PassQueen
a.k.a dumpsqueen.com

Huawei Certified ICT Professional - Constructing Terminal Security System

Huawei H12-723

Version Demo

Total Demo Questions: 24

Total Premium Questions: 244

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Regarding the policy for checking account security, which of the following descriptions are correct? (Multiple choice)

A. You can check whether there is a weak password.

B. You can check whether the account has joined a specific group.

C. It cannot be repaired automatically._

D. It is not possible to check whether the password length meets the requirements.

ANSWER: A B C

Explanation:

Account-security checking is intended to identify risky account configurations before they become an access-control weakness. It can inspect accounts for weak passwords, including passwords that do not satisfy configured password-complexity requirements. Password length is one of the core complexity attributes that can be assessed as part of this check. The checking policy can also verify whether an account belongs to a specified user group, which is important because group membership commonly controls an account's authorized roles, privileges, and service access. These inspections provide administrators with visibility into password and authorization risks so that they can make deliberate corrections under their organization's account-management procedures.

The check itself is an inspection mechanism rather than an automatic remediation mechanism. Consequently, detected account-security issues must be repaired by an administrator, such as by changing the affected password or adjusting the account's group membership. This approach preserves administrative control over credentials and authorization assignments, avoiding unplanned changes to operational accounts. Huawei's enterprise support resources provide product documentation and security-maintenance guidance at Huawei Enterprise Support; Huawei's broader security and trust practices are available at Huawei Trust Center.

QUESTION NO: 2

Which of the following series of devices does not support the function of accompanying business?

A. S5720HI Series Switch:

B. AR Series router

C. USG6000 Series firewall

D. SVN5600 series

ANSWER: B

Explanation:

AR Series router is the correct answer. In Huawei's Constructing Service Security Network context, "accompanying business" refers to the capability for security services and policies to follow a user or service as its access location changes. This requires integration with the solution's identity-, policy-, and security-service orchestration mechanisms, rather than merely basic routing and forwarding. The listed campus-switch, firewall, and security-virtualization product families are used as access, policy-enforcement, or virtualized security-service components in this architecture. The AR series is primarily positioned as an enterprise routing and WAN-access platform, and it is not listed as a device series providing the accompanying-business function in this solution's supported-device scope. Therefore, the appropriate selection is **AR Series router**.

Huawei's campus networking portfolio describes the roles of campus switches in access and policy-based networking, while its security portfolio describes firewall platforms as security-policy enforcement points. These product roles provide the

architectural context for distinguishing the routing platform from devices supporting accompanying security services. See Huawei's campus switch portfolio and firewall portfolio.

QUESTION NO: 3

Which of the following options is correct for the description of the role of the isolation domain?

A. Isolation domain refers to the area that the terminal host can access before passing the identity authentication, such as DNS server, external authentication source, business controller (SC)c The area where the service manager (SM) is located.

B. Isolation domain refers to the area that is allowed to be accessed when the terminal user passes the identity authentication but fails the security authentication, such as patch server, virus database server. The area where the server is located.

C. Isolation domain refers to the area that terminal users can access after passing identity authentication and security authentication, such as ERP system, financial system database system. The area where you are.

D. End users can access the isolated domain regardless of whether they pass identity authentication.

ANSWER: B

Explanation:

An isolation domain is the restricted remediation network used by Huawei endpoint-access/NAC designs when a user has successfully completed identity authentication but does not meet the required security posture or security-authentication conditions. Its purpose is to keep the endpoint separated from normal production services while still providing only the resources needed to repair the detected compliance issue. Therefore, access to services such as patch servers and antivirus or virus-definition database servers is permitted, enabling the terminal to obtain updates, install required patches, or correct its security status. Once the endpoint becomes compliant and passes the relevant security checks, access control can move it into the appropriate authorized service-access domain. This staged access model prevents a potentially insecure device from reaching business systems while preserving a practical path for self-remediation. Huawei's enterprise support portal provides product documentation and configuration guidance for campus access-control and endpoint-admission solutions: Huawei Enterprise Support. Huawei's campus-networking portfolio also describes the broader campus access-control environment in which these policy-based access domains are deployed: Huawei Campus Network.

