

Application of Cryptographic Technologies

Lecture 9

HCIA-Security

Prepared by
Dr. Abdelrhman Ahmed

- **Cryptographic technologies ensure the security of data transmission on the network and protect data from tampering and spying. Signature technologies ensure data integrity and prove the identity of the data sender. PKI certificate authentication technologies verify the validity of public keys and ensure that users access secure and legitimate networks.**
- **By using these technologies, enterprises can prevent unauthorized users from accessing their enterprise networks. Also, secure channels can be established between enterprise branches to ensure security of enterprise data.**

Objectives

- **Upon completion of this course, you will be able to:**
 - ❑ **Describe the scenarios in which cryptographic technologies are applied.**
 - ❑ **Configure different VPN technologies.**

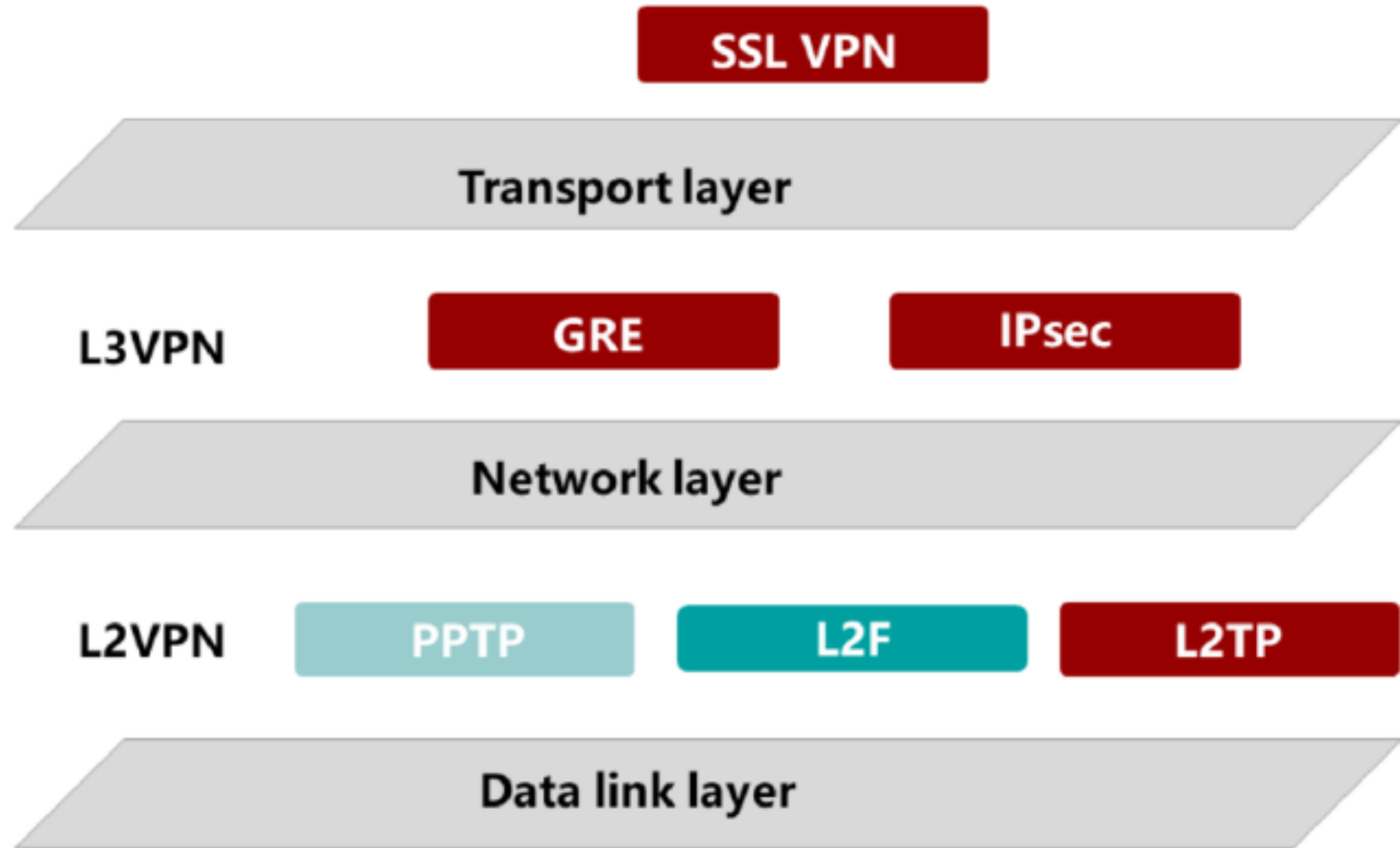
Application of Cryptography

- **Cryptography applications include digital envelopes, digital signatures, and digital certificates.**
 - **Digital envelope:** ensures the confidentiality of data in transit using symmetric and asymmetric encryption.
 - **Digital signature:** ensures the integrity of data transit using hash algorithms.
 - **Digital certificate:** ensures the non-repudiation of data transmission by authenticating the public key using a third-party authority (CA).

- Digital envelopes, digital signatures, and digital certificates are applied to different scenarios, listed as follows:
- VPN: To ensure data confidentiality, many VPN technologies need to use encryption and decryption technologies, such as IPsec VPN and SSL VPN.
- IPv6: To prevent the device from being spoofed, secure neighbor discovery (SEND) router authorization can be configured on the device. The digital certificate technology can be used for selecting legitimate gateway devices.
- HTTPS login: The administrator can use HTTPS to securely log in to the web UI of the HTTPS server and manage network devices. To improve security of SSL connections, the CA trusted by the web browser is configured to issue local certificates for the HTTPS client. Then the web browser can verify local certificates, avoiding malicious attacks and ensuring secure login.
- System login authorization: A digest algorithm processes the user password to generate a digest, which is stored and compared with the user-supplied password the next time the user logs in.
- The most important application scenario is VPN.
- This course introduces several encrypted VPNs and some common VPN technologies.

What is a VPN?

- **A virtual private network (VPN) is a private data channel established across a shared public network. It connects all networks or endpoint devices that need to access the virtual network to form a dedicated network that provides a certain degree of security and quality of service (QoS).**
- **Virtual: Users use the toll lines of the Internet to set up their own private networks, without requiring physical dedicated toll lines.**
- **Private network: Users can customize a network best suited to their needs.**



Application Scenarios of VPNs

- **Site-to-Site VPN**
 - **Connection between two LANs**
 - **Applicable VPN technologies: IPsec, L2TP, L2TP over IPsec, GRE over IPsec, and IPsec over GRE**
- **Client-to-Site VPN**
 - **Connection between clients and an enterprise intranet**
 - **Applicable VPN technologies: SSL, IPsec, L2TP, and L2TP over IPsec**

- **L2TP**

- ☐ **A tunneling protocol set to transparently transmit PPP packets between a user and an enterprise server. It provides support for the tunnel transmission of packets at the PPP link layer.**

