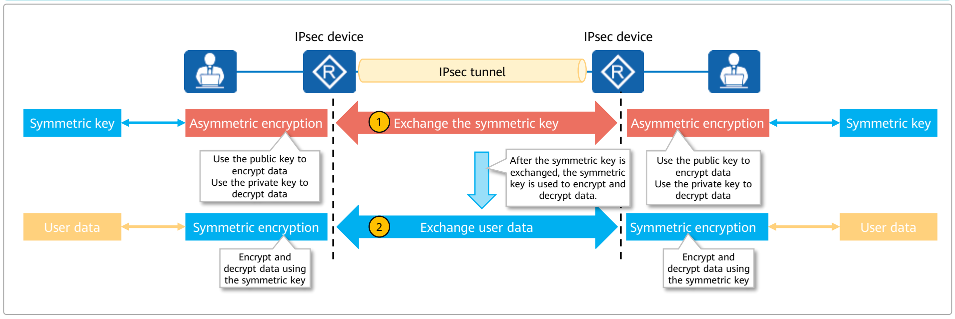
- The main purpose of data authentication is to check whether data is tampered with. Data authentication is mainly based on the hash algorithm.
  - A unique hash value is calculated based on the hash algorithm and then carried in the data before being forwarded to the peer device.
  - The peer device hashes the data again to obtain the hash value. It then compares the received hash value with the calculated one. If they are the same, the data is not tampered with.

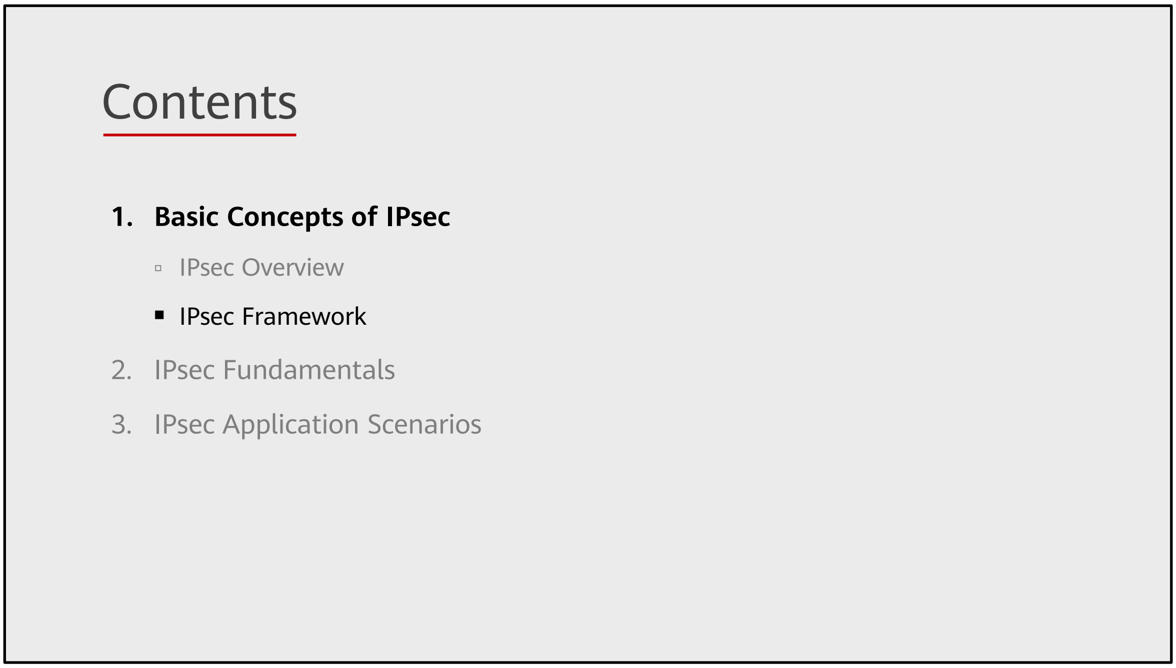


IPsec Encryption

- IPsec uses both symmetric encryption and asymmetric encryption, ensuring data security and performance.
  - Uses an asymmetric algorithm to encrypt and transmit the key used for symmetric encryption.
  - Uses the exchanged symmetric key to encrypt data.

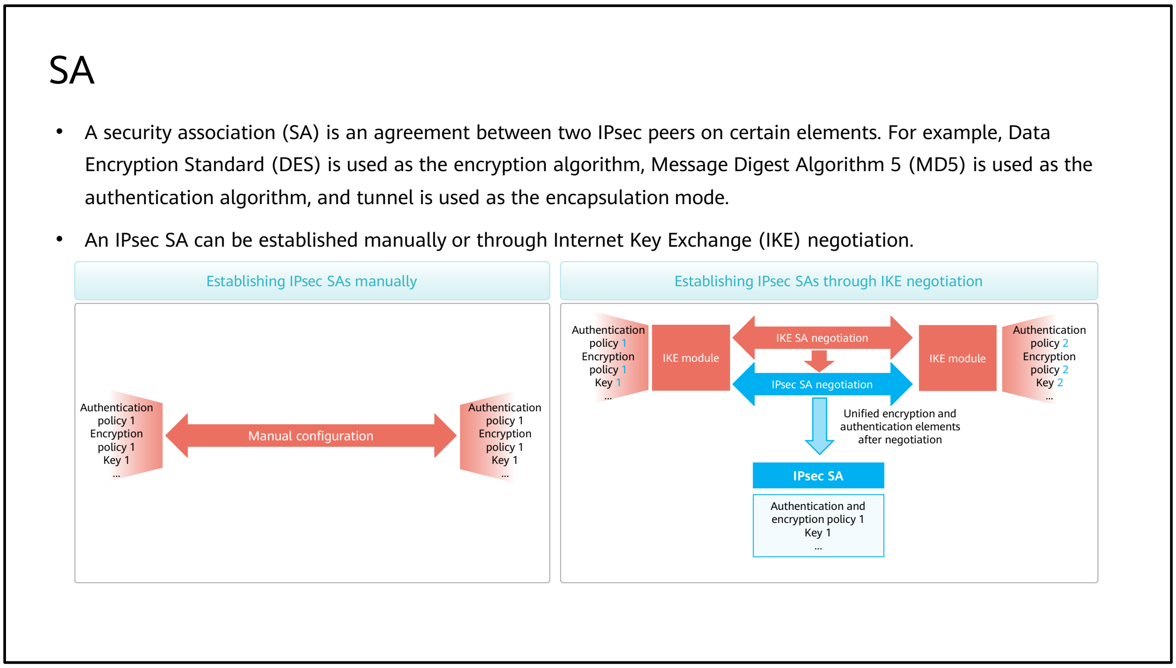
IPsec encryption and decryption


IPsec device
IPsec device
IPsec tunnel
Symmetric key
Asymmetric encryption
1 Exchange the symmetric key
Asymmetric encryption
Symmetric key
Use the public key to encrypt data Use the private key to decrypt data
After the symmetric key is exchanged, the symmetric key is used to encrypt and decrypt data.
Use the public key to encrypt data Use the private key to decrypt data
User data
Symmetric encryption
2 Exchange user data
Symmetric encryption
User data
Encrypt and decrypt data using the symmetric key
Encrypt and decrypt data using the symmetric key



