Huawei Certified ICT Professional - Constructing Infrastructure of Security Network

1. Each bandwidth policy that references a bandwidth channel is individually constrained by the bandwidth channel, that is, the traffic that meets the matching conditions of the bandwidth policy, and the maximum bandwidth resource is exclusive.

A. Dynamic sharing

B. Strategy Sharing

C. Bandwidth reuse

D. Exclusive strategy

Answer(s): D

---

2. Before using SSL VPN to communicate, the client and server establish a session through the Handshake protocol to negotiate the relevant security parameters to be used in data transmission.

A. False

B. True

Answer(s): B

---

3. To prevent applications such as Email and ERP from being affected during normal business hours, an enterprise wants the minimum bandwidth available for such traffic to be at least 60 Mbps.

A. time-range work_time period-range 09: 00: 00 to 18: 00: 00 working-day traffic-policy profile profile_email bandwidth guaranteed-bandwidth whole both 60000 rule name policy_email source-zone trust destination-zone untrust application app BT application app YouKu time-range work_time action qos profile profile_email

B. time-range work_time period-range 09: 00: 00 to 18: 00: 00 working-day traffic-policy profile profile_email bandwidth guaranteed-bandwidth whole both 60000 rule name policy_email source-zone trust destination-zone untrust application app LotusNotes application app OWA time-range work_time action qos profile profile_email

C. time-range work_time period-range 09: 00: 00 to 18: 00: 00 working-day traffic-policy profile profile_email bandwidth maximum-bandwidth whole both 60000 rule name policy_email source-zone trust destination-zone untrust application app LotusNotes application app OWA time-range work_time action qos profile profile_email

D. time-range work_time period-range 00: 00: 00 to 09: 00: 00 working-day traffic-policy profile profile_email bandwidth guaranteed-bandwidth whole both 60000 rule name policy_email source-zone trust destination-zone untrust application app LotusNotes application app OWA time-range work_time action qos profile profile_email

Answer(s): B

---

4. The two FWs are interconnected by IPSec. The display ike sa is executed in FW_A. The result is shown as following. Which of the following statements are correct? (Multiple Choices)

A. FW_B is the initiator of IKE security channel negotiation

B. FW_A is the initiator of IKE secure channel negotiation

C. SA between firewalls have not been established successfully

D. SA between firewalls has been successfully established

Answer(s): B,D

---

5. In the system view of the USG, you need to delete the sslconfig.cfg file in the hda1:/ directory. Which of the following commands can complete this operation?

A. cd: hda1:/ delete sslconfig.cfg

B. cd: hda1:/ remove sslconfig.cfg

C. cd: hda1:/ rmdir sslconfig.cfg

D. cd: hda1:/ mkdir sslconfig.cfg

Answer(s): A

---

6. The virtual system instance bound to the interface by the ip binding vpn-instance vpn-instance name is generated as the virtual system is created.

A. False

B. True

Answer(s): A

---

7. On a hot standby networking, if the peer heartbeat interface address is specified when the HRP heartbeat interface is configured, which of the following types of packets is the VGMP hello packet sent between the firewalls?

A. Broadcast packets

B. UDP packets

C. Unicast packets

D. Multicast packets

Answer(s): C

---

8. Which of the following device can detect unknown malicious files transmitted on the network in a virtual environment?

A. WAF

B. eSight

C. LogCenter

D. FireHunter

Answer(s): D

---

9. What are the load balancing algorithms supported by the Huawei USG6000 firewall?

A. Ratio

B. Weighted polling algorithm

C. Simple polling algorithm

D. Source IP hash algorithm

Answer(s): B,C,D

---

10. Which of the following statement about IKE is the correct? (Multiple choice)

A. IPSec has two negotiation modes to establish security associations. One is manual and the other is automatic IKE negotiation (isakmp).

B. IKE security mechanisms include DH Diffie-Hellman exchange and key distribution, Perfect Forward Secrecy PFS, and SHA1 encryption algorithms.

C. The aggressive mode of IKE v1 can choose to find the corresponding authentication key and finally complete the negotiation according to the IP address or Name of the negotiation initiator.

D. The NA7 traversal function deletes the UDP port number verification process during IKE negotiation and implements the discovery function of the NAT gateway device in the VPN tunnel. If the NAT gateway device is found, UDP encapsulation will be used in the subsequent IPSec data transmission.

Answer(s): A,C,D

---

11. Which of the following command express unlimited flow in the Huawei USG6000 series firewall?

A. no-limit

B. no-qos

C. no-profile

D. no-car

Answer(s): B

---

12. Which of the following VPN encapsulation protocols that do not provide encryption? (Multiple choices)

A. ESP

B. GRE

C. AH

D. L2TP

Answer(s): B,C,D

---

13. Users use SSL VPN to access intranet resources and use server authentication to authenticate users. In order to distinguish corporate users in different regions and establish different user domains for users in different regions. When a user use SSL VPN authentication, the authentication prompts that the password is incorrect.

A. The user domain was not entered when the user entered the user name.

B. The administrator has configured the wrong user domain.

C. The user entered the wrong user name and password.

D. The username and password do not exist.

Answer(s): A,B,C

---

14. A firewall device can create multiple virtual gateways. Each virtual gateway is independent and does not affect each other. Administrators can configure their own users, resources, and policies under the virtual gateway for independent management.

A. TRUE

B. FALSE

Answer(s): A

---

15. When the performance difference between servers is large, which of the following algorithms can be used for load balancing?

A. Weighted polling algorithm

B. The minimum connection algorithm

C. Simple polling algorithm

D. Source IP hash algorithm

Answer(s): A

---

16. Huawei Any Office provides an effective balance plan for the conflict between individual needs of employees and corporate policy compliance.

A. Device Compliance

B. Integrity

C. Identity and Device Identities

D. Data Privacy

Answer(s): A,C,D

---

17. As shown in the figure is the firewall hot standby networking environment. In this networking environment, which of the following commands can ensure that the device automatically adjusts the priority of the VGMP management group and automatically performs the active/standby switchover?

A. hrp ospf-cost adjust-enable

B. hrp interface GigabitEthernet 0/0/2

C. hrp preempt delay 60

D. hrp auto-sync config

Answer(s): A

---

18. Which of the following is correct about IKE? (Multiple choices)

A. IPSec use IKE negotiation SA to encrypt or verify packets.

B. IKE is a protocol carried by UDP and is the signaling protocol of IPSec.

C. IPSec must use IKE for key exchange

D. IKE negotiates security associations for IPSec and sends the established parameters and security associations to IPSec.

Answer(s): A,B,D

---

19. Which of the following information is involved in the process of the first stage main mode negotiation in IKE v1 negotiation? (Multiple Choice)

A. DH key exchanges public information

B. Both parties' identity information

C. IPSec proposal set

D. IKE proposal set

Answer(s): A,B,D

---

20. Which of the following is the possible cause of the failure?

A. The user is not assigned to the Web proxy resources.

B. The route between the gateway and intranet server is unreachable.

C. The security policy does not allow traffic from the external network to the intranet server.

D. SSL VPN is deployed on the firewall next to the one-arm deployment. You need to use NAT to map the private address of the SSL VPN gateway to public network address. The address mapping is incorrect.

Answer(s): A