KillTest

Higher Quality, Better Service!

Q&A

http://www.killtest.com

We offer free update service for one year.

Exam : **JN0-522**

Title : FXV,Associate (JNCIA-FWV)

Version : Demo

1.Address book entries identify hosts and networks by their location in relation to what?
A. Network entries in the routing table
B. A listing of addresses in the ARP table
C. Security zones on the firewall
D. An interface on the firewall
Answer: C

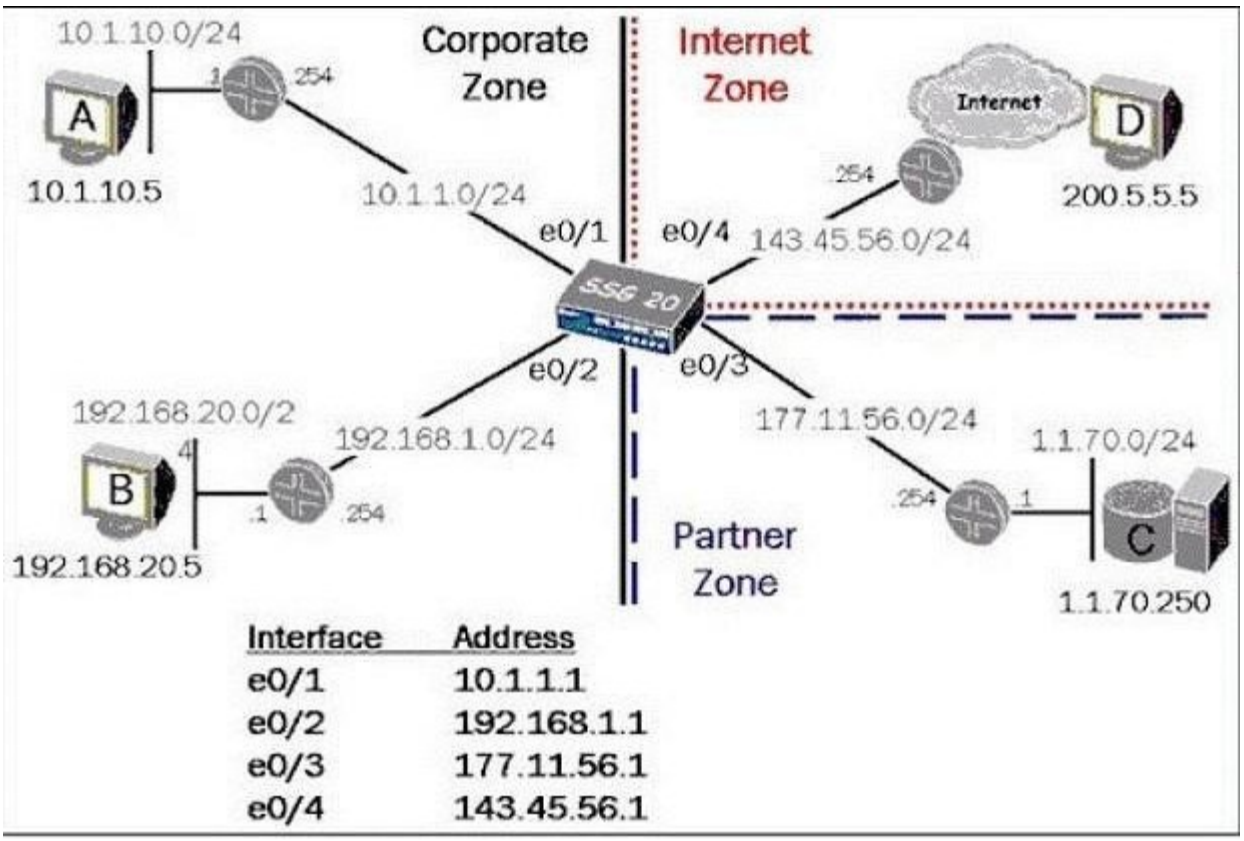
2.Which two options allow proper configuration of NAT-dst.? (Choose two.)
A. A static route to the appropriate subnet using a private interface as the outbound interface
B. The default address book entry of "any" in the internal zone
C. The default address book entry of "any" in the external zone
D. An address book entry for the address to be translated in the internal zone
Answer: AD

