HCIA SECURITY

1. Which of the following is the correct description of windows log event type? (Multiple Choice)
   A. A warning event is a successful operation event of an application, driver, or service.
   B. Error events usually refer to the loss of function and data. For example, if a service cannot be loaded as a system boot, an error event will be generated.
   C. When the disk space is insufficient, it will be recorded as an "information event"
   D. Failure audit event refers to a failed audit security login attempt, such as a failure when the user views accesses the network drive is logged as a failed audit event.

Answer: BCD

2. Which types of encryption technology can be divided into? (Multiple Choice)
   A. Symmetric encryption (Right Answers)
   B. Asymmetric encryption (Right Answers)
   C. Fingerprint encryption
   D. Data encryption

Answer: AB

3. HRP (Huawei Redundancy Protocol) Protocol to back up the connection state of data include: (Multiple Choice)
   A. TCP/UDP sessions table
   B. Ser/er Map table
   C. **the dynamic blacklist**
   D. the routing table

Answer: ABC

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

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

Answer: A

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

A. Relevance criterion means that if the electronic evidence can have a substantial impact on the facts of the case to s certain extent, the court should determine that it is relevant. (Right Answers)
B. Objective standard means that the acquisition, storage, and submission of electronic evidence should be legal, and the basic rights such as national interests, social welfare, and personal privacy are not strictly violated
C. Legality standard is to ensure that the electronic evidence is collected from the initial collection, and there is no change in the content of the evidence submitted as evidence.
D. Fairness standard refers to the evidence obtained by the legal subject through egal means, which has the evidence ability.

Answer: A

Data analysis technology is to find and -natch keywords or key ohrases in the acquired data stream or information flow, and analyze: he correlation of time. Which of the following is not an evidence analysis technique?

A. Password deciphering, data decryption technology
B. Document Digital Abstract Analysis Technology
C. Techniques for discovering the connections between different evidences
D. Spam tracking technology (Right Answers)

Answer: D

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

A. AH can provide encryption and verification functions
B. ESP can provide encryption and verification functions (Right Answers)
C. The agreement number of AH is 51. (Right Answers)
D. The agreement number of ESP is 51.

Answer: BC

Which of the following types of attacks does the DDoS attack belong to?

A. Snooping scanning attack
B. Malformed packet attack
C. Special message attack
D. Traffic attack (Right Answers) **Answer: D**

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

A. SSL VPN technology can be perfectly applied to NAT traversal scenarios
B. SSL VPN technology encryption only takes effect on the application layer
C. SSL VPN requires a dial-up client (Right Answers)
D. SSL VPN technology extends the network scope of the enterprise

Answer: C

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

A. Restore defaults (Right Answers)
B. Change notification rules (Right Answers)
C. Set connection security rules (Right Answers)
D. Set out inbound rules (Right Answers)

Answer: ABCD

When configuring NAT Server on the LSG series firewall, the server-map table will be generated. Which of the following does not belong in the table?

A. Destination IP
B. Destination port
C. Agreement number
D. Source IP (Right Answers)

Answer: D

Which of the following attacks does not belong to special packet attack?

A. ICMP redirect packet attack
B. ICMP unreachable packet attack
C. IP address scanning attack (Right Answers)
D. Large ICMP packet attack

Answer: C

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

A. Teardrop attack
B. Smurf attack
C. TCP fragment attack
D. ICMP unreachable packet attack (Right Answers)

Answer: D

Caesar Code is primarily used to encrypt data by using a stick of a specific specification

A. True
B. False (Right Answers)

Answer: B

Typical remote authentication modes are: (Multiple Choice)

A. RADIUS (Right Answers)
B. Local
C. HWTACACS (Right Answers)
D. LDP

Answer: AC

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

A. The administrator can advertise the content log to view the detection and defense records of network threats.
B. The administrator can use the threat log to understand the user's security risk behavior and the reason for being alarmed or blocked.
C. The administrator knows the user's behavior, the keywords explored, and the effectiveness of the audit policy configuration through the user activity log.
D. The administrator can learn the security policy of the traffic hit through the policy hit log. And use it for fault location when the problem occurs. (Right Answers)

Answer: D

17. In the Client-Initiated VPN configuration, generally it is recommended to plan the address pool and the headquarters or need to of the network address for the different network or need to open proxy forwarding on the gateway device

A. True (Right Answers)
B. False

Answer: A

18. Which of the following is the encryption technology used by digital envelopes?

A. Symmetric encryption algorithm
B. **Asymmetric encryption algorithm (Right Answers)**

Answer: B

19. Except built-in Portal authentication, firewall also supports custom Portal authentication, when using a custom Portal authentication, no need to deploy a separate external Portal sever.

A. True
B. False (Right Answers)

Answer: B

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

A. True (Right Answers)
B. False

Answer: A

21. IPSec VPN technology does not support NAT traversal when encapsulating with ESP security protocol, because ESP encrypts the packet header

A. True
B. False (Right Answers)

Answer: B

22. Which of the following is true about the description of SSL VPN?

A. Can be used without a client (Right Answers)
B. May encrypt to IP layer
C. There is a NAT traversal problem
D. No authentication required

Answer: A

23. Some applications, such as Oracle database application, there is no data transfer for a long time, so that firewall session connection is interrupted, thus resulting in service interruption, which of the following technology can solve this problem?

A. Configure a long business connection (Right Answers)
B. Configure default session aging time
C. Optimization of packet filtering rules
D. Turn fragment cache

Answer: A

24. What is the nature cf information security in "Implementation of security monitoring and management of information and information systems to prevent the illegal use of information and information systems"?

A. Confidentiality
B. Controllability (Right Answers)
C. Non-repudiation
D. Integrity

Answer: B

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

A. True (Right Answers)
B. False

Answer: A

26. Which of the following options is not the part of the quintet?

Source IP

Source MAC (Right Answers)

Destination IP

Destination Port

Answer: B

27. Which of the following statement about the L2TP VPN of Client-initialized is wrong?

A. After the remote user access to internet, can initiate L2TP tunneling request to the remote LNS directly through the client software
B. LNS device receives user L2TPconnection request, can verify based on user name and password.
C. LNS assign a private IP address for remote users
D. remote users do not need to install VPN client software (Right Answers)

Answer: D

28. Regarding the description of the vulnerability scanning, which of the following is wrong?

A. Vulnerability scanning is a technology based on network remote monitoring of target network or host security performance vulnerability, which can be used for simulated attack experiments and security audits.
B. Vulnerability scanning is used to detect whether there is a vulnerability in the target host system. Generally, the target host is scanned for specific vulnerabilities.
C. Vulnerability scanning is a passive preventive measure that can effectively avoid hacker attacks. (Right Answers)
D. Vulnerability scanning can be done based on the results of ping scan results and port scan

Answer: C

29. Regarding the firewall security policy, which of the following options is wrong?

A. If the security policy is permit, the discarded message will not accumulate the number of hits. (Right Answers)
B. When configuring the security policy name, you cannot reuse the same name
C. Adjust the order of security policies with immediate effect, no need to save the configuration file.
D. H D. Huawei's USG series firewalls cannot have more than 128 security policy entries.

Answer: A

30. Which of the following protection levels are included in the TCSEC standard? (Multiple Choice)

A. Verify protection level (Right Answers)
B. Forced protection level (Right Answers)
C. **Independent protection level (Right Answers)**
D. Passive protection level

Answer: ABC

31. Which of the following are parts of the PKI architecture? (Multiple Choice)

A. End entity (Right Answers)
B. Certification Authority (Right Answers)
C. Certificate Registration Authority (Right Answers)
D. **Certificate Storage organization (Right Answers)**

Answer: ABCD

32. ‘Being good at observation’ and 'keeping suspicion’ can help us better identify security threats in the online world

A. True (Right Answers)
B. False

Answer: A

33. Under the 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 using the new IP header to find the routing table.

A. True
B. False (RightAnswers)

Answer: B

34. Regarding the description of Windows Firewall, which of the following options are correct? (Multiple Choice)

A. Windows Firewall can only allow or prohibit preset programs or functions and programs installed on the system, and cannot customize the release rules according to the protocol or port number.
B. Windows Firewall not only allows or prohibits preset programs or functions and programs installed on the system, but also can customize the release rules according to the protocol or port number. (Right Answers)
C. If you are unable to access the Internet during the process of setting up the Windows Firewall, you can use the Restore Defaults feature to quickly restore the firewall to its initial state. (Right Answers)
D. Windows Firewall can also change notification rules when it is off. (Right Answers)

Answer: BCD

35. Which of the following is the correct description of the investigation and evidence collection?

A. Evidence is not necessarily required during the investigation
B. Evidence obtained by eavesdropping is also valid
C. In the process of all investigation and evidence collection, there are law enforcement agencies involved. (Right Answers)
D. Document evidence is required in computer crime

Answer: C

36. Which of the following is wrong about the management of Internet users?

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

Answer: B

37. Which of the following is not part of the method used in the Detection section of the P2DR model?

A. Real-time monitoring
B. Testing
C. Alarm (Right Answers)
D. Shut down the service

Answer: C

38. Which of the following is not part of the LINUX operating system?

A. CentOS
B. RedHat
C. Ubuntu
D. MAC OS (Right Answers)

Answer: D

In some scenarios, it is necessary to convert the source IP address and the destination IP address. Which of the following techniques is used in the scenario?

Two-way NAT (Right Answers)

Source NAT

NAT-Server

NAT ALG

Answer: A

40. Which of the following protocols can guarantee the confidentiality of data transmission? (Multiple Choice)

A. Telnet
B. SSH (Right Answers)
C. FTP
D. HTTPS (Right Answers)

Answer: BD

41. On the USG series firewall, after the web redirection function is configured, 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 the authentication policy is incorrectly configured
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 of service of authentication page is set to 8887 (Right Answers)

Answer: D

42. Which ofthe following options is the correct sequence ofthe four phases ofthe Information Security Management System (ISMS)?

