

Hongye Forum- HCNA-Security (H12-711) Question Bank V3.0

Number: H12-711

Passing Score: 600

Time Limit: 120 min

File Version: 3.0

Huawei Question **Bank Battle Report** Group: 69117678

Huawei's latest Q / latest battlefield report released

area: <http://bbs.hh010.com/forum.php?gid=486>

Download the official Genuine exam, the exam to see the latest battlefield report, please pay attention to the swan forum at any time <http://bbs.hh010.com>

Cisco Huawei exam registration national discount, please contact Hongye customer service for registration

QQ 613523101**QQ 613523103****QQ 613523105****QQ 613523107****QQ 613523108****QQ 613523109**Hongbao Forum official Taobao shop: <http://hh010.taobao.com/>

Hongye Forum Official WeChat Public Account:

Exam A**QUESTION 1**

Regarding the description of windows log event types, which options are correct? (Multiple choices)

- A. Warning events are events for the successful operation of an application, driver, or service.
- B. Error events usually refer to loss of functionality and data. For example, if a service cannot be loaded as a system boot, an error event is generated.
- C. When disk space is low, it will be recorded as an "information event"
- D. Failure audit event refers to a failed audit of a secure login attempt, such as a failure when the user view accesses a network drive, and it is recorded as a failure

Audit events.

Correct Answer: BCD**Section:** (none)**Explanation****Explanation / Reference:****QUESTION 2**

Which of the following types of encryption technology can be classified? (Multiple choices)

- A. Symmetric encryption
- B. Symmetric encryption
- C. Fingerprint encryption
- D. Data encryption

Correct Answer: AB**Section:** (none)**Explanation****Explanation / Reference:****QUESTION 3**

Which of the following state information can be backed up by Huawei Redundancy Protocol (HRP)? (Multiple choices)

- A. Session table
- B. ServerMap entry
- C. Dynamic blacklist
- D. Routing table

Correct Answer: ABC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 4

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

- A. Policy
- B. Protection
- C. Detection
- D. Response

Page 3

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 5

Evidence identification needs to address the verification of the completeness of the evidence and determine whether it meets the applicable standards. Regarding the standards of evidence identification, which of the following descriptions is correct?

A. Relevance criterion refers to the fact that if the evidence is able to have a substantial impact on the facts of the case to a certain extent, the court should rule that it is relevant.

Sex.

B. Objectivity standards mean that the acquisition, storage, and submission of electronic evidence should be legal, and should be based on national interests, social welfare, and personal privacy.

This right does not constitute a strict violation.

C. The standard of legality is to ensure that the content of electronic evidence has not changed from the initial collection to the submission as evidence of litigation.

Into.

D. The fairness standard refers to the evidence materials obtained by legal entities through legal means to have evidence capacity.

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 6

Data analysis technology is to find and match keywords or key phrases in the acquired data stream or information stream, and analyze the relevance of time. the following

Which is not an evidence analysis technique?

- A. Cryptographic decoding, data decryption technology
- B. Document Digital Digest Analysis Techniques
- C. Techniques to uncover the links between different pieces of evidence
- D. Spam tracking technology

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 7

Regarding AH and ESP security protocols, which of the following options is correct? (Multiple choices)

- A. AH can provide encryption and authentication functions
- B. ESP can provide encryption and authentication functions
- C. The agreement number of AH is 51
- D. The agreement number of ESP is 51

Correct Answer: BC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 8

DDoS attacks belong to which of the following attack types?

- A. Spying Scan Attack
- B. Malformed message attack
- C. Special message attacks
- D. Traffic attacks

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 9

Regarding SSL VPN technology, which of the following options is wrong?

- A. SSL VPN technology is perfect for NAT traversal scenarios
- B. The encryption of SSL VPN technology is only effective at the application layer
- C. SSL VPN requires a dial-up client
- D. SSL VPN technology extends the reach of an enterprise's network

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 10

Which of the following options can be operated in the advanced settings of windows firewall? (Multiple choices)

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

Correct Answer: ABCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 11

When a NAT server is configured on a USG series firewall, a server-map table is generated. Which of the following is not included in the performance?

- A. Destination IP
- B. Destination port number
- C. Agreement number
- D. Source IP

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 12

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

- A. ICMP redirect message attack
- B. ICMP Unreachable Packet Attack
- C. IP address scanning attack
- D. Oversized ICMP packet attack

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 13

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

- A. Teardrop attack
- B. Smurf attack

- C. TCP Fragmentation Attack
- D. ICMP Unreachable Packet Attack

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 14

The "Caesar cipher" is mainly used to encrypt data by using a stick of a specific specification.

- A. Yes
- B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 15

Which of the following are remote authentication methods? (Multiple choices)

- A. RADIUS
- B. Local

- C. HWTACACS
- D. LLDP

Correct Answer: AC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 16

When the firewall hard disk is in place, which of the following is a correct description of the firewall log?

- A. Administrators can publish content logs to view network threat detection and defense records
- B. Administrators can use the threat log to understand the user's security risk behavior and the reasons for being alerted or blocked
- C. The administrator learns the user's behavior, groped keywords, and the effectiveness of the audit policy configuration through the user activity log
- D. The administrator can learn the security policy of traffic hit through the policy hit log, which can be used for fault location when a problem occurs.

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 17

In the Client-Initiated VPN configuration, it is generally recommended to plan the address pool and the headquarters network addresses as different network segments, otherwise the gateway device must be configured

Enable proxy forwarding.

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 18

Which of the following is the encryption technology used in digital envelopes?

- A. Symmetric encryption algorithm
- B. Asymmetric encryption algorithm
- C. Hashing algorithm
- D. Stream encryption algorithm

Correct Answer: B

Section: (none)

Explanation

QUESTION 19

In addition to the built-in Portal authentication, the firewall also supports custom Portal authentication. When custom Portal authentication is used, it does not need to be deployed separately.

External Portal server.

- A. Yes
- B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 20

NAPT technology can implement one public network IP address for multiple private network hosts.

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 21

IPSec VPN technology does not support NAT traversal when using ESP security protocol encapsulation, because ESP encrypts the packet header

- A. Yes
- B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 22

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

- A. Can be used without a client
- B. Can encrypt the IP layer
- C. NAT traversal problem
- D. No authentication required

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 23

Some applications, such as Oracle database applications, have no data stream transmission for a long time, which interrupts the firewall session connection, resulting in business interruption. The following Which is the optimal solution?

- A. Configure a long service connection
- B. Enable ASPF function
- C. Optimizing security policies
- D. Enable shard cache

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 24

"Implement security monitoring and management of information and information systems to prevent illegal use of information and information systems" is to realize which features of information security Sex?

- A. Confidentiality
- B. Controllability
- C. Non-repudiation
- D. Integrity

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 25

When configuring a security policy, one security policy can reference an address set or configure multiple destination IP addresses.

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 26

Which of the following options does not fall into the 5-tuple range?

- A. Source IP
- B. Source MAC
- C. Destination IP
- D. Destination port

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 27

Regarding Client-Initialized L2TP VPN, which of the following statements is wrong?

- A. After a remote user accesses the Internet, the client software can directly initiate an L2TP tunnel connection request to the remote LNS.
- B. The LNS device receives the user's L2TP connection request and can authenticate the user based on the user name and password
- C. LNS assigns private IP addresses to remote users
- D. Remote users do not need to install VPN client software

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 28

Regarding the description of the vulnerability scan, which of the following is wrong?

- A. Vulnerability scanning is a technology that remotely monitors the vulnerability of the security performance of the target network or host based on the network. It can be used to simulate attacks. Inspection and security audit.
- B. Vulnerability scanning is used to detect the existence of vulnerabilities on the target host system. Generally, the target host is scanned for specific vulnerabilities.
- C. Vulnerability scanning is a passive precautionary measure that can effectively avoid hacking
- D. Vulnerability scanning can be performed based on the results of ping scanning and port scanning

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 29

Regarding the firewall security policy statement, what is wrong with the following options?

- A. If the security policy is permit, discarded packets will not accumulate "hits"
- B. When configuring a security policy name, you cannot reuse the same name
- C. Adjust the order of security policies, no need to save configuration files, take effect immediately

D. The security policy entries of Huawei USG series firewalls cannot exceed 128

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 30

Which of the following protection levels are included in the TCSEC standard? (Multiple choices)

Page 10

A. Verify protection level

B. Mandatory protection levels

C. Autonomous protection level

D. Passive protection level

Correct Answer: ABC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 31

Which of the following options are part of the PKI architecture? (Multiple choices)

A. End entity

B. Certificate authority

C. Certificate Registration Authority

D. Certificate storage

Correct Answer: ABCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 32

"Good observation" and "keep skepticism" can help us better identify security threats in the cyber world

A. Yes

B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 33

In tunnel encapsulation mode, IPSec configuration does not need to have a route to the destination private network segment, because the data will be re-encapsulated to use the new IP

Header looks up the routing table.