QUESTION NO: 4

When a guest needs to access the network through an account, which of the following methods can be used to access? (Multiple choice)

A. Create new account

B. Use existing social media accounts

C. No authentication, no account required

D. Scan public QR code

ANSWER: A B C D

Explanation:

Guest-access solutions can offer several portal and onboarding paths so that visitors can connect using the method appropriate to the venue's security and usability policy. **Create new account** is supported through guest self-registration or administrator-created guest credentials; the resulting account is then used by the access-control system to authorize network access. **Use existing social media accounts** represents social-login authentication, where a portal can use a supported third-party identity as the guest's access identity rather than requiring a separate local password.

No authentication, no account required is also a valid guest-access mode when the operator chooses an open or authentication-free visitor WLAN. Access can still be associated with WLAN, portal, time, bandwidth, or policy controls even

though no guest account is collected. **Scan public QR code** is a common simplified onboarding flow: scanning the organization's public-account QR code can direct the visitor into the portal or bind the visitor's public-account identity for access authorization. Huawei enterprise WLAN solutions support guest-oriented portal authentication and flexible access policies; see the Huawei Enterprise WLAN overview and Huawei's Enterprise Support documentation portal for product documentation and configuration guidance.

QUESTION NO: 5

Regarding patch management and Windows patch checking strategies, which of the following descriptions is wrong?

A. Patch management and Windows The patch check strategy can check whether the terminal host has installed the specified Windows Make system patches.

B. Windows Patch check strategy focuses on checking whether the terminal host is installed Windows Operating system patches.

C. When the terminal host does not install the specified Windows When making a system patch, according to Windows The patch check policy prohibits terminal hosts from accessing the controlled network.

D. Patch management focuses on checking whether the terminal host has installed the specified patch,Perform access control on the terminal host.

ANSWER: D

Explanation:

"Patch management focuses on checking whether the terminal host has installed the specified patch,Perform access control on the terminal host.

" is the incorrect description because it conflates patch-management functionality with a network-access enforcement policy. Patch management is principally the operational process of identifying required updates, obtaining and deploying approved patches, monitoring installation status, and maintaining endpoint patch compliance. Its purpose is to remediate endpoint vulnerabilities by ensuring that required software updates are applied. Access control based on an endpoint's compliance result is instead performed by the admission-control or endpoint-security policy framework, which can use a Windows patch-check result as a condition when determining whether an endpoint receives normal, restricted, or denied network access. This distinction is important in a Huawei service-security network: patch status is an endpoint-security posture signal, while network admission is an enforcement action applied by the access-control system. Huawei's enterprise access-control solutions integrate endpoint posture information into access decisions; see Huawei Access Controller. For background on the lifecycle and deployment of Windows updates that patch-management processes handle, see Microsoft documentation on managing Windows updates.

QUESTION NO: 6

Which of the statement is not correct according to following configuration?

[USG] pattern-group 6t type url

[USG-pattern-group-url-bt] pattern any bt.com [USG] url-filter policy urlpolicy3

[USG-urlfilter-policy-urlpolicy3] blacklist enable [USG-urlfilter-policy-urlpolicy3] whitelist enable [USG-urlfilter-policy-urlpolicy3] blacklist group 6t [USG] web-filter policy webpolicy3

[USG-web-filter-policy-webpolicy3] policy url-filter urlpolicy3 [USG-policy-interzone-trust-untrust-outbound] policy 3

[USG-policy-interzone-trust-untrust-outbound-3] action permit

[USG-policy-interzone-trust-untrust-outbound-3] policy source range 10.10.10.101 10.10.10.200 [USG-policy-interzone-trust-untrust-outbound-3] policy web-filter webpolicy3

A. users of IP address 10.10.10.120 can access bt.com website

B. users of IP address 10.10.10.199 cannot access bt.com website

C. users of IP address 10.10.10.100 can access bt.com website

D. users of IP address 10.10.10.220 can access bt.com website

ANSWER: A

Explanation:

The statement “users of IP address 10.10.10.120 can access bt.com website” is the incorrect statement. The source address 10.10.10.120 falls within the configured source range of 10.10.10.101 through 10.10.10.200, so security policy 3 matches traffic from that host. This policy applies the web-filter policy named `webpolicy3`.