A. Plan->Check->Do->Action
B. Check->Plan->Do->Action
C. **Plan->Do->Check->Action (Right Answers)**
D. Plan->Check->Action->Do

Answer: C

43. In the information security system construction management cycle, which of the following actions is required to be implemented in the "check' link?

A. Safety management system design
B. Implementation of the safety management system
C. **Risk assessment (Right Answers)**
D. Safety management system operation monitoring

Answer: C

44. Check the firewall HRP status information as follows:

HRP_S [USG_ B] display hrp state 16:90: 13 2010/11/29 The firewall's config state is : SLAVE

Current state of virtual routers configured as slave GigabitEthernet0/0/0 vird 1 : slave

GigabitEthernet0/0/1 vied 2 : slave Which of the following description is correct?

A. The firewall VGMP group status is Master
B. **The firewall G0/0/0 and 0/1 GO / interface of VRRP group status is Slave (Right Answers)**
C. The firewall of HRP heartbeats interface is G0/0/0 and G0/0/1
D. The firewall must be in a state of preemption

Answer: B

45. Classify servers based on the shape, what types of the following can be divided into? (Multiple choice)

A. Blade sen/er (Right Answers)
B. Tower server (Right Answers)
C. Rack server (Right Answers)
D. X86 server

Answer: ABC

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

A. **True (Right Answers)**
B. False

Answer: A

47. According to the protection object, the firewall is divided. Windows Firewall belongs to

A. Software firewall
B. Hardware firewall
C. Stand-alone firewall (Right Answers)
D. Network firewall

Answer: C

48. Which of the following are the ways in which a PKI entity applies for a local certificate from CA? (Multiple Choice)

A. **Online application (Right Answers)**
B. Local application
C. Network application
D. Offline application (Right Answers)

Answer: AD

49. IPS (Intrusion Prevention System) is a defense system that can block in real time when intrusion is discovered

True (RightAnswers)

False

Answer: A

50. The Huawei Redundancy Protocol (HRP) is used to synchronize the main firewall configuration and connection status and other data on the backup firewall to synchronize . Which of the following options is not in the scope of synchronization?

A. Security policy
B. NAT policy
C. Blacklist
D. IPS signature set (Right Answers) **Answer: D**

51. Which of the following are correct about configuring the firewall security zone? (Multiple Choice)

A. The firewall has four security zones by default, and the four security zone priorities do not support modification. (Right Answers)
B. Firewall can have 12 security zones at most.
C. The firewall can create two security zones of the same priority
D. When data flows between different security zones, the device security check is triggered and the corresponding security policy is implemented Answer: AD

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

A. True (RightAnswers)
B. False

Answer: A

53. Which of the following descriptions is wrong about the root CA certificate?

The issuer is CA

The certificate subject name is CA.

Public key information is the public key ofthe CA

Signature is generated by CA public key encryption (Right Answers)

Answer: D

54. Which configuration is correct to implement NAT ALG function?

A. nat alg protocol
B. alg protocol
C. nat protocol
D. detect protocol (Right Answers)

Answer: D

55. Which of the following statements is wrong about the firewall gateway's anti-virus response to the HTTP protocol?

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 (Right Answers)
C. Alarm mode device only generates logs and sends them out without processing the files transmitted by the HTTP protocol.
D. Blocking means that the device disconnects from the HTTP server and blocks file transfer.

Answer: B

56. Which ofthe following does not belong to the user authentication method in the USG firewall?

Free certification

Password authentication

Single sign-on

Fingerprint authentication (Right Answers)

Answer: D

57. Both the GE1/0/1 and GE1/0/2 ports of the firewall belong to the DMZ. If the area connected to GE1/0/1 can access the area connected to GE1/0/2, which of the following is correct?

A. Need to configure the security policy from Local to DMZ
B. **No need to do any configuration (Right Answers)**
C. Need to configure an interzone security policy
D. Need to configure security policy from DMZ to local

Answer: B

58. For the process of forwarding the first packet of the session between firewall domains, there are the following steps:

1. find the routing table

2. find inter-domain packet filtering rules

3. find the session table

4. find the blacklist

Which of the following is the correct order?

A. 1->3->2->4
B. 3->2->1->4
C. 3->4->1->2 (Right Answers)
D. 4->3->1->2

Answer: C

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

A. Clear firewall session table
B. Reset firewall session table (Right Answers)
C. Display firewall session table
D. Display session table

Answer: B

60. Which of the following are the basic functions of anti-virus software? (Multiple Choice)

A. Defend virus (Right Answers)
B. Find virus (Right Answers)
C. Clear virus (Right Answers)
D. Copy virus

Answer: ABC

61 The European TCSEC Code is divided into two modules, Function and Evaluation, which are mainly used in the miitary, government and commercial fields

A. True (Right Answers)
B. False

Answer: A

62. Terminal detection is an important part of the future development of information security. Which of the following methods belong to the category of terminal detection? (Multiple Choice)

A. Install host antivirus software (Right Answers)
B. Monitor and remember the external device
C. Prevent users from accessing public network search engines
D. Monitor the host registry modification record (Right Answers)

Answer: AD

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

A. Iptables -t filter -A INPUT -s 172.16.0.0/16 -p all -j DROP (Right Answers)
B. Iptables -t filter -P INPUT -s 172.16.0.0/16 -p all -j DROP
C. Iptables -t filter -P INPUT -s 172.1G.0.0/1G -p all -j ACCEPT
D. iptables -t filter -P INPUT -d 172.16.0.0/16 -p all -j ACCEPT

Answer: A

64. About the contents of HRP standby configuration consistency check, which of the following is not included?

A. NAT policy
B. If the heartbeat interface with the same serial number configured
C. Next hop and outbound interface of static route (Right Answers)
D. Certification strategy

Answer: C

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

A. Port mapping (Right Answers)
B. MAC and IP address binding
C. Packet filtering
D. Long connection **Answer: A**

66. Which of the following is not included in the design principles of the questionnaire?

A. Integrity
B. Openness
C. Specificity
D. Consistency (Right Answers)

Answer: D

67. To implement the " anti-virus function " in the security policy, you must perform a License activation

A. **True (Right Answers)**
B. False

Answer: A

68. The configuration commands for the NAT address pool are as follows: nat address-group 1

section 0 202.202.168.10 202.202.168.20 mode no-pat Of which, the meaning of no-pat parameters is:

A. Do not do address translation
B. Perform port multiplexing
C. Do not convert the source port (Right Answers)
D. Do not convert the destination port

Answer: C

69. On the surface, threats such as viruses, vulnerabilities, and Trojans are the cause of information security incidents, but at the root of it, information security incidents are also strongly related to people and information systems themselves.

A. True (Right Answers)
B. False

Answer: A

70. Which of the following behaviors is relatively safer when connecting to Wi-Fi in public places?

A. Connect Wi-Fi hotspots that are not encrypted
B. Connect to the paid Wi-Fi hotspot provided by the operator and only browse the web (Right Answers)
C. Connect unencrypted free Wi-Fi for online shopping
D. Connect encrypted free Wi-Fi for online transfer operations **Answer: B**

71. Which of the following is an action to be t3ken during the summary phase of the cyber security emergency response? (Multiple Choice)

A. Establish a defense system and specify control measures
B. Evaluate the implementation of the contingency plan and propose a follow-up improvement plan (Right Answers)
C. Determine the effectiveness nf the isnhtinn measures
D. Evaluation of members of the emergency response organization (Right Answers)

Answer: BD

72. Which of the following descriptions is correct about port mirroring? (Multiple Choice)

A. The mirrored port copies the packet to the observing port. (Right Answers)
B. **The observing port sends the "eceived packet to the monitoring device. (Right Answers)**
C. The mirrored port sends the received packet to the monitoring device.
D. The observing port copies the packet to the mirrored port.

Answer: AB

73. Which of the following is the GRE protocol number?

A. 46
B. 47 (Right Answers)
C. 89
D. 50

Answer: B

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

A. VGMP add multiple VRRP backup groups on the same firewall to a management group, uniformly manage all the VRRP group by management group.
B. VGMP ensure that all VRRP backup groups state are the same through a unified control of the switching of each VRRP backup group state
C. State of VGMP group is active, which will periodically send HELLO packets to the opposite end. Stdandby end only monitors the HELLO packets, which will not respond (Right Answers)
D. By default, when three HELLO packet cycle of Standby end does not receive HELLO packets which are sent from the opposite end, the opposite end will be considered a failure, which will switch itself to the Active state

Answer: C

75. Both A and B communicate data. If an asymmetric encryption algorithm is used for encryption, when A sends data to B. which of the following keys will be used for data encryption?

A. A public key
B. A private key
C. **public key (Right Answers)**
D. B private key

Answer: C

76. IPSec VPN uses an asymmetric encryption algorithm to encrypt the transmitted data

True

False (RightAnswers)

Answer: B

77. Based on the GRE encapsulation and de-encapsulation, which description is error?

A. Encapsulation Process: The original data packets transmit the data packets through looking up routing to the Tunnel interface to trigger GRE encapsulation.
B. Encapsulation Process: After GRE module packaging, the data packet will enter the IP module for further processing
C. De-encapsulation Process: After the destination receives GRE packets, transmitting the data packets through looking up the routing to the Tunnel interfaces to trigger GRE encapsulation. (Right Answers)
D. De-encapsulation Process: After GRE module de-encapsulation, the data packets will enter the IP module for further processing.

