HIGHER QUALITY
BETTER SERVICE

CERTTREE

QUESTION & ANSWER

Provide One Year
Free Update!

https://www.certtree.com

Exam : **JN0-533**

Title : FWV, Specialist (JNCIS-FWV)

Version : DEMO

1.Your ScreenOS device does not have a static IP address.You want to be able to access it using its FQDN.How would you implement this task?
A.Configure a domain in DNS.
B.Configure syslog.
C.Configure SNMP.
D.Configure DDNS.
Answer: D

2.You have just installed a new ScreenOS device in your network and you want only a select range of IP addresses to have administrative access to the device.Which choice will allow you to accomplish this?
A.Configure a manager IP.
B.Configure the management interface.
C.Configure a management IP on the trust interface.
D.Configure new system administrators.
Answer: A

3.A routing table contains an IBGP route for 192.168.0.0/24, a RIP route for 192.168.0.0/23, an OSPF route for 192.168.0.0/22, and a static route for 192.168.0.0/16.When the router receives traffic destined for 192.168.0.1, which route will the router use?
A.the IBGP route
B.the OSPF route
C.the RIP route
D.the static route
Answer: A

4.You are troubleshooting telnet traffic destined to IP address 10.10.10.1.You decide to run debug and want to set the flow filter.Which command will show only the telnet traffic going to the 10.10.10.1 address?
A.ssg5-serial-> set ffilter dst-ip 10.10.10.1 ssg5-serial-> set ffilter dst-port 23
B.ssg5-serial-> set ffilter dst-ip 10.10.10.1 dst-port 23
C.ssg5-serial-> set ffilter dst-port 23
D.ssg5-serial-> set ffilter dst-ip 10.10.10.1
Answer: B

5.You have enabled BGP on your ScreenOS device and configured a single EBGP peer.The CLI shows that the BGP connection is transitioning between the CONNECT and ACTIVE states, but never reaching the ESTABLISHED state.What are three reasons for this behavior? (Choose three.)
A.The peer is blocking traffic destined for TCP port 179.
B.The peer address is not configured correctly.
C.The enable statement has not been configured for the peer.
D.The peer AS number is not configured correctly.
E.BGP has not been enabled on the virtual router.
Answer: ABD

6

You want to set up a last resort route and prevent route lookups in either the source-based routing table or the destination-based routing table.What should you do?
A.Disable SIBR and create a default route in the trust-vr table using the null interface as the outgoing interface with a higher metric than other routes.
B.Disable SIBR and create a default route in the trust-vr table using the null interface as the outgoing interface with a lower metric than other routes.
C.Enable SIBR and create a default route in the SIBR table using the null interface as the outgoing interface with a higher metric than other routes.
D.Enable SIBR and create a default route in the SIBR table using the null interface as the outgoing interface with a lower metric than other routes.
Answer: C

7.You have the following BGP configuration in place to establish a session with a remote peer over your ethernet4 interface.
set vrouter trust-vr protocol bgp 65000 set vrouter trust-vr protocol bgp enable set vrouter trust-vr protocol bgp neighbor remote-as 65500 set vrouter trust-vr protocol bgp neighbor enable
Which additional statement is necessary to establish the session?
A.set interface protocol bgp enable
B.set interface ethernet4 bgp enable
C.set vrouter trust-vr protocol bgp interface ethernet4
D.set interface ethernet4 protocol bgp
Answer: D

8.You have only one public IP address available and you must allow external access to three servers on a DMZ network.Which two NAT types would allow you to accomplish your objective? (Choose two.)
A.MIP
B.VIP
C.NAT-dst
D.NAT-src
Answer: BC

9.Your ScreenOS device is configured with multiple NAT types.What is the order of precedence in this situation?
A.interface-based NAT -> VIP -> MIP -> policy-based NAT
B.VIP -> MIP -> policy-based NAT -> interface-based NAT
C.MIP -> VIP -> interface-based NAT -> policy-based NAT
D.MIP -> VIP -> policy-based NAT -> interface-based NAT
Answer: D

