

Huawei.H12-711.by.Atony.263q

Number: H12-711  
Passing Score: 800  
Time Limit: 120  
File Version: 4.0

**Exam Code: H12-711**

**Exam Name: HCNA-Security-CBSN (Huawei Certified Network Associate - Constructing Basic Security Network)**



## Exam A

### QUESTION 1

Social engineering is a means of harm such as deception, harm, etc., through psychological traps such as psychological weaknesses, instinctive reactions, curiosity, trust, and greed of victims.

- A. True
- B. False

**Correct Answer: A**

**Section:**

### QUESTION 2

Common information security standards and specifications mainly include the national level protection system (GB), \_\_\_\_\_, the American standard TCSEC and the European Union standard ITSEC.[fill in the blank]

- A. ISO27001

**Correct Answer: A**

**Section:**

### QUESTION 3

In the classification of information security classified protection systems, which of the following levels define if an information system is compromised. Will it cause damage to social order and public interests? ( ) [Multiple Choice Questions]

- A. The third level of security marking protection
- B. Level 4 Structural Protection
- C. Second-level system audit protection
- D. The first level of user self-protection

**Correct Answer: A, B, C**

**Section:**

### QUESTION 4

The attacker sends a SYN message with the same source address and destination address, or the source address is the loopback address to the target host (the source port and destination port are the same, causing the attacker to send a SYN-ACK message to its own address) What kind of attack is this behavior black? ( ) [Multiple choice]\*

- A. Smurf attack
- B. SYN Flood Attack
- C. TCP Spoofing Attack
- D. Land attack

**Correct Answer: D**

**Section:**

### QUESTION 5

Huawei's Agile-Controller products belong to \_\_\_\_\_ in the HiSec solution.[fill in the blank]

A. control

**Correct Answer: A**

**Section:**

**QUESTION 6**

In the Linux system, if the user wants to enter the tmp folder in the root directory, the command that needs to be entered is \_\_\_\_\_/tmp.[fill in the blank]\*

A. cd

**Correct Answer: A**

**Section:**

**QUESTION 7**

Applying for special funds for emergency response and purchasing emergency response software and hardware equipment belong to the work content of which stage of the network's complete emergency response?

- A. preparation stage
- B. Inhibition stage
- C. response phase
- D. recovery phase

**Correct Answer: A**

**Section:**



**QUESTION 8**

Equipment sabotage attacks are generally not easy to cause information leakage, but usually cause interruption of network communication services.

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 9**

about Internet users andVPNIn the description of access user authentication, which of the following is false?

- A. Internet users andVPNAccess to user shared data, user attribute check (user status, account expiration time, etc.) VPNAccess takes effect
- B. The process of online users using local authentication or server authentication is basically the same. Both users are authenticated through the authentication domain, and the user triggering method is also the same.
- C. VPNAfter users access the network, they can access the network resources of the enterprise headquarters, and the firewall can control the network resources that can be accessed based on the user name
- D. VPNAfter the access user is authenticated, it will go online in the user online list at the same time

**Correct Answer: D**

**Section:**

**QUESTION 10**

Which of the following statements about the patch is incorrect?

- A. A patch is a small program made by the original author of the software for a discovered vulnerability
- B. Not patching does not affect the operation of the system, so whether patching is irrelevant or not.
- C. Patches are generally updated continuously.
- D. Computer users should download and install the latest patches in a timely manner to protect their systems

**Correct Answer: B**

**Section:**

#### QUESTION 11

Which of the following is P2DR the core part of the model?

- A. PolicyStrategy
- B. Protectionprotection
- C. Detectiondetect
- D. Responseresponse

**Correct Answer: A**

**Section:**

#### QUESTION 12

Evidence identification needs to address the verification of the integrity of the evidence and determine whether it meets the applicable standards. Which of the following statements is correct about the criteria for identification of evidence?

- A. The relevance standard means that if the telephony evidence can have a substantial impact on the facts of the case to a certain extent, the court should rule that it is relevant.
- B. The standard of objectivity means that the acquisition, storage, and submission of electronic evidence should be legal, and not constitute a serious violation of basic rights such as national interests, social welfare, and personal privacy.
- C. The standard of legality is to ensure that the content of electronic evidence remains unchanged from the initial acquisition and collection to the submission and use as litigation evidence.
- D. The standard of fairness refers to the evidentiary material obtained by the legal subject through legal means, which has evidential capacity.

**Correct Answer: A**

**Section:**

#### QUESTION 13

Data analysis technology is to find and match keywords or key phrases in the acquired data stream or information stream, and analyze the correlation of time. Which of the following is not an evidence analysis technique?

- A. Cryptography, data decryption technology
- B. Digital Abstract Analysis Technology of Documents
- C. Techniques for discovering connections between different pieces of evidence
- D. Spam Tracking Technology

**Correct Answer: D**

**Section:**

#### QUESTION 14

about AH and ESP Security protocol, which of the following options is true? (multiple choice)

- A. AHCan provide encryption and authentication functions
- B. ESPCan provide encryption and authentication functions
- C. AH The protocol number is51
- D. ESPTThe protocol number is51

**Correct Answer: B, C**

**Section:**

**QUESTION 15**

Which of the following DDoS attack types is an attack?

- A. snooping scan attack
- B. Malformed Packet Attack
- C. special packet attack
- D. traffic attack

**Correct Answer: D**

**Section:**

**QUESTION 16**

aboutSSL VPNTechnology, which of the following statements is false?

- A. SSL VPNtechnology can be perfectly adapted toNATthrough the scene
- B. SSL VPNTThe encryption of the technology only takes effect at the application layer
- C. SSL VPNRequires a dial-up client
- D. SSL VPNTechnology expands the reach of the enterprise's network

**Correct Answer: C**

**Section:**

**QUESTION 17**

Which of the following options can bewindowsDo you do it in the advanced settings of the firewall?  
(multiple choice)

- A. Restore defaults
- B. Change notification rules
- C. Set up connection security rules
- D. Set up inbound and outbound rules

**Correct Answer: C, D**

**Section:**

**QUESTION 18**

existUSGConfiguration on the series firewallINAT Server, will produceserver-mapTable, which of the following is not part of this representation?

- A. PurposeIP
- B. destination port number



- C. agreement number
- D. sourceIP

**Correct Answer: D**

**Section:**

**QUESTION 19**

Which of the following attacks is not a special packet attack?

- A. ICMPredirected packet attack
- B. ICMPUnreachable Packet Attack
- C. IPaddress scanning attack
- D. oversizedICMPPacket attack

**Correct Answer: C**

**Section:**

**QUESTION 20**

Which of the following attacks is not a malformed packet attack?

- A. Teardropattack
- B. Smurfattack
- C. TCPFragmentation attack
- D. ICMPUnreachable Packet Attack

**Correct Answer: D**

**Section:**

**QUESTION 21**

"Caesar Cipher"Data is mainly encrypted by using a specific specification of stick.

- A. True
- B. False

**Correct Answer: B**

**Section:**

**QUESTION 22**

Which of the following are remote authentication methods? (multiple choice)

- A. RADIUS
- B. Local
- C. HWTACACS
- D. LLDP

**Correct Answer: A, C**

**Section:**



**QUESTION 23**

Which of the following is true about the firewall log when the firewall hard drive is in place?

- A. Administrators can post content logs to view network threat detection and defense records
- B. Administrators can learn about user security risk behaviors and the reasons for being alerted or blocked through threat logs
- C. Through the user activity log, administrators can obtain information such as user behaviors, searched keywords, and the effectiveness of audit policy configurations.
- D. The administrator can learn the security policy of the traffic hit through the policy hit log, which can be used for fault location when a problem occurs.

**Correct Answer: D**

**Section:**

**QUESTION 24**

existClient-Initiated VPNDuring the configuration, it is generally recommended to plan the address pool and the headquarters network address as different network segments. Otherwise, the proxy forwarding function needs to be enabled on the gateway device.

- A. True
- B. False

**Correct Answer: B**

**Section:**

**QUESTION 25**

Which of the following is an encryption technique used in digital envelopes?

- A. Symmetric encryption algorithm
- B. Asymmetric encryption algorithm
- C. hash algorithm
- D. Stream Encryption Algorithm

**Correct Answer: A, B**

**Section:**

**QUESTION 26**

Firewall in addition to supporting built-inPortalIn addition to authentication, it also supports customizationPortalauthentication, when using customPortalDuring authentication, there is no need to deploy externalPortalserver.

- A. True
- B. False

**Correct Answer: B**

**Section:**

**QUESTION 27**

NAPTtechnology can realize a public networkIPThe address is used by multiple private network hosts.

- A. True
- B. False



**Correct Answer: A**

**Section:**

**QUESTION 28**

IPSec VPN technology adoption ESP Security protocol encapsulation is not supported NAT cross because ESP The header of the message is encrypted

- A. True
- B. False

**Correct Answer: B**

**Section:**

**QUESTION 29**

about SSL VPN description, which of the following is correct?

- A. Can be used without a client
- B. yes IPsec to encrypt
- C. exist NAT crossing problem
- D. No authentication required

**Correct Answer: A**

**Section:**

**QUESTION 30**

some applications such as Oracle For database applications, the firewall session connection is interrupted due to no data flow transmission for a long time, resulting in service interruption. Which of the following is the optimal solution?

- A. Configure a long-term connection for a service
- B. turn on ASPF Features
- C. Optimize security policies
- D. Enable shard cache

**Correct Answer: A**

**Section:**

**QUESTION 31**

"Implement security monitoring and management of information and information systems to prevent illegal use of information and information systems", in order to achieve which feature in information security?

- A. confidentiality
- B. controllability
- C. non-repudiation
- D. integrity

**Correct Answer: B**

**Section:**

**QUESTION 32**





When configuring a security policy, a security policy can refer to an address set or configure multiple purposes IP address.

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 33**

Which of the following options is not part of the quintuple range?

- A. source IP
- B. source MAC
- C. Purpose IP
- D. destination port

**Correct Answer: B**

**Section:**

**QUESTION 34**

about Client-Initialized of L2TP VPN, which of the following statements is false?

- A. remote user access internet After that, it can be directly sent to the remote LNS initiate L2TP tunnel connection request
- B. LNS The device receives the user L2TP connection request, the user can be authenticated according to the user name and password
- C. LNS Assign private keys to remote users IP address
- D. Remote users do not need to install VPN client software

**Correct Answer: D**

**Section:**

**QUESTION 35**

Regarding the description of vulnerability scanning, which of the following is false?

- A. Vulnerability scanning is a network-based technology for remotely monitoring the security performance vulnerabilities of target networks or hosts, and can be used to conduct simulated attack experiments and security audits.
- B. Vulnerability scanning is used to detect whether there are vulnerabilities in the target host system, generally scanning the target host for specific vulnerabilities
- C. Vulnerability scanning is a passive preventive measure that can effectively avoid hacker attacks
- D. can be based on ping scan and port scan results for vulnerability scanning

**Correct Answer: C**

**Section:**

**QUESTION 36**

Regarding the statement of firewall security policy, which of the following options is false?

- A. If the security policy is permit, the discarded packets will not be accumulated "Hits"
- B. When configuring a security policy name, the same name cannot be reused

- C. Adjust the order of security policies without saving configuration files and take effect immediately
- D. HuaweiUSGThe security policy entries of the series firewall cannot exceed128strip

**Correct Answer: A**

**Section:**

**QUESTION 37**

TCSECWhich of the following protection levels are included in the standard? (multiple choice)

- A. Verify protection level
- B. Mandatory protection level
- C. autonomous protection level
- D. Passive protection level

**Correct Answer: A, B, C**

**Section:**

**QUESTION 38**

Which of the following options arePKIComponents of the architecture? (multiple choice)

- A. end entity
- B. Certificate Authority
- C. Certificate Registration Authority
- D. certificate store

**Correct Answer: A, B, C, D**

**Section:**

**QUESTION 39**

"observant"and"remain skeptical"Can help us better identify security threats in the online world

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 40**

In tunnel encapsulation mode.IPSecThere is no need to have a route to the destination private network segment during configuration, because the data will be re-encapsulated to use the newIPThe header looks up the routing table.

- A. True
- B. False

**Correct Answer: B**

**Section:**

**QUESTION 41**



aboutwindowsFirewall description, which of the following options are correct? (multiple choice)

- A. windowsThe firewall can only allow or prohibit preset programs or functions and programs installed on the system, and cannot customize the release rules according to the protocol or port number.
- B. windowsThe firewall can not only allow or prohibit preset programs or functions and programs installed on the system, but also support its own custom release rules based on protocols or port numbers.
- C. If you are settingwindowsDuring the firewall process, the Internet cannot be accessed. You can use the restore default function to quickly restore the firewall to its initial state.
- D. windows the firewall can also change the notification rules in a closed state

**Correct Answer: B, C**

**Section:**

#### QUESTION 42

Which of the following statements about investigation and evidence collection is correct?

- A. Evidence is not necessarily required during the investigation
- B. Evidence obtained by wiretapping is also valid
- C. Ideally, law enforcement agencies should be involved in all investigative and evidence-gathering processes
- D. Documentary evidence is required in computer crime

**Correct Answer: C**

**Section:**

#### QUESTION 43

Which of the following statements about Internet user management is false?

- A. Each user group can include multiple users and user groups
- B. Each user group can belong to multiple parent user groups
- C. The system has one by defaultdefaultUser group, which is also the system default authentication domain
- D. Each user belongs to at least one user group and can also belong to multiple user groups

**Correct Answer: B**

**Section:**

#### QUESTION 44

Which of the following does not belong toP2DRin the modelDetectionThe method used in the link?

- A. real time monitoring
- B. detect
- C. Call the police
- D. shut down service

**Correct Answer: D**

**Section:**

#### QUESTION 45

Which of the following does not belong toLINUXoperating system?

- A. CentOS



- B. RedHat
- C. Ubuntu
- D. MAC OS

**Correct Answer: D**

**Section:**

**QUESTION 46**

In some scenarios, it is necessary toIPAddress conversion, but also to the purposeIPaddress translation, which of the following techniques is used in this scenario?

- A. two-wayNAT
- B. sourceNAT
- C. NAT-Server
- D. NAT ALG

**Correct Answer: A**

**Section:**

**QUESTION 47**

Which of the following protocols can guarantee the confidentiality of data transmission? (multiple choice)

- A. Telnet
- B. SSH
- C. FTP
- D. HTTPS

**Correct Answer: B, D**

**Section:**

**QUESTION 48**

existUSGOn the series firewall, configurewebAfter the redirection function is enabled, the authentication page cannot pop up. Which of the following is not the cause of the failure?

- A. The authentication policy is not configured or the authentication policy is incorrectly configured
- B. UnopenedwebAuthentication function
- C. browserSSLVersion and Firewall Authentication PageSSLversion mismatch
- D. The port number of the authentication page service is set to8887

**Correct Answer: D**

**Section:**

**QUESTION 49**

One of the following options for information security management systems (ISMS) Which of the four stages describes the sequence correctly?

- A. Plan->Check->Do->Action
- B. Check->Plan->Do->Action
- C. Plan->Do->Check->Action
- D. Plan->Check->Action->Do



**Correct Answer: C**

**Section:**

**QUESTION 50**

In the information security system construction management cycle, which of the following behaviors is "check" What needs to be implemented in the link?

- A. Safety management system design
- B. Safety management system implementation
- C. Risk assessment
- D. Safety management system operation monitoring

**Correct Answer: C**

**Section:**

**QUESTION 51**

- A. this firewallVGMPgroup status isActive
- B. this firewallG1/0/0andG1/0/1interfaceVRRPgroup status isstandby
- C. this firewallHRPThe heartbeat line interface isG1/0/0andG1/0/1
- D. This firewall must be in preemptive state

**Correct Answer: B**

**Section:**

**QUESTION 52**

Servers are classified by form factor, which of the following types can be classified? (multiple choice)

- A. blade server
- B. tower server
- C. rack server
- D. x86server

**Correct Answer: A, B, C**

**Section:**

**QUESTION 53**

Common scanning attacks include: port scanning tools, vulnerability scanning tools, application scanning tools and database scanning tools, etc.

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 54**

The firewall is divided according to the protection object, windowsfirewall belongs toó ?



- A. Software Firewall
- B. hardware firewall
- C. Stand-alone firewall
- D. Internet Firewall

**Correct Answer: C**

**Section:**

**QUESTION 55**

Which of the following options are PKI entity orientation CA? How to apply for a local certificate?  
(multiple choice)

- A. Online Application
- B. local application
- C. online application
- D. Apply offline

**Correct Answer: A, D**

**Section:**

**QUESTION 56**

Intrusion Prevention System (IPS, intrusion prevention system) is a defense system that can block in real time when an intrusion is detected

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 57**

Which of the following is not a symmetric encryption algorithm?

- A. DES
- B. 3DES
- C. AES
- D. RSA

**Correct Answer: D**

**Section:**

**QUESTION 58**

Which of the following options are correct regarding configuring firewall security zones? (multiple choice)

- A. The firewall has four security zones by default, and the priority of the four security zones cannot be modified
- B. A firewall can have up to 12 safe areas
- C. Firewall can create two security zones of the same priority
- D. When data flows between different security zones, the security check of the device will be triggered and the corresponding security policy will be implemented



**Correct Answer: A, D**

**Section:**

**QUESTION 59**

certificates, self-signed certificates, etc.

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 60**

Which of the following attacks is not a cyber attack?

- A. IP spoofing attack
- B. Smurfl attack
- C. MAC address spoofing attack
- D. ICMP attack

**Correct Answer: C**

**Section:**

**QUESTION 61**

About the rootCACertificate, which of the following descriptions is incorrect?

- A. Issuer isCA
- B. The certificate subject name isCA
- C. public key information isCA's public key
- D. signature isCAgenerated by public key encryption

**Correct Answer: D**

**Section:**

**QUESTION 62**

Which of the following configurations can achieveNAT ALGFeatures?

- A. nat alg protocol
- B. alg protocol
- C. nat protocol
- D. detect protocol

**Correct Answer: D**

**Section:**

**QUESTION 63**

About firewall gateways forHTTPWhich of the following statements is false about the protocol'santivirus response?



- A. When the gateway device blocks HTTP after connecting, push to the client webpage and generate log
- B. Response methods include announcement and blocking
- C. In alarm mode, the device only generates logs, which is not correct. HTTP files transmitted by the protocol are processed and sent out
- D. Blocking means that the device is disconnected from the HTTP server connection and block file transfer

**Correct Answer: B**

**Section:**

#### QUESTION 64

Which of the following does not belong to USG User authentication method in firewall?

- A. Certification-free
- B. Password authentication
- C. sign in
- D. Fingerprint authentication

**Correct Answer: D**

**Section:**

#### QUESTION 65

firewall GE1/0/1 and GE1/0/2 mouth belongs to DMZ area, if you want to implement GE1/0/1 The connected area is accessible GE1/0/2 Connected area, which of the following is correct?

- A. needs to be configured Local arrive DMZ security policy
- B. No configuration required
- C. Interzone security policy needs to be configured
- D. needs to be configured DMZ arrive local security policy



**Correct Answer: B**

**Section:**

#### QUESTION 66

For the process of forwarding session header packets between firewall domains, there are the following steps:

- 1, look up the routing table
- 2, find the inter-domain packet filtering rules
- 3, lookup session table
- 4, find the blacklist

Which of the following is in the correct order?

- A. 1->3->2->4
- B. 3->2->1->4
- C. 3->4->1->2
- D. 4->3->1->2

**Correct Answer: C**

**Section:**



**QUESTION 67**

The administrator wants to be clear about the current session table. Which of the following commands is correct?

- A. clear firewall session table
- B. reset firewall session table
- C. display firewall session table
- D. display session table

**Correct Answer: B**

**Section:**

**QUESTION 68**

Which of the following are the basic functions of antivirus software? (multiple choice)

- A. virus protection
- B. Find viruses
- C. remove virus
- D. replication virus

**Correct Answer: A, B, C**

**Section:**

**QUESTION 69**

EuropeTCSECThe guidelines are divided into two modules, functional and evaluation, and are mainly used in the military, government and commercial fields

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 70**

In the future development trend of information security, terminal detection is an important part. Which of the following methods fall under the category of endpoint detection? (multiple choice)

- A. Install host antivirus software
- B. Monitor and remember external devices
- C. Block users from accessing public search engines
- D. Monitor host registry modification records

**Correct Answer: A, D**

**Section:**

**QUESTION 71**

useiptablesWrite a rule that doesn't allow172.16.0.0/16Which of the following rules is correct?

- A. iptables -t fielter -A INPUT -s 172.16.0.0/16 -p all -j DROP

- B. iptables -t fielter -P INPUT -s 172.16.0.0/16 -p all -j DROP
- C. iptables -t fielter -P INPUT -s 172.16.0.0/16 -p all -j ACCEPT
- D. iptables -t fielter -P INPUT -d 172.16.0.0/16 -p all -j ACCEPT

**Correct Answer: A**

**Section:**

#### QUESTION 72

aboutHRPWhich of the following options is not included in the content of the master/slave configuration consistency check?

- A. NATStrategy
- B. Whether the heartbeat interface with the same sequence number is configured
- C. The next hop and outgoing interface of the static route
- D. Authentication Policy

**Correct Answer: C**

**Section:**

#### QUESTION 73

existUSGseries firewall, you can use. The function provides well-known application services for nonwell- known ports.

- A. Port Mapping
- B. MACandIPaddress binding
- C. packet filtering
- D. Long connection

**Correct Answer: A**

**Section:**

#### QUESTION 74

Questionnaire design principles do not include which of the following?

- A. integrity
- B. openness
- C. specificity
- D. consistency

**Correct Answer: D**

**Section:**

#### QUESTION 75

want to implement security policy "Anti-virus function", must be License activation.

- A. True
- B. False

**Correct Answer: A**



**Section:**

**QUESTION 76**

About NAT The configuration commands for the address pool are as follows: no-pat The meaning of the parameters is:

```
nat address-group 1
section 0 202.202.168.10 202.202.168.20
mode no-pat
```

- A. no address translation
- B. port multiplexing
- C. Do not translate source ports
- D. Do not convert destination port

**Correct Answer: C**

**Section:**

**QUESTION 77**

On the surface, threats such as viruses, loopholes, and Trojan horses are the causes of information security incidents, but at the root, information security incidents are also closely related to people and the information system itself.

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 78**

When connecting in a public place Wi-Fi Which of the following actions is relatively safer?

- A. The connection is not encrypted Wi-Fi hot spot
- B. Connection is paid by the operator Wi-Fi hotspot and web browsing only
- C. connect unencrypted for free Wi-Fi make online shopping
- D. Connection encrypted for free Wi-Fi Perform online transfer operations

**Correct Answer: B**

**Section:**

**QUESTION 79**

Which of the following options are available in windows Do you do it in the advanced settings of the firewall? (multiple choice)

- A. Restore defaults
- B. Change notification rules
- C. Set up connection security rules
- D. Set up inbound and outbound rules

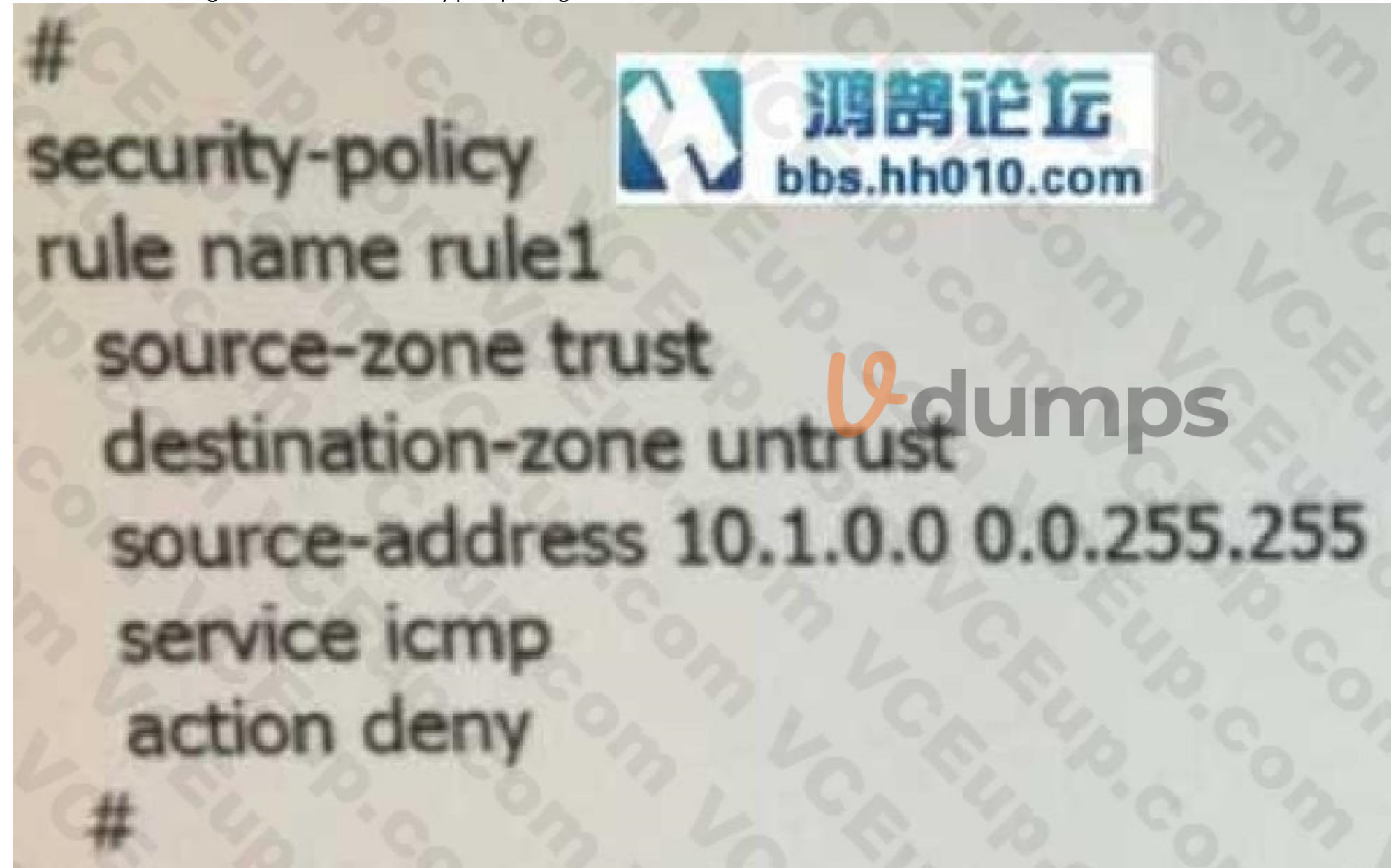
**Correct Answer: A, B, C, D**

**Section:**

**QUESTION 80**

Which of the following is true about the security policy configuration command?

```
#
security-policy
rule name rule1
source-zone trust
destination-zone untrust
source-address 10.1.0.0 0.0.255.255
service icmp
action deny
#
```



- A. prohibited fromtrustRegional accessuntrustarea and the destination address is10.1.10.10hostICMPmessage
- B. prohibited fromtrustRegional accessuntrustarea and the destination address is10.1.0.0/16All hosts on the segmentICMPmessage
- C. prohibited fromtrustRegional accessuntrustregion and the source address is10.1.0.0/16All hosts from the network segmentICMPmessage
- D. prohibited fromtrustRegional accessuntrustregion and the source address is10.2.10.10All hosts from hostICMPmessage

**Correct Answer: C**

**Section:**

**QUESTION 81**

In information security prevention, commonly used security products are firewalls, Anti-DDoS equipment and IPS/IDS equipment

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 82**

If the administrator uses the default authentication domain verifies the user, and the user only needs to enter the user name when logging in; if the administrator uses the newly created authentication domain to authenticate the user, the user needs to enter the user name when logging in. "username@Certified domain name"

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 83**

Digital certificate technology solves the problem that the public key owner cannot be determined in digital signature technology

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 84**

Which of the following options are technical characteristics of an intrusion prevention system?  
(multiple choice)

- A. online mode
- B. real-time blocking
- C. Self-learning and adaptive
- D. In-line deployment

**Correct Answer: A, B, C**

**Section:**

**QUESTION 85**

Regarding the firewall security policy, the following items are correct?

- A. By default, the security policy can control unicast packets and broadcast packets.
- B. By default, the security policy can control multicast
- C. By default, the security policy only controls unicast packets..



D. By default, the security policy can control unicast packets, broadcast packets, and multicast packets.

**Correct Answer: C**

**Section:**

**QUESTION 86**

Which of the following information is encrypted during the use of digital envelopes? (multiple choice)

- A. Symmetric key
- B. User data
- C. Receiver's public key
- D. Receiver's private key

**Correct Answer: A, B**

**Section:**

**QUESTION 87**

Which of the following options are ISO 27001 the field of certification? (multiple choice)

- A. Access control
- B. personnel safety
- C. Vulnerability Management
- D. business continuity management

**Correct Answer: A, B, C, D**

**Section:**

**QUESTION 88**

Which of the following statements about firewalls is correct?

- A. The firewall cannot transparently access the network.
- B. Adding a firewall to the network will inevitably change the topology of the network.
- C. To avoid a single point of failure, the firewall only supports bypass deployment
- D. Depending on the usage scenario, the firewall can be deployed in a transparent mode or a threebedroom type.

**Correct Answer: D**

**Section:**

**QUESTION 89**

at Huawei USG On a series device, the administrator wants to wipe the configuration file, which of the following commands is correct?

- A. clear saved-configuration
- B. reset saved-configuration
- C. reset current-configuration
- D. reset running-configuration

**Correct Answer: B**



**Section:**

**QUESTION 90**

Which of the following options is correct for the description of a buffer overflow attack?(multiple choice)

- A. Buffer overflow attacks exploit the flaws of software systems in memory operations to run attack code with high operating privileges.
- B. Buffer overflow attacks have nothing to do with the vulnerabilities and architecture of the operating system.
- C. Buffer overflow attacks are one of the most common ways to attack the behavior of software systems
- D. Buffer overflow attacks are application-layer attacks.

**Correct Answer: A, C, D**

**Section:**

**QUESTION 91**

Security technology has different methods in different technical levels and fields. Which of the following devices can be used for network layer security? (multiple choice)

- A. Vulnerability Scanning Device
- B. firewall
- C. Anti-DDoS equipment
- D. IPS/IDS equipment

**Correct Answer: B, C, D**

**Section:**

**QUESTION 92**

IPSEC VPN technology adoption ESP Security protocol encapsulation is not supported NAT cross because ESP The header of the message is encrypted

- A. True
- B. False

**Correct Answer: B**

**Section:**

**QUESTION 93**

Which of the following options are SSL VPN function? (multiple choice)

- A. User Authentication
- B. port scan
- C. File Sharing
- D. WEB rewrite

**Correct Answer: A, C**

**Section:**

**QUESTION 94**

In the process of digital signature, which of the following is mainly carried out HASH Algorithms thereby verifying the integrity of data transmissions?





- A. User data
- B. Symmetric key
- C. Receiver's public key
- D. Receiver's private key

**Correct Answer: A**

**Section:**

**QUESTION 95**

Which of the following traffic matches the authentication policy will trigger authentication?

- A. Access device or device-initiated traffic
- B. DHCP,BGP,OSPF,LDPmessage
- C. visitor accessHTTPbusiness traffic
- D. Article 1HTTPCorresponding to the business data flowDNSmessage

**Correct Answer: C**

**Section:**

**QUESTION 96**

firewallGE1/0/1andGE1/0/2mouth belongs toDMZarea, if you want to implementGE1/0/1The connected area is accessibleGE1/0/2Connected area, which of the following is correct?

- A. needs to be configuredlocalarriveDMZsecurity policy
- B. No configuration required
- C. Interzone security policy needs to be configured
- D. needs to be configuredDMZarrivelocalsecurity policy

**Correct Answer: B**

**Section:**

**QUESTION 97**

Ways to use a computer to store information about criminal activity that is not a computer crime

- A. True
- B. False

**Correct Answer: B**

**Section:**

**QUESTION 98**

aboutIKE SA, which of the following descriptions is false?

- A. IKE SAis bidirectional
- B. IKEis based onUDPapplication layer protocol
- C. IKE SAit's forIPSec SAServices
- D. The encryption algorithm used by user data packets isIKE SADecide





**Correct Answer: D**

**Section:**

**QUESTION 99**

aboutVPN, which of the following statements is false?

- A. Virtual private network is cheaper than private line
- B. VPNTechnology necessarily involves encryption
- C. VPNTechnology is a technology that multiplexes logical channels on actual physical lines
- D. VPNThe emergence of technology allows traveling employees to remotely access internal corporate servers

**Correct Answer: B**

**Section:**

**QUESTION 100**

Which of the following areFTPThe standard port number of the protocol? (multiple choice)

- A. 20
- B. twenty one
- C. twenty three
- D. 80

**Correct Answer: A, B**

**Section:**

**QUESTION 101**

The information security level protection is to improve the overall security level of the country, and at the same time reasonably optimize the allocation of security resources, so that it can send back the greatest security and economic benefits.

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 102**

For network security incidents that occur, remote emergency response is generally adopted first. If the problem cannot be solved for the customer through remote access, after confirmation by the customer, go to the local emergency response process

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 103**

Usually we divide servers into two categories: general-purpose servers and functional servers. Which of the following options meets this classification standard?



- A. By application level
- B. By use
- C. By shape
- D. By Architecture

**Correct Answer: B**

**Section:**

**QUESTION 104**

NAPT technology can realize a public network IP address is used by multiple private network hosts

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 105**

Firewall usage hrp standby config enable After the command to enable the configuration function of the standby device, all the information that can be backed up can be configured directly on the standby device, and the configuration on the standby device can be synchronized to the active device.

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 106**

Which of the following options are characteristic of symmetric encryption algorithms? (multiple choice)

- A. Fast encryption
- B. Confidential is slow
- C. Insecure key distribution
- D. High security of key distribution

**Correct Answer: A, C**

**Section:**

**QUESTION 107**

Which of the following options are at risk from traffic-based attacks? (multiple choice)

- A. network down
- B. Server down
- C. data stolen
- D. The web page has been tampered with

**Correct Answer: A, B**



**Section:**

**QUESTION 108**

Intrusion Prevention System (IPS) is a defense system that can block in real time when an intrusion is detected

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 109**

Which of the following options is not included about HRP in the content of the master/slave configuration consistency check?

- A. NATStrategy
- B. Whether the heartbeat interface with the same sequence number is configured
- C. The next hop and outgoing interface of the static route
- D. Authentication Policy

**Correct Answer: C**

**Section:**

**QUESTION 110**

about NAT Configuration statement, which of the following is false?

- A. Configure sources in transparent mode NAT, the firewall does not support easy-ip Way
- B. in the address pool IP address can be NAT server public network IP address overlap
- C. in the network VoIP When doing business, no configuration is required NAT ALG
- D. Firewall does not support ESP and AH message NAT convert

**Correct Answer: D**

**Section:**

**QUESTION 111**

Which of the following options is correct regarding the actions of the security policy and the description of the security profile? (multiple choice)

- A. If the action of the security policy is "prohibit", the device will discard this traffic, and will not perform content security checks in the future.
- B. The security profile can take effect even if the action is allowed under the security policy
- C. The security profile must be applied under the security policy whose action is allowed to take effect
- D. If the security policy action is "allow", the traffic will not match the security profile

**Correct Answer: A, C**

**Section:**

**QUESTION 112**

Which of the following options are included in the protection of data by encryption technology during data transmission? (multiple choice)



- A. confidentiality
- B. controllability
- C. integrity
- D. source check

**Correct Answer: A, C, D**

**Section:**

**QUESTION 113**

After a cyber-attack event occurs, set up an isolation area, summarize data, and estimate losses according to the plan. Which of the above actions belong to the work content of the cyber security emergency response?

- A. preparation stage
- B. detection stage
- C. Inhibition stage
- D. recovery phase

**Correct Answer: C**

**Section:**

**QUESTION 114**

IPSec VPNAn asymmetric encryption algorithm is used to encrypt the transmitted data

- A. True
- B. False



**Correct Answer: B**

**Section:**

**QUESTION 115**

The digital certificate fairs the public key through a third-party organization, thereby ensuring the non-repudiation of data transmission. Therefore, to confirm the correctness of the public key, only the certificate of the communicating party is required.

- A. True
- B. False

**Correct Answer: B**

**Section:**

**QUESTION 116**

Digital signature is to generate digital fingerprint by using hash algorithm, so as to ensure the integrity of data transmission

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 117**

About firewall fragmentation Which of the following options is correct? (multiple choice)

- A. By default, the firewall caches fragmented packets
- B. After the direct forwarding of fragmented packets is configured, the firewall will forward the fragmented packets that are not the first fragmented packets according to the interzone security policy.
- C. For fragmented packets, NATALGnot supportedSIPFragmented Packet Processing
- D. By default, aIPv4The maximum number of fragment buffers for packets is32,OneIPv6The maximum number of fragment buffers for packets is255

**Correct Answer: A, C, D**

**Section:**

**QUESTION 118**

SIPprotocol usageSDPmessage to establish a session,SDPThe message contains a remote address or a multicast address

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 119**

Which of the following attacks is not a cyber attack?

- A. IPspoofing attack
- B. Smurfattack
- C. MACaddress spoofing attack
- D. ICMPattack

**Correct Answer: C**

**Section:**

**QUESTION 120**

SNMPWhat versions of the protocol are there? (multiple choice)

- A. SNMPv1
- B. SNMPv2b
- C. SNMPv2c
- D. SNMPv3

**Correct Answer: A, C, D**

**Section:**

**QUESTION 121**

aboutVGMPDescription of the managed preemption function, which of the following is false?

- A. By default,VGMPThe preemption function of the management group is enabled
- B. By default,VGMPThe preemption delay time of the management group is40s
- C. Preemption means that when the original faulty master device recovers, its priority will be restored. At this time, it can preempt its own state as the master device again.



D. when VRRP Backup group added to VGMP After managing the group, VRRP The original preemption function on the backup group fails

**Correct Answer: B**

**Section:**

**QUESTION 122**

exist IPsec VPN In the transmission mode, which part of the encrypted data packet is?

- A. Network layer and upper layer data packets
- B. Original IP header
- C. new IP header
- D. Transport layer and upper layer data packets

**Correct Answer: D**

**Section:**

**QUESTION 123**

about windows log, which of the following descriptions is false?

- A. System logs are used to record events generated by operating system components, mainly including crashes of drivers, system components and application software, and data
- B. windows server 2008 The system logs are stored in Application.evtx middle
- C. The application log contains events recorded by applications or system programs, mainly recording program operation events
- D. windows server 2008 The security log is stored in security.evtx middle

**Correct Answer: B**

**Section:**



**QUESTION 124**

against IP spoofing attack (IP Spoofing), which of the following is an error?

- A. IP spoofing attacks are based on IP address trust relationship to initiate
- B. IP After a successful spoofing attack, the attacker can use forged arbitrary IP The address impersonates a legitimate host to access key information
- C. The attacker needs to put the source IP address masquerading as a trusted host and send SYN mark Note the data segment request connection
- D. based on IP The hosts in the trust relationship of the addresses can log in directly without entering password authentication.

**Correct Answer: C**

**Section:**

**QUESTION 125**

exist USG In the series firewalls, which of the following commands can be used to query NAT conversion result?

- A. display nat translation
- B. display firewall session table
- C. display current nat
- D. display firewall nat translation

**Correct Answer: B**

**Section:**

**QUESTION 126**

The preservation of electronic evidence is directly related to the legal validity of the evidence, and the authenticity and reliability of the preservation in compliance with legal procedures can be guaranteed. Which of the following is not an evidence preservation technique?

- A. Encryption Technology
- B. digital certificate technology
- C. digital signature technology
- D. Packet Tag Tracking Technology

**Correct Answer: D**

**Section:**

**QUESTION 127**

Which of the following areHRP(Huawei Redundancy Protocol) protocol can back up state information? (multiple choice)

- A. session table
- B. ServerMapentry
- C. Dynamic blacklist
- D. routing table

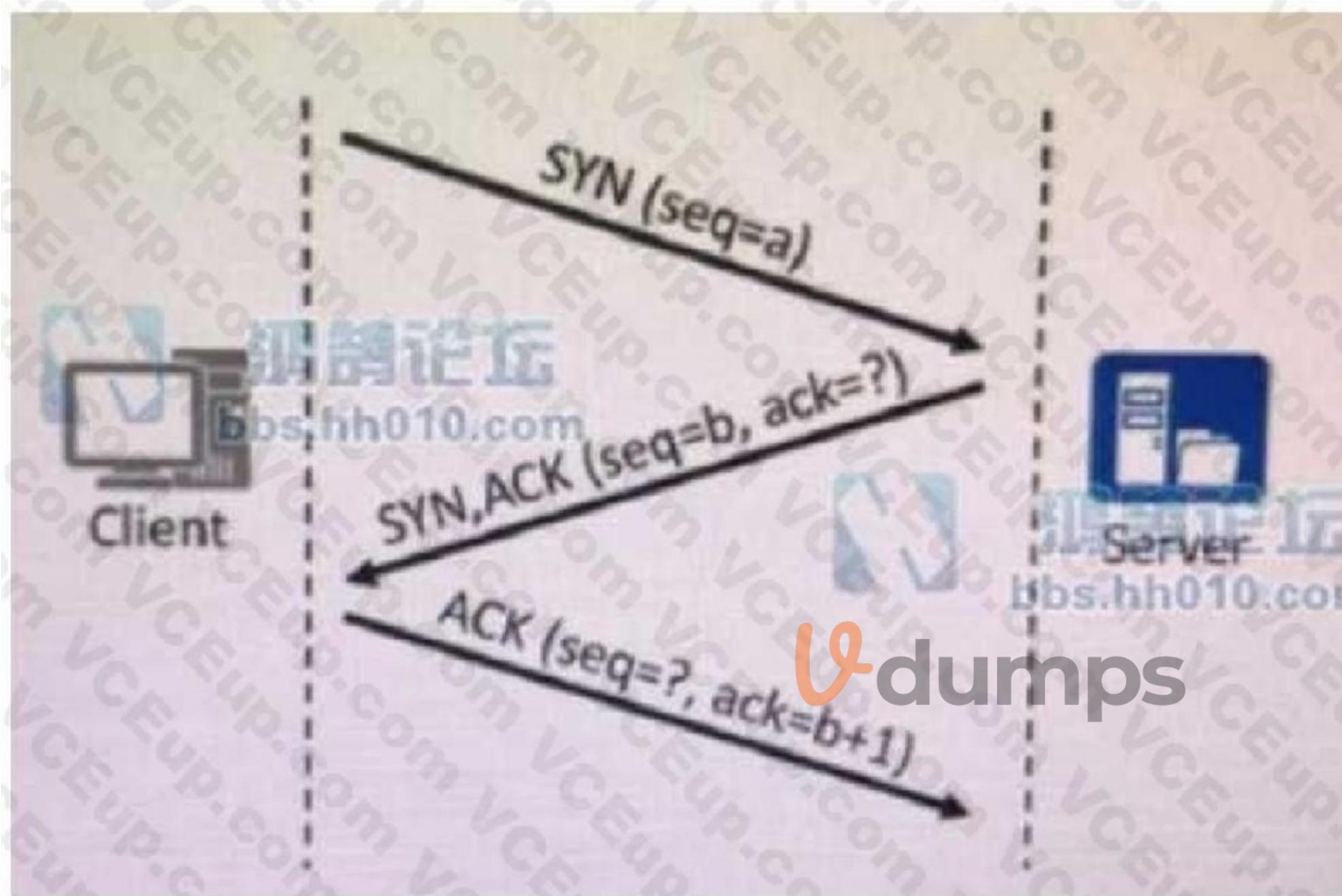
**Correct Answer: A, B, C**

**Section:**

**QUESTION 128**

As shown in the figure, the clientAand serverBestablished betweenTCPconnection, two places in the figure"?"The message sequence number should be which of the following?





- A. a+1:a
- B. a:a+1
- C. b+1:b
- D. a+1:a+1

Correct Answer: D

Section:

**QUESTION 129**

Digital certificates can be divided into local certificates, CA Certificates, root certificates, self-signed certificates, etc.

- A. True
- B. False



**Correct Answer: A**

**Section:**

**QUESTION 130**

Which of the following is an encryption technique used in digital envelopes?

- A. Symmetric encryption algorithm
- B. Asymmetric encryption algorithm
- C. hash algorithm
- D. Stream Encryption Algorithm

**Correct Answer: B**

**Section:**

**QUESTION 131**

Which of the following are remote authentication methods? (multiple choice)

- A. RADIUS
- B. Local
- C. HWTACACS
- D. LLDP

**Correct Answer: A, C**

**Section:**

**QUESTION 132**

aboutIPSec SA, which of the following statements is correct?

- A. IPSec SAis unidirectional
- B. IPSec SAis bidirectional
- C. Used to generate encryption keys
- D. Used to generate secret algorithms

**Correct Answer: A**

**Section:**

**QUESTION 133**

The steps of the security assessment method do not include which of the following?

- A. Manual audit
- B. Penetration testing
- C. Questionnaire
- D. data analysis

**Correct Answer: D**

**Section:**



**QUESTION 134**

waiting for insurance2.0Which one of the stipulations"Spam should be detected and protected at key network nodes, and spam protection mechanisms should be upgraded and updated?

- A. Malicious code prevention
- B. communication transmission
- C. Centralized control
- D. Border Protection

**Correct Answer: A**

**Section:**

**QUESTION 135**

Which of the following options is not part of the quintuple range?

- A. sourceIP
- B. sourceMAC
- C. PurposeIP
- D. destination port

**Correct Answer: B**

**Section:**

**QUESTION 136**

In a stateful inspection firewall, when the stateful inspection mechanism is enabled, the second packet of the three-way handshake (SYN+ACK) when reaching the firewall, which of the following descriptions is correct if there is no corresponding session table on the firewall?

- A. The firewall does not create a session table, but allows packets to pass through
- B. If the firewall security policy allows packets to pass, create a session table
- C. Packets must not pass through the firewall
- D. Packets must pass through the firewall and establish a session

**Correct Answer: C**

**Section:**

**QUESTION 137**

existUSGIn the system firewall, you can useóóóóThe function provides well-known application services for non-well-known ports.

- A. Port Mapping
- B. MACandIPaddress binding
- C. packet filtering
- D. Long connection

**Correct Answer: A**

**Section:**

**QUESTION 138**

Which of the following is true about the command to view the number of times security policy matches?

- A. display firewall session table
- B. display security-policy all
- C. display security-policy count
- D. count security-policy hit

**Correct Answer: B**

**Section:**

**QUESTION 139**

Which of the following options belongs to Tier 2VPNTechnology?

- A. SSL VPN
- B. L2TP VPN
- C. GRE VPN
- D. IPSec VPN

**Correct Answer: B**

**Section:**

**QUESTION 140**

aboutwindowsDescription of the firewall advanced settings, which of the following options is wrong?  
(multiple choice)

- A. When setting the stacking rules, only the local port can be restricted, and the remote port cannot be restricted
- B. When setting the stacking rules, you can restrict both the local port and the remote port.
- C. When setting the stacking rule, only the local port can be restricted, and the remote port cannot be restricted
- D. When setting the stacking rules, you can restrict both the local port and the remote port.

**Correct Answer: B, D**

**Section:**

**QUESTION 141**

aboutVGMPIn a description of group management, which of the following is false?

- A. VRRPbackup group master/All standby status changes need to be notified to theVGMPmanagement group
- B. The interface types and numbers of the heartbeat ports of the two firewalls can be different, as long as the Layer 2 interoperability can be guaranteed.
- C. Active and standby firewallsVGMPtimed starthellomessage
- D. The active and standby devices learn about the status of each other through the exchange of heartbeat messages, and back up related commands and status information.

**Correct Answer: B**

**Section:**

**QUESTION 142**

In the security assessment method, the purpose of security scanning is to scan the target system with scanning analysis and assessment tools in order to find relevant vulnerabilities and prepare for attacks.

- A. True

B. False

**Correct Answer: B**

**Section:**

**QUESTION 143**

Which of the following attacks is not a malformed packet attack?

- A. Teardropattack
- B. Smurfattack
- C. TCPFragmentation attack
- D. ICMPUnreachable Packet Attack

**Correct Answer: D**

**Section:**

**QUESTION 144**

aboutIKE SA, which of the following descriptions is false?

- A. IKE SAis bidirectional
- B. IKEis based onUDPapplication layer protocol
- C. IKE SAit's forIPSec SAServices
- D. The encryption algorithm used by user data packets isIKE SADecide

**Correct Answer: D**

**Section:**

**QUESTION 145**

HTTPmessage usageUDPcarry, andHTTPSprotocol based onTCPthree-way handshake, soHTTPSsaferand more recommendedHTTPS.

- A. True
- B. False

**Correct Answer: B**

**Section:**

**QUESTION 146**

Single sign-on function for Internet users, users directlyADServer authentication, the device does not interfere with the user authentication process,ADMonitoring services need to be deployed inUSGequipment, monitoringADAAuthentication information of the server

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 147**

UDPA port scan is when an attacker sends a zero byte lengthUDPmessage to a specific port of the target host, if the port is open, it will return aICMPPort reachable data packets.



- A. True
- B. False

**Correct Answer: B**

**Section:**

**QUESTION 148**

Which of the following statements is true about business continuity plans? (multiple choice)

- A. The business continuity plan does not require senior company involvement during the scoping phase of the project
- B. Because all possible accidents cannot be predicted,BCPFlexibility is required
- C. The business continuity plan does not require senior company involvement until it is formally documented
- D. Not all security incidents must be reported to company executives

**Correct Answer: B, D**

**Section:**

**QUESTION 149**

whenUSGWhich of the following logs can be viewed when the series firewall hard disk is in place?  
(multiple choice)

- A. Operation log
- B. business log
- C. Alarm information
- D. Threat log

**Correct Answer: A, B, C, D**

**Section:**

**QUESTION 150**

About intrusion prevention systems (IPS), which of the following is false?

- A. IDSThe device needs to be linked with the firewall to block intrusion
- B. IPSThe device cannot be deployed in bypass mode in the network
- C. IPSDevices can be connected in series at the network boundary and deployed online
- D. IPSOnce the device detects intrusion behavior, it can achieve real-time blocking

**Correct Answer: B**

**Section:**

**QUESTION 151**

Which of the following statements is true about Huawei's routers and switchers??(multiple choice)

- A. Routers can implement some security functions, and some routers can implement more security functions by adding security boards
- B. The main function of the router is to forward data. When the enterprise has security requirements, sometimes a firewall may be a more suitable choice
- C. Switches have some security functions, and some switches can realize more security functions by adding security boards



D. The switch does not have security features

**Correct Answer: A, B, C**

**Section:**

**QUESTION 152**

Which of the following options is NOT windowsOS log type?

- A. business log
- B. application log
- C. Security log
- D. System log

**Correct Answer: A**

**Section:**

**QUESTION 153**

After a network intrusion event occurs, the identity of the intrusion, the source of the attack and other information are obtained according to the plan, and the intrusion behavior is blocked. The above actions belong to PDRR. What are the links in the network security model? (multiple choice)

- A. Protection link
- B. Detection link
- C. response link
- D. recovery link

**Correct Answer: B, C**

**Section:**

**QUESTION 154**

Which of the following is false about scanning for vulnerabilities?

- A. Vulnerabilities are known in advance and discovered after the fact.
- B. Vulnerabilities are generally patchable
- C. Vulnerabilities are security risks that expose computers to hacking
- D. Vulnerabilities are avoidable

**Correct Answer: D**

**Section:**

**QUESTION 155**

When configuring user single sign-on, use the receivePCIn message mode, the authentication process has the following steps:

- A. visitorPCExecute the login script and send the user login information toADmonitor 2. Firewall extracts user andIPAdd the correspondence to the online user table 3. ADmonitor connected toADThe server queries the login user information and forwards the queried user information to the firewall 4. visitor loginADarea,ADThe server returns a login success message to the user and issues the login script. Which of the following is the correct order?
- B. 1-2-3-4
- C. 4-1-3-2



- D. 3-2-1-4
- E. 1-4-3-2

**Correct Answer: B**  
**Section:**

**QUESTION 156**

Admin wants to create web configuration administrator, device web access port number 20000, and the administrator is at the administrator level, which of the following commands is correct?

A.

```
Step1:  
web-manager security enable port 20000  
Step2:AAA View  
[USG] aaa  
[USG-aaa] manager-user client001  
[USG-aaa-manager-user-client001] service-type web  
[USG-aaa-manager-user-client001] level 15  
[USG-aaa-manager-user-client001] password cipher Admin@123
```

B.

```
Step1:  
web-manager enable port 20000  
Step2:AAA View  
[USG] aaa  
[USG-aaa] manager-user client001  
[USG-aaa-manager-user-client001] service-type web  
[USG-aaa-manager-user-client001] password cipher Admin@123
```

C.



```
Step1:
web-manager security enable port 20000
Step2:AAA View
[USG] aaa
[USG-aaa]manager-user client001
[USG-aaa-manager-user-client001]service-type web
[USG-aaa-manager-user-client001]password cipher
```

D.

```
Step1:
web-manager security enable port 20000
Step2:AAA View
[USG] aaa
[USG-aaa]manager-user client001
[USG-aaa-manager-user-client001]service-type web
[USG-aaa-manager-user-client001]level 1
[USG-aaa-manager-user-client001]password cipher Admin@123
```

Correct Answer: A

Section:

#### QUESTION 157

Which of the following options is correct regarding the actions of the security policy and the description of the security profile? (multiple choice)

- A. Prohibited if the action of the security policy is "prohibit", the device will discard this traffic, and will not perform content security checks in the future.
- B. The security profile can take effect even if the action is allowed under the security policy
- C. The security profile must be applied under the security policy whose action is Allowed to take effect.
- D. If the security policy action is "allow", the traffic will not match the security profile



**Correct Answer: A, C**

**Section:**

**QUESTION 158**

Which of the following options are window system and LINUX the same features of the system?  
(multiple choice)

- A. Support multitasking
- B. Support graphical interface operation
- C. open source system
- D. Support a variety of terminal platforms

**Correct Answer: A, B, D**

**Section:**

**QUESTION 159**

in configuration NAT During the process, in which of the following situations, the device will generate server-map table entry? (multiple choice)

- A. configuration source NAT automatically generated when server-map entry
- B. configure NAT server After success, the device will automatically generate server-map entry
- C. configure easy-ip will be generated when server-map entry
- D. configure NAT No-PAT After that, the device will establish a data stream for the configured multichannel protocol server-map surface

**Correct Answer: B, D**

**Section:**

**QUESTION 160**

NAT The technology can realize the secure transmission of data by encrypting the data.

- A. True
- B. False

**Correct Answer: B**

**Section:**

**QUESTION 161**

Which of the following is the correct order for incident response management?

- A. detect
- B. Report
- C. ease
- D. Lessons Learned
- E. repair
- F. recover
- G. response
- H. 1-3-2-7-5-6-4



- I. 1-3-2-7-6-5-4
- J. 1-2-3-7-6-5-4
- K. 1-7-3-2-6-5-4

**Correct Answer: D**

**Section:**

**QUESTION 162**

aboutL2TP VPNstatement, which of the following is false?

- A. It is suitable for employees on business to dial up to access the intranet
- B. Data will not be encrypted
- C. WithIPsec VPNIn conjunction with
- D. belonging to the third floorVPNTechnology

**Correct Answer: D**

**Section:**

**QUESTION 163**

Encryption technology can convert readable information into unreadable information through certain methods.

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 164**

ASPF (Application specific Packet Filter)It is a packet filtering technology based on the application layer, andserver-mapTables implement special security mechanisms. aboutASPFandservermapWhich of the following statements is correct? (multiple choice)

- A. ASPFMonitor messages during communication
- B. ASPFcan be created dynamicallyserver-map
- C. ASPFpass throughserver-mapTable implementation dynamically allows multi-channel protocol data to pass through
- D. Quintupleserver-mapThe table entry implements a similar function to the session table

**Correct Answer: A, B, C**

**Section:**

**QUESTION 165**

Antivirus software and host firewalls work the same way.

- A. True
- B. False

**Correct Answer: B**

**Section:**



**QUESTION 166**

The process of electronic forensics includes: protecting the scene, obtaining evidence, preserving evidence, identifying evidence, analyzing evidence, tracking and presenting evidence.

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 167**

Execute the command on the firewall and display the above information. Which of the following descriptions is correct? (multiple choice)

```
HRP_A[USG_A] display vrrp interface GigabitEthernet 1/0/1
GigabitEthernet1/0/1 | Virtual Router 1
VRRP Group : Active
state : Active
Virtual IP : 202.38.10.1
Virtual MAC : 0000-5e00-0101
Primary IP : 202.38.10.2
PriorityRun : 100
PriorityConfig : 100
MasterPriority : 100
Preempt : YES Delay Time : 10
```

- A. this firewall VRRP group status is Active
- B. this firewall G1/0/1 virtual interface IP address is 202.38.10.2
- C. this firewall VRRP for 1 of VRRP The priority of the backup group is 100
- D. When the main device USG\_A will not switch in the event of a failure

**Correct Answer: A, B, C**

**Section:**

**QUESTION 168**

exist USG In the series firewall system view, execute the command `reset saved-configuration` After that, the device configuration will be restored to the default configuration, and it will take effect without any other operations.

- A. True

B. False

**Correct Answer: B**

**Section:**

**QUESTION 169**

Which of the following is network address port translation (NAPT) and only translate network addresses (No-PAT) difference?

- A. go throughNo-PATAfter conversion, for external network users, all packets come from the sameIPaddress
- B. No-PATOnly supports protocol port translation at the transport layer
- C. NAPTOOnly supports protocol address translation at the network layer
- D. No-PATSupports protocol address translation at the network layer

**Correct Answer: D**

**Section:**

**QUESTION 170**

Which of the following options is correct for the description of a buffer overflow attack?

(multiple choice)

- A. Buffer overflow attacks exploit the flaws of software systems in memory operations to run attack code with high operating privileges
- B. Buffer overflow attacks have nothing to do with the vulnerabilities and architecture of the operating system
- C. Buffer overflow attacks are one of the most common ways to attack the behavior of software systems
- D. Buffer overflow attacks are application-layer attacks

**Correct Answer: A, C, D**

**Section:**

**QUESTION 171**

Which of the following is not the business scope of the National Internet Emergency Response Center?

- A. Emergency handling of security incidents
- B. Warning and notification of security incidents
- C. Provide security evaluation services for government departments, enterprises and institutions
- D. Cooperate with other institutions to provide training services

**Correct Answer: D**

**Section:**

**QUESTION 172**

Host firewalls are mainly used to protect hosts from attacks and intrusions from the network.

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 173**

Which of the following options belong to international organizations related to the standardization of information security? (multiple choice)

- A. International Organization for Standardization(ISO)International Organization for Standardization
- B. International Electrotechnical Commission(IEC) International Electrotechnical Commission
- C. International Telecommunication Union(ITU)ITU
- D. Wi-Fi Alliance Wi-Fi alliance organization

**Correct Answer: A, B, C**

**Section:**

**QUESTION 174**

In order to obtain criminal evidence, it is necessary to master the technology of intrusion tracking.

Which of the following options are correct for the description of tracking technology? (multiple choice)

- A. Packet logging technology through the tracedIPInsert trace data into packets to mark packets on each router they pass through
- B. Link testing technology determines the information of the attack source by testing the network link between routers
- C. Packet marking technology extracts attack source information by logging packets on routers and then using data drilling techniques
- D. Shallow mail behavior analysis can achieveIPAnalysis of addresses, sent time, sending frequency, number of recipients, shallow email headers, and more.

**Correct Answer: A, B, D**

**Section:**

**QUESTION 175**

Digital signature technology obtains a digital signature by encrypting which of the following data?

- A. User data
- B. Receiver's public key
- C. sender's public key
- D. digital fingerprint

**Correct Answer: D**

**Section:**

**QUESTION 176**

at HuaweiUSGOn the series firewalls, the default security policy does not support modification.

- A. True
- B. False

**Correct Answer: B**

**Section:**

**QUESTION 177**

In the classification of the information security level protection system, which of the following levels define that if the information system is destroyed, it will cause damage to social order and public interests? (multiple choice)



- A. first level  
User self-protection level
- B. second level  
System Audit Protection Level
- C. third level  
Safety Mark Protection
- D. fourth level structured protection

**Correct Answer: A, B, C, D**

**Section:**

**QUESTION 178**

at HuaweiSDSecIn the solution, which of the following is an analysis layer device?

- A. CIS
- B. Agile Controller
- C. switch
- D. Firehunter

**Correct Answer: D**

**Section:**

**QUESTION 179**

Control actions of firewall inter-domain forwarding security policypermitanddeny, which of the following options are correct? (multiple choice)

- A. The actions of the firewall's default security policy are:deny
- B. The packet matches the interzone security policydenyThe packet is discarded immediately after the action, and other interzone security policies will not continue to be executed.
- C. Even if the packet matches the security policypermitaction, and may not necessarily be forwarded by the firewall
- D. Whether the packet matches the security policypermitaction, ordenyaction, will go toUTMmodule handling

**Correct Answer: A, B, C**

**Section:**

**QUESTION 180**

Business Impact Analysis (BIA) does not include which of the following?

- A. business priority
- B. Incident handling priority
- C. impact assessment
- D. Risk Identification

**Correct Answer: C**

**Section:**

**QUESTION 181**

in deploymentIPSec VPN, which of the following is the main application scenario of tunnel mode?

- A. between host and host
- B. Between the host and the security gateway
- C. between security gateways
- D. between host and server

**Correct Answer: C**

**Section:**

**QUESTION 182**

HRP(Huawei Redundancy Protocol) protocol, which is used to synchronize data such as key configuration and connection status of the firewall to the standby firewall, which of the following options does not belong to the scope of synchronization?

- A. security strategy
- B. NATStrategy
- C. blacklist
- D. IPSSignature set

**Correct Answer: D**

**Section:**

**QUESTION 183**

Which of the following statements is true about business continuity plans? (multiple choice)

- A. The business continuity plan does not require senior company involvement during the scoping phase of the project
- B. I thought it was impossible to predict all possible accidents, soBCPFlexibility is required
- C. The business continuity plan does not require senior company involvement until it is formally documented
- D. Not all security incidents must be reported to company executives

**Correct Answer: B**

**Section:**

**QUESTION 184**

Regarding the NAT policy processing flow, which of the following options are correct? ( )\*

- A. Server-map is processed before the security policy is matched
- B. Source NAT policy is processed after security policy match
- C. Source NAT policy queries are processed after the session is created
- D. Server-map is processed after state detection

**Correct Answer: A, B, D**

**Section:**

**QUESTION 185**

technologies, namely NAT No-PAT, \_\_\_\_\_, Easy IP.[fill in the blank]\*

- A. NATP



**Correct Answer: A**

**Section:**

**QUESTION 186**

The default authentication domain of the USG6000 series firewall is the \_\_\_\_\_ domain.[fill in the blank]\*

A. default

**Correct Answer: A**

**Section:**

**QUESTION 187**

\_\_\_\_\_ Mode: Two devices, one master and one backup. Under normal circumstances, service traffic is handled by the active device. When the active device fails, the standby device replaces the active device to process service traffic to ensure that services are not interrupted.[fill in the blank]\*

A. Dual-system hot standby active/standby backup

**Correct Answer: A**

**Section:**

**QUESTION 188**

The administrator wishes to clear the current session table. Which of the following commands is correct? ( ) [Multiple choice]\*

- A. display session table
- B. display firewall session table
- C. reset firewall session table
- D. clear firewall session table



**Correct Answer: C**

**Section:**

**QUESTION 189**

If internal employees access the Internet through the firewall and find that they cannot connect to the Internet normally, what viewing commands can be used on the firewall to troubleshoot the interface, security zone, security policy and routing table? (Write any viewing command, requiring: the words on the command line must be complete and correct to score, and cannot be omitted or abbreviated)[fill in the blank]\* (

A. display zone display current-configuration | display ip routing-table | display security-polic rule all | display ip interface brief)

**Correct Answer: A**

**Section:**

**QUESTION 190**

If users from the external network (where the security zone is Untrust) are allowed to access the intranet server (where the security zone is DMZ), the destination security zone selected when configuring the security policy is \_\_\_\_\_.[fill in the blank]\*

A. DMZ

**Correct Answer: A**

**Section:**



**QUESTION 191**

Use the Ping command on the firewall to test the reachability to the server (the security zone where the server is located is the DMZ). If a security policy is configured to allow the test traffic, the source security zone is \_\_\_\_\_.[fill in the blank]

\*

A. local

**Correct Answer: A**

**Section:**

**QUESTION 192**

An employee of a company accesses the internal web server of the company through the firewall, and can open the web page of the website by using a browser, but the accessibility of the web server is tested by using the Pina command, and it shows that it is unreachable. What are the possible reasons? ( ) [Multiple choice]

- A. The security policy deployed on the firewall allows the TCP protocol, but not the ICMP protocol
- B. The interface of the firewall connecting to the server is not added to the security zone
- C. The security policy deployed on the firewall allows the HTTP protocol, but not the ICMP protocol
- D. WEB server is down

**Correct Answer: A**

**Section:**

**QUESTION 193**

As shown in the figure, two Server Map entries are generated after configuring NAT Server. Regarding the information presented in this figure, which of the following descriptions is wrong? [Multiple choice]\* Type: Nat Server. ANY?1.1.1.1 [192.168.1.1] Type: Nat Server Reverse. 192.168.1.1[1.1.1.1] ?ANY

- A. The second Server Map function is that when 192.168.1.1 accesses any address, the source address will be converted to 1.1.1.1 after passing through the firewall
- B. The first Server Map function is that when any address accesses 192.168.1.1, the destination IP will be converted to 1.1.1.1 after passing through the firewall.
- C. The Server Map with the Reverse logo can use the command to remove it.
- D. The two Server Map entries are static, that is, after the NAT Server is configured, the two Server Maps will be automatically generated and exist permanently.

**Correct Answer: B**

**Section:**

**QUESTION 194**

After an engineer configures the NAT-Server, in order to check the Server-map generated after the configuration, should he use the \_\_\_\_\_ command to query the Server-map?[fill in the blank]\*

A. display firewall server-map

**Correct Answer: A**

**Section:**

**QUESTION 195**

Which of the following options are suitable for business travelers to access the corporate intranet in the public network environment? ( )\*

- A. L2 TP over IPSec VPN
- B. GER VPN
- C. MPLS VPN

D. SSL VPN

**Correct Answer: A, D**

**Section:**

**QUESTION 196**

When using the \_\_\_\_\_ function of SSL VPN, the virtual gateway will assign an intranet IP address to the access user, which is used for the access user to access the P resources of the intranet[fill in the blank]\*

A. network extension

**Correct Answer: A**

**Section:**

**QUESTION 197**

Which of the following is not a common application scenario of digital certificates? ( ) [Multiple choice]\*

A. FTP

B. HTTPS

C. IPSEC VPN

D. SSL VPN

**Correct Answer: A**

**Section:**

**QUESTION 198**

In symmetric encryption algorithms, the \_\_\_\_\_ algorithm is used over a data communication channel, browser or network link.[fill in the blank]\*

A. Stream

**Correct Answer: A**

**Section:**

**Explanation:**

Encryption

**QUESTION 199**

Please order the following project implementation steps from project initiation.[fill in the blank]\*

|  |
|--|
| Risk assessment                          |
| System design and release                |
| Project initiation and variance analysis |
| Certification and Continuous Improvement |
| System operation and monitoring          |

A. project initiation and variance analysis, risk assessment, system design

**Correct Answer: A**

**Section:**

**QUESTION 200**

In the \_\_\_\_\_ view of the firewall, you can use the reboot command to restart the firewall.[fill in the blank]\*

A. user

**Correct Answer: A**

**Section:**

**QUESTION 201**

\_\_\_\_\_ is a flaw in the specific implementation of hardware, software, protocols, or system security policies that could enable an attacker to gain unauthorized access or compromise a system.[fill in the blank]\*

|  |
|--|
| The AD monitor forwards the user login message to F7, and the user goes online at F7.  |
| AD monitor through the WMI interface provided by AD server. Connect to the AD server to query the security log. Get the user login message.        |
| A visitor logs in to the AD domain, and the AD server records the user's online information in the security log.                                   |
| The AD monitor starts from the time when the AD single sign-on service starts, and regularly queries the security logs generated on the AD server. |

A. Vulnerability

**Correct Answer: A**

**Section:**

**QUESTION 202**

Gratuitous ARP can be used to detect whether the \_\_\_\_\_ address conflicts, and it can also refresh the switch MAC address table.[fill in the blank]\*

A. IP

**Correct Answer: A**

**Section:**

**QUESTION 203**

Personal information leakage is the destruction of the \_\_\_\_\_ characteristics of information.[fill in the blank]\*

A. confidential

**Correct Answer: A**

**Section:**

**QUESTION 204**

data transmission is the TCP\_\_\_\_\_ port.[fill in the blank]\*

A. 20

**Correct Answer: A**

**Section:**

**QUESTION 205**

If internal employees access the Internet through the firewall and find that they cannot connect to the Internet normally, what command can be used on the firewall to check the interface state security zone, security policy and routing table troubleshooting? (Write out any one of the viewing commands, requiring: the words on the command line must be complete and correct to score, and cannot be omitted or abbreviated)[fill in the blank]\*

A. display ip routing-table display zone

**Correct Answer: A**

**Section:**

**QUESTION 206**

When the FW is deployed at the network egress, if a fault occurs, it will affect the Zaonet service. to enhance the network Reliability, need to deploy two FWs and form \_\_\_\_\_[fill in the blank]\*

A. hot standby

**Correct Answer: A**

**Section:**

**QUESTION 207**

RFC (Request For Comment) 1918 reserves 3 IP addresses for private use, namely 10.0.0.0- 10.255.255.255, \_\_\_\_\_, 192.168.0.0-192.168.255.255[fill in the blank]\*

A. 172.16.0.0-172.31.255.255

**Correct Answer: A**

**Section:**

**QUESTION 208**

The reason why NAT can realize one-to-many address translation is that the \_\_\_\_\_ is also translated when the address is translated, so multiple private addresses can share the same public address.[fill in the blank]\*

A. IP

**Correct Answer: A**

**Section:**

**QUESTION 209**

When the company's network administrator is performing dual-system hot backup, due to the possibility of inconsistent round-trip paths, if he wants to enable the session fast backup function, the command that needs to be entered is \_\_\_\_\_[fill in the blank]\*

A. confidential

**Correct Answer: A**

**Section:**

**QUESTION 210**

Which of the following information is not the backup content included in the status information backup in the dual-system hot backup? ( ) [Multiple choice]\*

- A. IPSEC tunnel
- B. NAT related table items
- C. IPv4 session table
- D. Routing table

**Correct Answer: D**

**Section:**

**QUESTION 211**

When configuring user single sign-on, if you use the mode of querying the AD server security log, please check the following certified ProcedureEnterRow ordering: [fill in the blank]\* The AD monitor forwards the user login message to F7, and the user goes online at F7.

AD monitor through the WMI interface provided by AD server. Connect to the AD server to query the security log. Get the user login message. accessboardrecord AD domain, AD servicedevicerecorduseHouseholdsuperiorStringinformation into the security log.

The AD monitor starts from the time when the AD single sign-on service starts, and regularly queries the security logs generated on the AD server.

A. 4213

**Correct Answer: A**

**Section:**

**QUESTION 212**

When configuring security policies, you can control traffic based on the user's \_\_\_\_\_. [fill in the blank]\*

A. Services and Apps

**Correct Answer: A**

**Section:**

**Explanation:**

Apps

Explanation:



**QUESTION 213**

Which of the following descriptions about dual-system hot backup is wrong? ( ) [Multiple choice]\*

A. By default the preemption delay is 60s

B. Whether it is a Layer 2 or Layer 3 interface, whether it is a service interface or a heartbeat interface, it needs to be added to a security zone

C. By default, the active preemption function is enabled

D. Dual-system hot backup function requires license support

**Correct Answer: D**

**Section:**

**QUESTION 214**

IPv6 supports configuring router authorization function on the device, verifying peer identity through digital certificate, and selecting legal device. ( ) [Multiple choice]\*

A. True

B. False

**Correct Answer: A**

**Section:**

**QUESTION 215**

Which of the following SSL VPN functions can and can only access all TCP resources? ( ) [Multiple choice]\*

- A. Network expansion
- B. File Sharing
- C. WEB proxy
- D. port forwarding

**Correct Answer: D**

**Section:**

**QUESTION 216**

Which of the following descriptions about digital fingerprints in digital signatures is wrong? ( ) [Multiple choice]\*

- A. It is the data obtained by the sender after calculating the plaintext information through the HASH algorithm.
- B. The receiver will use the sender's public key to calculate the generated data fingerprint and compare it with the received digital fingerprint.
- C. Digital fingerprints are also known as information digests.
- D. The receiver needs to use the sender's public key to unlock the digital signature to obtain the digital fingerprint.

**Correct Answer: C**

**Section:**

**QUESTION 217**

In the architecture of PKI, \_\_\_\_\_ is the window for CA to face users, and is an extension of CA's certificate issuance and management functions. He is responsible for accepting user's certificate registration and revocation applications, reviewing employee identity information, and deciding Whether to submit an application to the CA to issue or revoke a digital certificate. [fill in the blank]\*

- A. RA

**Correct Answer: A**

**Section:**

**QUESTION 218**

The SSL VPN routing mode determines the routing of the packets sent by the client. In the \_\_\_\_\_ mode, no matter what resource is accessed, the data will be intercepted by the virtual network card and forwarded to the virtual gateway for processing. [fill in the blank]\*

- A. network extension

**Correct Answer: A**

**Section:**

**QUESTION 219**

User authentication is the authentication of the client identity by the SSL virtual gateway, including:

\_\_\_\_\_, server authentication, certificate anonymous authentication and certificate challenge authentication. [fill in the blank]

- A. local authentication

**Correct Answer: A**

**Section:**

**QUESTION 220**

When an information security incident occurs, give priority to using \_\_\_\_\_ emergency response to provide technical support to customers [fill in the blank]\*



A. MPDRR

**Correct Answer: A**

**Section:**

**QUESTION 221**

Drag the steps of electronic forensics on the left into the box on the right to summarize, and arrange them from top to bottom in the order of execution.

|                          |
|--------------------------|
| Preservation of evidence |
| to track                 |
| get evidence             |
| Analyze evidence         |

A. to track

**Correct Answer: A**

**Section:**

**QUESTION 222**

Regarding the description of risk assessment, which of the following is false? ( ) [Multiple choice]

- A. Risk assessment requires training in asset collection and risk assessment methods
- B. Risk assessment entails identifying threats, vulnerabilities, and scanning for security vulnerabilities.
- C. Risk assessment requires assessing risks and classifying risk levels
- D. Risk assessment requires monitoring system operation.



**Correct Answer: D**

**Section:**

**QUESTION 223**

The attacker searches the ports currently open by the attacked object by scanning the ports to determine the attack mode. In port scanning attacks, attackers usually use Port Scan attack software to initiate a series of TCP/UDP connections, and determine whether the host uses these ports to provide services according to the response packets. Such network probing is called \_\_\_\_\_ scanning. [fill in the blank]\*

A. port

**Correct Answer: A**

**Section:**

**QUESTION 224**

Please correspond the following protocols to their TCP/IP protocol stack levels

|                          |
|--------------------------|
| Preservation of evidence |
| to track                 |
| get evidence             |
| Analyze evidence         |

A. get evidence



Correct Answer: A

Section:

**QUESTION 225**

Please correctly categorize the main functions of the following operating systems.

|                               |                      |
|-------------------------------|----------------------|
| Content distribution          | processor management |
| File storage space management | memory management    |
| process control               | Device management    |
| Equipment allocation          | file management      |
| Task, interface management    | Job management       |

A. file management

Correct Answer: A

Section:

**QUESTION 226**

Please correctly categorize the following servers and their functions

|   |                 |
|---|-----------------|
| Provide domain name resolution services | Database Server |
| Provide agency services                 | DNS Server      |
| Database System Administration          | NTP Server      |
| Provide time synchronization service    | Prory Server    |
| Provide file sharing services           | ?le Server      |

A. Prory Server

Correct Answer: A

Section:

**QUESTION 227**

Which of the following is not a stand-alone anti-virus technology? ( ) [Multiple choice]\*

- A. Configure anti-virus technology on network firewall
- B. Use virus detection tools
- C. Patch the system

Correct Answer: A

Section:



**QUESTION 228**

Please match the following NAT technologies and the functions implemented one by one



|            |   |
|------------|---|
| NAT To-PAT | The firewall translates the destination address of the request packet from the external user into the private address of the internal server.   |
| NAPT       | During translation, only the address is translated, and the port is not translated. Implement one-to-one  |
|            | conversion from private network addresses to public network addresses. If all addresses in the address pool have been allocated, NAT translation will not be performed when the remaining hosts on the internal network access the external network. NAT translation will not be performed until there are free addresses in the address pool.          |
| Easy IP    | The public network address of the interface is directly used as the translated address, and the NAT address pool does not need to be configured. Both addresses and ports are translated during translation. It can realize the requirement that multiple private network addresses share the public network address of the external network interface. |
| NAT Server | The NAT address pool can contain one or more public network addresses. Both addresses and ports are translated during translation. It can realize the requirement that multiple private network addresses share one or more public network addresses.   |

A. NAI Server

**Correct Answer: A**

**Section:**

**QUESTION 229**

In which of the following scenarios does the firewall generate the Server map table? ( )

- A. NAT Server is deployed on the firewall
- B. ASPF is deployed on the firewall and forwards the traffic of the multi-channel protocol
- C. When the firewall generates a session table, it will generate a Server-map table
- D. Security policies are deployed on the firewall and traffic is released

**Correct Answer: A, B**

**Section:**

**QUESTION 230**

The direction of the traffic can be seen in the \_\_\_ of the firewall.[fill in the blank]\*

A. session table

**Correct Answer: A**

**Section:**

**QUESTION 231**

The firewall imports users locally, and supports importing user information from \_\_\_\_\_ format files and database dbm files to the local device.[fill in the blank]\*

A. CSV

**Correct Answer: A**

**Section:**

**QUESTION 232**

Which of the following protocols is not a protocol type that ASPF can detect? ( ) [Multiple choice]\*

- A. PPTP
- B. FTP
- C. MSTP
- D. DNS

**Correct Answer: C**

**Section:**

**QUESTION 233**

After the firewall detects a virus, which of the following will release the virus? ( ) [Multiple choice]\*

A. Not a protocol supported by the firewall



- B. Hit apply exception
- C. The source IP hits the whitelist
- D. Hit virus exception

**Correct Answer: D**

**Section:**

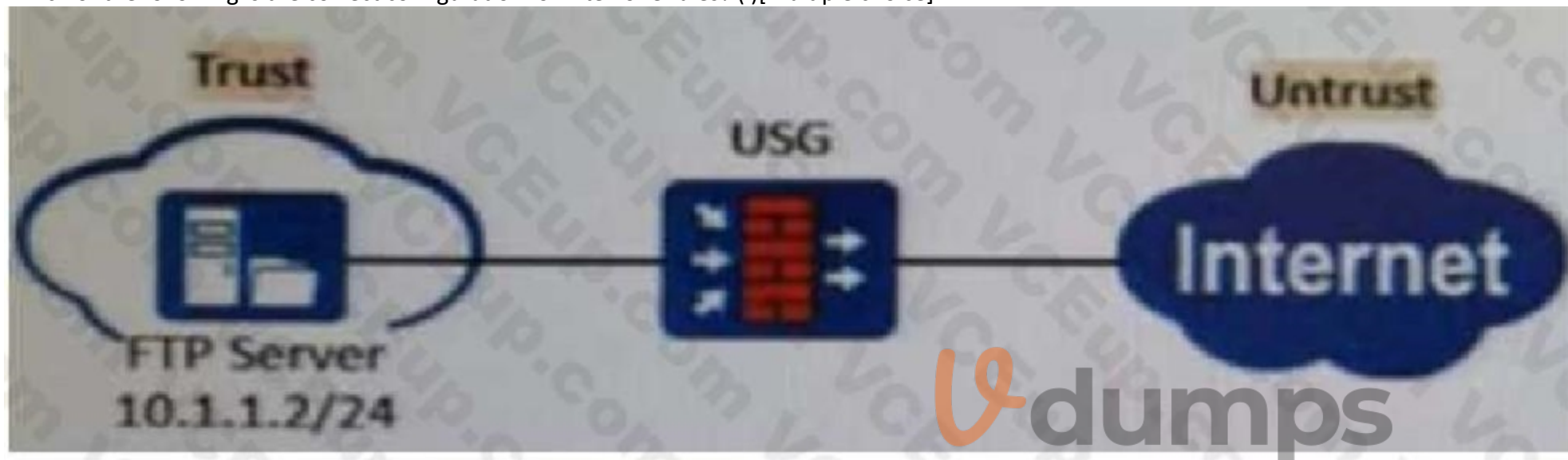
**Explanation:**

Topic 3, Exam Pool C

**QUESTION 234**

As shown in the figure, nat server global202.106.1.1 inside10.10.1.1 is configured on the firewall.

Which of the following is the correct configuration for interzone rules? ( ) [Multiple choice]\*



- A. rule name c, source-zone untrust, destination-zone trust, destination-address 202.106.1.132, action permit
- B. rule name d, source- zone untrust, destination- zone trust, destination- address10.10.1.1 32, action permit
- C. rule name b, source- zone untrust, destination- zone trust, source- address10.10.1.1 32, action permit
- D. rule name b, source-zone untrust, destination-zone trust, source-address202.106.l.1 32, action permit

**Correct Answer: B**

**Section:**

**QUESTION 235**

Which of the following NAT technologies can implement a public network address to provide source address translation for multiple private network addresses ( )\*

- A. NAT
- B. NAT Server
- C. Easy-ip  
CT Jinglu
- D. NAT No-PAT

**Correct Answer: B**

**Section:**



**QUESTION 236**

During the process of establishing IPSec VPN between peers FW\_A and FW\_B, two types of security associations need to be established in two stages. In the first stage, \_\_\_\_\_ is established to verify the identity of the peers.[fill in the blank]\*

A. IKE SA

**Correct Answer: A**

**Section:**

**QUESTION 237**

Using the \_\_\_\_ method of the Web proxy, the virtual gateway will encrypt the real URL that the user wants to access, and can adapt to different terminal types.[fill in the blank]\*

A. web rewrite

**Correct Answer: A**

**Section:**

**QUESTION 238**

Digital envelope technology means that the sender uses the receiver's public key to encrypt the data, and then sends the ciphertext to the receiver ( ) [Multiple choice]\*

A. TRUE

B. FALSE

**Correct Answer: B**

**Section:**

**QUESTION 239**

IPSec VPN uses an asymmetric algorithm to calculate the \_\_\_\_ key to encrypt data packets.[fill in the blank]

A. symmetry

**Correct Answer: A**

**Section:**

**QUESTION 240**

When IPSec VPN uses tunnel mode to encapsulate packets, which of the following is not within the encryption scope of the ESP security protocol? ( ) [Multiple choice]\*

A. ESP Header

B. TCP Header

C. Raw IP Header

D. ESP Tail

**Correct Answer: A**

**Section:**

**QUESTION 241**

Database operation records can be used as \_\_\_\_ evidence to backtrack security events.[fill in the blank]\*

A. electronic

**Correct Answer: A**

**Section:**

**QUESTION 242**

Drag the phases of the cybersecurity emergency response on the left into the box on the right, and arrange them from top to bottom in the order of execution.[fill in the blank]\*

|                   |
|-------------------|
| Inhibition stage  |
| recovery phase    |
| detection stage   |
| eradication phase |

A. 3142

**Correct Answer: A**

**Section:**

**QUESTION 243**

Drag the warning level of the network security emergency response on the left into the box on the right, and arrange it from top to bottom in order of severity.[fill in the blank]\*

|              |
|--------------|
| Orange Alert |
| Yellow Alert |
| red alert    |
| blue alert   |

A. 3124

**Correct Answer: A**

**Section:**

**QUESTION 244**

According to the level protection requirements, which of the following behaviors belong to the scope of information security operation and maintenance management? ( )\*

A. Participate in information security training

- B. Backup or restore data
- C. Develop an emergency response plan
- D. Security hardening of the host

**Correct Answer: A, B, C, D**

**Section:**

**QUESTION 245**

In the TCP/IP protocol core, which of the following protocols works at the application layer? ( ) [Multiple choice]\*

- A. IGMP
- B. ICMP
- C. RIP
- D. ARP

**Correct Answer: C**

**Section:**

**QUESTION 246**

When using passive mode to establish an FTP connection, the control channel uses port 20 and the data channel uses port 21. ( ) [Multiple choice]\*

- A. True
- B. False

**Correct Answer: B**

**Section:**

**QUESTION 247**

In the Linux system, which of the following is the command to query the IP address information? ( ) [Multiple choice]\*

- A. ifconfig
- B. display ip interface brief
- C. ipconfig
- D. display ip

**Correct Answer: A**

**Section:**

**QUESTION 248**

The trigger authentication method for firewall access user authentication does not include which of the following? ( ) [Multiple choice]\*

- A. MPLS VPN
- B. SSL VPN
- C. IPSec VPN
- D. L2TP VPN

**Correct Answer: A**



**Section:**

**QUESTION 249**

\_\_\_\_\_ Authentication is to configure user information (including local user's user name, password and various attributes) on the network access server. The advantage is that it is fast.[fill in the blank]\*

- A. local authentication

**Correct Answer: A**

**Section:**

**QUESTION 250**

Which of the following descriptions about the main implementation of single sign-on is wrong? ( ) [Multiple choice]\*

- A. Accept PC message mode
- B. Query the AD server security log mode
- C. Query the syslog server mode
- D. Firewall monitors AD authentication packets

**Correct Answer: C**

**Section:**

**QUESTION 251**

We should choose the encryption algorithm according to our own use characteristics. When we need to encrypt a large amount of data, it is recommended to use the \_\_\_\_\_ encryption algorithm to improve the encryption and decryption speed.[fill in the blank]\*

- A. ymmetry

**Correct Answer: A**

**Section:**

**QUESTION 252**

encapsulate IP packets using the AH+ESP protocol? ( ) [Multiple choice]\*

- A. 1
- B. 2
- C. 3
- D. 4

**Correct Answer: D**

**Section:**

**QUESTION 253**

Please order the following steps in the PKI life cycle correctly, 1. Issued, 2. storage, 3. Update, 4. verify[fill in the blank]\*

- A. 1243

**Correct Answer: A**

**Section:**





**QUESTION 254**

Drag the phases of the cybersecurity emergency response on the left into the box on the right, and arrange them from top to bottom in the order of execution. 1. Inhibition stage, 2. recovery phase, 3. Detection stage, 4. eradication phase[fill in the blank]\*

A. 3142

**Correct Answer: A**

**Section:**

**QUESTION 255**

Match the following survey methods to the descriptions one by one

|                           |  |
|---------------------------|--|
| operational investigation | Civil investigations typically do not involve internal employees and external consultants  |
| crime investigation       | It is mainly used to investigate the organization's computing facility problems, such as whether there are performance problems, configuration problems, etc. It is mainly used to analyze problems and does not require particularly rigorous evidence. |
| civil investigation       | Regulatory investigations are carried out by government agencies, where organizations may violate the law  |
| Regulatory investigation  | Investigations by law enforcement into violations of the law   |

A. crime investigation

**Correct Answer: A**

**Section:**

**QUESTION 256**

existVRRP(Virtual Router Redundancy Protocol) group, the primary firewall regularly sends notification messages to the backup firewall, and the backup firewall is only responsible for monitoring notification messages and will not respond

A. True

B. False

**Correct Answer: A**

**Section:**

**QUESTION 257**

HuaweiUSGfirewallVRRPThe advertisement packets are multicast packets, so each firewall in the backup group must be able to communicate directly at Layer 2.

- A. True
- B. False

**Correct Answer: A**

**Section:**

**QUESTION 258**

Because the server is a kind of computer, we can use our personal computer as a server in the enterprise.

- A. True
- B. False

**Correct Answer: B**

**Section:**

**QUESTION 259**

As shown in the figure, aNAT serverapplication scenarios, when usingwebWhen this configuration is performed in the configuration mode. Which of the following statements are correct? (multiple choice)



- A. When configuring the interzone security policy, you need to set the source security zone toUntrust, the target security area isDMZ
- B. configureNATServer, the internal address is10.1.1.2, the external address is200.10.10.1
- C. When configuring the interzone security policy, set the source security zone toDMZ, the target security area isUntrust
- D. configureNATServer, the internal address is200.10.10.1, the external address is10.1.1.2

**Correct Answer: A, B**

**Section:**

**QUESTION 260**

existL2TPconfiguration, for the commandTunnel Name, which of the following statements is true?  
(multiple choice)

- A. Used to specify the tunnel name of the local end
- B. Used to specify the tunnel name of the peer
- C. both endsTunnel Nnamemust be consistent
- D. If not configuredTunnel Name, the tunnel name is the local system name

**Correct Answer: A, D**

**Section:**

**QUESTION 261**

DDosWhich of the following attack types is an attack?

- A. snooping scan attack
- B. Malformed Packet Attack
- C. special packet attack
- D. traffic attack

**Correct Answer: D**

**Section:**

**QUESTION 262**

\_\_\_\_\_ - The goal is to provide a rapid, composed and effective response in emergency situations, thereby enhancing the ability of the business to recover immediately from a disruptive event.[fill in the blank]\*

- A. business continuity plan

**Correct Answer: A**

**Section:**

**QUESTION 263**

Social engineering is a means of harm such as deception, harm, etc. through psychological traps such as psychological weaknesses, instinctive reactions, curiosity, trust, and greed of victims ( )

- A. TURE
- B. False

**Correct Answer: B**

**Section:**

