DUMPSBOSS.

Huawei Certified ICT Professional - Constructing Infrastructure of Security Network

Huawei H12-721

Version Demo

Total Demo Questions: 46

Total Premium Questions: 468

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Security Network Basics	50
Topic 2, Firewall Technology	194
Topic 3, VPN Technology	140
Topic 4, IPS Technology	9
Topic 5, Anti-DDoS Technology	72
Topic 6, Security Network Solution	3
Total	468

QUESTION NO: 1

USG A and USG B are configured with a static BFD session. The following is true about the process of establishing and tearing down a BFD session.

A. USG A and USG B each start the BFD state machine. The initial state is Down and the BFD packet is Down. The value of Your Discriminator is 0.

B. After the local BFD status of USG B is Init, if it continues to receive packets with the Down status, it can re-process and update its local status.

C. After receiving the BFD packet in the Init state, USG B switches the local state to Up.

D. After the state transition of "DOWN-->INIT" occurs on USG A and USG B, a timeout timer is started. If no BFD packet in the Init or Up state is received before the timer expires, the local state is automatically switched back to Down.

ANSWER: C D

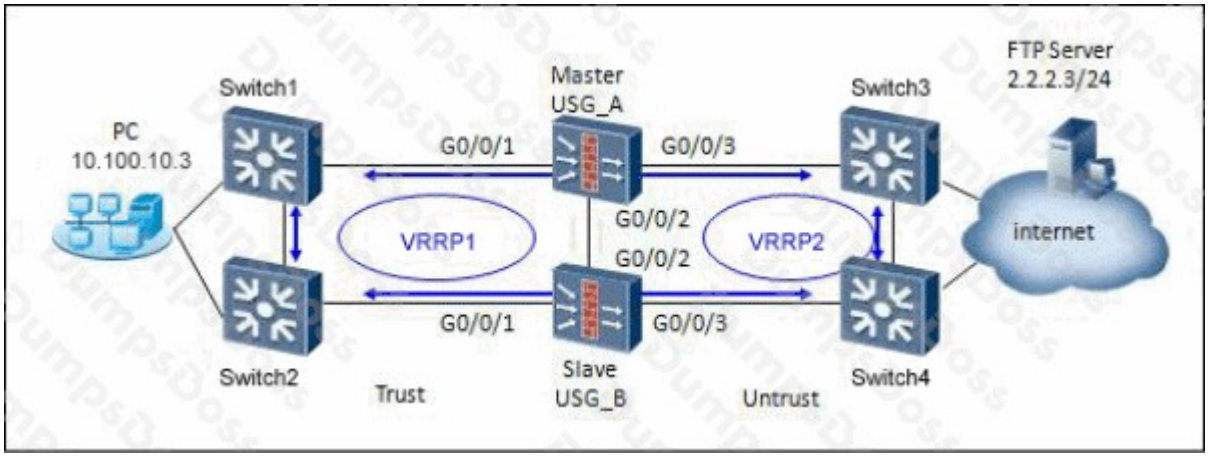
Explanation:

“After receiving the BFD packet in the Init state, USG B switches the local state to Up” is correct because the BFD finite-state machine uses the Init state to complete the bidirectional session handshake. Once a peer has progressed to Init and receives an Init control packet from the remote peer, it has confirmation that both directions of the BFD session are operating; it can therefore transition its local BFD state to Up. The same state-machine behavior occurs symmetrically on the other USG, resulting in an established BFD session.

“After the state transition of ‘DOWN-->INIT’ occurs on USG A and USG B, a timeout timer is started. If no BFD packet in the Init or Up state is received before the timer expires, the local state is automatically switched back to Down” is correct because BFD continuously verifies forwarding continuity through received control packets. The negotiated detection time determines how long a device can wait without receiving valid BFD packets. Expiry of that detection timer declares the session down and returns the local state to Down, allowing associated routing or protection mechanisms to react quickly. This behavior follows the BFD state-machine and timeout rules specified in RFC 5880; Huawei’s BFD feature documentation is available through the Huawei product documentation portal.

QUESTION NO: 2

In the dual-system hot backup networking environment as shown in the standby firewall also need to configure NAT function, assuming that the external address of the VRRP backup group. NAT address pool and NAT Server in the same network segment. Which of the following configuration needs to be on the Server? (choose two answers)



A. HRP_M [USG_A] nat address-group 1 2.2.2.5 2.2.2.6 vrrp 1

B. HRP_M [USG_A] nat address-group 1 2.2.2.5 2.2.2.6 vrrp 2

C. HRP_M [USG_A] nat server global 2.2.2.10 inside 10.100.10.3 vrrp 2

D. HRP_M [USG_A] nat server global 2.2.2.10 inside 10.100.10.3 vrrp 1

ANSWER: B C

Explanation:

The required configuration associates both the source-NAT address pool and the destination-NAT server mapping with VRRP group 2. In a dual-system hot-backup deployment, the public addresses used for NAT must be bound to the VRRP group that owns the external-side virtual gateway. This binding lets the active firewall use the relevant NAT resources while also allowing the standby firewall to take ownership of those resources consistently after a VRRP master/backup switchover. Therefore, `nat address-group 1 2.2.2.5 2.2.2.6 vrrp 2` binds the public source-NAT address range to the correct external VRRP group. Likewise, `nat server global 2.2.2.10 inside 10.100.10.3 vrrp 2` binds the published server address to that same group, so inbound traffic for the public address continues to reach the internal server after failover. The NAT pool and NAT Server public addresses being in the same external network does not remove the need for the explicit VRRP association; it is precisely what makes the public NAT identities movable with the active gateway role. Huawei's product documentation is available through the Huawei Enterprise documentation portal; VRRP's virtual-router ownership and failover model is defined in RFC 5798.

QUESTION NO: 3

The dual-system hot backup load balancing service interface works at Layer 3, and the upstream and downstream routers are connected to each other. The two USG devices are active and standby. Therefore, both the hrp track master and the hrp track slave must be configured on the morning service interface.

A. TRUE

B. FALSE

ANSWER: A

Explanation:

TRUE is correct. In a Layer 3 dual-system hot-standby deployment in which the upstream and downstream routers are interconnected, the service-side path may remain physically available even when a firewall or one of its service links can no longer correctly forward traffic. Configuring `hrp track master` and `hrp track slave` on the relevant service interfaces lets the Huawei USG hot-standby mechanism monitor those forwarding paths from both roles. The resulting interface-state information is used by HRP to support reliable active/standby service continuity and appropriate route handling during a service-link fault or role transition. This is especially relevant when each firewall participates in the Layer 3 topology rather than operating as a transparent inline pair. In this design, the standby device also uses an increased route cost for externally learned or advertised paths by default, helping ensure that the active device is preferred under normal conditions. Huawei's firewall high-availability documentation describes HRP-based active/standby networking and service-interface tracking configuration: Huawei Firewall Configuration Guide. Huawei's Enterprise support documentation portal also provides the applicable USG product-version command references for HRP configuration: Huawei Enterprise Documentation.

QUESTION NO: 4

Which protocol is normally used by a Huawei firewall to query the status of a member in an active/standby firewall hot standby group?

A. HRP

B. FTP

C. SNMP

D. DHCP

ANSWER: A

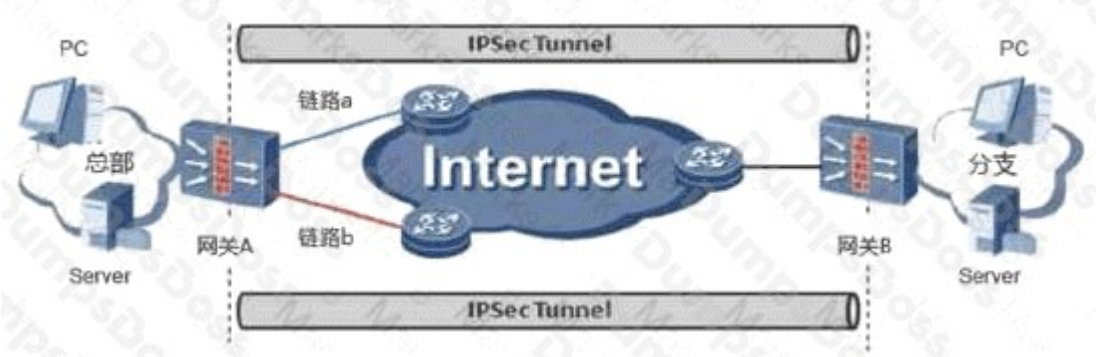
Explanation:

HRP is correct. Huawei firewalls use the High Reliability Protocol (HRP) to establish the backup relationship between devices and to synchronize relevant configuration and runtime information. HRP communication allows the active and standby devices to maintain awareness of each other and provides the data-synchronization foundation needed for service continuity after a switchover.

VRRP provides the virtual gateway and master/backup role mechanism used by many hot-standby deployments, but HRP is the Huawei firewall protocol used for backup-state communication and synchronization. Huawei firewall high-availability documentation is available through Huawei Enterprise Support.

QUESTION NO: 5

In the IPSec active/standby link backup application scenario, gateway B uses IPSec tunneling technology and gateway A to establish an IPSec VPN.



A. TRUE

B. FALSE

ANSWER: A

Explanation:

TRUE is correct. In an IPsec active/standby link-backup deployment, gateway A and gateway B act as the two IPsec peers. They establish an IPsec VPN by negotiating security associations and then protecting traffic exchanged across the selected tunnel. IPsec tunnel mode encapsulates the original IP packet inside a new IP packet, allowing private-network traffic to traverse an untrusted public network securely between the gateways. The active/standby aspect concerns path selection and failover: the preferred tunnel or route carries traffic under normal conditions, while the backup tunnel or route can take over if the preferred path becomes unavailable. This does not change the fundamental requirement that the gateways at the two ends establish the IPsec VPN tunnel and apply IPsec protection to the traffic. Huawei's IPsec documentation describes IPsec as a mechanism for establishing secure communication between IPsec peers and protecting transmitted data through authentication and encryption. See Huawei's IPsec VPN configuration documentation and the IETF's Security Architecture for the Internet Protocol.

QUESTION NO: 6

SSL VPN authentication is successful, but it can not access the Web-link resources. Which statement is correct? (Choose three answers)

A. The server is not open Web services.

B. Strategies to limit user access.

C. The equipment and network server is unreachable.

D. SSL VPN users have reached the maximum limit.

ANSWER: A B C

Explanation:

Successful SSL VPN authentication confirms that the user has passed the portal login stage, but Web-link access also depends on the availability, authorization, and reachability of the published internal web resource. “The server is not open Web services.” is therefore a valid cause: a Web-link ultimately connects the user to an HTTP or HTTPS service on the specified resource, so that service must be listening and operational. “Strategies to limit user access.” is also correct because the SSL VPN authorization configuration can control which users or user groups may use specific Web-link resources; the authenticated account must match the applicable resource-access policy. “The equipment and network server is unreachable.” is correct because the firewall or SSL VPN gateway must have network-layer connectivity to the internal server, including a valid route and permitted forwarding path. These checks reflect the normal troubleshooting sequence after login succeeds: validate the target service, confirm the user’s authorization for the resource, and verify gateway-to-server connectivity. Huawei’s security-product documentation and support resources provide SSL VPN configuration and troubleshooting guidance: Huawei Enterprise Support and Huawei HedEx Documentation.

QUESTION NO: 7

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

ANSWER: A

Explanation:

TRUE is correct. Huawei IP-Link provides end-to-end link-status detection rather than relying only on the physical state of an interface. After an IP-Link check is configured with a destination address, the device sends probe packets to that specified IP address to verify whether the upstream path remains reachable. The default failure threshold is three consecutive unsuccessful probes. When that threshold is reached, IP-Link regards the monitored path as unavailable and changes the relevant link state so that link-backup or route-selection mechanisms can move traffic away from the failed main path and onto the available backup path. This is important because a local Ethernet interface can remain physically up even when a remote device, provider path, or next-hop connectivity has failed. IP-Link therefore supplies the reachability information needed to trigger reliable active/standby switchover. Huawei’s documentation portal provides product configuration guides covering IP-Link and link-backup functions: Huawei Enterprise Documentation. Huawei’s Enterprise support portal is also the authoritative location for device-specific command references and configuration defaults: Huawei Enterprise Support.

QUESTION NO: 8

Scenario: In the virtual firewall technology which is more commonly used in business to provide a phase out of business. If the virtual firewall VFW1 leased to companies A, virtual firewall VFW2 leased enterprise B, which of the following statement is not correct?

A. The system is a virtual firewall VFW1, VFW2 respectively independent system resources among each other.

B. transparent to the user, the business between companies A and B is completely isolated from the enterprise, as with the use of a separate firewall deployment respectively.

C. firms A and B can address the overlap and use vlan divided into different virtual LANs.

D. firms A and B alone can not manage their own virtual firewall, management must be implemented by the lessor administrator.

ANSWER: D

Explanation:

“firms A and B alone can not manage their own virtual firewall, management must be implemented by the lessor administrator.” is the incorrect statement and therefore the correct selection for this question. Huawei virtual-firewall

technology creates logically separate virtual systems on one physical firewall. A key capability of this design is delegated administration: the overall device administrator can create virtual systems and assign administrators with management scope limited to a particular virtual system. Those delegated administrators can then configure and maintain the resources and security services assigned to their own virtual firewall, without receiving authority over another tenant's virtual system or over global device functions. This enables a service provider or enterprise to share hardware while preserving operational separation between departments or customers. The lessor's administrator still retains system-level control, including virtual-system creation, resource allocation, and global administration, but does not have to perform every tenant's day-to-day policy management. This administration model supports the practical use of virtual firewalls in multi-tenant deployments. Huawei's enterprise support documentation portal provides product configuration guides and feature references at Huawei Enterprise Documentation. Huawei's firewall product information, including virtualization-oriented capabilities, is available at Huawei Firewalls.

QUESTION NO: 9

The branch firewall of an enterprise is configured with NAT. As shown in the figure, USG_B is the NAT gateway. The USG_B is used to establish an IPSec VPN with the headquarters. Which parts of the USG_B need to be configured?

A. Configure the nat policy. The reference rule is to allow the source and destination of the intranet to be all ACLs.

B. Configure the IKE peer, use the name authentication, and remote-address is the outbound interface address of the headquarters.

C. Configure the nat policy. The reference rule is to protect the data flow from the enterprise intranet to the headquarters intranet in the first deny ipsec, and then permit the data flow from the intranet to the internet.

D. Configure an ipsec policy template and reference ike peer

ANSWER: B C

Explanation:

"Configure the IKE peer, use the name authentication, and remote-address is the outbound interface address of the headquarters." is required because the branch firewall must define the IKE negotiation parameters for its headquarters VPN peer. The peer configuration identifies the remote VPN gateway by its public-facing address and supplies the identity/authentication settings that allow IKE to establish the IPsec security association. This is the control-plane basis for creating the site-to-site tunnel.

"Configure the nat policy. The reference rule is to protect the data flow from the enterprise intranet to the headquarters intranet in the first deny ipsec, and then permit the data flow from the intranet to the internet." is also required. Traffic destined for the headquarters private network must match a higher-priority NAT-exemption (no-NAT) rule before the general Internet source-NAT rule. Preserving the original private source and destination addresses lets the traffic match the IPsec protected subnet selectors and be encrypted for the tunnel, while the subsequent permit/NAT rule continues to provide normal Internet access for other branch traffic. Huawei documentation on IPsec VPN configuration and NAT policy behavior is available through Huawei IPsec VPN Configuration resources and Huawei NAT policy resources.

QUESTION NO: 10

Which of the following is the role of Message5 and Message6 with the main mode IKE negotiation process?

A. Runs the DH algorithm

B. negotiate set of proposals

C. mutual authentication

D. negotiate IPsec SA

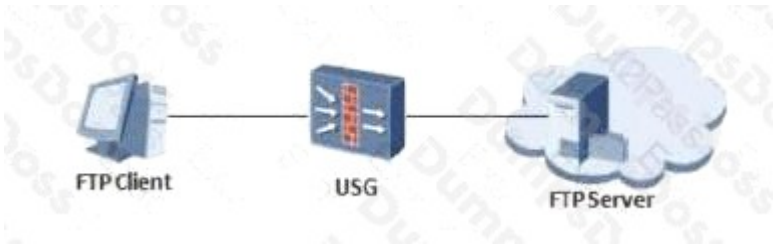
ANSWER: C

Explanation:

In IKEv1 Main Mode, Message 5 and Message 6 perform mutual authentication. By this point, the peers have already selected the IKE security policy and established the shared secret material needed to protect subsequent exchanges. Each peer sends its identity information together with authentication data, typically a hash derived from the negotiated parameters and the pre-shared key, or a digital signature when certificate-based authentication is used. The receiving peer validates that authentication data to confirm that the sender possesses the expected secret or private key and is the claimed identity. Consequently, both peers authenticate one another before relying on the resulting ISAKMP/IKE security association to negotiate IPsec protection. This exchange also protects the identities and authentication payloads because Main Mode encrypts these later messages using keys derived during the preceding key-exchange stage. The IKEv1 Main Mode message sequence and the authentication payload processing are specified in RFC 2409, The Internet Key Exchange, especially its Main Mode and authentication descriptions. Huawei security products support IKE as the key-management mechanism for establishing IPsec VPNs; see the Huawei Enterprise Support documentation portal for platform-specific IPsec and IKE configuration guidance.

QUESTION NO: 11

The FTP network diagram is as follows. The FTP server wants to use the 21000 control port to provide external FTP services. The FTP client cannot access the FTP server.



A. The FTP port mapping function is not used. Packets sent from the FTP client to the FTP server on port 21000 are treated as ordinary packets and are not recognized as FTP packets.

B. The firewall can only recognize the FTP traffic of port 21 and cannot identify the FTP traffic of port 21000.

C. The FTP ASPF function is not configured.

D. The device dropped all UDP traffic.

ANSWER: A C

Explanation:

When an FTP server listens on a nondefault control port such as 21000, the firewall must be told that this port carries FTP control traffic. Configuring FTP port mapping associates TCP port 21000 with the FTP application protocol so that the firewall's FTP application-level processing can parse FTP commands on that connection. This is necessary because FTP uses a control connection to negotiate separate, dynamically selected data connections; simply permitting a TCP service port does not provide the FTP protocol awareness needed to handle those negotiated flows.

FTP ASPF must also be enabled so the firewall can inspect the FTP control session and dynamically create temporary session entries for the associated FTP data channels. ASPF examines the FTP control information, including the address and port negotiation used by active or passive data transfer, and permits the related data traffic only for the established FTP session. Together, FTP port mapping for TCP 21000 and FTP ASPF allow a nonstandard-port FTP service to be recognized and its required data sessions to traverse the firewall securely. FTP's separate control and data connection model is defined in RFC 959; Huawei security feature documentation is available through the Huawei Enterprise Support portal.

QUESTION NO: 12

With the USG firewall, which two commands can be used to view equipment components (control board, fans, power supplies, etc.) run state and memory / CPU usage? (Choose two answers)

A. display device

B. display environment

C. display version

D. dir

ANSWER: A B

Explanation:

`display device` is used on Huawei USG firewalls to inspect device and board-related operating information. Its output provides the hardware inventory and operational state of installed components, such as processing/control boards and interface boards, and includes resource information relevant to board operation. This makes it a principal command when verifying the firewall chassis and component status.

`display environment` provides environmental and hardware-health information for the appliance. It is used to check the running condition of physical components including fan modules and power supplies, together with environmental operating data. In the context of routine USG maintenance, these two commands complement one another: the device view focuses on installed hardware and board/resource status, while the environment view confirms that supporting chassis components are operating normally. Administrators commonly use both outputs when assessing whether a firewall hardware condition or resource-utilization issue is affecting service operation. Huawei product documentation and command references are available through the Huawei Enterprise Support portal; Huawei's technical documentation portal also provides version-specific firewall command documentation.

QUESTION NO: 13

The malformed packet attack technology uses some legitimate packets to perform reconnaissance or data detection on the network. These packets are legal application types, but they are rarely used in normal networks.

A. TRUE

B. FALSE

ANSWER: B

Explanation:

FALSE is correct because the described behavior is a special-packet attack, not a malformed-packet attack. A special-packet attack uses packets that conform to legitimate application or protocol formats, but selects packet types, functions, or usage patterns that are uncommon in ordinary enterprise traffic. Attackers can use these less frequently observed yet valid packets for reconnaissance, probing, or information collection, potentially avoiding simplistic security policies that focus only on clearly invalid traffic.

In contrast, malformed-packet attacks depend on deliberately defective protocol fields, invalid lengths, fragmented-packet anomalies, or other construction errors intended to trigger implementation flaws or unstable processing in the target. The distinction is important for security operations: valid but unusual protocol behavior is evaluated through contextual inspection and anomaly detection, whereas malformed traffic is identified through protocol-compliance and packet-validity checks. Huawei security documentation describes intrusion prevention as detecting network attacks through deep packet inspection and protocol analysis, capabilities that support identifying both malformed traffic and abnormal use of valid protocols. See Huawei's HiSecEngine IPS Configuration Guide and the Huawei Firewall Product Documentation.

QUESTION NO: 14

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

ANSWER: B

Explanation:

FALSE is correct because malformed-packet attacks are characterized by traffic that violates expected protocol, header, field-length, encoding, sequencing, or application-format rules. The distinguishing feature is not that the packets are legitimate for the application type, but that one or more packet elements are deliberately invalid, abnormal, or inconsistent with the relevant protocol specification. Attackers can send such traffic during reconnaissance, evasion attempts, or exploit delivery to observe how network devices, hosts, and security controls parse and handle unexpected input. Security devices therefore inspect packet structure and protocol conformance, not merely whether traffic appears to be associated with a known application. Huawei security-network design practice uses intrusion prevention and protocol-aware inspection to identify abnormal traffic and enforce correct protocol behavior. This treatment is also consistent with the IETF description of malformed-packet vulnerabilities and attacks, which arise when implementations process invalid or unexpected protocol data. See RFC 4732: Internet Denial-of-Service Considerations and Huawei's firewall product documentation.

QUESTION NO: 15

USG5000A has an IPSEC connection to USG5000B and the "display ike sa" command was performed on USG5000A:

```
[USG A] display ike sa
conn-id    peer        flag     phase    doi
-------------------------------------------------
1          202.38.0.2  RD|ST    1        IPSEC
2          202.38.0.2  RD|ST    2        IPSEC
```

Based on the output shown, which of the following is correct?

A. USG5000A Firewall is a secure channel initiator IKE negotiation

B. USG5000B is the initiator of IKE negotiation of safe passage

C. The SA has been successfully established between the firewalls

D. The SA has not been established between the firewalls successfully.

ANSWER: A C

Explanation:

The correct statements are *USG5000A Firewall is a secure channel initiator IKE negotiation* and *The SA has been successfully established between the firewalls*. In Huawei `display ike sa` output, the local IKE role identifies whether the device that produced the output initiated the IKE negotiation. The displayed initiator role therefore shows that USG5000A started establishment of this IKE security association. IKE uses the authenticated exchange to establish an IKE SA, which protects subsequent negotiation and management traffic for the IPsec tunnel.

The established state in the output confirms that IKE negotiation completed successfully and that a usable IKE SA exists between the peers. An IKE SA is the control-plane security association required for negotiating IPsec protection; it represents a successfully authenticated, protected relationship between the firewall peers. This interpretation is consistent with the IKEv2 specification, which defines an IKE SA as the security association created to protect IKE exchanges, and with Huawei's firewall/IPsec product documentation. See RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2) and Huawei Firewall product documentation.

QUESTION NO: 16

USG dual-machine hot standby must meet certain conditions and can be used below. What are the following statements correct?

A. major and backup equipment must have the same product model

B. The software version of the active and standby devices must be the same.

C. The interface IP of the active and standby devices must be the same.

D. The primary device must be configured, and the standby device does not require any configuration.

ANSWER: A

Explanation:

major and backup equipment must have the same product model is a fundamental deployment requirement for Huawei USG active/standby hot backup. The two firewalls operate as a coordinated high-availability pair: they synchronize configuration and, where applicable, service-session and status information so that the standby firewall can assume forwarding responsibilities when the active firewall fails. Matching hardware models ensures compatible interface characteristics, processing capabilities, feature behavior, and HA synchronization mechanisms. This consistency is important for predictable failover and for avoiding incompatibilities between the devices' forwarding and service-processing resources. Before deploying hot standby, administrators should also follow the relevant product documentation for compatible software, licensing, interface connectivity, heartbeat links, and configuration synchronization procedures. Huawei's support documentation provides product-specific configuration guides and compatibility information through its enterprise support portal: Huawei Enterprise Documentation. Huawei's firewall product information and technical resources are also available at Huawei Enterprise Firewalls.

QUESTION NO: 17

What are the correct statements about the IP address scanning attack and prevention principles?

A. IP address scanning attack is an attacker that uses an ICMP packet (such as ping and tracert) to detect the target address.

B. IP address scanning attack is an attack method used by an attacker to detect a target address by using TCP/UDP packets.

C. IP address scanning attack defense detects the rate of address scanning behavior of a host. If the rate exceeds the threshold, it is blacklisted.

D. If the USG starts the blacklist function and is associated with IP address scanning attack prevention, when the scanning rate of a certain source exceeds the set threshold, the excess threshold will be discarded, and the packets sent by this source will be less than the subsequent time. Threshold, can also be forwarded

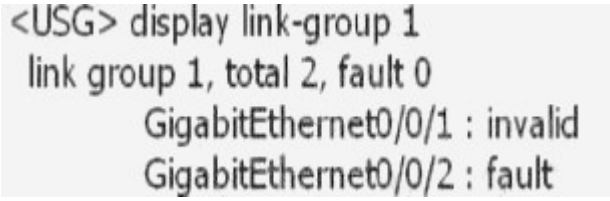
ANSWER: A B C

Explanation:

IP address scanning is reconnaissance in which an attacker probes a range of addresses to identify active hosts and potentially reachable services. "IP address scanning attack is an attacker that uses an ICMP packet (such as ping and tracert) to detect the target address" is correct because ICMP echo requests are commonly used to determine whether hosts respond, while traceroute-style probing helps reveal network-path information. ICMP behavior is standardized in RFC 792. "IP address scanning attack is an attack method used by an attacker to detect a target address by using TCP/UDP packets" is also correct: TCP and UDP probes can identify responsive addresses and support later service discovery. TCP's basic connection behavior is specified in RFC 793. On Huawei USG firewalls, address-scan defense is rate-based: the firewall tracks a source host's attempts to contact multiple destination addresses and compares that behavior with the configured threshold. "IP address scanning attack defense detects the rate of address scanning behavior of a host. If the rate exceeds the threshold, it is blacklisted" correctly describes the protection principle when the blacklist function is enabled and associated with scan-attack defense. Blacklisting provides a time-bound source-address response to excessive scanning activity, reducing continued reconnaissance traffic from that source.

QUESTION NO: 18

After the link-group is configured on the device, use the display link-group 1 command to obtain the following information. What information can I get?



A. GigabitEthernet 0/0/2 interface has failed.

B. GigabitEthernet 0/0/1 has failed.

C. GigabitEthernet 0/0/2 is forcibly converted to fault state because other interfaces in the group are faulty.

D. GigabitEthernet 0/0/1 is forcibly converted to fault state because other interfaces in the group are faulty.

ANSWER: B C

Explanation:

The output identifies the operational state of each member interface in link-group 1. GigabitEthernet 0/0/1 is shown as being in a fault/down condition, which means that the interface itself has failed the link-group status check. Accordingly, “GigabitEthernet 0/0/1 has failed.” is valid.

The same output shows GigabitEthernet 0/0/2 in a forced fault state rather than indicating an independent physical failure. Link-group protection associates the member interfaces and can administratively force another member into the fault state when the group’s fault-processing condition is met. Therefore, “GigabitEthernet 0/0/2 is forcibly converted to fault state because other interfaces in the group are faulty.” accurately describes the reported state. This distinction is important during troubleshooting: the first interface is the detected failed member, while the second interface has been placed into its state by link-group logic to preserve the intended protection behavior. Huawei documentation for link-group configuration and interface status interpretation is available in the Huawei enterprise documentation and the Huawei command reference for link-group.

QUESTION NO: 19

What is the correct statement about the binding of local users to VPN instances?

A. local user can be bound to a VPN instance by using the local-user user-name vpn-instance vpn-instance-name command.

B. By default, the binding between a local user and a VPN instance is implemented.

C. . After a local user is bound to a VPN instance, the local user can manage the entire firewall.

D. Local users cannot be bound to VPN instances.

ANSWER: A

Explanation:

The statement “local user can be bound to a VPN instance by using the local-user user-name vpn-instance vpn-instance-name command.” is correct. On Huawei firewalls, local-user configuration is performed in the AAA view, and the `local-user` command can associate an existing local account with a specified VPN instance. This association gives the account an identity within the designated VPN-instance context, allowing authentication and authorization to be applied according to that instance’s isolated routing and service environment. The username is followed by the `vpn-instance` keyword and the target VPN-instance name, so the administrator must first know the intended instance and configure the local user in the appropriate AAA context. Binding is an explicit administrative configuration; it is not inferred merely because either a local user or a VPN instance exists. This capability is useful in multi-tenant or logically separated firewall deployments, where administrators need user access and related services to remain scoped to a particular VPN instance. Huawei’s enterprise support portal provides product documentation and command references for firewall AAA and VPN-instance configuration: Huawei Enterprise Support. Huawei’s documentation search service is also available at Huawei Info-Finder.

QUESTION NO: 20

Which of the following configurations is mandatory when the IKE peer needs to be referenced to the IPSec policy template in the divquarters-branch-based IPSec VPN network (pre-shared key + traversal NAT)?

A. ipsec proposal

B. exchang-mode aggressive

C. pre-shared-key

D. remote-address

ANSWER: A C

Explanation:

ipsec proposal is required because an IPSec policy template must reference an IPSec proposal that defines the Phase 2/IPSec security parameters used to protect matching traffic. The proposal supplies the ESP or AH protection suite and associated encryption, authentication, and encapsulation settings; without it, the policy template has no IPSec transform set to apply to negotiated protected flows. **pre-shared-key** is also required for the stated authentication model. The configured IKE peer uses the shared secret during IKE authentication to validate the remote peer and establish IKE security associations before IPSec security associations can be created. NAT traversal changes how ESP traffic is carried across a NAT device, commonly by using UDP encapsulation, but it does not replace the need for a valid IPSec proposal or peer authentication credentials. These two configuration elements therefore provide the required Phase 2 protection definition and the required IKE authentication material for a pre-shared-key deployment. Huawei IPSec configuration concepts are documented in the Huawei IPsec Configuration Guide; the underlying IPsec security-architecture requirements are also described in RFC 4301.

QUESTION NO: 21

Which of the following statements about TCP SYN Flood attack defense are correct? (Choose three answers)

A. TCP proxy can validate completion of the client-side three-way handshake.

B. Source-address validation can help identify spoofed-source traffic.

C. Connection-rate limiting can reduce the impact of excessive SYN packets.

D. Increasing the TCP payload size prevents incomplete handshakes.

ANSWER: A B C

Explanation:

A SYN Flood attack attempts to consume connection resources by sending a large number of TCP SYN packets and failing to complete the three-way handshake. A firewall or protection device can use a TCP proxy mechanism to complete and validate the client-side handshake before allocating corresponding server-side connection resources. This reduces the effect of spoofed or incomplete connection attempts on the protected server.

Source-address validation and anti-spoofing controls are also useful because many SYN Flood attacks use forged source addresses. Rate limiting or connection-rate thresholds can limit the number of new connection attempts accepted from a source or toward a protected service. Increasing the TCP payload size is unrelated to validating the handshake and does not defend against a SYN Flood. See RFC 9293: Transmission Control Protocol and RFC 4987: TCP SYN Flooding Attacks and Common Mitigations.

QUESTION NO: 22

About VRRP packets, which of the following statements is correct? (Choose two answers)

A. VRRP packets using TCP

B. VRRP packets using UDP

C. VRRP packet destination address is 224.0.0.18

D. VRRP packet TTL value is 255

ANSWER: C D

Explanation:

“VRRP packet destination address is 224.0.0.18” is correct for VRRP operating over IPv4. VRRP routers send advertisements to the link-local multicast group 224.0.0.18, which is reserved specifically for VRRP. Because this is a link-local multicast destination, the advertisements are intended to remain within the local Layer 2 broadcast domain and allow routers participating in the same virtual-router group to monitor the master router’s status.

“VRRP packet TTL value is 255” is also correct. VRRP advertisements are IP packets using IP protocol number 112, and their IPv4 TTL is required to be 255. A receiving VRRP router validates this value, helping ensure that an advertisement originated on the directly connected local link rather than having been forwarded by a router. This supports the protocol’s local-segment scope and provides a basic protection against advertisements received from outside the intended VRRP network segment. Huawei VRRP implementations follow these standard VRRP packet characteristics when forming and validating IPv4 VRRP advertisements. The protocol requirements are specified in RFC 3768; the current VRRP specification is available in RFC 5798.

QUESTION NO: 23

In a dual-system hot standby environment, if the path of the packet back and forth is inconsistent, which of the following conditions may result in packet loss?

A. does not enable session fast synchronization

B. Heartbeat bandwidth is insufficient

C. turned off the status monitoring function

D. specifies the wrong heartbeat port

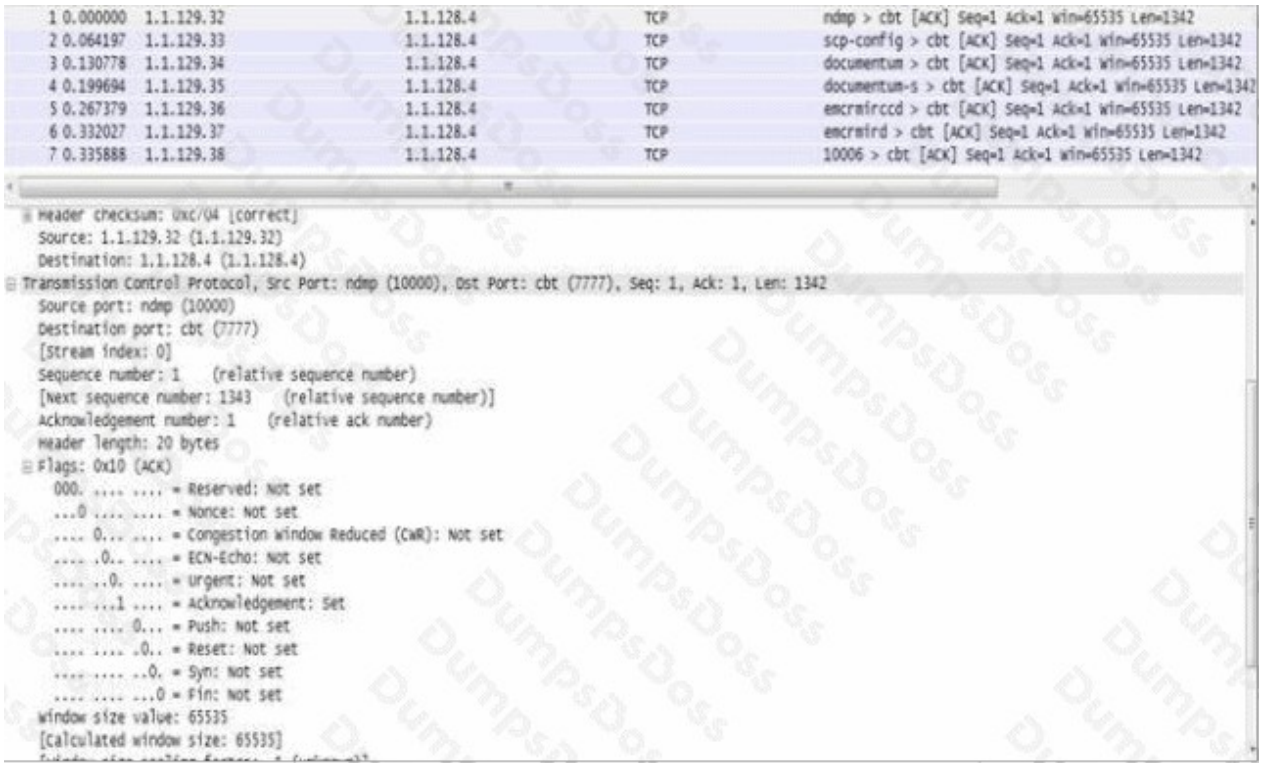
ANSWER: A B D

Explanation:

In an asymmetric forwarding scenario, the forward and return packets of a connection can be processed by different firewalls. Both devices therefore need an up-to-date session entry so that either device can recognize the traffic as belonging to an established flow. When *does not enable session fast synchronization* applies, session-state information may not reach the peer quickly enough for traffic arriving on the alternate path, and the peer can discard packets for which it has no matching state. *Heartbeat bandwidth is insufficient* can similarly prevent timely, reliable delivery of HRP control and session-synchronization information, particularly when connection creation rates are high. Configuring a device such that it *specifies the wrong heartbeat port* can prevent the intended heartbeat/session synchronization channel from operating correctly, leaving the peer without the session information required to forward asymmetric traffic. Huawei hot-standby deployments rely on the HRP connection for device status exchange and session backup; the heartbeat path must be correctly configured and appropriately sized. See Huawei’s enterprise product documentation for firewall HRP/session-backup configuration guidance and the stateful-flow behavior described in RFC 4787.

QUESTION NO: 24

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

ANSWER: C

Explanation:

ACK-Flood is correct because the captured traffic consists of a high volume of TCP segments with the ACK control flag set, directed at the victim. A TCP ACK flood is a denial-of-service technique in which an attacker sends numerous ACK packets, often using spoofed source addresses or varying flow information, to consume the target's packet-processing capacity, state-table resources, CPU capacity, or available bandwidth. The packets do not need to represent valid, established application sessions to impose processing work on the receiving host or an intervening stateful security device.

In TCP, the ACK flag indicates that the acknowledgment-number field is significant and is normally used to acknowledge received data during an established connection. This protocol behavior is defined in the TCP specification, which makes ACK-bearing traffic identifiable in a packet capture by inspecting the TCP flags. When the observable pattern is an abnormal, sustained stream of such packets rather than ordinary bidirectional session traffic, it supports identification as an ACK flood. See the TCP control-flag definition in RFC 9293: Transmission Control Protocol and the denial-of-service overview from CISA.

QUESTION NO: 25

Which of the statement is correct about the Eth-trunk function? (Choose three answers)

A. It improves communication bandwidth of the link

B. It improves data security

C. Traffic load balancing

D. It improves the reliability of the link

ANSWER: A C D

Explanation:

Eth-Trunk is Huawei's Ethernet link-aggregation function: it logically bundles multiple physical Ethernet interfaces into one aggregate interface. This aggregation increases the available communication bandwidth because member-link capacity is combined for traffic carried by the trunk. For example, several links of equal rate can provide greater aggregate forwarding capacity than a single physical link, subject to the traffic-distribution algorithm and flow characteristics.

Traffic load balancing is also a core Eth-Trunk function. The device selects member links using a load-balancing hash, commonly derived from packet fields such as source and destination MAC addresses, IP addresses, or transport-layer ports. This distributes eligible traffic flows across available physical members while presenting a single logical link to upper-layer protocols.

Eth-Trunk improves link reliability through redundancy. If one active member link fails, traffic can continue through the remaining active member links without requiring the entire logical connection to be removed. Link Aggregation Control Protocol can additionally negotiate and monitor aggregation dynamically. Huawei describes Eth-Trunk aggregation, load balancing, and link backup behavior in its Ethernet Link Aggregation documentation and Eth-Trunk configuration documentation.

QUESTION NO: 26

In USG equipment, which statement is correct on current-configuration files and saved-configuration profile? (Choose two answers)

A. After an administrator configures a feature on a USG device, the device immediately modifies the saved configuration.

B. The `display saved-configuration` command displays the configuration file that the device will load at the next startup.

C. When the `save` command is executed, the device copies the current configuration to the saved configuration.

D. When the `save` command is executed, current-configuration commands take effect.

ANSWER: B C

Explanation:

On a Huawei USG, the running configuration (current configuration) consists of the commands currently active in memory. The saved configuration is the configuration file retained in storage for use when the device next starts. Therefore, the `display saved-configuration` command is used to view the saved configuration file that is designated for the next startup, allowing an administrator to confirm what persistent configuration will be loaded. The `save` command copies the active current configuration into the saved configuration file. This is the essential step for making configuration changes survive a reboot or power cycle. In normal operational practice, administrators configure and verify features in the current configuration, then execute `save` after confirming the intended settings. Huawei documentation describes configuration-file management and the relationship between the current configuration, saved configuration, and startup configuration in its enterprise support resources. See the Huawei Enterprise Support portal and the Huawei technical documentation portal for USG command references and configuration-management guides.

QUESTION NO: 27

Two USG firewalls establish an IPSec VPN through the Site to Site mode. When viewing the status of a USG A, the following is displayed: display ipsec statistics the security packet statistics: input/output security paskets: 40 input/output security bytes: 400/0 input /output dropped security packets: 0/0 By status information, what information can be obtained correctly?

A. USG A has already encrypted 4 packets, and USG A has decrypted packets.

B. USG A has decrypted the data packet is 4, USG A has encrypted data packet is 0

C. Site A device on the intranet, there is no route, so the protection data may not be sent to USG A.

D. IPSec tunnel is not established

ANSWER: B C

Explanation:

The displayed IPsec security-packet counters indicate that USG A has received four protected packets and transmitted no protected packets. In Huawei IPsec statistics, the input security-packet counter records packets entering the IPsec processing path from the tunnel side; after successful security processing, these are the packets USG A decrypts. The corresponding 400 input bytes also aligns with four received protected packets, while the zero output packet and byte counters show that no traffic has been encrypted and sent through the IPsec tunnel by USG A during this statistics interval. Therefore, “USG A has decrypted the data packet is 4, USG A has encrypted data packet is 0” is supported directly by the counters. “Site A device on the intranet, there is no route, so the protection data may not be sent to USG A” is also a valid operational inference: if protected traffic from the local private network is not routed to USG A, no outbound interesting traffic reaches the firewall for IPsec encapsulation, so its output IPsec counters remain zero. Huawei documents IPsec traffic processing and troubleshooting counters in its USG configuration documentation: Huawei USG Configuration Guide and Huawei Firewall Product Documentation.

QUESTION NO: 28

Which is the correct packet encapsulation order for L2TP over IPSec?

A. The order from the first package to the post package is PPP-- > UDP-- > L2TP-- > IPSec

B. The order from the first package to the back package is PPP-- > L2TP-- > UDP-- > IPSec

C. The order of C from pre-package to post-encapsulation is IPSec -- > L2TP-- > UDP-- > PPP

D. The order of D from pre-package to post-encapsulation is IPSec -- > PPP -- > L2TP-- > UDP

ANSWER: B

Explanation:

The correct encapsulation sequence is **PPP → L2TP → UDP → IPSec**. L2TP is designed to carry PPP frames: the original user traffic is first placed into a PPP frame, and L2TP adds its tunnel header around that PPP payload. L2TP is then transported over UDP, conventionally using UDP port 1701, so a UDP header is added outside the L2TP packet. In an L2TP/IPSec VPN, IPSec protects that already formed L2TP-over-UDP traffic. IPSec therefore provides confidentiality, integrity protection, and peer authentication for the L2TP traffic while PPP remains the innermost encapsulation layer. In practical packet construction, normal IP headers also exist for UDP transport and for IPSec tunneling, but the answer lists only the four relevant protocol layers. This model is the standard L2TP/IPSec architecture: L2TP performs PPP tunneling, and IPSec secures the L2TP control and data packets. See RFC 3193, Securing L2TP using IPsec and RFC 2661, Layer Two Tunneling Protocol.

QUESTION NO: 29

In the DDoS attack defense, if the service learning function is used to find that there is no service or traffic of a certain service in normal traffic, you can use the blocking or traffic limiting method to defend against attacks on the Anti-DDoS device. .

A. TRUE

B. FALSE

ANSWER: A

Explanation:

TRUE is correct. Service learning establishes a baseline of legitimate service behavior by examining normal traffic, including the services and traffic characteristics that are expected to be present. If a particular service is not observed during normal operation, traffic directed at that service can be treated as anomalous when an attack occurs. This is especially useful when attackers send high volumes of packets toward unused ports or services in an effort to consume bandwidth, session resources, or device processing capacity.

On an Anti-DDoS device, the appropriate mitigation action for traffic that does not match the learned service baseline can be blocking or traffic limiting. Blocking prevents the unwanted traffic from reaching protected resources, while traffic limiting constrains its rate to reduce resource consumption while maintaining a controlled defense posture. Using the learned baseline therefore enables the device to apply protection based on the actual services exposed by the protected network rather than relying solely on static assumptions. This approach aligns with the general Anti-DDoS principle of detecting abnormal traffic against normal traffic characteristics and then applying a mitigation policy. Huawei's Anti-DDoS documentation describes protection policies and traffic-cleaning mechanisms at Huawei Cloud Anti-DDoS documentation; Huawei also provides DDoS-mitigation product information at Huawei DDoS Mitigation.

QUESTION NO: 30

In the IDC room, a USG firewall can be used to divide into several virtual firewalls, and then the root firewall administrator generates a virtual firewall administrator to manage each virtual firewall.

A. TRUE

B. FALSE

ANSWER: A

Explanation:

TRUE is correct. Huawei USG firewalls support virtualization through virtual systems (VSYSs), allowing one physical firewall to be logically partitioned into multiple independent virtual firewalls. This is particularly suitable for an IDC, where different tenants, departments, or service environments require separated security-policy administration while sharing the same physical device. Each virtual system has its own security zones, interfaces or interface resources, security policies, routing-related configuration, and administrator permissions within the scope assigned to that virtual system. The administrator of the root system has the highest administrative scope and is responsible for creating and managing virtual systems. The root administrator can also create virtual-system administrators and assign each administrator permission to manage a specified virtual system. This delegated-administration model enables operational separation: the root administrator retains control of global resources and tenancy boundaries, while each virtual firewall administrator manages the security configuration for the corresponding tenant or service domain. Huawei's documentation describes virtual systems as a mechanism for dividing a firewall into multiple logically independent security entities and supports administrators with different management scopes. See Huawei's USG firewall product documentation and the Huawei virtual system overview.

QUESTION NO: 31

Based on the following information analysis on the firewall, which of the following options are correct?

A. The first packet of this data flow enters from the Trust zone interface and is sent from the Untrust zone interface.

B. This data stream has been NAT translated

C. uses NAPT conversion technology

D. firewall has virtual firewall function enabled

ANSWER: A B C

Explanation:

The correct conclusions are that the initiating packet travels from a Trust-zone interface toward an Untrust-zone interface, that the session has undergone NAT processing, and that the address translation is NAPT. A stateful Huawei firewall creates a session when it receives the first packet and records the packet direction according to the ingress and egress security

zones. Therefore, a session whose initiation is Trust to Untrust represents an inside host initiating traffic toward an external network. NAT session information indicates that translation has been applied to the flow. Where the translated session distinguishes transport-layer ports in addition to addresses, the firewall is performing Network Address and Port Translation (NAPT), allowing multiple internal client flows to share a public address while retaining separate sessions through port mappings. This is the common source-NAT behavior for outbound enterprise access. Huawei firewall products provide stateful security-zone policy control and NAT capabilities; see the Huawei Firewall support portal. The general NAPT model, including address and transport-identifier translation, is defined in RFC 3022.

QUESTION NO: 32

Three physical interfaces have been added to the link-group group. When any one of the interfaces fails, what are the following descriptions correct?

A. If any interface in group A fails, the system sets the status of other interfaces in the group to down.

B. Any interface in group B fails, and the status of other interfaces in the group does not change.

C. After the interfaces in the group are restored to normal, the interfaces in the entire group are reset to up.

D. After all the interfaces in the group are restored, the interfaces in the entire group are reset to up.

ANSWER: A D

Explanation:

In Huawei link-group operation, member interfaces are treated as a linked availability unit rather than as independent forwarding links. The group provides fault linkage: when any physical member interface detects a failure and transitions down, the device drives the remaining interfaces in that link group down as well. This ensures that traffic is not forwarded through a partially available group when the service design requires all associated paths to be operational together. Therefore, “If any interface in group A fails, the system sets the status of other interfaces in the group to down.” correctly describes the link-group failure behavior.

Recovery is also coordinated at the group level. The group does not return its interfaces to the operational up state merely because one failed member has recovered while another member may still be unavailable. Only after all member interfaces have been restored does the device reset the interfaces throughout the link group to up. Thus, “After all the interfaces in the group are restored, the interfaces in the entire group are reset to up.” correctly states the recovery condition. This coordinated down/up mechanism supports consistent service-state handling for associated physical links. Huawei documentation is available through the Huawei Enterprise Technical Documentation portal and the Huawei Product Documentation portal.

QUESTION NO: 33

To establish IPsec VPN Security, ACL rules should mirror each other. This is the general requirement at both ends in Huawei firewall environment.

A. TRUE

B. FALSE

ANSWER: A

Explanation:

TRUE is correct. For a policy-based IPsec VPN on Huawei firewalls, the traffic selector defined by the protected-subnet ACL must describe the same traffic flow from each peer’s own perspective. Therefore, when one endpoint’s ACL matches packets sourced from its local protected network and destined for the remote protected network, the peer endpoint needs the reciprocal match: its local protected network as source and the first endpoint’s protected network as destination. These corresponding entries are commonly described as mirrored ACL rules.

This reciprocal definition ensures that packets selected for encryption at one gateway are recognized as protected VPN traffic when they arrive at the other gateway, and that return traffic is also selected for the same IPsec security association. The address direction is reversed between the two devices, while protocol and relevant port criteria must remain consistent. Correctly mirrored selectors are particularly important when negotiating traffic-based IPsec policies and when multiple protected subnet pairs are configured. Huawei's IPsec configuration guidance describes defining the protected traffic with ACLs and applying matching IPsec policies at the communicating endpoints. See the Huawei enterprise documentation portal and Huawei's Enterprise Support documentation and configuration resources for IPsec VPN configuration guidance.

QUESTION NO: 34

In the firewall DDoS attack defense technology, the data packet of the session table is not defended. If the data packet of the session has been established, it is directly released.

