H12-222

Number: H12-222
Passing Score: 800
Time Limit: 4 min

Exam A

QUESTION 1
The main method of caching servers DNS Request Flood defense is the use of DNS source authentication.

A. TRUE
B. FALSE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Refer to the following diagram in regards to Bypass mode.

Which of the following statements is correct a few? (Choose two answers)

A. When the interface is operating in a non-Bypass state, the flow from the inflow of USG Router_A interfaces from GE0, GE1 after USG treatment from the interface flow Router_B
B. When the Interface works in Bypass state, traffic flow from the interface by the Router_A GE0 USG, USG without any treatment, flows directly Router_B flows from the GE1 interfaces.
C. When there are firewall requirements to achieve security policies, while working at the interface Bypass state to operate without interruption. Therefore, the device can be maintained in the Bypass state job.
D. Power Bypass interface can work in bridge mode, and can work with the bypass circuit.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
QUESTION 3
With the Huawei abnormal flow cleaning solution, deployed at the scene of a bypass, drainage schemes can be used to have? (Choose three answers)

A. Dynamic routing drainage
B. Static routing strategy drainage
C. Static routing drainage
D. MPLS VPN cited

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Regarding IKE main mode and aggressive modes, which of the following statements is correct?

A. In savage mode with the the first phase of negotiation, all packets are encrypted
B. All main mode packts under the first phase of negotiation are encrypted
C. The DH algorithm is used in aggressive mode
D. Whether the negotiation is successful or not, IKE will enter into fast mode

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
A network is shown below.

A dial customer cannot establish a connection via a VPN client PC and USG (LNS) l2tp vpn. What are valid reasons for this failure? (Choose three answers)

A. LNS tunnel tunnel name change is inconsistent with the client name.
B. L2TP tunnel authentication failed.
C. PPP authentication fails, PPP authentication mode set on the client PC and LNS inconsistent.
D. Client PC can not obtain an IP address assigned to it from the LNS.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
From the branch offices, servers are accessed from the Headquarters via IPsec VPN. An IPSEC tunnel can be established at this time, but communication to the servers fails. What are the possible reasons? (Choose three answers)

A. Packet fragmentation, the fragmented packets are discarded on the link.
B. Presence opf dual-link load balancing, where the path back and forth may be inconsistent.
C. Route flapping.
D. Both ends of the DPD detection parameters are inconsistent.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
A user has been successfully authenticated using an SSL VPN. However, users can not access the Web-link resources through the Web server.

Using the information provided, which of the following is correct?

A. Network server does not have the Web services enabled.
B. Virtual Gateway policy configuration error
C. Virtual connection between the gateway and the network server is not normal

D. Virtual gateway and network server is unreachable

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 8
According to the network diagram regarding hot standby, which of the following are correct? (Choose three answers)

A. VRRP backup group itself has preemption. As shown, when USG_A failurs and is restored, USG_A re-use preemption becomes it has master status.
B. With VGMP management group preemption and VRRP backup groups, when the management group fails and recovers, the priority management group will also be restored.
C. By default, the preemption delay is 0.
D. If a VRRP group is added to the VGMP management group, preemption will fail. The VGMP unified management group decides this behavior.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following are correct regading TCP and TCP proxy on the reverse source detection? (Choose three answers)

A. TCP and TCP proxy detection can prevent reverse source SYN Flood.

B. TCP proxy acts as a proxy device. TP is connected between both ends, when one end initiates a connection with the device it must complete the TCP three-way handshake.
C. With TCP proxy mode attack prevention, detection mechanism must be turned on.
D. TP reverse source probes to detect the source IP packets by sending a Reset.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
QUESTION 10
IPsec tunneling is used as a backup connection as shown below:

Which of the following statements are true about the tunnel interface? (Choose two answers)

A. IPsec security policy should be applied to the tunnel interface
B. Protocol for the Tunnel Interface must be GRE.
C. Tunnel interface needs to be configured on the IP address and the IP address of the gateway. The external network IP address of the outgoing interface must be in the same network segment.
D. Tunnel interfaces can be added to any security zone, provided they have the appropriate interdomain security policies.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
The DHCP Snooping binding table function needs to maintain its binding table of contents that include? (Choose three answers)

A. MAC
B. Vlan
C. Interface
IP D. DHCP Server's

Correct Answer: ABC

Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Through the configuration of the Bypass interface, you can avoid network communication interruption caused by equipment failure and improve reliability. The power Bypass function can use any network interfaces to configure the Bypass GE parameters to achieve the Bypass function.

