PassQueen
a.k.a dumpsqueen.com

HCIP-Security-CTSS V3.0

Huawei H12-723_V3.0

Version Demo

Total Demo Questions: 19

Total Premium Questions: 190

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Cybersecurity Situation Awareness Overview	36
Topic 2, Network Traffic Analysis	6
Topic 3, Security Operations	95
Topic 4, Mix Questions	53
Total	190

QUESTION NO: 1

Regarding the file source set in the software management, which of the following descriptions is correct?

A. When the file source is an internal data source, when distributing software, the business manager will only send thepath of the data source of the software to be distributed to Any Office

B. When the file source is an external data source, Any 0fce will obtain the software to be distributed.

C. External data sources cannot distribute files from FTP-type file servers.

D. The Microsoft Windows file sharing server uses the UNC (Universal Naming Conversion) path (beginning with "\\") to provide waiting. The path to distribute the software.

ANSWER: D

Explanation:

The statement that the Microsoft Windows file sharing server uses a UNC (Universal Naming Convention) path beginning with “\\” as the path for distributing software is correct. In AnyOffice software management, an external file source can point to a shared Windows folder. The shared resource is identified by its UNC address, normally in the form `\\server-name\\share-name\\path`, rather than by a local drive letter. This format lets the AnyOffice components consistently locate the installation package across the network when a software-distribution task is created and executed. The share must be reachable from the relevant management or client component, and the configured account must have the permissions required to read the software package. UNC paths are the standard Windows network-path format for file shares, so using one provides an unambiguous network location for the distribution source. Huawei documentation is available through the Huawei Enterprise Support portal; Microsoft’s definition and syntax for UNC paths are documented in File path formats on Microsoft Learn.

QUESTION NO: 2

When deploying 802.1X authentication for employee terminals, which of the following practices can improve access security? (Multiple choice)

A. Use EAP-TLS with client certificates where possible.

B. Validate the authentication server certificate on the client.

C. Use dynamic VLANs or authorization ACLs according to the authentication result.

D. Configure all employees to use one shared authentication account.

ANSWER: A B C

Explanation:

Using EAP-TLS with client certificates provides strong mutual authentication and avoids transmitting reusable user passwords over the access network. Validating the authentication-server certificate helps the client avoid connecting to an untrusted server. Applying dynamic VLANs or authorization ACLs after successful authentication allows the access device to grant permissions according to the user identity and authorization result.

Using the same shared account for all employees weakens traceability and prevents reliable identity-based authorization. Huawei campus access-control solutions support 802.1X, RADIUS authorization, and identity-based policy enforcement. See the Huawei Enterprise Support portal and RFC 5216.

QUESTION NO: 3

VIP Experience guarantee, from which two aspects are the main guaranteesVIP User experience? (Multiple choice)

A. bandwidth

B. Forwarding priority

C. Authority

D. Strategy

ANSWER: A B

Explanation:

VIP user experience assurance is principally achieved through **bandwidth** and **forwarding priority**. Bandwidth assurance reserves or allocates sufficient network capacity for VIP application traffic, helping ensure that critical services have the throughput needed during periods of congestion. This is essential for maintaining predictable service quality for traffic such as key business applications, voice, video, or other latency-sensitive services.

Forwarding priority complements bandwidth assurance by determining the order in which traffic is processed and transmitted when network resources are contested. By classifying VIP traffic and placing it in an appropriate high-priority forwarding queue, QoS mechanisms can reduce delay, jitter, and packet loss for that traffic. Together, these controls provide both resource availability and preferential treatment: bandwidth supplies the capacity, while forwarding priority ensures VIP packets receive timely handling.

This approach aligns with Huawei QoS principles, which use traffic classification, queue scheduling, congestion management, and bandwidth allocation to differentiate service levels. It also follows the differentiated-services model described in RFC 2474. Huawei enterprise networking resources are available through the Huawei Enterprise Support Documentation portal.