A. Yes

B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 34

Regarding the description of windows firewall, which of the following options are correct? (Multiple choices)

Page 11

A. The windows firewall can only allow or prohibit preset programs or functions and programs installed on the system.

Custom release rules

B. Windows firewall not only allows or prohibits the preset programs or functions and programs installed on the system, but also supports itself based on the protocol or end

Slogan Custom Release Rules

C. If you cannot access the Internet during the Windows firewall setting process, you can use the Restore Defaults function to quickly restore the firewall to its original state.

state

D. Windows firewall can change notification rules even when it is turned off

Correct Answer: BCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 35

Which of the following statements about investigation and forensics is correct?

- A. Evidence may not be required during the investigation
- B. Evidence obtained by wiretapping is also valid
- C. Enforcement agencies are best involved in all investigations and evidence gathering processes
- D. Documentary evidence is required in computer crime

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 36

Regarding online user management, which of the following is wrong?

- 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 a default user group by default.
- D. Each user belongs to at least one user group or multiple user groups

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 37

Which of the following is not the method used in the Detection link in the P2DR model?

- A. Real-time monitoring
- B. Detection
- C. Alarm
- D. Closed Services

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 38

Which of the following is not a LINUX operating system?

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

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 39

In some scenarios, both source IP addresses and destination IP addresses need to be converted. Which of the following technologies is used in this scenario?

- A. Bidirectional NAT
- B. Source NAT
- C. NAT-Server
- D. NAT ALG

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 40

Which of the following protocols can guarantee the confidentiality of data transmission? (Multiple choices)

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

Correct Answer: BD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 41

After the web redirection function is configured on the USG series firewall, the authentication page cannot be displayed. Which of the following is not the cause of the fault?

- A. The authentication policy is not configured or is incorrectly configured

Page 13

- B. Web authentication is not enabled

- C. The browser SSL version does not match the SSL version of the firewall authentication page

- D. The port number of the authentication page service is set to 8887

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 42

Which of the following is the correct description of the order of the four phases of the Information Security Management System (ISMS)?

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

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 43

In the information security system construction management cycle, which of the following actions need to be implemented in the "check" link?

- A. Design of safety management system
- B. Safety management system implementation
- C. Risk assessment
- D. Safety management system operation monitoring

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 44

- A. The status of this firewall VGMP group is Active

- B. The VRRP group status of this firewall's G1 / 0/0 and G1 / 0/1 interfaces is standby

Page 14

- C. The HRP heartbeat interfaces of this firewall are G1 / 0/0 and G1 / 0/1

- D. This firewall must be in a preemptive state

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 45

Classification of servers by shape can be divided into the following types? (Multiple choices)

- A. Blade server

- B. Tower Server
- C. Rack Server
- D. X86 server

Correct Answer: ABC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 46

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

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 47

According to the protection object to divide the firewall, windows firewall belongs to-?

- A. Software firewall
- B. Hardware firewall
- C. Stand-alone firewall
- D. Network firewall

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 48

Which of the following options are ways for a PKI entity to apply for a local certificate from a CA? (Multiple choices)

-
- A. Apply online
 - B. Local application
 - C. Online Application
 - D. Offline application

Correct Answer: AD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 49

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

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 50

Which of the following is not a symmetric encryption algorithm?

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

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 51

Which of the following options are correct regarding configuring firewall security zones? (Multiple choices)

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

Correct Answer: AD

Section: (none)

Explanation

Explanation / Reference:

Page 16

QUESTION 52

Digital certificates can be divided into local certificates, CA certificates, root certificates, and self-signed certificates according to different usage scenarios.

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 53

Regarding the root CA certificate, which of the following is incorrect?

- A. Issuer is CA
- B. The certificate subject name is CA
- C. Public key information is the CA's public key
- D. The signature is generated by CA public key encryption

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 54

Which of the following configurations can implement the NAT ALG function?

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

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 55

Regarding the firewall gateway's anti-virus response method for the HTTP protocol, which of the following statements is wrong?

- A. When the gateway device blocks the HTTP connection, push the web page to the client and generate a log
- B. Response methods include announcement and blocking
- C. Alarm mode The device only generates logs and sends the files without processing the HTTP protocol.
- D. Blocking means that the device disconnects from the HTTP server and blocks file transfers

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

Page 17

QUESTION 56

Which of the following is not a user authentication method in the USG firewall?

- A. Certification Free

- B. Password authentication
- C. Single sign-on
- D. Fingerprint authentication

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 57

The firewall GE1 / 0/1 and GE1 / 0/2 ports belong to the DMZ area. If you want to realize that the area connected to GE1 / 0/1 can access the area Area, which of the following is correct?

- A. Need to configure Local to DMZ security policy
- B. No configuration required
- C. Inter-domain security policy needs to be configured
- D. Need to configure DMZ to local security policy

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 58

The process of forwarding the first packet of a session between firewall domains has the following steps:

- 1.Find routing table
- 2.Find inter-domain packet filtering rules
- 3.Find the session table
- 4.Find blacklist

Which of the following order is correct?

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

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 59

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

Page 18

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

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 60

Which of the following are the basic functions of antivirus software? (Multiple choices)

- A. Protection against viruses
- B. Finding viruses
- C. Remove the virus
- D. Replication virus

Correct Answer: ABC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 61

The European TCSEC Code is divided into two modules, functional and evaluation, mainly used in the military, government and commercial fields

A. Yes

B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 62

In the future development trend of information security, terminal detection is an important part. Which of the following methods fall into the category of terminal detection? (Multiple choices)

A. Install host anti-virus software

B. Monitor and remember external devices

C. Prevent users from accessing public search engines

D. Monitor host registry modification records

Correct Answer: AD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 63

Use iptables to write a rule that does not allow the network segment 172.16.0.0/16 to access the device. Which of the following rules is correct?

A.

B.

C.

D.

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 64

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

A. NAT Policy

B. Are heartbeat interfaces with the same serial number configured?

C. Next hop and outgoing interface of the static route

D. Authentication strategy

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 65

In the USG series firewall, you can use the _____ function to provide well-known application services for non-well-known ports.

A. Port mapping

B. MAC and IP address binding

C. Packet filtering

D. Long connection

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 66

The questionnaire design principles do not include which of the following?

A. Integrity

B. Openness

C. Specificity
D. Consistency
Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 67

To implement the "anti-virus function" in the security policy, you must activate the license.

A. Yes
B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 68

The configuration commands for the NAT address pool are as follows:

The meaning of the no-pat parameter is:

A. No address translation
B. Port multiplexing
C. Do not convert source ports
D. Do not convert the destination port

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 69

On the surface, threats such as viruses, vulnerabilities, and Trojan horses are the cause of information security incidents. However, the root cause is that information security incidents are related to people and information systems.

It is also very relevant in itself.

A. Yes
B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 70

When connecting to Wi-Fi in public places, which of the following actions is relatively more secure?

A. Connect to an unencrypted Wi-Fi hotspot
B. Connect to a paid Wi-Fi hotspot provided by the operator and only browse the web
C. Connect to unencrypted free Wi-Fi for online shopping
D. Connect encrypted free Wi-Fi for online transfer operations

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 71

Which of the following is an action to be taken during the summary phase in a cybersecurity emergency response? (Multiple choices)

A. Establish a defense system and specify control measures
B. Evaluate the implementation of emergency plans and propose follow-up improvement plans
C. Judging the effectiveness of isolation measures
D. Evaluation of emergency response organization members

Correct Answer: BD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 72

Regarding port mirroring, which of the following descriptions are correct? (Multiple choices)

- A. Mirrored port copies packets to observing port
- B. The observing port sends the received message to the monitoring device
- C. The mirrored port sends the received message to the monitoring device
- D. Observing port copies packets to mirrored port

Correct Answer: AB

Section: (none)

Explanation

Explanation / Reference:

QUESTION 73

Which of the following options is the protocol number for GRE?

- A. 46
- B. 47
- C. 89
- D. 50

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

Page 22

QUESTION 74

Which of the following is wrong about the VGMP protocol description?

- A. VGMP joins multiple VRRP backup groups on the same firewall to a management group, and all VRRP backup groups are managed by the management group.
- B. VGMP guarantees that the status of all VRRP backup groups in the management group is consistent by uniformly controlling the status of each VRRP backup group.
- C. The VGMP group device in the Active state periodically sends hello packets to the peer.
Respond
- D. By default, when the Hello side does not receive the Hello message sent by the peer for three hello packet cycles, it will consider that the peer has failed.
And switch yourself to Active state.

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 75

A and B communication parties perform data communication. If the asymmetric encryption algorithm is used for encryption, when A sends data to B, which of the following keys will be used

Data encryption?

- A. A's public key
- B. A's private key
- C. Public key of B
- D. B's private key

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 76

IPSec VPN uses asymmetric encryption algorithm to encrypt the transmitted data

- A. Yes
- B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 77

Regarding GRE encapsulation and decapsulation, which of the following descriptions is incorrect?

- A. The encapsulation process. The original data packet is sent to the Tunnel interface by looking up the route and then the GRE encapsulation is started.
- B. Encapsulation process. After encapsulation by the GRE module, this packet will enter the IP module for further processing.
- C. Decapsulation process. After receiving the GRE packet, the destination sends the packet to the tunnel interface by searching for the route and then decapsulates the GRE
- D. Decapsulation process. After decapsulation by the GRE module, this packet will enter the IP module for further processing.

