DUMPSARENA

HCIP-Security (Fast track) V1.0

Huawei H12-724

Version Demo

Total Demo Questions: 46

Total Premium Questions: 466

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which of the following options are relevant to Any Office The description of the solution content is correct? (Multiple choice)

A. Provide unified and secure access to enterprise mobile applications on mobile terminals.

B. The tunnel is dedicated and cannot be penetrated by viruses.

C. Applications are quickly integrated and can be extended.

D. It can be quickly integrated and docked with the enterprise application cloud platform.

ANSWER: A B C D

Explanation:

AnyOffice is Huawei's enterprise mobile-office solution, designed to let employees use mobile devices to access organizational services while keeping enterprise resources under centrally managed security controls. Therefore, "Provide unified and secure access to enterprise mobile applications on mobile terminals" accurately reflects its core purpose: mobile users access approved enterprise applications through a unified and protected access mechanism.

"The tunnel is dedicated and cannot be penetrated by viruses" describes the solution's secure-tunnel concept. Enterprise traffic is isolated from ordinary Internet access and protected through encrypted, authenticated communication channels, reducing exposure of business systems and data to mobile-network threats. AnyOffice is also intended to support flexible service onboarding, so "Applications are quickly integrated and can be extended" is correct: enterprises can incorporate existing and additional mobile applications as requirements grow. Finally, "It can be quickly integrated and docked with the enterprise application cloud platform" is consistent with its role as an enterprise mobility access layer that connects mobile users with internal application platforms and cloud-based enterprise services. Huawei's enterprise-security portfolio and mobile-access architecture emphasize secure remote connectivity, centralized management, and integration with enterprise services. See Huawei Enterprise Security and Huawei.

QUESTION NO: 2

When configuring the antivirus software policy, if you set"The required antivirus software violation level is not installed or running"for"generally"And check"out Now serious violation of the rules prohibits access to the network"Options. When the user uses Any office Certify, The certification is passed, but the result of the security check Can the user access the network when the virus software is not turned on?

A. Can access the network? Can also access network resources.

B. Cannot access the network.

C. Can access the network, but must be repaired before network resources can be accessed.

D. You can access the network, but you need to re-authenticate to access network resources.

ANSWER: C

Explanation:

Can access the network, but must be repaired before network resources can be accessed. This is the expected behavior because the endpoint's antivirus state—antivirus software not running—has been classified as a *general* violation. The user can therefore complete AnyOffice authentication and obtain basic network connectivity. However, the endpoint remains noncompliant until the required antivirus software is started or otherwise brought into the required state. The access-control system places the endpoint into a remediation-oriented state, allowing it to perform the actions needed to resolve the security posture issue while restricting access to protected network resources.

The selected setting to prohibit network access applies when an endpoint has a *serious* violation. It does not convert a violation explicitly classified as general into a serious violation. Consequently, the configured severity level is what determines the applicable enforcement result: general violations receive network access with remediation restrictions, and access to normal network resources is restored after the endpoint passes the follow-up security check. Huawei's enterprise support portal provides product documentation and configuration guidance for endpoint admission control and security-policy

enforcement: Huawei Enterprise Support. Huawei also describes its campus identity and access-management capabilities, including endpoint access control and security posture enforcement, at Huawei Campus Network Solutions.

QUESTION NO: 3

There are several steps in a stored XSS attack

①The attacker hijacks the user session

②The attacker submits an issue containing known JavaScript

③User login

④The user requests the attacker's question 5

⑤The server responds to the attacker's JavaScript

⑥ The user's browser sends a session token to the attacker

⑦The attacker's JavaScript is executed in the user's browser

For the ordering of these steps, which of the following options is correct?

A. ③②⑦⑥④⑤①

B. ③②④⑤⑦⑥①

C. ③②④⑥⑤⑦①
155955cc-666171a2-20fac832-0c042c0428

D. ⑧②⑤⑦④⑥①

ANSWER: B

Explanation:

The correct sequence is ③②④⑤⑦⑥①. In this scenario, a user first logs in, creating an authenticated browser session. The attacker then submits content—described as an issue or question—that contains malicious JavaScript. This is the defining characteristic of stored cross-site scripting: the application accepts the attacker-controlled payload and retains it so that it can later be delivered to another user. When the authenticated user requests the attacker's stored question, the server returns the page containing that stored JavaScript. Because the browser treats the returned content as part of the trusted site's page, it executes the script in the user's browser context. The malicious script can then exfiltrate a session token or otherwise perform actions using the victim's authenticated session. Once the attacker receives usable session information, the attacker can hijack the user session. This ordering reflects the persistent nature of stored XSS: payload submission occurs before the victim accesses the affected resource, and script execution occurs only after the server delivers that stored content to the victim. See the OWASP Cross Site Scripting overview and the OWASP XSS Prevention Cheat Sheet.

QUESTION NO: 4

The following is the 802.1X access control switch configuration:

[S5720]dot1x authentication-method eap

[S5720-GigabitEthernet0/0/1] port link-type access

[S5720-GigabitEthemet0/0/1] port default vlan 11

[S5720-GigabitEthernet0/0/1] authentication dot1x

Assuming that GE0/0/1 is connected to user 1 and user 2 through the HUB, which of the following options is correct?

A. After user 1 is authenticated, user 2 can access network resources without authentication

B. User 1 and User 2 must be individually authenticated before they can access network resources

C. GE0/0/1 does not need to enable dot1X

D. Neither user 1 nor user 2 can pass the authentication and access network resources.

ANSWER: A

Explanation:

After user 1 is authenticated, user 2 can access network resources without authentication. On Huawei switches, 802.1X authentication uses port-based access control by default unless the configuration explicitly changes the access-control mode to MAC-based authentication. In this configuration, GE0/0/1 is an access port in VLAN 11 and 802.1X is enabled on that physical interface. Because both users connect through a HUB, their traffic reaches the switch through the same physical port. Once user 1 successfully completes EAP authentication, the switch authorizes GE0/0/1. Authorization applies to the port as a whole in the default port-based mode, rather than separately tracking each endpoint behind the HUB. Consequently, user 2 can send traffic through the now-authorized interface without independently performing 802.1X authentication. This behavior is important when designing access-layer security: a HUB or another shared Layer 1/Layer 2 attachment can allow multiple devices to benefit from one successful port authentication. Huawei documentation for enterprise switch configuration is available through the Huawei Enterprise Documentation portal; the underlying access-control framework is defined by the IEEE 802.1X standard.

QUESTION NO: 5

What equipment do Policy Center supported servers include? (Choose 3 answers)

A. remote control device

B. mail server

C. Internet behavior management equipment

D. log collection server

ANSWER: A B C

Explanation:

Policy Center supports integration with remote control devices, mail servers, and Internet behavior management equipment. These systems provide policy-relevant capabilities that can be incorporated into centralized security-policy administration. Remote control devices are included because their controlled-access activity can be governed in conjunction with organizational security policies. Mail servers are supported because email services are a key enterprise application whose access and security handling may require policy coordination. Internet behavior management equipment is supported because it enforces and monitors users' web-access behavior, which is directly related to an organization's security and compliance policy requirements. Together, these supported systems allow Policy Center to extend policy-oriented management beyond a single security gateway and coordinate controls across commonly deployed enterprise service platforms. Huawei's enterprise security portfolio emphasizes centrally managed, integrated protection and policy control across multiple security domains; see the Huawei Network Security product portfolio and the Huawei Enterprise Support documentation portal for product documentation and compatibility information.

