CCNP 2 VPN

Læse status:

KVR: 3.2.5

Ord:
Encapsulating Security Payload (ESP)
Internet Key Exchange (IKE)
Authentication Header (AH)
Security Associations (SA)
Internet Security Association and Key Management Protocol (ISAKMP)
Data Encryption Standard [DES]
Message Digest 5 [MD5])
Challenge Handshake Authentication Protocol (CHAP), one-time passwords (OTPs), or Secure Key (S/Key)

3.1.4 Characteristics of a Secure VPNs

vpn er baseret på 3 ting

1.authentication (Authentication ensures that a message comes from an authentic source and goes to an authentic destination.)

autorisationen kan ske på flere måder bla. passwords certificater, chipkort og fingeraftryk.

2.encapsulation (**Data confidentiality:** One of the traditional security concerns is protecting data from eavesdroppers. As a design feature, data confidentiality aims at protecting the message contents from being intercepted by unauthenticated or unauthorized sources. VPNs achieve confidentiality using mechanisms of encapsulation and encryption.

3.encryption(**Data integrity:** Since you have no control over where the data has traveled and who has seen or handled the data you send or receive while the data journeys across the Internet, there is always the possibility that the data has been modified. Data integrity guarantees that no tampering or alterations occur to data while it travels between the source and destination. VPNs typically use one of three technologies to ensure data integrity: one-way hash functions, message authentication codes (MAC), or digital signatures.

eavesdroppers(en der lytter med)

3.1.5 VPN Security: Encapsulation

carrier protokoller (som overfører en vpn pakke) over feks framerelay atm mlps (multi protokol layer switching)

Encapsulating protocol:

The protocol (GRE, IPsec, L2F, PPTP, L2TP) that is wrapped around the original data. Not all protocols offer the same level of security (pptp yder ringe kryptering l2tp virker kun i mlps.

Passenger protocol: The original data (IPX, AppleTalk, IPv4, IPv6). hvor den orginale data blev overført.

Tunneling is the transmission of data through a public network so that routing nodes in the public network are unaware that the transmission is part of a private network. Tunneling allows the use of public networks (for example, the Internet) to carry data on behalf of users as though the users had access to a private network. This is where the name VPN comes from

måske en nem måde at forstå tunneling

To reinforce the concepts of tunneling, consider an example of sending a holiday card through traditional mail. The holiday card has a message inside and is the passenger protocol. The card is put inside an envelope (encapsulating protocol) with proper addressing applied. The envelope is put inside a mailbox for delivery. The Postal system (carrier protocol) picks up and delivers the envelope to your mailbox. The two end points in the carrier system are the “tunnel interfaces.” You remove the holiday card (extract the passenger protocol) and read the message.

3.1.6

When used alone, IPsec provides a private, resilient network for IP unicast only. Use IPsec in conjunction with GRE when support for IP multicast, dynamic IGP routing protocols, or non-IP protocols is required. Figure □ shows an example secure remote access VPN.

IPsec has two encryption modes:

- Tunnel mode
- Transport mode

unicast=en klient til en klient (http://en.wikipedia.org/wiki/Unicast)

multicast= en klient til det klienter der vil ønske den

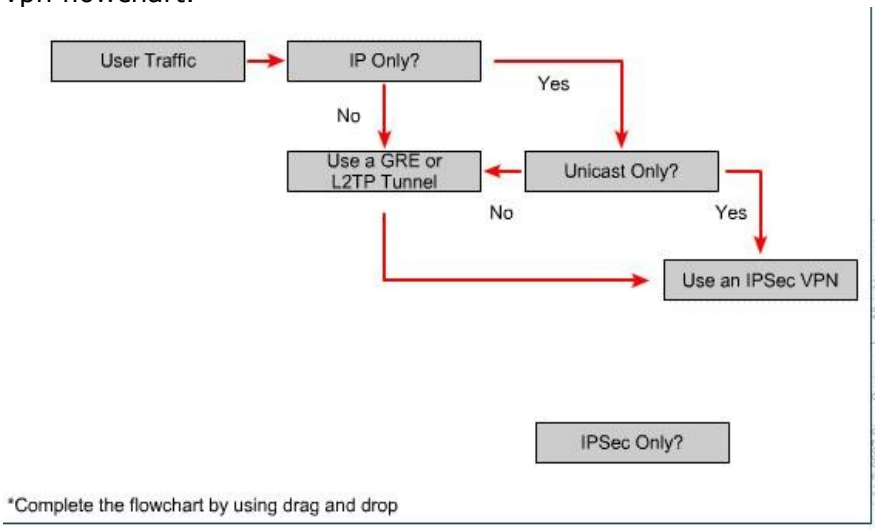
tunnelmode

Tunnel mode encrypts the header and the payload of each packet while transport mode only encrypts the payload. Only systems that are IPsec-compliant can take advantage of transport mode. Additionally, all devices must use a common key and the firewalls of each network must be set up with very similar security policies. IPsec can encrypt data between various devices, including router to router, firewall to router, PC to router, and PC to server.