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 78

The repair of anti-virus software only needs to repair some system files deleted by mistake when checking for viruses to prevent system crashes

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 79

Which of the following does not fall into the hierarchy of cybersecurity incidents?

- A. Major cybersecurity incidents
- B. Special cybersecurity incidents
- C. General cybersecurity incidents
- D. Major cybersecurity incidents

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 80

Which of the following statements is true about single sign-on? (Multiple choices)

- A. The device can identify users who have been authenticated by the identity authentication system
- B. AD domain single sign-on has only one deployment mode
- C. Although the user password is not required, the authentication server needs to interact with the user password to ensure that the authentication passes.
- D. AD domain single sign-on can be synchronized to the firewall by mirroring the login data stream

Correct Answer: AD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 81

Regarding the relationship and role of VRRP / VGMP / HRP, which of the following statements is correct? (Multiple choices)

- A. VRRP is responsible for sending free ARP to direct traffic to the new master device when the master and backup are switched
- B. VGMP is responsible for monitoring equipment failures and controlling fast switching of equipment

- C. HRP is responsible for data backup during hot standby operation
- D. Active VGMP group may include VRRP group in standby state

Correct Answer: ABC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 82

The administrator PC is directly connected to the USG firewall management interface and uses the web method to perform the initialization. Which of the following statements is correct? (Multiple choices)

- A. The browser of the management PC accesses http://192.168.0.1
- B. The IP address of the management PC is manually set to 192.168.0.2-192.168.0.254
- C. The browser of the management PC accesses http://192.168.1.1
- D. Set the network card of the management PC to obtain an IP address automatically

Correct Answer: AB

Section: (none)

Explanation

Explanation / Reference:

QUESTION 83

In the Huawei SDC solution, which layer of equipment does the firewall belong to?

- A. Analysis layer
- B. Control layer
- C. Executive layer
- D. Monitoring layer

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 84

When dual-system hot backup is deployed on the firewall, which of the following protocols is required to switch the overall state of the VRRP backup group?

- A. VRRP
- B. VGMP
- C. HRP
- D. OSPF

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 85

As shown in the figure, the online scenario of internal users of the enterprise is as follows:

1. The authentication is passed. The USG allows the connection to be established.
2. The user accesses the Internet and enters http://1.1.1.1
3. USG push authentication interface
4. The user successfully accesses http://1.1.1.1, and the device creates a session table
5. The user enters the correct username and password

The following correct process ordering should be:

- A. 2-> 5-> 3-> 1-> 4
- B. 2-> 3-> 5-> 1-> 4
- C. 2-> 1-> 3-> 5-> 4
- D. 2-> 3-> 1-> 5-> 4

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 86

Regarding the description of firewall dual-system hot backup, which of the following options are correct? (Multiple choices)

- A. When multiple areas on the firewall need to provide dual-system backup, multiple VRRP backup groups need to be configured on the firewall.
- B. Require that the status of all VRRP backup groups in the same VGMP management group on the same firewall be consistent
- C. The firewall dual-system hot backup needs to synchronize the backup of the session table, MAC table, routing table and other information between the master and slave

D. VGMP is used to ensure the consistency of all VRRP backup group switching

Correct Answer: ABD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 87

Which of the following is the encryption technology used in digital envelopes?

- A. Symmetric encryption algorithm
- B. Asymmetric encryption algorithm
- C. Hashing algorithm
- D. Feeding Algorithm

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

Page 26

QUESTION 88

Regarding the matching conditions of the security policy, which of the following options are correct? (Multiple choices)

- A. "Source Security Zone" is an optional parameter in the matching conditions
- B. "Time period" in the matching condition is optional
- C. "Apply" in matching conditions is optional
- D. "Service" is an optional parameter in the matching conditions

Correct Answer: ABCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 89

The attacker sends an ICMP response request and sets the destination address of the request packet as the broadcast address of the victim network.

What kind of attack does this behavior belong to?

- A. IP Spoofing Attack
- B. Smurf attack
- C. ICMP redirect attack
- D. SYN flood attack

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 90

Regarding the sequencing of PKI work processes, which of the following is correct?

- A. 1-2-6-5-7-4-3-8
- B. 1-2-7-6-5-4-3-8
- C. 6-5-4-1-2-7-3-8
- D. 6-5-4-3-1-2-7-8

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

Page 27

QUESTION 91

Clients in the firewall Trust domain can log in to the FTP server in the Untrust domain, but cannot download files. Which of the following methods can solve the problem? (Multiple choices)

- A. Allow port 21 between Trust and Untrust
- B. When FTP works in port mode, modify the security policy action from Trust to Untrust zone to allow

- C. Enable detect ftp
- D. When FTP works in Passive mode, modify the security policy action from Trust to Untrust zone to allow

Correct Answer: CD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 92

Which of the following is not part of the digital certificate?

- A. Public key
- B. Private key
- C. Validity period
- D. Issuer

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 93

Regarding the description of TCP / IP protocol stack decapsulation, which of the following is correct? (Multiple choices)

A. The data packet is first transmitted to the data link layer. After parsing, the data link layer information is stripped and the network layer information is known based on the parsing information.

Such as IP

B. After the transport layer (TCP) receives the data packet, the transport layer information is stripped after parsing, and the upper layer processing protocol is known based on the parsing information.

Such as UDP

C. After the network layer receives the data packet, the network layer information is stripped after parsing, and the upper layer processing protocol is known based on the parsing information, such as

HTTP

D. After the application layer receives the data packet, the application layer information is stripped after parsing, and the user data finally displayed and the number sent by the sender host

Data is exactly the same

Correct Answer: AD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 94

Which of the following is not a key technology of antivirus software?

- A. Shelling technology
- B. Self-protection
- C. Format the disk
- D. Upgrade virus database in real time

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 95

Which of the following options are malicious programs? (Multiple choices)

- A. Trojan horse
- B. Vulnerabilities
- C. Worms
- D. Viruses

Correct Answer: ACD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 96

Which of the following are key elements of information security? (Multiple choices)

- A. Asset management
- B. Security operations and management
- C. Security products and technologies
- D. People

Correct Answer: ABCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 97

Which of the following is not a major form of computer crime?

- A. Implant Trojan into target host
- B. Hacking the target host
- C. Personal surveys using computers
- D. Use scanning tools to collect network information without permission

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 98

When the IPSec VPN tunnel mode is deployed, AH protocol is used for packet encapsulation. In the new IP packet header field, which of the following parameters need not be performed Data integrity check?

-
- A. Source IP address
 - B. Destination IP address
 - C. TTL
 - D. Identification

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 99

When configuring a GRE tunnel interface, which of the following parameters does the destination address generally refer to?

- A. Local Tunnel Interface IP Address
- B. Outbound IP address of the local end
- C. Peer external IP address
- D. IP address of the peer tunnel interface

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 100

Which of the following options are application risks (multiple choices)

- A. Network viruses
- B. Email security
- C. Database system configuration security
- D. Web Services Security

Correct Answer: ABCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 101

Security policy conditions can be divided into multiple fields, such as source address, destination address, source port, and destination port.

"And" relationship, that is, only if the information in the message and all fields match, it is considered to hit this policy.

- A. Yes

B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

Page 30

QUESTION 102

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

- A. Can be used without a client
- B. Can encrypt the IP layer
- C. NAT traversal problem
- D. No authentication required

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 103

Regarding the description of the four-way handshake to disconnect the TCP connection, which of the following is wrong?

- A. The active closing party sends the first FIN to perform an active shutdown, while the other party receives this FIN to be closed.
- B. When the passive shutdown receives the first FIN, it will send back an ACK and randomly generate an acknowledgement sequence number.
- C. The passive closing party needs to send an end-of-file character to the application, and the application closes its connection and causes a FIN
- D. After the passive closing party sends FIN, the active closing party must send back a confirmation and set the confirmation serial number to the received serial number plus 1

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 104

Which of the following is not an asymmetric encryption algorithm?

- A. DH
- B. MD5
- C. DSA
- D. RSA

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 105

Which of the following statements about Client-Initiated VPN is correct? (Multiple choices)

- A. A tunnel is established between each access user and the LNS
- B. Only one L2TP session and PPP connection are carried in each tunnel
- C. Each tunnel carries multiple L2TP sessions and PPP connections
- D. Each tunnel carries multiple L2TP sessions and a PPP connection

Correct Answer: AB

Section: (none)

Explanation

Page 31

Explanation / Reference:

QUESTION 106

Regarding the firewall security policy statement, what is wrong with the following options?

- A. If the security policy permits, discarded packets will not accumulate "hits"
- B. When configuring a security policy name, you cannot reuse the same name

- C. Adjust the order of security policies, no need to save configuration files, take effect immediately
- D. The number of security policy entries of Huawei USG series firewalls cannot exceed 128

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 107

Which of the following options of VPN technology supports datagram encryption? (Multiple choices)

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

Correct Answer: AC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 108

Which of the following is the username / password for the first login of the USG series firewall?

- A. User name admin
Password Admin @ 123
- B. User name admin
Password admin @ 123
- C. User name admin
Password admin
- D. User name admin
Password Admin123

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 109

During the use of the server, there are various security threats. Which of the following options is not a server security threat?

- A. Natural disasters
- B. DDos attack
- C. Hacking
- D. Malicious programs

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 110

Regarding Client-Initialized L2TP VPN, which of the following statements is wrong?

