IT 认证电子书

质 量 更 高 服 务 更 好

Exam : **Jn0-521**

Title : Juniper FWV.Associate (JNCIA-FWV)

Version : Demo

1. Which statement accurately describes the "config rollback" feature?

A.Once the "config rollback" feature is enabled, it allows the administrator to re-apply a previously saved configuration file from flash.

B.The "config rollback" feature is enabled by default, it allows the administrator to re-apply a previously saved configuration file from flash.

C.Once the "config rollback" feature is enabled, it allows the administrator to re-apply a locked configuration file from a separate area in flash.

D.Once the "config rollback" feature is enabled, it allows the administrator to revert to the prior ScreenOS image or configuration file in the event an upgrade operation aborts.

Answer: C

2. Click the Exhibit button.

```
ssg550-> get route
IPv4 Dest-Routes for <untrust-vr> (0 entries)
----------------------------------------------------------------------
H: Host C: Connected S: Static A: Auto-Exported
I: Imported R: RIP P: Permanent D: Auto-Discovered
iB: IBGP eB: EBGP O: OSPF E1: OSPF external type 1
E2: OSPF external type 2
IPv4 Dest-Routes for <trust-vr> (11 entries)
----------------------------------------------------------------------
    ID          IP-Prefix    Interface       Gateway    P  Pref    Mtr    Vsys
----------------------------------------------------------------------
*   11         0.0.0.0/0        eth0/4       1.1.8.254   S   20      1     Root
*   10       1.1.70.0/24        eth0/3       1.1.7.254   S   20      1     Root
*   12      10.1.20.0/24        eth0/2      10.1.2.254   S   20      1     Root
*    3       10.1.1.1/32        eth0/1       0.0.0.0     H    0      0     Root
*    5       10.1.2.1/32        eth0/2       0.0.0.0     H    0      0     Root
*    7        1.1.7.1/32        eth0/3       0.0.0.0     H    0      0     Root
*    9        1.1.8.1/32        eth0/4       0.0.0.0     H    0      0     Root
*    2       10.1.1.0/24        eth0/1       0.0.0.0     C    0      0     Root
*    4       10.1.2.0/24        eth0/2       0.0.0.0     C    0      0     Root
*    6        1.1.7.0/24        eth0/3       0.0.0.0     C    0      0     Root
*    8        1.1.8.0/24        eth0/4       0.0.0.0     C    0      0     Root
```

In the exhibit, which interface would be used to forward traffic to host 1.1.7.5?

A.e0/1

B.e0/2

C.e0/3

D.e0/4

Answer: C

3. Which ScreenOS WebUI button reorders policies?

A.Shift

B.Move

C.Reorder

D.Transfer

Answer: B

4. Which type of NAT is performed when you implement interface-based NAT?

A.source IP address translation

B.destination IP address translation

C.source IP and port address translation

D.destination IP and port address translation

Answer: C

5. Click the Exhibit button.

In the exhibit, which two forms of address translation would have generated the output shown? (Choose two.)

A.MIP

B.NAT-src with no DIP

C.Interface-based translation

D.NAT-src with a DIP, fixed-port disabled

Answer: BC

6. You are looking at the event log of the responding device and it says,

"Rejected an initial Phase 1 packet from an unrecognized peer gateway"

What are three likely reasons for the failure? (Choose three.)

A.The peer ID is misconfigured.

B.The default gateway is missing.

C.The preshare keys are mismatched.

D.The gateway address is misconfigured.

E.The outgoing interface is misconfigured.

Answer: ADE

7. Which command would you run to check IPSec Phase 1 active status?

A.get sa

B.get event 427

C.get sa active

D.get ike cookie

Answer: D

8. By default, from which hardware component is the startup copy of the ScreenOS loaded?

A.NVRAM

B.TFTP server

C.internal flash

D.PCMCIA card

Answer: C

9. A ScreenOS firewall has the correct interfaces addressed and active. A policy is written allowing interzone FTP traffic from a directly connected client. But the traffic does not cross the firewall from the client to the server.

What is the most likely problem with the firewall?

A.The ScreenOS firewall has no physical connection to the FTP server.

B.The ALG option on the ScreenOS firewall has not been enabled for FTP traffic.

C.The ScreenOS firewall does not have a route defined to the FTP servers' subnet.

D.The ScreenOS firewall does not have a route defined to the FTP clients subnet.

Answer: C

10. When a firewall receives the first packet in a series, what will it immediately do?

A.Check its route table.

B.Check its session table.

C.Determine if traffic is crossing zones.

D.Verify that it is not malformed or a fragment.

Answer: D

11. In the packet forwarding decision process, how is the second packet handled differently than the first in a series of allowed interzone packets?

A.The second packet causes an ARP query.

B.The second packet is checked against the policy table.

C.The second packet is forwarded without a sanity check.

D.The second packet is forwarded without checking the route table.

Answer: D

12. You are configuring an interface in the untrust zone with an IP address, telnet enabled, and WebUI management.

Which sequence of steps must be performed to make the interface operational at the end of the configuration sequence?

A.Assign the interface to a zone, define the IP address, enable Web and telnet services.

B.Assign the interface to a zone, define the IP address, accept default management services.

C.Assign the interface to a virtual router, define the IP address, enable Web and telnet services.

D.Assign the interface to a zone, define the IP address, define a manage IP address, accept default management services.

Answer: A

13. What will change the root admin password?

A.set admin password

B.set root-admin password

C.set admin password

D.set admin user password

Answer: A

14. Telnet management has been enabled on an interface in the untrust zone.

What else should be completed to limit telnet access to the ScreenOS device from trusted management

PCs?