GRE encloses the IP header and payload of packets with a GRE-encapsulation header. Network designers use this method of encapsulation to hide the IP header of packets as part of the GRE-encapsulated payload. By hiding information, the designers separate, or “tunnel,” data from one network to another without making changes to the underlying common network infrastructure.

Site-to-site VPNs can also use IPsec in tunnel mode as the encapsulating protocol. IPsec works well on both remote-access and site-to-site VPNs. To use IPsec, both tunnel interfaces must support IPsec.

vpn flowchart.



3.1.7 VPN Security: Symmetric and Asymmetric Encryption Algorithms

Encryption is the process of taking all the data that one computer is sending to another computer and encoding the data into a form that only the intended destination computer will be able to decode.

The primary methods of encryption are symmetric-key (or secret key) encryption and asymmetric (or public key) encryption.

vigitigt

- **Symmetric-key encryption: Symmetric-key encryption, also called secret key encryption, works when each computer has a secret key (code) that the computer uses to encrypt information before the information is sent over the network to another computer. Symmetric-key encryption requires that someone know which computers will be talking to each other so that the person can configure the key on each computer. Symmetric-key encryption is a secret code, or key, that each of the two computers must know to decode the information.**

For example, a sender creates a coded message to send to a recipient where each letter in the message is substituted with the letter that is two letters down from the original in the alphabet; "A" becomes "C," and "B" becomes "D." In this case, the word SECRET, becomes UGETGV. The sender has already told the recipient that the secret key is "Shift by 2." When the recipient receives the message 'UGETGV', the recipient computer decodes the message by shifting back

two and calculating 'SECRET'. Anyone else who sees the message sees only the encrypted message, which looks like nonsense unless the person knows the secret key. The drawback of symmetric-key encryption is that it involves exchanging secret keys across the very insecure Internet.

- **Asymmetric Encryption: Introduced in 1976, asymmetric encryption uses different keys for encryption and decryption. Knowing one of the keys does not allow a hacker to deduce the second key and decode the information. One key encrypts the message, while a second key decrypts the message. It is not possible to encrypt and decrypt with the same key. Public-key encryption uses a combination of a private key and a public key. Only the sender knows the private key. The sender gives a public key to any recipient that the sender with whom he wants to communicate. To decode an encrypted message, the recipient must use the public key, provided by the originating sender, and the recipient's own private key.**

The following example of a locked mailbox with a mail slot helps to explain public key encryption. A mail slot is exposed and accessible to the public. The street address of the mail slot represents the public key. Anyone knowing the street address can go to the address and put a message through the slot. However, only the person who has the key to the mail slot (asymmetric encryption's private key) can open the mailbox and read the message.

Computing Power Requirements of Cryptographic Algorithms
Asymmetric encryption demands significantly more computing power than symmetric encryption demands. The table in Figure

compares symmetric key lengths to asymmetric key lengths. A symmetric algorithm using a 256-bit key is comparable to an asymmetric algorithm using a 15,360-bit key. The longer the key is, the more processing power is used.

Typically symmetric encryption is used to encrypt large amounts of data because it is far more efficient than using asymmetric encryption. Asymmetric encryption is typically used for authentication purposes. With IPsec, once the tunnel is active, traffic through the tunnel uses symmetric encryption if encryption is requested. However, to set up the tunnel, asymmetric encryption is used to authenticate both ends of the tunnel.

What Is Needed to Build a VPN?

Components required to establish a VPN include:

* An existing network with servers and workstations
* Connection to the Internet
* VPN gateways (i.e., routers, PIX, ASA, VPN concentrators) that act as endpoints to establish, manage, and control VPN connections
* Software to create and manage tunnels

VPNs secure data by encapsulating the data, encrypting the data, or both encapsulating the data and then encrypting it:

* Encapsulation is also referred to as tunneling because encapsulation transmits data transparently from network to network through a shared network infrastructure.
* Encryption codes data into a different format. Decryption decodes encrypted data into the data's original unencrypted format.

3.1.2 Overlay and Peer-to-Peer VPN Architecture

* L2 overlay VPN: L2 overlay VPNs are independent of the network protocol used by the customer meaning that the VPN is not limited to carrying IP traffic. If the carrier offers the appropriate ATM service, the overlay VPN will carry any kind of information. Frame Relay VPNs are normally limited to data applications, although voice over Frame Relay customer premises equipment (CPE) devices may be useable on some services.
* L3 overlay VPN: L3 Overlay VPNs most often use an “IP in IP” tunneling scheme using Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and IP security (IPsec). Figure summarizes the basic properties of these technologies.