- A. After a remote user accesses the Internet, he can initiate an L2TP tunnel connection request to the remote LNS directly through the client software.
- B.; The NS device receives the user's L2TP connection request, and can authenticate the user based on the user name and password
- C. LNS assigns private IP addresses to remote users
- D. Remote users do not need to install VPN client software

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 111

Which of the following options are not included in the survey target for the safety assessment method?

- A. Network System Administrator
- B. Security administrator

- C. HR
- D. Technical Leader

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 112

The undiscovered vulnerability is the 0 day vulnerability

- A. Yes
- B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

Page 33

QUESTION 113

Regarding the problem that two-way binding users without authentication can not access network resources, which of the following options are possible reasons? (Multiple choices)

- A. Authentication-free users and authenticated users are in the same security zone
- B. Authentication-free users do not use a PC with the specified IP / MAC address
- C. The authentication action in the authentication policy is set to "non-account / exempt authentication"
- D. Online users have reached the maximum

Correct Answer: BD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 114

ASPF (Application Specific Packet Filter) is a packet filtering technology based on the application layer, which is implemented through a server-map table.

Special security mechanisms.

Which of the following statements about ASPF and server-map tables is correct? (Multiple choices)

- A. ASPF monitors messages during communication
- B. ASPF can dynamically create a server-map table
- C. ASPF dynamically allows multi-channel protocol data to pass through the server-map table
- D. The five-tuple server-map entry implements a similar function to the session table

Correct Answer: ABC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 115

Which of the following are features of the address translation technology? (Multiple choice)

- A. Address translation allows internal network users (private IP addresses) to access the Internet
- B. Address translation can enable many hosts in the internal LAN to share an IP address to go online
- C. Address translation can handle encrypted IP headers
- D. Address translation can shield users on the internal network and improve the security of the internal network

Correct Answer: ABD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 116

Regarding NAT address translation, which of the following statements is wrong?

- A. Configure NAT address pool in source NAT technology, you can configure only one IP address
 - B. Address translation can provide FTP, WWW, Telnet and other services to the outside in the LAN according to the needs of users
 - C. Some application layer protocols carry IP address information in the data. When they are NATed, the IP address information in the upper layer data must be modified
 - D. For some non-TCP, UDP protocols (such as ICMP, PPTP), NAT cannot be performed
-

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 117

Regarding the relationship and role of VRRP / VGMP / HRP, which of the following statements are correct?

(Multiple choices)

- A. VRRP is responsible for sending gratuitous ARP to direct traffic to the new master device during the master / slave switchover.
- B. VGMP is responsible for monitoring equipment failures and controlling fast switching of equipment
- C. HRP is responsible for data backup during hot standby operation
- D. Active VGMP group may include VRRP group in Standby state

Correct Answer: ABC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 118

When the firewall upgrades the signature database and virus database online through the security service center, the firewall must be connected to the Internet first, and the configuration must be correct

DNS address

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 119

Which of the following is not a symmetric encryption algorithm?

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

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 120

The results you see with display ike sa are as follows. Which of the following statements is wrong?

- A. IKE SA has been established
- B. IPSec SA has been established
- C. The neighbor address is 2.2.2.1
- D. IKE uses V1 version

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 121

Regarding the comparison between windows and linux, which of the following statements is wrong?

- A. Linux newbies are difficult to get started and require some learning and guidance
- B. Windows can be compatible with most software and play most games
- C. Linux is open source and you can do whatever you want
- D. windows are open source, do whatever you want

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 122

Which of the following options are at the core of the IATF (Information Security Technology Framework) model? (Multiple choices)

- A. Environment
- B. People
- C. Technology
- D. Operation

Correct Answer: BCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 123

Which of the following are multi-user operating systems? (Multiple choices)

- A. MSDOS
- B. UNIX
- C. LINUX
- D. Windows

Correct Answer: BCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 124

The preservation of electronic evidence is directly related to the legal validity of evidence and the preservation of legal procedures can ensure its authenticity and reliability. Which of the following is not

On evidence preservation technology?

- A. Encryption technology
- B. Digital certificate technology
- C. Digital signature technology
- D. Message mark tracking technology

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 125

The VGMP group does not actively send VGMP packets to the peer when any of the following conditions occur:

- A. Dual-system hot backup function is enabled
- B. Manually switch the active / standby status of the firewall
- C. Firewall business interface failure
- D. Session table entry changes

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 126

Which of the following options can be operated in the advanced settings of windows firewall? (Multiple choices)

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

Correct Answer: ABCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 127

Regarding the security policy configuration command, which of the following is correct?

- A. Prohibit ICMP packets from the trust zone accessing the untrust zone and the destination address is 10.1.10.10.
- B. Forbid all ICMP packets from the trust zone to access all hosts in the untrust zone and the destination address is 10.1.0.0/16
- C. It is forbidden to access all host ICMP packets from the trust zone to the untrust zone and the source address is 10.1.0.0/16.
- D. Forbid all host ICMP packets from the trust zone to access the untrust zone and the source address is 10.2.10.10.

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 128

In information security prevention, commonly used security products include firewalls, Anti-DDos devices, and IPS / IDS devices

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 129

If the administrator uses the default authentication domain to authenticate the user, the user only needs to enter the user name when logging in; if the administrator

Use the newly created authentication domain to authenticate the user, the user needs to enter "username @ certificate domain name" when logging in

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 130

Digital certificate technology solves the problem that public key owners cannot determine in digital signature technology

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 131

Which of the following options are technical features of an intrusion prevention system? (Multiple choices)

- A. Online mode
- B. Real-time blocking
- C. Self-learning and adaptive
- D. Straight deployment

Correct Answer: ABC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 132

Regarding firewall security policies, are the following items correct?

- A. By default, the security policy can control unicast packets and broadcast packets.

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

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 133

Which of the following information is encrypted when using a digital envelope? (Multiple choices)

- A. Symmetric keys
- B. User data
- C. Recipient public key
- D. Receiver private key

Correct Answer: AB

Section: (none)

Page 39

Explanation

Explanation / Reference:

QUESTION 134

Which of the following options fall within the scope of ISO27001 certification? (Multiple choices)

- A. Access control
- B. Personnel safety
- C. Vulnerability Management
- D. Business Continuity Management

Correct Answer: ABCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 135

Regarding the description of the firewall, which of the following is correct?

- A. The firewall cannot access the network transparently.
- 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 side-by-side deployment
- D. Depending on the usage scenario, the firewall can be deployed in transparent mode or in three-bedroom mode.

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 136

On Huawei USG series devices, the administrator wants to erase 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: (none)

Explanation

Explanation / Reference:

QUESTION 137

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

- A. Buffer overflow attack exploits the defect of the software system's memory operation and runs the attack code with high operation authority.

Page 40

- B. Buffer overflow attacks are not related to operating system vulnerabilities and architecture.

- C. Buffer overflow attacks are one of the common ways to attack software systems
- D. Buffer overflow attacks are application-level attacks.

Correct Answer: ACD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 138

Security precaution technologies have different approaches at different technical levels and fields. Which of the following devices can be used for network layer security? (Multiple choices)

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

Correct Answer: BCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 139

IPSEC VPN technology does not support NAT traversal when using ESP security protocol encapsulation, because ESP encrypts the packet header

- A. Yes
- B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 140

Which of the following options are features of SSL VPN? (Multiple choices)

- A. User authentication
- B. Port scanning
- C. File sharing
- D. WEB rewriting

Correct Answer: AC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 141

In the digital signature process, which of the following is the HASH algorithm to verify the integrity of the data transmission?

- A. User data
- B. Symmetric keys
- C. Recipient public key
- D. Receiver private key

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 142

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

- A. Accessing devices or device-initiated traffic
- B. DHCP, BGP, OSPF, LDP packets
- C. Visitors accessing HTTP traffic
- D. DNS message corresponding to the first HTTP service data flow

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 143

The firewalls GE1 / 0/1 and GE1 / 0/2 both belong to the DMZ area. If you want to realize that the area connected to GE1 / 0/1 can access GE1 / 0/2

Which of the following is correct for the connected area?

- A. Need to configure local to DMZ security policy
- B. No configuration required
- C. Inter-domain security policy needs to be configured
- D. Need to configure DMZ to local security policy

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 144

The use of computers to store information about criminal activity is not a computer crime

- A. Yes
- B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 145

Page 42

Regarding IKE SA, which of the following is incorrect?

- A. IKE SA is bidirectional
- B. IKE is an application layer protocol based on UDP
- C. IKE SA is for IPSec SA
- D. The encryption algorithm used for user data packets is determined by IKE SA

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 146

Which of the following statements about VPN is wrong?

- A. Virtual private network costs less than leased lines
- B. VPN technology necessarily involves encryption technology
- C. VPN technology is a technology that reuses logical channels on actual physical lines
- D. The emergence of VPN technology enables employees on business trips to remotely access internal servers of the enterprise

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 147

Which of the following are standard port numbers for the FTP protocol? (Multiple choices)

- A. 20
- B. 21
- C. 23
- D. 80

Correct Answer: AB

Section: (none)

Explanation

Explanation / Reference:

QUESTION 148

The level of information security protection is to improve the overall level of national security, and to rationally optimize the allocation of security resources so that

Send back maximum safety and economic benefits

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Page 43

Explanation / Reference:

QUESTION 149

In response to network security incidents, remote emergency response is generally adopted first. If remote access is not available, it can be resolved for customers.