The web-filter policy invokes URL-filter policy `urlpolicy3`. In that URL-filter policy, blacklist processing is enabled and blacklist group `6t` is referenced. Pattern group `6t` is a URL-type group containing the pattern `bt.com`. Therefore, when the matched user attempts to access the specified domain, the URL matches a blacklist entry and the firewall blocks that web access. The permit action in the security policy permits traffic only subject to the associated web-filter inspection; it does not override a blacklist match.

Huawei’s product documentation and URL-filtering resources are available through the Huawei Enterprise Support URL-filter search and the Huawei Enterprise Documentation portal.

QUESTION NO: 7

The service free mobility function of the Agile Controller can guide the flow to the security center for processing according to the service, improving the utilization of physical equipment.

A. right

B. wrong

ANSWER: A

Explanation:

The statement is correct. Agile Controller’s service free mobility capability uses centralized policy control to identify services and steer their traffic to the required security service chain, such as a firewall, intrusion prevention system, or other security center function. The traffic is directed according to the service and policy requirements rather than being permanently tied to a particular physical security appliance or a fixed, manually designed path. This separation of service policy from the underlying forwarding topology lets the network allocate security-processing resources more flexibly. As service demand changes, traffic can be redirected to available or appropriate security resources, helping avoid rigid physical-device placement and improving the overall use of deployed equipment. This is consistent with Huawei’s intent for controller-driven campus networking: centralized orchestration and policy-based service provisioning simplify operations while allowing network and security resources to be used dynamically. Huawei describes its CloudCampus approach as using centralized management and automation for policy-driven network services; Agile Controller is part of Huawei’s broader controller-based networking evolution. See Huawei’s CloudCampus solution overview and campus network portfolio for the related controller-managed, policy-based networking architecture.

QUESTION NO: 8

The terminal host access control function does not take effect, the following is SACG View information on:

display right- manager role-id rule

Advanced ACL 3099 ,25 rules,not bingding with vpn-instance Ad's step is 1 rule 1000 permit ip (1280 times matched)

rule 1001 permit ip destination 172.18.11.2210 (581 times matched)

rule 1002 permit ip destination 172:18.11.2230 (77 times matched)

rule 1003 permit ip destination 172.19.0.0 0.0 255.255 (355 Book times matched) rule 1004 deny ip (507759 times matched)

Which of the following statements is correct?

A. 172.18.11.221 It is the server of the isolation domain.

B. The escape route was opened.

C. 172.18.11.223 It is a post-domain server.

D. The terminal host stream is the default ACL Blocked.

ANSWER: B

Explanation:

The escape route was opened. The displayed ACL begins with the rule `rule 1000 permit ip`, which is an unrestricted permit rule: it matches IP traffic without specifying a source, destination, protocol, or port restriction. Huawei ACLs evaluate rules in sequence and apply the action of the first matching rule. Consequently, traffic that reaches this ACL can be permitted immediately by rule 1000 rather than being constrained by the intended destination-specific permit entries or the later catch-all deny entry. This explains why terminal-host access control appears not to take effect: the broad permit rule effectively creates an unrestricted path through the policy. The match counter shown for this rule also confirms that traffic has matched it in operation. In a service-access control policy, broad permit entries must be placed only after any required restrictive rules, or they must be narrowed to the exact traffic that should be allowed. Huawei's product documentation and support resources describe ACL configuration and rule processing behavior, including the importance of rule order in traffic classification and filtering: Huawei Enterprise Documentation and Huawei Enterprise Knowledge Base.

QUESTION NO: 9

Regarding RADIUS accounting messages sent by an access device, which of the following descriptions are correct? (Multiple choice)

A. Accounting-Start can be sent when a user session starts.

B. Accounting-Stop can be sent when a user session ends.

C. Interim-Update can report information about an active session.

D. Access-Accept is an accounting message sent by the access device.

ANSWER: A B C

Explanation:

An access device acting as a RADIUS client can send an **Accounting-Start** message when an accounting session begins and an **Accounting-Stop** message when the session ends. These messages enable the RADIUS server to record session start time, end time, duration, user identity, and other accounting information.