By properly implementing security, successful VPN implementations meet three goals:

* Authentication: Authentication ensures that a message comes from an authentic source and goes to an authentic destination. User identification gives a user confidence that the party the user establishes communications with is who the user thinks the party is. VPN technologies are making use of several reputable methods for establishing the identity of the party at the other end of a network. These include passwords, digital certificates, smart cards, and biometrics.
* Data confidentiality: One of the traditional security concerns is protecting data from eavesdroppers. As a design feature, data confidentiality aims at protecting the message contents from being intercepted by unauthenticated or unauthorized sources. VPNs achieve confidentiality using mechanisms of encapsulation and encryption.
* Data integrity: Since you have no control over where the data has traveled and who has seen or handled the data you send or receive while the data journeys across the Internet, there is always the possibility that the data has been modified. Data integrity guarantees that no tampering or alterations occur to data while it travels between the source and destination. VPNs typically use one of three technologies to ensure data integrity: one-way hash functions, message authentication codes (MAC), or digital signatures

3.1.9 Asymetric Encryption

Two asymmetric algorithms used for IPsec are Diffie-Hellman (DH) and RSA. Cisco devices use RSA and Diffie-Hellman every time a new IPsec tunnel is established. RSA authenticates the remote device while Diffie-Hellman exchanges keys that are used for encryption . The Internet Security Association (ISA) implements these protocols in specialized hardware to ensure fast tunnel setup and high overall encryption throughput.

RSA (named after designers Rivest, Shamir, and Adelman) is an algorithm for public key encryption and was the first algorithm known to be suitable for signing as well as encryption. RSA was one of the first great advances in public key cryptography.

The security of the RSA cryptosystem is based on two mathematical problems: the problem of factoring very large numbers and the RSA algorithm itself. Full decryption of an RSA cipher text is thought to be impossible because both of these problems are difficult, and no efficient algorithm exists for solving them. No polynomial-time method for factoring large integers on a classical computer has yet been found, but it has not been proven that no method exists. As of 2005, the largest number that was factored by general-purpose methods was 663 bits long using state-of-the-art distributed methods. RSA keys are typically 1024 to 2048 bits long.

DH combined public key cryptography with secret key cryptography.

As symmetric algorithms, DES, 3DES, Message Digest 5 (MD5), and SHA require a shared secret key to perform encryption and decryption. The question is, how do the encrypting and decrypting devices both have the shared secret key? Possible solutions are that the keys can be sent via e-mail, courier, overnight express, or public key exchange. Another, easier and more secure method is DH public key exchange. The DH key agreement is a public key encryption

method that provides a way for two peers to establish a shared secret key that only the peers know, even though the peers are communicating over an insecure channel.

Public key cryptosystems rely on a two-key system:

- **Public key:** Exchanged between end users
- **Private key:** Kept secret by the original owners
-

3.1.12 VPN Security: Authentication

- **Username and password:** Uses the predefined usernames and passwords for different users or systems.
-
- **One Time Password (OTP) (Pin/Tan):** A stronger authentication method than username and password, this method uses new passwords that are generated for each authentication.
-
- **Biometric:** Biometrics usually refers to technologies that are used for measuring and analyzing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for authentication purposes.

- **Pre-shared keys:** This method uses a secret key value, manually entered into each peer, and then used to authenticate the peers.

- **Digital certificates:** Use the exchange of digital certificates to authenticate the peers.

Authentication, authorization, and accounting (AAA) servers are used for more secure access in a remote-access VPN environment. When a request to establish a session comes in from a dialup client, the request is proxied to the AAA server. AAA then checks and records the following:

- Who the client is (authentication)
- What the client is allowed to do (authorization)
- What the client actually does (accounting)

The accounting information is especially useful for tracking client use for security auditing, billing, or reporting purposes.

3.2.1 IPsec Security Features

IPsec encompasses a suite of protocols and is not bound to any specific encryption or authentication algorithms, key generation technique, or security association (SA). IPsec provides the rules while existing algorithms provide the encryption, authentication, key management, and so on.

IPsec acts at the network layer, protecting and authenticating IP packets between IPsec devices (peers), such as Cisco

PIX Firewalls, Adaptive Security Apliances (ASA), Cisco routers, the Cisco Secure VPN Client, and other IPsec-compliant products.

Data confidentiality: IPsec ensures confidentiality by using encryption. Data encryption prevents third parties from reading the data, especially data that is transmitted over public networks or wireless networks. The IPsec sender can encrypt packets before transmitting the packets across a network and prevent anyone from hearing or viewing the communication (eavesdropping). If intercepted, the data cannot be decoded. Encryption is provided using encryption algorithms including DES, 3DES, and AES. **Data integrity:** IPsec ensures that data arrives unchanged at the destination; that is, that the data is not manipulated at any point along the communication path. IPsec ensures data integrity by using hashes. A hash is a simple redundancy check. The IPsec protocol adds up the basic components of a message (typically the number of bytes) and stores the total value. IPsec performs a checksum operation on received data and compares the result to the authentic checksum. If the sums match, the data is considered not manipulated. Data integrity is provided through the Hash-based Message Authentication Code (HMAC) function. Supported HMAC functions include Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1). **Data origin authentication:** The IPsec receiver can authenticate the source of the IPsec packets. Authentication ensures that the connection is actually made with the desired communication partner. IPsec authenticates users (people) and devices that can carry out communication independently. The quality of Data origin authentication is dependent on the data integrity service that is provided. **Anti-replay:** Anti-replay protection verifies that each packet is unique, not duplicated. IPsec packets are protected by comparing the sequence number of the received packets and a sliding window on the destination host, or security gateway. A packet whose sequence number is before the sliding window is considered late, or a duplicate. Late and duplicate packets are dropped

3.2.2 IPsec Protocols and Headers

The IPsec standard provides a method to manage authentication and data protection between multiple peers engaging in secure data transfer. IPsec includes a protocol for exchanging keys called Internet Key Exchange (IKE) and two IPsec IP protocols, Encapsulating Security Payload (ESP) and Authentication Header (AH).