Contents

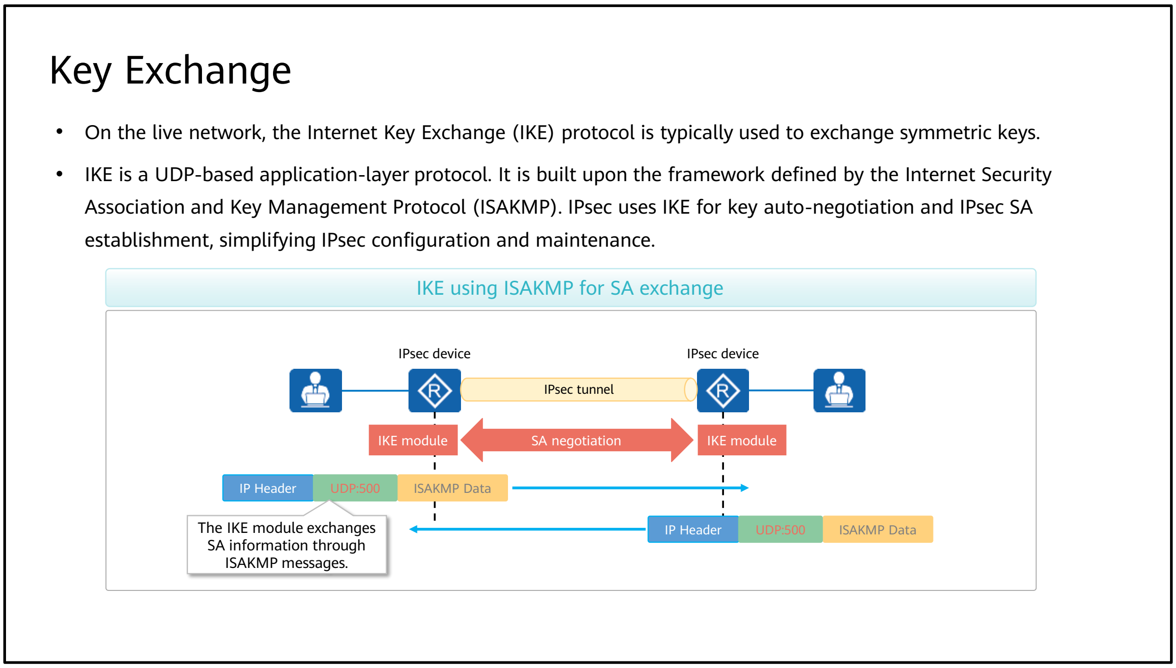
1. **Basic Concepts of IPsec**
    - IPsec Overview
    - IPsec Framework
2. IPsec Fundamentals
3. IPsec Application Scenarios



SA

- A security association (SA) is an agreement between two IPsec peers on certain elements. For example, Data Encryption Standard (DES) is used as the encryption algorithm, Message Digest Algorithm 5 (MD5) is used as the authentication algorithm, and tunnel is used as the encapsulation mode.
- An IPsec SA can be established manually or through Internet Key Exchange (IKE) negotiation.

- IPsec technology supports multiple data encryption, authentication, and encapsulation algorithms. When devices at both ends use IPsec for secure communication, they must use the same encryption and authentication algorithms. Therefore, a mechanism is required to help the devices negotiate these parameters.
- An IPsec SA can be established in either of the following ways:
  - Manual configuration: The management cost of manually established IPsec SAs is high. This is because the encryption and authentication modes need to be manually configured, SAs need to be manually updated, and SA information permanently exists, resulting in low security. This mode applies to small-scale networks.
  - IKE negotiation: The management cost of IPsec SAs established through IKE negotiation is low. The encryption and authentication modes are generated using the Diffie-Hellman (DH) algorithm, SA information is generated periodically, and SAs are dynamically updated. This mode applies to small-, medium-, and large-sized networks.
- An SA is uniquely identified by three parameters: security parameter index (SPI), destination IP address, and security protocol ID (AH or ESP).
- An IKE SA is used to establish a secure channel for exchanging IPsec SAs.



Key Exchange

- On the live network, the Internet Key Exchange (IKE) protocol is typically used to exchange symmetric keys.
- IKE is a UDP-based application-layer protocol. It is built upon the framework defined by the Internet Security Association and Key Management Protocol (ISAKMP). IPsec uses IKE for key auto-negotiation and IPsec SA establishment, simplifying IPsec configuration and maintenance.

IKE using ISAKMP for SA exchange

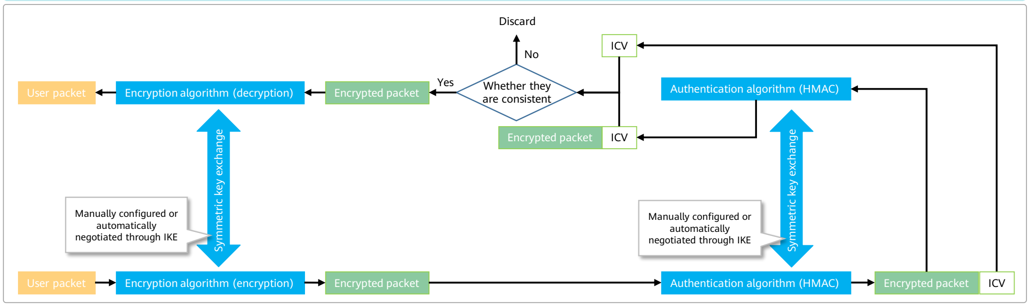
The IKE module exchanges SA information through ISAKMP messages.

- IKE supports the following authentication algorithms including MD5, Secure Hash Algorithm 1 (SHA1), SHA2-256, SHA2-384, SHA2-512, and Senior Middle 3 (SM3).
- IKE supports the following encryption algorithms: DES, 3DES, AES-128, AES-192, AES-256, SM1, and SM4.
- ISAKMP is defined in RFC 2408, which defines the procedures for negotiating, establishing, modifying, and deleting SAs and defines the ISAKMP message format. ISAKMP provides a general framework for SA attributes and the methods of negotiating, modifying, and deleting SAs, without defining the specific SA format.
- ISAKMP messages can be transmitted using UDP or TCP through port 500. In most cases, ISAKMP messages are transmitted using UDP.

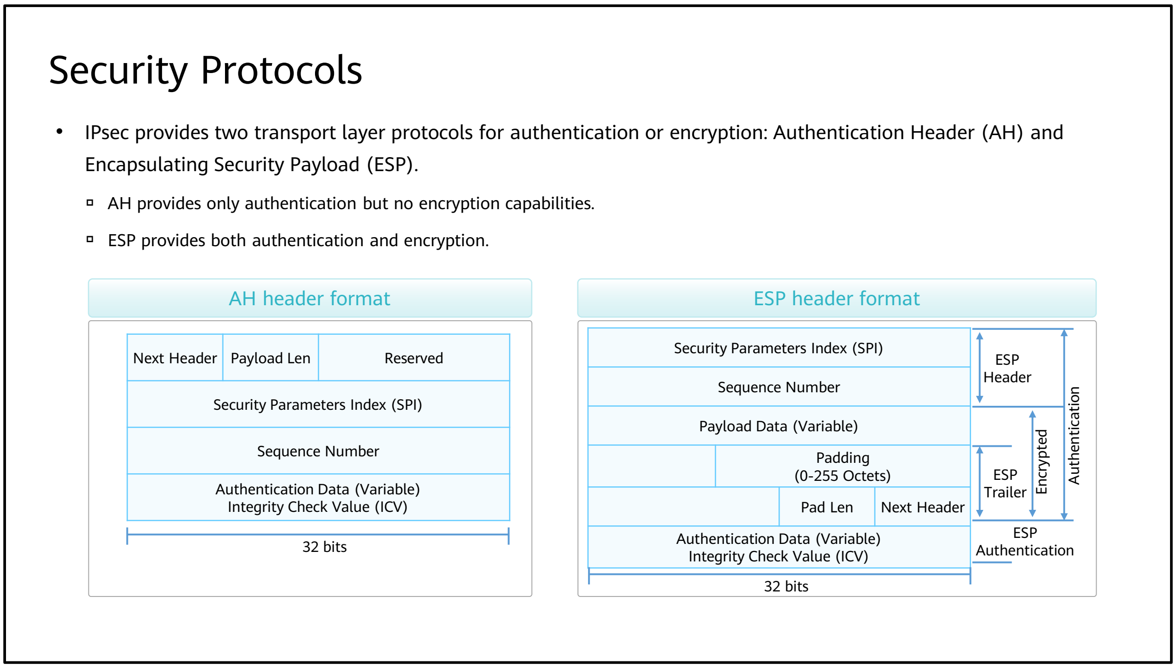
Data Encryption and Authentication

- IPsec provides two security mechanisms: authentication and encryption.
  - IPsec uses symmetric encryption algorithms to encrypt and decrypt data. These algorithms require that the sender and receiver use the same key (a symmetric key) to encrypt and decrypt data.
  - IPsec uses the Hash-based Message Authentication Code (HMAC) function to compare digital signatures to check data integrity and authenticity.