Answer: C

78. The repair of anti-virus software only needs to be able to repair some system files that were accidentally deleted when killing the virus to prevent the system from crashing

A. True (Right Answers)
B. False

Answer: A

79. Which of the following is not a rating in the network security incident?

A. Major network security incidents
B. Special network security incidents (Right Answers)
C. General network security incidents **Answer: B**

80. In the current network it has deployed other authentication system, device registration function by enabling a single point, reducing the user to re-enter the password. What are correct about single sign-on statements? (Multiple choice)

A. Device can identify the user through the authentication of the identity authentication system, user access, the device will not pis authentication pages, to avoid further asked to enter a username / password (Right Answers)

B. AD domain single sign-on is only one depbyment model

C. Although not require to enter a user password, but the authentication server needs to interact with the user password and devices used to ensure that certification through discussion

D. AD domain single sign-on login can be minored data stream synchronized manner to the firewall (Right Answers)

Answer: AD

81. Regarding the relationship and role of VRRP/VGMP/HRP, which of the following statements are correct? (Multiple choice)

VRRP is responsible for sending free ARP to direct traffic to the new primary device during active/standby switchover (RightAnswers)

VGMP is responsible for monitoring equipment failures and controlling fast switching of equipment. (Right Answers)

HRP is responsible for data backup during hot standby operation (Right Answers)

VGMP group in the active state may include the VRRP group in the standby state.

Answer: ABC

82. The administrator PC and the USG firewall management interface directly connected using the web the way initialization. Which nether following statements are true? (Multiple choice)

Manage PC browser access http://192.168.0.1 (Right Answers)

IP address ofthe management PC is manually set to 192.168.0.2-'92.168.0.254 (Right Answers) r C. Manage PC browser access http://192.168.1.1

Set the NIC ofthe management PC to automatically obtain the IP address.

Answer: AB

83. In Huawei SDSec solution, which layer of equipment does the firewall belong to?

A. Analysis layer
B. Control layer
C. Executive layer (Right Answers)
D. Monitoring layer

Answer: C

84. When Firewall does dual-system hot backup networking, in order to achieve the overall status of the backup group switching, which of the following protocol technology need to be used?

VRRP

VGMP (Right Answers)

HRP

OSPF

Answer: B

85. The scene of internal users access the internet as shown, the subscriber line processes are:

1. After authentication, USG allow the connection

2. The user input http://1.1.1.1 to access Internet

3. USG push authentication interface. User =? Password =?

4. The user successfully accessed http://1.1.1.1, equipment create Session table.

5. User input User = Password = *** which the following procedure is correct?

A. 2-5-3-1-4
B. 2-3-5-1-4 (RightAnswers)
C. 2-1-3-5-4
D. 2-3-1-5-4 **Answer: B**

86. About the description of firewall active-standby, which of the following is correct? (Multiple Choice)

A. When a plurality of regions on the firewall needs to provide dual-machine backup function, you need to configure multiple VRRP backup groups on the firewall. (Right Answers)
B. It requires the state of all the VRRP backup groups in the same VGMP management group on the same firewall should be consistent. (Right Answers)
C. The firewall active-standby requires the information such as the session table. MAC table, routing table and so on synchronous backup between primary devices and slave devices.
D. VGMP is to ensure all VRRP backup groups' consistency of switching (Right Answers)

Answer: ABD

87. Which ofjhe following is the encryption technology used in digital envelopes?

A. Symmetric encryption algorithm
B. Asymmetric encryption algorithm (Right Answers)
C. Hash algorithm
D. Streaming algorithm

Answer: B

88. Which of the following are correct regarding the matching conditions of the security policy? (Multiple choice)

A. 'The source security zone' is an optional parameter in the matehing condition. (Right Answers)
B. "Time period" in the matching condition is an optional parameter (Right Answers)
C. "Apply" in the matching condition is an optional parameter (Right Answers)
D. "Service" is an optional parameter in the matching condition (Right Answers)

Answer: ABCD

89. The attacker by sending ICMP response request, and will request packet destination address set to suffer Internet radio address. Which kind of attack does this behavior belong to9

A. IP spoofing attack
B. Smurf attack (Right Answers)
C. ICMP redirect attack
D. SYN flood attack **Answer: B**

91. Fire Trust domain FTP client wants to access an Um.rust server FTP service has allowed the client: to access the server TCP 21 port, the client in the Windows command line window can log into the FTP server, but can not download the file, what are the following solutions? (Multiple choice)

- **A. Take the Trust between Un:rust domain to allow two-way default access strategy (Right Answers)**
- **B. The ^TP works with the port mode modify the Untru3t Trust domain to allow the inbound direction between the default access strategy (Right Answers)**
- **C. Trust Untrust domain configuration is enabled detect ftp (Right Answers)**
- D. FTP works with Passive mode modify the domain inbound direction betv/een the Untrust Trust default access policy to allow

Answer: ABC

92. Which of the following is not part of a digital certificate?

- A. Public key
- **B. Private key (Right Answers)**
- C. Validity period
- D. Issuer

Answer: B

93. Which of the following is true about the description of the TCP/IP protocol stack packet encapsulation? (Multiple choice)

- **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 according to the parsing information, such as IP. (Right Answers)**
- B. After the transport layer (TCP) receives the data packet, the transport layer information is stripped after parsing, and the upper layer processing protocol, such as UDP, is known according to the parsing information
- C. After receiving the data packet, the network layer is stripped after parsing, and the upper layer processing protocol is known according to 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 displayed at the end is exactly the same as the data sent by the sender host. (Right Answers)**

Answer: AD

94. Which of the following is not a key technology for anti-virus software?

A. Shelling technology
B. Self-protection
C. Format the disk (Right Answers)
D. Real-time upgrade ofthe virus database

Answer: C

95. Which of the following are malicious programs? (Multiple choice)

A. Trojan horse (Right Answers)
B. Vulnerabilities
C. F C. worm (Right Answers)
D. F D. Virus (Right Answers)

Answer: ACD

96. Which of the following are key elements of information security prevention? (Multiple choice)

A. Asset management (Right Answers)
B. Security operation and management (Right Answers)
C. Security products and technologies (Right Answers)
D. Personnel (RightAnswers)

Answer: ABCD

97. Which of the following is not the main form of computer crime?

A. Implant a Trojan to the target host
B. Hacking the target host
C. Using a computer for personal surveys (Right Answers)
D. Use scanning tools to collect network information without permission

Answer: C

98. When the IPSec VPN tunnel mode is deployed, the AH protocol is used for packet encapsulation. In the new IP packet header field, which of the following parameters does not require data integrity check?

A. Source IP address
B. Destination IP address
C. TTL (Right Answers)
D. Idetification **Answer: C**

99. When configuring a GRE tunnel interface, the destination address generally refers to which of the following parameters?

Local tunnel interface IP address

Local end network export IP address

Peer external network export IP address (Right Answers)

IP address of the peer tunnel interface

Answer: C

100. In IPSEC VPN. Which of the following scenarios can be applied by tunnel mode?

A. between the host and the host
B. between hosts and security gateways
C. between security gateways (Right Answers)
D. Between tunnel mode and transport mode

Answer: C

1O1. Security policy conditions can be divided into multiple fields, such as source address, destination address, source port, destination port, etc. These fields are "and " , that is, only information in the message and all fields If you match, you can hit this strategy

A. True
B. False (RightAnswers)

Answer: B

102. Which cf the following is correct about the description of SSL VPN?

Can be used without a client (Right Answers)

may IP encrypt layer

There is a NAT traversal problem

No authentication required

Answer: A

103. Which description about disconnect the TCP connection 4 times-handshake is wrong?

A. initiative to shut down the sender first FIN active closed, while the other received this FIN perform passive shut down
B. when passive close receipt the first FIN. it will send back an ACK, and randomly generated to confirm the serial number (Right Answers)
C. passive closing party end need to send a file to the application, the application will close it connection and lead to send a FIN
D. in passive close the sender after the FIN. initiative to close must send back a confirmation, and will confirm the serial number is set to receive serial number 1

Answer: B

104. Which of the following is non-symmetric encryption algorithm?

A. RC4
B. 3DES
C. AES
D. DH (Right Answers)

Answer: D

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

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

Answer: AB

106. Regarding the firewall security policy, which of the following options are wrong?

A. If the security policy is permit, the discarded message will not accumulate the number of hits. (Right Answers)
B. When configuring the security policy name, you cannot reuse the same name.
C. Adjust the order of security policies without saving the configuration file.
D. The number of security policy entries of Huawei USG series firewalls cannot exceed 128.

Answer: A

107. Which of the following options are suppoied by VPN technology to encrypt data messages? (Multiple choice)

A. SSL VPN (Right Answers)
B. GRE VPN
C. IPSec VPN (Right Answers)
D. L2TP VPN

Answer: AC

108. Which ofthe following is the username / password for the first login ofthe USG series firewall?

Username admin, password Admin@123 (Right Answers)

User name admin, password admin@123

User name admin, password admin

User name admin, password Admin123

Answer: A

109. There ere various security threats in the use of the server. Which of the following options is not a server security threat?

A. Natural disasters (Right Answers)
B. DDos attack
C. Hacking
D. Malicious programs

Answer: A

110. Which of the following statement about the L2TP VPN of Clieit-initialized is wrong?

A. After the remote user access to internet, can initiate L2TP tunneling request to the remote LNS directly through the client software
B. LNS device receives user L2TPconnection request, can verify based on user name and password.
C. LNS assign a private IP address for remote users
D. remote users do not need to install VPN client software (Right Answers)

Answer: D

111. Which of the following options does not include the respondents in the questionnaire for safety assessment?

A. Network System Administrator
B. Security administrator
C. HR (Right Answers)
D. Technical leader

Answer: C

112. The vulnerability that has not been discovered is the 0 day vulnerability

A. True
B. False (Right Answers)

Answer: B

113. Regarding the problem that the two-way binding user of the authentication-free method cannot access the network resources, which of the following options are possible reasons? (Multiple choice)

A. The authentication-free user and the authenticated user are in the same security zone
B. The authentication-free user does not use the PC with the specified IP/MAC address. (Right Answers)
C. The authentication action in the authentication policy is se- to "No credit / free authentication"
D. Online users have reached a large value (Right Answers)

Answer: BD

114. ASPF (Application Specific Packet Filter) is a kind of packet filtering based on the application layer, it checks the application layer protocol information and monitor the connection state of the application layer protocol. ASPF by Server Map table achieves a special security mechanism. Which statement about ASPF and Server map table are correct? (Multiple choice)