A. TRUE
B. FALSE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following statements about IPsec and IKE following are correct? (Choose three answers)

A. With IPsec there are two ways to establish the security association, manual mode (manual) and IKE auto-negotiation (Isakmp) mode.
B. IKE aggressive mode can be selected based on negotitations initiated by the tunnel endpoint IP address or ID, to find the corresponding authentication word and finalize negotiations.
C. The NAT traversal function is used to delete the IKE negotiation verification process for UDP port numbers, while achieving a VPN tunnel to discover the NAT gateway function. If a NAT gateway device is used, then the data transfer after the IPsec uses UDP encapsulation.
D. IKE security mechanisms include DH Diffie-Hellman key exchange and distribution; improve the security front (Perfect Forward Secrecy PFS), encryption, and SHA1 algorithms.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
In the attack shown below, a victim host packet captures the traffic. According to the information shown, what kind of attack is this?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 15
In IPsec VPN with NAT traversal, you must use IKE aggressive mode.

A. TRUE
B. FALSE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
A man in the middle attack refers to an intermediate that sees the data exchange between server and client. To the server, all messages appear to be sent to or received from the client; and to the client all the packets appear to have been sent to or received from the server. If a hacker is using the man-in-the-middle attack, the hacker will send at least two data packets as shown to achieve this attack.

Which of the following packet 1 and packet 2 Field Description is correct? (Choose two answers)

A. Packet 1:
Source IP 1.1.1.1
Source MAC C-C-C
The purpose of IP 1.1.1.2
The purpose of Mac B-B-B

B. Packet 1:
Source IP 1.1.1.3
Source MAC C-C-C
The purpose of IP 1.1.1.2
The purpose of Mac B-B-B

C. Packet 2:
Source IP 1.1.1.2
Source MAC C-C-C
The purpose of IP 1.1.1.1
The purpose of Mac A-A-A

D. Packet 2:
Source IP 1.1.1.3
Source MAC C-C-C
The purpose of IP 1.1.1.1
The purpose of Mac A-A-A

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
In an Eth-Trunk interface, you can achieve load balancing by configuring different weights on each member link.

A. TRUE
B. FALSE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18

A SSL VPN login authentication is unsuccessful, and the prompt says "wrong user name or password." What is wrong?

A. The username and password entered incorrectly.
B. There is a user or group filter field configuration error.
C. There is a certificates filter field configuration error.
D. The administrator needs to configure the source IP address of the terminal restriction policy.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
SSL works at the application layer and is encrypted for specific applications, while IPsec operates at which layer and provides transparent encryption protection for this level and above?
A. The data link layer
B. Network Layer
C. Transport Layer
D. Presentation Layer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
The IP-MAC address binding configuration is as follows:
[USG] firewall mac-binding 202.169.168.1 00e0-fc00-0100
When the data packets travel through the Huawei firewall device, and other strategies such as packet filtering, attack prevention are not considered, the following data ttravels hrough the firewall device? (Choose two answers)

A. Packet source IP: 202.169.168.1
Packet source MAC: FFFF-FFFF-FFFF
B. Packet source IP: 202.169.168.2

Packet source MAC: 00e0-fc00-0100

C. Packet source IP: 202.1.1.1
Packet source MAC: 00e0-fc11-1111

D. Packet source IP: 202.169.168.1
Packet source MAC: 00e0-fc00-0100

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Dual hot standby load balancing service requires three interfaces, one for the line connecting the router, and two USG facilities mutual backup, configuration commands are “hrp track master” and “hrp track slave”

A. TRUE
B. FALSE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22

IP-link probe packets will be sent to the specified IP address by default when the probe fails three times, enabling this interface if the main link fails.

A. TRUE
B. FALSE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Two endpoints cannot build a successful IPsec VPN session. Which of the following firewall configuation errors could be the problem? (Choose three answers)

A. A device does not have a route to the peer within the network.
B. A gateway configuration on both ends with the referenced ACL security policy C. The gateway configuration on both ends of the IPsec proposal is inconsistent.
D. Both ends are not configured for DPD.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Testing Center is responsible for flow testing, and test results sent to the management center.

A. TRUE
B. FALSE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which of the following are scanned snooping attack??