QUESTION NO: 4

Which of the following equipment is suitable for use MAC Authentication access network?

A. Office Windows Systemhost

B. For testing Linux System host

C. Mobile client, such as smart phone, etc

D. Network printer 232335

ANSWER: D

Explanation:

Network printer 232335 is suitable for MAC authentication access because printers are typical non-user endpoints that often cannot run an 802.1X supplicant or present interactive credentials. With MAC authentication, the access device uses the endpoint's source MAC address as the identity submitted to the authentication server, commonly through RADIUS. After the printer's MAC address is registered or authorized according to the organization's access policy, the switch can permit the printer to access the required network or place it into an assigned VLAN. This makes MAC authentication a practical onboarding method for managed infrastructure devices such as printers, IP phones, cameras, and similar equipment that need network connectivity but have limited authentication capabilities. In a production deployment, administrators should maintain an accurate endpoint inventory and combine MAC-based access with controls such as port security, VLAN segmentation, and monitoring, because a MAC address can be imitated. Huawei access-switch documentation describes MAC authentication as an access-control method in which a device authenticates users based on MAC addresses and can use RADIUS to make authorization decisions. See Huawei's enterprise product documentation and the MAC authentication documentation.

QUESTION NO: 5

In a port-based 802.1X access scenario, which of the following descriptions are correct? (Multiple choice)

A. Successful authentication changes the authorization state of the controlled physical port.

B. Terminals connected through a HUB can share the authorized state of the same port.

C. MAC-based access control can provide independent control for endpoint MAC addresses.

D. Port-based control always requires every terminal behind a HUB to authenticate independently.

ANSWER: A B C

Explanation:

In port-based access control, the authenticator changes the authorization state of the physical controlled port after a user successfully authenticates. Therefore, if multiple terminals are connected behind the same Layer 2 device such as a HUB, successful authentication by one terminal can cause the shared physical port to become authorized.

This behavior differs from MAC-based access control, where authentication and authorization can be maintained separately for different endpoint MAC addresses on the same interface. Port-based mode is suitable where one user or terminal is expected on one physical access port. If a deployment requires separate authentication for multiple endpoints connected through the same interface, a per-user or MAC-based control mode supported by the device should be selected. The controlled-port model is described in RFC 3580.

QUESTION NO: 6

Use on the terminalPortal The authentication is connected to the network, but you cannot jump to the authentication page. The possible reason does not include which of the following options?

A. Agile Controller-Campus Configured on Portal The authentication parameters are inconsistent with the access control device.

B. Access device Portal The authentication port number of the template configuration is 50100 ,Agile Controlle-Campus The above is the default.

C. CS Did not start

D. When the page is customized, the preset template is used.

ANSWER: D

Explanation:

When the page is customized, the preset template is used. This is not, by itself, a reason that a terminal cannot be redirected to the Portal authentication page. Huawei campus access-control systems support both built-in preset Portal page templates and customized pages. A preset template is a valid page source that the controller can use to present the Portal login interface after the access device intercepts a user's web request and performs Portal redirection. Therefore, selecting the preset template during page customization does not inherently interrupt the redirect process or make the authentication page unavailable.

Portal access is a coordinated workflow: the access device identifies an unauthenticated user, redirects the user's request to the configured Portal service, and the controller supplies the relevant authentication page. The choice of a built-in template affects the appearance and content of that page, rather than the fundamental ability to trigger redirection. Huawei documentation describes Portal authentication and its controller-based configuration model in its campus-network documentation. See the Huawei CloudCampus Configuration Guide and the Huawei Campus Network Security Configuration Guide.