A. ASPF monitors the packets in the process of communication (Right Answers)
B. ASPF dynamically create and delete filtering rules (Right Answers)
C. ASPF through server map table realize dynamic to allow multi-channel protocol data to pass (Right Answers)
D. Quintuple server-map entries achieve a similar functionality with session table

Answer: ABC

115. What are the advantages of address translation techniques included? (Multiple choice)

A. Address conversion can make internal network users (private IP address) easy access to the Internet (Right Answers)
B. Many host address conversion can make the internal LAN to share an IP address on the Internet (Right Answers)
C. Address conversion that can handle the IP header of encryption
D. Address conversion can block internal network users, improve the safety of internal network (Right Answers)

Answer: ABD

116. Which of the following statement about :he NAT is wrong?

A. NAT technology can effectively hide the hosts of the LAN. it is an effective network security protection technology
B. Address Translation can follow the needs of users, providing FTP. WWW, Telnet and other services outside the LAN
C. Some application layer protocols earn/ IP address information in the data, but also modify the P address information in the data of the upper layer when they are as NAT
D. For some non-TCP. UDP protocols (such as ICMP. PPTP), unable to do the NAT translation (Right Answers)

Answer: D

117. Regarding the relationship and role of VRRPA/GMP/HRP. which of the following statements are correct? (Multiple choice)

A. VRRP is responsible for sending free ARP to direct traffic to the new primary device during active/standby switchover. (Right Answers)
B. VGMP is responsible for monitoring equipment failures and controlling fast switching of equipment. (Right Answers)
C. **HRP is responsible for data backup during hot standby operation (Right Answers)**
D. VGMP group in the active state may include the VRRP group in the standby state.

Answer: ABC

118. Firewall update signature database and Virus database online throjgh security service center, requires the firewall can connect to the Internet first, and then need to configure the correct DNS addresses.

A. TRUE (Right Answers)
B. FALSE

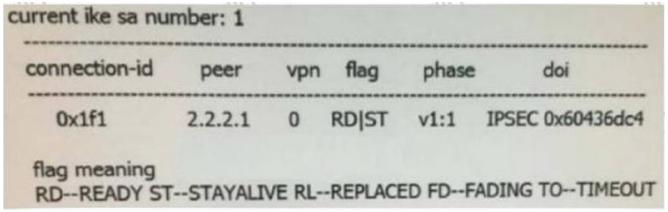
Answer: T

119. Which of the following option does not belong to symmetric encryption algorithm?

A. DES
B. 3DES
C. AES
D. RSA (Right Answers)

Answer: D

120. Through display ike sa to see the result as follows, which statements are correct? (Multiple choice)



A. The first stage ike sa has been successfully established (Right Answers)
B. The second stage ipsec sa has been successfully established
C. ike is using version v1 (Right Answers)
D. ike is using version v2

Answer: CA

121. Regarding the comparison between windows and Linux, which of the following statements is wrong?

A. Getting started with Linux is more difficult and requires some learning and guidance.
B. Windows can be compatible with most software playing most games
C. Linux is open source code, you can do what you want.
D. windows is open source, you can do what you want. (Right Answers)

Answer: D

122. Which ofthe following are core elements ofthe IATF (Information Assurance Technology Framework) model? (Multiple choice)

A. Environment
B. person (Right Answers)
C. Technology (Right Answers)
D. **Operation (Right Answers)**

Answer: BCD

123. Which of the following are multi-user operating systems? (Multiple choice)

A. MSDOS
B. UNIX (Right Answers)
C. LINUX (Right Answers)
D. Windows (Right Answers)

Answer: BCD

124. Electronic evidence preservation is directly related to the legal effect of evidence, in line with the preservation of legal procedures, and its authenticity and reliability are guaranteed. Which of the following is not an evidence preservation technology?

A. Encryption technology
B. Digital certificate technology
C. Digital signature technology
D. Message tag tracking technology (Right Answers)

Answer: D

125. When the following conditions occur in the VGMP group, the VGMP message will not be sent to the peer end actively?

A. Dual hot backup function enabled
B. Manually switch the active and standby status of the firewall.
C. Firewall service interface failure
D. Session table entry changes (Right Answers)

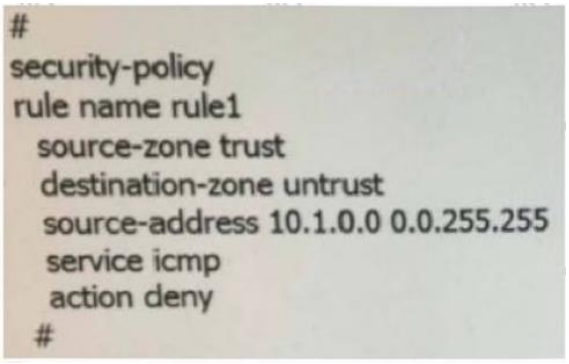
Answer: D

126. Which of the following options can be used in the advanced settings of Windows Firewall? (Multiple choice)

A. Restore defaults (Right Answers)
B. Change notification rules (Right Answers)
C. Set connection security rules (Right Answers)
D. Set out inbound rules (Right Answers)

Answer: ABCD

127. The following security policy command, representatives of the meaning:



A. banned from trust region access to untrust region and the destination address is 10 1 10 10 host ICMP message
B. banned from trust region access to untrust region and the destination address is 10.1 0 0/16 segment all hosts ICMP message
C. banned from trust region access to untrust region and the source address is 10.1 0 0/16 segment all the hosts ICMP message (Right Answers)
D. banned from trust region access to untrust region and the source address is 10.2.10.10 host to all the hosts ICMP message

Answer: C

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

A. True (Right Answers)
B. False

Answer: A

129 If the administrator uses ’he default authentication domain to authenticate a user, you only need to enter a user name when the user logs, if administrators use the newly created authentication domain to authenticate the user, the user will need to enter login "username @ Certified domain name"

A. True (Right Answers)
B. False

Answer: A

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

A. True (Right Answers)
B. False

Answer: A

131. Intrusion prevention system technical characteristics include (Multiple choice)

A. Online mode (Right Answers)
B. Real-time blocking (Right Answers)
C. Self-learning and adaptive (Right Answers)
D. Straight road deployment

Answer: ABC

132. Which of the following is true about firewall security policies?

A. By default, the security policy can control unicast packets and broadcast packets.
B. By default, the security policy can control multicast.
C. By default, the security policy only controls unicast packets. (Right Answers)
D. By default, the security policy can control unicast packets, broadcast packets, and multicast packets.

Answer: C

133. Which of the following information will be encrypted during the use of digital envelopes? (Multiple choice)

A. Symmetric key (Right Answers)
B. User data (Right Answers)
C. Receiver public key
D. Receiver private key

Answer: AB

134. Which of the following are in the certification area of IS027001? (Multiple choice)

A. Access control (Right Answers)
B. Personnel safety (Right Answers)
C. Vulnerability management (Right Answers)
D. Business continuity management (Right Answers)

Answer: ABCD

135. Which of the following io true about the description of the firewall?

A. The firewall cannot transparently access the network.
B. Adding a firewall to the network will inevitably change the :opology of the network.
C. In order to avoid single point of faiure. the firewall only supports side-by-side deplcyment.
D. Depending on the usage scenario, the firewall can be deployed in transparent moce or deployed in a three bedroom mode. (Right Answers)

Answer: D

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 (Right Answers)
C. reset current-configuration
D. reset running-configuration

Answer: B

137. Against Buffer overflow attacks, which description is correct? (Multiple choice)

A. Buffer overflow attack is use of the software system on memory operating defects, by using high operating permission to run attack code (Right Answers)
B. Buffer overflow attack has nothing to do with operating system's vulnerabilities and architecture
C. Buffer overflow attack is the most common method of attack software system's behaviors (Right Answers)
D. Buffer overflow attack belongs to the application layer attack behavior (Right Answers)

Answer: ACD

138. Security technology has different approaches at different technical levels and areas. Which of the following devices can be used for network layer security protection? (Multiple choice)

A. Vulnerability scanning device
B. Firewall (Right Answers)
C. Anti-DDoS equipment (Right Answers)
D. IPS/IDS equipment (Right Answers)

Answer: BCD

139. IPSEC VPN technology does not support NAT traversal when encapsulated in ESP security protocol because ESP encrypts the packet header.

A. True
B. False (Right Answers)

Answer: B

140. Which of the following are part of the SSL VPN function? (Multiple choice)

A. User authentication (Right Answers)
B. Port scanning
C. File sharing (Right Answers)
D. WEB rewriting

Answer: AC

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 (Right Answers)
B. Symmetric key
C. Receiver public key
D. Receiver private key

Answer: A

142 Which of the following traffic matches the authentication policy triggers authentication?

A. Access device or device initiated traffic
B. DHCP, BGP. OSPF and LDP packets
C. **Traffic of visitors accessing HTTP services (Right Answers)**
D. The first DNS packet corresponding to the HTTP service data flow

Answer: C

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

A. Need to configure local to DMZ security policy
B. No need to do any configuration (Right Answers)
C. Need to configure an interzone security policy
D. Need to configure DMZ to local security policy

Answer: B

144. Using a computer to store information about criminal activity is not a comouter crime

A. True
B. False (Right Answers)

Answer: B

145. Which of the following descriptions is wrong about IKE SA?

A. IKE SA is two-way
B. IKE is a UDP- based application layer protocol
C. IKE SA for IPSec SA services
D. The encryption algorithm used by user data packets is determined by IKE SA. (Right Answers)

Answer: D

146. Which of the following statements is wrong about VPN?

A. Virtual private network is cheaper than dedicated line
B. VPN technology necessarily involves encryption technology (Right Answers)
C. VPN technology is a technology that multiplexes logica channels on actual physical lines.
D. The generation of VPN technology enables employees on business trips to remotely access internal corporate servers.

