PassQueen
a.k.a dumpsqueen.com

HCIA-Security V4.0 Exam

Huawei H12-711_V4.0

Version Demo

Total Demo Questions: 11

Total Premium Questions: 113

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Security Overview	4
Topic 2, Network Security Basics	35
Topic 3, Network Security Products and Technologies	10
Topic 4, Firewall Basics	14
Topic 5, Firewall Security Policy	7
Topic 6, NAT	3
Topic 7, VPN	18
Topic 8, Security Operations	21
Topic 9, Mix Questions	1
Total	113

QUESTION NO: 1 - (DRAG DROP)

Please classify the following security defenses into the correct classification.

ANSWER:

Explanation:

Security defenses are commonly classified according to the layer or object they protect. Firewall belongs to Network Security because a firewall controls and filters traffic crossing network boundaries. It applies security policies to network connections, such as allowing authorized sessions and blocking traffic that does not meet the configured rules. This makes the firewall a foundational boundary-protection mechanism in a network security architecture. Huawei describes firewall capabilities and policy-based traffic control in its firewall product documentation.

Identity Authentication belongs to System Security. Authentication verifies the identity of a user, administrator, device, or process before access to operating-system resources, management functions, and protected services is granted. It is a core system access-control function and is normally combined with authorization and auditing to protect system resources.

Virus Defense belongs to Terminal Security because malware protection is deployed on endpoint devices such as PCs, laptops, and other hosts. Terminal defenses detect, prevent, quarantine, and remove malicious software at the device where files execute and user activity occurs. This is consistent with endpoint-protection practices described by CISA's malware guidance.

Server Security belongs to Application Security because servers host and deliver applications, web services, databases, and other business-facing services. Protecting those server-hosted services includes securing application deployment, service configurations, access paths, and the data-processing environment. Together, these mappings cover network boundaries, system access, endpoints, and server-hosted applications as distinct protection domains.

QUESTION NO: 2

Which of the following characteristics are usually associated with computer viruses?

A. Replication

B. Concealment

C. Destructive payload

D. It must provide normal network routing services

ANSWER: A B C

Explanation:

Computer viruses are malicious code that attach to a host program, document, boot record, or other carrier and execute when the infected carrier is run. A virus can replicate by copying itself into additional files or systems, which gives it the ability to spread. It can conceal itself to avoid detection, for example by using obfuscation or modifying infected files. A virus can also contain a payload that performs harmful actions, such as deleting data, changing files, disrupting system operation, or downloading additional malware.

A virus normally requires a host or execution mechanism to become active. Unlike a network worm, a traditional virus does not inherently spread independently across a network without a host program or user action. CISA provides malware background information at CISA: Malware.

QUESTION NO: 3

The following description of the intrusion fire protection system IPS, which is correct?

A. An inline IPS can be deployed in series at the network boundary.

B. The IPS cannot prevent intrusion from occurring in real time.

C. An IPS can be connected to a switch and inspect traffic mirrored by the switch.

D. An IPS can customize intrusion prevention rules.

ANSWER: A C D

Explanation:

An inline IPS can be deployed in series at the network boundary because this placement puts the device directly in the traffic path. It can therefore inspect packets and sessions against intrusion signatures and protocol-analysis rules before forwarding the traffic, allowing detected attacks to be blocked in real time. An IPS can also be connected to a switch and inspect traffic mirrored by the switch. Mirroring is useful for monitoring a selected interface, VLAN, or traffic flow without placing the IPS physically inline; this deployment is commonly used for visibility, analysis, and alerting, and can be combined with other response mechanisms where supported. An IPS can customize intrusion prevention rules because effective protection requires adapting detection to the organization's services, applications, assets, and threat environment. Administrators can tune signature behavior, define exceptions, and create custom signatures or rules to identify organization-specific malicious traffic while reducing unnecessary alarms. Huawei security products support IPS policy configuration and signature-based detection as part of their threat-defense capabilities. These deployment and policy concepts also align with the NIST guidance that distinguishes inline intrusion prevention from passive monitoring and emphasizes configurable detection and response policies. See Huawei Firewall and Threat Defense and NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems.

QUESTION NO: 4

Which of the following is not included in the Business Impact Analysis (BIA).

A. Risk identification

B. Impact assessment

C. Incident handling priority

D. Business priorities

ANSWER: A

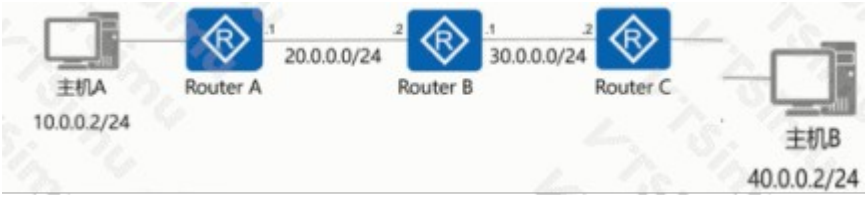
Explanation:

Risk identification is not included in a Business Impact Analysis (BIA). A BIA is a business-continuity activity that examines how disruption of business functions, processes, services, and supporting resources would affect the organization over time. Its purpose is to establish the importance of business activities, identify the consequences of outages, determine acceptable downtime and recovery objectives, and provide a basis for recovery sequencing and incident-response priorities. The resulting analysis helps an organization focus continuity and recovery resources on the business capabilities whose loss would have the greatest operational, financial, legal, or reputational effect.

Risk identification is instead a risk-management activity. It focuses on identifying threats, vulnerabilities, and risk scenarios that could cause an undesirable event. Although risk-management results can inform continuity planning, the BIA concentrates on the consequences to the business if a disruption occurs, rather than on identifying the sources or likelihood of that disruption. This distinction is reflected in NIST's contingency-planning guidance, which describes BIA as identifying and prioritizing critical information-system and business functions and their recovery requirements. See NIST SP 800-34 Rev. 1 and the ISO 22301 business continuity standard.

QUESTION NO: 5

As shown in the figure, the administrator needs to test the network quality of the 20.0.0/24 CIDR block to the 40.0.0/24 CIDR block on Device B, and the device needs to send large packets for a long time to test the network connectivity and stability.



A. tracert -a 20.0.0.1 -f 500 -q 9600 40.0.0.2

B. ping -a 20.0.0.1 -c 500 -s 9600 40.0.0.2

C. ping -s 20.0.0.1 -h 500-f 9600 40.0.0.2

D. tracert -a 20.0.0.1 -c 500 -w 9600 40.0.0.2

ANSWER: B

Explanation:

`ping -a 20.0.0.1 -c 500 -s 9600 40.0.0.2` is the appropriate command because it performs an extended ICMP Echo test with all required traffic characteristics. On Huawei VRP, `-a 20.0.0.1` specifies the source IPv4 address, ensuring that Device B sends probes through the interface in the 20.0.0.0/24 network. The destination `40.0.0.2` is the target host in the remote 40.0.0.0/24 network. The `-c 500` parameter requests 500 echo packets, providing a sustained test rather than a brief reachability check. The `-s 9600` parameter sets a large ICMP Echo payload size, which is useful for observing packet loss, delay, and potential MTU-related behavior under larger packets. Together, these settings test end-to-end connectivity and stability from the intended source address over an extended sequence of large packets. Huawei's product documentation and command references are available through the Huawei Enterprise Support portal; ICMP Echo behavior is standardized in RFC 792.

QUESTION NO: 6

The trigger modes of the built-in Portal authentication in the firewall include pre-authentication and ____ authentication[fill in the blank]*

A. session

ANSWER: A

Explanation:

The correct completion is **session**, producing the term “session authentication.” Huawei firewalls support built-in Portal authentication with pre-authentication and session-authentication trigger modes. In pre-authentication mode, users are directed to the Portal page before they can access controlled network resources, allowing the firewall to collect authentication information at the outset. Session authentication is designed around the user’s access session: the firewall triggers Portal authentication when traffic associated with an unauthenticated session requires access control, then associates the successful authentication result with that session. This allows the firewall to enforce identity-based access policy while maintaining the authenticated user’s session state for subsequent traffic. The wording in the question specifically asks for the paired built-in Portal trigger mode used in Huawei firewall documentation and training materials, and “session authentication” is that established term. Huawei’s enterprise support portal provides product documentation and configuration guidance for firewall Portal authentication features; see the Huawei Enterprise Support search for Portal authentication and the Huawei Enterprise Support portal.

QUESTION NO: 7

An enterprise wants to build a server system and requires the following functions: 1. The enterprise needs to have its own dedicated mailbox, and the sending and receiving of emails needs to go through the enterprise's server; 2. The server must provide file transfer and access services. Users in different departments of the enterprise provide accounts with different permissions: 3. When the enterprise accesses the internal webpage of the enterprise, the enterprise can directly enter the domain name in the browser to access. To meet the above requirements, which of the following servers do enterprises need to deploy? ( )*

A. Time synchronization server

B. FTP server (I)

C. DNS server

D. Mail server

ANSWER: B C D

Explanation:

FTP server (I), **DNS server**, and **Mail server** together meet the stated enterprise-service requirements. A mail server hosts enterprise mailboxes and processes the transfer of email between clients and mail systems. In a typical deployment, SMTP supports message submission and relay, while mailbox-access services such as IMAP or POP3 allow users to retrieve mail. SMTP’s core mail-transfer model is specified in RFC 5321.

An FTP server provides centralized file-transfer and file-access capabilities. It can authenticate enterprise users with individual accounts and apply authorization controls so that departments receive access appropriate to their assigned permissions. FTP defines the client-server mechanism for transferring files, including authenticated user sessions, as described in RFC 959.