QUESTION NO: 6

Which of the following features does Huawei NIP intrusion prevention equipment support? (multiple choice)

A. Virtual patch

B. Mail detection

C. SSL traffic detection

D. Application identification and control

ANSWER: A C D

Explanation:

Huawei NIP intrusion-prevention products provide prevention capabilities beyond simple signature matching. **Virtual patch** is a core IPS use case: the device can identify exploit attempts directed at a known vulnerability and block them at the network boundary, allowing protection to be applied before every affected endpoint has received its vendor patch. This reduces the exposure window for servers and client systems.

SSL traffic detection is also supported through encrypted-traffic inspection capabilities. After the device is configured with the appropriate certificates and decryption policy, it can inspect supported encrypted sessions so that threats hidden in encrypted application traffic can be identified and controlled. **Application identification and control** complements IPS protection by recognizing applications independently of port numbers and applying policy controls based on the application. This enables administrators to restrict risky, unnecessary, or non-business application traffic while retaining required services.

These functions align with Huawei's network-security approach of combining intrusion prevention, encrypted-traffic visibility, and application-aware policy enforcement. See Huawei's enterprise security product information and the Huawei Enterprise Support documentation portal for product documentation and configuration guidance.

QUESTION NO: 7

Which of the following methods can be used to protect enterprise terminal security?

A. Access control

B. Encrypted access

C. Business isolation

D. Audit billing

ANSWER: A

Explanation:

Access control is the appropriate method because it protects enterprise terminals by ensuring that only authenticated users and authorized devices can obtain access to enterprise network resources, applications, and services. In practice, terminal access control can verify user identity, assess device status, apply authorization policies, and restrict access according to the user's role, device type, location, or security posture. This reduces the risk that an unmanaged, compromised, or unauthorized endpoint can connect to protected enterprise resources. Huawei's campus-network security approach includes identity-based access control and policy enforcement as key mechanisms for controlling endpoint access to the network; see Huawei CloudCampus. The same principle is reflected in recognized security-control guidance: access enforcement requires an organization to enforce approved authorizations for logical access to information and systems. See the access-control family in NIST Special Publication 800-53. Therefore, access control directly provides a foundational protection mechanism for enterprise terminal security.

QUESTION NO: 8

Regarding security logs generated by a Huawei firewall, which of the following statements are correct? (multiple choice)

A. Security-policy logs can be used to investigate permitted and denied traffic.

B. Threat-defense logs can record matched malware or intrusion events.

C. Centralized log collection supports correlation and retention.

D. Enabling logs removes the need to configure security policies.

ANSWER: A B C

Explanation:

Security logs provide evidence of traffic processing and security events. Logs for permitted and denied security-policy traffic can help administrators verify policy behavior and investigate access attempts. Logs generated by threat-defense functions, such as antivirus or IPS, can identify matched threats, affected hosts, and the action taken by the device.

Exporting logs to a centralized log server improves retention, correlation, and incident investigation. Log generation does not replace a security policy: the policy still determines whether traffic is permitted or denied. NIST log-management guidance is available in NIST SP 800-92.

QUESTION NO: 9

Import the user information of the AD server on the Agile Controller-Campus to realize the user's access authentication. If the user is in the Agile.

The user information is not found on the Controller-Campus. Which of the following actions will be performed in the next step?

A. Straight forward to return authentication failure information.

B. Discard user information.

C. User information is sent to the AD server for verification.

D. Synchronize the database again.

ANSWER: C

Explanation:

User information is sent to the AD server for verification. is correct because Agile Controller-Campus can use Microsoft Active Directory as an external identity source during access authentication. Importing or synchronizing AD accounts supplies a local user-data cache and supports identity management, but an authentication request for a user that is not located in the controller's local user information must be handled by consulting the configured external AD source. The controller therefore sends the relevant user identity and authentication-verification request to the AD server, which is the authoritative directory for that user. AD validates the supplied credentials according to its domain account records and returns the authentication result; Agile Controller-Campus then uses that result to continue the access-control decision and apply the associated authorization policy. This behavior enables AD-managed accounts to remain centrally administered while the campus controller provides network access control. Huawei's enterprise support portal provides product documentation and configuration guidance for campus controllers and external authentication integration: Huawei Enterprise Support. Huawei's campus networking resources also describe the controller-based access-control architecture in which identity services are integrated with campus policy enforcement: Huawei Campus Network Solutions.

QUESTION NO: 10

In the visitor reception hall of a company, there are many temporary terminal users, and the administrator hopes that users do not need to provide any account numbers and passwords. access Internet. Which of the following authentication methods can be used for access?

A. Local account authentication

B. Anonymous authentication

C. AD Account Verification

D. MAC Certification

ANSWER: B

Explanation:

Anonymous authentication is appropriate for temporary visitors when the access policy is to provide Internet connectivity without asking users to enter an account name or password. In Huawei campus-network access-control deployments, this type of guest access can be used to present an authentication or portal page while allowing the visitor to proceed without supplying individual credentials. It is therefore suited to public or semi-public reception areas where user identity is not being used as the primary admission condition. The administrator can still apply network-side controls independently of a user account, such as placing visitors in a dedicated VLAN or user group, limiting accessible destinations to Internet resources, applying bandwidth limits, and enforcing session controls. This allows guest traffic to be separated from internal corporate resources while keeping the connection process simple for a high turnover of temporary users. Huawei describes its campus-network portfolio and related access-management capabilities at Huawei Campus Networking. Additional Huawei enterprise support and product documentation resources are available through Huawei Enterprise Support.

QUESTION NO: 11

Mobile smartphone, tablet PC users through Any Office Client and AE Establish IPSec Encrypted tunnel, After passing the certification and compliance check, visit the enterprise business.

A. True

B. False

ANSWER: A

Explanation:

True is correct. Huawei AnyOffice is designed to provide secure mobile access for users of smartphones and tablet devices when they connect to enterprise resources from outside the trusted corporate network. The AnyOffice client creates a protected remote-access connection to the enterprise access system using IPsec, which provides confidentiality, integrity protection, and peer authentication for traffic carried across an untrusted network. This is consistent with the IPsec architecture defined by the IETF: RFC 4301.

Access is not based solely on tunnel establishment. The solution can authenticate the user and evaluate endpoint compliance or security posture before permitting access to internal business systems. This allows the enterprise to apply access-control policy based on both identity and the condition of the mobile endpoint, helping prevent unmanaged or noncompliant devices from receiving the same access as approved devices. Huawei positions its enterprise security portfolio around secure remote connectivity, identity-aware access control, and protection of enterprise resources; see the Huawei Enterprise Security product information. Therefore, the described sequence—mobile client connection, IPsec encryption, authentication and compliance validation, then access to enterprise services—correctly represents the intended secure mobile-office access workflow.

QUESTION NO: 12

Which of the following options belongs to MC prioritized pail Authentication application scenarios?

A. User use portal Page for authentication

B. Users follow WeChat for authentication.

C. User use IAC Client authentication

D. For MAC-prioritized Portal authentication, a user first completes Portal authentication. The RADIUS server caches the terminal MAC address; if it reconnects within the cache validity period, the cached MAC address is used for authentication.

ANSWER: D

Explanation:

“For MAC-prioritized Portal authentication, a user first completes Portal authentication. The RADIUS server caches the terminal MAC address; if it reconnects within the cache validity period, the cached MAC address is used for authentication.” describes the intended MAC-prioritized Portal authentication scenario. This mechanism combines an initial interactive Portal login with subsequent convenience for the same endpoint. When a terminal first accesses the network, the user completes

Portal authentication and the authentication system associates the successful session with the terminal's MAC address. The RADIUS server retains that MAC-address information for a configured validity period. If the endpoint disconnects and returns before the cache expires, the access device can use the cached MAC identity to recognize the terminal and authorize it without requiring the user to perform the Portal interaction again. This is particularly useful in environments where users frequently roam, sleep and wake devices, or briefly lose connectivity, while the organization still wants initial user authentication and controlled cache lifetime. Huawei enterprise documentation is available through the Huawei Enterprise Documentation portal; the related RADIUS protocol and its role in centralized authentication are defined in RFC 2865.