Answer: B

147. Which ofthe following are the standard port numbers for the FTP protocol? (Multiple choice)

A. 20 (Right Answers)
B. **21 (Right Answers)**
C. 23
D. 80

Answer: AB

148. Information security level protection is to improve the overall national security level, while rationally optimizing the distribution of security resources, so that it can return the greatest security and economic benefits

A. True (Right Answers)
B. False

Answer: A

149. For the occurrence of network security incidents, the remote emergency response is generally adopted first. If the problem cannot be solved for the customer through remote access, after the customer confirms, it is transferred to the local emergency response process.

A. True (Right Answers)
B. False

Answer: A

150. Which of the following is not included in the Corporate Impact Analysis (BIA)?

A. Business priority
B. Accident handling priority
C. **Impact assessment (Right Answers)**
D. Risk identification

Answer: C

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

A. True (Right Answers)
B. False

Answer: A

152. After the firewall uses the hrp standby config enable command to enable :he standby device configuration function all the information that can be backed up can be directly configured on the standby device, and the configuration on the standby device can be synchronized to the active device.

A. True (Right Answers)
B. False

Answer: A

153. Which of the following are the characteristics of a symmetric encryption algorithm? (Multiple choice)

A. **Fast encryption (Right Answers)**
B. Confidential speed is slow
C. **Key distribution is not secure (Right Answers)**
D. Key distribution security is high

Answer: AC

154. Which of the following are the hazards of traffic attacks? (Multiple choice)

A. Network paralysis (Right Answers)
B. Server downtime (Right Answers)
C. Data is stolen
D. The page has been tampered with

Answer: AB

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

A. True (Right Answers)
B. False

Answer: A

156. Regarding the HRP master and backup configuration consistency check content, which of the following is not included?

A. NAT policy
B. Is the heartbeat interface configured with the same serial number?
C. Next hop and outbound interface of static route (Right Answers)
D. Authentication Policy

Answer: C

157. Which of the following statement about the NAT configuration is wrong?

A. Configure source NAT in -.transparent mode, the 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 in the network, you do not need to configure NAT ALG
D. The firewall does not support NAPT conversion for ESP and AH packets. (Right Answers)

Answer: D

158. Which of the following descriptions about the action and security profile of the security policy are correct? (Multiple choice)

A. If the action of the security policy is "prohibited", the device will discard this traffic, and then no content security check will be performed. (Right Answers)
B. The security profile may know: be applied to the security policy tfat the action is allowed and take effect.

C. The security profile must be applied to the security policy that s allowed to take effect. (Right Answers)

D. If the security policy action is "Allow", the traffic will not match the security profile.

Answer: AC

159. Which of the following does the encryption technology support for data during data transmission? (Multiple choice)

A. **Confidentiality (Right Answers)**
B. Controllability
C. Integrity (Right Answers)
D. Source verification (Right Answers)

Answer: ACD

160. After the network attack event occurs, set the isolation area, summary data, and estimated loss according to the plan. Which stage does the above actions belong to the work contents of in the network security emergency response?

A. Preparation stage
B. Detection phase
C. Inhibition phase (Right Answers)
D. Recovery phase

Answer: C

161. IPSec VPN uses an asymmetric encryption algorithm to encrypt the transmitted data

True

False (Right Answers)

Answer: B

162. Digital certificates are fair to public keys through third-party agencies, thereby ensuring the non-repudiation of data transmission. Therefore, to confirm the correctness of the public key, only the certificate of the communicating party is needed.

True

False (Right Answers)

Answer: B

163. Digital signatures are used to generate digital fingerprints by using a hashing algorithm to ensure the integrity of data transmission

A. True (Right Answers)
B. False

Answer: A

164. Which of the following descriptions of the firewall fragment cache function are correct? (Multiple choice)

A. By default, the firewall caches fragmented packets. (Right Answers)
B. After the fragmented packet is directly forwarded, the firewall forwards the fragment according to the interzone security policy if it is not the fragmented packet of the first packet.
C. For fragmented packets, NAT ALG does not support the processing of SIP fragmen:ed packets. (Right Answers)
D. By default, the number of large fragment caches of an IPV4 packet is 32, and the number of large fragmentation buffers of an IPV6 packet is 255 (Right Answers)

Answer: ACD

165. The SIP protocol establishes a session using an SDP message, and the SDP message contains a remote address or a multicast address

A. True (Right Answers)
B. False

Answer: A

166. Which of the following attacks is not a cyber-attack?

A. IP spoofing attack
B. Smurf attack
C. MAC address spoofing attack (Right Answers)
D. ICMP attack

Answer: C

167. Which of the following 3re the versions of the SNMP protocol? (Multiple choice)

A. SNMPvl (Right Answers)
B. SNMPv2b
C. SNMPv2c (Right Answers)
D. SNMPv3 (Right Answers) **Answer: ACD**

168. About the description about the preemption function of VGMP management, which of the following statements is? wrong?

A. By default, the preemption function of the VGMP management group is enabled.
B. By default, the preemption delay of the VGMP management group is 40s. (Right Answers)
C. Preemption means that when the faulty primary device recovers, its priority will be restored. At this time, it can regain its own state.
D. After the VRRP backup group is added to the VGMP management group, the original preemption function on the VRRP backup group is invalid.

Answer: B

169. In the IPSec VPN transmission mode, which part ofthe data packe: is encrypted?

Network layer and upper layer data packet

Original IP packet header

New IP packet header

Transport layer and upper layer data packet (Right Answers)

Answer: D

170. Which of the following descriptions about windows logs is wrong?

A. The system log is used to record the events generated by the operating system components, including the crash of the driver, system components and application software, and data
B. Windows server 2008 system logs stored in the Application.evtx (Right Answers)
C. The application log contains events logged by the application or system program, mainly recording events in the running of the program.
D. Windows seiver 2008 security lug is sluied in security.evtx

Answer: B

171. Against IP Spoofing, which of the following description is wrong?

A. IP spoofing is to use the hosts' normal trust relationship based on the IP address to launch it
B. Af-.er IP spoofing attack is successful, the attacker can use forged any IP address to imitate legitimate hast to access to critical information (Right Answers)
C. An attacker would need to cisguise the source IP addresses as trusted hosts, and send the data segment with the SYN flag request for connection **Answer: B**

172. In the USG series firewall, which of the following commands can be used to query the NAT translation result?

A. display nat translation
B. display firewall session table (Right Answers)
C. display current nat
D. display firewall nat translation

Answer: B

173. The preservation of electronic evidence is directly related to the legal effect of evidence, and it is in conformity with the preservation of legal procedures, and its authenticity and reliability are guaranteed. Which of the following is not an evidence preservation technique?

A. Encryption technology
B. Digital certificate technology
C. Digital signature technology
D. Packet tag tracking technology (Right Answers)

Answer: D

174. Which of the following are the status information that can be backed up by the HRP (Huawei Redundancy Protocol) protocol? (Multiple choice)

A. Session table (Right Answers)
B. ServerMap entry (Right Answers)
C. Dynamic blacklist (Right Answers)
D. Routing table

Answer: ABC

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

A. **True (Right Answers)**
B. False

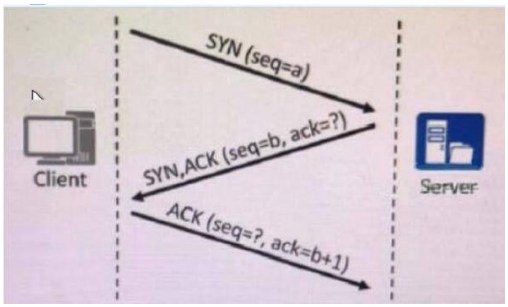
Answer: A

177. Winch of the following is the encryption technology used in digital envelopes?

A. Symmetric encryption algorithm
B. **Asymmetric encryption algorithm (Right Answers)**

Answer: B

175. As shown in the figure, a TCP connection is established between client A and server B Which of the following two “T packet numbers should be?



A. a+1: a
B. a: a+1
C. b+1: b
D. a+1: a+1 (Right Answers) **Answer: D**

178. Which of the following are remote authentication methods? (Multiple choice)

A. RADIUS (Right Answers)
B. Local
C. HWTACACS (Right Answers)
D. LLDP

Answer: AC

179. Which of the following statements about IPSec SA is true?

A. IPSec SA is one-way (Right Answers)
B. IPSec SA is two-way
C. used to generate an encryption key
D. Used to generate a secret algorithm

Answer: A

180. Which of the following does not include the steps of the safety assessment method?

A. Manual audit
B. Penetration test I-
C. Questionnaire survey
D. Data analysis (Right Answers)

Answer: D

181. Which of the following guarantees "should detect and protect spam at critical network nodes and maintain upgrades and updates of the spam protection mechanism" in security 2.0?

A. **Malicious code prevention (Right Answers)**
B. Communication transmission
C. Centralized control
D. Border protection

Answer: A

182. Which of the following is not in the quintuple range?

Source IP

Source MAC (Right Answers)

Destination IP

Destination port

Answer: B

183. In stateful inspection firewall, when opening state detection mechanism, three-way handshake's second packet (SYN + ACK) arrives the firewall. If there is still no corresponding session table on the firewall, then which of the following statement is correct?

A. If the firewall security policy allows packets through, then the packets can pass through the firewall
B. If the firewall security policy allows packets through, then creating the session table
C. Packets must not pass through the firewall (Right Answers)
D. Packets must pass through the firewall, and establishes a session table

Answer: C

184. In the VRRP (Virtual Router Redundancy Protocol) group, the primary firewall periodically sends advertisement packets to the backup firewall. The backup firewall is only responsible for monitoring advertisement packets and will not respond.