After the customer confirms the problem, go to the local emergency response process

A. Yes

B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 150

Generally, we will divide the server into two categories: general server and function server. Which of the following options meets this classification criteria?

A. By application level

B. By purpose

C. Divided by shape

D. Divided by architecture

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 151

NAPT technology can implement a public IP address for multiple private network hosts

A. Yes

B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 152

After the firewall uses the hrp standby config enable command to enable the standby device configuration function, all the information that can be backed up can be

Configure directly on the standby device, and the configuration on the standby device can be synchronized to the active device

A. Yes

B. wrong

Correct Answer: A

Section: (none)

Explanation

Page 44

Explanation / Reference:

QUESTION 153

Which of the following options are characteristic of symmetric encryption algorithms? (Multiple choices)

A. Fast encryption

B. Confidentiality is slow

C. Insecure key distribution

D. High key distribution security

Correct Answer: AC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 154

Which of the following options are harms of a traffic attack? (Multiple choices)

- A. Network is down
- B. Server is down
- C. Data is stolen
- D. Web pages are tampered with

Correct Answer: AB

Section: (none)

Explanation

Explanation / Reference:

QUESTION 155

Intrusion prevention system (IPS) is a defense system that can block in real time when intrusion behaviors are discovered

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 156

Regarding the consistency check of the HRP master / backup configuration, which of the following options is not included?

- A. NAT Policy
- B. Are heartbeat interfaces with the same serial number configured?
- C. Next hop and outgoing interface of the static route
- D. Authentication strategy

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 157

Regarding NAT configuration, which of the following is wrong?

- A. Configure source NAT in transparent mode, firewall does not support easy-ip mode
- B. The IP address in the address pool can overlap with the public IP address of the NAT server
- C. When there is VoIP service on the network, NAT ALG does not need to be configured
- D. The firewall does not support NAPT conversion of ESP and AH packets

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 158

Regarding the description of security policy actions and security profiles, which of the following options are correct? (Multiple choices)

- A. If the action of the security policy is "Forbidden", the device will discard this traffic and no further content security checks will be performed.
- B. Security profiles can take effect without being applied to security policies whose actions are allowed
- C. The security profile must be applied under a 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: AC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 159

Encryption technology protects data during data transmission. Which of the following options are included? (Multiple choices)

- A. Confidentiality
- B. Controllability

C. Integrity
D. Source verification
Correct Answer: ACD
Section: (none)

Explanation

Explanation / Reference:

QUESTION 160

After a cyber attack event, set up an isolation area, summarize data, and estimate losses according to the plan.
The above actions are a cyber security emergency
At what stage of the response is the work involved?

- A. Preparation stage
- B. Detection phase
- C. Inhibition phase
- D. Recovery phase

Page 46

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 161

IPSec VPN uses asymmetric encryption algorithm to encrypt the transmitted data

- A. Yes
- B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 162

The digital certificate is fair to the public key through a third party organization, thereby ensuring the non-repudiation of data transmission. So confirm the public key is correct
Sex requires only the certificate of the correspondent

- A. Yes
- B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 163

Digital signature is to generate a digital fingerprint by using a hashing algorithm to ensure the integrity of data transmission

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 164

Regarding the description of the firewall fragment cache function, which of the following options are correct? (Multiple choices)

- 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 fragment according to the inter-domain security policy.
- C. For fragmented packets, NAT ALG does not support the processing of SIP fragmented packets
- D. By default, the maximum number of fragment caches for an IPv4 packet is 32, and the maximum number of fragment caches for an IPv6 packet is 255

Page 47

Correct Answer: ACD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 165

The SIP protocol uses SDP messages to establish sessions. SDP messages contain remote addresses or multicast addresses.

A. Yes

B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 166

Which of the following attacks is not a cyber attack?

A. IP Spoofing Attack

B. Smurf attack

C. MAC Address Spoofing Attack

D. ICMP attack

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 167

What versions of the SNMP protocol? (Multiple choices)

A. SNMPv1

B. SNMPv2b

C. SNMPv2c

D. SNMPv3

Correct Answer: ACD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 168

Regarding the description of the preemption function of VGMP management, which of the following is wrong?

A. By default, the preemption function of the VGMP management group is enabled.

B. By default, the preemption delay time of the VGMP management group is 40s.

C. Preemption refers to the restoration of the priority of the original faulty master device when it fails. At this time, you can reset your status

Preemptive

D. After the VRRP backup group is added to the VGMP management group, the original preemption function on the VRRP backup group becomes invalid

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 169

In the IPSec VPN transmission mode, what part of the data packet is encrypted?

A. Network layer and upper layer data messages

B. Original IP header

C. New IP packet header

D. Transport layer and upper layer data messages

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 170

Regarding windows logs, which of the following descriptions is incorrect?

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

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 171

For the description of IP Spoofing, which of the following is wrong?

- A. IP spoofing attacks are launched using the normal IP address-based trust relationship between hosts.
- B. After a successful IP spoofing attack, an attacker can use a forged IP address to impersonate a legitimate host to access key information
- C. The attacker needs to disguise the source IP address as a trusted host and send a data segment with a SYN tag to request a connection
- D. Hosts based on IP address trust relationship can log in directly without entering password authentication

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 172

In the USG series firewall, which command can be used to query the NAT translation result?

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

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 173

The preservation of electronic evidence is directly related to the legal validity of evidence and the preservation of legal procedures, so that its authenticity and reliability can be guaranteed. Which of the following is not On evidence preservation technology?

- A. Encryption technology
- B. Digital certificate technology
- C. Digital signature technology
- D. Message mark tracking technology

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 174

Which of the following state information can be backed up by Huawei Redundancy Protocol (HRP)? (Multiple choices)

- A. Session table
- B. ServerMap entry
- C. Dynamic blacklist
- D. Routing table

Correct Answer: ABC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 175

As shown in the figure, a TCP connection is established between client A and server B. Which of the following "?" Message sequence numbers should be in the figure?

Page 50

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

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 176

Digital certificates can be divided into local certificates, CA certificates, root certificates, and self-signed certificates according to different usage scenarios.

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 177

Which of the following is the encryption technology used in digital envelopes?

- A. Symmetric encryption algorithm
- B. Asymmetric encryption algorithm
- C. Hashing algorithm
- D. Stream encryption algorithm

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

Page 51

QUESTION 178

Which of the following are remote authentication methods? (Multiple choices)

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

Correct Answer: AC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 179

Which of the following statements about IPSec SA is correct?

- A. IPSec SA is unidirectional
- B. IPSec SA is bidirectional
- C. Used to generate encryption keys
- D. Used to generate confidential algorithms

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 180

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

- A. Human audit
- B. Penetration testing
- C. Questionnaire

D. Data analysis

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 181

In Equal Guarantee 2.0, which stipulates that "spam emails should be detected and protected at key network nodes, and upgrades to spam protection mechanisms should be maintained

And update ""?

A. Malicious code prevention

B. Communication transmission

C. Centralized control

D. Border protection

Page 52

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 182

Which of the following options does not fall into the 5-tuple range?

A. Source IP

B. Source MAC

C. Destination IP

D. Destination port

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 183

In the state detection firewall, when the state detection mechanism is enabled, the second packet (SYN + ACK) of the three-way handshake reaches the firewall.

At this time, if there is no corresponding session table on the firewall, which of the following is correct?

A. The firewall does not create a session table, but allows packets to pass

B. If the firewall security policy allows packets to pass, create a session table

C. Messages must not pass through the firewall

D. The packets must pass through the firewall and establish a session

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 184

In a VRRP (Virtual Router Redundancy Protocol) group, the primary firewall periodically sends notification packets to the backup firewall.

The backup firewall is only responsible for listening to the notification message and will not respond.

A. Yes

B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 185

Huawei USG firewall VRRP notification messages are multicast packets, so each firewall in the backup group must be able to implement direct Layer 2 interworking.

Page 53

A. Yes

B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 186

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

A. Yes

B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 187

As shown in the figure is an application scenario of a NAT server, when the configuration is performed using the web configuration mode. Which of the following statements is true?

(Multiple choices)

A. When configuring the interzone security policy, you need to set the source security zone to Untrust and the target security zone to DMZ.

B. When configuring NAT Server, the internal address is 10.1.1.2 and the external address is 200.10.10.1

C. When configuring the interzone security policy, set the source security zone to DMZ and the target security zone to Untrust

D. When configuring NAT Server, the internal address is 200.10.10.1 and the external address is 10.1.1.2

Correct Answer: AB

Section: (none)

Explanation

Explanation / Reference:

QUESTION 188

In the configuration of L2TP, which of the following statements is correct for the Tunnel Name command? (Multiple choices)

A. Used to specify the local tunnel name

B. Tunnel name used to specify the peer

C. Tunnel Nname must be the same at both ends

D. If Tunnel Name is not configured, the tunnel name is the local system name

Correct Answer: AD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 189

Which of the following attack types does a DDos attack have?