The device can also send **Interim-Update** messages during an active session. Interim updates provide periodic accounting information before the session ends, which is useful for online accounting, usage tracking, and auditing. An Access-Accept message is an authentication and authorization response from the RADIUS server; it is not an accounting message sent by the access device. RADIUS accounting is defined in RFC 2866.

QUESTION NO: 10

Which statement is wrong about SA principle configuration?

A. feature detection to identify the different applications by matching message feature and Knowledge Base feature set

B. reduces the maximum number of packets detection threshold, can reduce the sas module identification number of packets, thus improve the recognition rate agreement

C. There are some protocol packets are carried in other agreements, enable sa whole packet inspection can better detect such messages

D. Configure SA associated protocol identification is mainly used for the same data stream signaling channel and data channel associated with the identification , and thus identify protocol

ANSWER: B

Explanation:

The statement “reduces the maximum number of packets detection threshold, can reduce the sas module identification number of packets, thus improve the recognition rate agreement” is the wrong statement. The maximum packet-detection threshold controls how many packets the Security Awareness (SA) engine can examine while attempting to identify an application or protocol flow. Reducing this value causes the engine to stop inspecting earlier and use fewer packets for classification. Although this can reduce inspection workload and may improve processing efficiency, it does not improve protocol-recognition accuracy. Some applications, particularly those with delayed negotiation, fragmented exchanges, or signatures appearing later in a session, require additional packets before they can be reliably identified. Therefore, setting too small a detection threshold can decrease the recognition rate or leave traffic unidentified. Huawei’s SA/application-identification configuration should balance recognition completeness against device performance; a higher inspection allowance generally gives the signature engine more evidence for an accurate classification. See Huawei’s Enterprise Documentation portal and the Huawei Enterprise knowledge base for product-specific SA and application-identification configuration guidance.

QUESTION NO: 11

If you are deploying BYOD When the system is installed, use a stand-alone installation SM, Dual-machine installation SC, Stand-alone hardware deployment AE,Which of the following descriptions are correct? (Multiple choice)

A. AE Server priority use)SC server.

B. Install AE When the server, you need to configure the main and standby SC Server IP address.

C. If the Lord SC After the server fails,AE The server will use the backup SC server.

D. host SC After the server is restored,AE Server will not switch back to master SC The server handles the business.

ANSWER: A B C D

Explanation:

In this BYOD deployment model, the dual Security Controller deployment provides service-controller redundancy for the independently deployed Access Engine. The AE must be configured with the IP addresses of both the active and standby SC servers during installation, so it has an alternate controller endpoint available without requiring a configuration change during a fault. Under normal conditions, the AE preferentially establishes and maintains service interaction with the active (primary) SC server. If that SC server becomes unavailable, the AE uses the standby SC server so that BYOD access-control and related service processing can continue.

This failover behavior is designed to preserve service stability. After the primary SC server recovers, the AE does not automatically move its current service processing back to that recovered server. Remaining on the currently active controller prevents an unnecessary second switchover and avoids disrupting established processing merely because the previously active peer is reachable again. Therefore, the statements concerning primary preference, configuration of both SC addresses, failover to the standby SC, and no automatic failback after recovery are all correct. Huawei’s enterprise support portal provides the relevant product documentation and configuration references: Huawei Enterprise Support and Huawei Enterprise Documentation.

QUESTION NO: 12

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. The terminal connected to the access device has not enabled the 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: C D

Explanation:

A successful `test-aaa` result verifies that the aggregation-layer access-control device can send an AAA request and receive a successful response using the tested credentials. It does not establish that the endpoint has initiated an 802.1X exchange or that EAPOL frames can travel from the endpoint to the aggregation-layer authenticator.