Data encryption, decryption, and authentication


Discard
No
ICV
Yes
Whether they are consistent
User packet
Encryption algorithm (decryption)
Encrypted packet
Authentication algorithm (HMAC)
Encrypted packet
ICV
Symmetric key exchange
Manually configured or automatically negotiated through IKE
Symmetric key exchange
Manually configured or automatically negotiated through IKE
User packet
Encryption algorithm (encryption)
Encrypted packet
Authentication algorithm (HMAC)
Encrypted packet
ICV

- Integrity check value (ICV) is used by the receiver for integrity check. Available authentication algorithms are MD5, SHA1, SHA2, and SM3.
- Common symmetric encryption algorithms used by IPsec include Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), and algorithms approved by State Cryptography Administration, such as SM1 and SM4. DES and 3DES are not recommended because they are insecure and pose security risks.
- Common authentication algorithms used by IPsec include MD5, SHA1, SHA2, and SM3. MD5 and SHA1 are not recommended because they are insecure and pose security risks.
- IPsec encryption cannot verify the authenticity or integrity of information after decryption. IPsec uses the HMAC function to compare digital signatures to check integrity and authenticity of data packets. In most cases, encryption and authentication are used together. The IPsec sender uses the authentication algorithm and symmetric key to generate a digital signature for the encrypted packet and sends the IP packet and digital signature to the receiver. The receiver uses the same authentication algorithm and symmetric key to process the encrypted packet and then generates a digital signature. Then the receiver compares the received and generated digital signatures to verify the data integrity and authenticity. If the packet passes the verification, the receiver decrypts it. Otherwise, the receiver discards it.



Security Protocols

- IPsec provides two transport layer protocols for authentication or encryption: Authentication Header (AH) and Encapsulating Security Payload (ESP).
  - AH provides only authentication but no encryption capabilities.
  - ESP provides both authentication and encryption.

AH header format

Next Header	Payload Len	Reserved
Security Parameters Index (SPI)		
Sequence Number		
Authentication Data (Variable) Integrity Check Value (ICV)		

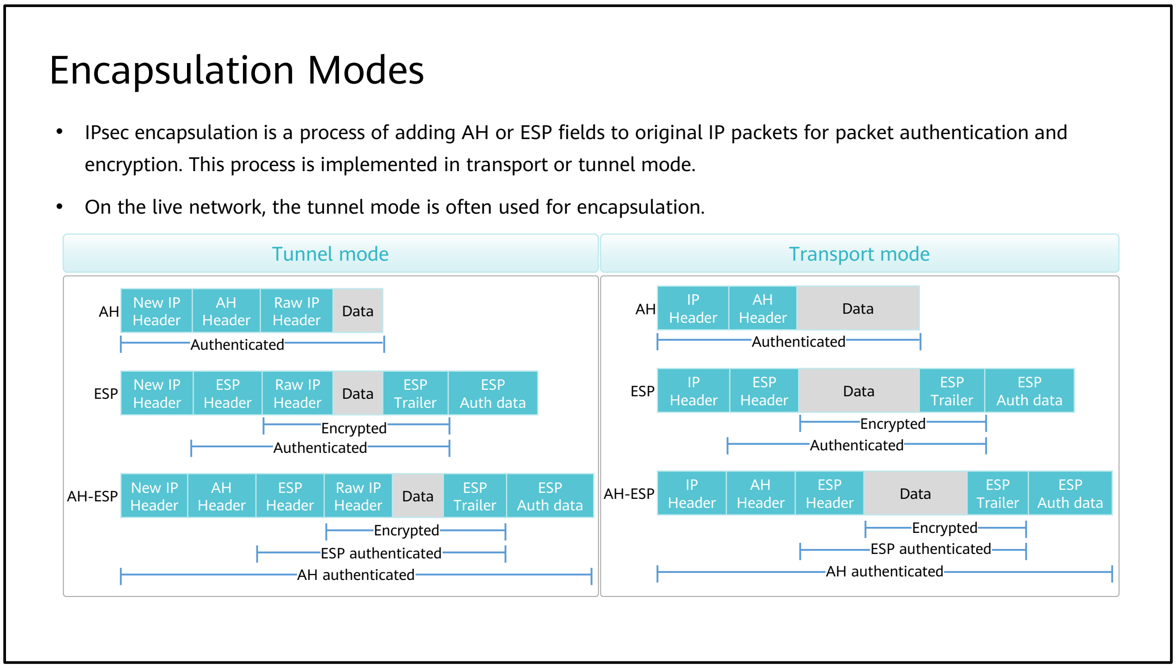
32 bits

ESP header format

Security Parameters Index (SPI)			ESP Header
Sequence Number			
Payload Data (Variable)			
	Padding (0-255 Octets)		ESP Trailer
	Pad Len	Next Header	
Authentication Data (Variable) Integrity Check Value (ICV)			ESP Authentication

32 bits

- AH provides only authentication but no encryption capabilities. According to the AH protocol, an AH header is appended to the standard IP header in each packet. The sender performs hash calculation on packets and an authentication key. After packets carrying the calculation result arrive at the receiver, the receiver also performs hash calculation and compares the calculation result with the received calculation result. Any changes to the data during transmission will make the calculation result invalid. This implements data origin authentication and integrity verification. AH provides data integrity check on an entire IP packet.
- ESP provides both authentication and encryption. An ESP header is appended to the standard IP header in each data packet, and the ESP Trailer and ESP Auth data fields are appended to each data packet. In contrast to AH, ESP encrypts the payload before encapsulating it into a data packet to ensure data confidentiality, and protects the IP header only in tunnel mode.
- Key fields:
  - Sequence Number: This field is a counter that monotonically increases from 1. It uniquely identifies a packet to prevent replay attacks.
  - SPI: This field uniquely identifies an IPsec SA.
  - Authentication Data: This field contains the Integrity Check Value (ICV) and is used by a receiver for data integrity check. Available authentication algorithms are MD5, SHA1, SHA2, and SM3.



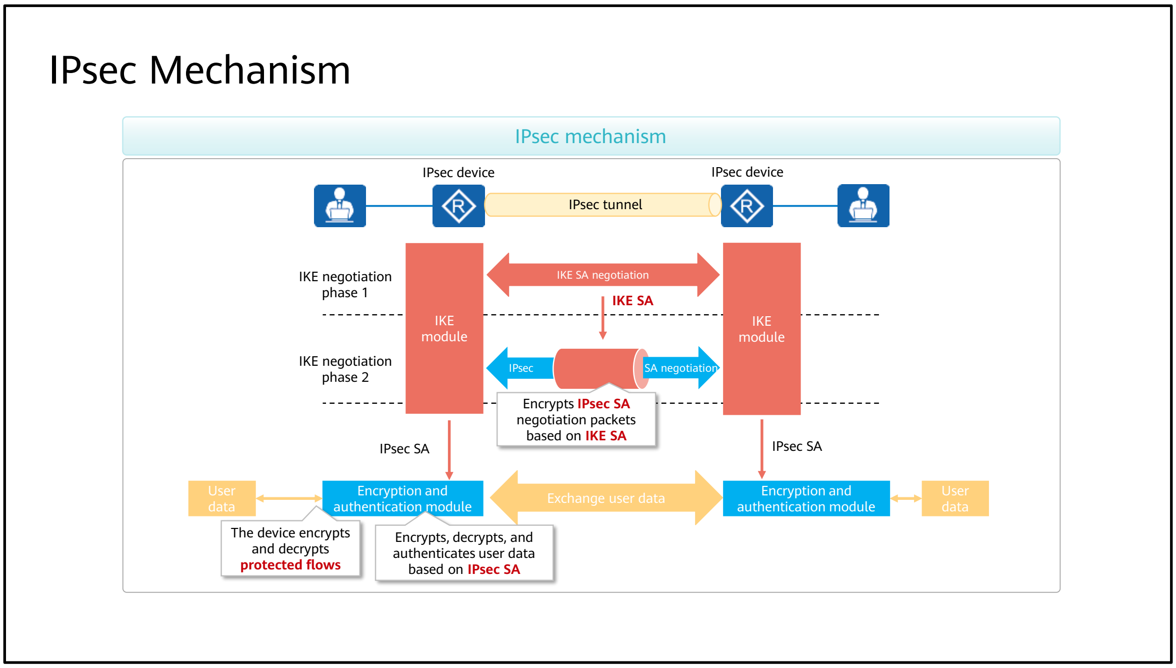
Encapsulation Modes

- IPsec encapsulation is a process of adding AH or ESP fields to original IP packets for packet authentication and encryption. This process is implemented in transport or tunnel mode.
- On the live network, the tunnel mode is often used for encapsulation.

