Juniper

JN0-636
Security, Professional

Questions And Answers PDF Format:

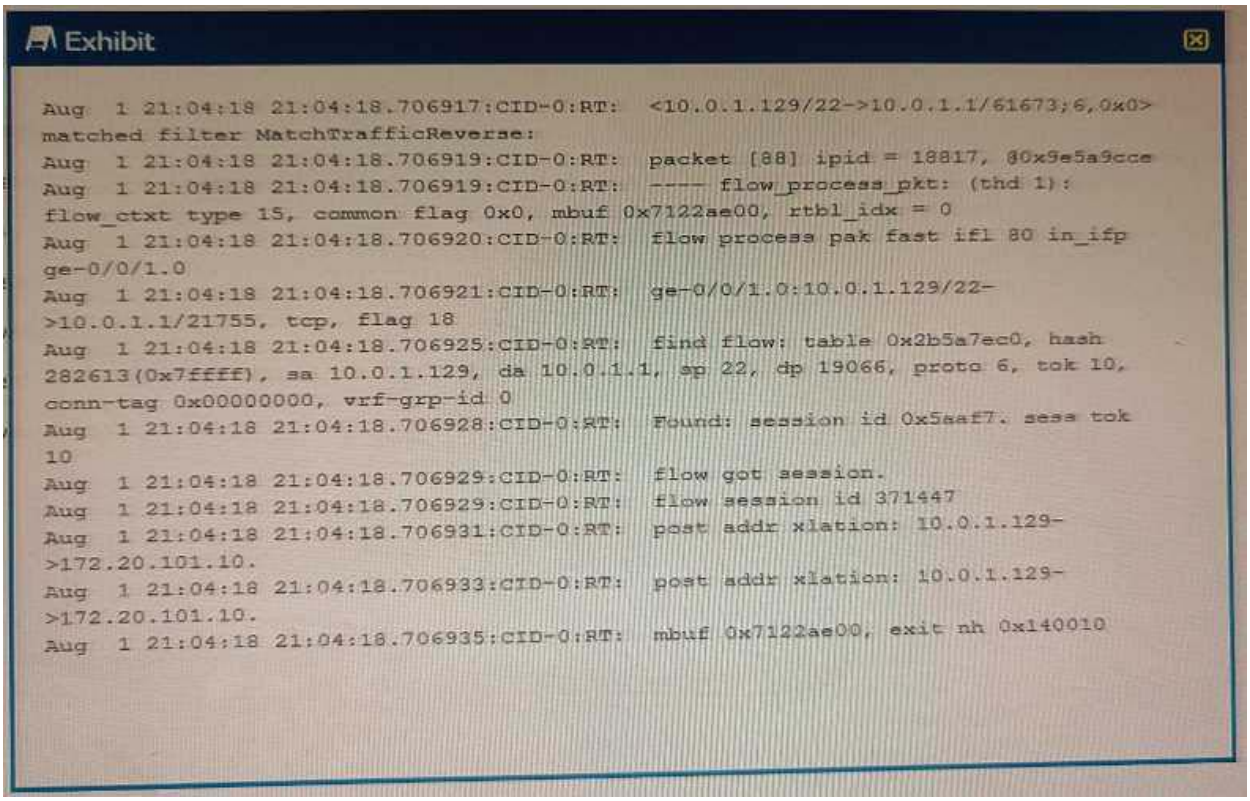
For More Information – Visit link below:
https://www.certsgrade.com/

Version = **Product**

Latest Version: 7.0

Question: 1

Exhibit



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

A. This packet is part of an existing session.
B. The SRX device is changing the source address on this packet from
C. This is the first packet in the session
D. The SRX device is changing the destination address on this packet 10.0.1 1 to 172 20.101.10.