The terminal connected to the access device has not enabled the 802.1X function is therefore a valid cause. In an 802.1X deployment, the supplicant on the user terminal must be enabled and configured to start the EAPOL authentication process. Without an active supplicant, the aggregation device receives no usable client authentication exchange even though its independent AAA test succeeds.

The Layer 2 link is used between the access device and the aggregation device, and the 802.1X transparent transmission function is not enabled is also a valid cause. Because the authenticator is located at the convergence layer while the terminal is attached through an access device, the intermediate Layer 2 device must transparently forward the EAPOL frames used by 802.1X. Enabling 802.1X transparent transmission allows those frames to reach the aggregation-layer authenticator and permits the authentication workflow to proceed. The IEEE overview of the roles and EAPOL-based operation is available at IEEE 802.1X; Huawei enterprise documentation is available through the Huawei Enterprise Support portal.

QUESTION NO: 13

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 91 Information sent to AD The server performs verification.

D. Synchronize the database again.

ANSWER: C

Explanation:

User 91 Information sent to AD The server performs verification. Agile Controller-Campus can use an Active Directory server as an external identity source for access authentication. When an access user is not found in the controller’s locally available user information, the controller proceeds by forwarding the authentication request to the configured AD server. The AD server then validates the user’s identity information, such as the supplied account name and password, against its directory records and returns the authentication result to the controller. This lets an organization retain AD as the authoritative user repository while using Agile Controller-Campus to enforce campus access policies and manage authentication workflows. Importing or synchronizing directory information supports user and group visibility, but an absent local record does not by itself terminate the authentication process when AD authentication has been configured. The controller uses the external AD service for the next verification step, enabling directory-based authentication without requiring every user credential to be maintained independently on the controller. Huawei’s campus access-control documentation describes the controller’s

integration with external authentication and directory services: Huawei Agile Controller-Campus Documentation. General Microsoft Active Directory Domain Services authentication concepts are documented at Microsoft Active Directory Domain Services overview.

QUESTION NO: 14

According to different reliability requirements, centralized networking can provide different reliability networking solutions. Regarding these solutions, which of the following descriptions are correct? (Multiple choice)

A. Basic networking includes deploying one SM Server, one SC Server, one DB and a AE server.

B. AE In addition to the deployment of basic networking components, the reliability of the network also requires the deployment of an additional backup SC server.

C. SC In addition to the deployment of basic networking components, the reliability of the network also requires the deployment of an additional backup SM server.

D. DB In addition to the deployment of basic networking components, the reliability of the network also requires the deployment of an additional backup DB..

ANSWER: A D

Explanation:

Basic networking includes deploying one SM Server, one SC Server, one DB and a AE server. This is the baseline centralized deployment: the SM Server, SC Server, database, and AE Server each provide their required service role as a single instance. It is appropriate where the required availability level does not require service-node redundancy.

DB In addition to the deployment of basic networking components, the reliability of the network also requires the deployment of an additional backup DB.. is also correct. Database reliability is achieved by adding a backup database in addition to the database in the basic topology. The backup DB preserves database-service availability and enables service data to be protected through synchronization and recovery mechanisms when the active database is unavailable. This is a distinct reliability enhancement because the DB stores the system's persistent operational data; protecting that data and providing a standby database are necessary parts of a database-reliable centralized solution.

Huawei enterprise documentation organizes installation, deployment, and high-availability guidance by product and component role; consult the relevant product-version documentation when planning the active/standby roles and synchronization configuration: Huawei Enterprise Support and Huawei Enterprise Networking.

QUESTION NO: 15

Which of the following behaviors IPS can not detect?

A. Virus

B. Worm

C. Spam

D. DOS

ANSWER: A C

Explanation:

In this exam context, **Virus** and **Spam** are the behaviors an IPS is not intended to detect as its primary security function. An IPS performs deep inspection of traffic against intrusion signatures, protocol anomalies, and attack patterns. Its principal purpose is to identify and block exploit attempts, unauthorized access attempts, scanning activity, and network-layer or application-layer attacks as packets traverse the device.