IPsec uses three main protocols to create a security framework:

- **IKE:** Provides a framework for the negotiation of security parameters and establishes authenticated keys. IPsec uses symmetrical encryption algorithms for data protection, which are more efficient and easier to implement in hardware than other types of algorithms. These algorithms need a secure method of key exchange to ensure data protection. The IKE protocols provide the capability for secure key exchange.
- **AH:** The IP Authentication Header (AH) provides connectionless integrity and data origin authentication for IP datagrams and optional protection against replays. AH is embedded in the data that needs to be protected. ESP has replaced the AH protocol, and AH is no longer used very often in IPsec.
- **ESP:** Encapsulating Security Payload (ESP) provides a framework for encrypting, authenticating, and securing data. ESP provides data privacy services, optional data authentication, and anti-replay services. ESP encapsulates the data that needs protection. Most IPsec implementations use the ESP protocol.

IPsec Headers
IPsec provides authentication, integrity, and encryption via the insertion of one or both of two specific headers, AH or ESP, into the IP datagram.

The AH provides authentication and integrity checks on the IP datagram. Successful authentication means that the packet was, indeed, sent by the apparent sender. Integrity means the packet was not changed during transport.

The ESP header provides information that indicates encryption of the datagram payload contents. The ESP header also provides authentication and integrity checks.
AH and ESP are used between two hosts. These hosts may be end stations or gateways.

> **Note**
> AH and ESP provide services to transport layer protocols such as TCP and User Datagram Protocol (UDP). AH and ESP are Internet protocols and are assigned numbers 51 (AH) and 50 (ESP) by the Internet Assigned Numbers Authority (IANA).

AH and ESP solutions require a standards-based way to secure data from modification and being read by a third party. IPsec has a choice of different encryptions (Data Encryption Standard [DES], Triple Data Encryption Standard [3DES], and Advanced Encryption Standard [AES]) so that users can choose the strength of their data protection.

IPsec also has several hash methods to choose from (Hash-based Message Authentication Code [HMAC], Message Digest 5 [MD5], and Secure Hash Algorithm 1 [SHA-1]), each giving different levels of protection

IKE uses UDP port 500

IPsec uses the IKE protocol to provide these functions:

- Negotiation of SA characteristics
- Automatic key generation
- Automatic key refresh
- Manageable manual configuration

3.2.4 ike phases and modes

IKE is executed in two phases to establish a secure communication channel between two peers

2.3.2 step2 ike phase 1

ike phase 2

Exam help

High availability

crypto isakmp keepalive 10 5 periodic

configure router RTA to encrypt traffic

interface Tunnel0
tunnel source Serial0
tunnel destination 192.168.23.3

Two components of Cisco Easy VPN:

Cisco Easy VPN Remote

Cisco Easy VPN Server

First step SDM Easy VPN Server wizard to set up an IPsec VPN server

Select the interface for terminating IPsec.

Act as remote VPN clients

Cisco PIX firewalls

Cisco IOS routers
Cisco VPN 3002 hardware clients

Transparent tunneling in Cisco VPN client
IPsec over UDP is selected, the port number is negotiated.

creating a new VPN connection entry in the Cisco VPN client

The Name field in the Group Authentication form in the Authentication tab is case sensitive.

use of SDM to configure a site-to-site VPN between two Cisco routers

The SDM can autodetect site-to-site VPN misconfigurations and propose fixes.
With the use of SDM, no Cisco IOS command-line interface experience is required to configure a site-to-site VPN.

Which statement about high availability for IOS IPsec VPNs is true?
When outbound IPsec traffic must be sent and the peer does not respond, the router sends a DPD message to the peer.