QUESTION NO: 13 - (SIMULATION)

For special message attacks, which of the following option descriptions is correct?

A Special control packet attack is a potential attack and does not have direct destructive behavior

B. The attacker probes the network structure by sending special control messages to launch a real attack.

C. Special control message attacks do not have the ability to detect the network structure. Only scanning attacks can detect the network.

D. Special control message items can only use ICMP to construct attack messages.

ANSWER: Check the explanation for the answer

Explanation:

Correct answers: A and B.

A: Special control-packet attacks are generally reconnaissance/probing attacks. They are potentially dangerous but normally do not directly cause destructive effects themselves.
B: An attacker can send special control messages to discover network topology, host information, routing behavior, or security policy characteristics, then use the results to perform a subsequent real attack.

C is incorrect because special control messages can also be used for network discovery. **D** is incorrect because such attacks are not limited to ICMP; other protocol control messages may also be used.

QUESTION NO: 14

Use hardware SACG Access control,,In hardware SACG View the results of the conversation table on the deduction.

Which of the following statements are correct? (Multiple choice)

A. 192.168.1.0 is definitely the Agile Controller-Campus Manager IP address.

B. If 192.168.200.11 is a server in the authentication-free domain, a terminal with IP address 192.168.0.1 can access the server even if it has not passed authentication.

C. 192.168.100.1 definitely is Agile Controller-Campus Controller IP address.

D. If the session 192.168.0.119:154 to 192.162.0.11:15080 is not refreshed within 6 minutes, 192.168.0.119 must establish a new session to communicate with 192.168.200.11.

ANSWER: A B D

Explanation:

The SACG session-table information supports identifying 192.168.1.0 as the Agile Controller-Campus Manager address because the associated control-plane session is the Manager-facing communication shown in the table. SACG uses these established sessions to communicate with the campus access-control platform and to obtain or apply user access-control information. Huawei's enterprise security documentation portal provides the product documentation context for SACG access control and controller integration: Huawei Enterprise Support.

A server placed in an authentication-free domain is intentionally reachable before a user completes authentication. Therefore, a terminal such as 192.168.0.1 can access 192.168.200.11 while unauthenticated when that server is configured as an authentication-free-domain resource. This is used for resources required before authentication, such as portal, DNS, DHCP, or supporting service infrastructure.

The stated session-aging conclusion is also correct. A session entry represents state maintained for a specific traffic flow, and traffic matching that flow refreshes its aging timer. If the session from 192.168.0.119 to 192.162.0.11 on the stated port is not refreshed for six minutes, it ages out. Subsequent communication from 192.168.0.119 to 192.168.200.11 is a distinct flow and requires a session to be created again. See the Huawei documentation portal at Huawei Enterprise Documentation for session-management and access-control references.

QUESTION NO: 15

If you deploy Free Mobility, in the logic architecture of Free Mobility, which of the following options should be concerned by the administrator?

A. Is the strategy automatically deployed?

B. Choose the appropriate policy control point and user authentication point

C. Does the strategy deployment target a single user?

D. Does the strategy deployment target a single department?

ANSWER: B

Explanation:

Choose the appropriate policy control point and user authentication point is correct because Free Mobility relies on a logical separation between identity authentication, policy decision/control, and policy enforcement. An administrator must plan where users are authenticated and which component acts as the policy control point so that a user's identity, role, and associated access policy can be obtained consistently when the user connects from different locations or through different access devices. Correct placement and selection of these functions ensures that access permissions follow the authenticated user rather than being tied only to a physical port, VLAN, or department. It also allows the network to deliver unified access control across the campus while maintaining centralized policy administration and reliable communication with enforcement devices. This architecture planning is therefore a prerequisite for deploying identity-based, location-independent access control. Huawei campus networking solutions describe centralized policy and identity-based access as core capabilities for campus access control; see the Huawei Campus Network product information and the Huawei Enterprise Support documentation portal for product documentation and configuration guidance.

QUESTION NO: 16

The configuration command to enable the attack prevention function is as follows; n

[FW] anti-ddos syn-flood source-detect

[FW] anti-ddos udp-flood dynamic-fingerprint-learn

[FW] anti-ddos udp-frag-flood dynamic fingerprint-learn

[FW] anti-ddos http-flood defend alert-rate 2000

[Fwj anti-ddos htp-flood source-detect mode basic

Which of the following options is correct for the description of the attack prevention configuration? (multiple choice)

A. The firewall has enabled the SYN Flood source detection and defense function

B. The firewall uses the first packet drop to defend against UDP Flood attacks.

C. HTTP Flood attack defense uses enhanced mode for defense

D. The threshold for HTTP Flood defense activation is 2000.

ANSWER: A B D

Explanation:

The firewall has enabled the SYN Flood source detection and defense function because `anti-ddos syn-flood source-detect` explicitly enables source-based detection for SYN flood protection. This allows the firewall to identify sources exhibiting SYN-flood characteristics and apply the relevant protection processing.

The firewall uses the first packet drop to defend against UDP Flood attacks because `anti-ddos udp-flood dynamic-fingerprint-learn` enables dynamic fingerprint learning for UDP flood defense. Dynamic fingerprint learning establishes characteristics for UDP traffic and supports first-packet-based processing to distinguish and control anomalous flood traffic. The analogous UDP-fragment command enables the same dynamic-fingerprint capability for fragmented UDP flood traffic.

The threshold for HTTP Flood defense activation is 2000 because `anti-ddos http-flood defend alert-rate 2000` sets the HTTP flood alert rate to 2000. In this configuration, 2000 is the configured rate threshold used by the HTTP flood defense mechanism for alerting and attack-defense handling. The HTTP source-detection command is explicitly configured with `mode basic`, while the alert-rate command separately supplies the numeric threshold. Huawei product documentation and security configuration resources are available through the Huawei Enterprise Support portal and its technical documentation catalog.

QUESTION NO: 17

View on the switch Agile Controller-Campus The policy issued by the server is as follows:

For this strategy, which of the following options are correct? (Multiple choice)

A. Common_ user Users can access Internet www H.

B. VIP Users can access Internet WWW resources.

C. VIP can visit Mail Server resources.

D. Common_user users can access Mail_Server resources.

ANSWER: B C D

Explanation:

The effective authorization represented by the issued policy grants the **VIP** user group access to both the Internet WWW service and the Mail Server resource. Therefore, “VIP Users can access Internet WWW resources.” and “VIP can visit Mail Server resources.” are valid descriptions of the permissions delivered for that group. The policy also grants the **Common_user** group permission to use the Mail_Server resource, so “Common_user users can access Mail_Server resources.” is also correct. In Agile Controller-Campus, the controller delivers user- and group-based access policies to network devices, which then enforce permissions according to the authenticated user’s assigned group and the resources/services defined by the authorization policy. A user’s ability to reach a particular destination is consequently determined by the authorization entries applicable to that user group, rather than merely by successful authentication. This centralized policy model allows differentiated access—for example, granting VIP users both web and mail services while granting common users only the specifically authorized internal resource. Huawei describes its campus management and control capabilities at Huawei Campus Network Management and Control; Huawei’s enterprise support portal provides product documentation and configuration guidance at Huawei Enterprise Support.

QUESTION NO: 18

Which of the following options are relevant to MAC Certification and MAC The description of bypass authentication is correct? (Multiple choice)

A. MAC Certification is based on MAC The address is an authentication method that controls the user's network access authority. It does not require the user to install any client software.

B. MAC Bypass authentication is first performed on the devices that are connected to the authentication 802 1X Certification;If the device is 802. 1X No response from authentication, re-use MAC The authentication method verifies the legitimacy of the device.