- In transport mode, an AH or ESP header is added between an IP header and a transport-layer protocol (TCP, UDP, or ICMP) header to protect the TCP, UDP, or ICMP payload. As no additional IP header is added, IP addresses in the original packets are visible in the IP header of the post-encrypted packet.
- In tunnel mode, an AH or ESP header is added before the raw IP header and then encapsulated into a new IP packet with a new IP header to protect the IP header and payload.

Contents

1. Basic Concepts of IPsec
2. **IPsec Fundamentals**
3. IPsec Application Scenarios



IPsec Mechanism

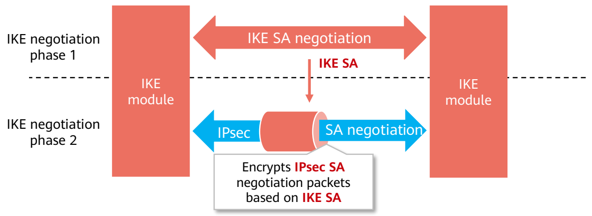
IPsec mechanism
IPsec device
IPsec device
IPsec tunnel
IKE negotiation phase 1
IKE negotiation phase 2
IKE module
IKE module
IKE SA negotiation
IKE SA
IPsec
SA negotiation
Encrypts IPsec SA negotiation packets based on IKE SA
IPsec SA
IPsec SA
User data
Encryption and authentication module
Exchange user data
Encryption and authentication module
User data
The device encrypts and decrypts protected flows
Encrypts, decrypts, and authenticates user data based on IPsec SA

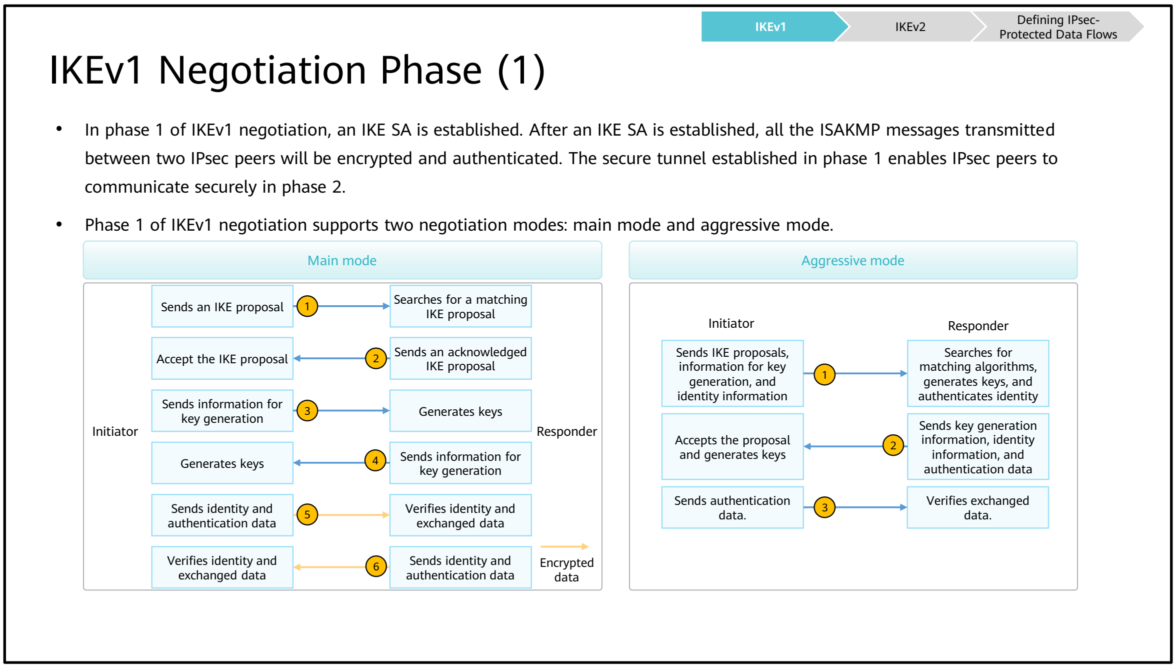
- The IPsec mechanism is as follows:
  - An IKE SA is negotiated in the first phase of IKE negotiation.
  - The IKE SA is used to encrypt the packets in the second phase of IKE negotiation. That is, IPsec SAs are negotiated in the second phase of IKE negotiation.
  - IPsec SAs are used to encrypt data.

IKEv1

- IKEv1 negotiation goes through two phases: In phase 1, two IPsec peers negotiate and establish a secure tunnel (an IKE SA). In phase 2, the two IPsec peers establish a pair of IPsec SAs for secure data transmission through the secure tunnel established in phase 1.

IKEv1 negotiation process





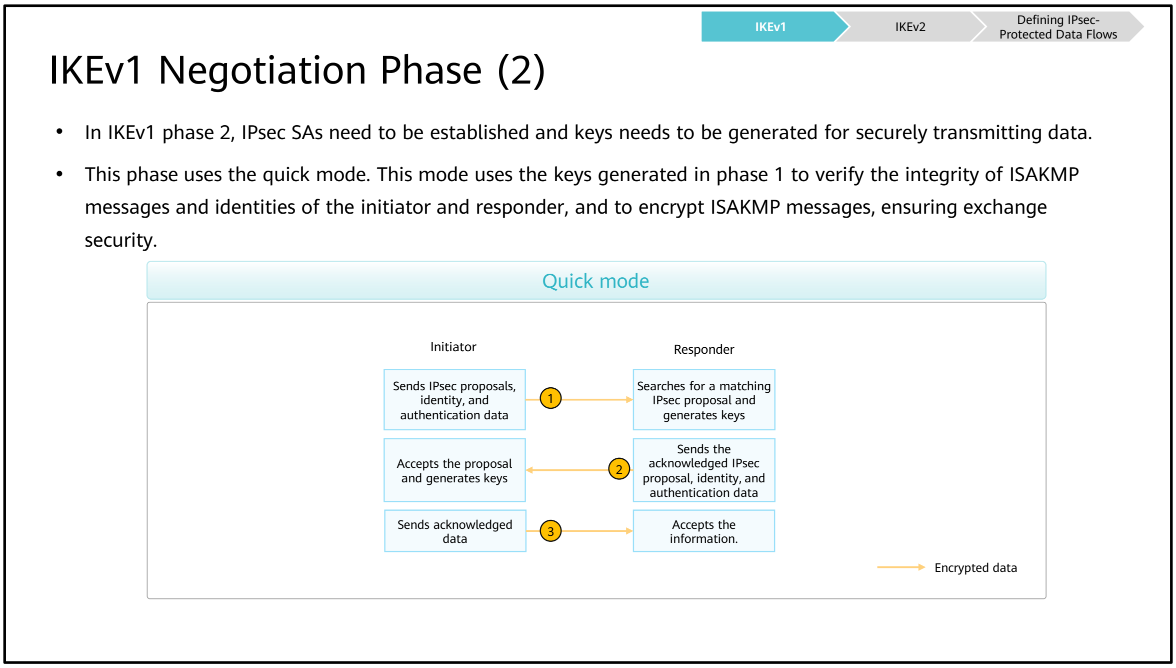
IKEv1 | IKEv2 | Defining IPsec-Protected Data Flows

IKEv1 Negotiation Phase (1)

- In phase 1 of IKEv1 negotiation, an IKE SA is established. After an IKE SA is established, all the ISAKMP messages transmitted between two IPsec peers will be encrypted and authenticated. The secure tunnel established in phase 1 enables IPsec peers to communicate securely in phase 2.
- Phase 1 of IKEv1 negotiation supports two negotiation modes: main mode and aggressive mode.