A. Spying Scan Attack

B. Malformed message attack

C. Special message attacks

D. Traffic attacks

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 190

In the USG system firewall, you can use the function to provide well-known application services for non-well-known ports.

A. Port mapping

B. MAC and IP address binding

C. Packet filtering

D. Long connection

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 191

Regarding the command to check the number of security policy matches, which of the following is correct?

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

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 192

Which of the following options is a Layer 2 VPN technology?

Page 55

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

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 193

About the description of advanced settings of windows firewall, which of the following options are wrong? (Multiple choices)

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

Correct Answer: BD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 194

Regarding the description of VGMP group management, which of the following is wrong?

- A. The master / backup status of a VRRP backup group needs to be notified to the VGMP management group to which it belongs.
- B. The interface types and numbers of the heartbeat interfaces of the two firewalls can be different, as long as the Layer 2 communication
- C. Periodic hello messages between VGMPs of the active and standby firewalls
- D. The master and backup devices learn the status of each other through heartbeat exchange messages, and back up related commands and status information.

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 195

In the security assessment method, the purpose of a security scan is to scan the target system with a scan analysis and evaluation tool in order to find related vulnerabilities.

Prepare for the attack

- A. Yes
- B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 196

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

- A. Teardrop attack
- B. Smurf attack
- C. TCP Fragmentation Attack
- D. ICMP Unreachable Packet Attack

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 197

Regarding IKE SA, which of the following is incorrect?

- A. IKE SA is bidirectional
- B. IKE is an application layer protocol based on UDP
- C. IKE SA is for IPSec SA
- D. The encryption algorithm used for user data packets is determined by IKE SA

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 198

In the construction of an information security system, the relationship between important aspects of security and system behavior needs to be accurately described through a security model

- A. Yes
- B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 199

Security policy conditions can be divided into multiple fields, such as source address, destination address, source port, and destination port.

"And" relationship, that is, only if the information in the message and all fields match, it is considered to hit this policy.

- A. Yes
- B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 200

The matching principle of the security policy is: first find the manually-configured inter-domain security policy, and if it does not match, directly discard the data packet.

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 201

Which of the following is the response action of the gateway antivirus after detecting a mail virus? (Multiple choices)

- A. Alarm
- B. Block
- C. Declaration
- D. Delete attachments

Correct Answer: ABCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 202

Digital signature is to generate a digital fingerprint by using a hashing algorithm to ensure the integrity of data transmission

A. Yes

B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 203

Regarding NAT address translation, which of the following statements is wrong?

A. Configure NAT address pool in source NAT technology, you can configure only one IP address

B. Address translation can provide FTP, WWW, Telnet and other services to the outside in the LAN according to the needs of users

C. Some application layer protocols carry IP address information in the data. When they are NATed, the IP address information in the upper layer data must be modified

D. For some TCP and UDP protocols (such as ICMP, PPTP), NAT cannot be performed.

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 204

When a NAT server is configured on the firewall of the USG system, a server-map table is generated. Which of the following is not included in the performance?

A. Destination IP

B. Destination port number

C. Agreement number

D. Source IP

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 205

Which of the following options are malicious programs? (Multiple choices)

A. Trojan horse

B. Vulnerabilities

C. Worms

D. Viruses

Correct Answer: ACD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 206

Which of the following are the main implementation methods of gateway antivirus? (Multiple choices)

A. Agent scanning method

B. Stream scanning method

C. Package inspection and killing methods

D. File killing methods

Correct Answer: AB

Section: (none)

Explanation

Explanation / Reference:

QUESTION 207

Which of the following options is not part of the hashing algorithm?

- A. MD5
- B. SHA1
- C. SM1
- D. SHA2

Correct Answer: C

Section: (none)

Explanation

Page 59

Explanation / Reference:

QUESTION 208

Regarding the description of firewall dual-system hot backup, which of the following options are correct? (Multiple choices)

- A. When multiple areas on the firewall need to provide dual-system backup, multiple VRRP backup groups need to be configured on the firewall.
- B. Require that the status of all VRRP backup groups in the same VGMP management group on the same firewall be consistent
- C. The firewall dual-system hot backup needs to synchronize the backup of the session table, MAC table, routing table and other information between the master and slave
- D. VGMP is used to ensure the consistency of all VRRP backup group switching

Correct Answer: ABD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 209

Which of the following options is not a certificate save file format supported by the USG6000 series device?

- A. PKCS # 12
- B. DER
- C. PEM
- D. PKCS #

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 210

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

- A. ICMP redirect message attack
- B. ICMP Unreachable Packet Attack
- C. IP address scanning attack
- D. Oversized ICMP packet attack

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 211

Security precaution technologies have different approaches at different technical levels and fields. Which of the following devices can be used for network layer security? (Multiple choices)

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

Page 60

Correct Answer: BCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 212

Which of the following is used in digital signature technology to encrypt digital fingerprints?

- A. Sender public key
- B. Sender private key
- C. Recipient public key
- D. Receiver private key

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 213

The reason OSPF is more commonly used than RIP is that OSPF has device authentication and is more secure

- A. Yes
- B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 214

The content of intrusion detection covers authorized and unauthorized intrusion behaviors. Which of the following behaviors does not fall into the scope of intrusion detection?

- A. Impersonating another user
- B. The administrator deletes the configuration by mistake
- C. Worm Trojans
- D. Leaked data

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 215

For the description of ARP spoofing attack, which of the following is wrong

- A. The ARP implementation mechanism only considers normal business interactions, and does not verify any abnormal business interactions or malicious behaviors.
- B. ARP spoofing attacks can only be implemented through ARP responses, not through ARP requests

- C. When a host sends a normal ARP request, the attacker will respond preemptively, causing the host to establish an incorrect IP-MAC mapping
- D. ARP static binding is a solution to ARP spoofing attacks. It is mainly used in small network scenarios.

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 216

Which of the following mechanisms are used for MAC flood attacks? (Multiple choices)

- A. MAC learning mechanism of the switch
- B. Switch forwarding mechanism
- C. ARP learning mechanism
- D. Limit on the number of MAC entries

Correct Answer: ABCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 217

After the firewall uses the hrp standby config enable command to enable the standby device configuration function, all the information that can be backed up can be

Configuration is performed directly on the standby device, and the configuration on the standby device can be synchronized to the active device.

- A. Yes

B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 218

In practical applications, asymmetric encryption is mainly used to encrypt user data

A. Yes

B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 219

When the enterprise establishes its own information system, it checks each operation according to the internationally established authoritative standards and can detect its own information.

Is the system secure

A. Yes

B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 220

Which of the following options is the port number used for L2TP packets?

A. 17

B. 500

C. 1701

D. 4500

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 221

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

A. Human audit

B. Penetration testing

C. Questionnaire

D. Data analysis

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 222

IPSec VPN uses asymmetric encryption algorithm to encrypt the transmitted data

A. Yes

B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 223

Regarding firewall security policies, which of the following is correct?

A. By default, security policies can control unicast and broadcast packets

B. By default, security policies can control multicast

C. By default, the security policy controls only unicast packets

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

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 224

Which of the following information is encrypted when using a digital envelope? (Multiple choices)

A. Symmetric keys

B. User data

C. Recipient public key

D. Receiver private key

Correct Answer: AB

Section: (none)

Explanation

Explanation / Reference:

QUESTION 225

Which of the following is an action to be taken during the eradication phase in a cybersecurity emergency response?

(Multiple choice)

A. Find sick Trojan horses, illegal authorization, system loopholes, and deal with them in time

B. Revise security policies based on security incidents and enable security audits

C. Blocking attacks and reducing their scope

D. Confirm the degree of damage caused by the security incident and report the security incident

Correct Answer: AB

Section: (none)

Explanation

Explanation / Reference:

QUESTION 226

Which of the following attacks can DHCP Snooping prevent? (Multiple choices)

A. DHCP Server Phishing Attack

B. Man in the Middle and IP / MAC spoofing Attacks

C. IP spoofing attacks

D. Counterfeit DHCP lease renewal message attack using option82 field

Correct Answer: ABCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 227

In the Huawei SDSec solution, which of the following options belong to the equipment of the execution layer? (Multiple choices)

A. CIS

B. Fierhunter

C. Router

D. AntiDDoS

Correct Answer: BCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 228

A company employee account has expired, but the account can still be used to access the company server. What security risks does the above scenario belong to? (Multiple choices)

A. Managing security risks

B. Access security risks

C. System security risks

D. Physical security risks

Correct Answer: ABC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 229

What is the default backup mode for dual-system hot backup?