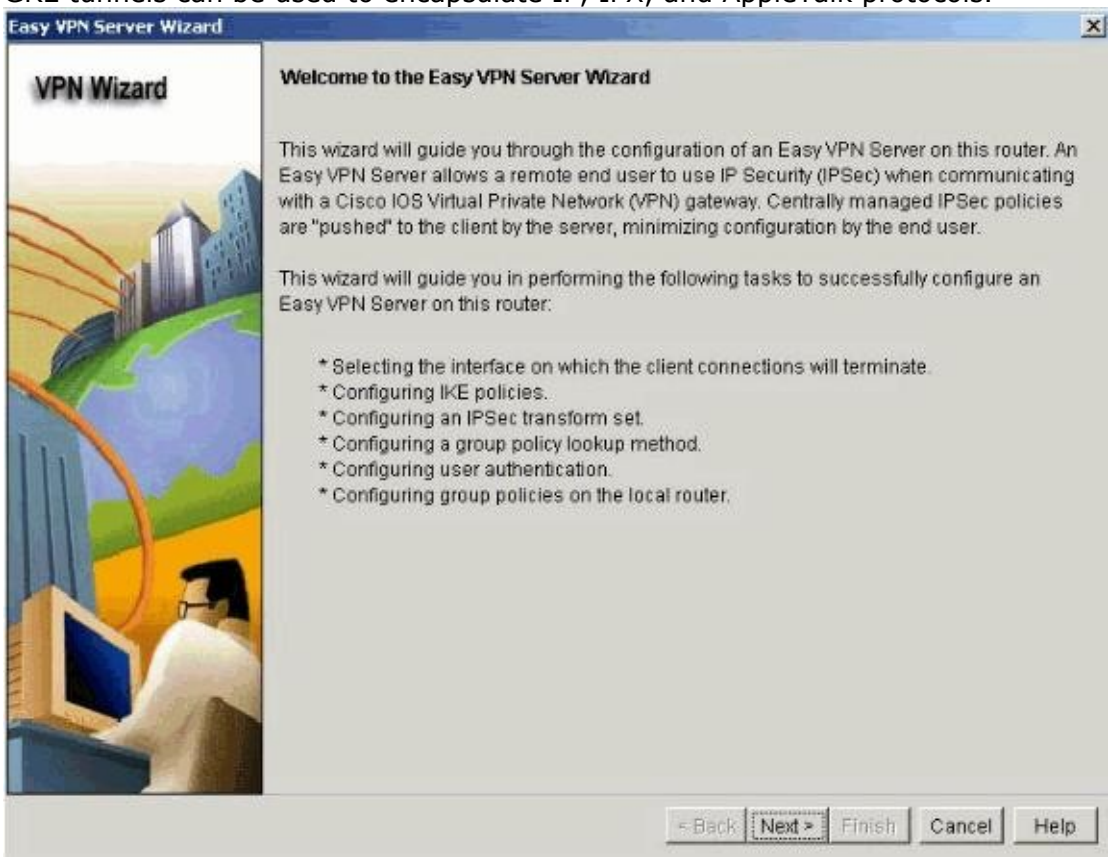
Which two statements about the Authentication Header (AH) and Encapsulating Security Payload (ESP) protocols are true?
With the use of ESP in transport mode, only the data portion of the original IP datagram is encrypted.
Tunnel mode and transport mode can be deployed with either ESP or AH or both.

Internet Key Exchange (IKE)
IKE provides anti-replay services.

two features of the Internet Key Exchange (IKE) protocol
automatic key regeneration
negotiation of SA characteristics

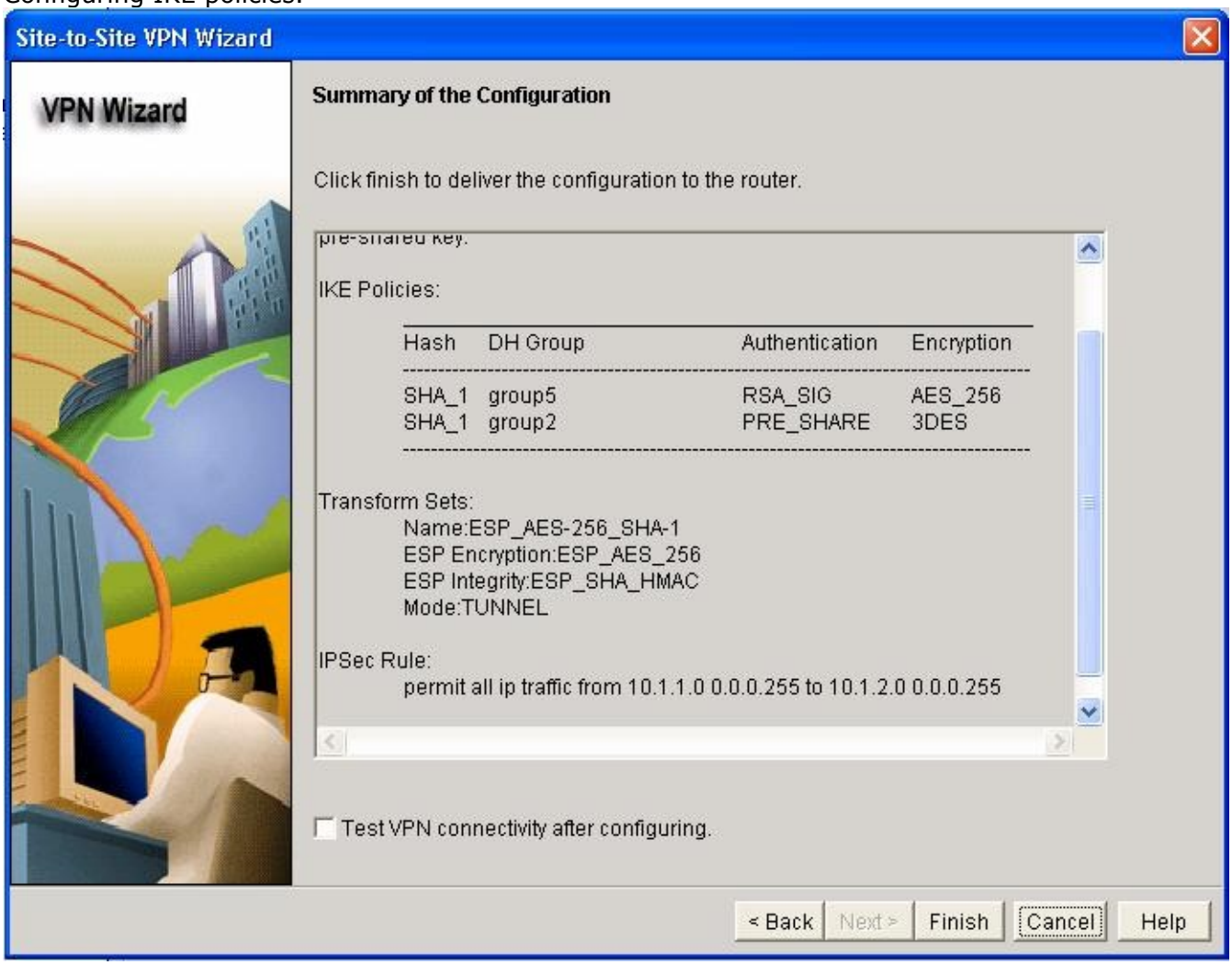
secure GRE tunnels
IPsec can be used to secure OSI Layer 3 traffic across a GRE tunnel.