Main mode
Initiator
Responder
Sends an IKE proposal
1
Searches for a matching IKE proposal
Accept the IKE proposal
2
Sends an acknowledged IKE proposal
Sends information for key generation
3
Generates keys
Generates keys
4
Sends information for key generation
Sends identity and authentication data
5
Verifies identity and exchanged data
Verifies identity and exchanged data
6
Sends identity and authentication data
Encrypted data
Aggressive mode
Initiator
Responder
Sends IKE proposals, information for key generation, and identity information
1
Searches for matching algorithms, generates keys, and authenticates identity
Accepts the proposal and generates keys
2
Sends key generation information, identity information, and authentication data
Sends authentication data.
3
Verifies exchanged data.

- The main mode requires three exchanges between the peers, totaling six ISAKMP messages. The three exchanges are described as follows:
  - Messages 1 and 2 are used for IKE proposal exchange.
    - The initiator sends one or more IKE proposals to the responder. The responder searches for the first matching IKE proposal and then sends it to the initiator. IKE proposals of the initiator and responder match if they have the same encryption algorithm, authentication algorithm, authentication method, and DH group identifier.
  - Messages 3 and 4 are used for key information exchange.
    - The initiator and responder exchange the DH public value and nonce value to generate the IKE SA authentication key and encryption key.
  - Messages 5 and 6 are used for identity and authentication information exchange. (Both parties use the generated keys to exchange information.)
    - The initiator and responder use the generated keys to authenticate each other and the information exchanged in main mode.
- The aggressive mode uses only three messages. Messages 1 and 2 are used to negotiate IKE proposals and exchange the DH public value, mandatory auxiliary information, and identity information. Message 2 also contains the identity information sent by the responder to the initiator for authentication. Message 3 is used by the responder to authenticate the initiator.
- Compared with the main mode, the aggressive mode reduces the number of exchanged messages and speeds up the negotiation. However, the aggressive mode does not encrypt identity information.



IKEv1 | IKEv2 | Defining IPsec-Protected Data Flows

IKEv1 Negotiation Phase (2)

- In IKEv1 phase 2, IPsec SAs need to be established and keys needs to be generated for securely transmitting data.
- This phase uses the quick mode. This mode uses the keys generated in phase 1 to verify the integrity of ISAKMP messages and identities of the initiator and responder, and to encrypt ISAKMP messages, ensuring exchange security.

Quick mode

Initiator

Responder

Sends IPsec proposals, identity, and authentication data

1

Searches for a matching IPsec proposal and generates keys

Accepts the proposal and generates keys

2

Sends the acknowledged IPsec proposal, identity, and authentication data

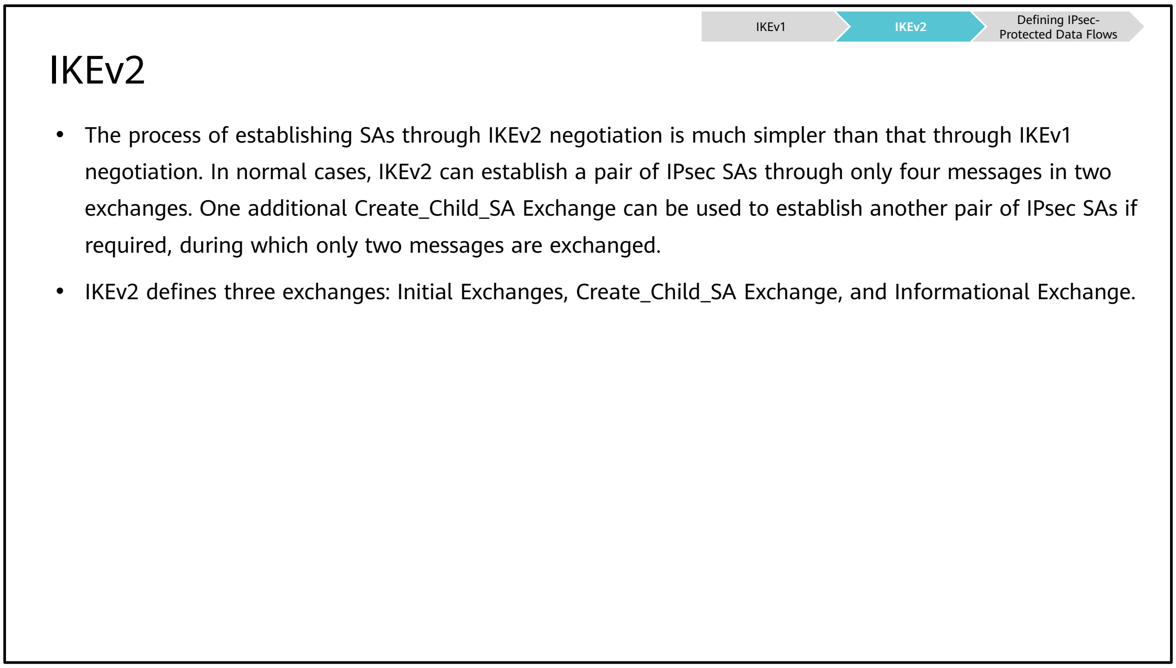
Sends acknowledged data

3

Accepts the information.

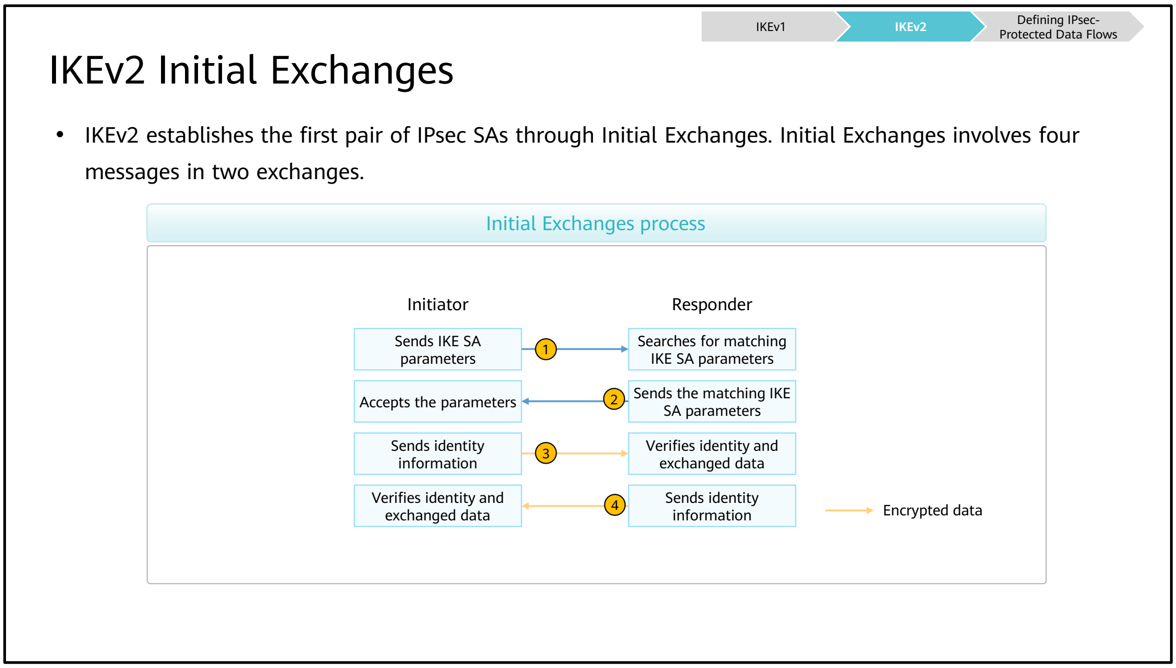
Encrypted data

- In IKEv1 phase 2, two IPsec SAs are established through three ISAKMP messages:
  - Message 1 is used by the initiator to send local security parameters and identity authentication information to the responder.
    - Security parameters include protected data flows and parameters to be negotiated, such as an IPsec proposal. Identity authentication information includes the keys generated in phase 1 and keying materials generated in phase 2, and can be used to authenticate the peer again.
  - Message 2 is used by the responder to send acknowledged security parameters and identity authentication information, and to generate new keys.
    - The encryption key and authentication key used for secure data transmission over IPsec SAs are generated based on the keys generated in phase 1 and parameters such as the SPI and protocol. This ensures that each IPsec SA has unique encryption and authentication keys.
  - Message 3 is used by the initiator to send acknowledged information to communicate with the responder. IKEv1 negotiation then ends and IPsec SAs are established.