- A. Automatic backup
- B. Manual batch backup
- C. Quick session backup
- D. Configuration of the active and standby FWs after the device restarts

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 230

Network administrators can collect data to be analyzed on network devices through packet capture, port mirroring, or logs

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 231

The world's first worm, the "Morris Worm," made people realize that as people's dependence on computers grew,

The possibility of attack on computer networks is also increasing, and it is necessary to establish a comprehensive emergency response system

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 232

Which of the following is required for IPSec VPN? (Multiple choices)

- A. Configure IKE neighbors
- B. Configure IKE SA related parameters
- C. Configure IPSec SA related parameters
- D. Configure the flow of interest

Correct Answer: ABCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 233

Which of the following categories are included in Huawei firewall user management? (Multiple choices)

- A. Internet user management
- B. Access user management
- C. Administrator User Management
- D. Device user management

Correct Answer: ABC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 234

In order to obtain criminal evidence, it is necessary to master the technology of intrusion tracking. Which of the following options is correct for the description of tracking technology? (Multiple choices)

- A. The packet recording technology inserts the trace data in the traced IP data packet, so as to mark the packet on each router that has been talked about.
- B. Link detection technology determines the source of the attack by testing the network connection between routers
- C. Packet marking technology records the packets on the router and then uses data drilling techniques to extract the source of the attack
- D. Shallow email behavior analysis can realize information such as sending IP address, sending time, sending frequency, number of recipients, shallow email header Analysis

Correct Answer: ABD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 235

When a user uses session authentication to trigger the built-in Portal authentication of the firewall, the user does not actively perform identity authentication, advanced service access, Device pushes "redirect" to authentication page

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 236

For the description of the intrusion detection system, which of the following is wrong ?.

- A. Intrusion detection system can dynamically collect a large amount of key information through the network and computer, and can analyze and judge the entire system environment in time.
- Current status
- B. Once the intrusion detection system finds that it violates the security policy or the system has traces of being attacked, it can implement blocking operations.
- C. Intrusion detection system includes all software and hardware systems used for intrusion detection
- D. The immersion detection system can be linked with firewalls and switches to become a powerful "assistant" for firewalls, to better and more accurately control inter-domain traffic

Volume visit

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 237

Which of the following options are encapsulation modes supported by IPSec VPN? (Multiple choices)

- A. AH mode
- B. Tunnel mode
- C. Transmission mode
- D. ESP mode

Correct Answer: BC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 238

Tunnel addresses at both ends of the GRE tunnel can be configured as addresses on different network segments

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation**Explanation / Reference:****QUESTION 239**

Regarding the description of the packet during the iptables transmission, which of the following options is wrong?

- A. When a data packet enters the network card, it first matches the PREROUTING chain
- B. If the destination address of the packet is local, the system will send the packet to the INPUT chain.
- C. If the destination address of the packet is not local, the system sends the packet to the OUTPUT chain
- D. If the destination address of the data packet is not the local machine, the system sends the data packet to the FORWARD chain.

Correct Answer: C

Section: (none)

Explanation**Explanation / Reference:****QUESTION 240**

Regarding the description of the operating system, which of the following is wrong?

- A. The operating system is the interface between the user and the computer
- B. The operating system is responsible for managing all hardware resources of the computer system and controlling the execution of software.
- C. The interface between the operating system and the user is a graphical interface
- D. The operating system itself is software

Correct Answer: C

Section: (none)

Explanation**Explanation / Reference:****QUESTION 241**

Which of the following is not a requirement for dual-system hot backup of the firewall?

- A. The firewall hardware model is the same
- B. The firewall software version is the same
- C. The type and number of the interfaces used are the same
- D. The firewall interface IP address is the same

Correct Answer: D

Section: (none)

Explanation**Explanation / Reference:****QUESTION 242**

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

- A. Server-map is processed after state detection
- B. Source NAT policy query is processed after session creation
- C. Source NAT policy is processed after security policy matches
- D. Server-map processing before security policy matching

Correct Answer: ACD

Section: (none)

Explanation**Explanation / Reference:****QUESTION 243**

Which of the following options are required for a dual-system hot backup scenario?
(Multiple choice)

- A. hrp enable
- B. hrp mirror session enable
- C. hrp interface interface-type interface-number
- D. hrp preempt [delay interval]

Correct Answer: AC

Section: (none)

Explanation**Explanation / Reference:**

QUESTION 244

Manual audit is a supplement to tool evaluation. It does not need to install any software on the target system being evaluated.

Operation and status have no effect. Which of the following options is not included in the manual audit?

- A. Manual detection of the host operating system
- B. Manual inspection of the database
- C. Manual inspection of network equipment
- D. Manual inspection of the process of the administrator operating the equipment

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 245

Which of the following options belong to the default security zone of Huawei Firewall? (Multiple choices)

- A. Zone
- B. Trust area
- C. Untrust Zone
- D. Security area

Correct Answer: BC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 246

What level of early warning corresponds to a major cyber security event?

- A. Red alert
- B. Orange warning
- C. Yellow warning
- D. Blue warning

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 247

Regarding the source of electronic evidence, which of the following is incorrect?

- A. Facsimile information, mobile phone recordings are electronic evidence related to communication technology.
- B. Movies and TV series are electronic evidence related to network technology.
- C. Database operation records, operating system logs are computer-related electronic evidence •
- D. Operating system, e-mail, chat records can be used as the source of electronic evidence

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 248

Regarding the sequence of call establishment processes in the L2TP corridor, which of the following descriptions is correct?

- 1. Establish L2TP tunnel
 - 2. Establish a PPP connection
 - 3. LNS authenticates users
 - 4. Users access intranet resources
 - 5. Establish L2TP Session
- A. 1-> 2-> 3-> 5-> 4
 - B. 1-> 5-> 3-> 2-> 4
 - C. 2-> 1-> 5-> 3-> 4
 - D. 2-> 3-> 1-> 5-> 4

Correct Answer: B

Section: (none)

Explanation
Explanation / Reference:

Page 70

QUESTION 249

The protocol field in the IP packet header identifies the protocol used by its upper layer. Which of the following field values indicates that the upper layer protocol is

UDP protocol?

- A. 6
- B. 17
- C. 11
- D. 18

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 250

Carry out regular inspections of network security systems and equipment, upgrade patches, and organize cyber security emergency response drills in accordance with management specifications.

Which part of the MPDRR network security mode does the above action belong to?

- A. Protection link
- B. Testing
- C. Response
- D. Management

Correct Answer: BC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 251

Information security level protection is the basic system of national information security protection work

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 252

Which of the following options is not the identity of an IPSec SA?

- A. SPI
- B. Destination address
- C. Source address
- D. Security protocols

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

Page 71

QUESTION 253

What is the difference between the pre-accident prevention strategy and the post-accident recovery strategy? (Multiple choices)

A. Prevention strategies focus on minimizing the possibility of accidents before the story begins. Recovery strategies focus on minimizing

Impact and loss

B. The role of pre-disaster prevention strategies does not include minimizing economic and reputational losses due to accidents

C. Recovery strategies to improve business high availability

D. Recovery strategies are part of the business continuity plan

Correct Answer: ACD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 254

During the administrator's upgrade of the USG firewall software version, which of the following operations are necessary? (Multiple choices)

- A. Upload firewall version software
- B. Restart the device
- C. Factory reset
- D. Specify the software version to be loaded at the next startup

Correct Answer: ABD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 255

If the company's structure changes in reality, the business continuity plan needs to be retested

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 256

HTTP packets are carried using UDP, while HTTPS protocol is based on TCP three-way handshake, so HTTPS is more secure and more recommended

Use HTTPS.

- A. Yes
- B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 257

Single sign-on for Internet users, users directly authenticate to the AD server, and the device does not interfere with the user authentication process. AD monitoring services require

Deployed on the USG to monitor the authentication information of the AD server

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 258

UDP port scanning refers to an attacker sending a zero-byte length UDP packet to a specific port on the target host. If the port is open,

An ICMP port reachable data message will be returned.

- A. Yes
- B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 259

Regarding the business continuity plan, what is the following statement correct? (Multiple choices)

- A. The business continuity plan does not require senior company involvement during the scoping phase
- B. BCP needs flexibility because it cannot predict all possible accidents

- C. The business continuity plan does not require senior company involvement before it is formally documented
- D. Not all security incidents must be reported to company executives

Correct Answer: BD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 260

When the USG series firewall hard disk is in place, which of the following logs can be viewed? (Multiple choices)

- A. Operation log
- B. Business logs
- C. Alarm information
- D. Threat log

Correct Answer: ABCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 261

Social engineering is a kind of psychological trapping through victim's psychological weakness, instinct reaction, curiosity, trust, greed, etc.

Harms such as deception and injury.

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 262

Apply for emergency response special funds and purchase emergency response software and hardware equipment in which stage of the network's full emergency response?

- A. Preparation stage
- B. Inhibition phase
- C. Response phase
- D. Recovery phase

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 263

Device sabotage attacks are generally not easy to cause information leakage, but usually cause network service interruption.

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 264

Regarding the description of online user and VPN access user authentication, which of the following is wrong?

A. Internet users and VPN access users share data, and user attribute checks (user status, account expiration time, etc.) are also correct.

VPN access takes effect

B. Local users or server authentication processes are basically the same for online users. Both use the authentication domain to authenticate users.

The same

C. After VPN users access the network, they can access the network resources of the corporate headquarters.

The firewall can control the accessible network resources based on user names

D. VPN access users will go online at the same time after being authenticated

Page 74

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 265

Which of the following descriptions of the patch is wrong?

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

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 266

Regarding the description of the Intrusion Prevention System (IPS), which of the following is incorrect?