- **The L2TP VPN applies to the following scenarios:**

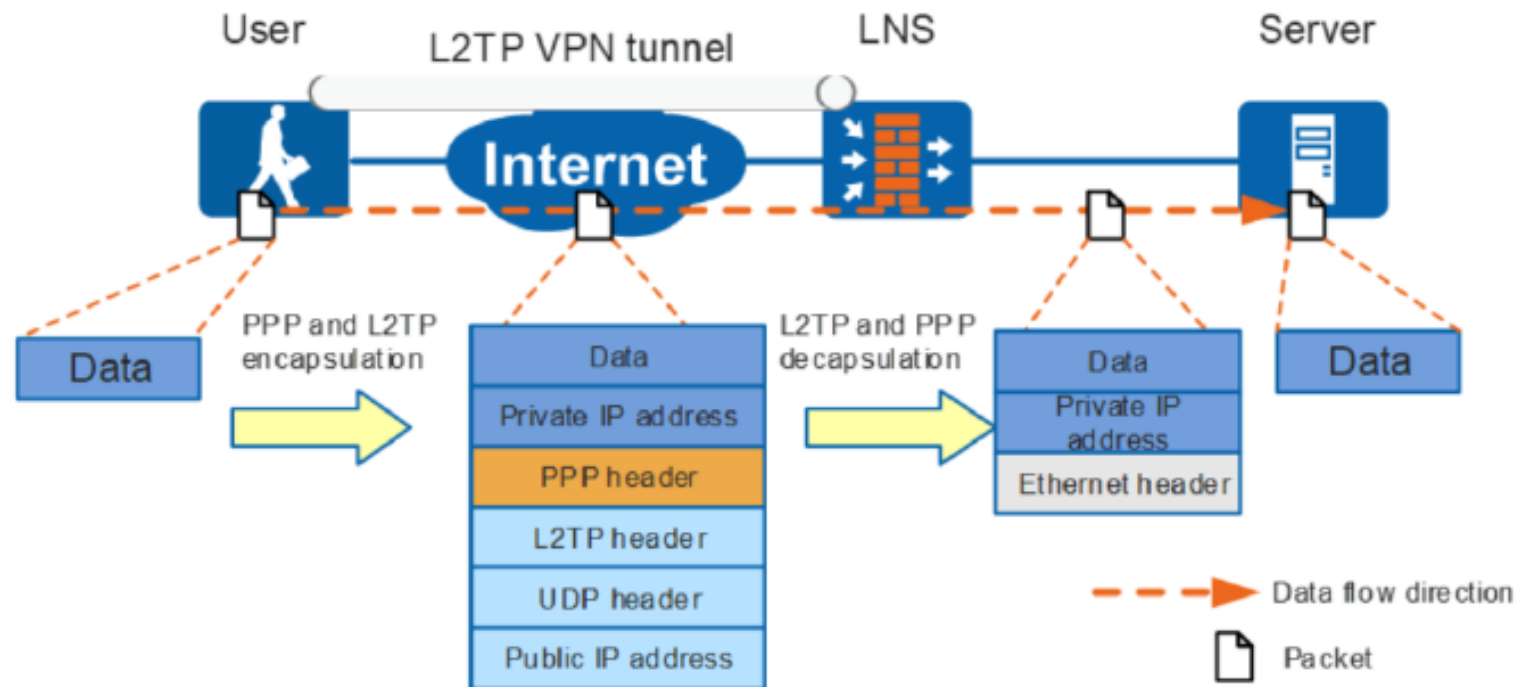
- ☐ **NAS-initiated VPN**

- ☐ **Automatic dialing on the LAC**

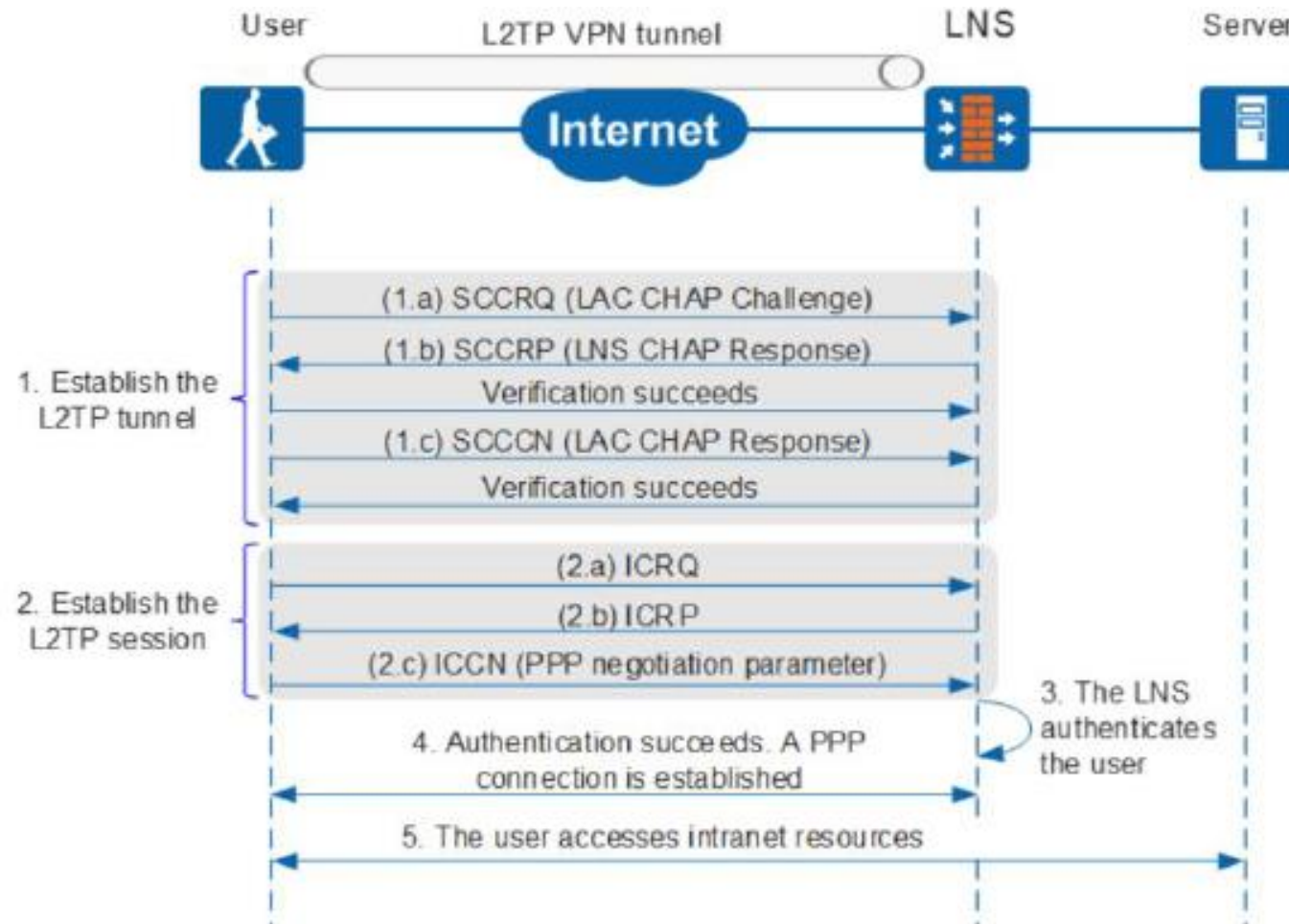
- ☐ **Client-initiated VPN**

Client-Initiated L2TP VPNs

Generally, this type of L2TP VPN is used when employees need to access servers at HQ using devices such as PCs and mobile phones when they are on business trips. This is the most commonly used L2TP dial-up mode.



Client-Initiated VPN Tunneling & Session Establishment Process

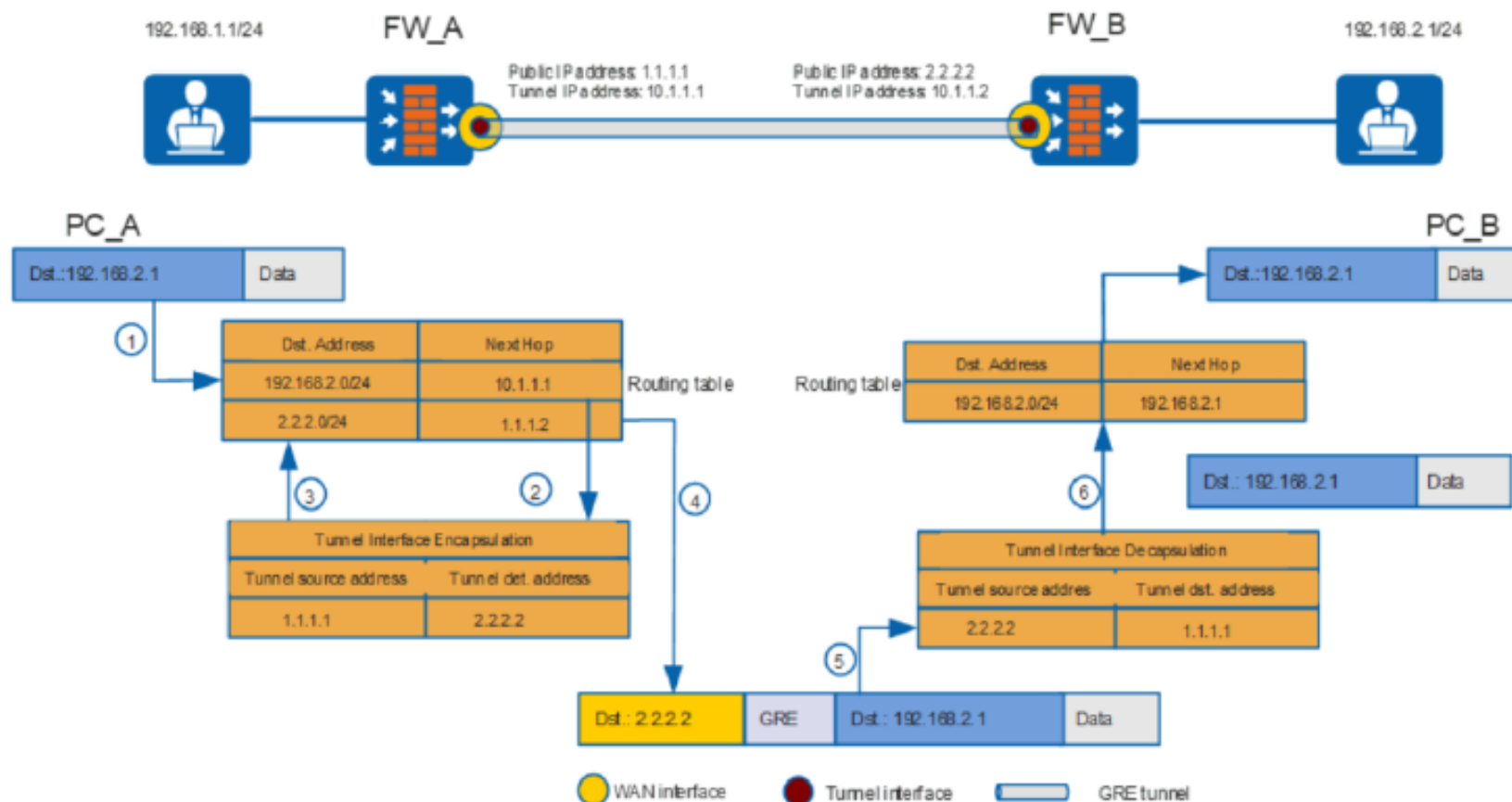


Overview of GRE VPNs

- **General Routing Encapsulation (GRE) is a L3VPN encapsulation technology. GRE encapsulates the packets of a wide variety of network layer protocols, such as Internetwork Packet Exchange (IPX), IP, and AppleTalk, into IP tunneling packets, so that these packets can be transmitted over heterogeneous networks. The channel for transmitting packets over heterogeneous networks is called a 'tunnel'.**

Chapter
09

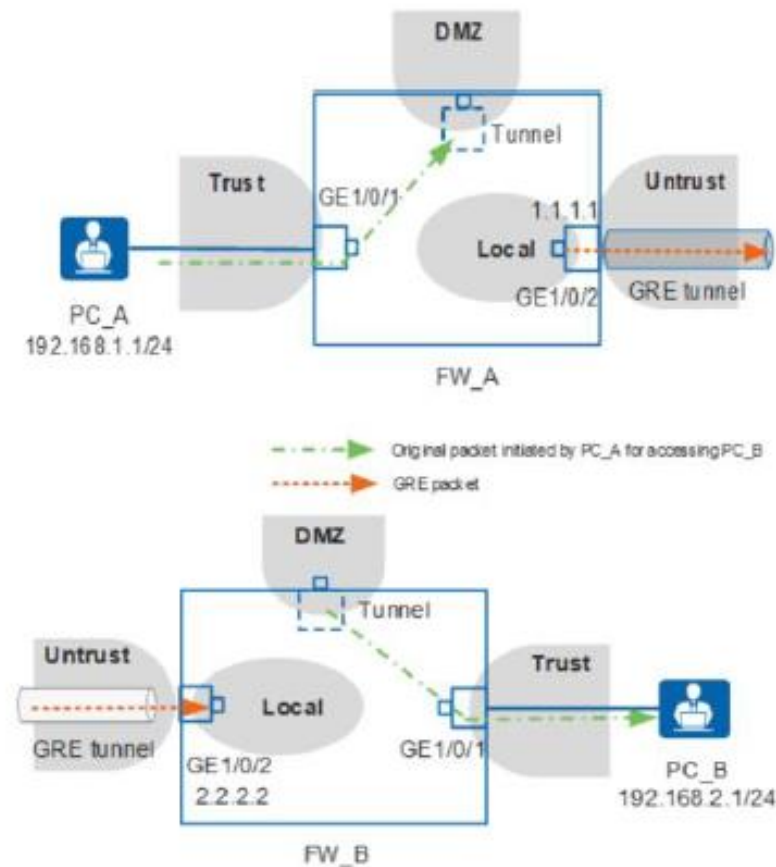
GRE Packet Handling Process



Chapter
09

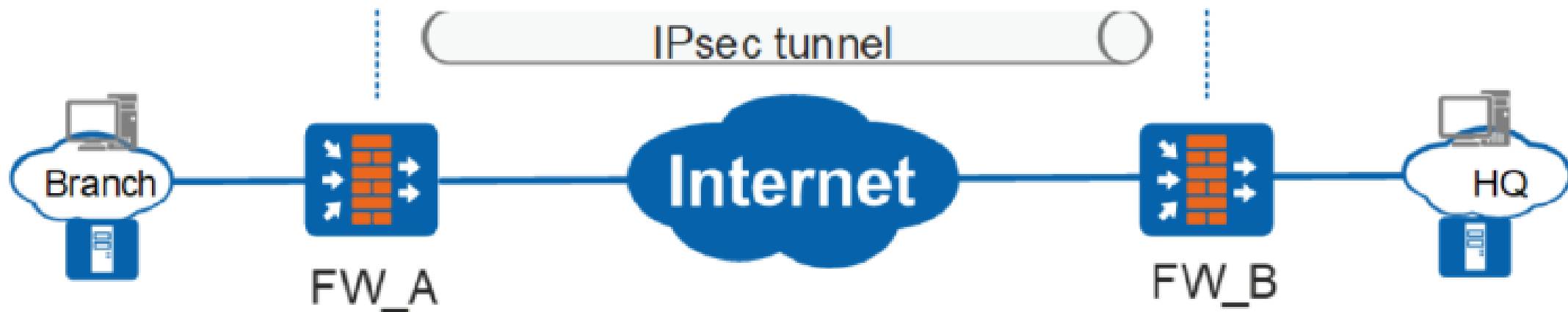
GRE Security Policies

- When an original packet is sent from PC_A to the tunnel interface, the packet is sent from the Trust zone to the DMZ. When FW_A encapsulates and forwards it, it is sent from the Local zone to the Untrust zone.
- Upon reaching FW_B, FW_B decapsulates it. In this process, the packet is sent from the Untrust zone to the Local zone. When FW_B decapsulates the GRE packet and forwards the original packet, the packet is sent from the DMZ to the Trust zone.



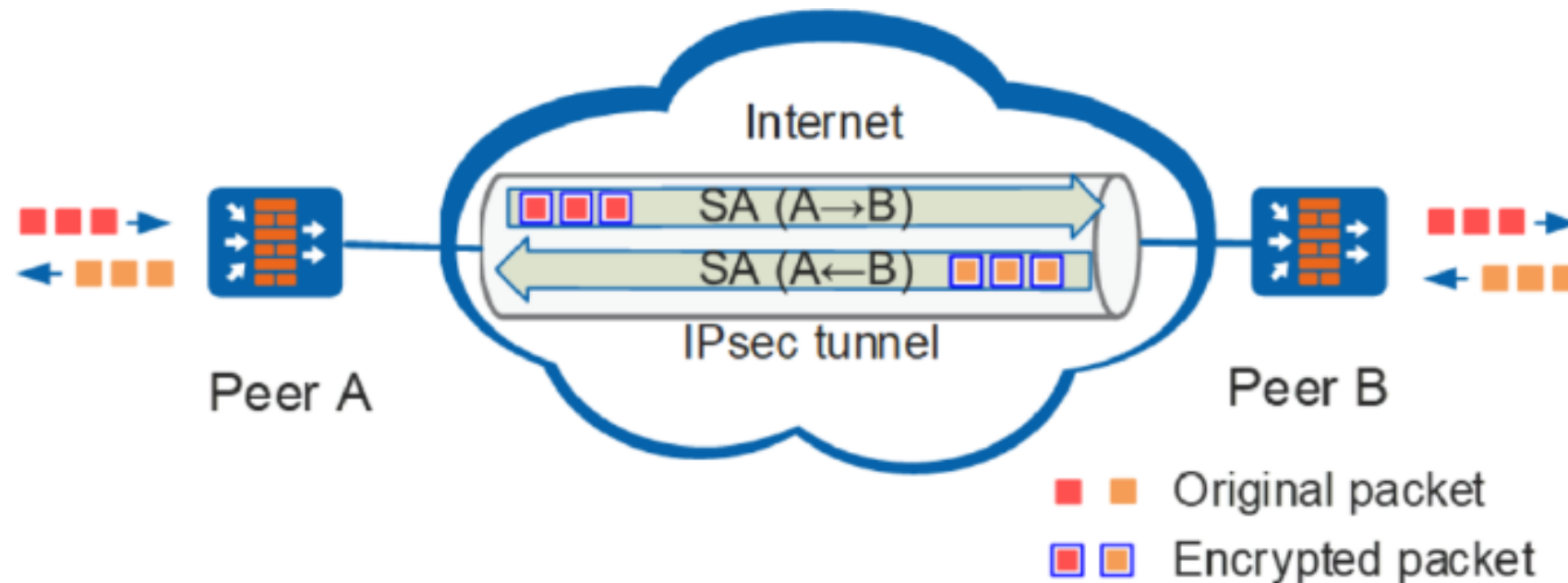
Overview of IPsec VPNs

- The IP Security (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. An IPsec VPN is a network layer VPN established through an IPsec tunnel.



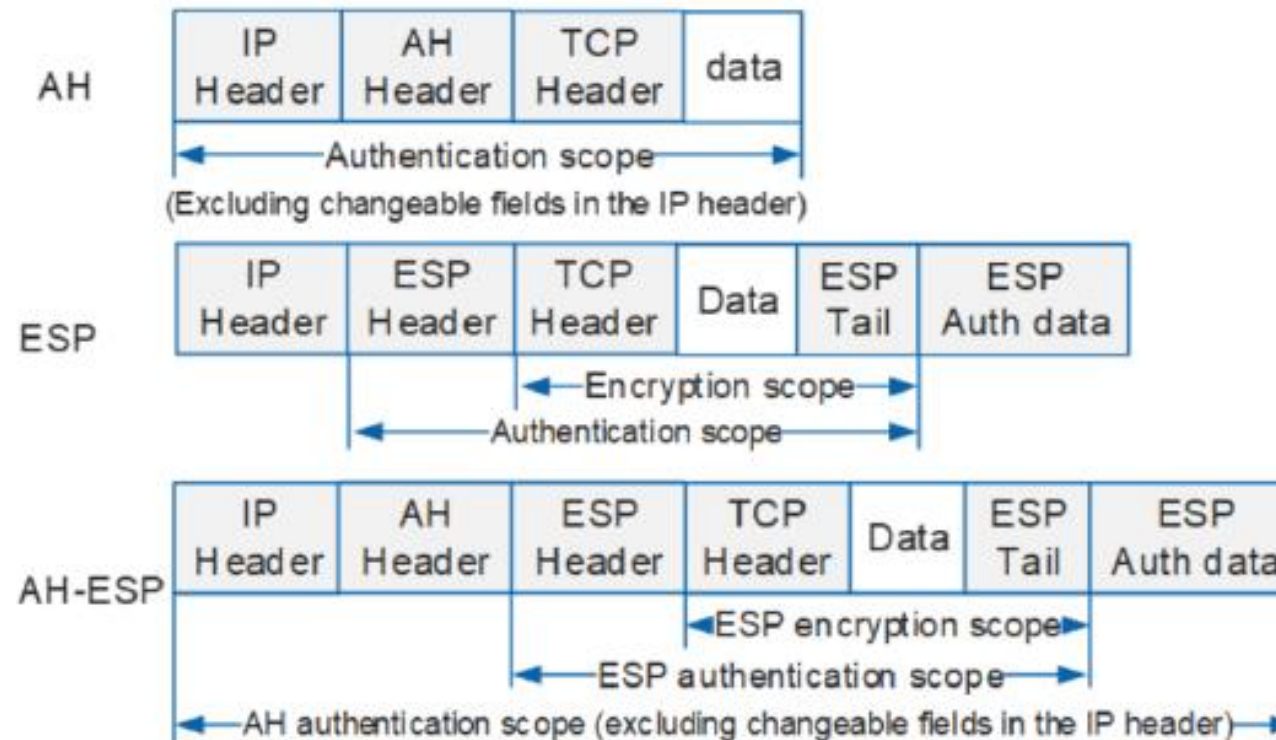
IPSec SA

- An IPsec security association (SA) needs to be established between IPsec peers (two IPsec endpoints) before IPsec implements secure data transmission.
- The SA is an agreement between IPsec peers in communication.

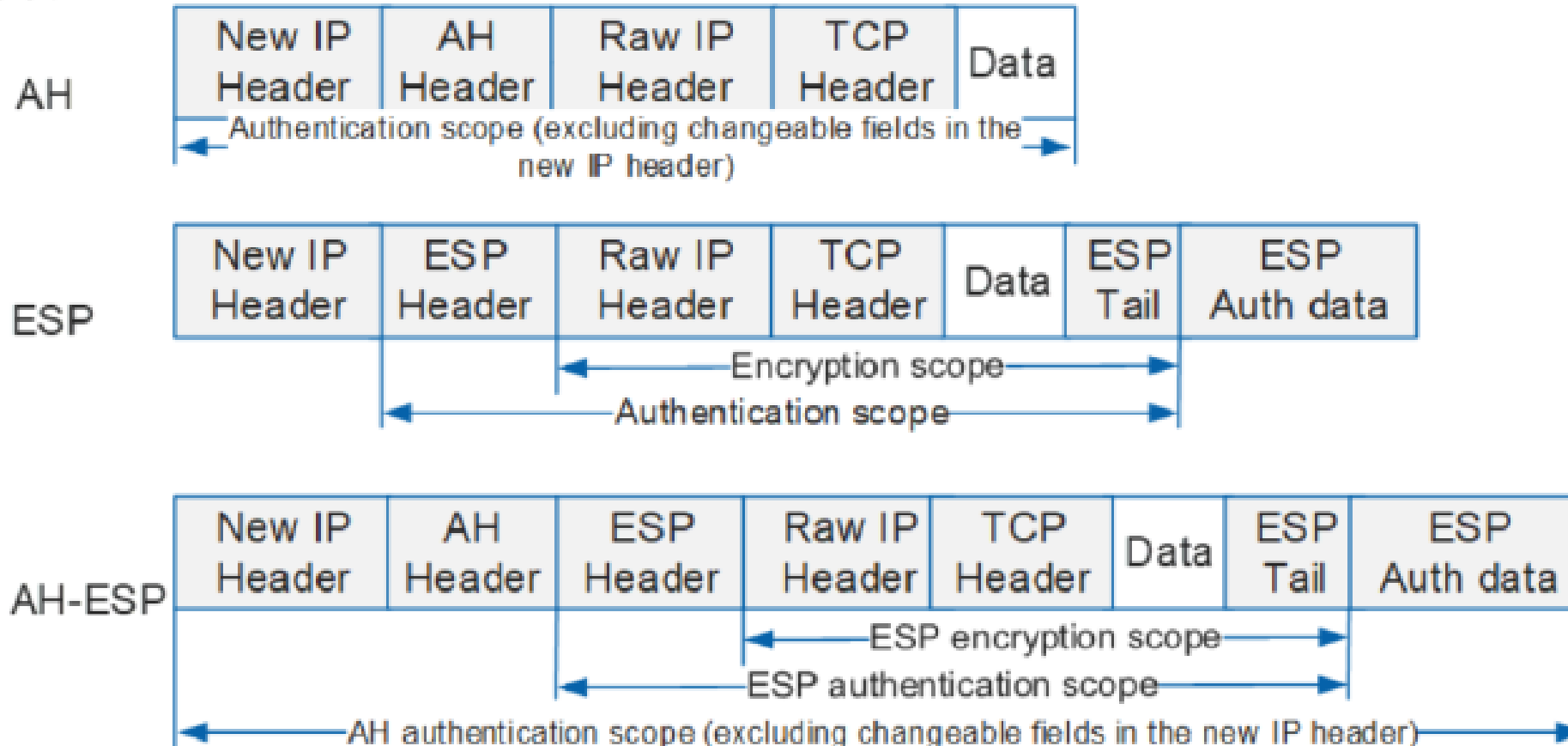


Encapsulation in Transport Mode

- In transport mode, an AH or ESP header is added between an IP header and a transport-layer protocol header to protect the TCP, UDP, or ICMP payload.