IKEv2

- The process of establishing SAs through IKEv2 negotiation is much simpler than that through IKEv1 negotiation. In normal cases, IKEv2 can establish a pair of IPsec SAs through only four messages in two exchanges. One additional Create_Child_SA Exchange can be used to establish another pair of IPsec SAs if required, during which only two messages are exchanged.
- IKEv2 defines three exchanges: Initial Exchanges, Create_Child_SA Exchange, and Informational Exchange.



IKEv1 | IKEv2 | Defining IPsec-Protected Data Flows

IKEv2 Initial Exchanges

- IKEv2 establishes the first pair of IPsec SAs through Initial Exchanges. Initial Exchanges involves four messages in two exchanges.

Initial Exchanges process

Initiator

Responder

Sends IKE SA parameters

1

Searches for matching IKE SA parameters

Accepts the parameters

2

Sends the matching IKE SA parameters

Sends identity information

3

Verifies identity and exchanged data

Verifies identity and exchanged data

4

Sends identity information

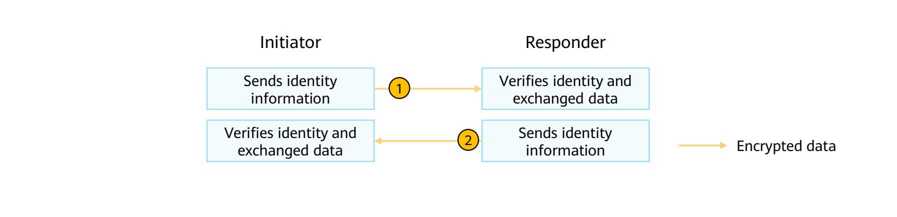
Encrypted data

- Messages 1 and 2 are used in exchange 1 (called IKE_SA_INIT). In exchange 1, IKE SA parameters are negotiated in plain text, including the encryption key, authentication key, random number, and DH key. After IKE_SA_INIT is complete, shared keying material is generated, from which all keys used by IPsec SAs are derived.
- Messages 3 and 4 are used in exchange 2 (called IKE_AUTH). In exchange 2, identities of the two parties and the first two messages are authenticated, and IPsec SA parameters are negotiated. IKEv2 supports Rivest-Shamir-Adleman (RSA) signature authentication, pre-shared key (PSK) authentication, and Extensible Authentication Protocol (EAP) authentication. The initiator omits the AUTH payload in message 3 to indicate that EAP authentication is required.

IKEv2 Create_Child_SA Exchange

- After one pair of IPsec SAs is established based on an IKE SA, Create_Child_SA Exchange can be performed to negotiate more pairs of IPsec SAs. In addition, Create_Child_SA Exchange can be performed for IKE SA re-negotiation.
- Create_Child_SA Exchange involves two messages in one exchange and corresponds to IKEv1 phase 2. The initiator in Create_Child_SA Exchange can be the initiator or responder in Initial Exchanges.

Create_Child_SA Exchange process



Initiator

Responder

Sends identity information

1

Verifies identity and exchanged data

Verifies identity and exchanged data

2

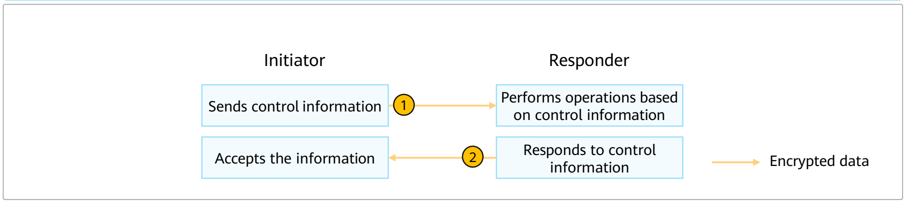
Sends identity information

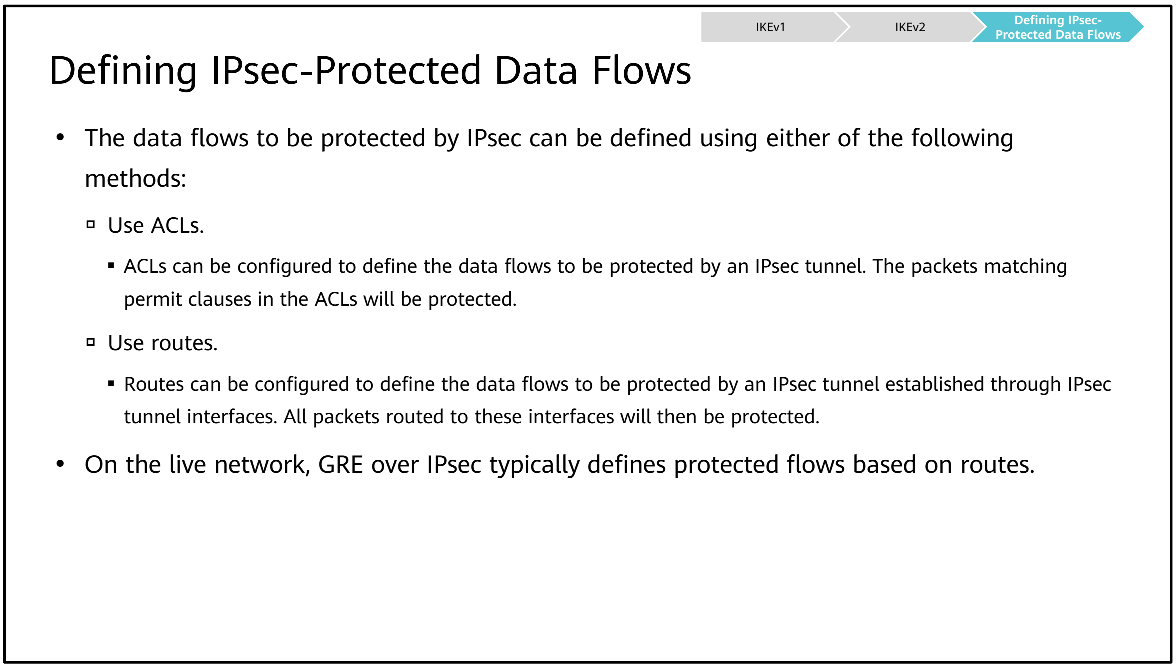
Encrypted data

IKEv2 Informational Exchange

- IKEv2 peers perform Informational Exchange to exchange control information, including error information and notifications.
- Informational Exchange must be performed under the protection of an IKE SA. Specifically, Informational Exchange is performed after Initial Exchanges are complete. Control information may belong to an IKE SA or a child SA. Therefore, Informational Exchange must be protected by the IKE SA or the IKE SA based on which the child SA is established accordingly.

Informational Exchange process


Initiator
Responder
Sends control information
1
Performs operations based on control information
Accepts the information
2
Responds to control information
Encrypted data

