# Testpassport Q&A

*La meilleure qualité le meilleur service*

**Exam** : **JN0-531**

**Title** : FWV, Specailist(JNCIS-FWV)

**Version** : Demo

1. Which two statements are correct regarding NHTB? (Choose two.)

A. The NHTB table can be viewed with the command get nhtb.

B. The NHTB table can be viewed with the command get interface <tunnel interface>.

C. The NHTB table can be viewed with the command get interface <physical interface>.

D. NHTB is enabled automatically when multiple VPNs are bound to a single tunnel interface.

Answer: BD

2. Which two statements are true regarding the use of dialup VPNs? (Choose two.)

A. They are initiated only by the remote host PC.

B. They can only be connected to the trust zone on a ScreenOS device.

C. They are configured so that the first IKE message will always have the SA proposal list.

D. They can be used as an alternative to connect remote users when a ScreenOS device has reached the maximum number of LAN-to-LAN tunnels.

Answer: AC

3. Your ScreenOS device has come under a SYN flood attack. In the logs, which severity level would you search to see this event?

A. Alert

B. Critical

C. Warning

D. Emergency

Answer: D

4. Which command will show address translation for sessions that have ended?

A. snoop

B. get session

C. get log traffic

D. get dbuf stream

Answer: C

5. Which item in a virtual system is shared by default?

A. trust zone in the trust-vr

B. trust zone in the untrust-vr

C. untrust zone in the trust-vr

D. untrust zone in the untrust-vr

Answer: C

6. What should you configure to insure an HA cable failure does not result in both devices attempting to become master?

A. failover count

B. secondary path

C. monitor threshold

D. heartbeat threshold

Answer: B

7. What will happen if you type the command unset protocol vrouter trust-vr protocol ospf?

A. OSPF stops running, but the OSPF configuration is left intact.

B. All OSPF configuration parameters are removed from the vrouter only.

C. All OSPF configuration parameters are removed from all interfaces in the vrouter.

D. All OSPF configuration parameters are removed from the vrouter and from all interfaces in the vrouter.

Answer: D

8. To which three ScreenOS components can a policy-based routing policy be bound? (Choose three.)

A. zone

B. policy

C. interface

D. virtual router

E. virtual system

Answer: ACD

9. Which ScreenOS CLI command is necessary for configuring IGMP on interface ethernet0/1?

A. set igmp interface ethernet0/1

B. set multicast interface ethernet0/1

C. set interface ethernet0/1 igmp router

D. set igmp interface ethernet0/1 enable

Answer: C

10. Which command is used to verify that IGMP is running correctly?

A. get route igmp

B. get igmp query

C. set igmp query interface e0/1

D. exec igmp interface e0/1 query

Answer: D

11. Which CLI command identifies the multicast sources visible to your ScreenOS device?

A. get route pim

B. get igmp source all

C. exec pim interface all query

D. get vrouter trust-vr protocol pim

Answer: D

12. Click the Exhibit button.

```
SSG_5->get vrouter trust protocol pim mroute
trust-vr - PIM-SM routing table
------------------------------------------------------------------------------
Register - R, Connected members - C, Pruned - P, Pending SPT Alert - G
Forward - F, Null - N , Negative Cache - E, Local Receivers - L
SPT - T, Proxy-Register - X, Imported - I, SGRpt state - Y, SSM Range Group - S
Turnaround Router - K
------------------------------------------------------------------------------
Total PIM-SM mroutes: 2
(*, 236.1.1.1)    RP 20.20.20.10       01:54:20/-          Flags: LF
Zone                : Untrust
Upstream            : ethernet1/2       State           : Joined
RPF Neighbor        : local             Expires         : -
Downstream          :
ethernet1/2 01:54:20/-          Join          0.0.0.0           FC
(10.10.10.1/24, 238.1.1.1)        01:56:35/00:00:42  Flags: TLF  Register Prune
Zone                : Trust
Upstream            : ethernet1/1       State           : Joined
RPF Neighbor        : local             Expires         : -
Downstream :
ethernet1/2 01:54:20/-          Join          236.1.1.1         20.20.20.200 FC
```

In the exhibit, what is the source IP address of the multicast traffic?

