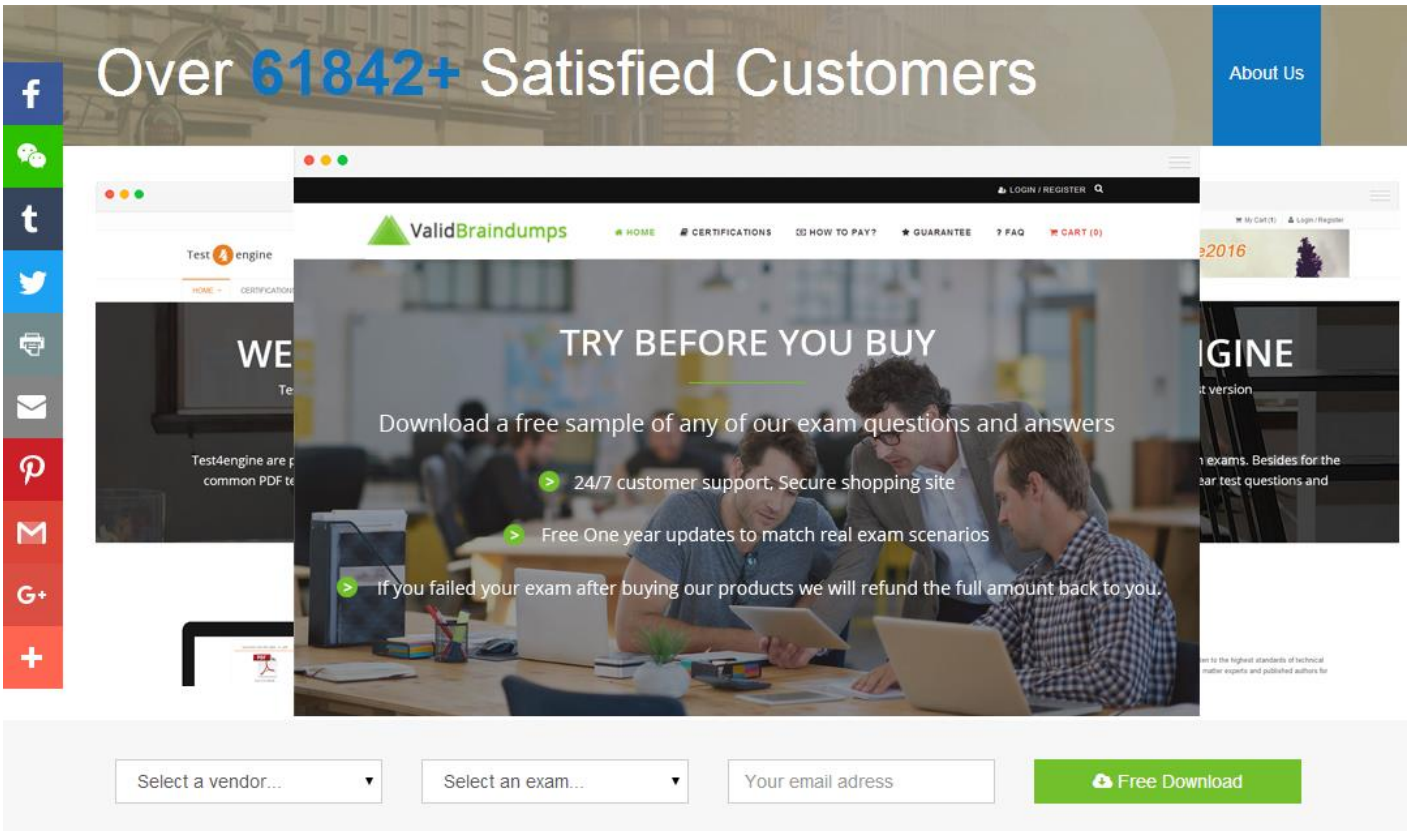
ValidBraindumps



Try Before You Buy

Download a free sample of any of our exam questions and answers

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

http://www.validbraindumps.com

Free valid test braindumps for IT certification valid exam

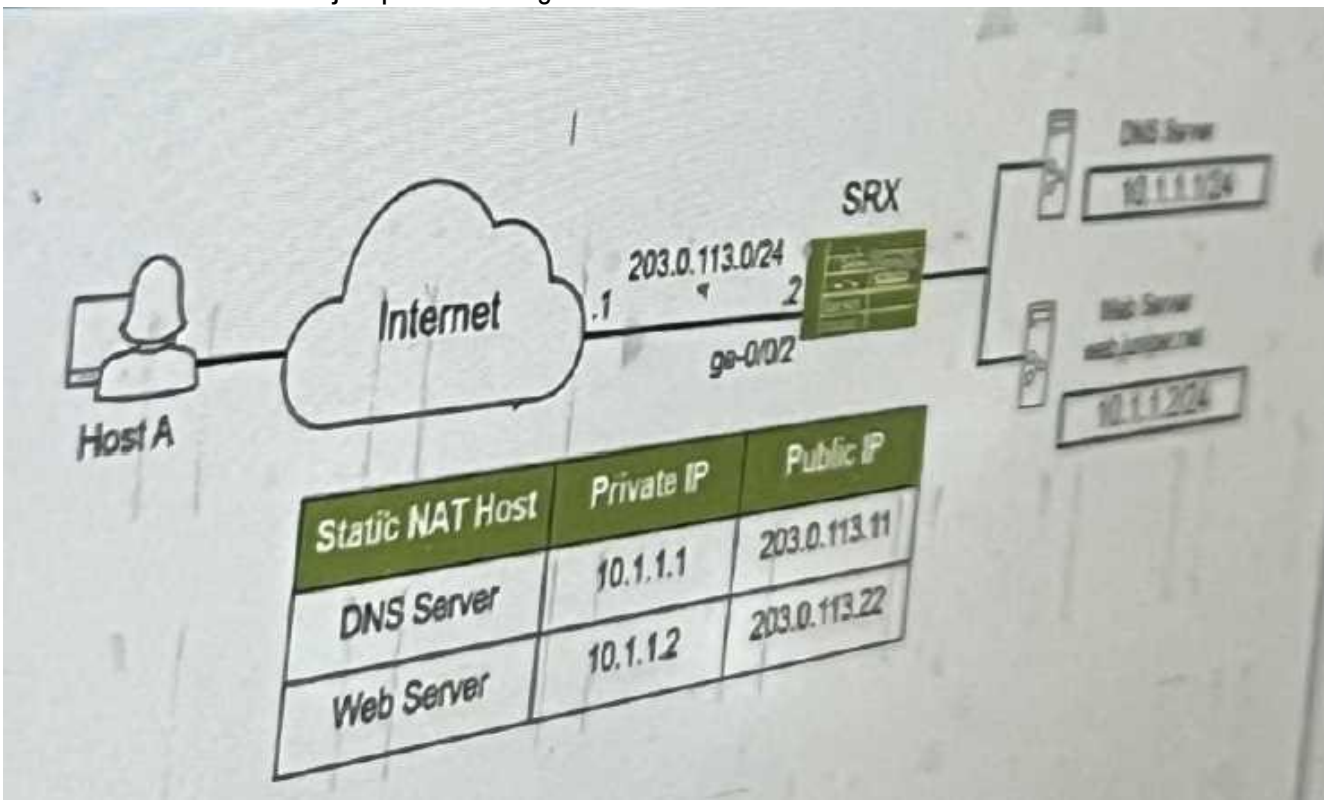
Exam : **JN0-637**

Title : Security, Professional (JNCIP-SEC)

Vendor : Juniper

Version : DEMO

NO.1 The SRX series device is performing static NAT. you want to ensure that host A can reach the internal webserver www.juniper.net using domain name.



Referring to the exhibit, which two Junos features are required to accomplish this task? (Choose two.)

A. DNS doctoring

B. proxy ARP

C. persistent NAT

D. STUN

Answer: AB

NO.2 You are attempting to ping an interface on your SRX Series device, but the ping is unsuccessful. What are three reasons for this behavior? (Choose three.)

A. The interface is not assigned to a security zone.

B. The interface's host-inbound-traffic security zone configuration does not permit ping

C. The ping traffic is matching a firewall filter.

D. The device has J-Web enabled.

E. The interface has multiple logical units configured.

Answer: ABC

NO.3 You have an initial setup of ADVPN with two spokes and a hub. A host at partner Spoke-1 is sending traffic to a host at partner Spoke-2.
In this scenario, which statement is true?

A. Spoke-1 will establish a VPN to Spoke-2 when this is first deployed, so traffic will be sent immediately to Spoke-2.

B. Spoke-1 will send the traffic through the hub and not use a direct VPN to Spoke-2.

C. Spoke-1 will establish the tunnel to Spoke-2 before sending any of the host traffic.
D. Spoke-1 will send the traffic destined to Spoke-2 through the hub until the VPN is established between the spokes.
Answer: A

NO.4 All interfaces involved in transparent mode are configured with which protocol family?
A. ethernet - switching
B. inet
C. bridge
D. mpls
Answer: C

NO.5 You need to set up source NAT so that external hosts can initiate connections to an internal device, but only if a connection to the device was first initiated by the internal device. Which type of NAT solution provides this functionality?
A. Address persistence
B. Persistent NAT with any remote host
C. Persistent NAT with target host
D. Static NAT
Answer: C
Explanation:
Persistent NAT with target host allows external hosts to establish connections only when the internal device initiates a session first, ideal for specific interactive applications.
The scenario requires that external hosts be able to initiate a connection only if the internal device has already initiated a connection. The correct solution is Persistent NAT with target host, which ensures that a specific external host can initiate new connections back to the internal device, but only after the internal device has established a session first. Persistent NAT with Target Host (Answer C): This allows the internal device to initiate a connection, and once established, the specified external host can also initiate new connections to the internal device on the same NAT mapping.

NO.6 A company has acquired a new branch office that has the same address space of one of its local networks, 192.168.100/24. The offices need to communicate with each other. Which two NAT configurations will satisfy this requirement? (Choose two.)
A. [edit security nat source]
user@OfficeA# show rule-set OfficeBtoA {
from zone OfficeB;
to zone OfficeA;
rule 1 {
match {
source-address 192.168.210.0/24;
destination-address 192.168.200.0/24;
}
then {
source-nat {
interface;

```
}
}
}
}
```

B. [edit security nat static]

```
user@OfficeA# show rule-set From-Office-B {
from interface ge-0/0/0.0;
rule 1 {
match {
destination-address 192.168.200.0/24;
}
then {
static-nat {
prefix 192.168.100.0/24;
}
}
}
}
```

C. [edit security nat static]

```
user@OfficeB# show rule-set From-Office-A {
from interface ge-0/0/0.0;
rule 1 {
match {
destination-address 192.168.210.0/24;
}
then {
static-nat {
prefix 192.168.100.0/24;
}
}
}
}
```

D. [edit security nat source]

```
user@OfficeB# show rule-set OfficeAtoB {
from zone OfficeA;
to zone OfficeB;
rule 1 {
match {
source-address 192.168.200.0/24;
destination-address 192.168.210.0/24;
}
then {
source-nat {
interface;
}
}
```

}
}
Answer: AD
Explanation:
The problem describes two offices needing to communicate, but both share the same IP address space, 192.168.100.0/24. To resolve this, NAT must be configured to translate the conflicting address spaces on each side. Here's how each of the configurations works:
Option A (Correct):
This source NAT rule translates the source address of traffic from Office B to Office A. By configuring source NAT, the source IP addresses from Office B (192.168.210.0/24) will be translated when communicating with Office A (192.168.200.0/24). This method ensures that there is no overlap in address space when packets are transmitted between the two offices.
Option D (Correct):
This is a source NAT rule configured on Office B, which translates the source addresses from Office A to prevent address conflicts. It ensures that when traffic is initiated from Office A to Office B, the overlapping address range (192.168.100.0/24) is translated.

NO.7 Which two statements are correct about advanced policy-based routing?
A. It can use the application system cache to route traffic.
B. The associated routing instance should be configured as a virtual router instance.
C. It cannot use the application system cache to route traffic.
D. The associated routing instance should be configured as a forwarding instance.
Answer: AD

NO.8 The exhibit shows part of the flow session logs.

```
Mar  7 01:28:23 01:28:23.434801:CID-0:THREAD_ID-01:RT:<172.20.201.10/59009->10.0.1.129/22;6,0x0> matched filter
MatchTraffic:
Mar  7 01:28:23 01:28:23.434817:CID-0:THREAD_ID-01:RT: ge-0/0/4.0:172.20.101.10/59009->10.0.1.129/22, tcp, flag 2 syn
Mar  7 01:28:23 01:28:23.434819:CID-0:THREAD_ID-01:RT: find flow: table 0x206a60a0, hash 43106(0xffff), sa 172.20.101.10, da
10.0.1.129, sp 59009, dp 22, proto 6, tok 9, conn-tag 0x00000000
Mar  7 01:28:23 01:28:23.434822:CID-0:THREAD_ID-01:RT:  no session found, start first path. in_tunnel - 0x0, from_cp_flag -
0
Mar  7 01:28:23 01:28:23.434826:CID-0:THREAD_ID-01:RT: flow_first_create_session
Mar  7 01:28:23 01:28:23.434834:CID-0:THREAD_ID-01:RT:  flow_first_in_dst_nat: in <ge-0/0/3.0>, out <N/A> dst_adr
10.0.1.129, sp 59009, dp 22
Mar  7 01:28:23 01:28:23.434835:CID-0:THREAD_ID-01:RT:  chose interface ge-0/0/4.0 as incoming nat if.
Mar  7 01:28:23 01:28:23.434838:CID-0:THREAD_ID-01:RT:flow_first_rule_dst_xlate: DST no-xlate: 0.0.0.0(0) to 10.0.1.129(22)
```

Which two statements are true in this scenario? (Choose two.)
A. The existing session is found in the table, and the fast path process begins.
B. This packet arrives on interface ge-0/0/4.0.
C. Junos captures a TCP packet from source address 172.20.101.10 destined to 10.0.1.129.
D. Destination NAT occurs.
Answer: BD

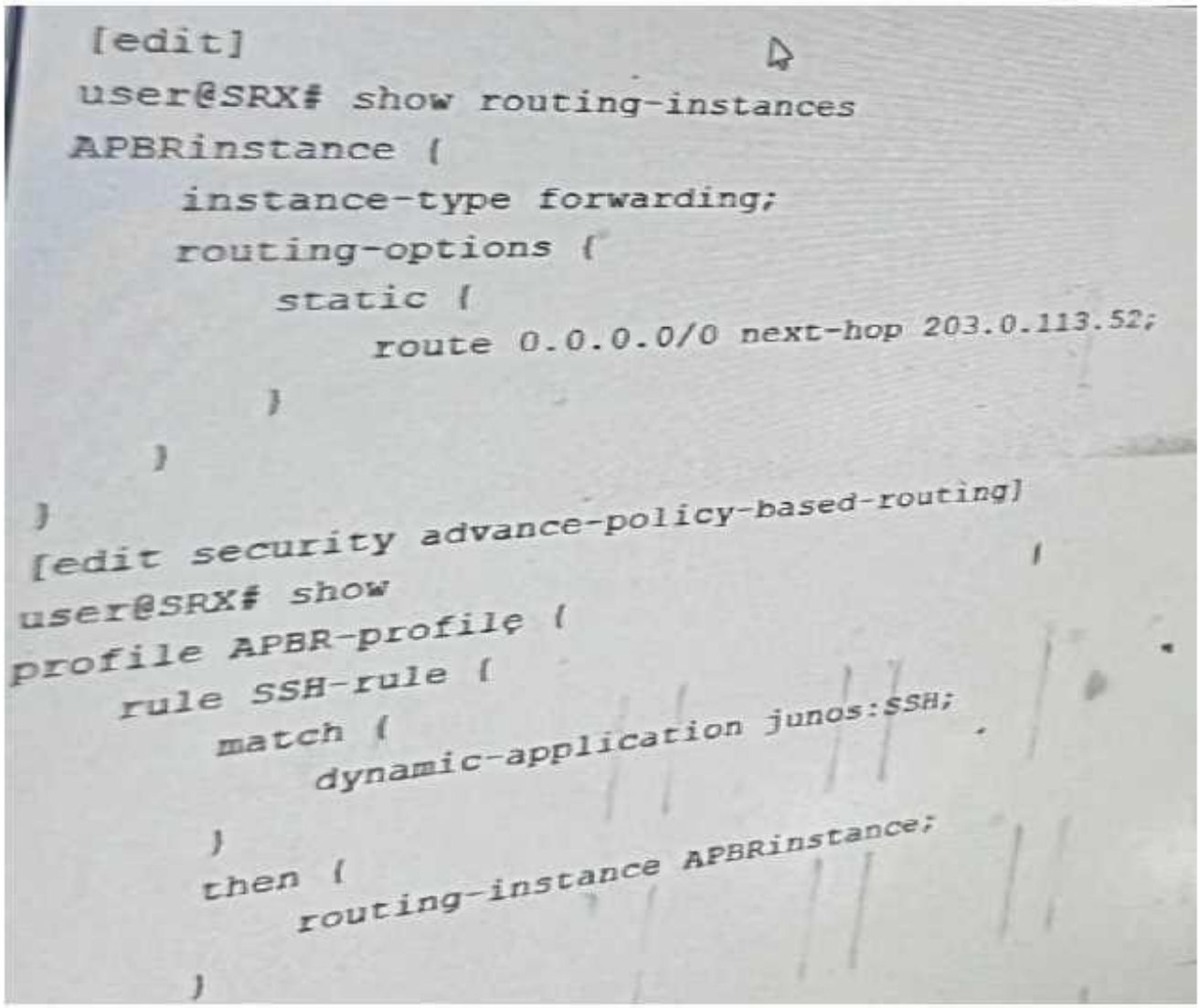
NO.9 How does secure wire mode differ from transparent mode?
A. In secure wire mode, traffic can be modified using source NAT.
B. In secure wire mode, no switching lookup takes place to forward traffic.

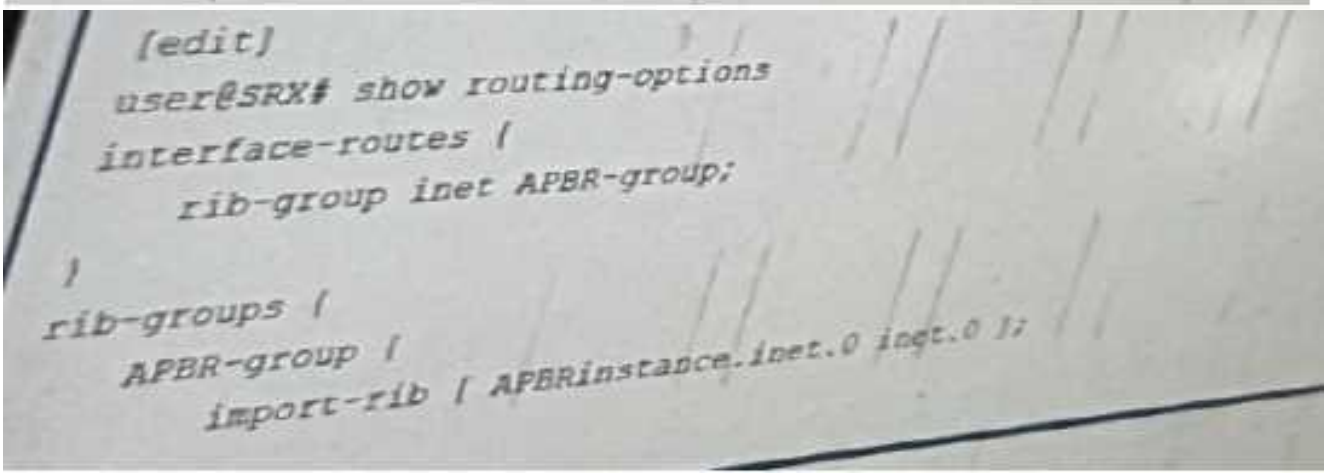
C. In secure wire mode, security policies cannot be used to secure intra-VLAN traffic.
D. In secure wire mode, IRB interfaces can be configured to route inter-VLAN traffic.
Answer: B

NO.10 What are three core components for enabling advanced policy-based routing? (Choose three.)
A. Filter-based forwarding
B. Routing options
C. Routing instance
D. APBR profile
E. Policies
Answer: ACD
Explanation:
To enable Advanced Policy-Based Routing (APBR) on SRX Series devices, three key components are necessary: filter-based forwarding, routing instances, and APBR profiles. Filter- based forwarding is utilized to direct specific traffic flows to a routing instance based on criteria set by a policy. Routing instances allow the traffic to be managed independently of the main routing table, and APBR profiles define how and when traffic should be forwarded. These elements ensure that APBR is flexible and tailored to the network's requirements. Refer to Juniper's APBR Documentation for more details.

NO.11 Which two statements are correct about automated threat mitigation with Security Director? (Choose two.)
A. It works with third-party switches.
B. It provides endpoint protection by running a Juniper ATP Cloud agent on the servers.
C. It provides endpoint protection by running a Juniper ATP Cloud agent on EX Series devices.
D. It works with SRX Series devices.
Answer: AD

NO.12 You are configuring advanced policy-based routing. You have created a static route with next hop of an interface in your inet.0 routing table





Referring to the exhibit, what should be changed to solve this issue?

A. You should change the routing instance type to virtual-router.

B. You should move the static route configuration to the main routing instance.

C. You should move the inet. o table before the routing instance table in your rib-groups configuration.

D. You should delete the interface-routes configuration under the routing-options hierarchy.

Answer: C