A. True (Right Answers)
B. False

Answer: A

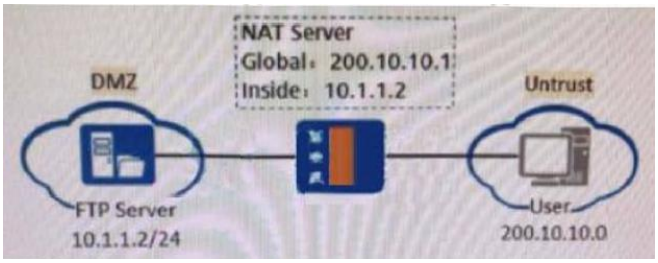
185. The VRRP advertisement packet of the Huawei USG firewall is a multicast packet. Therefore, each firewall in the backup group must be able to implement direct Layer 2 interworking

A. True (Right Answers)
B. False **Answer: A**

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

A. True
B. False (Right Answers) **Answer: B**

187. As shown in the figure, a NAT server application scenario is configured when the web configuration mode is used



Which of the following statements are correct"? (Multiple choice)

A. When configuring an interzone secunty policy, set the source security zone to Untrust and the target security zone to DMZ (Right Answers)
B. When configuring NAT Server, the internal address is 10 1.1 2 and the external address is 200.10.10.1. (Right Answers)
C. When configuring an interzone secunty policy, set the source security zone to DMZ and the target secunty 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. **Answer: AB**

188. In L2TP configuration for command Tunnel Name, which statements are correct? (Multiple choice)

A. Used to specify the name of the end of the tunnel (Right Answers)
B. Used to specify the name of the peer tunnel
C. Must be consistent with Tunnel Name peer configuration
D. If do not configure the Tunnel Name, the tunnel name is the name of the local system (Right Answers)

Answer: AD

189. Which of the following types of attacks does the DDos attack belong to?

Snooping scanning attack

Malformed packet attack

Special packet attack

Traffic attack (Right Answers)

Answer: D

190. In the USG system firewall, the_____function can be used to provide well-known applica'.ion services for non-known ports.

Port mapping (Right Answers)

MAC and IP address binding

Packet filtering

Long connection

Answer: A

191. Which of the following is correct for the command to view the number of security pclicy matches?

A. display firewall sesstion table
B. display security-policy all (Right Answers)
C. display security-policy count
D. count security-policy hit

Answer: B

192. Which of the following belongs to Layer 2 VPN technology?

A. SSL VPN
B. L2TP VPN (Right Answers)
C. GRE VPN
D. IPSec VPN

Answer: B

193. About the descriptions of windows Firewall Advanced Settings, which of the following is wrong? (Multiple choice)

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 rule, both the local port and the remote port can be restricted. (Right Answers)
C. When setting the pop-up rule, only the local port can be restricted, and the remote port cannot be restricted,
D. When setting the pop-up rule, both local ports and remote ports can be restricted. (Right Answers)

Answer: BD

194. Which of the following description about the group management for VGMP is wrong?

A. Master/slave status change of VRRP backup group needs to notify its VGMP management group
B. The interface type and number of two firewalls heartbeat port may be different, as long as they can communicate with each other (Right Answers)
C. Periodically sends Hello packets between VGMP of master/slave firewall
D. master/slave devices exchange packets to understand each other through the heartbeat line, and backup the related commands and status information

Answer: B

195, In the security assessment method, the purpose ofthe security scan is to scan the target system with a scan analysis evaluation tool to discover related vulnerabilities and prepare for the attack.

True

False (Right Answers)

Answer: B

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 (Right Answers)

Answer: D

197 Which of the following descriptions about IKE SA is wrong?

A. IKE SA is two-way
B. IKE is a UDP- based application layer protocol
C. IKE SA servers for IPSec SA
D. The encryption algorithm used by user data packets is determined by IKE SA. (Right Answers)

Answer: D

198. In the construction of information security system, the security model is needed to accurately describe the relationship between important aspects of security and system behavior

A. True
B. False (Right Answers)

Answer: B

199. Security policy conditions can be divided into multiple fields, such as source address, destination address, source port, destination port, etc. These fields are "and", that is, only information in the packet match all fields, and then hit this policy.

True

False (Right Answers)

Answer: B

200. The matching principle of the security policy is: firstly, find the inter-domain security policy configured manually, and if there is no match, the data packet is directly discarded

A. True (Right Answers)
B. False

Answer: A

201. Which of the following are the response actions after the gateway antivirus detects the mail virus? (Multiple choice)

A. **Alarm (Right Answers)**
B. **Blocking (Right Answers)**
C. Announcement (Right Answers)
D. Delete attachments (Right Answers)

Answer: ABCD

202. Digital signature is to achieve the integrity of data transmission by using a hash algorithm to generate digital fingerprints.

A. **True (Right Answers)**
B. False

Answer: A

203. Which of the following statement is wrong about NAT?

A. Configure a NAT address pool in the source NAT technology. You can configure only one IP address in the address pool.
B. Address Translation can follow the needs of users, providing FTP. WWW, Telnet and other services outside the LAN
C. Some application layer protocols carry IP address information in the data, but also to modify the data in the upper layer of the IP address information when they make NAT
D. For some non-TCP. UDP protocols (such as ICMP. PPTP), unable to do NAT. (Right Answers)

Answer: D

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

Destination IP

Destination port number

Protocol number

Source IP (Right Answers)

Answer: D

205. Which of the following are malicious programs? (Multiple choice)

A. Trojan horse (Right Answers)
B. Vulnerabilities
C. Worm (Right Answers)
D. Virus (Right Answers)

Answer: ACD

206. Which of the following are the main implementations of gateway anti-viru3? (Multiple choice)

A. Agent scanning method (Right Answers)
B. Stream scanning method (Right Answers)
C. Package inspection method
D. File killing method

Answer: AB

207. Which of the following is not a hash algorithm?

A. MD5
B. SHA1
C. SM1 (Right Answers)
D. SHA2

Answer: C

208. Which of the following desciipliuri uf firewall hul standby is cuie? (multiple choice)

A. When multiple areas of the firewall need to provide dual-system backup, you need to configure multiple VRRP backup groups on the firewall. (Right Answers)
B. The status of all VRRP backup groups in the same VGMP management group on the same firewall is the same (Right Answers)
C. The hot standby of the firewall needs to synchronize the backup between the master device and the slave device by using the session table. MAC table, and routing table.
D. VCMP i3 to ensure the consistency of all VRRP backup group switching (Right Answers)

Answer: ABD

209. Which of the following is not the certificate save file format supported by the USG6000 series?

A. PKCS#12
B. DER
C. PEM
D. PKCS# (Right Answers)

Answer: D

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

A. ICMP redirect packet attack
B. ICMP unreachable packet attack
C. IP address scanning attack (Right Answers)
D. Large ICMP packet attack

Answer: C

211. Security technology has different methods at different technical levels and areas. Which of the following devices can be used for network layer security protection? (Multiple choice)

A. Vulnerability scanning device
B. Firewall (Right Answers)
C. Anti-DDoS device (Right Answers)
D. IPS/IDS device (Right Answers)

Answer: BCD

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

A. sender public key
B. sender private key (Right Answers)
C. Receiver public key
D. Receiver private key

Answer: B

213. OSPF is more commonly used than RIP because OSPF has device authenticatior and is more secure

A. True
B. False (Right Answers)

Answer: B

214. The content of intrusion detection covers authorized and unauthorized intrusions. Which of the following is not in the scope of intrusion detection?

A. Pretending to be another user
B. Administrator mistakenly delete configuration (Right Answers)
C. Planting worms and Trojans
D. Leaking data information

Answer: B

215. For the description of ARP spoofing attacks, which the following statements is wrong?

A. The ARP implementation mechanism only considers the normal interaction of the service and does not verify any abnormal business interactions or malicious behaviors.
B. ARP spoofing attacks can only be implemented through ARP replies and cannot be implemented through ARP requests (Right Answers)
C. When a host sends a normal ARP request, the attacker will respond preemptively, causing the host to establish an incorrect IP and MAC mapping relationship.
D. ARP static binding is a solution to ARP spoofing attacks. It is mainly applied to scenarios where the network size is small.

Answer: B

216. Which of the following mechanisms are used in the MAC flooding attack? (Multiple choice)

A. MAC learning mechanism of the switch (Right Answers)
B. forwarding mechanism of the switch (Right Answers)
C. ARP learning mechanism (Right Answers)
D. Number of MAC entries is limited (Right Answers)

Answer: ABCD

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

True (Right Answers)

False

Answer: A

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

A. True
B. False (Right Answers) **Answer: B**

219. When establishing their own information systems, companies check each operation according to internationally established authoritative standards and can check whether their information systems are safe

A. True (Right Answers)
B. False **Answer: A**

220. Which of the following is the port number used by L2TP packets?

A. 17
B. 500
C. 1701 (Right Answers)
D. 4500

Answer: C

221. Which of the following is not included in the steps of tie safety assessment method?

A. Manual audit
B. Penetration test
C. Questionnaire survey
D. Data analysis (Right Answers)

Answer: D

222. IPSec VPN uses an asymmetric encryption algorithm to encrypt the transmitted data

A. True
B. False (Right Answers)

Answer: B

223. Which of the following is correct about firewall IPSec policy?

A. By default, IPSec policy can control unicast packets and broadcast packets.
B. By default, IPSec policy can control multicast.
C. By default. IPSec policy only controls unicast packets. (Right Answers)
D. By default, IPSec policy can control unicast packets, broadcast packets, and multicast packets °

Answer: C

224. Which of the following information will be encrypted during the use of digital envelopes? (Multiple Choice)

A. Symmetric key (Right Answers)
B. User data (Right Answers)
C. Receiver public key
D. Receiver private key

Answer: AB

225. Which of the following is an action to be taken during the eradication phase of the cyber security emergency response? (Multiple Choice)

A. Find sick Trojans, illegal authorization, system vulnerabilities, and deal with it in time (Right Answers)
B. Revise the security policy based on the security incident that occurred, enable security auditing (Right Answers)
C. Block the behavior ofthe attack, reduce the scope of influence
D. Confirm the damage caused by security incidents and report security incidents

Answer: AB

226. Which of the following attacks can DHCP Snooping prevent? (Multiple Choice)

A. DHCP Server counterfeiter attack (Right Answers)
B. Intermediaries and IP/MAC spoofing attacks (Right Answers)
C. IP spoofing attack (Right Answers)
D. Counterfeit DHCP lease renewal packet attack using option82 field (Right Answers)

Answer: ABCD

227. Which of the following belongs to the devices at the execution layer in the Huawei SDSec solution? 'Multiple Choice)

A. cis
B. Fierhunter (Right Answers)
C. Router (Right Answers)
D. AntiDDoS (Right Answers)

Answer: BCD

228. A company employee account authority expires, but can still use the account to access the company server. What are the security risks of the above scenarios? (Multiple Choice)

A. Managing security risk (Right Answers)
B. Access security risk (Right Answers)
C. System security risk (Right Answers)
D. Physical security risk

Answer: ABC

229. Which of the following is the default backup method for double hot standby?

A. Automatic backup (Right Answers)
B. Manual batch backup
C. Session fast backup
D. Configuration of the active and standby FWs after the device is restarted

Answer: A

230. The network administrator can collect data to be analyzed on the network device by means of packet capture, port mirroring, or log, etc.

