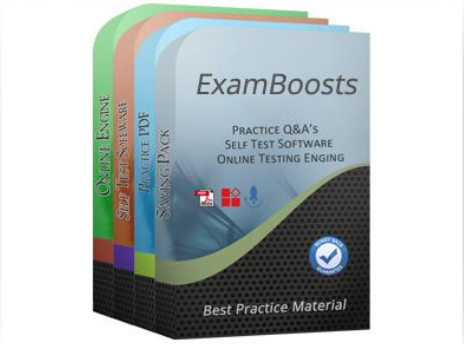
ExamBoosts

TRY BEFORE YOU BUY

Download a free sample of any of our exam questions and answers

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.



365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

http://www.examboosts.com/

Reliable & Efficient Test Practice Questions to Satisfy All Candidates

Exam : **H12-721-ENU**

Title : HCIP-Security-CISN(Huawei Certified ICT Professional - Constructing Infrastructure of Security Network)

Vendor : Huawei

Version : DEMO

NO.1 Which of the following descriptions is correct for the services supported by SSL VPN? (Multiple choices)

A. The file sharing service provides the shared resources of different system servers to the user in the form of web pages.

B. Network Expansion Service the remote client will automatically install a virtual network card to obtain a virtual IP address, just as it can use various services on the LAN, and can freely access any intranet resources.

C. Port forwarding is to obtain the specified destination IP address and port UDP packets on the client to access the specified resources on the intranet.

D. Web proxy service implements clientless page access. An HTTP session is established between the remote user and the firewall virtual gateway, and then the firewall virtual gateway establishes an HTTPS session with the Web Server.

Answer: A,B

NO.2 After importing the ISP address file on the Huawei USG6000 firewall, specify the outbound interface to be associated with an operator name. The firewall then generates the ISP route to this carrier network in batches. Which of the following description about this route is correct?

A. The protocol type displayed in the routing table is UNR (user network route).

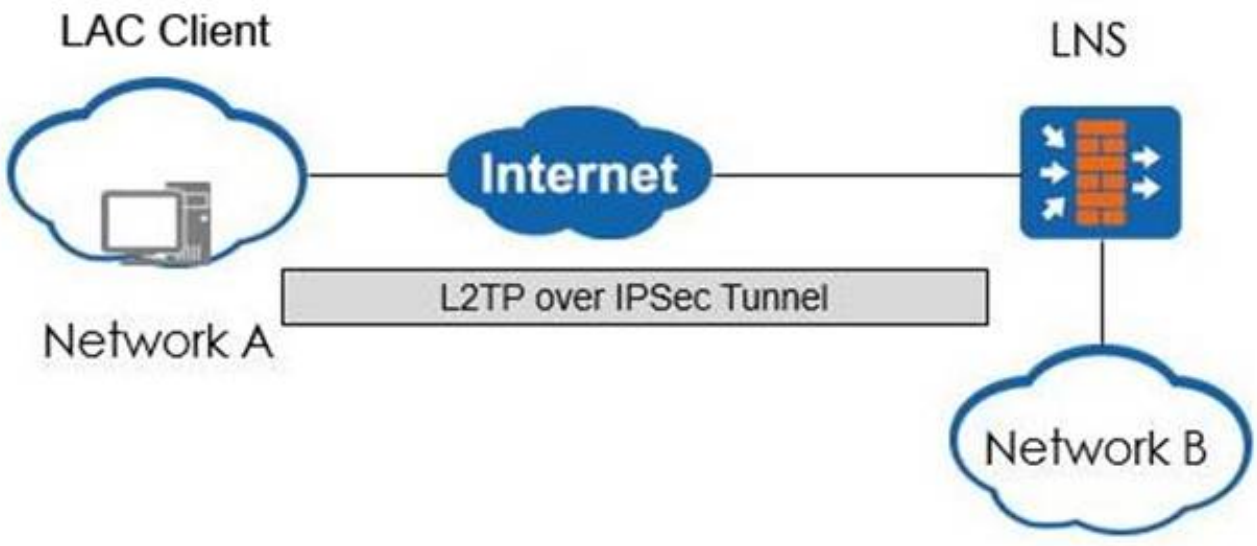
B. The next hop is the address of the device on the carrier's network.

