## Question: 1

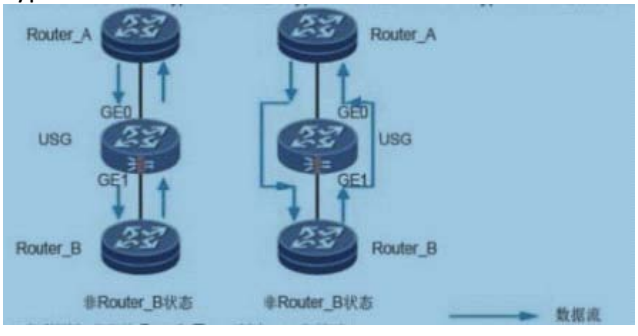
Defense against the cache server The main method of DNS request flood is to use the DNS source authentication technology:

A. TRUE
B. FALSE

**Answer: A**

## Question: 2

The figure shows the data flow direction of the Bypass interface in the Bypass working mode and the non-Bypass working mode. What are the following statements about the working flow of the electrical Bypass interface?




A. When the interface is in the non-bypass state, the traffic flows from the GE0 interface to the USG through Router_a. After the USG processes, the traffic flows from the GE1 interface to Router_B.
B. When the interface is working in the Bypass state, the traffic is forwarded from the GE0 interface to the USG. The USG does not pass any processing and flows directly from the GE1 interface to Router_B.
C. When the firewall is configured to implement the security priority, the uplink and downlink services are not interrupted when the interface works in the bypass state. Therefore, the device can be kept in the Bypass state.
D. The electrical bypass interface can only work in Layer 2 mode and has circuit bypass function.

**Answer: A, B**

## Question: 3

What are the drainage schemes that can be used in the scenario of bypass deployment in Huawei's abnormal traffic cleaning solution?

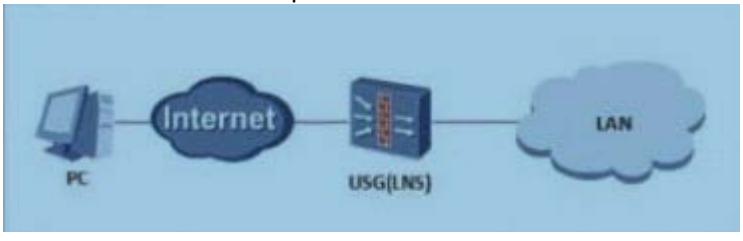
A. dynamic routing drainage

B. static policy routing drainage
C. static route drainage
D. MPLS VPN drainage

**Answer: ABCD**

## Question: 4

A network is as follows: The l2tp vpn is established through the VPN Client and the USG (LNS). What are the reasons for the dialup failure?




A. The tunnel name of the A LNS is inconsistent with the tunnel name of the client.
B. L2TP tunnel verification failed
C. 0PPP authentication failed, the PPP authentication mode set on the client PC and LNS is inconsistent.
D. The client PC cannot obtain the IP address assigned to it from the LNS.

**Answer: B, C, D**

## Question: 5

Which of the following statements is correct about the IKE main mode and the aggressive mode?

A. All negotiation packets in the first phase of the aggressive mode are encrypted.
B. All the negotiation packets of the first phase in the main mode are encrypted.
C. barbarian mode uses DH algorithm
D. will enter the fast mode regardless of whether the negotiation is successful or not.

**Answer: C**

## Question: 6

Accessing the headquarters server through the IPSec VPN from the branch computer. The IPSec tunnel can be established normally, but the service is unreachable. What are the possible reasons?

A. packet is fragmented, and fragmented packets are discarded on the link.

B. There is load sharing or dual-machine link, which may be inconsistent with the back and forth path.
C. route oscillating
D. DPD detection parameters are inconsistent at both ends

**Answer: A**

## Question: 7

When the user's SSL VPN has been successfully authenticated, the user cannot access the Web-link resource. On the Web server, view the information as follows: netstat -anp tcp With the following information, which of the following statements is correct?

Active Connections

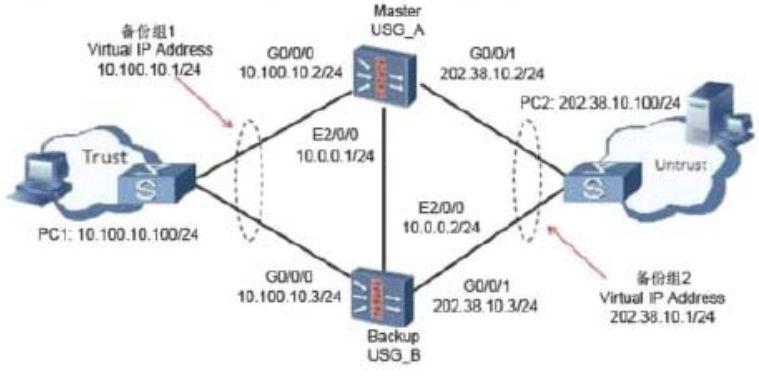
| Proto | Local Address | Foreign Address | State |
|---|---|---|---|
| TCP | 0.0.0.0:135 | 0.0.0.0:0 | LISTENING |
| TCP | 0.0.0.0:445 | 0.0.0.0:0 | LISTENING |
| TCP | 0.0.0.0:3389 | 0.0.0.0:0 | LISTENING |
| TCP | 0.0.0.0:9593 | 0.0.0.0:0 | LISTENING |
| TCP | 0.0.0.0:9594 | 0.0.0.0:0 | LISTENING |

