**VPN Configuration Overview**

**VPN Components**

VPNs have two important components:

* Tunneling to create the virtual network
* Encryption to enable privacy and security

**Virtual Network**

To build a virtual network, a tunnel is created between the two endpoints. In a site-to-site VPN, hosts send and receive normal TCP/IP traffic through a VPN gateway. A gateway can be a router, firewall, VPN concentrator, or security appliance. The gateway is responsible for encapsulating outbound traffic from one site and sending it through a tunnel over a network to a peer gateway at the remote site. A tunnel by itself may not guarantee security. The tunnel simply creates an extension of the local network across the WAN or public network. Tunnels can carry either encrypted or unencrypted content. Upon receipt, the remote peer gateway strips the headers, decrypts the packet, and relays it toward the target host inside its private network. In a remote-access VPN, the VPN client on the user computer contacts the gateway to set up the tunnel.

**VPN Tunnel Protocols**

VPN tunnels are created using a number of different encapsulation protocols. These protocols include:

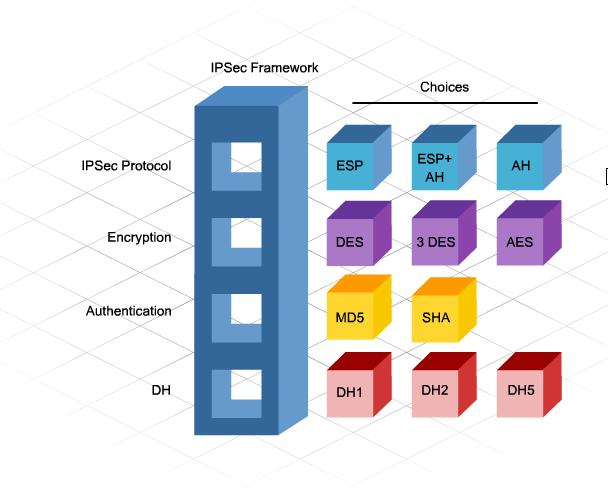
* Generic Routing Encapsulation (GRE)
* IP Security (IPSec)
* Layer 2 Forwarding (L2F) Protocol
* Point-to-Point Tunneling Protocol (PPTP)
* Layer 2 Tunneling Protocol (L2TP)

Not all protocols offer the same level of security.

**IPSec Tunnels**

IPSec is a framework of open standards. It provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at Layer 3. IPSec relies on existing algorithms to implement the encryption, authentication, and key exchange. When configuring the VPN server, the following settings must be configured:

* An IPSec protocol - The choices are Encapsulating Security Payload (ESP), Authentication Header (AH), or ESP with AH.
* An encryption algorithm that is appropriate for the desired level of security - The choices are DES, 3DES, or AES.
* An authentication algorithm to provide data integrity - The choices are MD5 or SHA.
* A Diffie-Hellman group - The choices are DH1, DH2, and DH5, if supported.



**VPN Encryption and Key Strategies**

VPN technologies use encryption algorithms that prevent data from being read if it is intercepted. An encryption algorithm is a mathematical function that combines the message with a string of digits called a key. The output is an unreadable cipher string. Decryption is extremely difficult or impossible without the correct key. The most common encryption methods used for VPNs are Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES), and Rivest, Shamir, and Adleman (RSA).

DES - Uses a 56-bit key, ensuring high-performance encryption. DES is a symmetric key cryptosystem.

3DES - A variant of the 56-bit DES. 3DES uses three independent 56-bit encryption keys per 64-bit block, providing significantly stronger encryption strength over DES. 3DES is a symmetric key cryptosystem.

AES - Provides stronger security than DES and is computationally more efficient than 3DES. AES offers three different key lengths: 128 bits, 192 bits, and 256 bits. AES is a symmetric key cryptosystem.

**Encryption Algorithms**

Encryption algorithms, such as DES and 3DES, require a symmetric, shared secret key to perform encryption and decryption. The network administrator can manually configure keys.

Email, courier, or overnight express can be used to send the shared secret keys to the administrators of the devices. But the easiest key exchange method is a public key exchange method between the encrypting and decrypting devices.

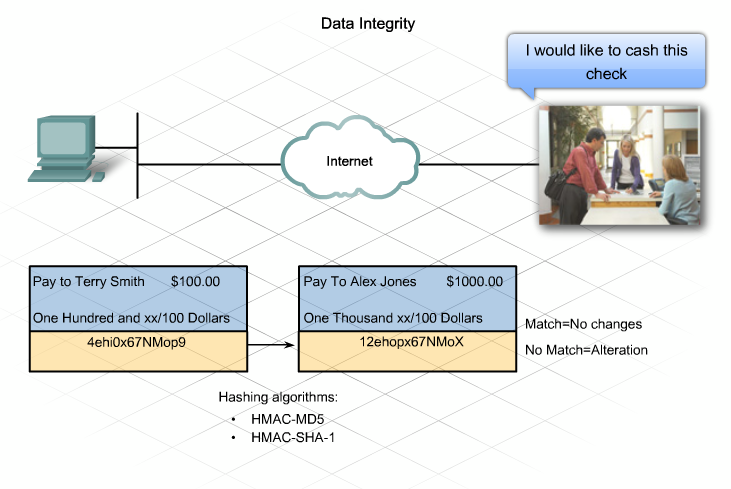
Alternatively, keys can be configured through the use of a key exchange method. The Diffie-Hellman (DH) key agreement is a public key exchange method. It provides a way for two peers to establish a shared secret key, which only they recognize, while communicating over an unsecured channel. Diffie-Hellman groups specify the type of cryptography to be used:

* DH GROUP 1 - Uses 768-bit cryptography.
* DH GROUP 2 - Cisco IOS, PIX Firewall, and Cisco Adaptive Security Appliances (ASA) devices only. Specifies to use 1024-bit cryptography.
* DH GROUP 5 - Supported if the software system requirements are met. Specifies to use 1536-bit cryptography.

**Data Integrity Algorithms**

To guard against the interception and modification of VPN data, a data integrity algorithm can be used. A data integrity algorithm adds a hash to the message. If the transmitted hash matches the received hash, the received message is accepted as an exact copy of the transmitted message. Keyed Hashed Message Authentication Code (HMAC) is a data integrity algorithm that guarantees the integrity of the message. There are two common HMAC algorithms:

* HMAC-Message Digest 5 (MD5) - This algorithm uses a 128-bit shared secret key. The variable length message and 128-bit shared secret key are combined and run through the HMAC-MD5 hash algorithm. The output is a 128-bit hash. The hash is appended to the original message and forwarded to the remote end.
* HMAC-Secure Hash Algorithm 1 (HMAC-SHA-1) - This algorithm uses a 160-bit secret key. The variable length message and the 160-bit shared secret key are combined and run through the HMAC-SHA-1 hash algorithm. The output is a 160-bit hash. The hash is appended to the original message and forwarded to the remote end.



**Security Associations**

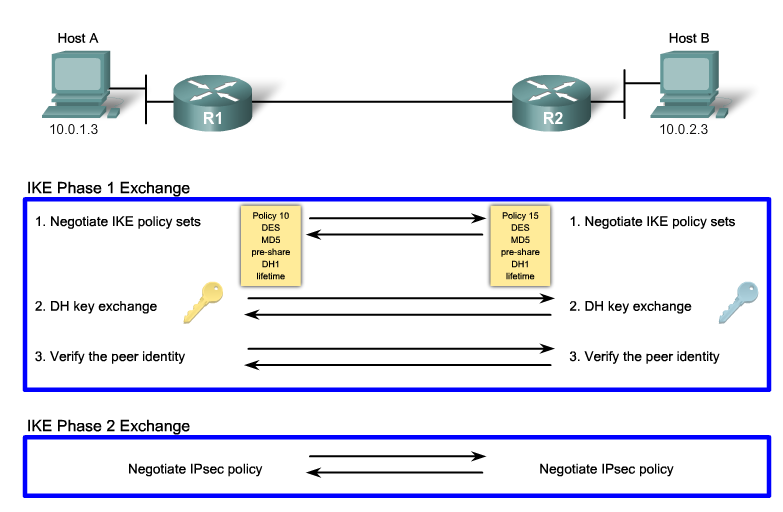
An SA is a basic building block of IPsec. Security associations are maintained within a SA database (SADB), which is established by each device. A VPN has SA entries defining the IPsec encryption parameters as well as SA entries defining the key exchange parameters.

Diffie-Hellman (DH) is used to create the shared secret key. However, IPsec uses the Internet Key Exchange (IKE) protocol to establish the key exchange process.

Instead of transmitting keys directly across a network, IKE calculates shared keys based on the exchange of a series of data packets. This disables a third party from decrypting the keys even if the third party captured all exchanged data that is used to calculate the keys. To establish a secure communication channel between two peers, the IKE protocol executes two phases:

Phase 1 - Two IPsec peers perform the initial negotiation of SAs. The basic purpose of Phase 1 is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers. It can be implemented in main mode (longer, initial contact) or aggressive mode (after initial contact).

Phase 2 - SAs are negotiated by the IKE process ISAKMP on behalf of IPsec. It can be negotiated in quick mode.



**Configuring a Site-to-Site VPN**

Some basic tasks must be completed to configure a site-to-site IPsec VPN.

Task 1. Gather information about the two endpoints of the site-to-site VPN. You will need to know the interface to use, the peer IP address, as well as the LAN IP addresses of any LANs that will use the VPN to send secure data between them.

Task 2. Create an ISAKMP policy to determine the ISAKMP parameters that will be used to establish the tunnel.

Task 3. Define the IPsec transform set. The definition of the transform set defines the parameters that the IPsec tunnel uses. The set can include the encryption and integrity algorithms.

Task 4. Create a crypto ACL. The crypto ACL defines which traffic is sent through the IPsec tunnel and protected by the IPsec process.

Task 5. Create and apply a crypto map. The crypto map groups the previously configured parameters together and defines the IPsec peer devices. The crypto map is applied to the outgoing interface of the VPN device.