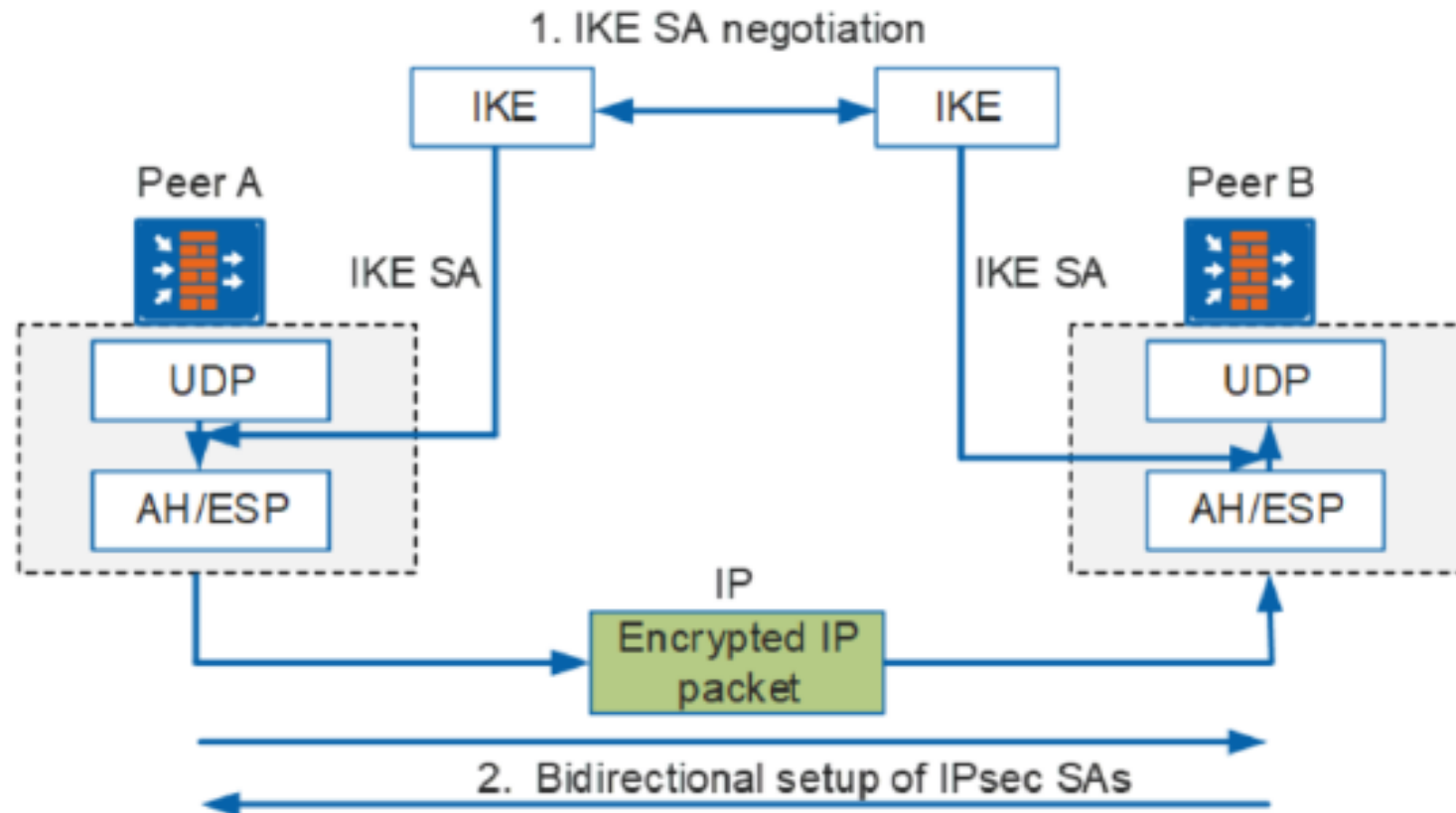


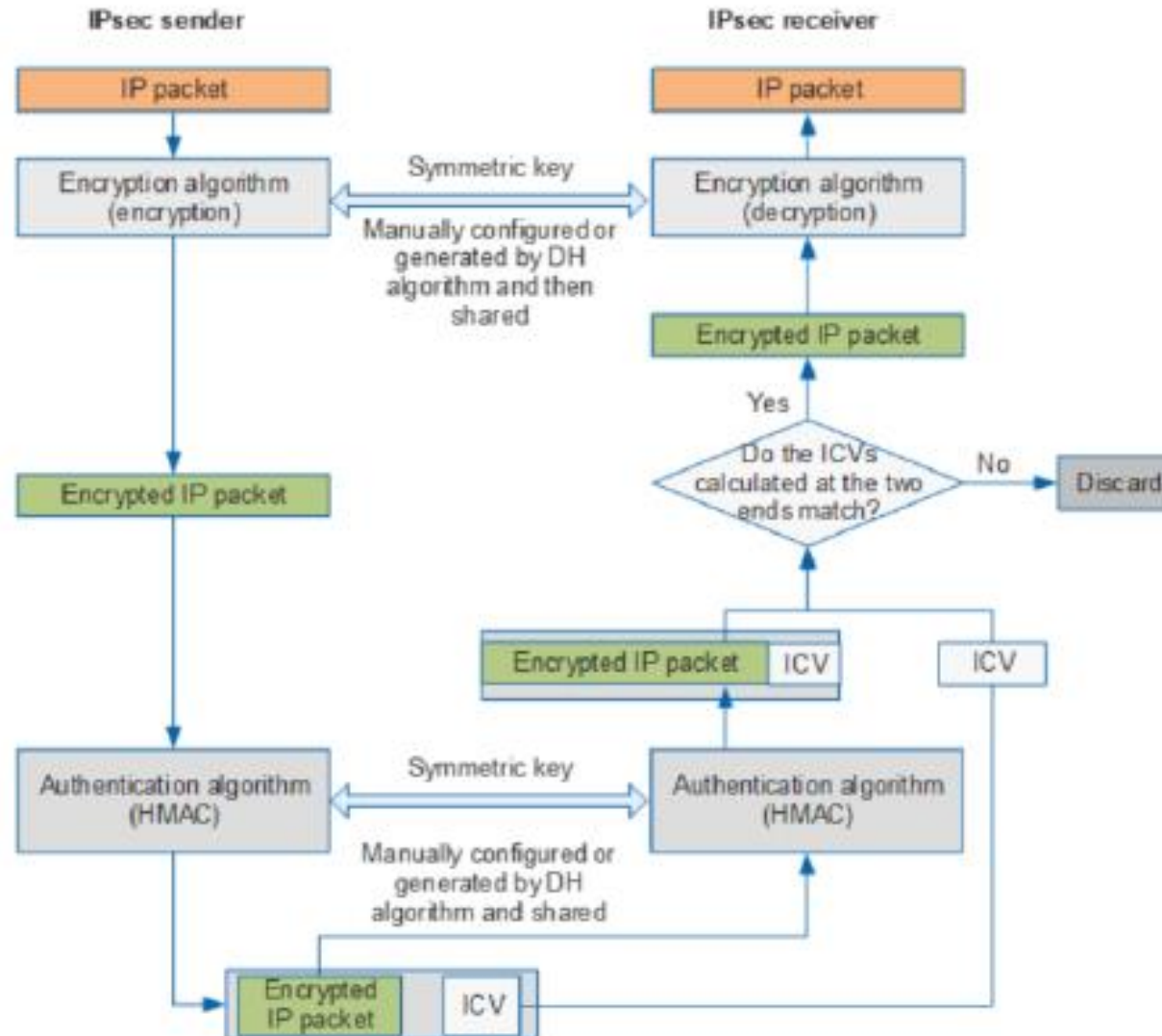
- In tunnel mode, an AH or ESP header is added outside the raw IP header, and a new IP header is added outside the AH or ESP header to protect the IP header and Payload.



IKE SA

- The IKE SA serves the IPsec SA by providing automatic key negotiation and establishing the IPsec SA.

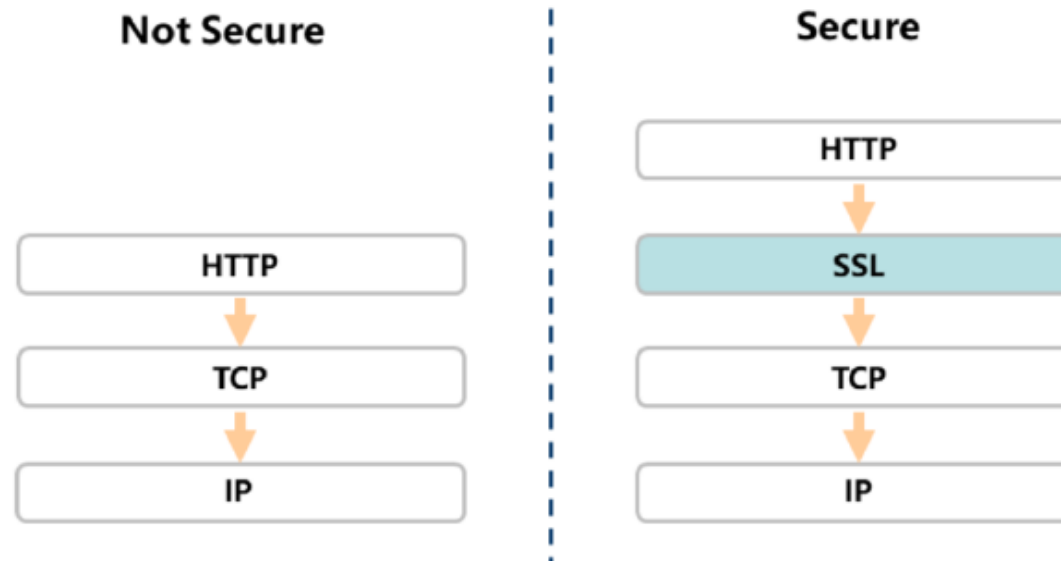




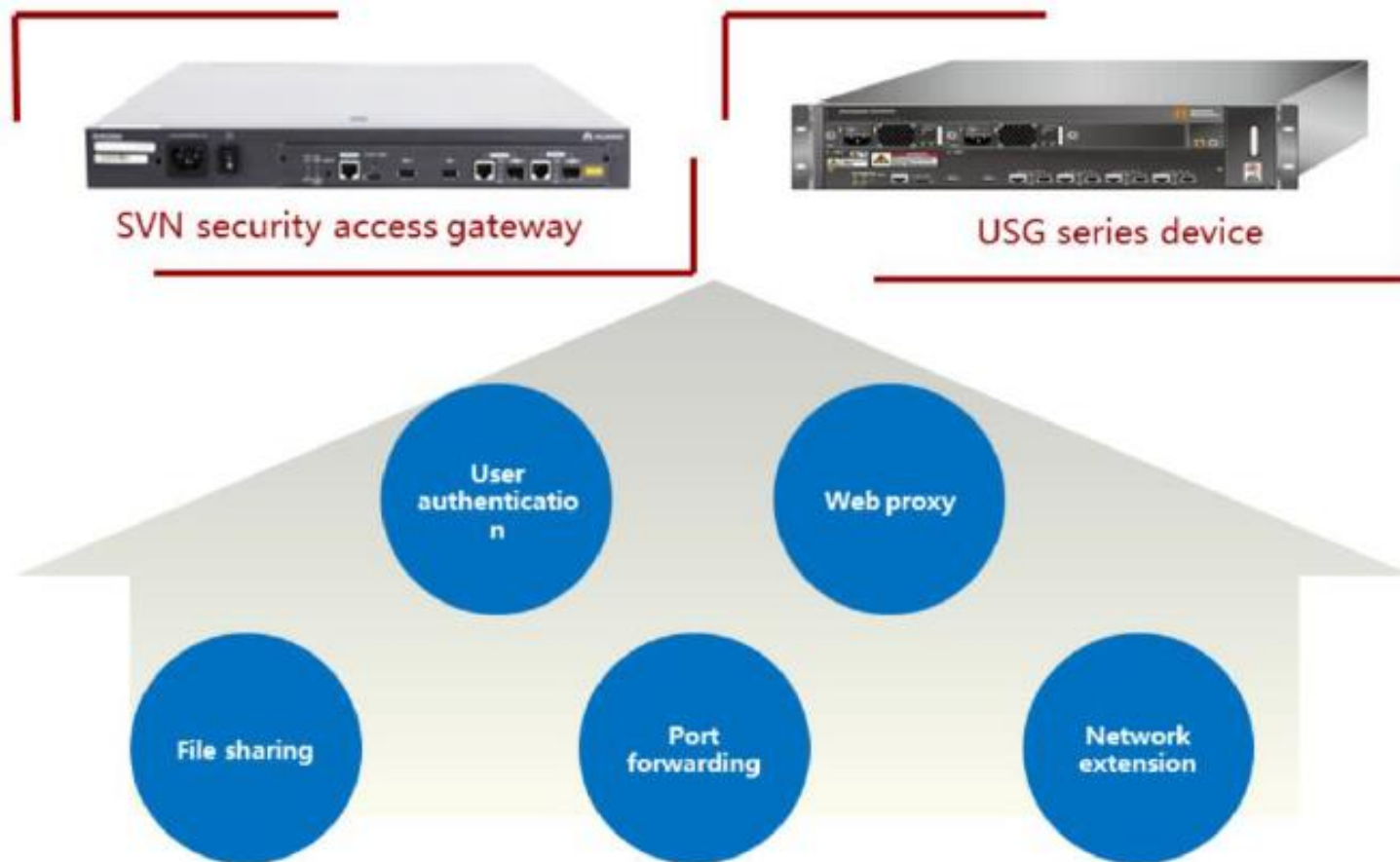
- **IPsec uses symmetric encryption algorithms to encrypt and decrypt data.**
- **The authentication mechanism allows the data receiver to identify the data sender in IP communications and determines whether data is tampered with during transmission.**
- **IPsec uses the Keyed-Hash Message Authentication Code (HMAC) function for authentication. The HMAC function verifies the integrity and authenticity of data packets by comparing digital signatures.**