C. The route priority is 60.

D. The source address is the IP address in the ISP address file.

Answer: A

NO.3 The following figure shows the L2TP over IPSec application scenario. The client uses the method of pre-shared-key for IPSec authentication. How to configure the IPSec security policy on the LNS port? (Multiple Choice)



A. Using IKE v2 for negotiation

B. Using IKE v1 main mode for negotiation

C. Configuring IPSec Security Policy

D. Configuring IPSec Policy Template
Answer: A,D

NO.4 Which of the following message information does not exist in IPSec VPN?
A. ESP message end
B. AH message header
C. AH message end
D. ESP message header
Answer: C

NO.5 As shown in the figure, BFD is bound to a static route. The administrator configures firewall A as follows:
[USG6000_A] bfd
[USG6000_A-bfd] quit
[USG6000_A] bfd as bind peer-ip 1.1.1.2
[USG6000_A-bfd-session-aa] discriminator local 10
[USG6000_A-bfd-session-aa] discriminator remote 20
[USG6000_A-bfd-session-aa] commit
[USG6000_A-bfd-session-aa] quit
Which of the following statements is correct for this configuration? (Multiple Choices)

A. [USG6000_A-bfd-session-aa] commit is optional. If you do not configure, the system default submits configuration and generates BFD session log information but does not create a session table.
B. Use the command of "bfd as bind peer-ip 1.1.1.2" to create a BFD session binding policy for detecting the link status.
C. In this command, [USG6000_A] bfd is incorrectly configured. Change it to [USG6000_A] bfd enable to enable BFD function.
D. The command to bind the BFD session to the static route is also required on the firewall:
[USG6000_A] ip route-static 0.0.0.0 0 1.1.1.2 track bfd-session aa
Answer: B,D

NO.6 Which of the following encryption methods is used by IPsec VPN to encrypt the communication data stream?
A. Symmetric key encryption
B. Public key encryption
C. Private key encryption
D. Pre-shared key encryption
Answer: A

NO.7 A virtual system is a plurality of mutually independent logical devices divided on a single physical device. Each virtual system is equivalent to a real device and has its own interface, address set, user/group, routing table entries, and policies. It can also be configured and managed by a virtual system administrator.
A. True
B. False
Answer: A

NO.8 Load balancing implements the function of allocating user traffic accessing the same IP address to different servers. Which of the following are main technologies?
A. Hot Standby Technology
B. Virtual Service Technology
C. Server health check
D. Load balancing algorithm
Answer: B,C,D

NO.9 Ensure that the traffic is not affected by the server or link failure. The administrator has configured the link health check. However, after the configuration is complete, the health check status is still Down. What are the possible causes? (Multiple Choice)
A. Health check is not invoked on the interface
B. The link for the health check has failed
C. The peer device did not release the corresponding protocol and port
D. Security policy did not release traffic
Answer: B,C,D

NO.10 IP-Link sends a probe packet to the specified IP address. By default, if three probes fail, the link to this IP address is considered to be faulty.
A. False
B. True
Answer: B

NO.11 Which of the following descriptions is incorrect regarding the authentication method used by the SSL VPN virtual gateway?
A. Local authentication means that the user name and password of the SSL VPN user are saved locally on the firewall and user authentication is performed on the firewall.
B. Certificate Challenge Authentication refers to the combination of authenticating client certificates with local or server authentication.
C. Anonymous certificate authentication means that the firewall only verifies the identity of the user by verifying the validity of the client certificate and password.
D. Server authentication means that the user name and password of the SSL VPN user are saved on the remote server. User authentication is required on the server.
Answer: C