QUESTION NO: 7

On WIDS functional WLAN Regarding the judgment of illegal devices in the network, which of the following statements are correct? (Multiple choice)

A. all Ad-hoc The device will be directly judged as an illegal device

B. Not this AC Access AP Is illegal AP

C. Not this AC Access STA Is illegal STA

D. Not this AC Access STA,Also need to check access AP Does it contain law

ANSWER: A D

Explanation:

WIDS identifies devices by correlating over-the-air observations with the WLAN's managed-device information, rather than treating every nearby wireless device as hostile. An Ad-hoc device is directly classified as an illegal device because it forms a peer-to-peer wireless network outside the managed AP-based WLAN infrastructure. Such a network bypasses the organization's normal WLAN access control, authentication, and policy enforcement, so it is a direct WIDS concern. IEEE 802.11 defines ad-hoc operation as an independent basic service set, distinct from an infrastructure BSS built around an AP; see IEEE 802.11.

For a STA that is not associated with this AC, WIDS must also examine the AP to which that STA is associated. The STA should be identified as illegal only when the associated AP is determined to be illegal; a station observed through a legitimate AP is not automatically an illegal station merely because it is not managed by the local AC. This association-based correlation prevents device classification from being based solely on AC membership and reflects the managed WLAN security model used by Huawei WLAN solutions. Huawei's enterprise WLAN portfolio and security capabilities are described at Huawei WLAN.

QUESTION NO: 8

BY00 The products and textiles provided by the history solution program cover the entire terminal network\Application and management and other fields/include: Serialization BC Equipment, paperless network system network access support, VPN Gateway, terminal security customer ladder software, authentication system, mobile device management(MDN),move eSpace UC.

A. True

B. False

ANSWER: A

Explanation:

True is correct. The statement describes the breadth of a Huawei BYOD-oriented enterprise solution: it is not limited to onboarding a device onto Wi-Fi, but spans endpoint access, network connectivity, application access, identity authentication, endpoint protection, and centralized device management. A complete BYOD architecture normally combines network-access control and authentication with secure remote access through a VPN gateway. It also requires client-side security controls and mobile-device-management capabilities so that administrators can apply access policies, manage device status, and protect organizational resources on personally owned or mobile endpoints.

The inclusion of unified communications, represented by eSpace UC, is also consistent with an enterprise mobility solution because users need secure access to collaboration and communications services after their identities and devices have been validated. Huawei's enterprise campus-network portfolio similarly presents a converged approach in which wired, wireless, and access-control capabilities support secure user and terminal connectivity. Huawei's WLAN portfolio further documents enterprise wireless access as a foundation for connecting and managing diverse terminal types. These linked components therefore appropriately cover the terminal, network, application, and management layers identified in the statement. See Huawei Campus Network Solutions and Huawei WLAN Products.

QUESTION NO: 9

Typical application scenarios of terminal security include: Desktop management, illegal outreach and computer peripheral management.

A. True

B. False

ANSWER: A

Explanation:

“True” is correct because terminal security is intended to centrally control and protect endpoint devices, such as employee desktops and laptops, across their operational lifecycle. Desktop management is a core endpoint-security scenario because administrators need visibility into terminal status and the ability to apply standardized security configurations and policies. Preventing illegal outreach is also an endpoint-security use case: controls on network access and external communications help reduce the risk of data leaving the organization through unauthorized channels or terminals connecting to untrusted networks. Computer peripheral management is equally relevant because removable storage devices and other peripherals can introduce malware or enable unauthorized copying of sensitive data. A terminal-security platform therefore commonly combines endpoint management, data-loss prevention controls, device-control policies, and security monitoring to address these scenarios in a coordinated way. Huawei’s enterprise security portfolio describes endpoint security as part of a broader protection approach for devices, users, and data, while its cybersecurity materials emphasize controlling data-access and leakage risks at organizational boundaries and endpoints. See Huawei Enterprise Security and Huawei Cyber Security.

QUESTION NO: 10

Deployed by an enterprise network managerAgile Controller-Campus withSACG Later;Identityauthentication is successful but cannot access the post-authentication domain, This phenomenon may be caused by any reason? (Multiple choice)

A. A serious violation will prohibit access to the post-authentication domain.

B. The access control list of the post-authentication domain has not been delivered SACG.

C. ALC The number of rules issued is too many, and a lot of time is required to match, causing interruption of access services.

