Juniper

Exam JN0-740

ACX, Specialist (JNCIS-ACX)

Version: 6.0

[Total Questions: 270]

Question No : 1

What is the initial default username and password for all ScreenOS devices?

A. administrator/password
B. root/password
C. netscreen/netscreen
D. admin/netscreen1

Answer: D

Question No : 2

Which operating system is used on a NetScreen device?

A. IOS
B. Junos
C. FreeBSD
D. ScreenOS

Answer: A

Question No : 3

When is NAT used?

A. for Layer 2 switching
B. for MPLS VPNs
C. to translate between IP addresses
D. for secure tunnels

Answer: B

Question No : 4

What is a zone used for?

A. to bundle interfaces together for redundancy
B. to bundle interfaces sharing identical security requirements
C. to provide a tunneled connection across a network
D. to protect against spam attacks

Answer: D

Question No : 5

Which two devices run ScreenOS software? (Choose two.)

A. NetScreen-5200
B. NetScreen-5400
C. SRX240
D. MX480

Answer: C,D

Question No : 6

Which security feature provides secure tunnels across a public network?

A. dynamic routing
B. Web filtering
C. IPsec
D. firewall filters

Answer: A

Question No : 7

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

A. ROM
B. NVRAM
C. TFTP server
D. Internal Flash

E. PCMCIA Card

Answer: D

Question No : 8

Using the CLI, if the startup copy of the ScreenOS on a NS-204 is corrupted, from which two (2) alternate locations can an image be loaded?

A. ROM
B. TFTP server
C. Internal Flash
D. PCMCIA Card
E. Compact Flash Card

Answer: B,E

Question No : 9

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

Question No : 10

Using the CLI, if the startup copy of the ScreenOS is corrupted, from which location can an image be loaded?

A. TFTP server
B. internal flash
C. PCMCIA card
D. Compact Flash Card

Answer: A

Question No : 11

In the packet flow decision process, which pair identifies interzone traffic?

A. source and destination MAC
B. source and destination interface
C. source and destination TCP port
D. source and destination IP address

Answer: B

Question No : 12

A ScreenOS firewall has one interface in the user zone and one interface in the servers zone. Both interfaces are addressed and active. The configured policy allows user traffic from the user zone to the FTP server in the servers zone, 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 server's subnet.
D. The ScreenOS firewall does not have a route defined to the FTP client's subnet.

Answer: C

Question No : 13

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

Question No : 14

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

Question No : 15

In the flow decision process, the system has found a route entry matching the packet destination IP.

Which pair will identify the policy that is applied to this packet?

A. source and destination MAC
B. source and destination interface
C. source and destination TCP port
D. source and destination IP address

Answer: B

Question No : 16

Assuming factory default settings, which statement describes the minimum requirements for WebUI management access?

A. Connect a PC addressed on the 192.168.1.0 subnet to any interface, open a browser and access 192.168.1.1

B. Terminate the bootup sequence from the console device, open a browser on the console device and access 192.168.1.1
C. Connect a PC addressed on the 192.168.1.0 subnet to the lowest numbered interface, open a browser and access 192.168.1.1
D. Using the CLI, define an IP address on a physical interface, connect a PC to the interface and open a browser to the interface address
E. Using the CLI, assign an IP address to the VLAN1 interface, connect a PC to any interface and open a browser to the VLAN interface address

Answer: C

Question No : 17

When configuring the Untrust interface with an IP address and enabling Telnet 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
E. Assign the interface to a virtual router, define the IP address, define a manage IP address, enable Web and Telnet services

Answer: A

Question No : 18

Assuming factory default settings, which statement describes the minimum requirements for WebUI management access?

A. Connect a PC addressed on the 192.168.1.0 subnet to any interface, open a browser and access 192.168.1.1
B. Terminate the bootup sequence from the console device, open a browser on the console device and access 192.168.1.1
C. Connect a PC addressed on the 192.168.1.0 subnet to the product-specific interface for the device, open a browser and access 192.168.1.1

D. Using the CLI, define an IP address on a physical interface, connect a PC to the interface and open a browser to the interface address.

Answer: C

Question No : 19

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

Question No : 20

What will change the root admin password?

A. set admin password <password>
B. set root-admin password <password>
C. set admin <name> password <password>
D. set admin user <name> password <password>

Answer: A

Question No : 21

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

What else should be configured 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

Question No : 22

Assuming factory default settings, which statement describes the minimum requirements for WebUI management access to the SSG 5?

A. Connect a PC addressed on the 192.168.1.0 subnet to any interface, open a browser and access 192.168.1.1.
B. Terminate the bootup sequence from the console device, open a browser on the console device and access 192.168.1.1.
C. Connect a PC addressed on the 192.168.1.0 subnet, to the highest numbered interface and open a browser and access 192.168.1.1.
D. Using the CLI, define an IP address on a physical interface, connect a PC to the interface and open a browser to the interface address.

Answer: C

Question No : 23

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

Question No : 24

What is the purpose of the 'Permitted IP' address on a NetScreen device?

A. It defines which range of address can access devices connected to the NetScreen
B. It defines a list of addresses that are trusted to perform management on the NetScreen
C. It is used in policy rules to determine which user traffic is allowed through the NetScreen
D. It is the address that an external device uses to gain management access to a NetScreen
E. It defines a list of devices whose traffic can pass through the NetScreen without being authenticated

Answer: B

Question No : 25

Which three (3) statements are correct regarding tasks that can be performed only by the Root administrator?

A. reset command
B. unset all command
C. ScreenOS upgrade
D. traceroute command
E. On-line asset recovery

Answer: B,C,D

Question No : 26

What is the purpose of the 'Manage-IP' address on a NetScreen device?

A. It defines which range of address can access devices connected to the NetScreen
B. It defines a list of addresses that are trusted to perform management on the NetScreen
C. It is used in policy rules to determine which device is allowed to manage the NetScreen
D. It is the address that an external device uses to gain management access to a NetScreen
E. It defines a list of device addresses that can manage the NetScreen without being authenticated prior to session establishment