3.Which three options allow proper configuration of NAT-dst? (Choose three.)
A. The default address book entry of "any" in the external zone
B. An address book entry for the address to be translated in the internal zone
C. A static route to the appropriate subnet using a private interface as the outbound interface
D. The default address book entry of "any" in the internal zone
E. A secondary address on one of the interfaces in the internal zone
Answer: BCE

4.Which two protocols are defined in the IPSec standard? (Choose two.)
A. ESP
B. IKE
C. GRE
D. AH
Answer: AD

5.What is the purpose of the "Permitted IP" address on a ScreenOS device?
A. It is used in policy rules to determine which user traffic is allowed through the ScreenOS device
B. It defines a list of addresses that are trusted to perform management on the ScreenOS device
C. It is the address that an external device uses to gain management access to a ScreenOS device
D. It defines which range of addresses that can access devices connected to the ScreenOS device
Answer: B

6.In the exhibit, which routing command would allow Host A to communicate with host C?



A. Set route 0.0.0.0/0 int e0/3 gateway 177.11.56.254
B. Set route 1.1.70.0 interface e0/3 gateway 177.11.56.254
C. Configure route 1.1.70.0/24 gateway 177.11.56.254 int e0/3
D. Set route 1.1.70.0/24 interface e0/3 gateway 177.11.56.254
Answer: D

7.What are two benefits of configuring a ScreenOS device in transparent mode? (Choose two.)
A. Policies are easier to create since you do not have to include source and destination IP addresses
B. There is no need to create MIPs or VIPs for incoming traffic to reach protected servers
C. The product can support more VPNs and obtain greater throughput because there is less overhead to manage
D. There is no need to reconfigure the IP addresses of routers or protected servers
Answer: BD

8.Which statement accurately describes the "config rollaback" feature?
A. Once the "Config rollback" feature is enabled, it allows the administrator to re-apply a previously saved configuration file from the flash
B. Once the "Config rollback" feature is enabled, it allows the administrator to revert to the prior ScreenOS image or configuration file in event an upgrade operation aborts
C. The "Config rollback" feature is enabled by default, it allows the administrator to re-reply a previously saved configuration file from flash
D. Once the "Config rollback" feature is enabled, it allows the administrator to re-apply a locked configuration file from a separate area in flash

Answer: D

9.See the exhibit.
Which order of policies would allow all five policies to be effective in matching traffic?

```
ssg-550-> get policy
Total regular policies 5, Default deny.
ID From     To     Src-address    Dst-address    Service Action State   ASTLCB
 1 Private  Public Any            1.1.70.0/24    ANY     Permit enabled -----X
 2 Private  Public 10.1.10.16/28  1.1.70.200/32  FTP     Permit enabled -----X
 3 Private  Public 10.1.10.18/32  1.1.70.200/32  ANY     Permit enabled -----X
 4 Private  Public Any            1.1.70.100/24  HTTP    Deny   enabled -----X
 5 Private  Public 10.1.10.0/24   1.1.70.0/24    FTP     Deny   enabled -----X
```

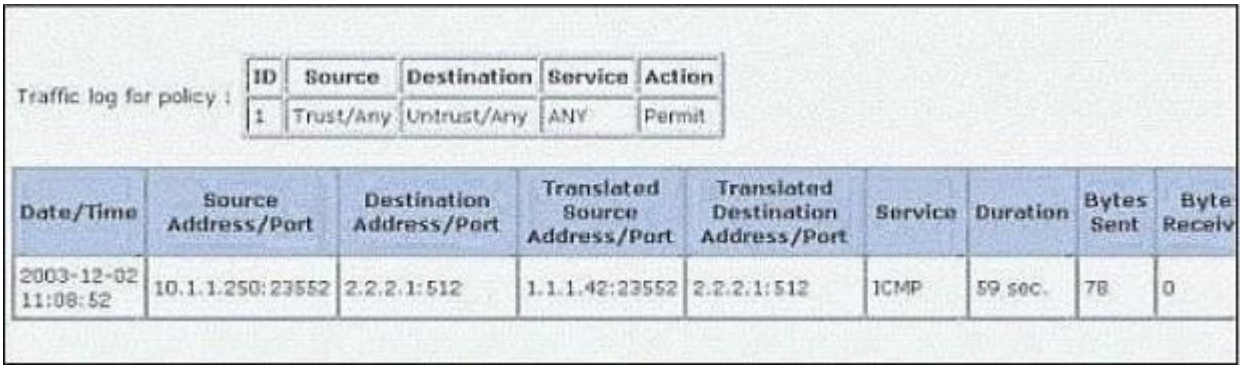
A. 3,4,2,5,1
B. 3,2,1,5,4
C. 5,3,1,2,4
D. 4,5,3,2,1
Answer: A

10.Which ScreenOS CLI commands would be used to enable traffic logging in policy edit mode?
A. Set policy traffic-log
B. Set traffic-log
C. Set log
D. Set logging
Answer: C

11.Which command would you run to check IPSec Phase 1 active status?
A. Get event 427
B. Get sa active
C. Get sa
D. Get ike cookie
Answer: D

12.Telnet management has been enabled on an interface in the untrust zone.
What else should be configured to limit telnet access to the ScreenOS devie from trusted management PCs?
A. Define a manage IP address on this interface
B. Define a policy from trust to untrust
C. Define a permitted IP address
D. Define a trusted IP in the address table
Answer: C

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



Traffic log for policy :

ID	Source	Destination	Service	Action
1	Trust/Any	Untrust/Any	ANY	Permit

Date/Time	Source Address/Port	Destination Address/Port	Translated Source Address/Port	Translated Destination Address/Port	Service	Duration	Bytes Sent	Byte Receiv
2003-12-02 11:08:52	10.1.1.250:23552	2.2.2.1:512	1.1.1.42:23552	2.2.2.1:512	ICMP	59 sec.	78	0

A. NAT-src with no DIP
B. Interface-based translation
C. NAT-src with a DIP, fixed-port disabled
D. MIP
Answer: AB

14.Which statement accurately describes the "config rollaback" feature?
A. Once the "Config rollback" feature is enabled, it allows the administrator to re-apply a locked configuration file from a separate area in flash
B. The "Config rollback" feature is enabled by default, it allows the administrator to re-reply a previously saved configuration file from flash
C. Once the "Config rollback" feature is enabled, it allows the administrator to re-apply a previously saved configuration file from the flash
D. Once the "Config rollback" feature is enabled, it allows the administrator to revert to the prior ScreenOS image or configuration file in event an upgrade operation aborts
Answer: A

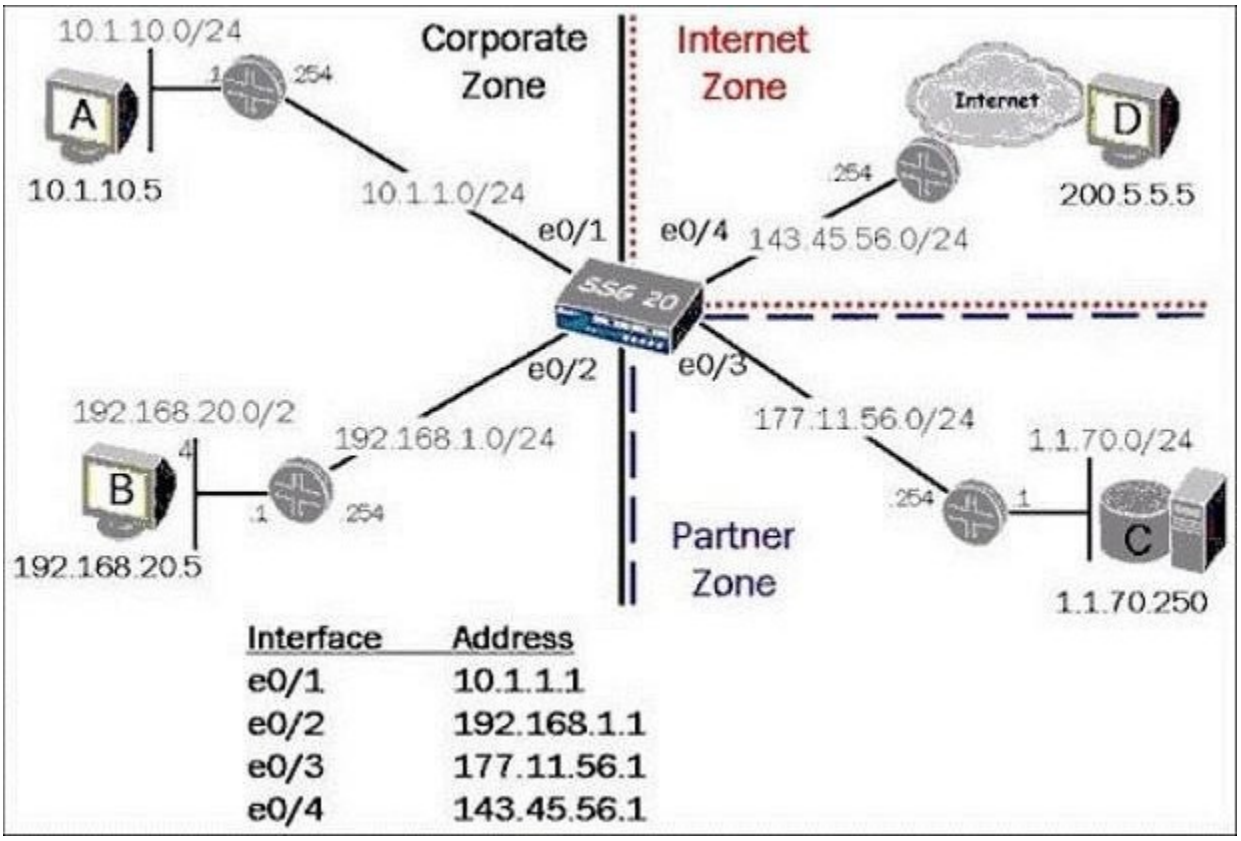
15.What needs to be configured in Phase 2 of a route-based VPN that does not need to be configured in a policy-based VPN?
A. Proxy-id
B. Custom proposals
C. Tunnel-binding
D. Transport mode
Answer: C

16.You are looking at the event log of the responding device and it says " Rejected an initial Phase 1 packet from un unrecognized peer gateway".
What are three likely reasons for the failure? (Choose three.)
A. The Peer ID is misconfigured
B. The gateway address is misconfigured
C. The preshare keys are mismatched
D. The outgoing interface is misconfigured
E. The default gateway is missing
Answer: ABD

17.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. Perform a policy lookup and determine the interfaces to which the source address is permitted and flood the packet out of those interfaces
C. 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
D. Check its route table for interzone destination
Answer: C

18.you are looking at the event log of the responding device and it says " Rejected an initial Phase 1 packet from un unrecognized peer gateway".
What are three likely reasons for the failure? (Choose three.)
A. The gateway address is misconfigured
B. The default gateway is missing
C. The Peer ID is misconfigured
D. The outgoing interface is misconfigured
E. The preshare keys are mismatched
Answer: ACD

19.See the Exhibit: For the SSG 20 to have full reachability to all host in the network, how many static routes need to be added?



A. 5

B. 3
C. 4
D. 2
Answer: C

20.You have created a route-based VPN in your ScreenOS device. When the remote device tries to connect you see the following message in your event log, "No Policy exist for the proxy id received". Which two would cause this to occur? (Choose two.)
A. The tunnel interface is configured in a different zone than the physical interface
B. A proxy-id conflict
C. The remote device is a policy-based VPN
D. An unbound tunnel interface
Answer: BC