Virus protection normally requires dedicated anti-malware capability. This capability uses malware scanning engines, file reputation, file-type analysis, and often sandboxing to inspect files or executable content. Although some security gateways may integrate multiple inspection engines, virus identification is not inherently an IPS detection function. Similarly, spam is primarily an email-security problem. Effective spam detection depends on mail-specific context such as sender reputation, message headers, recipient policies, content classification, and anti-spam filtering rules rather than IPS attack signatures.

Huawei's security-gateway materials distinguish intrusion prevention from specialized anti-virus and anti-spam services, which are configured as separate content-security functions. See Huawei's firewall security configuration documentation and the NIST overview of intrusion detection and prevention systems.

QUESTION NO: 16

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 association and communication process between a wireless client and the WLAN. "Link authentication" is part of this protection because it authenticates the wireless connection at the link layer, commonly through 802.1X/EAP or related WLAN authentication methods. It helps ensure that a station is permitted to establish and retain access to the wireless network.

"User access authentication" is also user access security because it verifies the identity and authorization of the person or terminal requesting network service. Huawei WLAN deployments commonly integrate this function with an authentication server, such as RADIUS, so that access-control policy can be applied to authenticated users.

"data encryption" protects the confidentiality and integrity of traffic after a client is admitted. WLAN security protocols use negotiated cryptographic keys to protect frames transmitted over the radio medium, which is inherently susceptible to interception. Therefore, authentication of the connection, authentication of the user, and encryption of user data together form the relevant user-access-security functions. Huawei's enterprise WLAN overview is available at Huawei Enterprise WLAN; the Wi-Fi Alliance provides further security background at Wi-Fi Security.

QUESTION NO: 17

If you use a normal account for authentication, which of the following descriptions is wrong?

A. Users can use Any Office Perform authentication.

B. User can't use web Way to authenticate.

C. Users can use Web Agent Perform authentication.

D. Users can use their own 802. 1X The client authenticates.

ANSWER: B

Explanation:

The statement "User can't use web Way to authenticate." is the incorrect description. A normal account is intended to be used by a regular network user and can participate in the authentication methods supported by the Huawei access-control system, including browser-based web authentication when that authentication service and its associated portal policy are

configured. In this model, the user accesses the authentication page, provides the normal account credentials, and the controller validates the credentials before applying the authorized access policy. The availability of web authentication is therefore determined by the configured access/authentication policy and network service, not by an inherent prohibition on normal accounts. Huawei's enterprise access-control solutions support centrally managed user identities and multiple access authentication mechanisms so that the same managed user account can be used in the applicable authentication scenarios. For Huawei product documentation and configuration guidance, consult the Huawei Enterprise Support documentation portal and Huawei's Identity and Access Management solution information.

QUESTION NO: 18

If the self-determined meter function is enabled on the Agile Controller-Campus and the account PMAC address is bound, Within a period of time, the number of incorrect cipher input by the end user during authentication exceeds the limit. Which of the following descriptions is correct? (multiple choice)

A. When the account number is reserved, only the sword type number cannot be authenticated on the bound terminal device, and it can be authenticated normally on other terminal devices.

B. The account is locked on all terminal devices and cannot be recognized.

C. If you want to lock out the account, the administrator can only delete the account from the list.

D. After the lock time, the account will be automatically unlocked

ANSWER: A D

Explanation:

When password-error protection is configured and a user account is bound to a PMAC address, the authentication failure restriction is applied in the context of that account's bound endpoint. Therefore, after the configured number of incorrect password entries is exceeded within the monitoring interval, the account is prevented from authenticating on the bound terminal device, while the same account can still be authenticated from another terminal device. This behavior lets the controller mitigate repeated password-guessing attempts without unnecessarily disabling the account across the entire network.

The restriction is also time based. Once the configured lock period expires, Agile Controller-Campus automatically clears the temporary lock state, allowing the account to authenticate again without requiring an administrator to manually restore access. This is consistent with the platform's account-security design: failed-authentication thresholds and lock durations provide automated protection and recovery, while PMAC binding identifies the endpoint associated with the account. Huawei product and documentation resources are available through the Huawei Enterprise Support portal and the Agile Controller-Campus product page.