C. MAC During the authentication process, the user is required to manually enter the user name or password.

D. MAC The bypass authentication process does not MAC The address is used as the user name and password to automatically access the network.

ANSWER: A B

Explanation:

MAC authentication controls network access by identifying a terminal through its MAC address. Because the access device can obtain the source MAC address directly from received frames, this method does not require a supplicant or other client software to be installed on the endpoint. The device's MAC address is commonly supplied to the authentication system as the credential used to determine whether the endpoint is authorized and which access policy should apply.

MAC bypass authentication is designed to accommodate terminals that cannot participate in 802.1X authentication, such as many printers, cameras, and other non-interactive devices. The access device initially attempts 802.1X authentication. When the attached terminal does not respond as an 802.1X supplicant, the device falls back to MAC-based authentication and uses the learned MAC address to validate the endpoint through the configured authentication infrastructure. This provides a practical way to apply authenticated access control to both 802.1X-capable users and devices that lack 802.1X client capability. Huawei's enterprise documentation resources are available through the Huawei Enterprise Documentation portal; the underlying port-based access-control framework is defined by IEEE 802.1X.

QUESTION NO: 19

Agile Controller-Campus The system can manage the software installed on the terminal, define the black and white list of software, and assist the terminal to install necessary software and uninstall the software that is not allowed to be installed by linking with the access control equipment,Regarding the definition of black and white lists, which of the following statements is correct?

A. Check for prohibited software licenses and sub-licensed software

B. Check for prohibited software

C. Check for prohibited software and software that must be installed

D. Check the software that must be installed

ANSWER: C

Explanation:

Check for prohibited software and software that must be installed is correct because Agile Controller-Campus endpoint software management uses two complementary policy categories. A blacklist identifies software that is not permitted on managed terminals. When access-control linkage and endpoint management are applied, detection of such software can trigger the configured handling process, including requiring its removal. A whitelist, in this context, identifies required or approved software that a terminal must have installed to satisfy the organization's endpoint security and operational requirements. The controller can therefore assess both conditions during endpoint compliance management: whether disallowed applications are present and whether mandatory applications are installed. This combined check supports a complete software-compliance posture rather than merely identifying one class of software. It is particularly useful for ensuring terminals have required enterprise security agents, business applications, or other mandated tools while preventing the use of unauthorized applications. Huawei's enterprise support portal provides product documentation and software-management resources for campus-network management products at Huawei Enterprise Support. Huawei's campus network product information, including centralized management capabilities, is available at Huawei Campus Network.

QUESTION NO: 20

Hardware in useSACG At the time of certification,SACG After the configuration is completed, you can seeSACG andAgile Agile Controller-Campus The linkage is successful, but the user authentication fails. This phenomenon may be caused by the following reasons? (Multiple choice)

A. User flow has not passed SAC

B. SACG has not permitted the user traffic.

C. State detection has not been disabled on the SACG.

D. Agile Controller-Campus On and SACG Wrong key configuration for linkage

ANSWER: B C

Explanation:

“SACG has not permitted the user traffic” is a valid cause because successful controller linkage verifies that the SACG can communicate with Agile Controller-Campus, but user authentication also requires the user’s actual authentication and redirected traffic to be allowed through the SACG. If the applicable traffic-release policy is absent, the user’s authentication exchange cannot complete even though the management-plane connection is healthy.

“State detection has not been disabled on the SACG” is also a valid cause in this linkage deployment. The SACG must use the state-detection behavior required for the controller-integrated authentication service; leaving state detection enabled can cause the gateway to handle or validate authentication-related flows in a way that prevents the expected controller-driven authentication process. Therefore, both user-flow release and the prescribed state-detection setting must be checked independently of the displayed linkage status. Huawei’s enterprise support portal provides product documentation and configuration guidance for SACG and campus-controller interoperability: Huawei Enterprise Support. Huawei’s documentation finder is also available for locating the relevant SACG software-version configuration guide: Huawei Info-Finder.

QUESTION NO: 21

Which of the following statement is correct about Policy Center system client function?

A. NAC Agent support MAC account login.

B. Web page login for authentication and can perform checks Strategy.

C. Web Agent login for identity certification and security certification.

D. NAC Agent cannot be installed on Windows Vista operating system.

ANSWER: A

Explanation:

NAC Agent support MAC account login. In Huawei Policy Center’s network-access-control workflow, the NAC Agent is an endpoint client used to submit authentication information and cooperate with access-control policy enforcement. A MAC account is an account form based on the endpoint’s MAC address, allowing the system to identify and authenticate a terminal by using that address as the account credential. This is useful where administrators want a simplified onboarding or identification method for managed endpoints while retaining centralized policy control. The client obtains the relevant local terminal information, uses the configured authentication method, and communicates with the access-control system so that the user or endpoint can be assigned the appropriate network-access result. Huawei’s campus access-control solutions combine endpoint identity, access authentication, and centralized policy enforcement; MAC-address-based identification is one supported identity mechanism in such deployments. The Policy Center client capability therefore includes support for MAC account login. See Huawei’s campus network solution overview and the Huawei enterprise documentation portal for product documentation and configuration guidance.

QUESTION NO: 22

Which of the following files can the sandbox detect? (multiple choice)

A. Web page files and PE files

B. Mail

C. Picture file

ANSWER: A B C

Explanation:

Huawei sandboxing is designed to identify advanced threats by obtaining suspicious objects from several security-inspection channels and executing or analyzing them in an isolated environment. This scope includes web-delivered content, executable content such as PE files, email-borne objects, and image files. Web page files can carry malicious scripts, exploit content, or links that lead to malicious payloads, while PE files are a primary format for Windows malware and can be observed during execution for behaviors such as process creation, persistence, network communication, and file modification.

Email is also a relevant sandbox inspection source because malicious campaigns commonly deliver harmful attachments or embedded content through messages. Picture files can be submitted for inspection as well, particularly where malformed image content, embedded payloads, or exploitation attempts are suspected. The sandbox's value is not limited to a file-name extension; it combines static analysis, dynamic execution where applicable, and threat-intelligence correlation to determine whether an inspected object is malicious. Huawei describes its cloud sandbox capability as providing advanced-threat detection through multi-dimensional analysis and integration with security devices. See Huawei Cloud Sandbox and Huawei Enterprise Security solutions.

QUESTION NO: 23

Regarding the mail content filtering configuration of Huawei USG6000 products, which of the following statements is wrong?.

A. Mail filtering will only take effect when the mail filtering configuration file is invoked when the security policy is allowed.

B. When a POP3 message is detected, if it is judged to be an illegal email, the firewall's response action only supports sending alarm information, and will not block the email.

C. When an IMAP message is detected, if it is judged to be an illegal email; the firewall's response action only supports sending alarm messages and will not block the email.

D. The attachment size limit is for a single attachment, not for the total size of all attachments.

ANSWER: B

Explanation:

"When a POP3 message is detected, if it is judged to be an illegal email, the firewall's response action only supports sending alarm information, and will not block the email." is the incorrect statement. For POP3 mail-content inspection on Huawei USG6000 firewalls, the response to a mail that matches a configured illegal-content condition is not limited to generating an alert. The mail-filtering profile can apply a blocking response, preventing delivery of the matching mail content to the POP3 client, in addition to producing a log or alarm event as configured. This behavior is significant because POP3 is commonly used to download messages from a mail server, and content filtering must be able to enforce the organization's mail-security policy at the firewall rather than merely report a detected violation. The exact available actions and configuration fields can vary with the USG software release, so the applicable product version's Content Security or Configuration Guide should be consulted when implementing the policy. Huawei's enterprise support documentation portal provides the version-specific guides and command references: Huawei Enterprise Documentation. Product family and security-feature information is also available at Huawei Firewall Products.