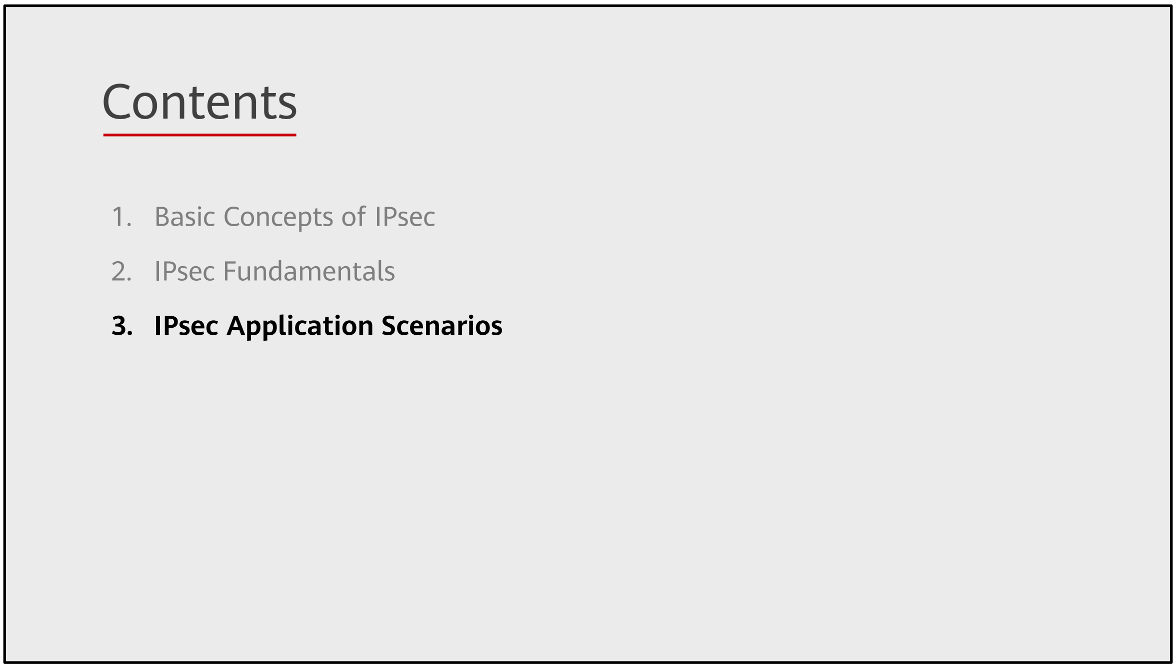


IKEv1 | IKEv2 | Defining IPsec-Protected Data Flows

Defining IPsec-Protected Data Flows

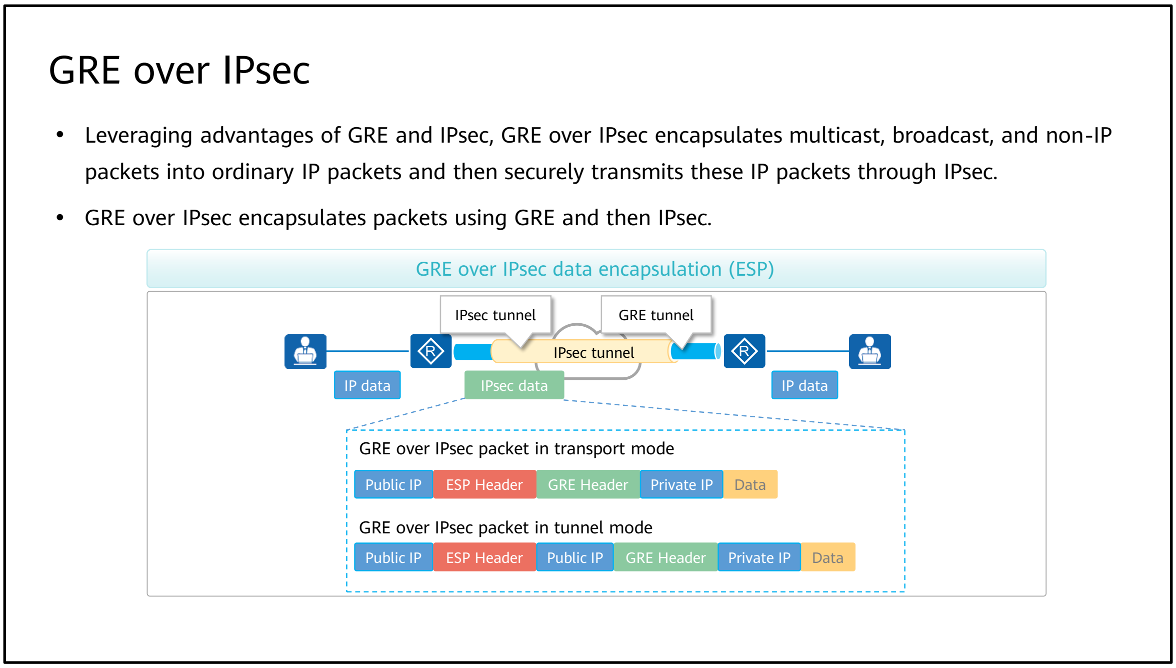
- The data flows to be protected by IPsec can be defined using either of the following methods:
  - Use ACLs.
    - ACLs can be configured to define the data flows to be protected by an IPsec tunnel. The packets matching permit clauses in the ACLs will be protected.
  - Use routes.
    - Routes can be configured to define the data flows to be protected by an IPsec tunnel established through IPsec tunnel interfaces. All packets routed to these interfaces will then be protected.
- On the live network, GRE over IPsec typically defines protected flows based on routes.

- The method of using routes has the following advantages:
  - Simplifies the IPsec configuration: IPsec-protected data flows are routed to tunnel interfaces, without the need to use ACLs to define the characteristics of traffic to be encrypted or decrypted.
  - Supports dynamic routing protocols.
  - Protects multicast traffic through GRE over IPsec.



Contents

1. Basic Concepts of IPsec
2. IPsec Fundamentals
3. **IPsec Application Scenarios**



GRE over IPsec

- Leveraging advantages of GRE and IPsec, GRE over IPsec encapsulates multicast, broadcast, and non-IP packets into ordinary IP packets and then securely transmits these IP packets through IPsec.
- GRE over IPsec encapsulates packets using GRE and then IPsec.

GRE over IPsec data encapsulation (ESP)

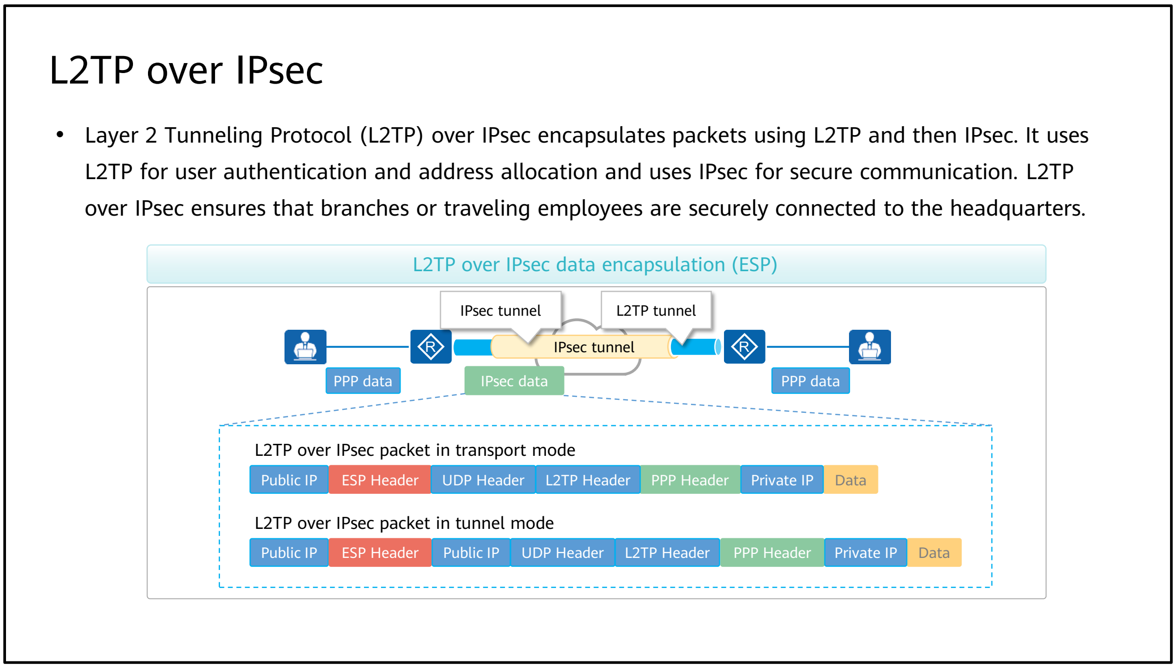
GRE over IPsec packet in transport mode

Public IP	ESP Header	GRE Header	Private IP	Data

GRE over IPsec packet in tunnel mode

Public IP	ESP Header	Public IP	GRE Header	Private IP	Data

- GRE over IPsec supports encapsulation in both tunnel and transport modes. An IPsec header needs to be added to packets if GRE over IPsec in tunnel mode is used, resulting in longer packets. In this case, packets are more likely to be fragmented. Therefore, GRE over IPsec in transport mode is recommended.
- In the IP header added during IPsec encapsulation, the source and destination addresses are the IP addresses of the local interface and remote interface to which an IPsec policy is applied.
- IPsec protects data flows from the GRE tunnel source to the GRE tunnel destination. In the IP header added during GRE encapsulation, the source and destination addresses are the source and destination addresses of a GRE tunnel.