QUESTION NO: 19

How to check whether the SM and SC silverware start normally after installing the Agile Controller-Campus) (multiple delivery)

A. Open https://SM server IP:8943 in the browser, enter the account admin and the default password Changeme123, if the login is successful, it will be explained. The SIM components are normal.

B. After logging in to SC, select Resources>Users>User Management to create a common account. Open https://SM server IP:8447 in the browser newauth, if you can successfully log in using the account created in the previous step, the SM component is normal.

C. Open https://SC Server IP:8443 in the browser and enter the account admin and the default password Changeme123. If the login is successful, it will be explained. The SC component is normal.

D. After logging in to SM, select Ziyuan>User>User Management, and Xinlu has a common part number. Open https://SC server IP:8447 newauth in the browser. If you can successfully log in with the account created in the previous step, it means that the SC component is Wang Chang.

ANSWER: A D

Explanation:

Opening `https://SM server IP:8943` and successfully authenticating with the initial administrator credentials is a direct service-availability check for the SM-side management portal. A successful login demonstrates that the relevant SM web service has started, is listening on its expected secure port, and can complete administrator authentication. This is an appropriate immediate post-installation check before performing higher-level service operations.

Creating a standard user through SM resource and user management, then signing in through `https://SC server IP:8447/newauth`, verifies the SM-to-SC service chain rather than merely confirming that a web page responds. Successful authentication proves that the user information managed by SM is available to SC's authentication entry point and that the SC component can process the login request. Together, these checks validate both the SM management service and the SC authentication integration expected after an Agile Controller-Campus deployment. Huawei's enterprise support portal provides the product documentation and version-specific installation/operation guides: Huawei Enterprise Support. Product context and controller-management information are available from Huawei Agile Controller.

QUESTION NO: 20

In a campus admission-control deployment, an administrator needs to change the authorization attributes of a user who has already been authenticated, without requiring the user to log in again. Which RADIUS function can be used?

A. Change of Authorization (CoA)

B. EAPOL-Start

C. DHCP Relay

D. CAPWAP discovery

ANSWER: A

Explanation:

RADIUS Change of Authorization (CoA) is correct. CoA allows a RADIUS server to send a dynamic authorization request to a network access device for an existing user session. The access device can then apply updated authorization information, such as a different user role, VLAN, ACL, or other access policy, without requiring the user to perform a new authentication.

RADIUS CoA is particularly useful when a user group, endpoint posture, or access permission changes after the original authentication has completed. The RADIUS Dynamic Authorization Extensions are defined in RFC 5176. Huawei AAA and access-control configuration documentation is available through Huawei Enterprise Support.

QUESTION NO: 21

802.1 X During the authentication, if the authentication point is at the aggregation switch, in addition to RADIUS,AAA,802.1X In addition to the conventional configuration, what special configuration is needed?

A. Both the aggregation layer and the access layer switches need to be turned on 802.1X Function.

B. Access layer switch needs to be configured 802. 1X Transparent transmission of messages.

C. The aggregation switch needs to be configured 802 1X Transparent transmission of messages.

D. No special configuration required

ANSWER: B

Explanation:

When the aggregation switch acts as the 802.1X authenticator, the access switch is located between the endpoint (the supplicant) and the authenticator. The access-layer device must therefore be configured for 802.1X packet transparent transmission. This permits the endpoint's EAPOL authentication frames to traverse the access switch and reach the aggregation switch, where the actual 802.1X access control and RADIUS interaction occur. It also allows the corresponding EAPOL responses generated by the aggregation switch to return to the endpoint through the same access-layer device. In this design, the authentication point remains centralized on the aggregation switch, while the access layer forwards the required authentication protocol traffic rather than independently performing authentication. This is particularly useful where centralized user-access control is required but users physically connect to downstream access ports. The underlying IEEE 802.1X architecture defines communication between a supplicant and an authenticator using EAPOL, with the authenticator relaying authentication information to the authentication server. Huawei enterprise documentation and product configuration resources are available through Huawei Enterprise Support; the IEEE 802.1X standard family is described at IEEE 802.1X.