QUESTION NO: 24

A network adopts 802. 1X To authenticate access users, the access control equipment is deployed at the convergence layer, and after the deployment is completed, it is used on the access control equipment t-aa The command test is successful, but the user cannot access the network. The failure may be caused by the following reasons? (Multiple choice)

A. The aggregation layer device is not configured RADIUS Certification template.

B. Agile Controller-Campus The switch is not added on NAS equipment.

C. Connect to the terminal on the device to open 802.1X Function.

D. The Layer 2 link is used between the access device and the aggregation device, and it is not turned on 802 Instrument transparent transmission function

ANSWER: B C D

Explanation:

“Agile Controller-Campus The switch is not added on NAS equipment.” is a valid cause because the controller/RADIUS service must identify the network access server that sends the live 802.1X authentication request. A successful `test-aaa` confirms basic reachability and the configured AAA credentials from the aggregation device, but it does not by itself ensure that the controller authorizes that device as a managed NAS for actual user access requests. “Connect to the terminal on the device to open 802.1X Function.” is also required: the endpoint-facing access port must have 802.1X enabled so that it can initiate EAP authentication and remain controlled until authorization succeeds. Where authentication enforcement is located at the aggregation layer and the endpoint connects through a Layer 2 access switch, “The Layer 2 link is used between the access device and the aggregation device, and it is not turned on 802 Instrument transparent transmission function” can prevent EAPOL/802.1X frames from reaching the enforcement device. Therefore, 802.1X transparent transmission must be enabled across that Layer 2 path. These requirements align with the NAS role defined for IEEE 802.1X/RADIUS deployments and Huawei enterprise campus access-control guidance. See RFC 3580 and the Huawei Enterprise Support portal.

QUESTION NO: 25

Visitors refer to users who need temporary access to the network at a specific location.

A. True

B. False

ANSWER: A

Explanation:

True is correct. In Huawei campus and wireless-access scenarios, visitors (also commonly called guests) are users who are not regular internal users of the organization but require network connectivity for a limited period. Their access is typically associated with a particular physical site, such as an office, branch, campus, meeting room, reception area, or venue. This definition supports the practical purpose of visitor access: providing controlled, temporary connectivity to people such as customers, partners, contractors, and event attendees without treating them as permanent enterprise users.

Visitor access is generally implemented through a separate guest or visitor access policy, allowing the organization to define the applicable access duration, authentication method, permitted network resources, and Internet-access controls for that location. Huawei’s enterprise campus networking materials describe campus networks as supporting differentiated connectivity and policy control for distinct user groups, including guest users. Huawei’s support portal provides product documentation and configuration guidance for these access-control capabilities: Huawei Enterprise Support. Huawei’s campus-network solution overview also describes policy-based, scenario-oriented network access services: Huawei Campus Network.

QUESTION NO: 26

What are the three main steps of business free deployment? (Multiple choice)

A. Define security group

B. Define and deploy group policies

C. The system runs automatically

D. Security group reported by the system

E. Define user groups

ANSWER: A B C

Explanation:

Business free deployment uses a group-based policy model rather than requiring administrators to configure a separate rule manually for each individual user or endpoint. The workflow begins with **Define security group**, which establishes the security classification and identifies the protected objects to which access controls will apply. The administrator then performs **Define and deploy group policies**, associating the required access-control policy with the relevant source and destination security groups. This makes the intended business access relationship explicit and reusable.

After the groups and group policies have been configured, **The system runs automatically** describes the automated enforcement stage. The management system translates the group-based policy relationships into the required device-side controls and maintains policy enforcement as group membership or endpoint location changes. This is the key benefit of the model: policy is centered on security groups and business intent, allowing consistent automated deployment instead of repeated per-device rule configuration. Huawei documentation similarly describes security groups as logical collections to which common access rules are applied and managed. See Huawei Cloud Security Group overview and Huawei Cloud security-group rule documentation.

QUESTION NO: 27

USG6000V software logic architecture is divided into three planes: management plane, control plane and

A. Configuration plane

B. Business plane

C. Log plane

D. Data forwarding plane

ANSWER: D

Explanation:

The correct completion is **Data forwarding plane**. The USG6000V virtual firewall uses a layered software architecture that separates management, control, and packet-processing responsibilities. The management plane provides administrative access and supports activities such as configuration, monitoring, and maintenance. The control plane processes protocol and policy-control information, establishes the information required for services, and coordinates how traffic should be handled. The data forwarding plane performs the high-volume, real-time processing of service traffic. It receives packets and applies the established forwarding and security-processing decisions, including firewall policy enforcement, session handling, NAT, and other enabled security services. This separation lets the device preserve efficient traffic forwarding while management and control functions operate independently. Huawei's USG documentation describes the product as a next-generation firewall platform with integrated security and traffic-forwarding capabilities; the logical division is foundational to understanding how those functions are implemented in a virtualized USG6000V deployment. See Huawei's USG6000V documentation portal and the Huawei Security Configuration Guide documentation for product architecture and operational documentation.

QUESTION NO: 28

Regarding intrusion detection I defense equipment, which of the following statements are correct? (multiple choice)

A. It cannot effectively prevent the virus from spreading from the Internet to the intranet.

B. The number of applications that NIP6000 can recognize reaches 6000+, which realizes refined application protection, saves export bandwidth, and guarantees key business services

C. Protect the intranet from external attacks, and inhibit malicious flows, such as spyware, worms, etc. from flooding and spreading to the intranet.

D. Ability to quickly adapt to threat changes

ANSWER: B C D

Explanation:

Intrusion detection and prevention equipment is deployed at network boundaries or critical internal segments to identify application traffic, detect known attack patterns and malicious behavior, and enforce blocking or mitigation policies in real time. “The number of applications that NIP6000 can recognize reaches 6000+, which realizes refined application protection, saves export bandwidth, and guarantees key business services” describes the application-awareness capability associated with Huawei NIP products: recognizing applications enables differentiated control and protection policies, prioritizing important services and reducing unnecessary bandwidth use. “Protect the intranet from external attacks, and inhibit malicious flows, such as spyware, worms, etc. from flooding and spreading to the intranet.” accurately reflects IPS protection goals. By inspecting traffic and applying signatures, reputation intelligence, and behavior-based detection, the device can stop or contain malicious traffic before it reaches protected internal assets. “Ability to quickly adapt to threat changes” is also essential because threat-defense systems require continuously updated threat intelligence, signatures, and detection mechanisms to respond to newly discovered vulnerabilities and changing attack techniques. Huawei’s IPS documentation describes its role in detecting and defending against network attacks, while Huawei’s product information outlines application identification and intelligent threat-defense capabilities. See Huawei IPS documentation and Huawei Intrusion Prevention System.

QUESTION NO: 29

Configure the following commands on the Huawei firewall:

[USG] interface G0/0/1

[USG] ip urpf loose allow-defult-route acl 3000

Which of the following options are correct? (multiple choice)

A. For loose inspection, if the source address of the packet exists in the FIB of the firewall, the packet passes the inspection directly.

B. When a default route is configured but the parameter allow-defult-route is not configured, if the source address of the packet does not exist in the firewall FIB table, the packet will be rejected.

C. When a default route is configured and the parameter allow-defult-route is configured, if the source address of the packet does not exist in the firewall FIB table, all packets will pass the URPF check and be forwarded normally in loose check mode.

D. When a default route is configured and the parameter allow-defult-route is configured, if the source address of the packet does not exist in the firewall FIB table, the packet cannot pass the URPF check in loose check mode.