GRE tunnels over IPsec
GRE allows the use of routing protocols across the tunnel.
GRE tunnels are stateless.
GRE tunnels can be used to encapsulate IP, IPX, and AppleTalk protocols.



specify the encryption algorithm, authentication algorithm, and key exchange method to be used when negotiating a VPN connection with the remote device

Configuring IKE policies.



On the basis of the information that is displayed in the VPN Wizard configuration summary, which two statements are true?

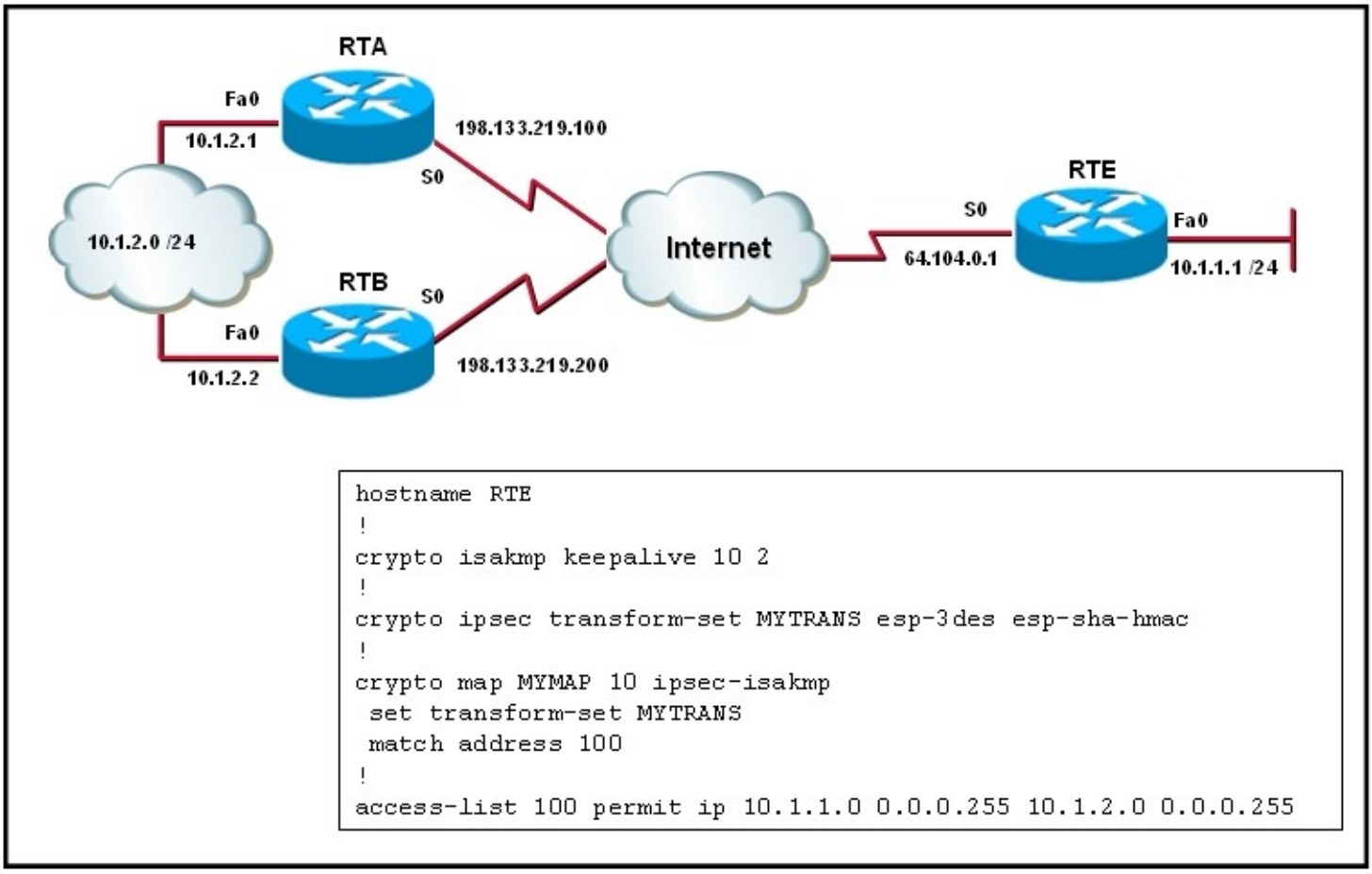
A VPN peer must support one of the two IKE policies.