Overview of SSL VPNs

- SSL is a security protocol. It provides secure connections for TCP-based application layer protocols.
- IPsec implements encryption for secure transmission. However, IPsec encryption and authentication have problems in some scenarios, for example, NAT traversal. Because of its unique attributes, the SSL VPN takes effect only at the application layer and does not require a user security VPN client. Therefore, its application scope is wider, and it is more convenient.
- SSL provides secure connections for HTTP and is widely used in various fields, such as e-commerce and online banking, to ensure secure data transmission.



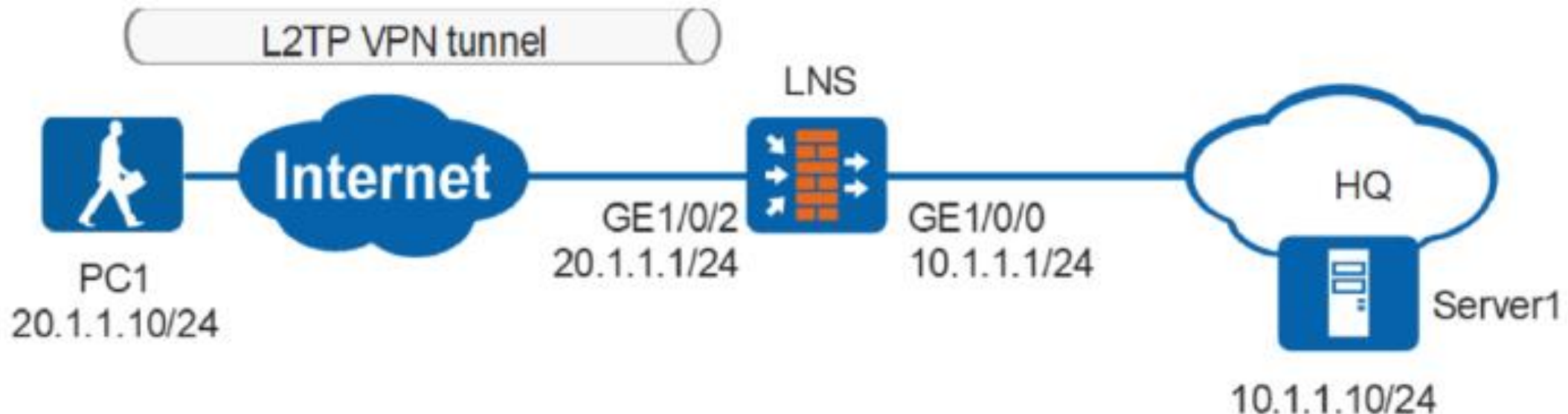
Main Functions of an SSL VPN



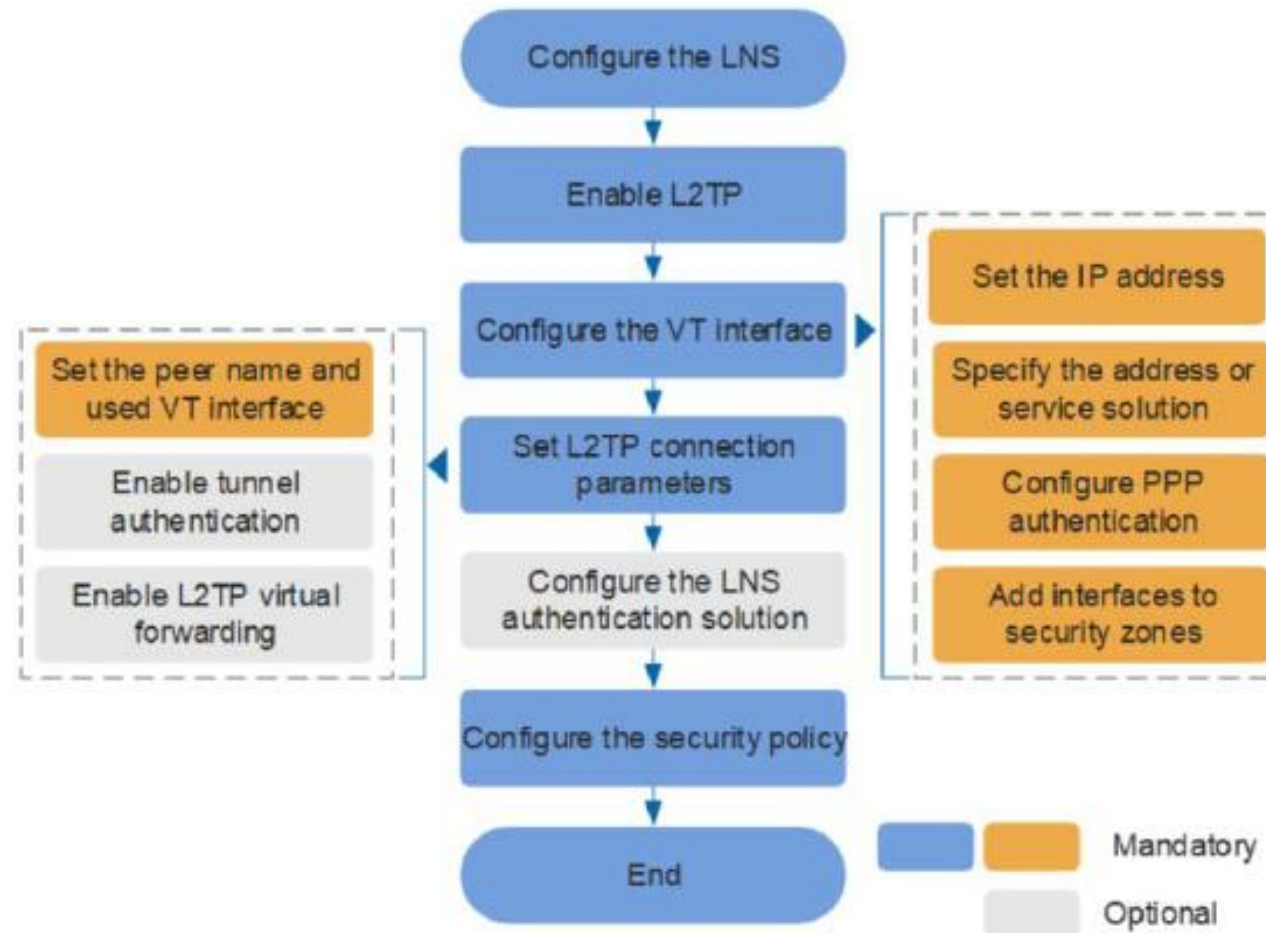
Application Scenario of Client-Initialized L2TP VPN

- Requirements

- A company has its own VPN and a VPN gateway (USG firewall) is deployed at the Internet egress of the headquarters. Employees on the move need to communicate with the company's internal servers through L2TP tunnels.



L2TP VPN Configuration Procedure



Enabling the L2TP Function

- Choose Network > L2TP > L2TP. On the Configure L2TP page, select Enable for L2TP and click Apply.

The screenshot displays the Huawei USG6330 web management interface. The top navigation bar includes 'Dashboard', 'Monitor', 'Policy', 'Object', 'Network' (highlighted with a red box and a red circle with '1'), and 'System'. The left sidebar lists various configuration options, with 'L2TP' (highlighted with a red box and a red circle with '2') selected under the 'Network' category. The main content area shows the 'Configure L2TP' page. The 'L2TP' checkbox is checked and labeled 'Enable' (highlighted with a red box and a red circle with '3'). The 'Idle Tunnel Timeout' is set to 1800 seconds. The 'Apply' button is highlighted with a red box and a red circle with '4'. Below the configuration section, the 'L2TP Group List' is shown, containing a table with one entry: 'default-ins' with group type 'LNS'.

Group Name	Group Type	Local Tunnel Name
default-ins	LNS	

Chapter
09

Setting the L2TP Parameters

- In L2TP Group List, click Add to set L2TP group parameters.

The screenshot shows the 'Add L2TP' configuration window with the following settings:

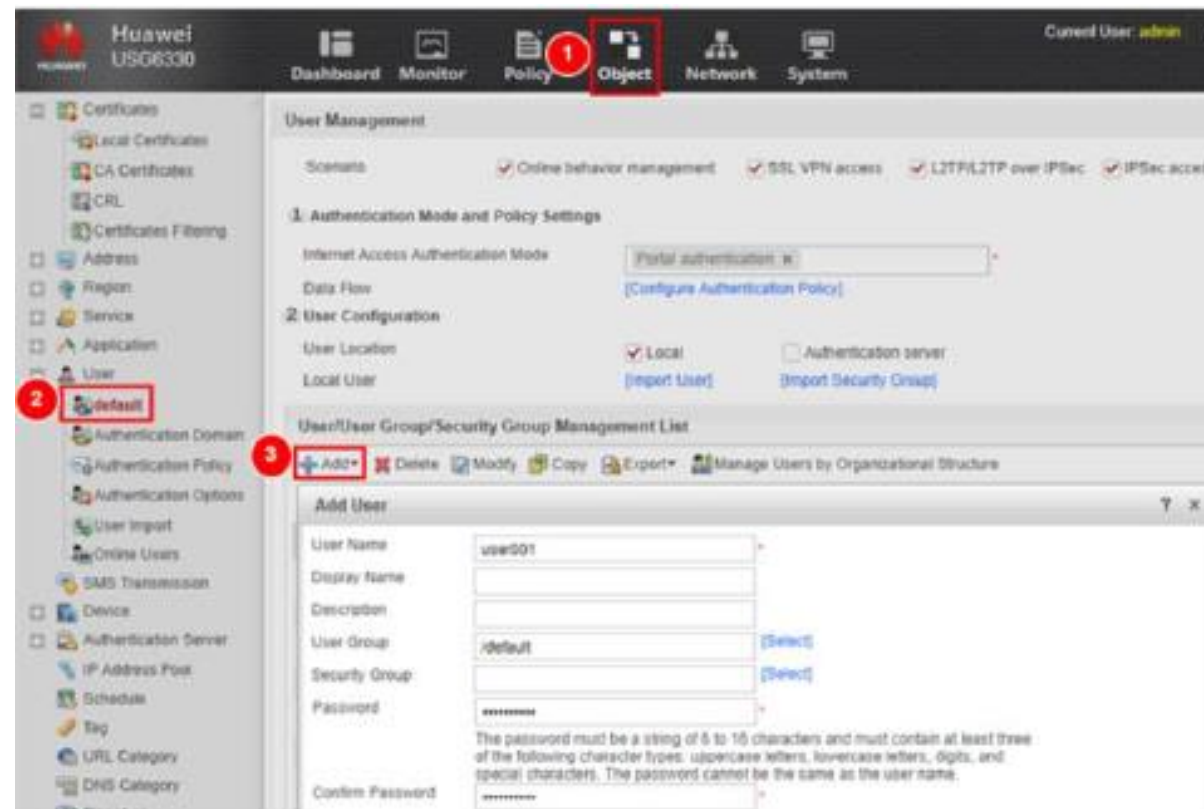
- Group Name: g1
- Group Type: ☒ LNS
- Local Tunnel Name: client
- Peer Tunnel Name: client
- Tunnel Password Authentication: ☒
- Password: [Redacted]
- Confirm Password: [Redacted]
- Authentication Domain: default
- Associated Zone: untrust
- L2TP Authentication: ☐ PAP, ☒ CHAP
- Tip: To ensure that the negotiation messages are interworking, you need to enable the two-way security policy. [\[Add Security Policy\]](#)
- User Address Assignment Setting:
 - Server Address/Subnet Mask: 192.168.1.1/255.255.255.0
 - Address/Address Pool: ☐ IP Address Pool, ☒ PeerAddress
 - PeerAddress: 192.168.1.10
- Advanced: [Expanded]

Buttons: OK, Cancel

Chapter
09

Setting Dial-up User Information

- Choose Object > User. Click the default authentication domain. On the User Management page, click Add and set the username and password.



Chapter
09

Setting the VPN Client & Authentication



New Connection

SSL VPN
L2TP/IPSec
L2TP
IPSec
Import

L2TP Configuration

Connection Name: L2TP

Description:

DNS Server Address: 20.1.1.1

Tunnel Configuration

Tunnel Name: client

Authentication Mode: CHAP

☒ Enable Tunnel Authentication

☒ Show Authentication Password

Use VPN connections to access the following addresses:

IP Address	Subnet Mask
10.1.1.0	255.255.255.0

SecoClient HUAWEI

Login Information

Server Address: 20.1.1.1

User Name: user001

Password:

☒ Save password ☐ Automatic login

Login

SecoClient HUAWEI

Connect: L2TP

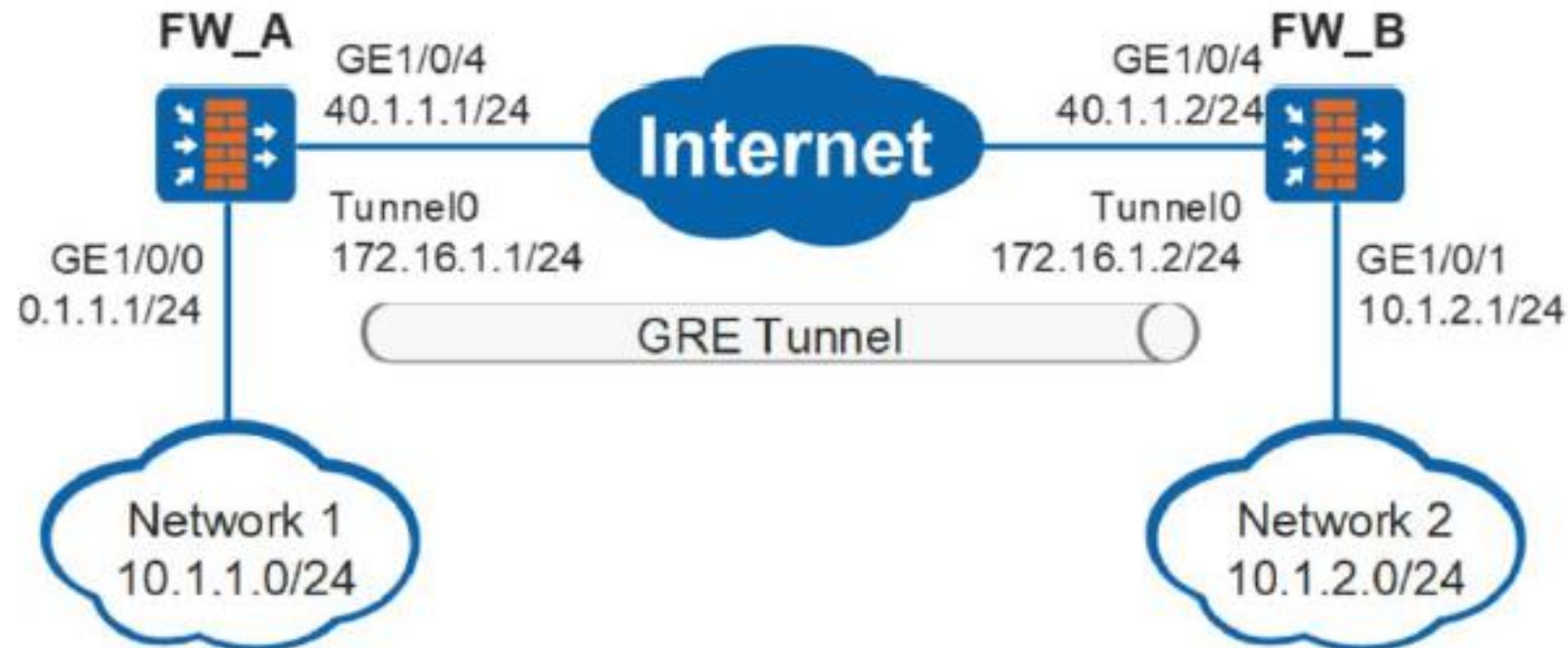
Disconnect

Proxy Settings

Application Scenario of GRE

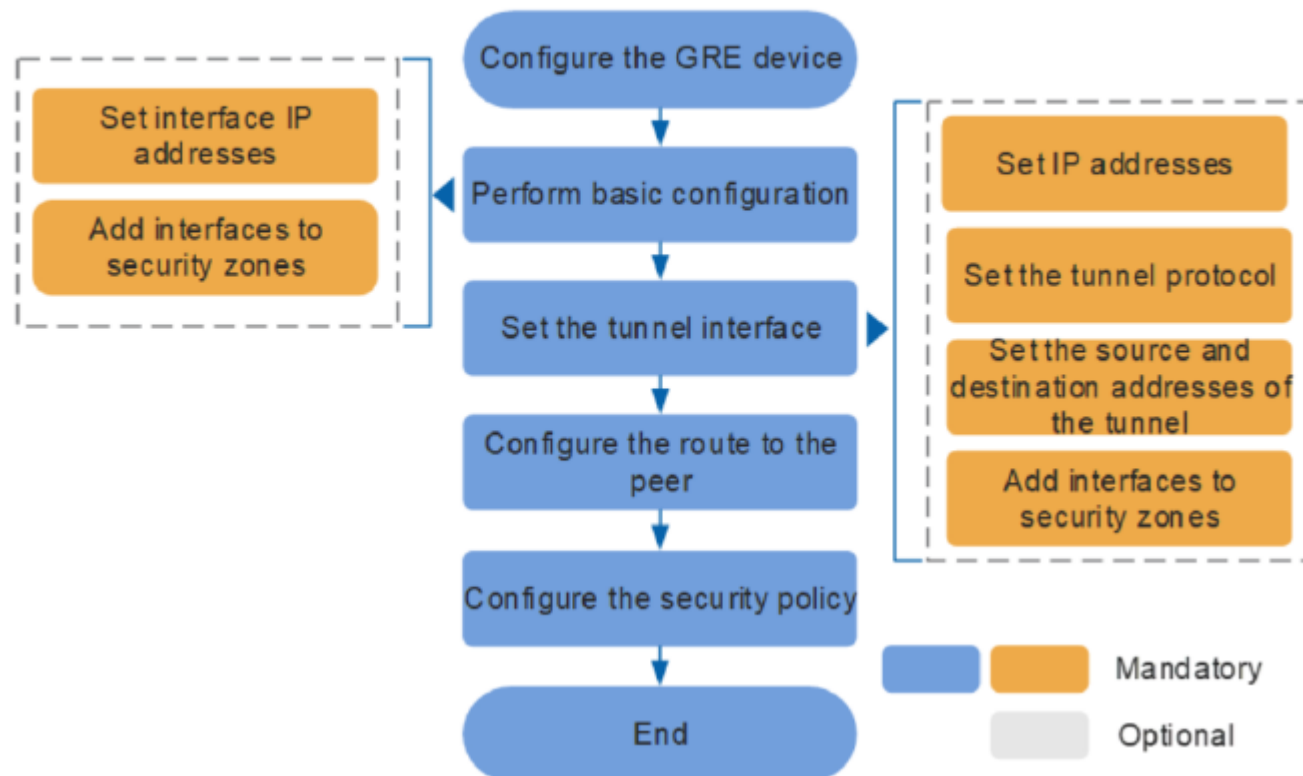
- Requirements

- The two subnets (Network 1 and Network 2) that run the IP protocol communicate with each other through the GRE tunnel established between FW A and FW B.



