Chapter 16: Quiz – Overlay Tunnels (Answers) CCNPv8 ENCOR

itexamanswers.net/chapter-16-quiz-overlay-tunnels-answers-ccnpv8-encor.html

January 11, 2021

14. What is a function of the GRE protocol?

- to configure the set of encryption and hashing algorithms that will be used to transform the data sent through the IPsec tunnel
- **to encapsulate multiple OSI Layer 3 protocol packet types inside an IP tunnel**
- to configure the IPsec tunnel lifetime
- to provide encryption through the IPsec tunnel

Explanation: The transform set is the set of encryption and hashing algorithms that will be used to transform the data sent through the IPsec tunnel. GRE supports multiprotocol tunneling. It can encapsulate multiple OSI Layer 3 protocol packet types inside an IP tunnel. Routing protocols that are used across the tunnel enable dynamic exchange of routing information in the virtual network. GRE does not provide encryption.

15. Refer to the exhibit. A tunnel was implemented between routers R1 and R2. Which two conclusions can be drawn from the R1 command output? (Choose two.)

```
R1# show interface Tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 172.16.1.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.200.1, destination 209.165.200.2
  Tunnel protocol/transport GRE/IP

<output omitted>
```

- This tunnel mode is not the default tunnel interface mode for Cisco IOS software.
- This tunnel mode provides encryption.
- **The data that is sent across this tunnel is not secure.**
- This tunnel mode does not support IP multicast tunneling.
- **A GRE tunnel is being used.**

Explanation: According to the R1 output, a GRE tunnel mode was specified as the tunnel interface mode. GRE is the default tunnel interface mode for Cisco IOS software. GRE does not provide encryption or any other security mechanisms. Therefore, data that is sent across a GRE tunnel is not secure. GRE supports IP multicast tunneling.

16. For a VPN, which technology provides secure remote access over broadband?

- QoS
- ADSL
- LTE
- **IPsec**

Explanation: The IPsec (IP Security) applies security at the network layer of the OSI model and is used to secure VPN communication.

17. What is the purpose of LISP?

- It authenticates vSmart controllers and SDWAN routers.
- **It is an architecture created to address routing scalability problems.**
- It provides a permanent control plane connection over a DTLS tunnel.
- It performs load balancing of SD-WAN routers across vSmart controllers.

Explanation: Locator/Identifier Separation Protocol (LISP) is used by Internet providers, data centers, branch networks, and campus networks to address routing scalability problems and provide an overlay tunneling technology.

18. Which two protocols must be allowed for an IPsec VPN tunnel is operate properly? (Choose two.)

- **50**
- **51**
- 168
- 169
- 500
- 501

Explanation: ESP uses protocol 50. AH uses protocol 51. ISAKMP uses UDP port 500.

19. What is the purpose of a VXLAN?

- It provides site-to-site VPNs between cloud providers.
- It is an architecture created to address routing scalability problems.
- **It provides Layer 2 and Layer 3 overlay networks across a Layer 3 underlay network.**

- It encapsulates a variety of network layer protocols inside virtual point-to-point links.

Explanation: A virtual extensible local-area network (VXLAN) helps when virtualization is used and with Layer 2 problems that have arisen as a result. VXLAN extends Layer 2 and Layer 3 overlay networks over a Layer 3 underlay network using MAC-in IP/UDP tunneling.

20. What are the two peer authentication methods used by IPsec? (Choose two.)

- **PSK**
- GRE
- HMAC
- MD5
- **RSA signatures**

Explanation: IPsec can use pre-shared keys (PSK) and RSA signatures for peer authentication. GRE (Generic Routing Encapsulation) is a mechanism to implement a VPN. HMAC and MD5 relate to hashing algorithms not authentication processes.

21. When GRE is configured on a router, what do the tunnel source and tunnel destination addresses on the tunnel interface refer to?

- the IP addresses of the two LANs that are being connected together by the VPN
- the IP address of host on the LAN that is being extended virtually
- **the IP addresses at each end of the WAN link between the routers**
- the IP addresses of tunnel interfaces on intermediate routers between the connected routers

vA site-to-site VPN is established with a GRE tunnel. It does not link two LANs, but rather it extends the reach of a single LAN across a WAN. Tunnel interfaces are configured on routers at each end of the VPN, not in the intermediate routers.[/alert-success]

22. How does LISP resolve an EID into an RLOC?

- by using DNS
- **by sending a map request to the MR**
- by tunneling data from the interior routing protocol
- by encapsulating the EID packet and adding an outer header with the RLOC IP address

Explanation: The map resolver (MR) is a device such as a router that consults with the map server (MS) to locate and communicate with the proper tunnel router. This router then sends a map reply message to the originating router that includes the endpoint identifier (EID) to routing locator (RLOC) mapping.

23. Which algorithm is an asymmetrical key cryptosystem?

- **RSA**
- AES
- 3DES
- DES

Explanation: RSA is a cryptosystem for asymmetrical keys. AES, DES, and 3DES are all symmetric key cryptosystems.

24. Which remote access implementation scenario will support the use of generic routing encapsulation tunneling?

- a mobile user who connects to a router at a central site
- a branch office that connects securely to a central site
- a mobile user who connects to a SOHO site
- **a central site that connects to a SOHO site without encryption**

Explanation: The GRE tunneling protocol is used for site-to-site VPNs, not for remote access VPNs for mobile users. GRE alone does not provide any encryption, so the traffic is not secure between the endpoints.

25. Which UDP port number is assigned to VXLAN by IANA?

- 4341
- 4342
- **4789**
- 8472

Explanation: Linux servers use UDP port number 8472 for VXVLAN by default, but the IANA-issued port number is 4789. Port 4341 and 4342 are used with LISP.