A. SIP Flood attacks
B. HTTP Flood Attack
C. IP address scanning attack
D. ICMP redirect packet attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following VPN protocols do not provide encryption? (Choose three answers)

A. ESP
B. AH
C. L2TP
D. GRE

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
When a Haiwei Secure VPN client connection initializes using L2TP, the L2TP packet uses a source port of 1710, and a destination port of 1710.

A. TRUE
B. FALSE

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
A user logs into the Virtual Gateway Web Page but receives a "can not display the webpage" message. What are possible causes for this? (Choose two answers)

A. Virtual Gateway Router unreachable from user PC
B. Virtual Gateway IP address has been changed.
C. Using a Shared Web Gateway
D. Client browser set up a proxy server.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
See the following firewall information:

Based on the output, which of the following answers are correct? (Choose three answers)

A. The first packet interface to enter this data stream from the Trust zone, issuing from the Untrust zone interfaces
B. This data stream has been NATed
C. NAPT conversion technology is being used
D. The virtual firewall feature is enabled firewall

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
In the Huawei abnormal flow cleaning solution, deployed at the scene of a bypass, the re-injection scheme can be used to have which of the following? (Choose three answers)

A. routing strategy
B. MPLS VPN tunnel mode
C. routing
D. Layer 2 VPN mode

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
When an attack occurs, the attacked host (1.1.129.32) was able to capture many packets as shown. Based on the information shown, what kind of attack is this?

A. Smurf attack
B. Land Attack
C. WinNuke
D. Ping of Death attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Refer to the following NIP firewall intrusion detection actions:
1 records the invasion process, alarm logging
2. NIP attack detection
3 reconfigure the firewall
4 Termination invasion
Which of the following is the correct sequence of events?

A. 1 -> 2 -> 3 -> 4
B. 2 -> 1 -> 3 -> 4
C. 3 -> 1 -> 2 -> 4
D. 1 -> 2 -> 4 -> 3

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
An administrator views the status information and IPsec Debug information as follows:

What is the most likely reason for failure?

A. The end ike ike peer strategies and policies do not match
B. The end ike remote name and peer ike name does not match
C. The end ipsec proposal and peer ipsec proposal does not match
D. The end of the Security acl or does not match the peer Security acl

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
PCA has an IP address of 192.168.3.1 in the Trust area. In the Untrust zone users cannot access the Internet server.

Based on the configuration of the Trust and Untrust fields above, what is the most likely cause of the failure?

A. A misconfigured security policies, the direction should be Outbound.
B. Since the first rule of the firewall is the default packet-filter deny, the configuration is not implemented.
C. The policy source of 192.168.3.0 0.0.0.255 is incorrect; you need to modify a policy source 192.168.3.0 0.0.255.255.
D. The policy destination any is incorrect; you must define a clear destination IP address.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which of the following is a drawback of an L2TP VPN?

A. It cannot be routed in two layers
B. You must use L2TP Over IPsec
C. No authentication
D. No encryption

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 36
Regarding the Radius authentication process, refer to the following steps:
1. Network device Radius client (network access server) receives the user name and password, and sends an authentication request to the Radius server.
2. When a user logs into the USG access servers and other network devices, the user name and password will be sent to the network access server.
3. After the Radius server receives a valid request to complete the request and the required user authorization information is sent back to the client. Which of the following is a correct sequence?

A. 1-2-3
B. 2-1-3
C. 3-2-1
D. 2-3-1

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
With IP-link, information is sent to the destination address specified with continuous ICMP packets or ARP request packets, and checks whether you can receive the destination IP response icmp echo reply packets or ARP reply packets.

A. TRUE
B. FALSE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
With the Huawei abnormal flow cleaning solution, deployed at the scene of a bypass, dynamic routing drainage occurs without human intervention. When an abnormality is detected, the management center will generate a draining task automatically, and the task is done directly after the drainage cleaning equipment is issued if testing equipment.
A. TRUE
B. FALSE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which of the following statements is wrong regarding IPsec?

A. Under Transfer Mode, ESP does not validate the IP header
B. AH can not verify that the data uses encrypted packets
C. ESP can support NAT traversal
D. The AH protocol uses the 3DES algorithm for data validation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Malformed packet attack techniques would use some legitimate packet data for network reconnaissance or testing. Tthese packets are legitimate for the application type; while normal network packets are rarely used.