ANSWER: A B C

Explanation:

Loose uRPF validates a packet by looking up its source address in the firewall forwarding information base (FIB). When a usable route to that source exists, loose-mode validation succeeds; it does not require that the route’s outbound interface be the same interface on which the packet arrived. Thus, the statement that a source address existing in the FIB passes loose inspection is correct.

A default route is not used as uRPF validation evidence unless `allow-default-route` is configured. Therefore, where a default route exists but that parameter is absent, packets whose source addresses have no more-specific FIB route fail the uRPF lookup and are discarded. With `allow-default-route` configured, the default route may satisfy the loose uRPF lookup. Consequently, if the FIB contains a default route, even source addresses without a specific route can be validated through that default route, so packets subject to this loose uRPF policy pass the check. The ACL identifies the traffic to which the configured uRPF policy is applied; it does not change the fundamental loose-mode route-lookup behavior. Huawei describes uRPF as a mechanism for source-address validation and anti-spoofing protection in its security configuration documentation. The underlying loose-versus-strict reverse-path validation model is also defined in RFC 3704.

QUESTION NO: 30

Regarding the enhanced mode in HTTP Flood source authentication, which of the following descriptions are correct? Multiple choices

A. Enhanced mode refers to the authentication method using verification code.

B. Some bots have a redirection function, or the free proxy used during the attack supports the redirection function, which leads to the failure of the basic mode of defense; enhanced mode can effectively defend.

C. The enhanced mode is superior to the basic mode in terms of user experience.

D. Enhanced mode supports all HTTP Flood source authentication fields.

ANSWER: A B

Explanation:

“Enhanced mode refers to the authentication method using verification code.” is correct because enhanced HTTP Flood source authentication presents a verification-code challenge to distinguish legitimate interactive users from automated attack clients. A client that successfully completes the challenge demonstrates that it can process the page and submit the required verification information, allowing the firewall to identify a valid source more reliably before permitting subsequent access.

“Some bots have a redirection function, or the free proxy used during the attack supports the redirection function, which leads to the failure of the basic mode of defense; enhanced mode can effectively defend.” is also correct. Basic source authentication relies on a redirect-based interaction, so attack tools or proxy services that follow redirects can make that mechanism less effective as a discriminator. The verification-code interaction in enhanced mode adds a human-oriented challenge that is substantially more resistant to automated redirect handling, improving protection when HTTP flood traffic is generated through redirect-capable bots or proxies.

Huawei’s security documentation is published through the Huawei Enterprise Support portal and the Huawei product documentation portal, where HTTP flood defense and source-authentication behavior are documented by product and software version.

QUESTION NO: 31

According to the different user name format and content used by the access device to verify user identity, the user name format used for MAC authentication can be changed.

There are three types. Which of the following formats is not included?

A. MAC Address format

B. Fixed username form

C. DHCP Option format

D. ARP Option format

ANSWER: D

Explanation:

ARP Option format is not a Huawei MAC-authentication user-name format. In MAC authentication, the access device derives or assigns the user name that it submits for identity verification according to the configured user-name mode. Huawei supports using the terminal's MAC address as the user name, using a fixed user name, or obtaining the user name from DHCP option information. These modes allow the device to send an identity acceptable to the configured RADIUS server or other authentication backend while associating access control with the endpoint's MAC address.

ARP is used to resolve an IPv4 address into a link-layer MAC address on a local network. Although the device can maintain ARP entries as part of normal IP forwarding, ARP option data is not defined as a selectable source or formatting mode for the MAC-authentication user name. Therefore, it is not one of the three listed MAC-authentication user-name formats. Huawei's enterprise support documentation includes configuration and feature references for access authentication, including MAC authentication: Huawei Enterprise Documentation. Huawei's support portal also provides product-specific VRP configuration guides and command references: Huawei Enterprise Support.

QUESTION NO: 32

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. The traffic undergoes decryption, threat detection, and re-encryption.

ANSWER: D

Explanation:

The traffic undergoes decryption, threat detection, and re-encryption. This describes the SSL/TLS encrypted-traffic inspection workflow used by an intrusion prevention system when SSL threat detection is enabled and the device is deployed with the necessary certificate and traffic-forwarding configuration. Since the payload of an SSL/TLS session is encrypted, the NIP6000 must first establish visibility into the protected content by decrypting the applicable traffic. It can then apply its intrusion-prevention and threat-detection capabilities to the clear-text payload, including inspection for attacks, malware characteristics, or policy violations. Before forwarding permitted traffic, it re-encrypts the traffic so that encryption protection is maintained on the relevant network segment and the server-side connection remains protected. This workflow allows organizations to retain the confidentiality benefits of TLS while avoiding a monitoring blind spot created by encrypted application traffic. SSL inspection must be planned carefully because it requires trusted certificate handling and policies that define which encrypted sessions are inspected. Huawei identifies NIP appliances as network-security products providing intrusion prevention and threat detection; see the Huawei NIP product information. The TLS protocol's use of encryption to protect application data is specified in RFC 8446.

QUESTION NO: 33

Which of the following options is about Portal The description of the certification process is correct?

A. Portal The certification process is only used in Web Certification

B. Server for a terminal Portal Certification will only give one Portal Device sends authentication message

C. After the switch receives a Portal authentication request, it sends a RADIUS authentication request to the RADIUS server.

D. Portal The authentication message will not carry the result of the security check

ANSWER: C

Explanation:

“After the switch receives a Portal authentication request, it sends a RADIUS authentication request to the RADIUS server” correctly describes the key interaction in Huawei Portal authentication. A user first accesses the network and is redirected to the Portal page, where credentials or other identity information are collected. The Portal server then submits a Portal authentication request to the access device, such as the switch. Acting as the RADIUS client, the switch constructs and sends a RADIUS Access-Request to the configured RADIUS server. The RADIUS server validates the user and returns the authentication result, allowing the access device to apply the appropriate authorization and online-access policy. This division of responsibility is fundamental: the Portal server provides the web-based user interaction, while the access device controls network access and communicates with the RADIUS server for AAA processing. Huawei’s Portal documentation can be located through the Huawei Enterprise Support Portal authentication search. The RADIUS Access-Request/Access-Accept exchange used by the switch is defined in RFC 2865.

QUESTION NO: 34

For the convenience of visitors, different authentication and master pages can be distributed for different visitors. When configuring the push page strategy, different matching conditions need to be defined, so which of the following options can be used as the limited matching conditions? (Multiple choice)

A. Terminal P address

B. Location information of the access device

C. Priority of guest accounts

D. Connected to the network SSID'

ANSWER: A B D

Explanation:

A portal push-page strategy uses terminal and access-context attributes to select the appropriate authentication page or portal home page for a visitor. A terminal IP address is a valid restriction condition because it identifies the client’s network segment or assigned address scope, allowing differentiated portal presentation for terminals in specified IP ranges. Location information of the access device is also a valid condition: administrators can associate a visitor’s access with the physical or logical location of the device through which the visitor connects, such as a branch, floor, or site. This enables location-specific content and authentication experiences. The connected network SSID is likewise a valid condition because the SSID identifies the WLAN service set used by the visitor; separate guest, employee, event, or partner SSIDs can therefore receive separate pages. These criteria support targeted portal delivery before or during authentication and are appropriate for matching a push-page policy. Huawei’s enterprise documentation resources for WLAN and portal-access configuration are available through Huawei Enterprise Support and the Huawei documentation portal.

QUESTION NO: 35

For the description of the principles of HTTP Flood and HTTPS Flood blow defense, which of the following options are correct? (multiple choice)

A. HTTP Flood defense modes include basic mode, enhanced mode and 302 redirection.

B. HTTPS Flood defense can perform source authentication and limit the request rate of packets.

C. The principle of HTTP Flood attack is to request URIs involving database operations or other URIs that consume system resources, causing server resource consumption.
Failed to respond to normal requests.