A.Define a permitted IP address.

B.Define a policy from trust to untrust.

C.Define a trusted IP in the address table.

D.Define a manage IP address on this interface.

Answer: A

15. Which statement is correct regarding administrator privileges?

A.Any administrator can change their privileges on an as-needed basis.

B.Administrator privileges can only be established and changed by the root administrator.

C.Administrator privileges can be established and changed by the root and all-privilege administrator.

D.Administrator privileges can only be established by the root and can be changed by the root and

all-privilege administrator.

Answer: B

16. What is the purpose of the "Permitted IP" address on a ScreenOS device?

A.It defines a list of addresses that are trusted to perform management on the ScreenOS device.

B.It is used in policy rules to determine which user traffic is allowed through the ScreenOS device.

C.It defines which range of addresses that can access devices connected to the ScreenOS device.

D.It is the address that an external device uses to gain management access to a ScreenOS device.

Answer: A

17. What is the purpose of the "Manage-IP" address on a ScreenOS device?

A.It defines a list of addresses that are trusted to perform management on the ScreenOS device.

B.It is used in policy rules to determine which device is allowed to manage the ScreenOS device.

C.It is the address that an external device uses to gain management access to a ScreenOS device.

D.It defines a list of device addresses that can manage the ScreenOS device without being authenticated prior to session establishment.

Answer: C

18. An operational firewall needs a configuration loaded and executed while it is passing user data.

Which CLI command will perform this process without interrupting traffic?

A.save config from tftp 1.1.7.250 15June06.cfg to flash

B.save config from tftp 1.1.7.250 15June06.cfg to ram

C.save config from tftp 1.1.7.250 15June06.cfg merge

D.save config from tftp 1.1.7.250 15June06.cfg to flash

Answer: C

19. When configuring a firewall in a critical environment where a local backup configuration is quickly needed, what should be completed on a periodic basis?

A.Execute exec config rollback.

B.Execute save config to last-known-good.

C.Execute save regularly or create a script that does this.

D.Execute save software from flash to pcmcia .

Answer: B

20. When managing a ScreenOS device using the WebUI and performing an image upgrade, from which hardware component will the ScreenOS image be loaded?

A.TFTP server

B.PC local disk

C.internal flash

D.Compact Flash Card

Answer: B

21. When performing an image upgrade using the CLI, which three locations would be a source for this

image? (Choose three.)

A.FTP server

B.TFTP server

C.internal flash

D.PC local disk

E.Compact Flash Card

Answer: BCE

22. In the command, save config from tftp 1.1.7.250 abcd.cfg merge, which function does the merge parameter specify?

A.The config file from the TFTP server will replace the configuration in RAM.

B.The config file from the TFTP server will replace the startup configuration file in internal flash.

C.The merge parameter is not valid for TFTP files, it is only valid for configuration files stored in internal flash.

D.The config file from the TFTP server will be combined with the configuration file in RAM and the combined result will be saved in internal flash.

Answer: D

23. By default, where are changes stored when a save command is issued from the CLI during a management session?

A.NVRAM

B.internal flash

C.PCMCIA card

D.Compact Flash Card

Answer: B

24. When changes are made to the running config during a WebUI management session, to what external hardware component can the changes be saved?

A.FTP server

B.TFTP server

C.PC local disk

D.Compact Flash Card

Answer: C

25. Which process describes how an addressed physical interface is moved into a Layer 2 zone?

A.Place the required interface into the VLAN zone.

B.Place the required interface into L2 zones such as V1-Trust, V1-Untrust

C.Remove the interface from the L3 zone such as Trust and place it into a L2 zone such as V1-Trust

D.Remove the address from the interface, remove the interface from the L3 zone, and then place interface in the L2 zone.

Answer: D

26. Which command is used when configuring web management on the VLAN1 interface for a client connected to an e3 interface in the DMZ zone?

A.set int eth3 manage web

B.set zone v1-dmz manage web

C.set int dmz zone manage web

D.set int VLAN1 zone dmz manage web

Answer: B

27. A ScreenOS firewall is running in transparent mode. The firewall receives a packet which has no entry in its forwarding table.
What will the firewall do?

A.Flood out all ports.

B.Check its route table for interzone destination.

C.Perform a policy lookup to determine the interfaces to which the source address is permitted, and flood the packet out of those interfaces.

D.Perform a policy lookup to determine the zones to which the source address is permitted, and flood the packet out the interfaces bound to those zones.

Answer: D

28. What is the purpose of the VLAN1 interface?

A.It provides policy-based NAT for 802.1Q VLANs.

B.It provides an interface that can be used with 802.1Q VLANs in transparent mode.

C.It provides the ScreenOS device with a routable IP address while operating in route mode.

D.It provides an interface that can be used to remotely manage the ScreenOS device while operating in

transparent mode.

Answer: D

29. Which two statements are true in regards to a ScreenOS firewall in transparent mode? (Choose two.)

A.VPNs can terminate to the VLAN1 interface IP address.

B.Static routes must be configured if multiple virtual routers are going to be used.

C.It can be installed in a network without the requirement to reconfigure IP addressing schemes.

D.You must use the console port to manage the device as you cannot manage the device using an

Ethernet port.

Answer: AC

30. What are two benefits of configuring a ScreenOS device in transparent mode? (Choose two.)

A.There is no need to reconfigure the IP addresses of routers or protected servers.

B.There is no need to create MIPs or VIPs for incoming traffic to reach protected servers.

C.Policies are easier to create since you do not have to include source and destination IP addresses.

D.The product can support more VPNs and obtain greater throughput because there is less overhead to

manage.

Answer: AB