A. intranet server does not open web service
B. virtual gateway policy configuration error
C. The connection between the virtual gateway and the intranet server is incorrect.
D. Virtual gateway and intranet server are unreachable

**Answer: A**

## Question: 8

According to the dual-system hot backup network diagram, what are the correct descriptions in the following dual-system hot backup preemption function?



A. VRRP backup group itself has a preemption function. As shown in the figure, after USG_A fails and recovers, USG_A will use the preemption function to change to the master state again.
B. The preemption function of the V VGMP management group is similar to that of the VRRP backup group. When the faulty backup group in the management group recovers, the management group priority will be restored.
C. By default, when the preemption delay is 0, the preemption is never preempted.
D. After the VRRP backup group is added to the VGMP management group, the original preemption function on the backup group will be invalid.

**Answer: A, B, D**

## Question: 9

Is the correct statement about TCP proxy and TCP reverse source probing?
A.TCP proxy and TCP reverse source probe can prevent SYN Flood
B. The principle of the TCP proxy is that the device acts as a proxy for the TCP connection between the two ends. When one end initiates the connection, it must first complete the TCP 3 handshake with the device.
C. Use TCP proxy mode for attack defense, you must enable the state detection mechanism.
D. TCP reverse source detection detects the source IP by sending a Reset packet.

**Answer: A, B, C**

Explanation:
Note: TCP reverse source detection principle, when the device receives a SYN message, it will detect the existence of the source IP. The TCP reverse source detects the SYN-ACK sequence number that is sent incorrectly. If the source exists, it will send an RST message to request a three-way handshake. Because the reverse source detection mechanism is not affected by the successful establishment of the session table, it is recommended to use the reverse source detection technology to defend against SYN flood attacks. If you use TCP proxy attack defense, you must enable the state detection mechanism.

## Question: 10

In dual-system hot backup, the backup channel must be the primary interface on the interface board. Which type is not supported?

A. Ethernet
B. GigabitEthernet
C. E1
D. Vlan-if

**Answer: C**

## Question: 11

The DHCP snooping function needs to maintain the binding table. What are the contents of the binding table?

A. MAC
B. Vlan
C. interface
D. DHCP Server IP

**Answer: A, B, C**

Explanation:
Note: The DHCP snooping function needs to maintain the binding table. The contents of the binding table include: MAC, Vlan, and interface.

## Question: 12

By configuring the Bypass interface, you can avoid the network interruption caused by the device fault and improve the reliability of the network. The bypass function can be used to configure the Bypass function by configuring the Bypass parameters on any GE interface.

A. TRUE
B. FALSE

**Answer: A**

## Question: 13

What are the correct descriptions of IPSec and IKE below?

A. IPSec has two negotiation modes to establish an SA. One is manual (manual) and the other is IKE (isakmp) auto-negotiation.
B. IKE aggressive mode can choose to find the corresponding authentication key according to the negotiation initiator IP address or ID and finally complete the negotiation.
C. NAT traversal function deletes the verification process of the UDP port number during the IKE negotiation process, and implements the discovery function of the NAT gateway device in the VPN tunnel. That is, if the NAT gateway device is found, it will be used in the subsequent IPSec data transmission. UDP encapsulation
D. IKE security mechanisms include DH Diffie-Hellman exchange and key distribution, complete forward security and SHA1 encryption algorithms.

**Answer: A, B, C**

## Question: 14

In the case of IPSec VPN NAT traversal, you must use IKE's aggressive mode.

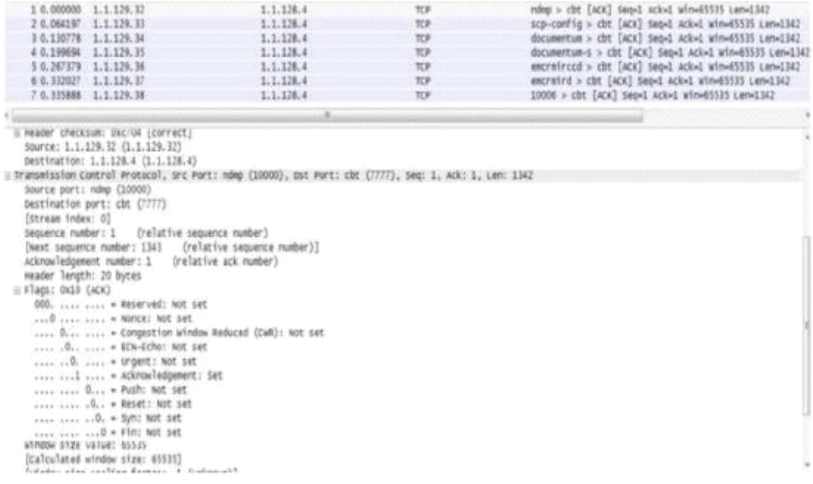
A. TRUE
B. FLASE

**Answer: B**

Explanation:
Note: The IKE master mode of the certificate mode can also implement NAT traversal of IPSec VPN.