The mode that is chosen encrypts both the data and the IP header.

```
Router# show crypto isakmp policy

Protection suite priority 15
        encryption algorithm:  DES - Data Encryption Standard (56 bit keys)

        hash algorithm: Message Digest 5
        authentication method: Rivest-Shamir-Adleman Signature
        Diffie-Hellman Group:  #2 (1024 bit)
        lifetime:      5000 seconds, no volume limit
Protection suite priority 20
        encryption algorithm:  DES - Data Encryption Standard (56 bit keys)

        hash algorithm: Secure Hash Standard
        authentication method: preshared Key
        Diffie-Hellman Group:  #1 (768 bit)
        lifetime:      10000 seconds, no volume limit
```

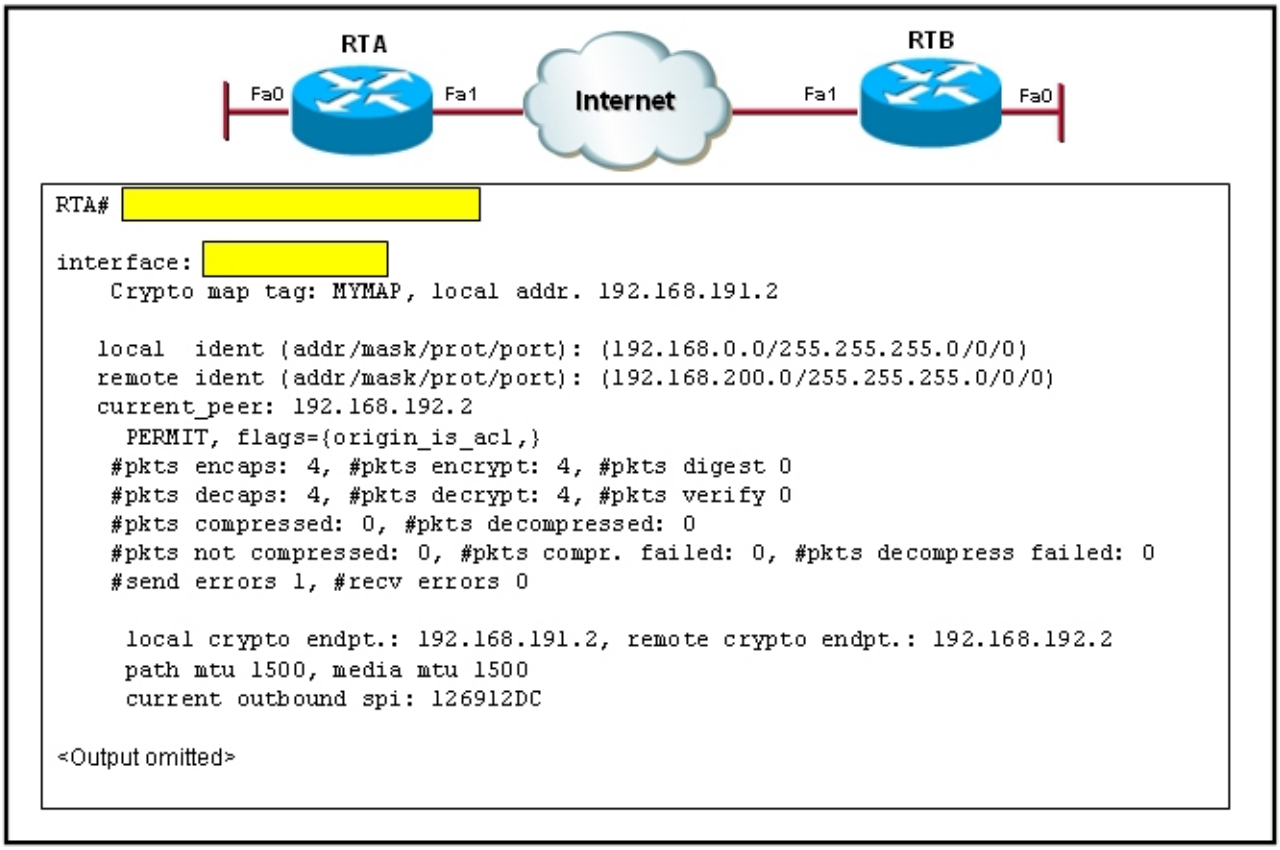
Which set of commands would correctly configure this router to display the output that is generated for policy 20 in the exhibit?