D. Agile Controller-Campus Wrong post-authentication domainresources are configured on the server.

ANSWER: A B D

Explanation:

Successful identity authentication confirms that the user has passed the authentication stage, but access to the post-authentication domain additionally depends on the authorization result being correctly generated and enforced by SACG. “A serious violation will prohibit access to the post-authentication domain.” is correct because Agile Controller-Campus can associate users or endpoints with violation handling and remediation policies. Where a serious violation triggers access restriction, the user may remain authenticated while being prevented from reaching ordinary post-authentication resources.

“The access control list of the post-authentication domain has not been delivered SACG.” is also correct. SACG must receive and apply the authorization ACL associated with the user’s post-authentication domain. If that policy is absent from the device, traffic cannot be permitted according to the intended post-authentication access rules.

“Agile Controller-Campus Wrong post-authentication domainresources are configured on the server.” is correct because the controller supplies authorization information and domain resource definitions. If the configured resources, addresses, or service ranges do not represent the required destination services, an authenticated user cannot access the intended domain even though authentication succeeded. Huawei campus policy control separates identity authentication from subsequent authorization and policy enforcement; see Huawei’s Campus Network documentation and Enterprise Support documentation portal.

QUESTION NO: 11

When performing terminal access control, the authentication technology that can be used does not include which of the following options?

A. 8021X Certification

B. SACG Certification p2-

C. Bypass authentication

D. Portal Certification

ANSWER: C

Explanation:

Bypass authentication is the correct answer because it describes an access exception rather than a technology that authenticates a terminal or user. In terminal access control, authentication technologies establish an identity before authorizing network access. They do this by collecting and validating credentials, identity information, or other authentication data, after which access-control policy can be applied to the identified endpoint. In contrast, bypass authentication means that a device or user is permitted to proceed without undergoing an authentication exchange. It may be used operationally for exceptional scenarios, such as onboarding constraints or explicitly trusted devices, but it does not itself verify identity and therefore is not an authentication technology. This distinction is important in campus security design: authentication provides the identity input required for accountable, policy-driven access control, whereas a bypass is a policy decision to omit that identity-verification step. Huawei's enterprise campus networking materials describe access control as part of a broader secure-campus architecture; see Huawei Campus Network solutions. For the underlying standard model of port-based network access control and authenticated access decisions, see IEEE 802.1X.

QUESTION NO: 12

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 an authentication account has a bound physical MAC address and the configured limit for consecutive incorrect password entries is exceeded within the specified period, the lockout applies to the account's bound endpoint relationship rather than universally preventing use of that account on every endpoint. Therefore, the account cannot authenticate from the bound terminal during the lockout interval, while authentication from another terminal remains possible under the relevant access-policy conditions.

The lock is also time-based. The controller applies the configured lock duration as a protection against repeated password guessing, and automatically removes the lock when that period expires. This enables normal authentication to resume without requiring an administrator to manually delete the user account. Such controls are part of account and access-security policy configuration in Huawei campus management platforms, where account credentials, endpoint bindings, failed-authentication thresholds, and lock durations are evaluated together. See Huawei's iMaster NCE-Campus product documentation and the Huawei Enterprise Support documentation portal for platform documentation and configuration guidance.

QUESTION NO: 13

After configuring theannouncement,Agile Controller-Campus The system cannot assign this announcement to which of the following objects?

A. Assign to user

B. Assigned to account

C. Assign to terminal IP Address range

D. Assigned to places

ANSWER: D

Explanation:

Assigned to places is correct. In Agile Controller-Campus, an announcement is a portal-facing notification that is delivered according to identity- and access-related targeting information maintained by the controller. Its assignment mechanism is designed to select the relevant audience from managed user, account, and endpoint-address information so that the message can be presented to the intended users during access or portal interactions. A physical place is not an announcement-recipient object in this delivery model. Although sites and locations can be important for network planning, device management, and service deployment, they do not form the supported audience target for an announcement. Consequently, the controller cannot assign a configured announcement to places. This distinction ensures that announcement visibility is tied to identifiable access subjects and endpoint scope, allowing the system to apply the notification consistently when those subjects use campus access services. Huawei's enterprise support portal provides the Agile Controller-Campus product documentation and version-specific operation guides, including the administrator procedures for portal and user-access services: Huawei Enterprise Support. Product and solution context for Huawei campus-management services is also available through Huawei Campus Network solutions.

QUESTION NO: 14

In some scenarios, ananonymous account can be used for authentication. What are the correct descriptions of the following options for the anonymous account?? (Multiple choice)

A. The use of anonymous accounts for authentication is based on the premise of trusting the other party,
and the authentication agency does not need the other party to provide identity information to provide services to the other party.

B. Agile Controller-Campus Need to be manually created"~anonymous"account number.

C. By default, the access control andpolicy of anonymous accounts cannot be performed. 1 Operations such as invoking patch templates and software distribution.

D. Administrators cannot delete anonymous accounts"~anonymous*.

ANSWER: A D

Explanation:

"The use of anonymous accounts for authentication is based on the premise of trusting the other party, and the authentication agency does not need the other party to provide identity information to provide services to the other party" correctly describes the anonymous-authentication model. It is intended for trusted scenarios in which the system can authorize access without collecting or validating a specific user identity. The account represents an unauthenticated or guest-like access context rather than a manually identified person, allowing the controller to apply the predefined behavior appropriate for that context.

"Administrators cannot delete anonymous accounts"~anonymous*" is also correct. The `~anonymous` account is a built-in system account used to support anonymous authentication behavior. Because it is system-reserved and required by the platform's authentication design, it is protected from administrator deletion. Retaining that account ensures that services using anonymous access continue to have a defined internal account context and avoids breaking dependent authentication or authorization processing. Huawei's enterprise support portal provides product documentation and configuration guidance for Agile Controller-Campus: Huawei Enterprise Support. Huawei's enterprise product documentation catalog is also available at Huawei Documentation.

QUESTION NO: 15

Install Agile Controller-Campus Which of the following steps do not need to be completed before?

A. Install the operating system

B. Install the database

C. Install antivirus software

D. Import License

ANSWER: D

Explanation:

Import License is the step that does not need to be completed before Agile Controller-Campus is installed. A license is normally applied after the controller software has been deployed and its services are available. At that point, an administrator can access the product's management interface, enter or upload the license entitlement, and verify that the required licensed features and capacity have taken effect. This ordering is practical because the entitlement is associated with the installed controller instance and is managed from the running system rather than being a prerequisite for laying down the software itself.

Huawei enterprise products commonly separate initial deployment from post-deployment commissioning activities such as license activation. The installation process establishes the controller environment first; licensing then authorizes use of applicable functions once the platform can be accessed and managed. Therefore, importing the license is an operational activation task performed after installation, not a pre-installation requirement. Huawei's enterprise support portal provides product documentation and licensing resources, while its network-management portfolio describes the role of centralized management software in enterprise deployments. See Huawei Enterprise Support and Huawei Network Management and Analysis Software.

QUESTION NO: 16

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:

"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." is correct. In Huawei campus access-control and endpoint-admission scenarios, the isolation domain is a restricted remediation network. A user or terminal that has completed identity authentication but does not meet endpoint-security requirements, such as required antivirus status, patch level, or security-policy compliance, is placed in this limited-access area rather than receiving normal business-network access.

The purpose is to let the endpoint reach only the resources needed to become compliant. Typical resources include patch-management servers, antivirus or virus-definition update servers, and related remediation services. After the endpoint completes the required remediation and passes the security assessment, access control can authorize it for the normal service domain. This design protects production resources while allowing noncompliant devices to update and recover without requiring manual network intervention. Huawei's campus-security materials describe this type of identity- and security-posture-based access control: Huawei Campus Security. Official Huawei enterprise documentation can also be accessed through the Huawei Enterprise Support documentation portal.

QUESTION NO: 17

In the campus network, employees can use 802.1X, Portal,MAC Address or SACG Way to access. Use different access methods according to different needs to achieve the purpose of user access control.

A. True

B. False

ANSWER: A

Explanation:

True is correct. Huawei campus-network access-control designs support multiple authentication and admission methods so that an organization can apply an appropriate method to each endpoint and user scenario. 802.1X is typically used for identity-based access from managed employee devices, while Portal authentication supports web-based user onboarding and access. MAC-address-based access is useful for endpoints that cannot perform interactive authentication, such as some printers, cameras, and IoT devices. SACG access is also part of Huawei's campus access-control capability, enabling controlled access in applicable gateway-based scenarios. These methods can be used with centralized policy enforcement to determine whether a user or endpoint is admitted to the network and what authorization is applied after admission. This flexibility is a key campus-network requirement: authentication is selected according to endpoint capability, user type, and the organization's security policy rather than requiring one method for all clients. Huawei describes campus networking as providing unified access and policy-based management, including user and terminal access control. See Huawei's Campus Network solution overview and the Huawei Enterprise Support documentation portal for product documentation on campus access authentication and policy configuration.

QUESTION NO: 18

For hardware SACC Access control, if the terminal does not pass the authentication, it can access the resources of the post-authentication domain. This phenomenon may be caused by the following reasons? (Multiple choice)

A. Authentication data flow has passed SACG filter.

B. TSM No hardware is added to the system SACG equipment.

C. SACG Enable the default inter-domain packetfiltering.

D. Privileges are misconfigured IP

ANSWER: B D

Explanation:

"TSM No hardware is added to the system SACG equipment." is a valid cause because hardware SACC enforcement relies on the linkage between Terminal Security Management (TSM) and the Security Access Control Gateway (SACG). TSM must manage the SACG device and deliver the terminal identity, authentication status, and authorization information needed for the gateway to distinguish unauthenticated terminals from authorized terminals. If the SACG is not added or managed, the expected authorization state may not be applied to that gateway, allowing traffic to be forwarded without the intended post-authentication-domain restriction.

"Privileges are misconfigured IP" is also a valid cause. Hardware access-control policies commonly use IP-based authorization objects or IP groups to define which resources a terminal can reach before and after authentication. An incorrect address, mask, range, group membership, or privilege mapping can mistakenly classify an unauthenticated terminal as permitted for a post-authentication resource. Correct operation therefore requires verification of the managed gateway relationship and the IP-based privilege definitions delivered to the enforcement point. Huawei's enterprise support portal provides product documentation and configuration guidance at Huawei Enterprise Support; Huawei's security portfolio overview is available at Huawei Security.

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/newauth in the browser. 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 Resources>Users>User Management and create a common account. Open https://SC server IP:8447/newauth in the browser. If you can successfully log in with the account created in the previous step, the SC component is normal.

ANSWER: A B C D

Explanation:

All listed checks are valid startup-verification procedures for the Agile Controller-Campus Service Manager (SM) and Service Controller (SC) components. Directly signing in to the SM management portal at port 8943 with the initial administrator credentials confirms that the SM management service is available. Likewise, signing in to the SC management portal at port 8443 with the initial administrator credentials confirms that the SC management service is available. The default password must be changed after the initial login as part of secure deployment practice.

The cross-component user-authentication tests provide additional validation beyond basic web-service reachability. Creating a common user in SC and successfully authenticating through the SM newauth service at port 8447 confirms that SM authentication and its connection to SC-managed user information are functioning. Creating a common user in SM and then authenticating through the SC newauth service at port 8447 similarly verifies that SC can provide the expected authentication service. Together, direct administrator login and normal-user newauth login verify both component availability and the SM–SC interaction required after installation. Huawei product documentation and support resources are available through Huawei Enterprise Support and Huawei Network Security.