A. TRUE
B. FALSE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 41
Which ofthe following statements is correct about the blacklist? (Choose three answers)

A. When you log into a device and incorrectly enter the username/password three times, the IP address of the administrator will be added to the blacklist via Web or Telnet.
B. Blacklist is divided into static and dynamic.
C. When the device is perceived to have behavioral characteristics of packets to a user's attempt to attack a specific IP address, it will use a dynamic IP address blacklist technology.
D. When the packet reaches the firewall, the first thing to check for is packet filtering, and then it will match the blacklist.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
In a stateful standby failover switchover what will the firewall do? (Choose two answers)

A. Send a gratuitous ARP
B. Send proxy ARP
C. The VRRP backup group virtual address will be unavailable
D. The switchover automatically updates the relevant MAC table

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
In L2TP over IPsec scenarios, The USG device will first use the original data packet that is encrypted using IPsec, and then encapsulates the data packets using L2TP.

A. TRUE
B. FALSE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
The Huawei abnormal flow cleaning solution must be deployed in an independent testing center.

A. TRUE
B. FALSE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Regarding IKE DPD, which statement is incorrect?

A. IKE is used to detect the state of a neighbor
B. DPD regularly send messages between IKE peers.
C. When DPD messages are not received within the specified time DPD sends a request to the remote side and waits for response packets.
D. DPD sends encrypted queries only when the timer expires.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 46
Refer to the following hot standby and IP-link linkage networking environment shown below:

Which configuration will enable hot standby configuration key linkage?

A. hrp mirror ip-link 1
B. hrp track ip-link 1 master
C. hrp track ip-link 1 slave
D. ip-link check enable

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Virtual firewall technology does not include which of the following characteristics?

A. Provides multi-instance routing, security, multi-instance, multi-instance configuration, NAT multi-instance, VPN multi-instance application flexibility to meet a variety of networking needs.
B. Each virtual firewalls can support four separate security zones TRUST, UNTRUST, DMZ, etc., flexible interface partitioning and allocation.
C. It guarantee that every virtual system and a separate firewall instance, and can be safely implement access between each virtual system.
D. Each virtual system provides independent administrator privileges.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which statement is correct regarding load checks and fingerprint learning with UDP Flood defenses.

A. UDP packet data segments are exactly the same content that can be used to check the load defense.
B. Fingerprint learning is dynamically generated by cleaning equipment, the attack packets after learning some salient features of the fingerprint, fingerprint matching packets will be dropped.
C. Load inspection checks all UDP packets of data.
D. Load checks need to set the offset number of bytes, fingerprint learning does not need to set the offset number of bytes.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
When there is a lot BFD sessions in a system, in order to prevent periodic OFD control packets from affecting the normal operation of the system, you can use what mode of BFD?

A. Synchronous Mode
B. Detection Mode
C. Asynchronous Mode
D. Query Mode

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Three FTP servers are configured with load balancing on a USG firewall. The address and weights of the three real servers are 10.1.1.3/24 (weight 16), 10.1.1.4/24 (weight 32), 10.1.1.5 / 24 (weight 16), while the virtual server address is 202.152.26.123/24. A host address with the IP address 202.152.26.3/24 initiates access to the FTP server.
On the firewall running the display firewall session table command detection configuration, which of the following situations illustrate the successful implementation of load balancing?

A. <USG> display firewall session tableCurrent total
sessions: 1
ftp VPN: public -> public 202.152.26.3:3327 -> 10.1.1.4:21
B. <USG> display firewall session tableCurrent total
sessions: 3 ftp VPN: public -> public
202.152.26.3:3327 -> 202.152.26.123:21
[10.1.1.3:21] ftp VPN: public -> public

202.152.26.3:3327 -> 202.152.26.123:21
[10.1.1.4:21]
ftp VPN: public -> public 202.152.26.3:3327 -> 202.152.26.123:21 [10.1.1.5:21]

C. <USG> display firewall session tableCurrent total
sessions: 1
ftp VPN: public -> public 202.152.26.3:3327 -> 202.152.26.123:21

D. <USG> display firewall session tableCurrent total
sessions: 3 ftp VPN: public -> public
202.152.26.3:3327 -> 10.1.1.3:21 ftp VPN: public -
> public 202.152.26.3:3327 -> 10.1.1.4:21 ftp
VPN: public -> public 202.152.26.3:3327 ->
10.1.1.5:21

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference: