PassQueen
a.k.a dumpsqueen.com

HCIP-Security-CSSN V3.0

Huawei H12-722_V3.0

Version Demo

Total Demo Questions: 21

Total Premium Questions: 210

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Network Security Overview	33
Topic 2, Firewall Basic Principles	3
Topic 3, Firewall Security Policy	4
Topic 4, Firewall Content Security	91
Topic 5, Firewall User Management	10
Topic 6, Firewall Attack Defense	62
Topic 7, Firewall High Reliability	4
Topic 8, Mix Questions	3
Total	210

QUESTION NO: 1

In order to protect the security of data transmission, more and more websites or companies choose to use SSL to encrypt transmissions in the stream. About using Huawei NIP6000

The product performs threat detection on (SSL stream boy, which of the following statements is correct?

A. NIP0OO does not support SSL Threat Detection.

B. The traffic after threat detection is sent directly to the server without encryption

C. NIP can directly crack and detect SSL encryption.

D. After the process of "decryption", "threat detection", and "encryption"

ANSWER: D

Explanation:

“After the process of "decryption", "threat detection", and "encryption"” correctly describes the SSL inspection workflow used by a Huawei NIP6000 when it is deployed to inspect encrypted traffic. SSL/TLS protects the payload from ordinary in-path inspection, so the device must first establish an inspection context and decrypt the applicable traffic. It can then apply its security engines, such as intrusion prevention, antivirus, and content-based threat detection, to the clear-text content. Before the traffic continues toward its destination, the device encrypts it again so that the protected communications remain encrypted on the next network segment. This decrypt–inspect–encrypt sequence enables the NIP6000 to identify threats that would otherwise be hidden within encrypted sessions while preserving secure transport for the forwarded traffic. In practice, SSL inspection requires the relevant certificates, policies, and deployment configuration so endpoints can trust the inspection process. Huawei identifies the NIP6000 as a network intrusion prevention product with advanced threat-detection capabilities; its placement and policy configuration determine which traffic is inspected. See Huawei’s NIP6000 product information and the Huawei Enterprise Support documentation portal for product documentation and configuration guidance.

QUESTION NO: 2

Which of the following technologies can achieve content security? (multiple choice)

A. Web security protection

B. Global environment awareness

C. Sandbox and big data analysis

D. Intrusion prevention

ANSWER: A B C D

Explanation:

Content security protects users and networks from threats delivered through web pages, files, applications, and network traffic. Web security protection is part of this capability because it controls access to risky web resources and helps block malicious or inappropriate content. Global environment awareness contributes by using broader threat intelligence and security context to identify emerging threats and improve the accuracy of content-based detection. Sandbox and big data analysis provide advanced inspection: suspicious files or objects can be analyzed in an isolated environment, while large-scale analysis correlates threat indicators and behaviors. Intrusion prevention is also a core content-security technology because it inspects traffic and payloads for known exploits, attack signatures, and malicious protocol behavior, then blocks detected attacks inline. Together, these technologies provide layered inspection and threat detection across different forms of content rather than relying on a single control. Huawei’s security portfolio describes integrated threat defense capabilities and cloud-based intelligence that support this approach; see Huawei Enterprise Security and Huawei HiSecEngine USG6000F Series.

QUESTION NO: 3

Which of the following behaviors is a false positive of the intrusion detection system?

A. Unable to detect new types of worms

B. The process of trying to log in to the system is recorded

C. Use Ping to perform network detection and be alerted as an attack

D. Web-based attacks are not detected by the system

ANSWER: C

Explanation:

“Use Ping to perform network detection and be alerted as an attack” describes a false positive. A false positive occurs when an intrusion detection system generates an alarm for activity that is actually legitimate and non-malicious. Ping is commonly used by administrators and monitoring tools for basic connectivity checks, latency testing, and network troubleshooting. Although ICMP traffic can sometimes be associated with reconnaissance or certain denial-of-service techniques, ordinary Ping-based reachability testing is normal network behavior. If the detection system classifies that legitimate diagnostic activity as an attack solely because it matches an overly broad signature or an insufficiently tuned policy, the resulting alert is a false positive.

False-positive handling is an important operational aspect of IDS/IPS deployment. Detection profiles, thresholds, signature settings, and trusted-network policies should be tuned to the organization’s environment so that genuine operational traffic does not overwhelm analysts with unnecessary alerts. NIST defines false positives as alerts incorrectly identifying benign activity as malicious and discusses the importance of tuning intrusion-detection technologies. See NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems and Huawei’s HiSecEngine documentation for security-policy and intrusion-prevention configuration guidance.

QUESTION NO: 4

The network-based intrusion detection system is mainly used to monitor the information of the critical path of the network in real time, listen to all packets on the network, collect data, and divide

Analyze the suspicious object, which of the following options are its main features? (multiple choices)

A. Good concealment, the network-based monitor does not run other applications, does not provide network services, and may not respond to other computers, so

Not vulnerable to attack.

B. The monitoring speed is fast (the problem can be found in microseconds or seconds, and the host-based DS needs to take an analysis of the audit transcripts in the last few minutes

C. Need a lot of monitors.

D. It can detect the source address and destination address, identify whether the address is illegal, and locate the real intruder.

ANSWER: A B

Explanation:

Network-based intrusion detection systems are commonly deployed at critical network locations, such as network boundaries or key internal segments, where they inspect copies of traffic in real time. “Good concealment, the network-based monitor does not run other applications, does not provide network services, and may not respond to other computers, so

Not vulnerable to attack.
” describes the passive nature of a network sensor. A sensor that primarily receives mirrored traffic and exposes few or no network-facing services has a smaller attack surface and is more difficult for an attacker to identify or directly target. In practice, it still must be securely managed and protected, but passive deployment provides the stated concealment advantage.

“The monitoring speed is fast (the problem can be found in microseconds or seconds, and the host-based DS needs to take an analysis of the audit transcripts in the last few minutes” is also a core characteristic. Because packet collection and analysis occur as traffic traverses or is copied from a monitored link, alerts can be generated immediately when signatures, protocol anomalies, or suspicious traffic patterns are observed. This provides timely visibility into attacks against protected network paths. Huawei’s enterprise security portfolio includes network-security monitoring capabilities, and NIST describes network-based IDS sensors as monitoring network traffic for malicious activity. See Huawei Enterprise Security and NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems.

QUESTION NO: 5

Due to differences in network environment and system security strategies, intrusion detection systems are also different in specific implementation. From the perspective of system composition, the main

Which four major components are included?

A. Event extraction, intrusion analysis, reverse intrusion and remote management.

B. Incident extraction, intrusion analysis, intrusion response and on-site management.

C. Incident recording, intrusion analysis, intrusion response and remote management.

D. Incident extraction, intrusion analysis, intrusion response and remote management.

ANSWER: D

Explanation:

Incident extraction, intrusion analysis, intrusion response and remote management. correctly identifies the four functional components commonly used to describe an intrusion detection system’s composition. Incident extraction collects and normalizes security-relevant events from monitored hosts, networks, logs, or sensors. Intrusion analysis then correlates and evaluates those events to determine whether they indicate malicious activity, typically using signature-based, anomaly-based, or policy-based methods. Intrusion response provides the mechanism for acting on confirmed or suspected detections, such as generating alarms, recording evidence, notifying administrators, or triggering coordinated protective actions. Remote management enables centralized configuration, status monitoring, policy administration, and operational control of distributed detection sensors and analysis components. Together, these functions form a complete operational IDS workflow: acquire relevant security events, determine whether an intrusion is occurring, respond to the finding, and administer the system from a central location. This model aligns with the standard IDS concepts of monitoring, analysis, response, and management described in security architecture guidance. Huawei’s enterprise security resources are available through the Huawei Enterprise Network Security support portal; broader IDS terminology is also defined in NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems.

QUESTION NO: 6

The status code in the HTTP response message indicates the type of the response message, and there are many possible values. Which of the following status codes represents the client request

The resource does not exist?

A. 400.

B. 404

C. 200

D. 503

ANSWER: B

Explanation:

The correct status code is **404**. HTTP status code 404, named *Not Found*, means that the server successfully received and understood the client's request but cannot locate a current representation of the requested target resource. In practical terms, the URI may identify a page, API endpoint, file, or other resource that is absent, has been removed, or is not available at that path. It is a client-error response in the 4xx class because the requested resource cannot be provided for the specific request URI. A server can return a 404 response for either a permanently missing resource or a resource whose availability is not known; when the server knows the resource has been permanently removed, it may instead use 410 Gone. The HTTP Semantics specification defines 404 as indicating that the origin server did not find a current representation for the target resource or is unwilling to disclose that one exists. This makes 404 the standard response code for a requested resource that does not exist. See the RFC 9110 definition of 404 Not Found and the MDN HTTP 404 reference.

QUESTION NO: 7

Content filtering is a security mechanism for filtering the content of files or applications through Huawei USCG00 products. Focus on the flow through deep recognition

Contains content, the device can block or alert traffic containing specific keywords.

A. True

B. False

ANSWER: A

Explanation:

True is correct. On Huawei USG-series firewalls, content filtering is a security-control capability that inspects traffic content and applies configured content-security policies when defined conditions are detected. The firewall performs deep inspection of supported application traffic rather than relying only on basic network-layer addressing or ports. Administrators can define keyword-based content filtering rules and associate an action with a match, including generating an alert/log event or blocking the matching traffic. This enables an organization to enforce policies intended to prevent the transmission of sensitive terms, prohibited text, or other defined content through supported protocols and applications.

For effective enforcement, the relevant security policy must permit the traffic to reach the content-inspection function, the content-filtering profile must be applied to that policy, and any encrypted traffic requiring inspection must first be made inspectable through the appropriate decryption configuration. Huawei describes its firewall products as providing application-aware, content-oriented security inspection and policy enforcement. Huawei's firewall product overview is available at Huawei Firewalls, and Huawei's enterprise support portal, including product documentation and configuration guidance, is available at Huawei Enterprise Support.

QUESTION NO: 8

Among the following options, which attack is a malformed packet attack based on the TCR protocol?

A. Teardrop attack

B. Ping of Death attack

C. IP Spoofng attack

D. Land attack

ANSWER: D

Explanation:

Land attack is the TCP-based malformed-packet attack. It is constructed by forging a TCP/IP packet so that its source IP address and source port are identical to its destination IP address and destination port. When such a packet is delivered to a vulnerable host, the host can attempt to establish or process a connection to itself. Historically, this malformed combination could trigger excessive processing, instability, or denial of service in implementations that did not correctly validate the packet's addressing and TCP endpoint information.

The attack is associated with TCP because its packet format includes source and destination port fields in addition to the IP source and destination addresses. Defensive devices such as firewalls and intrusion prevention systems can inspect these header values and discard packets whose source and destination address-and-port tuples are identical when that traffic is not valid for the deployment. TCP's endpoint and connection semantics are defined in the current TCP specification, while IP addressing behavior is defined in the Internet Protocol specification. See RFC 9293: Transmission Control Protocol and RFC 791: Internet Protocol.

QUESTION NO: 9

UDP is a connectionless protocol. UDP Flood attacks that change sources and ports will cause performance degradation of network devices that rely on session forwarding.

Even the session table is exhausted, causing the network to be paralyzed. Which of the following options is not a preventive measure for UDP Flood attacks?

A. UDP fingerprint learning

B. Associated defense

C. current limit

D. First packet discarded

ANSWER: D

Explanation:

First packet discarded is not a standard preventive measure for UDP Flood attacks in Huawei's UDP Flood defense framework. UDP Flood protection is designed to identify and control large volumes of connectionless packets, especially when attackers continuously vary source addresses and UDP ports to create excessive session-processing workload. Huawei security products provide purpose-built UDP Flood controls that assess packet characteristics, learn normal UDP traffic behavior, correlate suspicious traffic patterns, and apply rate control when traffic exceeds expected thresholds. These mechanisms are intended to preserve processing capacity and prevent the session table or related forwarding resources from being consumed by attack traffic.