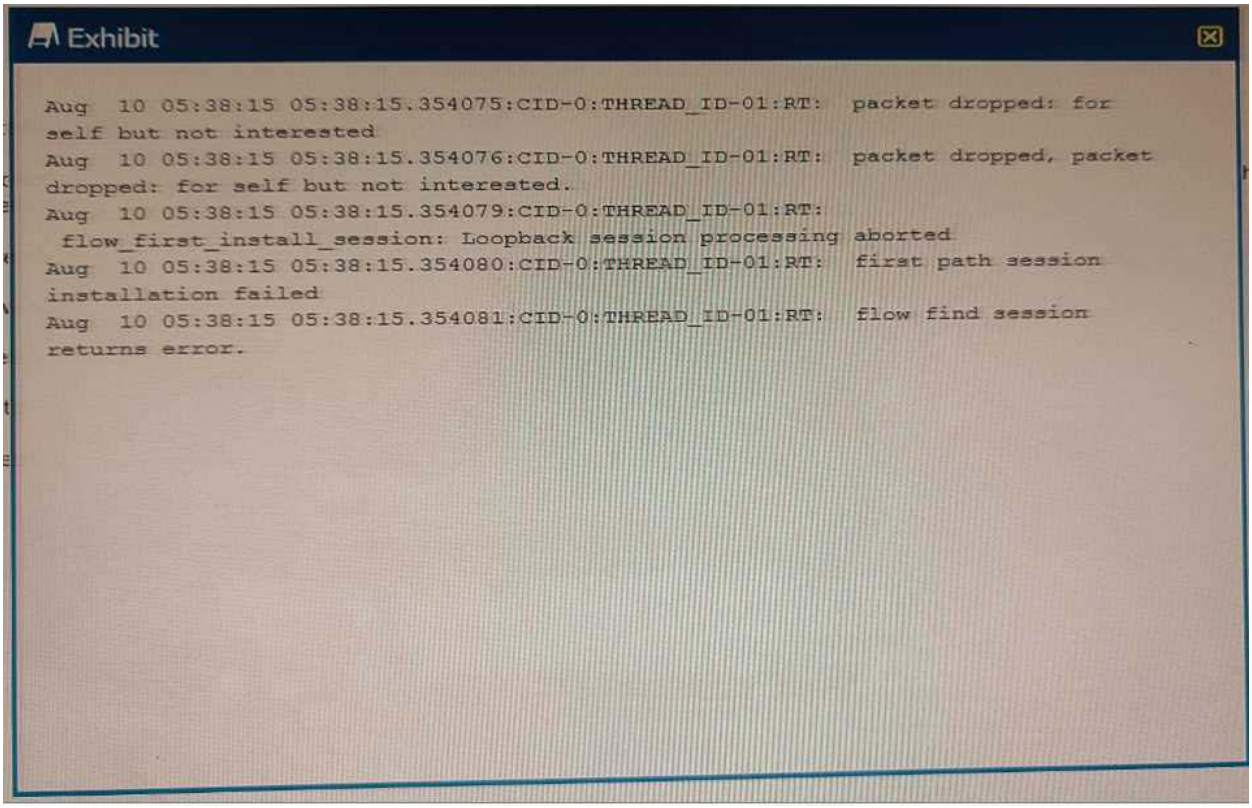
Answer: AD

Explanation:
According to the trace options output in the exhibit, the following statements are correct:
This packet is part of an existing session. This is indicated by the line flow session id 0x00000000, hash 0x00000000, table 0x00000000, flow process exit, which shows that the packet matches an existing session entry in the flow table1.
The SRX device is changing the destination address on this packet from 10.0.1.1 to 172.20.101.10. This is indicated by the line nat: translated 10.0.1.1->172.20.101.10, which shows that the packet undergoes

destination NAT2.
The following statements are incorrect:
The SRX device is changing the source address on this packet. There is no indication of source NAT in the trace options output2.
This is the first packet in the session. The first packet in a session would have a different trace options output, which would include the line flow_first_inline_processing and show the creation of a new session entry in the flow table1.
Reference: 1: SRX Getting Started – Troubleshooting Traffic Flows and Session Establishment 2: SRX Getting Started - Configure NAT (Network Address Translation)

Question: 2

Exhibit



You are asked to establish an IBGP peering between the SRX Series device and the router, but the session is not being established. In the security flow trace on the SRX device, packet drops are observed as shown in the exhibit.
What is the correct action to solve the problem on the SRX device?

A. Create a firewall filter to accept the BGP traffic
B. Configure destination NAT for BGP traffic.
C. Add BGP to the Allowed host-inbound-traffic for the interface
D. Modify the security policy to allow the BGP traffic.

Answer: C

Explanation:
According to the security flow trace in the exhibit, the packets are dropped for self but not interested. This means that the SRX device is receiving packets destined to itself, but it does not have the corresponding service configured in the host-inbound-traffic stanza for the interface1. In this case, the service is BGP, which uses TCP port 179. Therefore, the correct action to solve the problem on the SRX device is to add BGP to the allowed host-inbound-traffic for the interface. This can be done by using the following command:
set security zones security-zone <zone-name> interfaces <interface-name> host-inbound-traffic systemservices bgp
This command will allow the SRX device to accept BGP packets on the specified interface and zone. Alternatively, the command can be applied to all interfaces in a zone by using the allinterfaces option2.
Reference: 1: SRX Getting Started - Troubleshoot Security Policy 2: Configuring System Services Allowed for Host Inbound Traffic

Question: 3

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

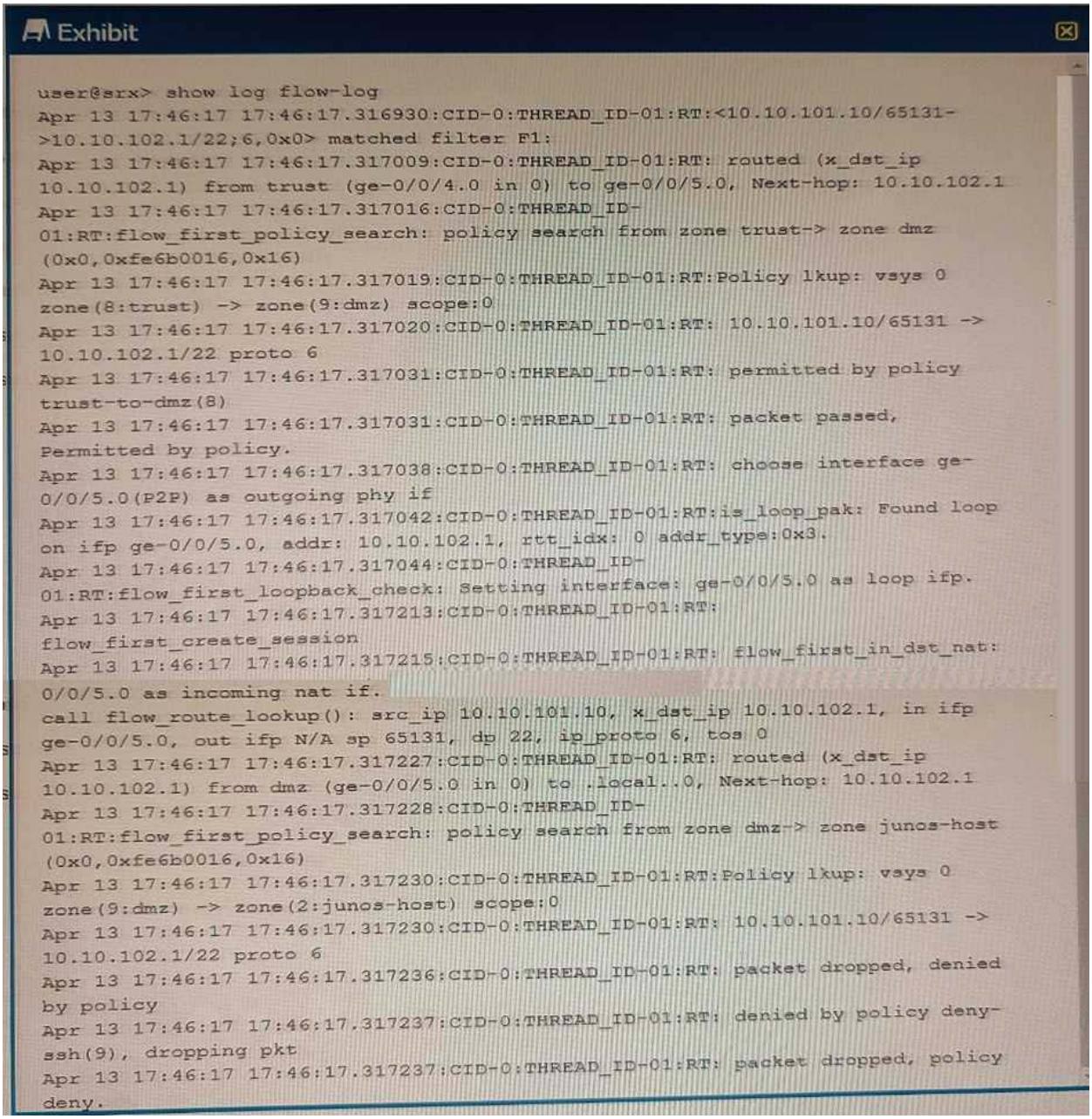
Answer: C

Explanation:
According to the output of the command show configuration services security-intelligence url, the SRX Series device is directly enrolled with Juniper ATP Cloud. This is indicated by the URL https://cloudfeeds.argon.junipersecurity.net/api/manifest.xml, which is the default URL for Juniper ATP Cloud1. This means that the device is not enrolled with Policy Enforcer, which would use a different URL that includes the IP address of the Policy Enforcer server2. Therefore, the problem in this scenario is that the device is directly enrolled with Juniper ATP Cloud, which prevents it from being enrolled with Policy Enforcer.
To enroll the device with Policy Enforcer, the user needs to disenroll the device from Juniper ATP Cloud first. This can be done by using the following command:
delete services security-intelligence url
This command will remove the Juniper ATP Cloud URL from the device configuration and stop the device from receiving threat feeds from Juniper ATP Cloud1. After that, the user can enroll the device with

Policy Enforcer by using the Security Director GUI or the SLAX script2.
Reference: 1: Configuring Juniper ATP Cloud on SRX Series Devices 2: Enrolling SRX Series Devices with Policy Enforcer

Question: 4

Exhibit



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

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.

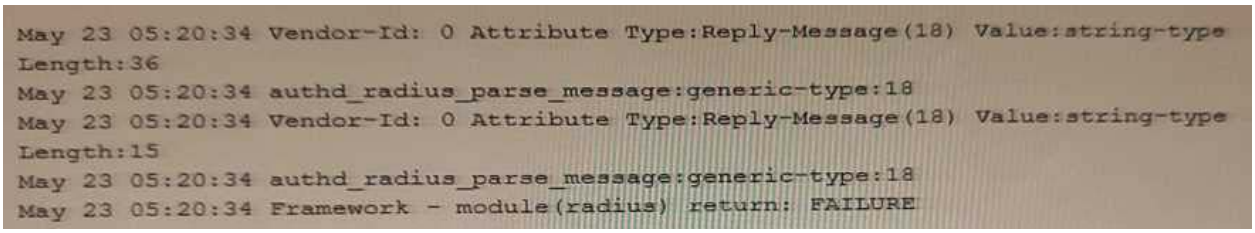
C. The packet originated within the Trust zone.
D. The packet is dropped before making an SSH connection.
E. The packet is allowed to make an SSH connection.

Answer: ACD

Explanation:
According to the exhibit, which is a security flow trace on an SRX Series device, the following statements are true:
The packet's destination is to an interface on the SRX Series device. This is indicated by the line packet dropped for self but not interested, which means that the packet is destined to the SRX device itself, but the device does not have the corresponding service configured in the host-inbound-traffic stanza for the interface1.
The packet originated within the Trust zone. This is indicated by the line zone name: Trust, which shows that the packet belongs to the Trust zone. The Trust zone is typically the zone where the internal network
is connected to the SRX device2.
The packet is dropped before making an SSH connection. This is indicated by the line flow_first_inline_processing: pak(0x4a9c0d0), which shows that the packet is the first packet in the session and is processed by the firewall. The packet is dropped because it does not match any security policy or host-inbound-traffic rule1. The packet is trying to make an SSH connection, which uses TCP port 22, as shown by the line source port: 22.
The following statements are false:
The packet's destination is to a server in the DMZ zone. There is no indication of the DMZ zone in the trace output. The DMZ zone is typically the zone where the external servers are connected to the SRX device2.
The packet is allowed to make an SSH connection. The packet is not allowed to make an SSH connection, as explained above.
Reference: 1: SRX Getting Started - Troubleshoot Security Policy 2: SRX Getting Started - Configure Security Zones

Question: 5

Exhibit



You configure a traceoptions file called radius on your returns the output shown in the exhibit
What is the source of the problem?

A. An incorrect password is being used.
B. The authentication order is misconfigured.
C. The RADIUS server IP address is unreachable.

D. The RADIUS server suffered a hardware failure.

Answer: A

Explanation:
According to the output of the traceoptions file called radius, the source of the problem is that the RADIUS server IP address is unreachable. This is indicated by the line FAILURE: sendto: No route to host, which shows that the SRX device cannot send the authentication request to the RADIUS server. This could be due to a network issue, such as a misconfigured route, a firewall blocking the traffic, or a physical link failure.
To troubleshoot this issue, the user should check the following:
The RADIUS server IP address and port are correctly configured on the SRX device. The user can verify this by using the command show configuration access radius-server1.
The SRX device can ping the RADIUS server IP address. The user can use the command ping <RADIUSserver-
IP> to test the connectivity2.
The SRX device has a valid route to the RADIUS server IP address. The user can use the command show route <RADIUS-server-IP> to check the routing table3.
The SRX device and the RADIUS server are using the same shared secret key. The user can verify this by using the command show configuration access radius-server secret1.
The SRX device and the RADIUS server are using the same authentication protocol. The user can verify this by using the command show configuration access profile <profile-name>4.
The firewall policies on the SRX device and any intermediate devices are allowing the RADIUS traffic. The user can use the command show security policies from-zone <source-zone> to-zone <destinationzone> to check the firewall policies5.
Reference: 1: Configuring RADIUS Server Parameters 2: ping - Technical Documentation - Support - Juniper Networks 3: show route - Technical Documentation - Support - Juniper Networks 4: Configuring Authentication Profiles 5: show security policies - Technical Documentation - Support - Juniper Networks

For More Information – Visit link below:

https://www.certsgrade.com/

PRODUCT FEATURES

- 100% Money Back Guarantee
- 90 Days Free updates
- Special Discounts on Bulk Orders
- Guaranteed Success
- 50,000 Satisfied Customers
- 100% Secure Shopping
- Privacy Policy
- Refund Policy

16 USD Discount Coupon Code: NB4XKTMZ