PSec Introduction

1. Which of the following is true concerning IPSec? ?

A. It provides authentication, confidentiality, packet integrity, and encapsulation functions, but not antireplay capabilities.
B. IKE is used to securely share keys between IPSec peers during Phase 1.
C. Cisco routers use transform sets to define interesting traffic.
D. It supports IPv4 and IPv6.

Answers

1.
- ☑ **D.** IPSec is a group of open standards referenced in RFC 2401 and is compatible with IPv4 and IPv6.
- ☒ **A** is incorrect because antireplay capabilities are supported. **B** is incorrect because DH performs this process. **C** is incorrect because crypto ACLs perform this process.

ISAKMP/IKE Phase 1

2. Which of the following is not a mode supported by ISAKMP/IKE? ?

A. Quick
B. Main
C. Aggressive
D. Tunnel

3. Which of the following is true concerning DH? ?

A. Before DH can begin, both parties must agree upon two non-secret numbers.
B. Before DH can begin, both parties must agree upon two secret numbers.
C. DH uses symmetric keys.
D. DH is used to protect the authentication credentials shared between two parties.

4. Which of the following is true concerning DH? (Choose two.) ?

A. Group 1 keys uses an elliptical curve function.
B. Group 2 keys are 1,024 bits in length.
C. Group 5 keys are the most secure.
D. Group 1 keys are the least secure.

Answers

2.
- ☑ **D.** Tunnel mode is an operational mode used by AH and ESP
- ☒ **A**, **B**, and **C** are modes supported by ISAKMP/IKE in Phase 1 and Phase 2.

3.
- ☑ **A.** Before DH can begin, both parties must agree upon two non-secret numbers.
- ☒ **B** is incorrect because they are non-secret numbers. **C** is incorrect because DH uses asymmetric keys. **D** is incorrect because DH is used to securely

share symmetric keys between peers for encryption algorithms and HMAC functions.

4.
- ☑ **B** and **C.** Group 2 keys are 1,024 bits in length. Group 5 keys support 1,536 bits and are the most secure for IPSec.
- ☒ **A** uses a straight function; group 7 uses an elliptical curve function. Group 7 keys are the least secure, making **D** incorrect.

ISAKMP/IKE Phase 1 Authentication

5. Which is not an authentication mode used to authenticate peers when building an IPSec session? ?

A. RSA signatures
B. Preshared keys
C. DH secret keys
D. RSA encrypted nonces

6. What defines how to encrypt and sign certificate enrollment messages? ?

A. SCEP
B. PKCS #7
C. PKCS #10
D. CRL

Answers

5.
- ☑ **C.** The DH-derived secret key is used to securely share symmetric keys between peers for encryption algorithms and HMAC functions.
- ☒ **A**, **B**, and **D** are supported authentication methods for IPSec.

6.
- ☑ **B.** PKCS #7 defines how to encrypt and sign certificate enrollment messages.
- ☒ **A** defines an in-band method of obtaining certificates. **C** defines how to handle certificate requests from network devices. **D** is a list of revoked certificates maintained by a CA.

ISAKMP/IKE Phase 2

7. Which of the following are true concerning Phase 2? (Choose two.) ?

A. ISAKMP/IKE negotiates security parameters for the data SAs.
B. PFS can be used to periodically refresh keying information.
C. Main mode establishes the data connections.
D. An SA is a number that uniquely identifies a data connection.

8. Which of the following is true concerning IPSec Phase 2 data connections? ?

A. AH works with NAT, but not PAT.
B. AH and ESP break with any type of address translation.
C. IPSec over TCP is a Cisco-proprietary solution to tunnel AH and ESP traffic through an address translation or firewall device.
D. ESP uses a protocol number of 50.

9. Which AH and ESP mode exposes the real source and destination addresses involved with the session? ?

A. Tunnel

B. Transport
C. Quick
D. Aggressive

Answers

7.
- ☑ **A** and **B.** ISAKMP/IKE negotiates the security parameters for the data IPSec SA, which includes the transform set to use. It is also responsible for periodically refreshing keying information. The existing management connection can be used or Perfect Forward Secrecy (PFS) can be used: PFS basically performs DH again, but for the keying information for the data connections.
- ☒ Quick mode is used, making **C** incorrect. An SPI uniquely identifies a data connection, making **D** incorrect.

8.
- ☑ **D.** ESP uses a protocol number of 50 and AH a protocol number of 51.
- ☒ **A** breaks with any type of address translation. **B** is incorrect because NAT does not break ESP connections. **C** is incorrect because IPSec over TCP only supports ESP.

9.
- ☑ **B.** In transport mode, the real source and destination are protecting traffic.
- ☒ With **A**, internal addresses are hidden, where the packets are being protected, typically, by intermediate devices, as with a site-to-site connection. **C** is used to build the Phase 2 data connections. **D** can be used to build the Phase 1 management connection.

Building Tunnels with IPSec

10. Place the following Phase 1 main mode steps in the correct order: ?

- Verify the remote peer's identity.
- Use DH to establish a shared secret key over an unprotected communications channel.
- Negotiate the ISAKMP/IKE policy to use.

Answers

10.
- ☑ ISAKMP/IKE main mode goes through three steps during Phase 1: (1) negotiate the ISAKMP/IKE policy to use; (2) use DH to establish a shared secret key over an unprotected communications channel; and (3) verify the remote peer’s identity.