QUESTION NO: 22

Regarding the basic principles of user access security, it is wrong not to list any description?

A. When a terminal device accesses the network, it first authenticates the user's identity through the access device, and the access device cooperates with the authentication server to complete the user Authentication.

B. The terminal device directly interacts with the security policy server, and the terminal reports its own status information, including virus database version, operating system version, and terminal Information such as the patch version installed on the device.

C. The security policy server checks the status information of the terminal, and for terminal devices that do not meet the corporate security standards, the security policy server reissues. The authorization information is given to the access device.

D. The terminal device selects the answer to the resource to be accessed according to the result of the status check.

ANSWER: D

Explanation:

The statement "The terminal device selects the answer to the resource to be accessed according to the result of the status check." is the incorrect description of the user-access-security process. In Huawei campus access-control and Network Admission Control designs, the endpoint supplies identity and, where required, posture information such as its antivirus and patch status. The access-control system then evaluates that information against the organization's access policy. The endpoint is not the policy-enforcement point and must not independently decide which protected resources it may use.

Access authorization is instead determined centrally by the security-policy or authentication components and enforced by the network access device. Based on the authorization result, the access device can permit normal network access, place the endpoint into a restricted or remediation area, apply a VLAN or user group, or apply a downloadable access-control policy. This separation ensures that a compromised or noncompliant terminal cannot grant itself broader access merely by reporting a status result. Huawei's campus access-control approach similarly uses identity and terminal-security status to drive centrally defined admission policies and network-side enforcement. See Huawei's Campus Network Access Control overview and the IETF's IEEE 802.1X RADIUS Usage Guidelines for the authorization model between authentication services and network access equipment.

QUESTION NO: 23

After opening IP strategy, found part of the business fails, what are the possible reasons? (Choose 2 answers)

A. message through the firewall only one direction

B. the same message repeatedly through the firewall

C. IP omission

D. heavy traffic cause Bypass features enabled

ANSWER: A B

Explanation:

The applicable causes are “message through the firewall only one direction” and “the same message repeatedly through the firewall.” IPS processing is stateful: it needs to observe the relevant traffic exchange in both directions so that it can build and maintain an accurate session and protocol-inspection context. If only one direction of a flow traverses the firewall, such as when asymmetric routing is present, the inspection engine has incomplete session information. This can result in valid application traffic being unable to proceed normally after an IPS policy is enabled.

Repeated traversal of the same packets through the firewall can also disrupt IPS-protected services. Re-injected, duplicated, or looping packets may cause the firewall to process traffic more than once within its state and inspection context. This can interfere with orderly protocol parsing and session tracking, particularly for applications that require a consistent packet sequence. When investigating failures after enabling an IPS policy, confirm that forwarding is symmetric and that the network topology does not cause traffic to loop back through the firewall. Huawei’s security product information and technical-support portal provide product documentation and troubleshooting resources: Huawei Firewall and Huawei Enterprise Support.

QUESTION NO: 24

In Portal authentication, which of the following parameters must be configured on the switch? (Multiple choice)

A. Portal server IP

B. Portal page URL

C. shared-key

D. Portal Protocol version

ANSWER: A B C

Explanation:

Portal authentication requires the access switch to establish a defined relationship with the external Portal server and to redirect unauthenticated users to that server. Therefore, **Portal server IP** must be configured so that the switch knows the Portal server endpoint to which it exchanges Portal authentication and notification messages. The **Portal page URL** is also required because it supplies the redirection address presented to users who need to open the Portal login page. Finally, the **shared-key** must be configured consistently on both the switch and Portal server. This key protects the trust relationship between the devices and allows the Portal protocol messages to be validated correctly.

These values are normally configured in the switch’s Portal server template or Portal access profile and then applied to the relevant access interface, VLAN, or authentication domain. Huawei’s configuration documentation describes Portal authentication as a coordinated switch-and-Portal-server deployment in which the server address, web redirection URL, and communication key are core connection parameters. See the Huawei Enterprise product documentation and the Huawei documentation portal for Portal server configuration and command-reference details.