D. The principle of HTTPS Flood attack is to initiate a large number of HTTPS connections to the target server, causing the server resources to be exhausted and unable to respond to regular requests.
begging.

ANSWER: A B C D

Explanation:

HTTP Flood and HTTPS Flood are application-layer denial-of-service attacks, but their resource-exhaustion mechanisms differ. “HTTP Flood defense modes include basic mode, enhanced mode and 302 redirection” is correct: basic defense applies request-rate controls, enhanced defense adds client/source verification, and 302 redirection can be used to distinguish normal clients from automated attack traffic. “HTTPS Flood defense can perform source authentication and limit the request rate of packets” is also correct. HTTPS Flood mitigation combines request-rate controls with source authentication; inspection and protection of encrypted web traffic require the firewall to process the HTTPS service traffic according to the configured protection policy. “The principle of HTTP Flood attack is to request URIs involving database operations or other URIs that consume system resources” correctly describes application-request flooding against costly dynamic resources. “The principle of HTTPS Flood attack is to initiate a large number of HTTPS connections to the target server” correctly describes exhaustion caused by large volumes of SSL/TLS connection establishment and associated cryptographic processing. Huawei firewall documentation is available through the Huawei Enterprise Documentation portal; Huawei’s security product resources are also available from the Huawei Security product page.

QUESTION NO: 36

In the WLAN wireless access scenario, which of the following network security technologies belong to user access security? (Multiple choice)

A. AP Certification

B. Link authentication

C. User access authentication

D. data encryption

ANSWER: B C D

Explanation:

In a WLAN, user access security protects the process by which a wireless terminal joins the network and protects traffic after access is granted. **Link authentication** is part of this protection because it establishes authentication at the wireless link layer between the station and WLAN infrastructure. Depending on the deployed WLAN security mode, this can involve mechanisms such as IEEE 802.11 authentication and the key-establishment procedures associated with protected wireless access.

User access authentication is also user access security because it verifies the identity or authorization of the person or endpoint requesting network service. Huawei WLAN deployments can apply methods such as 802.1X, MAC-address authentication, or Portal authentication, often using an AAA server to make authorization and accounting decisions.

data encryption completes the access-security protections by providing confidentiality for user data carried over the WLAN radio link. Encryption keys are derived or negotiated as part of the applicable WLAN security process and are used to prevent unauthorized parties from reading protected wireless frames. Together, link authentication, user access authentication, and encryption secure association, identity validation, and transmitted user data. Huawei WLAN security documentation is available through the Huawei WLAN Product Documentation and the Huawei WLAN Configuration Documentation.

QUESTION NO: 37

Which of the following measures can reduce the risk of ARP spoofing attacks on a LAN? (multiple choice)

A. Dynamic ARP inspection

B. IP-MAC binding

C. VLAN segmentation

D. Increase the DNS TTL

ANSWER: A B C

Explanation:

Dynamic ARP inspection, IP-MAC binding, and VLAN segmentation are valid measures. Dynamic ARP inspection validates ARP packets against trusted bindings and can discard invalid ARP replies. IP-MAC binding restricts the relationship between an IP address and a MAC address, reducing the ability of an attacker to impersonate another host through forged ARP information. VLAN segmentation limits the Layer 2 broadcast domain, thereby reducing the scope in which an ARP spoofing attack can affect hosts. Increasing the DNS TTL does not validate ARP packets or prevent a host ARP cache from being poisoned. ARP is defined in RFC 826.

QUESTION NO: 38

Regarding the network intrusion detection system (NIDS), which of the following statements is wrong?

A. It is mainly used for real-time monitoring of the information of the critical path of the network, listening to all packets on the network, collecting data, and analyzing suspicious objects

B. Use the newly received network packet as the data source;

C. Real-time monitoring through the network adapter, and analysis of all communication services through the network;

D. Used to monitor network traffic, and can be deployed independently.

ANSWER: B

Explanation:

“Use the newly received network packet as the data source;” is the wrong statement because it describes the NIDS data source too narrowly. A network IDS is not defined by processing only newly received packets. It passively observes traffic at a selected network location, generally through a TAP, SPAN/port-mirroring session, or another monitoring interface. The sensor can inspect traffic flowing in either direction across that observation point and uses the captured packet stream, including headers and, where supported, payloads and reconstructed sessions, for detection analysis. The essential NIDS characteristic is visibility into traffic traversing the monitored network segment, rather than reliance on a host’s newly received packets. This distinction matters in deployment: traffic must be copied to the sensor or otherwise made visible, and the NIDS analyzes what it captures without normally being inline in the forwarding path. NIST’s intrusion-detection guidance describes network-based IDS technologies as monitoring network traffic for suspicious activity and identifies packet-level observation as their data-collection method. See NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems and the associated full NIST publication.

QUESTION NO: 39

The process of a browser carrying a cookie to request resources from a server is shown in the following figure. Which of the following steps contains SessionID information in the message?

A. ③④

B. ①③④

C. ⑤⑥

D. ②④

ANSWER: A

Explanation:

The correct answer is ③④. In a cookie-based session mechanism, the server first creates or obtains a session identifier and communicates that identifier to the browser in an HTTP response, normally using the `Set-Cookie` response header. This is represented by step ③, whose message includes the SessionID as cookie data. The browser stores the cookie according to its attributes, such as its scope, lifetime, Secure flag, and HttpOnly flag.

When the browser subsequently requests a protected or session-aware resource, it returns the stored cookie in the HTTP request's `Cookie` header. This is represented by step ④, so that message also contains the SessionID. The server can then use the received identifier to locate the associated server-side session state and process the request in the context of that session. This request/response handoff is the fundamental cookie session flow: the response delivers the session cookie, and later requests present it back to the server. RFC 6265 defines the `Set-Cookie` and `Cookie` header behavior: RFC 6265. For secure session-ID handling practices, see the OWASP Session Management Cheat Sheet.

QUESTION NO: 40

Regarding uninstalling the Agile Controller-Campus in Windows and Linux systems, which of the following descriptions is correct?

A. Use a common account to execute sh uninstall.sh in the Agile Controller/Uninstall directory to start the uninstallation program.

B. Use the root account to execute sh uninstall.sh in the Agile Controller directory to start the uninstallation program. :

C. On the Windows platform, select "Start>All Programs>Huawei>Agile Controller>Server Startup config".

D. On the Windows platform, select "Start>All Programs> Huawei> Agile Controller>Uninstall

ANSWER: D

Explanation:

On the Windows platform, select "Start>All Programs> Huawei> Agile Controller>Uninstall is correct because Agile Controller-Campus installs a dedicated uninstallation entry as part of its Windows program group. Launching that entry starts the product's supported uninstall workflow, which is designed to stop relevant components and remove the installed application in the proper order. This is preferable to manually deleting program files because an application uninstall routine can also process installed services, shortcuts, configuration references, and other resources registered during setup. The menu path is therefore the expected operational method for initiating removal on Windows, subject to the account having the local administrative permissions required by the system. Administrators should also ensure that any required configuration, database, or service information has been backed up according to their organization's change and recovery procedures before beginning removal. Huawei's enterprise support portal is the appropriate source for the version-specific Agile Controller-Campus installation and maintenance documentation, patches, and release notes: Huawei Enterprise Support. Huawei's documentation resources can also be accessed through the enterprise documentation portal: Huawei Enterprise Documentation.

QUESTION NO: 41

Huawei WAF products are mainly composed of front-end execution, back-end central systems and databases. Among them, the database mainly stores the front-end detection rules and black

Whitelist and other configuration files.

