JN0-636^{Q&As}

Service Provider Routing and Switching Professional (JNCIP-SP)

Pass Juniper JN0-636 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/jn0-636.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Juniper Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

SRX Series device enrollment with Policy Enforcer fails To debug further, the user issues the following command show configuration services security--intelligence url

https : //cloudfeeds . argon . juniperaecurity . net/api/manifeat. xml

and receives the following output:

What is the problem in this scenario?

A. The device is directly enrolled with Juniper ATP Cloud.

B. The device is already enrolled with Policy Enforcer.

C. The SRX Series device does not have a valid license.

D. Junos Space does not have matching schema based on the

Correct Answer: C

QUESTION 2

Exhibit

```
user@srx> show log flow-log
Apr 13 17:46:17 17:46:17.316930:CID-0:THREAD_ID-01:RT:<10.10.101.10/65131-
>10.10.102.1/22;6,0x0> matched filter F1:
Apr 13 17:46:17 17:46:17.317009:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.1) from trust (ge-0/0/4.0 in 0) to ge-0/0/5.0, Next-hop: 10.10.102.1
Apr 13 17:46:17 17:46:17.317016:CID-0:THREAD_ID-
01:RT:flow_first_policy_search: policy search from zone trust-> zone dmz
(0x0,0xfe6b0016,0x16)
Apr 13 17:46:17 17:46:17.317019:CID-0:THREAD_ID-01:RT:Policy lkup: vsys 0
zone(8:trust) -> zone(9:dmz) scope:0
Apr 13 17:46:17 17:46:17.317020:CID-0:THREAD_ID-01:RT: 10.10.101.10/65131 ->
10.10.102.1/22 proto 6
Apr 13 17:46:17 17:46:17.317031:CID-0:THREAD_ID-01:RT: permitted by policy
trust-to-dmz(8)
Apr 13 17:46:17 17:46:17.317031:CID-0:THREAD_ID-01:RT: packet passed,
Permitted by policy.
Apr 13 17:46:17 17:46:17.317038:CID-0:THREAD_ID-01:RT: choose interface ge-
0/0/5.0(P2P) as outgoing phy if
Apr 13 17:46:17 17:46:17.317042:CID-0:THREAD_ID-01:RT:is_loop_pak: Found loop
on ifp ge-0/0/5.0, addr: 10.10.102.1, rtt_idx: 0 addr_type:0x3.
Apr 13 17:46:17 17:46:17.317044:CID-0:THREAD_ID-
01:RT:flow_first_loopback_check: Setting interface: ge-0/0/5.0 as loop ifp.
Apr 13 17:46:17 17:46:17.317213:CID-0:THREAD_ID-01:RT:
flow_first_create_session
Apr 13 17:46:17 17:46:17.317215:CID-0:THREAD_ID-01:RT: flow_first_in_dst_nat:
0/0/5.0 as incoming nat if.
call flow_route_lookup(): src_ip 10.10.101.10, x_dst_ip 10.10.102.1, in ifp
ge-0/0/5.0, out ifp N/A sp 65131, dp 22, ip_proto 6, tos 0
Apr 13 17:46:17 17:46:17.317227:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.1) from dmz (ge-0/0/5.0 in 0) to .local..0, Next-hop: 10.10.102.1
Apr 13 17:46:17 17:46:17.317228:CID-0:THREAD_ID-
01:RT:flow_first_policy_search: policy search from zone dmz-> zone junos-host
(0x0,0xfe6b0016,0x16)
Apr 13 17:46:17 17:46:17.317230:CID-0:THREAD_ID-01:RT:Policy lkup: vsys 0
zone(9:dmz) -> zone(2:junos-host) scope:0
Apr 13 17:46:17 17:46:17.317230:CID-0:THREAD_ID-01:RT: 10.10.101.10/65131 ->
10.10.102.1/22 proto 6
Apr 13 17:46:17 17:46:17.317236:CID-0:THREAD_ID-01:RT: packet dropped, denied
by policy
Apr 13 17:46:17 17:46:17.317237:CID-0:THREAD_ID-01:RT: denied by policy deny-
ssh(9), dropping pkt
Apr 13 17:46:17 17:46:17.317237:CID-0:THREAD_ID-01:RT: packet dropped, policy
deny.
```

You are using traceoptions to verify NAT session information on your SRX Series device. Referring to the exhibit, which two statements are correct? (Choose two.)

A. This is the last packet in the session.

B. The SRX Series device is performing both source and destination NAT on this session.

C. This is the first packet in the session.

D. The SRX Series device is performing only source NAT on this session.

Correct Answer: AB

QUESTION 3

You are deploying a virtualization solution with the security devices in your network Each SRX Series device must support at least 100 virtualized instances and each virtualized instance must have its own discrete administrative domain. In this scenario, which solution would you choose?

A. VRF instances

B. virtual router instances

C. logical systems

D. tenant systems

Correct Answer: C

Explanation: A logical system is a virtualization feature in SRX Series devices that allows you to create multiple, isolated virtual routers within a single physical device. Each logical system has its own routing table, firewall policies, and interfaces, and it can be managed and configured independently of the other logical systems. Logical systems are an effective way to isolate different administrative domains and to support a large number of virtualized instances.

QUESTION 4

You are not able to activate the SSH honeypot on the all-in-one Juniper ATP appliance. What would be a cause of this problem?

A. The collector must have a minimum of two interfaces.

B. The collector must have a minimum of three interfaces.

C. The collector must have a minimum of five interfaces.

D. The collector must have a minimum of four interfaces.

Correct Answer: D

Explanation: https://www.juniper.net/documentation/en_US/release- independent/jatp/topics/task/configuration/jatp-traffic-collectorsetting-ssh-honeypot- detection.html

QUESTION 5

You are required to deploy a security policy on an SRX Series device that blocks all known Tor network IP addresses. Which two steps will fulfill this requirement? (Choose two.)

A. Enroll the devices with Juniper ATP Appliance.

B. Enroll the devices with Juniper ATP Cloud.

C. Enable a third-party Tor feed.

D. Create a custom feed containing all current known MAC addresses.

Correct Answer: AB

Explanation: To block all known Tor network IP addresses on an SRX Series device, the following steps must be taken:

Enroll the devices with Juniper ATP Appliance or Juniper ATP Cloud: both of these services provide threat intelligence feeds that include known IP addresses associated with the Tor network. By enrolling the SRX Series device, the device

will have access to the latest Tor network IP addresses, and it can then use this information to block traffic from those IP addresses. Creating a custom feed containing all current known MAC addresses, is not a valid option since Tor network

uses IP addresses, MAC addresses are not used to identify the Tor network.

Enable a third-party Tor feed may be used but it\\'s not necessary as Juniper ATP Appliance and Juniper ATP Cloud already provide the same feature.

[JN0-636 VCE Dumps](#)   [JN0-636 Practice Test](#)   [JN0-636 Study Guide](#)