

Exam Code: jn0-330

Exam Name: JN0-330-Enhanced Services,
Specialist(JNCIS-ES)

Vendor: Juniper Networks

Version: DEMO

Part: A

1: Click the Exhibit button.

Which type of source NAT is configured in the exhibit?

```
user@host# run show security nat source-nat pool pool-1
Pool name      Address      Status      Host          References PAT
pool-1         1.1.1.10    free        10.1.1.10     0 no
pool-1         1.1.1.11    free        10.1.1.11     0 no
pool-1         1.1.1.12    free        10.1.1.12     0 no
pool-1         1.1.1.13    free        10.1.1.13     0 no
pool-1         1.1.1.14    free        10.1.1.14     0 no
```

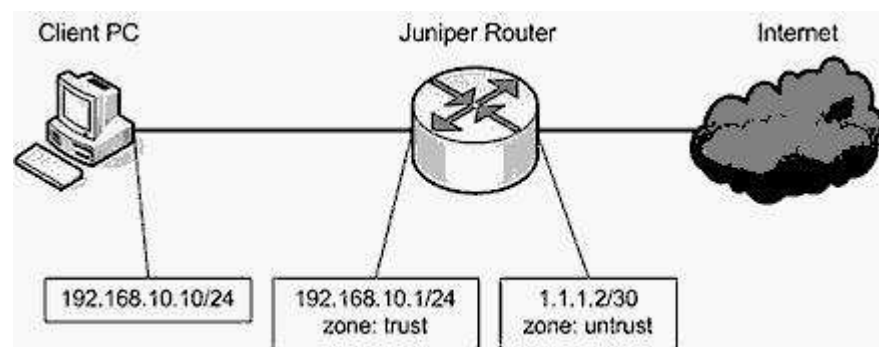
- A.static source pool
- B.interface source pool
- C.source pool with PAT
- D.souce pool without PAT

Correct Answers: A

2: Click the Exhibit button.

Based on the exhibit, client PC 192.168.10.10 cannot ping 1.1.1.2.

Which is a potential cause for this problem?



- A.The untrust zone does not have a management policy configured.
- B.The trust zone does not have ping enabled as host-inbound-traffic service.
- C.The security policy from the trust zone to the untrust zone does not permit ping.
- D.No security policy exists for the ICMP reply packet from the untrust zone to the trust zone.

Correct Answers: C

3: A traditional router is better suited than a firewall device for which function?

- A.VPN establishment
- B.packet-based forwarding
- C.stateful packet processing
- D.network address translation

Correct Answers: B

4: You must configure a SCREEN option that would protect your router from a session table flood.

Which configuration meets this requirement?

- A.[edit security screen]

```
user@host1# show
ids-option protectFromFlood {
icmp {
ip-sweep threshold 5000;
flood threshold 2000;
}
```

B.[edit security screen]

```
user@host1# show
ids-option protectFromFlood {
tcp {
syn-flood {
attack-threshold 2000;
destination-threshold 2000;
}
```

C.[edit security screen]

```
user@host1# show
ids-option protectFromFlood {
udp {
flood threshold 5000;
}
```

D.[edit security screen]

```
user@host1# show
ids-option protectFromFlood {
limit-session {
source-ip-based 1200;
destination-ip-based 1200;
}
```

Correct Answers: D

5: Click the Exhibit button.

In the exhibit, what is the priority for Router B in VRRP group 100?

```

Router A:
[edit]
user@RouterA# show interfaces ge-0/0/1
unit 0 {
    family inet {
        address 192.168.1.253/24 {
            vrrp-group 100 {
                virtual-address 192.168.1.1;
                priority 110;
                no-preempt;
            }
        }
    }
}

Router B:
[edit]
user@RouterB# show interfaces ge-0/0/1
unit 0 {
    family inet {
        address 192.168.1.254/24 {
            vrrp-group 100 {
                virtual-address 192.168.1.1;
                no-preempt;
            }
        }
    }
}

```

- A.1
- B.100
- C.110
- D.255

Correct Answers: B

6: In a JSRP cluster with two J6350 routers, the interface ge-7/0/0 belongs to which device?

- A.This interface is a system-created interface.
- B.This interface belongs to NODE0 of the cluster.
- C.This interface belongs to NODE1 of the cluster.
- D.This interface will not exist because J6350 routers have only six slots.

Correct Answers: C

7: Click the Exhibit button.

Based on the configuration shown in the exhibit, what will happen to the traffic matching the security policy?

```

[edit schedulers]
user@host# show
scheduler now {
    monday all-day;
    tuesday exclude;
    wednesday {
        start-time 07:00:00 stop-time
18:00:00;
    }
    thursday {
        start-time 07:00:00 stop-time
18:00:00;
    }
}

[edit security policies from-zone Private
to-zone External]
user@host# show
policy allowTransit {
    match {
        source-address PrivateHosts;
        destination-address ExtServers;
        application ExtApps;
    }
    then {
        permit {
            tunnel{
                ipsec-vpn myTunnel;
            }
        }
    }
    scheduler-name now;
}

```

- A. The traffic is permitted through the myTunnel IPSec tunnel only on Tuesdays.
- B. The traffic is permitted through the myTunnel IPSec tunnel daily, with the exception of Mondays.
- C. The traffic is permitted through the myTunnel IPSec tunnel all day on Mondays, Wednesdays between 7:00 am and 6:00 pm, and Thursdays between 7:00 am and 6:00 pm.
- D. The traffic is permitted through the myTunnel IPSec tunnel all day on Mondays, Wednesdays between 6:01 pm and 6:59 am, and Thursdays between 6:01 pm and 6:59 am.

Correct Answers: C

8: Which parameters must you select when configuring operating system probes SCREEN options?

- A. syn-fin, syn-flood, and tcp-no-frag
- B. syn-fin, port-scan, and tcp-no-flag
- C. syn-fin, fin-no-ack, and tcp-no-frag
- D. syn-fin, syn-ack-ack-proxy, and tcp-no-frag

Correct Answers: C

9: A route-based VPN is required for which scenario?

A.when the remote VPN peer is behind a NAT device

B.when multiple networks need to be reached across the tunnel

C.when the remote VPN peer is a dialup or remote access client

D.when a dynamic routing protocol such as OSPF is required across the VPN

Correct Answers: D

10: On which three traffic types does firewall pass-through authentication work? (Choose three.)

A.ping

B.FTP

C.Telnet

D.HTTP

E.HTTPS

Correct Answers: B C D