A. TRUE

B. FALSE

ANSWER: A

Explanation:

TRUE is correct. Huawei firewalls use session-based stateful processing: after the first packet creates a valid session entry, subsequent packets that match that session are handled through the established-session forwarding path. DDoS defense inspection is principally applied when traffic is attempting to establish new connections or create new session state, because floods such as SYN floods and UDP/ICMP floods can consume session, CPU, and bandwidth resources by generating large volumes of new flows. Packets that already match an existing session are therefore normally forwarded directly rather than being repeatedly subjected to the new-session DDoS defense checks. This design improves forwarding performance while retaining stateful control over connection establishment. The statement accurately describes this session-table-based behavior: packets belonging to an established session are released directly. Huawei's firewall portfolio and documentation describe its stateful inspection and attack-defense capabilities; see the Huawei firewall product information and the Huawei Enterprise Support documentation portal.

QUESTION NO: 35

USG remote capture device configuration functions in a way that the device can grab packets downloaded to the device. Users can download to a local service via FTP and use Firewall Packetyzer to analyze packet.

A. TRUE

B. FALSE

ANSWER: A

Explanation:

TRUE is correct. USG firewalls provide packet-capture capabilities to help administrators diagnose traffic-forwarding, policy, protocol, and connectivity issues. In a remote packet-capture workflow, the firewall captures packets that reach or traverse the device according to the configured capture conditions, such as an interface, protocol, source or destination address, and port. The captured traffic is saved as a capture file on the firewall, enabling analysis without requiring a packet sniffer to be physically connected to the monitored link.

After the capture is completed, an administrator can use FTP to transfer the capture file from the firewall to a local host or FTP service for offline inspection. Huawei's Firewall Packet Analyzer/Packetyzer can then open and analyze the captured packet data, allowing the administrator to inspect packet headers, sessions, and communication behavior. This workflow is particularly useful when a problem occurs at a remote site and direct access to the network segment is impractical. Huawei identifies packet capture as a core troubleshooting capability of its next-generation firewall products; see the Huawei Next-Generation Firewall product page and the Huawei Enterprise Support documentation portal for product documentation and configuration resources.

QUESTION NO: 36

An IPsec VPN connection established by two USG firewalls in NAT traversal mode fail to see any information from the “display ike sa” command. Neither session information nor UDP port 500 information is displayed. What are possible reasons for this? (Choose two answers)

A. public network unreachable.

B. middle device blocking UDP 500 port.

C. middle device blocking UDP 4500 port.

D. middle device blocking ESP packets.

ANSWER: A B

Explanation:

public network unreachable. and **middle device blocking UDP 500 port.** are the applicable causes because IKE negotiation must first be able to reach the remote peer over the public network and begin communication using UDP port 500. An IKE security association cannot be created until the peers exchange the initial IKE messages. Therefore, if routing, Internet connectivity, addressing, or return-path reachability to the peer’s public address is unavailable, the firewall has no remote IKE exchange from which to build or display an IKE SA.

Likewise, filtering UDP port 500 at an intervening firewall, NAT device, ACL, or service-provider boundary prevents the initial IKE packets from reaching the peer. NAT traversal does not eliminate this initial requirement: NAT detection occurs during the initial IKE exchange on UDP 500. After NAT is detected, IKE and protected traffic can use UDP 4500, but that transition depends on successful initial UDP 500 communication. Consequently, the absence of both session information and UDP 500-related activity directly points to a public-path reachability issue or UDP 500 filtering. This behavior follows the IKE protocol’s initial exchange requirements and the IPsec NAT-traversal procedure described in RFC 7296 and RFC 3947.

QUESTION NO: 37

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

A. ESP

B. AH

C. L2TP

D. GRE

ANSWER: B C D

Explanation:

AH, **L2TP**, and **GRE** do not themselves provide payload encryption. IPsec Authentication Header (AH) protects packets through integrity checking and data-origin authentication, with optional anti-replay protection, but its defined security services do not include confidentiality. Therefore, AH can validate that protected traffic has not been modified and came from an authenticated peer, while the packet contents remain readable to an observer. The IPsec AH specification is available in RFC 4302.

L2TP is a Layer 2 tunneling protocol: it carries PPP frames through an IP network and provides tunneling/session functionality rather than cryptographic confidentiality. In secure deployments, it is commonly paired with IPsec, whose ESP protection supplies encryption. Likewise, GRE encapsulates traffic so that routed protocols or multicast traffic can traverse an IP network, but its base header and encapsulation format contain no encryption mechanism. Secure GRE designs therefore commonly apply IPsec protection to the GRE packets. The GRE protocol definition in RFC 2784 describes its encapsulation behavior, while RFC 3193 documents using L2TP with IPsec for secure remote access.

QUESTION NO: 38

The load balancing function is configured on the USG firewall for three FTP servers. The IP addresses and weights of the three physical servers are 10.1.13/24 (weight 16); 10.1.1.4/24 (weight 32); 10.1.1.5 /24 (weight 16), and the virtual server address is 202.152.26.123/24. A PC with the host address of 202.152.26.3/24 initiates access to the FTP server. Run the display firewall session table command on the firewall to check the configuration. Which of the following conditions indicates that the load balancing function is successfully implemented?

A. < USG > display firewall session table Current total sessions: 1 ftp VPN: public-- > public 202.152.26.3:3327-- > 10.1.1.4:21

B. < USG > display firewall session table Current total sessions:3 ftp VPN: 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 table Current total sessions: 1 ftp VPN: 202.152.26.3:3327-- > 202.152.26.123:21

D. < USG > display firewall session table Current total sessions: 3 ftp VPN: ftp VPN: 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-- > 10.1.1.4:21 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

ANSWER: B

Explanation:

`< USG > display firewall session table Current total sessions:3 ftp VPN: 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]` confirms successful load balancing because each session retains the client-facing virtual-server destination, `202.152.26.123:21`, while the address in square brackets identifies the physical FTP server selected as the actual destination. This is the expected session-table representation when the firewall accepts traffic for a virtual IP and performs server selection plus destination translation to a real server. The entries demonstrate that the virtual service can be mapped to the configured real-server pool, including the three listed backend addresses. The weights influence the relative selection frequency over an appropriate number of new connections; they do not remove the virtual-server-to-real-server mapping shown in each established session. FTP is stateful and its control connection is tracked by the firewall, so verification through the firewall session table is an appropriate method for confirming the forwarding decision. This behavior aligns with the stateful NAT/session model described in RFC 5382 and with Huawei's enterprise firewall product documentation at Huawei Firewalls.

QUESTION NO: 39

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

ANSWER: A B C

Explanation:

In a bypass deployment, Huawei’s abnormal-traffic-cleaning solution redirects selected service traffic to a cleaning device and then returns cleaned traffic to the original forwarding path. **Dynamic routing drainage** is supported where routing protocols, commonly BGP in larger networks, advertise or withdraw routes so traffic is redirected automatically when attack conditions trigger cleaning. This approach is useful when the network requires rapid, automated steering and recovery.

Static routing drainage is also supported. Administrators can configure explicit routes toward the cleaning device or diversion path, making it appropriate for smaller or stable topologies in which the diversion path is known in advance. **Static routing strategy drainage** refers to policy-based steering: traffic matching configured characteristics, such as source or destination addresses, protocol, or service port, is redirected through the cleaning path while other traffic retains its normal route. This provides granular control in asymmetric or mixed-service environments.

These three mechanisms provide the routing and policy controls needed to send attack traffic through the bypass cleaning path without placing the cleaner inline. Huawei's Anti-DDoS portfolio and security-solution material describe traffic detection, diversion, cleaning, and return as core parts of DDoS mitigation architecture. See Huawei Anti-DDoS and Huawei Enterprise Network Security Solutions.

QUESTION NO: 40

When there are a large number of BFD sessions in a system, what mode can be used to prevent BFD detection when the cost of sending BFD control packets periodically affects the normal operation of the system?

A. sync mode

B. detection mode

C. asynchronous mode

D. demand mode

ANSWER: D

Explanation:

demand mode is the appropriate BFD operating mode when maintaining periodic BFD control packets for many sessions creates excessive device overhead. In normal asynchronous operation, each endpoint periodically transmits BFD control packets, so packet generation, processing, and timer handling scale with the number of sessions. Demand mode is designed to reduce that steady-state control traffic after the session has been established and connectivity is otherwise being verified. Rather than requiring continuous periodic BFD control-packet transmission in the normal state, it allows failure detection to rely on another mechanism that confirms forwarding continuity; BFD control packets can still be exchanged when needed, such as for state changes or verification. This substantially lowers the ongoing processing burden on a system carrying a large number of BFD sessions while retaining BFD session functionality. The term "query mode" in the original option is not the standardized BFD name; the applicable formal term is demand mode. RFC 5880 defines demand mode and explains that it may be used when the system can reliably determine that the connection is operational without continuously receiving BFD control packets. See RFC 5880, BFD Demand Mode and Huawei's BFD configuration documentation.

QUESTION NO: 41

Load balancing has the following configuration:

[USG] slb enable

[USG] slb

[USG-slb] rserver 1 rip 10.1.1.3 weight 32

[USG-slb] rserver 2 rip 10.1.1.4 weight 16

[USG-slb] rserver 3 rip 10.1.1.5 weight 32

[USG-slb] group test

[USG-slb-group-test] metric srchash

[USG-slb-group-test] add rserver 1

[USG-slb-group-test] add rserver 2

[USG-slb-group-test] add rserver 3

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

A. Load balancing algorithm for the polling algorithm.

B. The configuration is complete load balancing configuration.

C. Value judgments based on weight which server data stream should flow, the smaller the weight value, the corresponding real server processing capacity should be more weak.

D. weight is the weight of a real server weight.

ANSWER: C D

Explanation:

The correct statements are “Value judgments based on weight which server data stream should flow, the smaller the weight value, the corresponding real server processing capacity should be more weak.” and “weight is the weight of a real server weight.” In Huawei SLB configuration, `weight` is an attribute of each real server. It represents the relative service-processing capability assigned to that server by the administrator. A server configured with weight 32 is intended to have a greater relative capacity than a server configured with weight 16; therefore, the lower-weight server is treated as having comparatively weaker processing capability. In this configuration, real servers 10.1.1.3 and 10.1.1.5 each have a weight of 32, while 10.1.1.4 has weight 16. The configured values consequently express a 2:1:2 relative capacity relationship. The server group uses the source-address hash metric, which establishes a deterministic selection basis from client source addresses; the real-server weight remains the configured parameter that describes each member’s relative load-handling capability. Huawei’s enterprise documentation portal provides product configuration guidance for USG security gateways and related service features at Huawei Enterprise Support Documentation. Huawei’s technical knowledge resources are also available through the Huawei Enterprise Encyclopedia.

QUESTION NO: 42

Which of the following is the primary purpose of a firewall blacklist?

A. To block traffic from specified or dynamically identified malicious sources

B. To select the preferred route to a destination network

C. To negotiate IPsec security associations

D. To allocate IP addresses to DHCP clients

ANSWER: A

Explanation:

To block traffic from specified or dynamically identified malicious sources is correct. A blacklist contains addresses or other matching objects associated with untrusted or malicious activity. A firewall can use static blacklist entries configured by an administrator or dynamic entries generated by attack-defense functions to block matching traffic for a configured period.

A blacklist is not a routing protocol and does not create a VPN tunnel. It is also different from a whitelist: a whitelist identifies sources or objects that are explicitly permitted, whereas a blacklist identifies sources or objects that should be denied. Huawei firewall security features and configuration resources are available through Huawei Enterprise Support.

QUESTION NO: 43

The USG limited flow policy configuration is as follows:

[USG] car-class class1 type shared

[USG-shared-car-class-class1] car 1000

[USG-shared-car-class-class1] quit

[USG-traffic-policy-interzone-trust-untrust-outbound-shared

[USG-traffic-policy-interzone-trust-untrust-outbound-shared-1] policy 1

[USG-traffic-policy-interzone-trust-untrust-outbound-shared-1] policy car-class class1

[USG-traffic-policy-interzone-trust-untrust-outbound-shared-1] policy source 192.168.1.0.0.0.255

[USG-traffic-policy-interzone-trust-untrust-outbound-shared-1] policy destination 192.168.2.0 0.0.0.255

[USG-traffic-policy-interzone-trust-untrust-outbound-shared-1] action car

Based on this information, which of the following statements is correct?

A. Class1 limits the definition of the overall car-class, and limits to 1000bps

B. Policy1 traffic will match without limiting the direct release

C. Traffic from 192.168.1.0/24 hosts to 192.168.2.0/24 will be rate-limited.

D. Matching Policy1 traffic will be flow controlled for each source IP

ANSWER: C

Explanation:

Traffic from 192.168.1.0/24 hosts to 192.168.2.0/24 will be rate-limited because policy 1 explicitly defines those source and destination address ranges and applies the `car` action. The wildcard masks `0.0.0.255` identify the respective /24 networks, so traffic that matches both conditions is selected by the policy. The associated CAR class is configured as a shared class, meaning that matching traffic uses one common policing allowance rather than receiving a separate allowance for every individual source address. The configured `car 1000` value establishes the traffic-policing rate for that shared class; on Huawei VRP/USG platforms, CAR rate values are normally expressed in kbit/s unless a command specifies another unit. Therefore, the policy controls the aggregate of traffic matching the defined flow, including traffic initiated by hosts in 192.168.1.0/24 toward 192.168.2.0/24. Huawei documentation and command references for USG products are available through the Huawei Enterprise Support portal.

QUESTION NO: 44

In IPsec VPN with NAT traversal, you must use IKE aggressive mode.

A. TRUE

B. FALSE

ANSWER: B

Explanation:

FALSE is correct because NAT traversal does not impose a requirement to use IKE aggressive mode. NAT traversal, commonly called NAT-T, detects the presence of a NAT device during IKE negotiation and encapsulates ESP traffic in UDP, normally using UDP port 4500. This UDP encapsulation allows encrypted IPsec traffic to cross devices that translate IP addresses or ports. The requirement is that the peers negotiate and support NAT-T; it is independent of the IKEv1 exchange mode selected for the negotiation. IKE main mode can therefore establish an IPsec VPN through NAT when NAT-T is enabled and successfully negotiated. Aggressive mode is a separate IKEv1 negotiation method that reduces the initial exchange to fewer messages, rather than a mechanism required for NAT handling. In practice, main mode is generally preferred where applicable because it protects peer identity information during the initial negotiation. The NAT-T behavior and UDP encapsulation procedure are standardized in RFC 3947. Huawei's IPsec configuration documentation also treats NAT traversal as an IPsec/IKE feature that is configured or negotiated separately from the choice of IKE exchange mode; see the Huawei IPsec configuration guide.

QUESTION NO: 45

The testing center is responsible for detecting the traffic and sending the inspection result to the management center. The management center sends the drainage strategy to the cleaning center for drainage cleaning.

A. TRUE

B. FALSE

ANSWER: B

Explanation:

FALSE is correct because the described responsibility chain incorrectly assigns traffic-drainage handling to the cleaning center. In Huawei Anti-DDoS architectures, the detection center monitors traffic and reports detection results, alarms, or attack information to the management center. The management center provides centralized policy control and, after an attack is identified, coordinates the mitigation process. However, a drainage or traffic-diversion policy is delivered to the traffic scheduling or diversion devices, which redirect the attacked traffic toward the cleaning center. The cleaning center then applies the relevant attack-defense and traffic-cleaning policies to the traffic it receives, removes malicious traffic, and forwards legitimate service traffic as required. Therefore, traffic detection and reporting are associated with the detection center, while traffic drainage is an action performed by scheduling/diversion infrastructure under management-center control; it is not a drainage strategy sent to the cleaning center for that purpose. Huawei describes its DDoS-protection solutions as combining attack detection, traffic diversion, and traffic scrubbing capabilities in a coordinated protection architecture. See Huawei DDoS Protection and Huawei Enterprise Support.

QUESTION NO: 46

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.

ANSWER: A B C

Explanation:

“Packet fragmentation, the fragmented packets are discarded on the link.” is a valid cause because IPsec encapsulation adds headers and increases packet size. If the resulting encrypted packet exceeds an effective path MTU and an intermediate device drops fragments or required ICMP fragmentation feedback, the IKE/IPsec security associations can remain established while application traffic fails. “Presence opf dual-link load balancing, where the path back and forth may be inconsistent.” is also valid: stateful IPsec forwarding requires protected traffic to reach the expected VPN gateway and tunnel context. Unequal or asymmetric forwarding can send return traffic outside the expected protected path, preventing successful end-to-end server communication despite an established tunnel. “Route flapping.” is valid because unstable routes can repeatedly change reachability to protected subnets or next hops. The tunnel control plane may continue to show as established, but data packets can be forwarded to an unavailable or unintended path during route changes. These are data-plane forwarding, MTU, and path-stability conditions that must be checked separately from tunnel establishment status. IPsec architecture and the treatment of protected traffic are described in RFC 4301; IP packet fragmentation behavior is specified in RFC 791.