A. True (Right Answers)
B. False

Answer: A

231. The world's first worm "Morris worm" made people realize that as people become more dependent on computers, the possibility of computer networks being attacked increases, and it is necessary to establish a comprehensive emergency response system.

A. True (Right Answers)
B. False

Answer: A

232. Which of the following are the necessary configurations of IPSec VPN? (Multiple Choice)

A. Configuring IKE neighbors (Right Answers)
B. Configure IKE SA related parameters (Right Answers)
C. Configuring IPSec SA related parameters (Right Answers)
D. Configure the stream of interest (Right Answers)

Answer: ABCD

233. Which ofthe following types are included in Huawei firewall user management? (Multiple Choice)

A. Internet user management (Right Answers)
B. H B. Access user management (Right Answers)
C. **Administrator User Management (Right Answers)**
D. Device User Management

Answer: ABC

234. In order to obtain evidence of crime, it is necessary to master :he technology of intrusion tracking. Which of the following descriptions are correct about the tracking technology? (Multiple Choice)

A. Packet Recording Technology marks packets on each router that has been spoken by inserting trace data into the tracked IP packets. (Right Answers)
B. Link detection technology determines the source of the attack by testing the network connection between the routers (Right Answers)
C. Packet tagging technology extracts information from attack sources by recording packets on the router and then using data drilling techniques
D. Analysis of shallow mail behavior can analyze the information such as sending IP address, sending time, sending frequency, number of recipients, shallow email headers, etc. (Right Answers)

Answer: ABD

235. When the sesson authentication mode is used to trigger the firewall's built-in Portal aithentication. the user does not actively perform identity authentication, advanced service access, and device push "redirect" to the authentication page? .. ' • ’

A. True (Right Answers)
B. False

Answer: A

226. Which of the following description is wrong aoout the intrusion detection system?

A. The intrusion detection system can dynamically collect a large amount of key information 3nd materials through the network and computer, and can timely analyze and judge the current state of the entire system environment.
B. The intrusion detection system can perform blocking operation if it finds that there is a violation of the security policy or the system has traces of being attacked.
C. Intrusion detection system includes all hardware and software systems for intrusion detection (Right Answers)
D. The flood detection system can be linked with firewalls and switches to become a powerfu 'helper' of the firewall, which is better and more precise to control traffic access between domains.

Answer: C

237. Which of the following options belong to the encapsulation mode supported by IPSec VPN? (Multiple Choice)

A. AH mode
B. Tunnel mode (Right Answers)
C. Transmission mode (Right Answers)
D. ESP mode

Answer: BC

238. The tunnel addresses at both ends ofthe GRE tunnel can be configured as addresses of different network segments.

A. True (Right Answers)
B. False

Answer: A

239. Regarding Ihe description of the packe: in the iptables transmission process, which of the following option is wrong?

A. When a packet enters the network card, it first matches the PREROUTING chain
B. If the destination address of the packet is local, the packet will be sent to the INPUT chain
C. If the destination address of the packet is not local, the system sends the packet to the OUTPUT chain. (Right Answers)
D. If the destination address of the packet is not local, the system sends the packet to the FORWARD chain.

Answer: C

240. Which of the following description is wrong about the operating system?

A. The operating system is the interface between the user and the computer
B. The operating system is responsible for managing the execution of all hardware resources and control software of the computer system.
C. The interface between the operating system and the user is a graphical interface. (Right Answers)
D. The operating system itself is also a software

Answer: C

241. Which of the following is null a itjquiiemeiil fui (bewail duuble hul standby?

A. The firewall hardware model is consistent
B. The firewall software version is consistent
C. The type and number of the interface used are the same
D. The firewall interface has the same IP address. (Right Answers)

Answer: D

242. Which of the following options are correct about the NAT policy processing flow? (Multiple Choice)

A. Server-map is processed after status detection (Right Answers)
B. Source NAT policy query is processed after the session is created
C. The source NAT policy is processed after the security policy is matched. (Right Answers)
D. Server-map is processed before the security policy matches (Right Answers)

Answer: ACD

243. Which of the following options belong to the necessary configuration for the firewall double hot standby scenario? (Multiple Choice)

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

Answer: AC

244. Manual auditing is a supplement to tool evaluation. It does not require any software to be installed on the target system being evaluated, and has no effect on the operation and status of the target system. Which of the following options does not include manual auditing?

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 administrator's operation of the equipment process (Right Answers)

Answer: D

245. Which of the following are the default security zones of Huawei firewall? (Multiple Choice)

A. Zone area
B. Trust area (Right Answers)
C. Untrust area (Right Answers)
D. Security area

Answer: BC

246. Which level is the corresponding warning for major network security incidents that occur?

Red warning

Orange warning (Right Answers)

Yellow warning

Blue warning

Answer: B

247. Which of the following descriptions is wrong ebout the source of electron c evidence?

A. Fax data, mobile phone recording is an electronic evidence related to communication technology.
B. Movies and TV shows belong to electronic evidence related to network technology. (Right Answers)
C. Database opera'.ion records, operating system logs are computer-related electronic evidence
D. Operating system, e-mail, chat records car be used as a source of electronic evidence

Answer: B

248. Which of the following description is correct about the sort of the call setup process for L2TP corridors?

1. L2TP tunnel 2. PPP connection

3. LNS authenticates users 4. Users access intranet resources

5. Establish an L2TP session

A. 1->2->3->5->4
B. **1->5->3->2->4 (Right Answers)**
C. 2->1->5->3->4 T

249. The Protocol field in the IP header identifies the protocol used by the 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

Answer: B

250. According to the management specifications, the network security system and equipment are regularly checked, the patches are upgraded, and the network security emergency response drill is organized. Which of the following belongs to the MPDRR network security modes of the above actions?

Protection link

Testing link (Right Answers)

Response link (Right Answers)

Management link

Answer: BC

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

A. **True (Right Answers)**
B. False

Answer: A

252. Which of the following is not the identity of the IPSec SA?

spi

Destination address

Source address (Right Answers)

Security policy

Answer: C

253. Which of the following statements are correct about the differences between pre-accident prevention strategies and post-accident recovery strategies? (H/multiple Choice)

The prevention strategy focuses or minimizing the likelihood of an accident before the story occurs. The recovery strategy focuses on minimizing the impact and loss on the company after the accident (Right Answers)

The role of pre-disaster prevention strategies does not include minimizing economic, reputational, and other losses caused by accidents.

Recovery strategy is used to imprcve business high availability (Right Answers)

Recovery strategy is part of the business continuity plan (Right Answers)

Answer: ACD

254. Which of the following operations are necessary during the administrator upgrade of the USG firewall software version? (Multiple Choice)

A. **Upload the firewall version software (Right Answers)**
B. **Restart the device (Right Answers)**
C. Device factory reset
D. **Specify the next time you start loading the software version. (Right Answers)**

Answer: ABD

255. If the company structure has undergone a practical change, it is necessary to retest whether the business continuity plan is feasible

A. **True (Right Answers)**
B. False

Answer: A

256. HTTP packets are carried by UDP. and the HTTPS protocol is based on TCP three-way handshake. Therefore. HTTPS is relatively secure, and HTTPS is recommended.

A. True
B. **False (Right Answers)**

Answer: B

257. The single-point login function of the online user, the user authenticates directly to the AD server, and the device does not interfere with the user authentication process. The AD monitoring service needs to be deployed on the USG device to mcnitorthe authentication information of the AD server.

A. True
B. False (Right Answers)

Answer: B

258. UDP port scanning means that the attacker sends a zero-byte UDP packet to a specific port of the target host. If the port is open, it will return an ICMP port reachable data packet

A. True
B. False (Right Answers)

Answer: B

259. Which of the following statements are correct about the business continuity plan? (Multiple Choice)

A. Business continuity plan rines nnt require high-level participation Nfthe Company in determining the project scope phase
B. BCP needs flexibility because it cannot predict all possible accidents (Right Answers)
C. Business continuity plan does not require high-level participation of the company before forming a formal document
D. Not all security incidents must be reported to company executives (Right Answers)

Answer: BD

260. When the USG series firewall hard disk is ir place, which of the following logs can be viewed? (Multiple Choice)

A. Operation log (Right Answers)
B. Business log (Right Answers)
C. Alarm information (Right Answers)
D. **Threat log (Right Answers)** **Answer: ABCD**

261. Social engineering is a means of harm such as deception, injury, etc. through psychological traps such as psychological weakness, instinctive reaction, curiosity, trust, and greed

A. True (Right Answers)
B. False **Answer: A**

262. Apply for emergency response special funds, which stage work content does procurement emergency response software and hardware equipment belong to in the network full emergency response?

A. Preparation stage (Right Answers)
B. Inhibition phase
C. Response phase
D. Recovery phase

Answer: A

263. Device destruction attacks are generally not easy to cause information leakage, but usually cause network communication services to be interrupted.