- A. IDS equipment needs to cooperate with firewall to block intrusion
- B. IPS equipment cannot be bypassed in the network
- C. IPS devices can be connected at the network boundary and deployed online
- D. Once the IPS device detects the intrusion behavior, it can realize real-time blocking

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 267

Guan Zihua's routers and routers, which of the following statements are correct? (Multiple choices)

- A. Routers can implement some security functions, and some routers can implement more security functions by adding security cards
- B. The main function of the router is to forward data. When enterprises have security requirements, sometimes a firewall may be a more suitable choice.
- C. The switch has some security functions, and some switches can implement more security functions by adding security cards.
- D. Switches do not have security features

Correct Answer: ABC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 268

Which of the following options is not a log type for the windows operating system?

- A. Business logs
- B. Application logs
- C. Security logs

Page 75

D. System logs

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 269

After the network intrusion event, obtain the identity of the intrusion, the source of the attack and other information according to the plan, and block the intrusion behavior. The above actions

What links belong to the PDRR network security model? (Multiple choices)

- A. Protection link
- B. Testing

C. Response

D. Recovery

Correct Answer: BC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 270

Regarding scanning of vulnerabilities, which of the following is wrong?

A. The loopholes were previously unknown and discovered afterwards.

B. Vulnerabilities are generally patchable

C. Vulnerabilities are security risks that can expose computers to hacking

D. Vulnerabilities are avoidable

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 271

When the user is configured for single sign-on, the PC message mode is used. The authentication process includes the following steps:

1 The visitor PC executes the login script and sends the user login information to the AD monitor

2 The firewall extracts the correspondence between the user and the IP from the login information and adds it to the online user table

3 The AD monitor connects to the AD server to query login user information, and forwards the queried user information to the firewall

4 The visitor logs in to the AD domain. The AD server returns a login success message to the user and issues a login script.

Which of the following is correct?

A. 1-2-3-4

B. 4-1-3-2

C. 3-2-1-4

D. 1-4-3-2

Correct Answer: B

Section: (none)

Page 76

Explanation

Explanation / Reference:

QUESTION 272

The administrator wants to create a web configuration administrator, the device web access port number is 20000, and the administrator is an administrator level. Which of the following commands

Is it correct?

A.

B.

C.

D.

Page 77

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 273

Regarding the description of security policy actions and security profiles, which of the following options are correct? (Multiple choices)

A. Forbidden If the action of the security policy is "Forbidden", the device will discard this traffic and no further content security checks will be performed.

B. Security profiles can take effect without being applied to security policies whose actions are allowed

C. The security profile must be applied under a 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: AC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 274

Which of the following options are the same characteristics of windows system and LINUX system? (Multiple choices)

- A. Support for multitasking
- B. Support graphical interface operation
- C. Open source systems
- D. Support for multiple terminal platforms

Correct Answer: ABD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 275

During the NAT configuration process, in which of the following situations, the device generates a server-map entry? (Multiple choices)

- A. Automatically generate server-map entries when configuring source NAT
- B. After the NAT server is successfully configured, the device will automatically generate a Server-map entry.
- C. Server-map entries are generated when easy-ip is configured
- D. After NAT No-PAT is configured, the device will create a server-map table for the configured multi-channel protocol data flow.

Correct Answer: BD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 276

NAT technology can realize data security transmission by encrypting data.

A. Yes

B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 277

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

- 1 detection
- 2 reports
- 3 remission
- 4 summarize experience
- 5 fixes
- 6 recovery
- 7 responses

A. 1-3-2-7-5-6-4

B. 1-3-2-7-6-5-4

C. 1-2-3-7-6-5-4

D. 1-7-3-2-6-5-4

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 278

Which of the following statements about L2TP VPN is wrong?

- A. Applicable to employees on business trip dial-up access to the intranet
- B. Data will not be encrypted

- C. Can be used with IPsec VPN
- D. Belongs to Layer 3 VPN technology

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 279

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

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Page 79

Explanation / Reference:

QUESTION 280

ASPF (Application Specific Packet Filter) is a packet filtering technology based on the application layer. Implemented special security mechanisms. Which of the following statements about ASPF and server-map tables is correct? (Multiple choices)

- A. ASPF monitors messages during communication
- B. ASPF can create server-map dynamically
- C. ASPF dynamically allows multi-channel protocol data to pass through the server-map table
- D. The five-tuple server-map entry implements a similar function to the session table

Correct Answer: ABC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 281

The role of antivirus software and host firewall is the same.

- A. Yes
- B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 282

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

- A. Yes
- B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 283

Page 80

The command is executed on the firewall and the above information is displayed. Which of the following descriptions is correct? (Multiple choices)

- A. The status of this firewall VGMP group is Active
- B. The virtual IP address of this firewall G1 / 0/1 interface is 202.38.10.2
- C. The priority of the VRRP backup group whose firewall VRID is 1 is 100
- D. Will not switch when the master device USG_A fails

Correct Answer: ABC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 284

In the USG series firewall system view, after the reset saved-configuration command is executed, the device configuration is restored to the default configuration.

No further action is required to take effect.

A. Yes

B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 285

Which of the following is the difference between Network Address Port Translation (NAPT) and No Network Address Translation (No-PAT)?

A. After No-PAT conversion, for external users, all packets are from the same IP address

B. No-PAT only supports protocol port conversion at the transport layer

C. NAPT only supports protocol address translation at the network layer

D. No-PAT supports protocol address translation at the network layer

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 286

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

(Multiple choice)

A. Buffer overflow attack exploits the defect of the software system's memory operation and runs the attack code with high operation authority

B. Buffer overflow attacks have nothing to do with the vulnerability and architecture of the operating system

C. Buffer overflow attacks are one of the common ways to attack software systems

D. Buffer overflow attacks are application-level attacks

Correct Answer: ACD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 287

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

A. Emergency handling of security incidents

B. Early warning 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: (none)

Explanation

Explanation / Reference:

QUESTION 288

The host firewall is mainly used to protect the host from attacks and intrusions from the network.

A. Yes

B. wrong

Correct Answer: A

Section: (none)

Explanation

Explanation / Reference:

QUESTION 289

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

A. International Organization for Standardization (ISO)

B. International Electrotechnical Commission (IEC)

C. International Telecommunication Union (ITU)

D. Wi-Fi Alliance

Correct Answer: ABC

Section: (none)

Explanation

Explanation / Reference:

Page 82

QUESTION 290

In order to obtain criminal evidence, it is necessary to master the technology of intrusion tracking. Which of the following options is correct for the description of tracking technology? (Multiple choices)

A. The packet recording technology inserts trace data in the traced IP data packets, so Marking packets

B. Link test technology determines the source of the attack by testing the network link between routers

C. Packet marking technology records the packets on the router and then uses data drilling techniques to extract the source of the attack

D. Shallow email behavior analysis can realize sending IP address, sending time, sending frequency, number of recipients, shallow email header

Analysis of information.

Correct Answer: ABD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 291

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

A. User data

B. Recipient's public key

C. Sender public key

D. Digital fingerprint

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 292

On Huawei USG series firewalls, the default security policy cannot be modified.

A. Yes

B. wrong

Correct Answer: B

Section: (none)

Explanation

Explanation / Reference:

QUESTION 293

In the classification of the information security level protection system, which of the following levels defines if the information system is damaged, it will affect social order and society.

Damage to the public interest? (Multiple choices)

A. First level

User autonomous protection level

B. Second level

System audit protection level

C. Third level

Security mark protection

D. Level 4

Structured protection

Page 83

Correct Answer: ABCD

Section: (none)

Explanation

Explanation / Reference:

QUESTION 294

In the Huawei SDSec solution, which of the following is an analysis layer device?

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

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 295

Regarding the control action permit and deny of the firewall inter-domain forwarding security policy, which of the following options are correct? (Multiple choices)

- A. The action of the firewall's default security policy is deny
- B. Packets are discarded immediately after the deny action of the inter-domain security policy is matched, and other inter-domain security policies will not continue to be executed.
- C. Even if the packet matches the permit action of the security policy, it may not be forwarded by the firewall
- D. Whether the packet matches the permit action or deny action of the security policy, it will be transferred to the UTM module for processing.

Correct Answer: ABC

Section: (none)

Explanation

Explanation / Reference:

QUESTION 296

Which of the following is not included in a business impact analysis (BIA)?

- A. Business priorities
- B. Incident handling priorities
- C. Impact assessment
- D. Risk identification

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 297

When deploying IPSec VPN, which of the following is the main application scenario of tunnel mode?

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

Correct Answer: C

Section: (none)

Explanation

Explanation / Reference:

QUESTION 298

Huawei Redundancy Protocol (HRP) protocol is used to synchronize key firewall configuration and connection status data to the standby firewall

, Which of the following options is not in the scope of synchronization?

- A. Security policy
- B. NAT policy
- C. Blacklist
- D. IPS Signature Set

Correct Answer: D

Section: (none)

Explanation

Explanation / Reference:

QUESTION 299

Regarding the business continuity plan, what is the following statement correct? (Multiple choices)

- A. The business continuity plan does not require senior company involvement during the scoping phase
- B. Thought that it is impossible to predict all possible accidents, so BCP needs to be flexible
- C. The business continuity plan does not require senior company involvement before it is formally documented
- D. Not all security incidents must be reported to company executives

Correct Answer:

Section: (none)

Explanation

Explanation / Reference: