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.pass2lead.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

You are asked to detect domain generation algorithms

Which two steps will accomplish this goal on an SRX Series firewall? (Choose two.)

A. Define an advanced-anti-malware policy under [edit services].

B. Attach the security-metadata-streaming policy to a security

C. Define a security-metadata-streaming policy under [edit

D. Attach the advanced-anti-malware policy to a security policy.

Correct Answer: BD

Explanation: To detect domain generation algorithms (DGAs) on an SRX Series firewall, you can use the security-metadata-streaming and advanced-anti-malware features. The first step is to define a security-metadata-streaming policy under

[edit services], which allows the firewall to receive and process metadata from a third- party security intelligence service. This metadata includes information about DGAs, which the firewall can use to identify and block malicious traffic. The

second step is to attach the security-metadata-streaming policy to a security policy, this will enable the firewall to inspect traffic against the DGA domains provided by the intelligence service.

The third step is to enable the advanced-anti-malware feature on the firewall, and attach an advanced-anti-malware policy to a security policy. This allows the firewall to detect and block malware based on signatures and behavioral analysis,

which can also detect and block traffic associated with DGAs.

QUESTION 2

You have a webserver and a DNS server residing in the same internal DMZ subnet. The public Static NAT addresses for the servers are in the same subnet as the SRX Series devices internet-facing interface.

You implement DNS doctoring to ensure remote users can access the webserver.

Which two statements are true in this scenario? (Choose two.)

A. The DNS doctoring ALG is not enabled by default.

B. The Proxy ARP feature must be configured.

C. The DNS doctoring ALG is enabled by default.

D. The DNS CNAME record is translated.

Correct Answer: BC

QUESTION 3

You are requested to enroll an SRX Series device with Juniper ATP Cloud.

Which statement is correct in this scenario?

A. If a device is already enrolled in a realm and you enroll it in a new realm, the device data or configuration information is propagated to the new realm.

B. The only way to enroll an SRX Series device is to interact with the Juniper ATP Cloud Web portal.

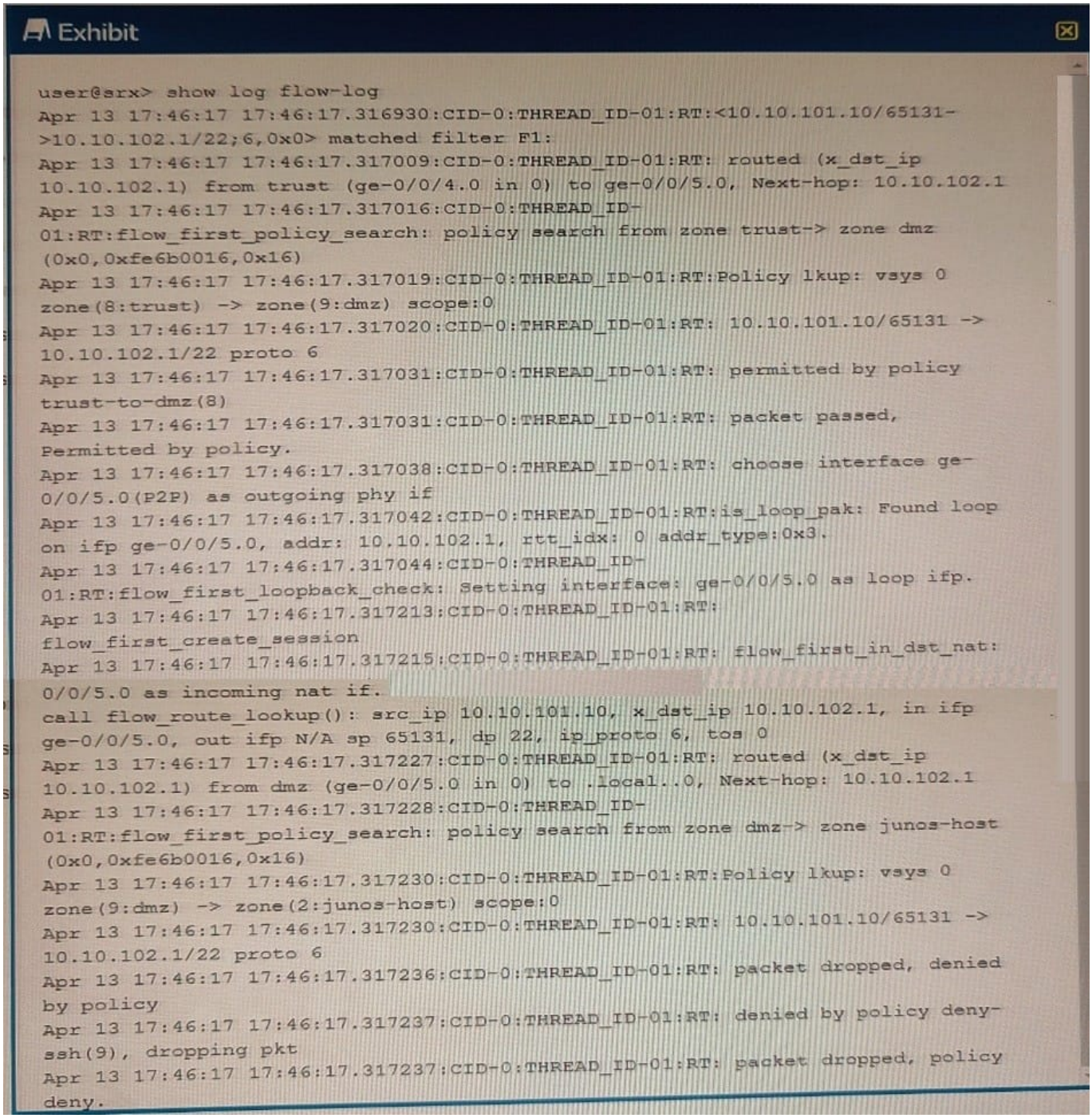
C. When the license expires, the SRX Series device is disenrolled from Juniper ATP Cloud without a grace period

D. Juniper ATP Cloud uses a Junos OS op script to help you configure your SRX Series device to connect to the Juniper ATP Cloud service.

Correct Answer: D

QUESTION 4

Exhibit Referring to the exhibit, which three statements are true? (Choose three.)



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.
```

A. The packet\\'s destination is to an interface on the SRX Series device.

B. The packet\\'s destination is to a server in the DMZ zone.

C. The packet originated within the Trust zone.

D. The packet is dropped before making an SSH connection.

E. The packet is allowed to make an SSH connection.

Correct Answer: ACD

QUESTION 5

You are asked to deploy filter-based forwarding on your SRX Series device for incoming traffic sourced from the 10.10 100 0/24 network in this scenario, which three statements are correct? (Choose three.)

A. You must create a forwarding-type routing instance.

B. You must create and apply a firewall filter that matches on the source address 10.10.100.0/24 and then sends this traffic to your routing

C. You must create and apply a firewall filter that matches on the destination address 10 10.100.0/24 and then sends this traffic to your routing instance.

D. You must create a RIB group that adds interface routes to your routing instance.

E. You must create a VRF-type routing instance.

Correct Answer: BCD

Explanation: In order to deploy filter-based forwarding on an SRX Series device for incoming traffic sourced from the 10.10.100.0/24 network, you must first create and apply a firewall filter that matches on the source address 10.10.100.0/24. Then, you must create a RIB group that adds interface routes to your routing instance and apply it. The filter will forward the traffic matching the source address to the routing instance. You don\\'t need to create a forwarding-type routing instance or a VRF-type routing instance.