GRE VPN Configuration Procedure

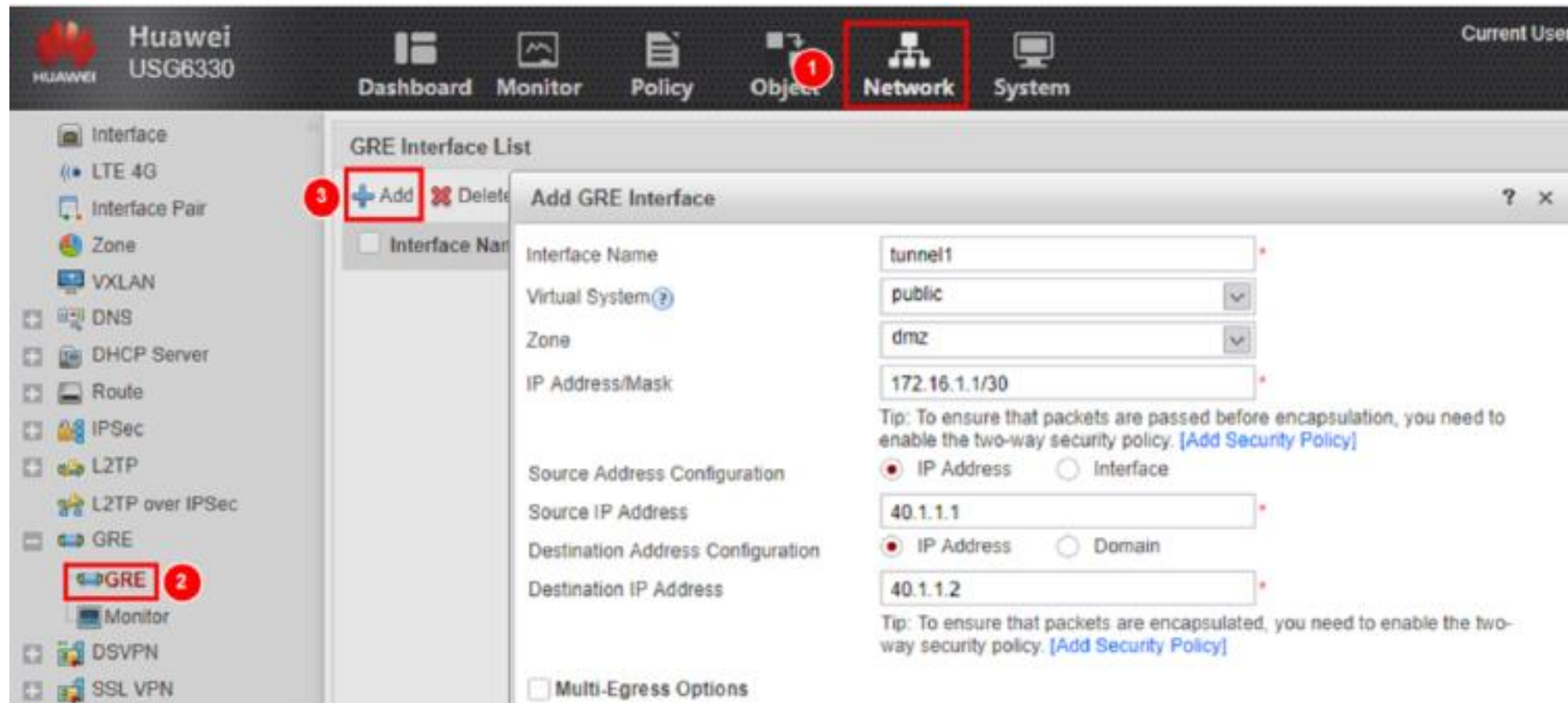
GRE VPN Configuration Procedure



Chapter
09

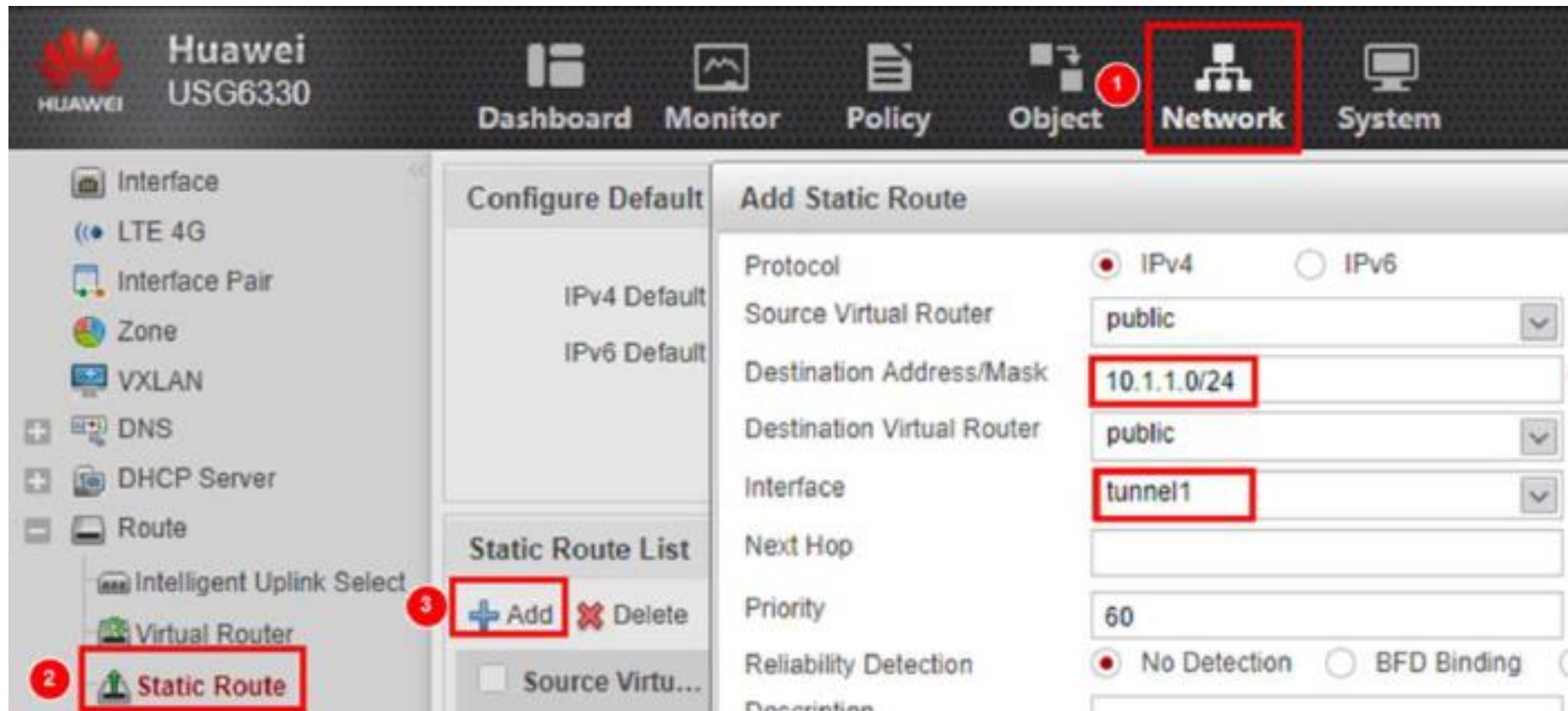
GRE Interface Configuration- FW_A

- Choose Network > GRE > GRE. Click Add to set GRE interface parameters.



Route Configuration- FW_A

- Choose Network > Static Route. Click Add to configure a static route to Network 2.



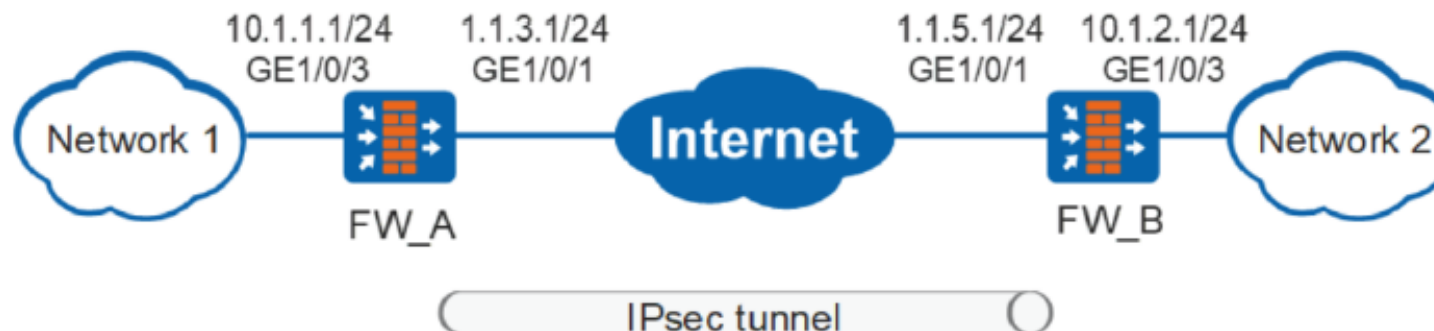
Configuration Verification

- **Verify the following:**
 - ❖ **PCs on Networks 1 and 2 can ping each other.**
 - ❖ **A router whose outbound interface is Tunnell and is destined for 10.1.2.0/24 can be found (by choosing Network > Route > Routing Table) in the routing table on FW_A.**

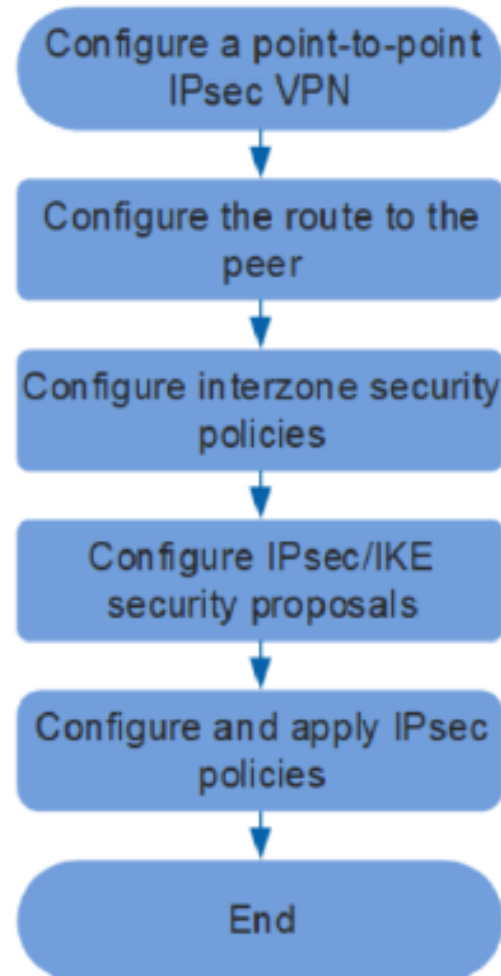
Application Scenario of Point-to-Point IPsec VPN

- Requirements

- Network 1 and Network 2 are interconnected through an IPsec tunnel established between FW_A and FW_B.
- The default values in IPsec and IKE proposals are used.
- The IPsec tunnel is established in IKE mode.