crypto isakmp policy 20
authentication pre-share
lifetime 10000

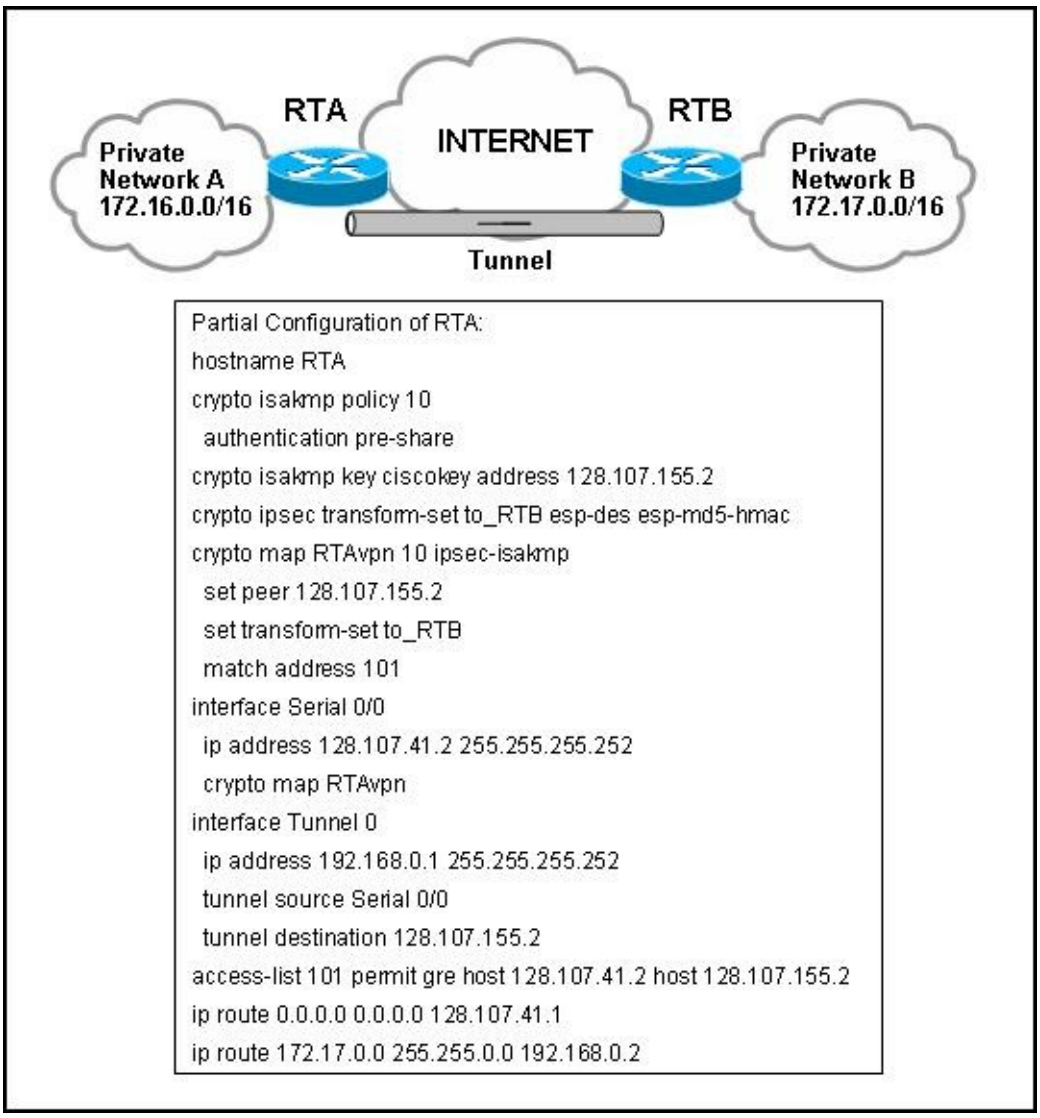


High availability has been configured on router RTE by using the dead peer detection (DPD) mechanism. Router RTA must be the primary peer, and router RTB the backup peer. Which set of commands would correctly configure this on router RTE?

crypto map MYMAP 10 ipsec-isakmp
set peer 198.133.219.100 default
set peer 198.133.219.200



On the basis of the provided information, which two statements must be true?
The command crypto map MYMAP has been issued on interface Fa1 of router RTA.
The command ip address 192.168.191.2 255.255.255.0 has been issued on interface Fa1 of router RTA.



A tunnel is established between routers RTA and RTB. Which two statements are true about traffic that flows from network A to network B?
Routers inside the Internet will see packets with the destination IP address of 128.107.155.2.
Traffic will go through a GRE tunnel.

Hvad vi skal ind på:
Conf af High availability (DPD, backup peer)

Kort om Cisco Easy VPN (step by step IPsec VPN server)

Tunnel conf på router

Cisco VPN client

Brug af SDM til VPN

Hurtig om ESP

GRE, IKE, IPSec