Discarding a generic "first packet" is not an appropriate UDP Flood mitigation principle because UDP has no connection establishment handshake and legitimate UDP applications may send important data in their initial datagram. A blanket first-packet action therefore does not provide the behavioral analysis, correlation, or traffic-volume control required to distinguish a flood from normal UDP service traffic. Huawei's security documentation and product information describe anti-DDoS capabilities and UDP Flood-oriented traffic controls in the context of attack detection and mitigation: Huawei Enterprise Support search: UDP Flood Defense and Huawei Anti-DDoS solutions.

QUESTION NO: 10

The most common form of child-like attack is to send a large number of seemingly legitimate packets to the target host through Flood, which ultimately leads to network bandwidth.

Or the equipment resources are exhausted. Which of the following options is not included in traffic attack packets?

A. TCP packets

B. UDP packet

C. ICMP message

D. FTP message

ANSWER: D

Explanation:

FTP message is the correct choice because FTP is an application-layer protocol and an FTP message represents application-level control or data communication rather than a fundamental network traffic packet category used to characterize common flood attacks. FTP defines commands, replies, and file-transfer behavior over transport connections; its protocol semantics are described in RFC 959. In contrast, the question is describing volumetric or resource-exhaustion flooding, where defensive classification commonly focuses on high-volume traffic at the transport or network/control-message level. These attacks consume bandwidth, connection state, processing capacity, or other device resources by sending very large quantities of traffic that appears syntactically valid. The Internet Engineering Task Force's discussion of denial-of-service mechanisms explains that flooding and resource consumption are central characteristics of such attacks; see RFC 4732. Therefore, an FTP message is not included in the packet categories intended by this traffic-flood attack classification.

QUESTION NO: 11

Regarding the description of keywords, which of the following is correct? (multiple choice)

A. Keywords are the content that the device needs to recognize during content filtering.

B. Keywords include predefined keywords and custom keywords.

C. The minimum length of the keyword that the text can match is 2 bytes. ,

D. Custom keywords can only be defined in text mode.

ANSWER: A B

Explanation:

Keywords are the recognition objects used by the firewall's content-filtering function. When traffic is inspected, the device compares content against configured keyword entries and can apply the associated filtering action when a match is detected. Therefore, "Keywords are the content that the device needs to recognize during content filtering." correctly describes the role of a keyword: it identifies the content pattern that the security policy needs the device to detect.

"Keywords include predefined keywords and custom keywords." is also correct. Predefined keywords provide built-in entries that can be selected for content-control scenarios, while custom keywords let an administrator create organization-specific recognition content. This distinction supports both rapid use of standard keyword resources and tailored enforcement for an enterprise's own security or compliance requirements. The keyword mechanism is consequently part of content-based inspection rather than simply a URL or IP-address matching feature. Huawei's enterprise support portal provides product documentation and configuration guidance for security-policy and content-security features at Huawei Enterprise Support. Additional technical documentation and knowledge resources are available through the Huawei Enterprise Knowledge Center.

QUESTION NO: 12

With the continuous development of the network and the rapid development of applications, companies are making users more and more frequently start to transfer files on the network.

Virus threats are becoming more and more serious. Only by rejecting the virus outside the network can data security and system stability be guaranteed. So, which of the following are

What harm might be caused by illness? (multiple choices)

A. Threaten the security of the user's host and network.

B. Some viruses can be used as intrusion tools, such as Trojan horse viruses,

C. Control the host computer's accumulated limit and the user's data, and some viruses may even cause damage to the host's hardware.