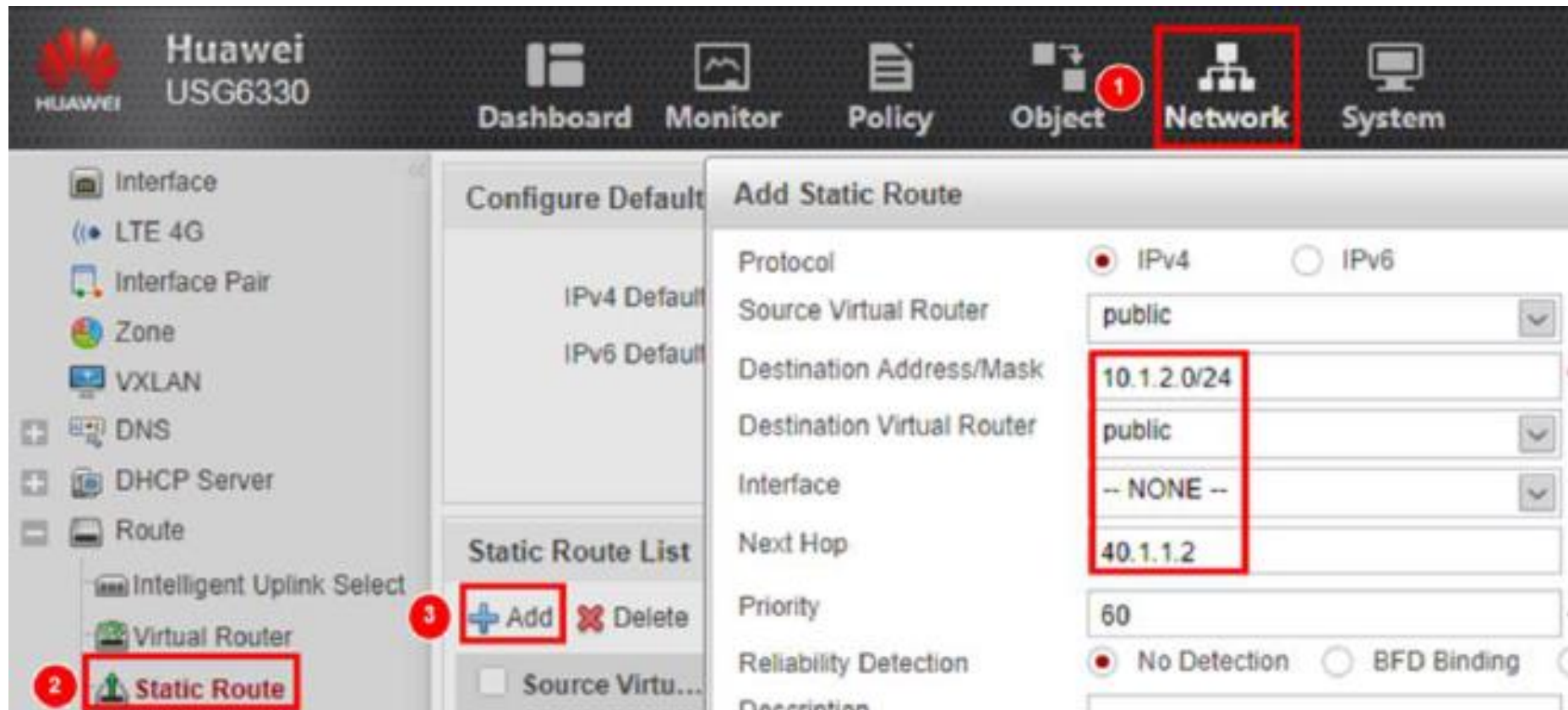


IPSec VPN Configuration Procedure



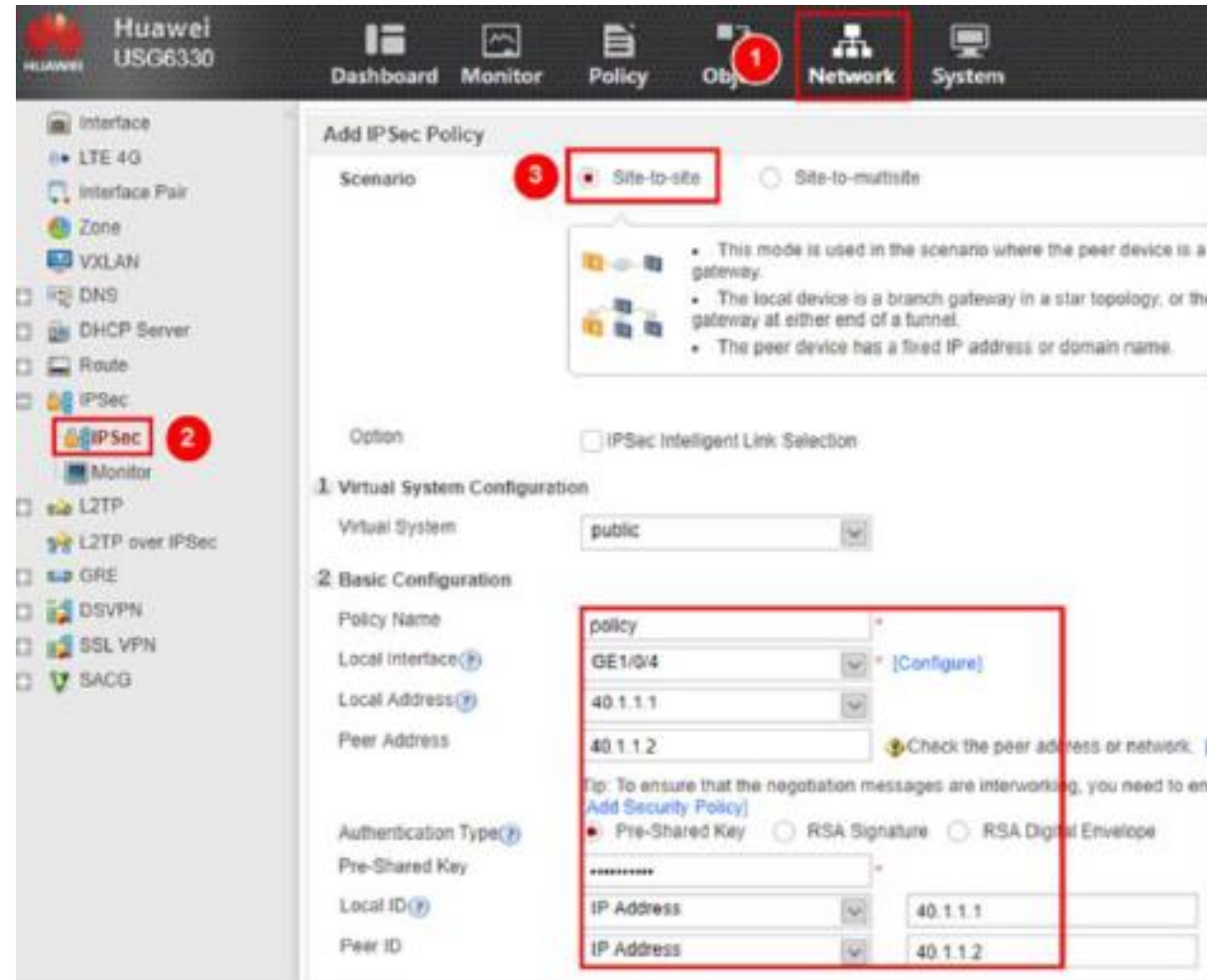
Configure Routes

- Set the route to the peer end. For example, on FW A, set the next hop to the address of FW B.



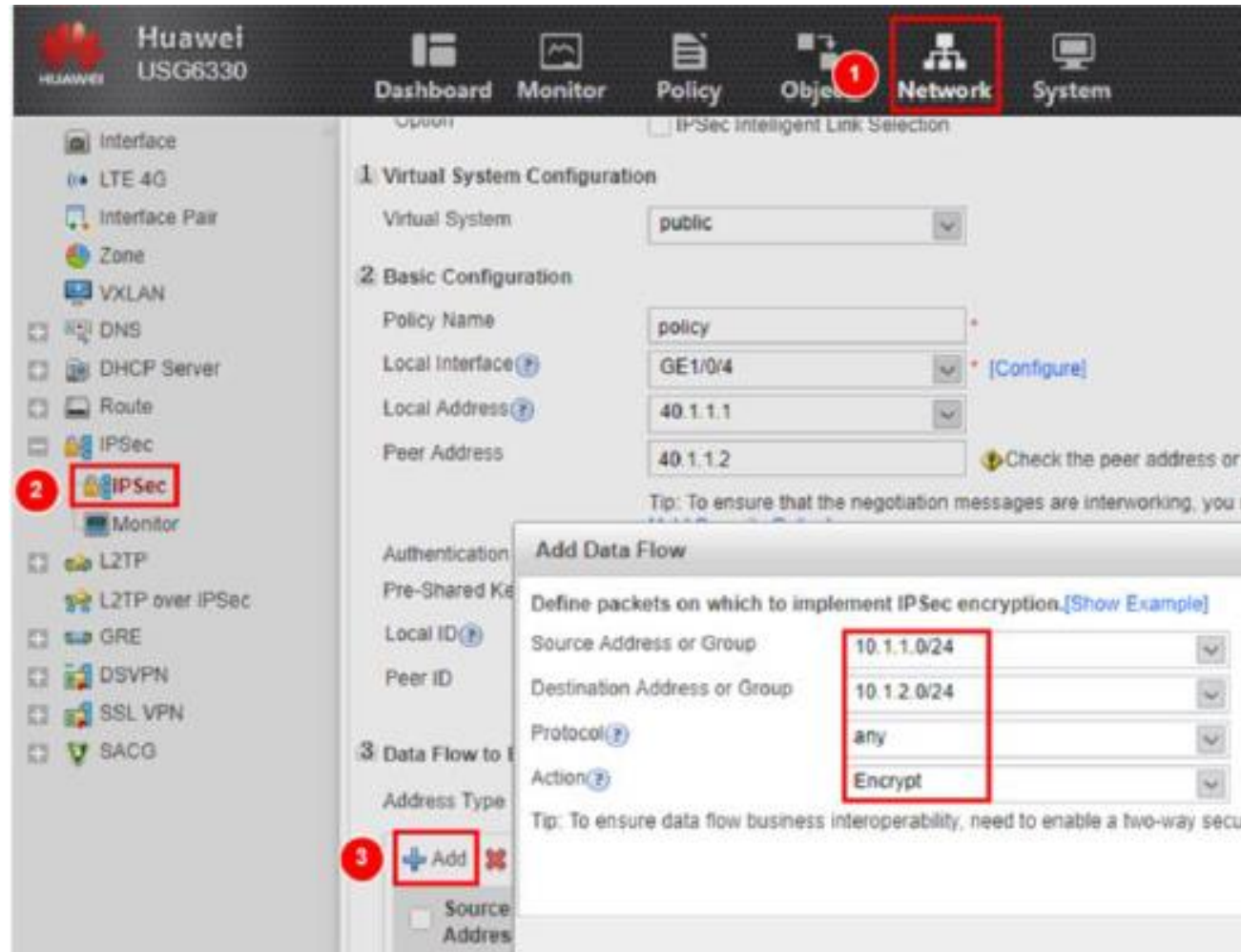
Chapter 09

Setting IPSec Policy Parameters- FW_A



Chapter
09

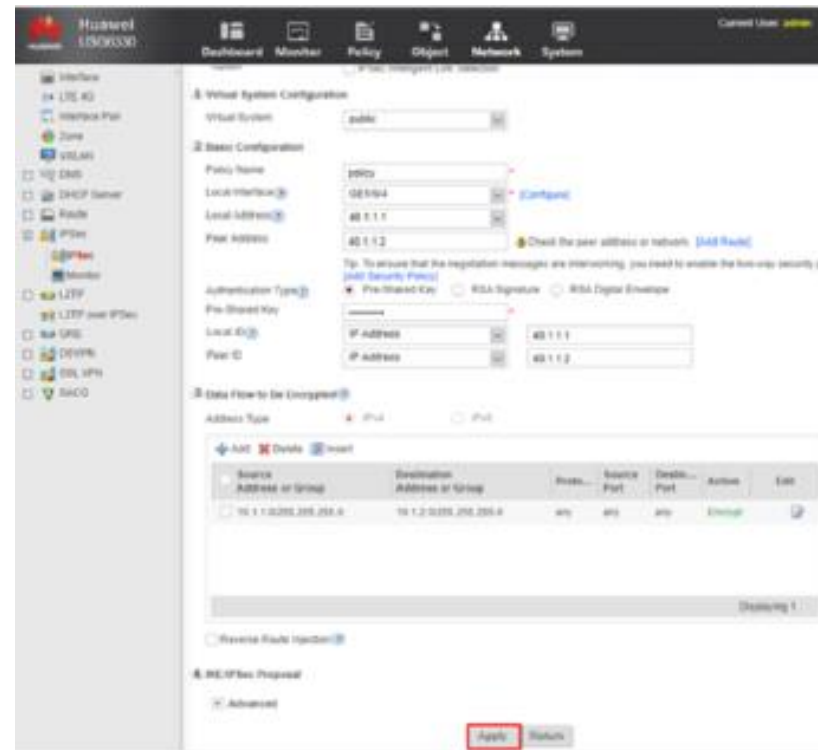
Configure Encrypted Data Flows



Chapter
09

Application an IPsec Policy

- After the configuration is complete, click Apply at the bottom of the configuration page to save and apply the IPsec policy.





Thank You