A. 236.1.1.1

B. 10.10.10.1

C. 20.20.20.10

D. 20.20.20.200

Answer: B

13. During main mode negations a failure has occurred while using IKE certificates.

Which message pair would you review to troubleshoot this failure?

A. messages 1 & 2

B. messages 2 & 3

C. messages 3 & 4

D. messages 5 & 6

Answer: D

14. Which two item pairs are exchanged during Phase 2 negotiations? (Choose two.)

A. proxy-id, SA proposal list

B. IKE cookie, SA proposal list

C. hash [ID + Key], DH key exchange

D. SA proposal list, optional DH key exchange

Answer: AD

15. What must be enabled to protect Phase 2 key exchanges?

A. Phase 1 PFS

B. Phase 2 SHA

C. Phase 2 3-DES

D. Phase 2 DH key exchange

Answer: D

16. Which three statements are true regarding IKE Phase 1? (Choose three.)

A. Placing the SA proposal list in message 1 is an option.

B. The digital certificate is used to decrypt the session key.

C. The DH key exchange is used to validate the session key.

D. The DH key exchange and digital certificates are both optional.

E. The proxy-id is used to determine which SA is referenced for the VPN.

Answer: ABC

17. What must be configured differently for a route-based VPN and a policy-based VPN?

A. proxy-id

B. proposals

C. remote gateway type

D. binding the tunnel interface

Answer: D

18. You have configured the following on your device.

```
set address trust MyPC 10.1.1.5/32
set address untrust CorpNet 10.10.0.0/16
set policy from trust to untrust MyPC CorpNet any permit
set int tunnel.1 zone untrust
set int tunnel.1 ip unnumbered int bgroup1
set ike gateway GW address 1.1.1.1 outgoing-interface e0/1 preshare Secret sec-level standard
set vpn VPN gateway GW sec-level standard
```

The VPN is not working properly. What is the problem?

A. The policy needs to have the action tunnel.

B. The VPN needs to be bound to the tunnel interface.

C. The tunnel interface needs to be placed in the trust zone.

D. The tunnel interface needs to be associated with the interface in the untrust zone.

Answer: B

19. You create a policy-based VPN, and select an address group for the source address.

What will be the source component of the proxy-id seen by the remote security gateway?

A. the default 0.0.0.0/0

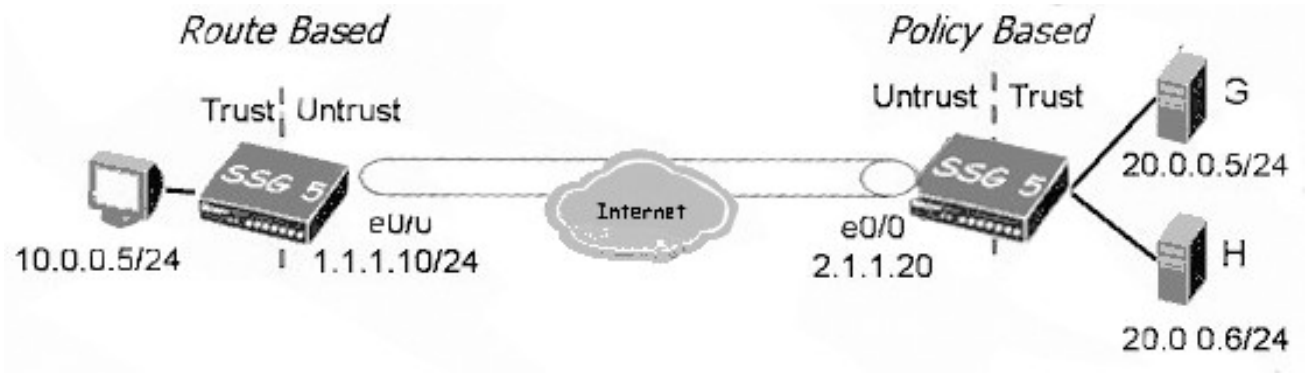
B. the last member of the address group

C. the first member of the address group

D. the subnet that contains all addresses in the address group

Answer: A

20. Click the Exhibit button.




In the exhibit, the route-based VPN on the SSG 5 needs to configured to allow access only from your PC to Server G. The SSG 550 is configured with a policy-based VPN from Server G to your PC's host address.

Assume the gateways are static.

Which proxy-id must be configured?

A. Local: 10.0.0.5/24Remote: 20.0.0.5/24

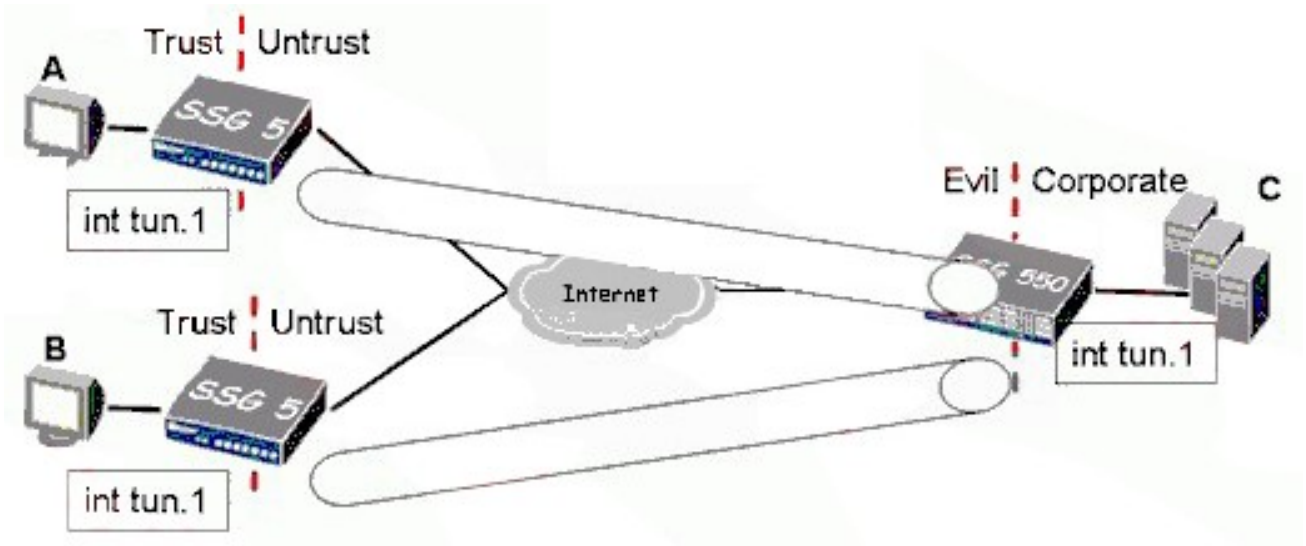
B. Local: 10.0.0.5/32Remote: 20.0.0.5/32

C. Local: 1.1.1.250/32Remote: 4.4.4.250/32

D. Local: 1.1.1.250/24Remote: 4.4.4.250/24

Answer: B

21. Click the Exhibit button.




In the exhibit, the hub and spoke VPN uses route-based VPNs.

What is the minimum number of policy rules required to establish full, bi-directional communications

between all locations?

A. 0

B. 3

C. 4

D. 6

Answer: A

22. How many tunnels would need to be created to build a full mesh between 10 VPN devices?

A. 10

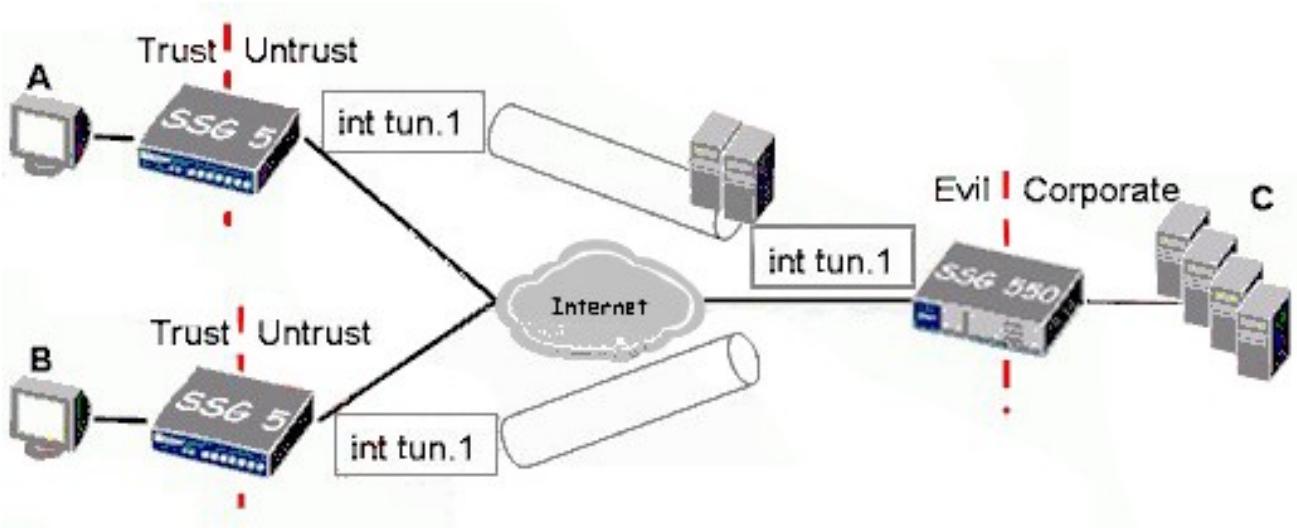
B. 20

C. 45

D. 100

Answer: C

23. Click the Exhibit button.




In the exhibit, the hub and spoke VPN uses route-based VPNs and has intra-zone blocking enabled on the Evil zone.

What is the minimum number of policy rules required to establish full, bi-directional communications between all locations?

A. 3

B. 4

C. 6

D. 7

Answer: D

24. You have implemented a hub and spoke VPN. On the hub, there are two tunnel interfaces, one to each spoke. Both tunnel interfaces are in the same zone.

Which two configuration options will control traffic between the spokes? (Choose two.)

A. Configure the common zone to block inter-zone traffic.

B. Configure the common zone to block intra-zone traffic.

C. Configure each tunnel interface to block intra-zone traffic.

D. Configure one of the tunnel interfaces in a different zone a set policies.

Answer: BD

25. Which two statements regarding NHTB are correct? (Choose two.)

A. If the spoke device is not a ScreenOS device, manual configuration of NHTB is required on the hub.

B. If the spoke device is not a ScreenOS device, manual configuration of NHTB is required on the spoke.

C. When configuring routing on a spoke device with one tunnel interface the route to the tunnel interface does not require a routing gateway address.

D. When configuring routing on a hub device with one tunnel interface terminating multiple VPN spokes, the route to the tunnel interface does not require a routing gateway address.

Answer: AC

26. A VPN tunnel that uses a CA certificate will not become active.

What would be causing this problem?

A. The CA certificate has been revoked.

B. The devices are not synced with the NTP server.

C. The device certificates were generated before the CRL was downloaded thus making them invalid.

D. The CRL has been downloaded, but the certificates have a CDP extension thus making them invalid.

Answer: B

27. A VPN tunnel that uses a CA certificate has failed Phase 1 negotiations. The peer's certificate has been rejected.

What would be causing this problem?

A. The CA certificate has been revoked.

B. One of the peering devices are not synced with the NTP server.

C. The device certificates were generated before the CRL was downloaded thus making them invalid.

D. The CRL has been downloaded, but the certificates have a CDP extension thus making them invalid.

Answer: B

28. Which three items do you need to download and install on your ScreenOS device for IKE gateways to be able to use digital certificates without OCSP? (Choose three.)

A. the CRL list

B. the SCEP list

C. a local certificate

D. the CA public key certificate

E. the CA private key certificate

Answer: ACD

29. What do you need to change in your VPN configuration to use certificates for authentication?

A. Replace the preshared key with the certificate name.

B. Select PFS in Phase 2, then select the certificate to be used.

C. Use a custom set of Phase 1 proposals, all beginning with rsa-.

D. Use a custom set of Phase 2 proposals, all beginning with rsa-.

Answer: C

30. You have created a VPN to a dynamic peer.

Which two configured parameters must match? (Choose two.)

A. static side peer-id

B. dynamic side local-id

C. static side IP address

D. dynamic side IP address

Answer: AB