A DNS server enables users to enter a domain name, such as an internal web address, rather than memorizing an IP address. The server resolves that name to the IP address of the internal web server, allowing browsers to establish the required connection. In an enterprise network, internal DNS zones can provide this name-resolution service for private web resources. These services directly correspond to dedicated mail processing, controlled file services, and domain-name access to internal webpages.

QUESTION NO: 8

What is the security level of the Untrust zone in Huawei firewalls?

A. 10

B. 20

C. 5

D. 15

ANSWER: C

Explanation:

The correct security level is **5**. Huawei firewalls assign default security levels to predefined security zones so that the device can make an initial determination about the relative trustworthiness of traffic sources and destinations. The Untrust zone represents networks that are outside the organization's security boundary, most commonly the Internet or another external network with a low level of trust. Its default level is therefore 5. This value is used in the firewall's zone-based traffic-processing model: by default, traffic initiated from a higher-security zone toward a lower-security zone is permitted, while traffic in the opposite direction requires an explicitly configured security policy. Administrators can use this baseline behavior together with security policies, NAT, and inspection profiles to control access between internal resources and external networks. The predefined-zone security-level design is a foundational Huawei firewall concept and is important when evaluating traffic direction and planning policy rules. Huawei's enterprise support portal provides firewall product documentation and configuration guidance at Huawei Enterprise Support. Additional Huawei firewall product information is available at Huawei Firewall Products.

QUESTION NO: 9

An engineer needs to back up the firewall configuration. Now he wants to use a command to view all the current configurations of the firewall. May I ask the command he uses is ____[fill in the blank]*

A. display current-configuration

ANSWER: A

Explanation:

`display current-configuration` is the Huawei VRP command used to display the device's current, active configuration. This is the configuration presently loaded and used by the firewall, including configured interfaces, security policies, zones, routing features, AAA settings, logging parameters, and other enabled functions that are applicable to the device and its current context. Reviewing this output is an important preparation step before a backup because it lets the engineer inspect the effective configuration, confirm that recent changes are present, and collect the content that should be retained. On Huawei firewalls, the command is entered in the user view or system view as `display current-configuration`; the space between `display` and `current-configuration` is required command syntax. The output can be viewed directly in the CLI and, where operational procedures require it, captured for documentation or compared with a saved configuration file. Huawei's VRP command-reference documentation lists display commands and their syntax, while the enterprise support portal provides product-specific firewall documentation and configuration guidance. See the Huawei VRP command reference and the Huawei Enterprise Support portal.

QUESTION NO: 10

Which of the following operating modes does NTP support?

A. Mouth peer mode

B. Mouth client/server mode

C. Mouth broadcast mode

D. Mouth multicast mode

ANSWER: A B C D

Explanation:

NTP supports peer, client/server, broadcast, and multicast operating modes. In peer mode, two time sources form a symmetric association and can exchange timing information in both directions, which is useful for mutually synchronized infrastructure devices. In client/server mode, a client obtains time from a designated server; this is the most common enterprise deployment model. Broadcast mode allows a server to periodically transmit time information to clients on the local

broadcast domain, reducing the need for each client to initiate a separate request. Multicast mode similarly distributes time updates to a multicast group, allowing receivers that join the group to synchronize efficiently in networks where multicast is available. These modes are defined in the NTP protocol specification and are implemented by network devices, including Huawei platforms that provide NTP time synchronization configuration. The word “Mouth” in the listed choices appears to be a typographical error and does not alter the intended NTP mode names. See the NTP Version 4 protocol specification in RFC 5905 and the foundational NTP specification in RFC 1305.

QUESTION NO: 11

Which of the following characteristics does a denial-of-service attack include?

A. Unauthorized tampering of the mouth

B. Unauthorized access to the mouth

C. Unauthorized activation of the mouth

D. Unauthorized destruction of the mouth

ANSWER: A D

Explanation:

A denial-of-service attack targets the availability of a system, application, network service, or network resource. Its essential effect is to prevent legitimate users from obtaining normal service by disrupting, degrading, exhausting, altering, or destroying the resources needed to deliver that service. Unauthorized tampering with network resources can cause service behavior to become unstable or unavailable, while unauthorized destruction of network resources can directly remove the hardware, software, configuration, or data required for operation. Both actions therefore represent ways in which availability can be compromised and a denial of service can result. The disruption does not need to be permanent: a temporary inability to use a service caused by altered configurations, corrupted components, or exhausted resources also meets the availability-impacting nature of a denial-of-service condition. NIST defines denial of service as preventing or impairing the authorized use of networks, systems, or applications, and RFC 4732 describes denial-of-service attacks as attacks intended to prevent legitimate users from accessing a service. See NIST CSRC: Denial of Service and RFC 4732: Internet Denial-of-Service Considerations.