L2TP over IPsec

- Layer 2 Tunneling Protocol (L2TP) over IPsec encapsulates packets using L2TP and then IPsec. It uses L2TP for user authentication and address allocation and uses IPsec for secure communication. L2TP over IPsec ensures that branches or traveling employees are securely connected to the headquarters.

L2TP over IPsec data encapsulation (ESP)

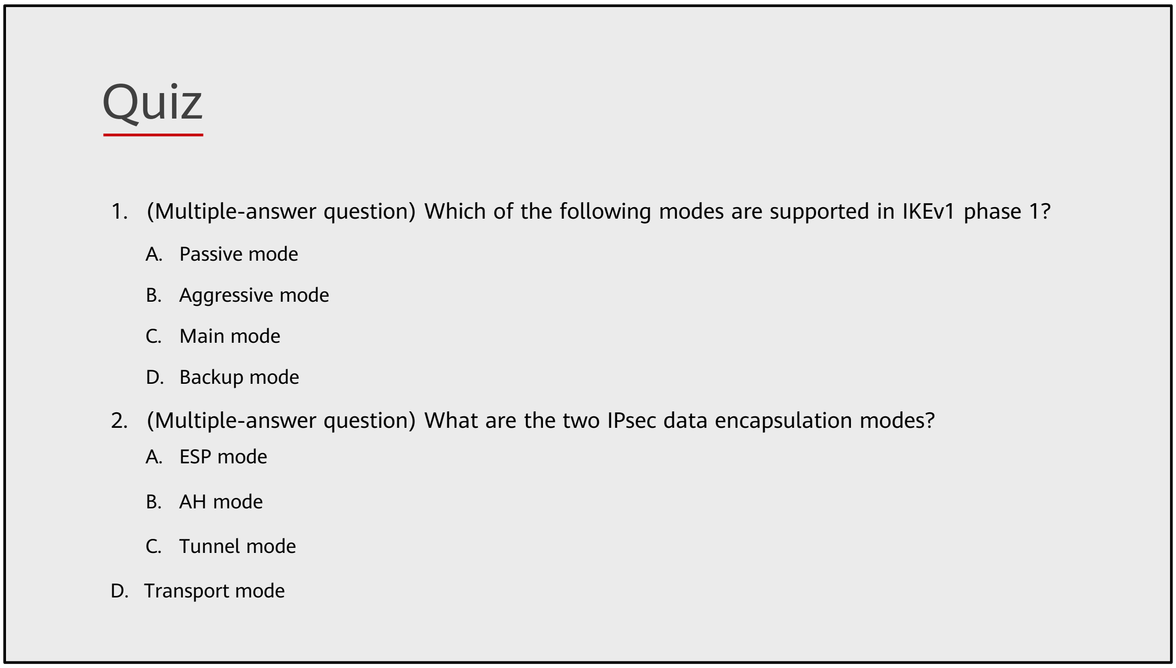
L2TP over IPsec packet in transport mode

Public IP	ESP Header	UDP Header	L2TP Header	PPP Header	Private IP	Data

L2TP over IPsec packet in tunnel mode

Public IP	ESP Header	Public IP	UDP Header	L2TP Header	PPP Header	Private IP	Data

- L2TP encapsulation and then IPsec encapsulation are performed on packets transmitted over an L2TP over IPsec tunnel. In the IP header added during IPsec encapsulation, the source and destination addresses are the IP addresses of the local interface and remote interface to which an IPsec policy is applied.
- IPsec needs to protect the data flows from the L2TP tunnel source to the L2TP tunnel destination. In the IP header added to packets during L2TP encapsulation, the source and destination addresses are the source and destination addresses of an L2TP tunnel. When a branch connects to the headquarters, the source address of the L2TP tunnel is the IP address of the outbound interface on the L2TP access concentrator (LAC), and the destination address is the IP address of the inbound interface on the L2TP network server (LNS).
- A public IP header is added to packets during L2TP encapsulation, and another public IP header is added to packets if L2TP over IPsec in tunnel mode is used, resulting in longer packets, which are prone to being fragmented. Therefore, L2TP over IPsec in transport mode is recommended.
- The L2TP over IPsec negotiation process and packet encapsulation process are similar when traveling employees are remotely connected to the headquarters and when branch employees are connected to the headquarters. The difference is that, L2TP and IPsec encapsulation is performed on clients when traveling employees are remotely connected to the headquarters. The L2TP tunnel source address is the private address assigned to a client and can be any address in the IP address pool configured on the LNS. The L2TP tunnel destination address is the address of the inbound interface on the LNS.

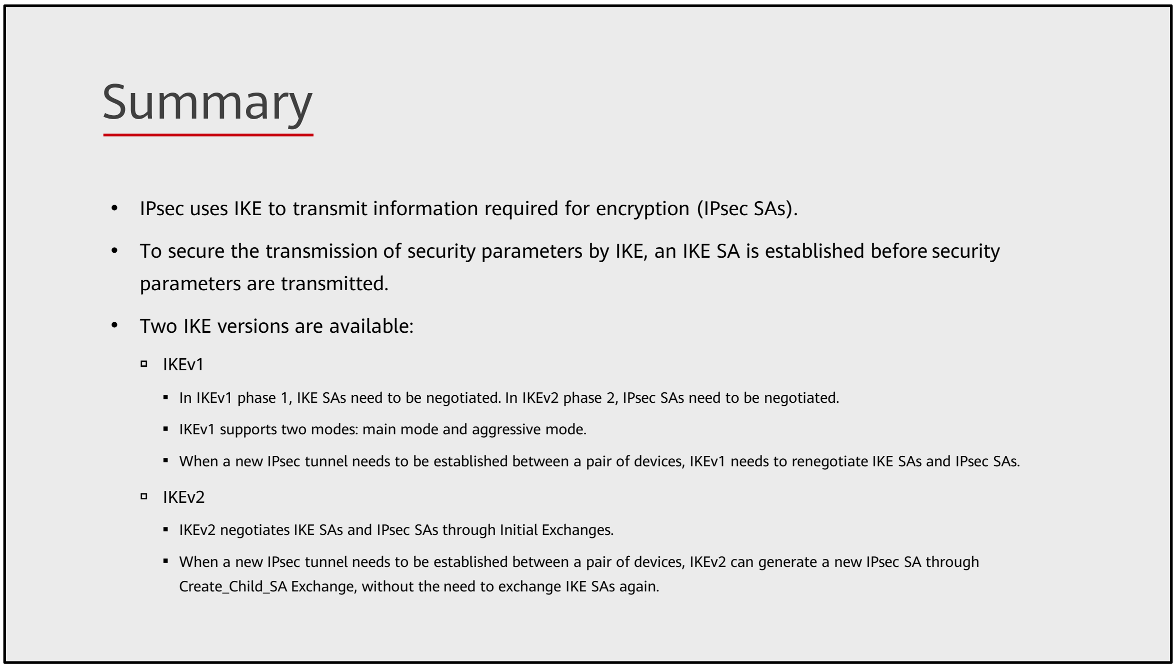


Quiz

1. (Multiple-answer question) Which of the following modes are supported in IKEv1 phase 1?
   - A. Passive mode
   - B. Aggressive mode
   - C. Main mode
   - D. Backup mode
2. (Multiple-answer question) What are the two IPsec data encapsulation modes?
   - A. ESP mode
   - B. AH mode
   - C. Tunnel mode

D. Transport mode

- 1. BC
- 2. CD



Summary

- IPsec uses IKE to transmit information required for encryption (IPsec SAs).
- To secure the transmission of security parameters by IKE, an IKE SA is established before security parameters are transmitted.
- Two IKE versions are available:
  - IKEv1
    - In IKEv1 phase 1, IKE SAs need to be negotiated. In IKEv2 phase 2, IPsec SAs need to be negotiated.
    - IKEv1 supports two modes: main mode and aggressive mode.
    - When a new IPsec tunnel needs to be established between a pair of devices, IKEv1 needs to renegotiate IKE SAs and IPsec SAs.
  - IKEv2
    - IKEv2 negotiates IKE SAs and IPsec SAs through Initial Exchanges.
    - When a new IPsec tunnel needs to be established between a pair of devices, IKEv2 can generate a new IPsec SA through Create_Child_SA Exchange, without the need to exchange IKE SAs again.