## Question: 15

When attacked, the screenshot of the message captured by a victim host is as follows. According to the analysis, what is the attack?

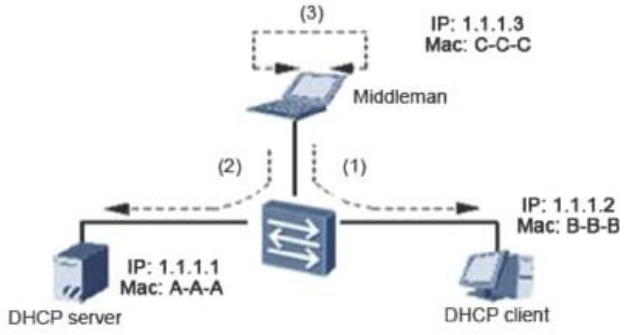



A. SYN Flood
B. SYN-ACK Flood
C. ACK-Flood
D. Connection Flood

**Answer: C**

## Question: 16

Man-in-the-middle attacks are: the middleman completes the data exchange between the server and the client. In the server's view, all messages are sent or sent to the client. From the client's point of view, all messages are also sent or sent.




A. Packet 1: Source IP 1.1.1.1 Source MAC C-C-C Destination IP 1.1.1.2 Destination MAC B-B-B
B. Packet 1: Source IP 1.1.1.3 Source MAC C-C-C Destination IP 1.1.1.2 Destination MAC B-B-B
C. Packet 2: Source IP 1.1.1.2 Source MAC C-C-C Destination IP 1.1.1.1 Destination MAC A-A-A
D. Packet 2: Source IP 1.1.1.3 Source MAC C-C-C Destination IP 1.1.1.1 Destination MAC A-A-A

**Answer: A, C**

## Question: 17

The SSL VPN authentication login is unsuccessful and the message "Bad username or password" is displayed. Which one is wrong?

A. username and password are entered incorrectly
B. user or group filter field configuration error
C. certificate filter field configuration error
D. administrator configured a policy to limit the source IP address of the terminal

**Answer: D**

## Question: 18

On an Eth-Trunk interface, traffic load balancing can be implemented by configuring different weights on member links.

A. TRUE
B. FLASE

**Answer: A**

## Question: 19

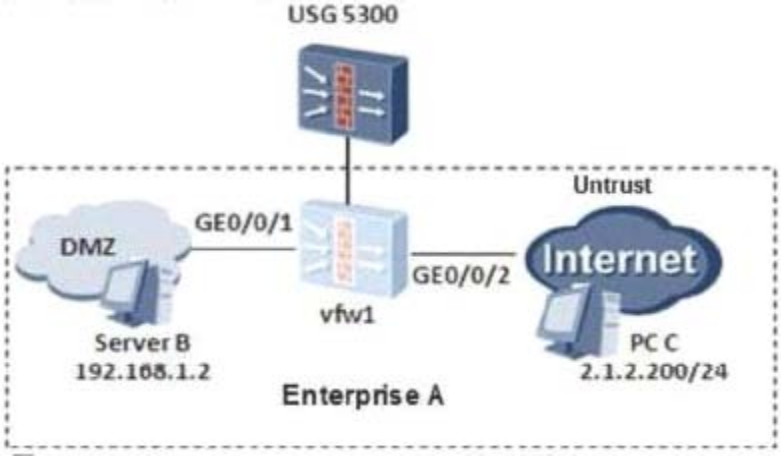
SSL works at the application layer and encrypts specific applications. Which layer does IPSec work on and provides transparent encryption protection for this layer and above?

A. data link layer
B. network layer
C. transport layer
D. representation layer

**Answer: B**

## Question: 20

On the following virtual firewall network, the USG unified security gateway provides leased services to the enterprise. The VPN instance vfw1 is leased to enterprise
A. The networking diagram is as follows. The PC C of the enterprise A external network user needs to access the intranet DMZ area server B through NAT. To achieve this requirement, what are the following key configurations?




A. [USG] ip vpn-instance vfw1 vpn-id
B. [USG] ip vpn-instance vfw1 [USG-vpn-vfw1] route-distinguisher 100:1 [USG-vpn-vfw1] quit
C. [USG] nat server zone vpn-instance vfw1 untrust global 2.1.2.100 inside 192.168.1.2 vpn-instance vfw1
D. [USG]nat address-group 1 2.1.2.5 2.1.2.10 vpn-instance vfw1

**Answer: A, B, C**

Explanation:
key configuration: First, create/delete VPN instance [undo] ip vpn-instance vpn-instance-name [vpn-id vpn-id] Second, specify the route ID for the VPN instance route-distinguisher vpn-route-distinguisher