D. Can easily pass the defense of Huawei USG6000 products

ANSWER: A B C

Explanation:

“Threaten the security of the user's host and network.” is correct because malware infections can compromise endpoint confidentiality, integrity, and availability, and can also provide a foothold for further activity across connected network systems. “Some viruses can be used as intrusion tools, such as Trojan horse viruses,” is correct because Trojan malware commonly enables unauthorized remote access, command execution, credential theft, or delivery of additional malicious payloads. “Control the host computer's accumulated limit and the user's data, and some viruses may even cause damage to the host's hardware.” is also correct in its intended meaning: viruses can consume or control host computing resources, alter, steal, encrypt, or destroy user data, and can disrupt system operation. In severe cases, malware can affect firmware or force harmful operating conditions, creating potential physical-device impact. These risks support using gateway anti-virus inspection, endpoint protection, signature updates, and file-transfer security controls to reduce exposure. CISA describes malware as malicious software capable of harming systems and data, while NIST identifies malware as a significant threat to information-system security. See CISA malware guidance and NIST's malware glossary entry.

QUESTION NO: 13

Which of the following are typical intrusions? "Multiple choice)

A. Computer is infected by U disk virus

B. Abnormal power interruption in the computer room

C. Tampering with Web pages

D. Copy/view sensitive data

ANSWER: A C D

Explanation:

Typical intrusions are security events in which malicious code or an unauthorized party gains access to systems or information, then affects the confidentiality or integrity of those assets. “Computer is infected by U disk virus” is an intrusion because removable media can introduce malware into a host. Such malware may execute without authorization, establish persistence, spread to other hosts, steal information, or enable further unauthorized control. “Tampering with Web pages” is also an intrusion: unauthorized modification of website content is a direct compromise of information integrity and commonly results from a compromised web server, application, or administrator account. “Copy/view sensitive data” represents unauthorized access to protected information and is an intrusion because it compromises confidentiality, even if no data is deleted or service disruption occurs. These events align with incident-handling guidance that treats malicious-code activity, unauthorized access, and unauthorized changes to systems or data as security incidents requiring investigation and response. Huawei security guidance likewise emphasizes protecting systems and data from unauthorized access, modification, and malware threats. See NIST SP 800-61 Rev. 2 and Huawei Trust Center: Security.

QUESTION NO: 14

Which of the following statements about URL filtering on a Huawei firewall are correct? (multiple choice)

A. URL filtering can control user access based on website categories.

B. A custom URL category can be used to classify specified websites.

C. URL filtering can be applied through a security policy.

D. URL filtering automatically creates a route to every permitted website.

ANSWER: A B C

Explanation:

URL filtering can control user access based on website categories is correct. A URL filtering profile can apply actions to predefined or customized URL categories, allowing access to be permitted, blocked, or monitored according to organizational policy.

A custom URL category can be used to classify specified websites is correct. Administrators can add URLs or domain names to a custom category and then define the action for that category. **URL filtering can be applied through a security policy** is also correct because the URL filtering profile must be referenced by the policy that processes the relevant traffic. URL filtering does not replace routing; it is a content-security control applied after the traffic matches a permit policy. See Huawei Enterprise Support: URL filtering.

QUESTION NO: 15

Cloud sandbox refers to deploying the sandbox in the cloud and providing remote detection services for tenants. The process includes:

1. Report suspicious files

2. Retrospective attack

3. Firewall linkage defense

4. Prosecution in the cloud sandbox

For the ordering of the process, which of the following options is correct?

A. 1-3-4-2

B. 1-4-2-3

C. 1-4-3-2

D. 3-1-4-2:

ANSWER: C

Explanation:

The correct sequence is **1-4-3-2**. A cloud sandbox workflow starts when a security device identifies and reports a suspicious file to the cloud-based analysis service. The cloud sandbox then processes the sample, typically by performing static inspection, dynamic execution, behavioral analysis, and reputation or threat-intelligence correlation. This analysis produces a verdict and associated indicators of compromise.

Once a malicious verdict is available, the firewall linkage-defense stage applies the intelligence operationally. It can use the returned indicators, such as malicious file hashes, domains, URLs, IP addresses, or behavioral signatures, to block related communications and prevent additional compromise. Retrospective attack analysis follows this enforcement stage: the organization can search historical logs and traffic records for prior activity involving the identified indicators, determine the scope of exposure, and support incident response and remediation. This order reflects the normal detection-to-analysis-to-enforcement-to-tracing lifecycle used by cloud sandbox integrations. Huawei describes cloud sandbox capabilities and security-service integration at Huawei Cloud Sandbox; Huawei's enterprise support portal provides product documentation and configuration guidance at Huawei Enterprise Support.

QUESTION NO: 16

Which of the following options are benefits of deploying an IPS in inline mode? (multiple choice)

A. Blocking matching attack traffic in real time

B. Preventing a detected attack from reaching the protected server

C. Generating alarms for matched intrusion signatures

D. Receiving only a copy of traffic and never affecting the forwarding path

ANSWER: A B C

Explanation:

Blocking matching attack traffic in real time is correct. An inline IPS is placed in the forwarding path, allowing it to discard packets or terminate sessions when a configured signature is matched.

Preventing a detected attack from reaching the protected server is also correct because enforcement occurs before the malicious traffic is forwarded downstream. **Generating alarms for matched intrusion signatures** is correct as the IPS can create logs and alarms while inspecting traffic inline. A passive, mirrored deployment can provide detection visibility, but it cannot directly stop the observed packet by itself. NIST describes the distinction between detection and inline prevention in NIST SP 800-94.

QUESTION NO: 17

When you suspect that the company's network has been attacked by hackers, you have carried out a technical investigation. Which of the following options does not belong to the behavior that occurred in the early stage of the attack?

A. Planting malware

B. Vulnerability attack

C. Web application attacks

D. Brute force

ANSWER: A

Explanation:

Planting malware is the behavior that does not normally belong to the early stage of an attack. Early-stage activity is primarily concerned with obtaining an initial foothold: adversaries attempt to reach an exposed service, exploit an entry point, or authenticate to a target. Once access has been obtained, an attacker may deliver or install malicious code to establish persistence, create a backdoor, enable remote control, steal data, or support later movement through the environment. Therefore, malware implantation is generally an action following successful initial access rather than an initial intrusion attempt itself.

This distinction is important during technical investigation because the discovery of planted malware often indicates that the incident has progressed beyond attempted compromise. Investigators should preserve relevant evidence, identify the malware's execution and persistence mechanisms, determine its first appearance, and use those findings to scope affected systems and accounts. The NIST incident-handling guidance emphasizes collecting and analyzing indicators and determining the incident's extent, while the ATT&CK framework separates initial access from later execution and persistence activities. See NIST SP 800-61 Rev. 2 and MITRE ATT&CK: Initial Access.

QUESTION NO: 18

Which of the following statements about IPS is wrong?

A. The priority of the coverage signature is higher than that of the signature in the signature set.

B. When the "source security zone" is the same as the "destination security zone", it means that the IPS policy is applied in the domain.

C. Modifications to the PS policy will not take effect immediately. You need to submit a compilation to update the configuration of the IPS policy.

D. The signature set can contain either predefined signatures or custom signatures.

ANSWER: D

Explanation:

The statement “The signature set can contain either predefined signatures or custom signatures.” is wrong. On Huawei firewalls, an IPS signature set is used to group and manage predefined IPS signatures that share characteristics, allowing the administrator to apply a common action, such as alert, block, or permit, to that group through an IPS profile. User-defined (custom) signatures are created separately to detect traffic patterns not covered by the built-in signature database. Their actions and settings are configured as individual custom signatures rather than by placing them into a predefined-signature set. This distinction helps preserve predictable management of Huawei’s maintained signature database while allowing tailored detection for organization-specific threats. In an IPS profile, signature-set settings establish the handling for included predefined signatures, while exception/override signature settings can take precedence for particular signatures. Huawei documents IPS configuration, including signature management and IPS-profile application, in its firewall product documentation. See Huawei Firewall Configuration Guide and Huawei Firewall Product Documentation.