A. **True (Right Answers)**
B. False

Answer: A

264. Which of the following description is wrong about the Internet users and VPN access user authentication?

A. The Internet user and the VPN access user share data, and the users attribute check (user status, account expiration time, etc.) also takes effect on the VPN access.
B. The local authentication or server authentication process is basically the same for the Internet users. The authentication is performed on the user through the authentication domain.
C. After the VPN user accesses the network, it can access the network resources of the enterprise headquarters. The firewall can control the accessible network resources based on the user name.
D. After the VPN access user passes the authentication, it will be online on the user online list. (Right Answers)

Answer: D

265. Which of the following descriptions about the patch is wrong?

A. Patch is a small program made by the original author of the software for the discovered vulnerability.
B. No patching does not affect the operation of the system, so it is irrelevant whether to patch or not. (Right Answers)
C. Patches are generally updated.
D. Computer users should download and install new patches to protect their systems in a timely manner **Answer: B**

266. Which of the following description is wrong about the Intrusion Prevention System (IPS)?

A. IDS devices need to be linked to the firewall to block the intrusion
B. IPS devices cannot be bypassed in the network. (Right Answers)
C. IPS devices can be cascaded at the network boundary and deployed online
D. IPS devices can be blocked in real time once they detect intrusion

Answer: B

267. Which of the following statements are correct about Huawei routers and switches? (Multiple Choice)

A. **The router can implement some security functions, and some routers can implement more security functions by adding security boards. (Right Answers)**

B. The main function of the router is to forward data. Sometimes the firewall may be a more suitable choice when the enterprise has security requirements. (Right Answers)
C. The switch has some security features, and some switches can implement more security functions by adding security boards. (Right Answers)
D. The switch does not have security features

Answer: ABC

268. Which of the following options does not belong to the log type of the Windows operating system?

A. Business log (Right Answers)
B. Application log
C. Security log
D. System log

Answer: A

269. After the network intrusion event occurs, according to the plan to obtain the identity of the intrusion, the attack source and other information, and block the intrusion behavior, which links of the above actions are involved in the PDRR network security model? (Multiple Choice)

A. Protection link
B. Testing link (Right Answers)
C. **Response link (Right Answers)**
D. Recovery link

Answer: BC

270. Which of the following is wrong about the scanning of vulnerabilities?

A. The vulnerability was discovered beforehand and discovered afterwards
B. Vulnerabilities are generally repairable
C. Vulnerabilities are security risks that can expose computers to hackers
D. Vulnerabilities can be avoided (Right Answers)

Answer: D

271. When the user single sign-on is configured, the receiving PC message mode is adopted. The authentication process has 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. Add to the online user table 3 AD monitor connects to the AD server to query the login user information, and f?rwards the queried user information to the firewall. 4 The visitor logs in to the AD domain. The AD server returns the login success message to the user and delivers the login script, which of the following order is correct?

A. 1-2-3-4
B. 4-1-3-2 (Right Answers)
C. 3-2-'-4
D. 1-4-3-2

Answer: D

272. The administrator wants to create a web configuration administrator, and set the Https device management port number to 20000, and set the administrator to the administrator level, which of the following commands are correct?

A. Stepl: web-manager security enable port 20000 Step2: AAA View [USG] aaa [USG aaa] manager-user client001 [USG-aaa-manager-user-client001] service-type web [USG-aaa-manager-user-client001] level 15 [USG-aaa- manager-user-client001] password cipher Admin@123 (Right Answers)
B. Stepl: web-manager enable port 20000 Step2. AAA View [USG] aaa [USG aaa] manager-user clientO01 [USG-aaa-manager-user-client001] service-type web [USG-aaa-manager-user-client001] password cipher Admin@123
C. Stepl: web-manager security enable port 20000 Step2: AAA View [USG] aaa [USG aaa] manager-user client001 [USG-aaa-manager-user-client001] service-type web [USG-aaa manager-user-client001] password cipher
D. Stepl: web-manager security enable port 20000 Step2: AAA View [USG] aaa [USG aaa] manager-user client001 [USG-aaa-manager-user-client001] service-type web [USG-aaa-manager-user-client001] level 1 [USG-aaa- manager-user-client001] password cipher Admin@123 **Answer: A**

273. Which of the following description are correct about the security policy action and security configuration file? (Multiple Choice)

A. If the action of the security policy is 'prohibited', the device will discard this traffic and will not perform content security check later. (Right Answers)
B. The security configuration file can be applied without being applied to the security policy allowed by the action
C. The security configuration file must be applied to the security policy that is allowed to take effect. (Right Answers)
D. If the security policy action is "Allow", the traffic will not match the security configuration file.

Answer: AC

274. Which of the following are the same features of Windows and LINUX systems? (Multiple Choice)

A. Support multitasking (Right Answers)
B. Support graphical interface operations (Right Answers)
C. Open source system
D. Support multiple terminal platforms (Right Answers)

Answer: ABD

275. During the configuration of NAT. which of the following will the device generate a Server-map entry? (Multiple Choice)?

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

Answer: BD

276. NAT technology can securely transmit data by encrypting data.

A. True
B. False (Right Answers)

Answer: B

277. Which of the following is the correct order for event response management?

1 detection 2 report

3 relief 4 summarizing experience

5 repair 6 recovery 7 response

A. 1-3-2-7-5-64
B. 1-3-2-7-5-54
C. 1-2-3-7-5-54
D. 1-7-3-2-5-54 (Right Answers)

278. Which of the following statement is wong about L2TP VPN?

A. Applicable to business employees dialing access to the intranet
B. Will not encrypt the data
C. Can be used in conjunction with IPsec VPN
D. Belongs to Layer 3 VPN technology (Right Answers)

Answer: D

279. Encryption technology can transform readable information into unreadable information in a certain way

A. **True (Right Answers)**
B. False

Answer: A

280. ASPF (Application Specific Packet Filter) is a packet filtering technology based on the application layer, and implements a special security mechanism through the server-map table. Which of the following statements about the ASPF and server-map tables are correct? (Multiple Choice)

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

Answer: ABC

281. Antivirus software and host firewall have the same effect

A. True
B. False (best choice)

Answer: B

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

A. True (Right Answers)
B. False

Answer: A

283. Execute the command on the firewall and display the following information, which of the following description is correct? (Multiple Choice)

HRP_A [USG_A] display vrrp interfaceGigabitEthernet 0/0/1 \ GigabitEthernet9/0/1 | Virtual Router 1VRRP Group: Active state: Active Virtual IP: 202.38.10.1 Virtual MAC: 0000-5e00-0101 Primary IP: 202 38.10.2 PriorityRun: 100 PriorityConfig: 100 MasterPriority: 100 Preempt: YES Delay Time: 10

A. The status of this firewall VGMP group is Active. (Right Answers)
B. This firewall G1 / 0/1 virtual interface IP address 202.30.10.2
C. This firewall VRID is 1 the VRRP priority to backup g'oup 100 (Right Answers)
D. Will not switch when the primary device fails

Answer: AC

284. In the USG series firewall system view, the device configuration will be restored to the default configuration after the reset saved-configuration command is executed. No other operations are required

A. True
B. False (Right Answers)

Answer: B

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

A. True (Right Answers)
B. False

Answer: A

285. What is the difference between network address port translation (NAT) and conversion-only network address (No- PAT)? (Multiple Choice)

A. After NATP conversion, for external network users, all messages are from the same IP address or several IP addresses. (RightAnswers)
B. No-PAT only supports protocol address translation at the application layer.
C. NAPT only supports protocol address translation at the network layer.
D. No-PAT supports protocol address translation at the network layer (Right Answers)

Answer: AD

286. Which of the following descriptions are correct about the buffer overflow attack? (Multiple Choice)

A. Buffer overflow attack is the use of software system for memory operation defects, running attack code with high operation authority (Right Answers)
B. Buffer overflow attacks are not related to operating system vulnerabilities and architectures
C. Buffer overflow attacks are the most common method of attacking software systems (Right Answers)
D. Buffer overflow attack belongs to application layer attack behavior (Right Answers)

Answer: ACD

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

A. Emergency handling of security incidents
B. Early warning rotification of security incidents
C. Providing security evaluation services for government departments, enterprises and institutions
D. Cooperate with other agencies to provide training services (Right Answers)

Answer: D

289. Which of the following are international organizations related to information security standardization? (Multiple Choice)

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

Answer: ABC

290. In o der to obtain evidence of crime, it is necessary to master the technology of intrusion tracking Which of the following descriptions are correct about the tracking technology? (Multiple Choice)

- **A. Packet Recording Technology marks packets on each passing router by inserting trace data into the tracked IP packets (Right Answers)**
- **B. Link test technology determines the source of the attack by testing the network link between the routers (Right Answers)**
- C. Packet tagging technology extracts information from attack sources by recording packets on the router and then using data drilling techniques
- **D. Snallow mail behavior analysis can analyze the information such as sending IF address, sending time, sending frequency, number of recipients, shallow email heacers and so on. (Right Answers)**

Answer: ABD

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

- A. User data
- B. Receiver public key
- C. sender public key
- **D. Digital fingerprint (Right Answers)**

Answer: D

292. On the USG series firewalls, the default security policy does not support modification

- A. True
- **B. False (Right Answers)**

Answer: B

293. In the classification of the information security level protection system, which of the following levels defines the damage to the social order and the public interest if the information system is destroyed? (Multiple choice)

- **A. First level User-independent protection level (Right Answers)**
- **B. Second level System audit protection level (Right Answers)**
- **C. Third level Security mark protection (Right Answers)**
- **D. Fourth level Structured protection (Right Answers)**

Answer: ABCD

294. Which of the following is the analysis layer device in the Huawei SDSec solution? r a.

A. cis
B. Agile Controller
C. switch
D. Firehunter (Right Answers)

Answer: D

295. Which of the following options are correct about the control actions permit and deny of the firewall interzone forwarding security policy? (Multiple Choice)

A. The action of the firewall default security policy is deny (Right Answers)
B. The packet is matched immediately after the inter-domain security policy deny action, and the other interzone security policy will not be executed. (Right Answers)
C. Even if the packet matches the permit action of the security policy, it will not necessarily be forwarded by the firewall. (Right Answers)
D. Whether the message matches the permit action of the security policy or the deny action, the message will be processed by the UTM module.

Answer: ABC