Juniper

Exam JN0-533

FWV, Specialist (JNCIS-FWV)

Version: 6.1

[Total Questions: 110]

Question No : 1

Which two statements are true about redundant interfaces on a ScreenOS device? (Choose two.)

A. With two interfaces in a redundant interface, only one link is primary at any given time.
B. On high-end models with multi-ASIC cards, redundant Ethernet ports must be in the same ASIC group.
C. With two interfaces in a redundant interface, both links pass traffic at the same time.
D. On high-end models with multi-ASIC cards, redundant Ethernet ports can be used on different ASIC groups.

Answer: A,B

Question No : 2

What is an aggregate interface?

A. An aggregate interface binds two physical interfaces together to create a redundant interface.
B. An aggregate interface binds two or more physical interfaces that share the traffic load.
C. An aggregate interface is the management interface.
D. An aggregate interface is used for VPN tunnels.

Answer: B

Question No : 3

You want to centralize the logging for all your ScreenOS devices and you must be able to synchronize the log. Which two actions would you perform to accomplish this? (Choose two.)

A. Enable logging to the console.
B. Enable logging to syslog.
C. Enable NTP and set to UTC/GMT time.
D. Enable logging to the USB.

Answer: B,C

Question No : 4

Policy-based routing consists of which three ScreenOS objects? (Choose three.)

A. extended access lists
B. match groups
C. action groups
D. address books
E. security policy

Answer: A,B,C

Question No : 5

What is required to route traffic from one virtual system to another virtual system?

A. Configure the same dynamic routing protocol in each virtual system.
B. Configure a virtual system profile with a shared forwarding table.
C. Configure a private virtual router in each virtual system.
D. Configure a shared root-level virtual router.

Answer: D

Question No : 6

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

Question No : 7

You have configured deep-packet inspection on a ScreenOS device. You have not modified the default threshold values. The device detects a single session that matches an attack.

Which two actions can you configure the device to take? (Choose two.)

A. Close the connection and disallow further connections from the client to the server.
B. Close the connection and rate-limit further connections to the server.
C. Discard all additional packets related to the session.
D. Send a TCP RST message to both the client and server.

Answer: C,D

Question No : 8

-- Exhibit --

NSPROD1(M)-> get nsrp ha-link

total_ha_port = 2

probe on ha-link is disabled

unused channel: ethernet8 (ifnum: 11) maC. 0010db1d1e8b statE. down

unused channel: ethernet7 (ifnum: 10) maC. 0010db1d1e8a statE. down

ha control link not available

ha data link not available

ha secondary path link not available

-- Exhibit --

Referring to the exhibit, both clustered devices are in a master state.

What is the cause of this situation?

A. The cluster is not configured for NSRP.
B. The cluster is in the process of failing over from the primary node to the secondary node.
C. Probes on the HA links have been disabled, causing the HA links to go down.
D. The control and the data link is down.

Answer: D

Question No : 9

Click the Exhibit button.

```
ns5-> get session

if 2(nspflag 800801):192.168.1.11/49237->74.125.235.48/443,6,a4badbf6bc41,sess token 3,vlan 0,tun 0,vsd 0,route
1,wsf 6
 if 8(nspflag 10800800):173.209.131.114/1034<-74.125.235.48/443,6,00222d52786c,sess token 4,vlan 0,tun 0,vsd
0,route 7,wsf 2
id 1568/s**,vsys 0,flag 00000000/0000/0001,policy 1,time 26, dip 2 module 0
 if 2(nspflag 800801):192.168.1.113/53514->123.176.112.241/80,6,842b2b91c303,sess token 3,vlan 0,tun 0,vsd
0,route 1,wsf 0
 if 8(nspflag 10800800):173.209.131.114/2120<-123.176.112.241/80,6,00222d52786c,sess token 4,vlan 0,tun 0,vsd
0,route 7,wsf 2
id 1571/s**,vsys 0,flag 00000000/0000/0001,policy 1,time 178, dip 2 module 0
```

Referring to the exhibit, what does the log show?

A. The device is using VIP.
B. The device is using DIP ID 4.
C. The device is using source NAT.
D. The device is using destination NAT.

Answer: C

Question No : 10

-- Exhibit --

ssg5-> get conf | include syn

set zone untrust screen syn-flood attack-threshold 625

set zone untrust screen syn-flood alarm-threshold 250

set zone untrust screen syn-flood timeout 20

set zone untrust screen syn-flood queue-size 1000

set zone untrust screen syn-flood

set flow syn-proxy syn-cookie

-- Exhibit --

A host in the untrust zone sends 1000 SYN packets in a single second to a host in your trust zone destined for port 80.

Referring to the exhibit, which statement describes the behavior of the ScreenOS device?

A. It will maintain this state for all 1000 connection attempts.
B. It will begin to drop the SYN packets.
C. It will block further connection attempts from this host for 20 seconds.
D. It will reply with SYN-ACK packets.

Answer: D

Question No : 11

What is a zone?

A. a set of rules that controls traffic from a specified source to a specified destination using a specified service
B. a collection of subnets and interfaces sharing identical security requirements
C. a method of providing a secure connection across a network
D. a tool to protect against DoS attacks

Answer: B

Question No : 12

What are two advantages for using the count parameter on a security policy? (Choose two.)

A. to see any NAT traffic drops for that policy
B. to see how many times users log in to the ScreenOS device
C. to count the total number of bytes of traffic for that policy
D. to see if the policy is temporarily not being used

Answer: C,D

Question No : 13

Policy-based routing (PBR) policies can be bound to which three ScreenOS objects? (Choose three.)

A. virtual routers
B. interfaces
C. zones
D. security policies
E. virtual system

Answer: A,B,C

Question No : 14

What are three valid states for an NSRP member? (Choose three.)

A. backup
B. feasible successor
C. ineligible
D. master
E. standby

Answer: A,C,D

Question No : 15

-- Exhibit --

SSH V2 is active

ns5gt-> get int et1

Interface ethernet1:

description ethernet1

number 2, if_info 176, if_index 0, mode nat

link up, phy-link up/full-duplex

status change:1, last change:02/06/1997 18:02:32

vsys Root, zone Trust, vr trust-vr

dhcp client disabled

PPPoE disabled

admin mtu 0, operating mtu 1500, default mtu 1500

*ip 192.168.1.1/24

*manage ip 192.168.1.1,

route-deny disable

pmtu-v4 disabled

ping enabled, telnet enabled, SSH enabled, SNMP enabled

web enabled, ident-reset disabled, SSL enabled

SSH is enabled

SSH is ready for connections

Maximum sessions: 3

Active sessions: 3

-- Exhibit --

You are the administrator of a NetScreen 5GT. The system administrator cannot use SSH to log in to the NetScreen 5GT. Referring to the exhibit, what is the problem?

A. Interface eth1 does not permit logins using SSH.
B. SSH is not enabled on the NetScreen 5GT.
C. Interface eth1's link status is down.
D. The maximum SSH session has been used.

Answer: D

Question No : 16

You want to enable IPv6 on your ScreenOS device.

Which command should you use to accomplish this goal?

A. set envar ipv6=enable
B. set ipv6 enable
C. set envar ipv6=yes
D. set ipv6 yes

Answer: C

Question No : 17

When you create a new virtual system, which zone is automatically created within the vsys-specific VR?

A. trust zone
B. untrust zone
C. shared zone
D. null zone

Answer: A

Question No : 18

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: A,C

Question No : 19

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

Question No : 20

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

Question No : 21

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

Question No : 22