A. True

B. False

ANSWER: A

Explanation:

True is correct. In a centrally managed Huawei web application firewall deployment, the front-end execution component is responsible for applying inspection and protection policies to web traffic, while the back-end central system provides centralized administration, policy management, and operational coordination. The database supports this architecture by retaining the policy and configuration data needed for protection, including detection-rule content and blacklist/whitelist information. This persistent storage allows rule sets and access-control lists to be managed consistently and made available to front-end protection nodes, rather than relying only on temporary runtime state. Detection rules define the signatures, matching logic, and protection behavior used to identify attacks against web applications. Blacklists and whitelists are configuration objects that control whether specified sources, destinations, or request characteristics are denied or permitted. Storing these items in the database is therefore essential for centralized maintenance, recovery, synchronization, and controlled policy updates across the WAF system. Huawei's security product information describes WAF as a solution for protecting web applications and managing web attack defenses; see Huawei Web Application Firewall and Huawei's WAF product documentation.

QUESTION NO: 42

Network attacks are mainly divided into two categories: single-packet attacks and streaming attacks. Single-packet attacks include scanning and snooping attacks, malformed packet attacks, and special reports.

Wen attack.

A. True

B. False

ANSWER: A

Explanation:

True is correct. Huawei firewall attack-defense materials classify network attacks by whether identification requires an individual packet or traffic state across a flow. Single-packet attacks can be detected by inspecting the fields, protocol conformance, flags, lengths, and other characteristics of one packet. This category includes reconnaissance behavior such as scanning and snooping, malformed-packet attacks that violate expected protocol formats, and special-packet attacks. The phrase "special reports" in the question is evidently a translation issue for special packets, but it does not change the intended classification. In contrast, stream attacks require the firewall to track session or traffic-stream behavior over time, because no single packet alone necessarily identifies the attack. This distinction is foundational to firewall attack-defense capabilities: packet-level inspection handles anomalies visible immediately, while stateful analysis is needed for attacks expressed through a sequence of packets. Huawei's enterprise security documentation and firewall product materials describe these attack-defense and stateful inspection capabilities; see Huawei Enterprise Support and Huawei Network Security.

QUESTION NO: 43

A network adopts 802. 1X To authenticate access users, the access control equipment is deployed at the convergence layer, and after the deployment is completed, it is used on the access control equipment t-aa The command test is successful, but the user cannot access the network. The failure may be caused by the following reasons? (Multiple choice)

A. The aggregation layer device is not configured RADIUS Certification template.

B. The switch is not added as a NAS device on Agile Controller-Campus.

C. The terminal connected to the device has not enabled the 802.1X function.

D. The Layer 2 link is used between the access device and the aggregation device, and the 802.1X transparent transmission function is not enabled.

ANSWER: B C D

Explanation:

A successful `test-aaa` result verifies that the access-control device can communicate with the AAA/RADIUS service using the configured test parameters, but it does not prove that an actual user's EAPOL authentication exchange can reach the authenticator and be accepted by the controller. The switch must be added as a NAS device on Agile Controller-Campus so that the controller recognizes the source NAS and can apply the appropriate authentication and authorization policy to live access requests. The endpoint also needs an enabled and correctly configured 802.1X supplicant; this component initiates EAPOL authentication and supplies the user or device credentials. Without it, an 802.1X-protected port cannot complete normal user authentication. In a centralized deployment where the access device and aggregation-layer access-control device are separated by a Layer 2 path, the intermediate access device must enable 802.1X transparent transmission (EAPOL passthrough). This preserves the Layer 2 EAPOL frames between the endpoint and the actual authentication device, allowing the complete 802.1X exchange to occur. Huawei's enterprise documentation portal provides configuration guidance for access authentication and NAC features: Huawei Enterprise Support. Huawei also describes its Campus Network and access-control capabilities at Huawei Campus Network.

QUESTION NO: 44

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, then spread laterally or use the infected device to attack other network resources. "Some viruses can be used as intrusion tools, such as Trojan horse viruses," is also correct: a Trojan commonly masquerades as legitimate content and can establish unauthorized remote access, execute attacker commands, download additional malicious payloads, or steal credentials. "Control the host computer's accumulated limit and the user's data, and some viruses may even cause damage to the host's hardware." describes the potential loss of control over a system and its information. Malware can alter, encrypt, delete, or exfiltrate user data, consume computing resources, and destabilize systems. In exceptional cases, malicious code can also manipulate firmware or hardware operating conditions, creating physical-device risk. These impacts are why enterprise security designs use layered controls, including file and malware inspection at the network boundary, endpoint protection, timely signature or intelligence updates, and isolation of infected hosts. Huawei's firewall portfolio provides security-inspection capabilities intended to help identify and block network threats, while CISA describes malware as software that can disrupt operations and compromise systems and data. See Huawei Firewall and CISA: Malware.

QUESTION NO: 45

About the hardware SACG Certification deployment scenarios, which of the following descriptions are correct? (Multiple choice)

A. SACG Authentication is generally used in scenarios where a stable network performs wired admission control.

B. SACG Authentication is generally used in scenarios where new networks are used for wireless admission control.

C. SACG It is generally deployed in a bypass mode without changing the original network topology.

D. SACG Essentially through 802.1X Technology controls access users.

ANSWER: A B C

Explanation:

Hardware SACG authentication is intended to provide centralized access admission while fitting different existing or newly constructed network environments. “SACG Authentication is generally used in scenarios where a stable network performs wired admission control.” is correct because SACG can be introduced to enforce admission for wired users in an established campus network without requiring a wholesale redesign of the access network. “SACG Authentication is generally used in scenarios where new networks are used for wireless admission control.” is also correct: in a new wireless deployment, the wireless infrastructure and SACG can be planned together so that user access is admitted through the centralized authentication and policy-control design. “SACG It is generally deployed in a bypass mode without changing the original network topology.” is correct because bypass deployment is a core practical deployment approach for an access-control gateway: traffic can be steered through the device for authentication and authorization while preserving the original network’s main forwarding topology. This allows organizations to introduce access admission with limited disruption, while retaining their current network structure. Huawei’s enterprise security portfolio and product documentation describe SACG as an enterprise access-control/security gateway solution; see the Huawei enterprise network security portfolio and the Huawei Enterprise Support documentation portal for product documentation and deployment guidance.

QUESTION NO: 46

Regarding HTTP behavior, which of the following statements is wrong?

A. HTTP POST is generally used to send information to the server through a web page, such as forum posting x form submission, username I password login.

B. When the file upload operation is allowed, the alarm threshold and blocking threshold can be configured to control the size of the uploaded file.

C. When the size of the uploaded or downloaded file and the size of the content of the POST operation reach the alarm threshold, the system will generate log information to prompt the device management
And block behavior.

D. When the uploaded or downloaded file size, POST operation content size reaches the blocking threshold, the system will only block the uploaded or downloaded file, POST
operate.

ANSWER: C

Explanation:

“When the size of the uploaded or downloaded file and the size of the content of the POST operation reach the alarm threshold, the system will generate log information to prompt the device management
And block behavior.” is the wrong statement because an alarm threshold is intended to provide visibility, not enforcement. In Huawei firewall HTTP behavior control, file-transfer and POST-content size monitoring can use an alarm threshold to generate a log event when the configured size is reached. This alerts the administrator to a potentially abnormal or policy-relevant transfer while allowing the HTTP transaction to continue. Enforcement occurs only when the configured blocking threshold is reached; at that point, the firewall terminates or prevents the applicable upload, download, or POST operation. Keeping alarm and blocking thresholds separate lets an administrator monitor emerging risks and tune policy before traffic is actively denied. HTTP POST is the request method commonly used by web applications to submit data to a server, as defined by the HTTP semantic model in RFC 9110. Huawei’s firewall product capabilities, including application-layer traffic inspection and policy enforcement, are described on the Huawei Firewall product page.