NO.12 Users use SSL VPN to access intranet resources and use server authentication to authenticate

users. In order to distinguish corporate users in different regions and establish different user domains for users in different regions. When a user use SSL VPN authentication, the authentication prompts that the password is incorrect.
Which of the following are the possible causes of this failure? (Multiple choices)
A. The user entered the wrong user name and password.
B. The username and password do not exist.
C. The user domain was not entered when the user entered the user name.
D. The administrator has configured the wrong user domain.
Answer: A,C,D

NO.13 IPSec tunnel can use GRE over IPSec to propagate multicast packets.
A. True
B. False
Answer: A

NO.14 A company has three departments: research, marketing, and finance. The enterprise uses the local authentication of the firewall to perform user authentication for employees in each department. The authentication domain is default. Authenticated users can gain access to the company's internal network.Now companies want their employees to use the Webmail system to send and receive emails when they travel, and use ERP systems to work. How to deploy if using SSL VPN to access the network?
A. It is only necessary to allow external users to access the SSL VPN virtual gateway traffic on the firewall so that employees on business trips can use Webmail and ERP systems.
B. Because both the Webmail system and the ERP system can be accessed using the Web interface, the Web proxy function of the SSL VPN needs to be configured in order to meet employees' needs for accessing the internal server.
C. If employees on business trips use Webmail to send files, they need to enable file sharing.
D. Users can be divided into different user groups according to department attributes, and different SSL VPN services can be authorized for user groups.
Answer: B,D

NO.15 An enterprise deploys the Huawei USG6000 series firewall on the network. Users must log in to the firewall through Telnet or SSH. Each command entered by the user must be authorized by the server.
Which of the following authentication methods can meet the requirements?
A. HWTACACS
B. Radius
C. LDAP
D. AD
Answer: A

NO.16 In the IDC room, a Huawei USG6000 series firewall can be divided into several virtual systems. Then, the root firewall administrator generates virtual system administrators to manage each virtual system separately.

A. False
B. True
Answer: B

NO.17 When traffic is finally sent from the outgoing interface, it is limited by the bandwidth of the outgoing interface. If the traffic is greater than the outbound interface bandwidth, which of the following will be used to do queue scheduling for traffic to ensure that high-priority packets are sent preferentially?
A. Remark DSCP priority
B. QoS
C. Forwarding priority
D. Bandwidth policy matching order
Answer: C

NO.18 Huawei has the following bandwidth policy configuration command on the USG6000:
[USG] traffic-policy
[USG-policy-traffic] profile class1
[USG-policy-traffic-profile-class1] bandwidth maximum-bandwidth whole both 1000
[USG-policy-traffic-profile-class1] bandwidth connection-limit whole both 20
[USG-policy-traffic-profile-class1] quit
[USG-policy-traffic] rule name policy1
[USG-policy-traffic-rule-policy1] source-zone untrust
[USG-policy-traffic-rule-policy1] destination-zone dmz
[USG-policy-traffic-rule-policy1] destination-address 10.10.10.0 mask 255.255.255.0
[USG-policy-traffic-rule-policy1] action cos profile class1
[USG-policy-traffic-rule-policy1] quit
[USG-policy-traffic] rule name policy2
[USG-policy-traffic-rule-policy2] source -zo ne dmz
[USG-policy-traffic-rule-policy2] destination-zone untrust
[USG-policy-traffic-rule-policy2] destination-address 10.10.10.5 mask 255.255.255.255
[USG-policy-traffic-rule-policy2] action no-qos
Which of the following statements are correct? (Multiple choices)
A. When accessing a host with a destination address of 10.10.10.5, the number of connections will be limited
B. When accessing a host with a destination address of 10.10.10.5 will not be limited by the bandwidth policy
C. When accessing the destination network segment 10.10.10.0/24, it will not be restricted by the maximum number of connections 20
D. When accessing the destination network segment 10.10.10.0/24, traffic will be limited by a maximum of 20 connections.
Answer: B,D