QUESTION NO: 19

Use BGP protocol to achieve diversion, the configuration command is as follows

[sysname] route-policy 1 permit node 1

[sysname-route-policy] apply community no-advertise [sysname-route-policy] quit

[sysname]bgp100

155955cc-666171a2-20fac832-0c042c04

29

[sysname-bgp] peer

[sysname-bgp] import-route unr [sysname- bgpl ipv4-family unicast

[sysname-bgp-af-ipv4] peer 7.7.1.2 route-policy 1 export

[sysname-bgp-af-ipv4] peer 7.7. 1.2 advertise community [sysname-bgp-af-ipv4] quit

[sysname-bgp]quit

Which of the following options is correct for the description of BGP diversion configuration? (multiple choice)

A. Use BGP to publish UNR routes to achieve dynamic diversion.

B. After receiving the UNR route, the peer neighbor will not send it to any BGP neighbor.

C. You also need to configure the firewall ddos bgp-next-hop fib-filter command to implement back-injection.

D. The management center does not need to configure protection objects. When an attack is discovered, it automatically issues a traffic diversion task.

ANSWER: A B C

Explanation:

This configuration implements dynamic diversion by importing UNR routes into BGP with `import-route unr` and advertising them to the designated BGP peer. When a diversion task creates or withdraws the relevant UNR route, BGP can correspondingly advertise or withdraw the diversion prefix, allowing traffic steering to be controlled dynamically rather than through manual route changes. The export route policy applies the well-known `no-advertise` community, and `peer ... advertise-community` ensures that this community is included in the advertised BGP update. A receiving BGP neighbor that receives a route carrying `no-advertise` must not advertise that route to any of its BGP peers. This limits propagation of the diversion route while retaining the required direct diversion relationship. In the complete firewall-based diversion solution, `ddos bgp-next-hop fib-filter` is also required for traffic back-injection handling; it controls FIB processing of the BGP diversion next hop so that traffic returned after DDoS cleaning can be forwarded correctly. The definition and required handling of the `NO_ADVERTISE` community are specified in RFC 1997. Huawei configuration documentation is available from the Huawei Enterprise documentation portal.

QUESTION NO: 20

Which of the following measures are important for protecting a cloud tenant environment? (multiple choice)

A. Apply least-privilege permissions to tenant accounts.

B. Separate tenant networks and workloads by using appropriate isolation controls.

C. Enable logging and monitoring for tenant resources.

D. Assign administrator permissions to all tenant users for easier maintenance.

ANSWER: A B C

Explanation:

Applying least-privilege permissions to tenant accounts is correct because access rights should be limited to the resources and operations required by each user, role, or service. **Separating tenant networks and workloads by using appropriate isolation controls** is also correct. Network segmentation, security groups, and workload isolation reduce the possibility that a compromise in one environment affects another. **Enabling logging and monitoring for tenant resources** is correct because audit trails and security monitoring provide the visibility needed to identify unauthorized access, configuration changes, and suspicious behavior.

Cloud security requires both provider controls and tenant-side configuration. The tenant remains responsible for securely managing identities, data, workloads, and services it deploys in the cloud. Huawei Cloud security information is available at Huawei Cloud Security.

QUESTION NO: 21

Which of the following technology, administrators can according to business requirements, to scale to achieve load sharing of business flow?

A. Resource pool mechanism

B. weighting mechanism

C. load balancing

D. Hot Standby

ANSWER: A B

Explanation:

The **Resource pool mechanism** and **weighting mechanism** are the relevant technologies for scaling the handling of service traffic and implementing traffic sharing according to business requirements. A resource pool combines the available processing resources or service members into a logical set, allowing traffic-processing capacity to be expanded as resources are added. This provides the foundation for distributing service flows rather than restricting processing to a single device or member.

The weighting mechanism then lets an administrator control the relative proportion of new service flows assigned to each available member. Weight values can reflect differences in device performance, available capacity, or the intended service-share ratio. For example, a higher-capacity member can be assigned a larger weight so that it receives a correspondingly larger portion of sessions. Together, resource pooling supplies scalable resources, while weighting supplies the policy control needed to distribute business flows in the desired ratio. These concepts align with Huawei firewall high-availability and traffic-processing design principles documented in Huawei's enterprise support resources and firewall product information: Huawei Enterprise Support and Huawei Firewall Products.