10.You must translate a range of public IP addresses to a range of internal IP addresses.Which two mechanisms would you use to accomplish your objective? (Choose two.)
A.MIP using masks
B.VIP using masks
C.policy-based NAT-dst

D.policy-based NAT-src
Answer: AC

11.Your ScreenOS device is using NAT.Which NAT function allows you to use a single IP address from an untrust zone to communicate to multiple IP addresses in a trust zone?
A.NAT-src with PAT enabled
B.NAT-dst with PAT enabled
C.NAT-src using a DIP pool with PAT enabled
D.NAT-dst using a DIP pool with PAT disabled
Answer: B

12.Which two statements are true about NAT? (Choose two.)
A.Managed IP is one-to-one address mapping for bidirectional access.
B.Mapped IP is one-to-one address mapping for bidirectional access.
C.Dynamic IP is the public address that can be used for external access to your Web server.
D.Dynamic IP is the public address that internal users can use to access the Internet.
Answer: BD

13.Which NAT has bidirectional translation by default?
A.NAT-src
B.NAT-dst
C.VIP
D.MIP
Answer: D

14.You are using interface-based NAT for traffic passing from the trust zone to the untrust zone.What will occur?
A.The source IP address is not translated.
B.The source IP address is translated to the trust interface IP address.
C.The network address and port translation (NAPT) is performed on the loopback interface.
D.The source IP address is translated to the untrust interface IP address.
Answer: D

15.You have configured a single-port VIP to forward HTTP traffic from the untrust interface on your ScreenOS device to an internal Web server.You have configured a policy to allow this traffic.Traffic from the untrust interface that matches this policy is unable to connect to the Web server.What is a solution to this problem?
A.You must reboot the ScreenOS device for the VIP to become active.
B.You must ensure the ScreenOS device has a route to the Web server.
C.You must ensure the Web server is directly connected to the ScreenOS device.
D.You must save the ScreenOS device configuration for the VIP to become active.
Answer: B

16.You must verify on your ScreenOS device that you have configured the correct tunnel peer and

determine which IKE proposals the remote device is sending and accepting.Which command should you use?
A.get ike gateway
B.get ike peer
C.get sa active
D.get ike active
Answer: A

17.You are building an IPsec VPN and want to authenticate and encrypt the content.Which two Phase 1/ Phase 2 (P1/P2) proposals would achieve this goal? (Choose two.)
A.P1: pre-g5-3des-sha, P2: g5-esp-3des-sha
B.P1: pre-g2-aes128-sha, P2: g5-ah-aes128-sha
C.P1: pre-g5-des-md5, P2: g5-ah-des-md5
D.P1: pre-g2-esp128-sha, P2: g2-esp-aes128-sha
Answer: AD

18.You are configuring a VPN with IKE between headquarters and a branch office that uses a dynamic public IP address.Which IKE mode should you use?
A.quick mode
B.main mode
C.aggressive mode
D.wizard mode
Answer: C

19.Which two statements are true about policy-based VPNs as compared to route-based IPsec VPNs when using ScreenOS devices? (Choose two.)
A.For policy-based IPsec VPNs, you can configure 0.0.0.0/0 as the proxy ID on both VPN gateways regardless of the security policy.
B.For route-based IPsec VPNs, you can configure 0.0.0.0/0 as the proxy ID on both VPN gateways regardless of the security policy.
C.For route-based IPsec VPNs, the proxy ID is derived from the policy.
D.For policy-based IPsec VPNs, the proxy ID is derived from the policy.
Answer: BD

20.You want to ensure that the IKE Phase 2 key is totally independent of the IKE Phase 1 key.Which IKE feature would you enable?
A.Perfect Forward Secrecy
B.Diffie-Hellman Group 5
C.Replay Protection
D.Rekey Protection
Answer: A