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.leads4pass.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

Which two features would be used for DNS doctoring on an SRX Series firewall? (Choose two.)

A. The DNS ALG must be enabled.

B. static NAT

C. The DNS ALG must be disabled.

D. source NAT

Correct Answer: AD

Explanation: DNS Doctoring is a feature that allows a firewall to rewrite the source IP address of DNS requests to match the address of the interface on which the request is received. In order to achieve this two main features are used:

The DNS ALG (Application Layer Gateway) must be enabled: The DNS ALG is responsible for tracking and modifying DNS requests and responses. It allows the SRX Series firewall to understand the DNS protocol and to be able to rewrite

the source IP address of DNS requests.

Source NAT (Network Address Translation) is used: It is used to change the source IP address of the DNS request to match the address of the interface on which the request is received.

QUESTION 2

You opened a support ticket with JTAC for your Juniper ATP appliance. JTAC asks you to set up access to the device using the reverse SSH connection. Which three setting must be configured to satisfy this request? (Choose three.)

A. Enable JTAC remote access

B. Create a temporary root account.

C. Enable a JATP support account.

D. Create a temporary admin account.

E. Enable remote support.

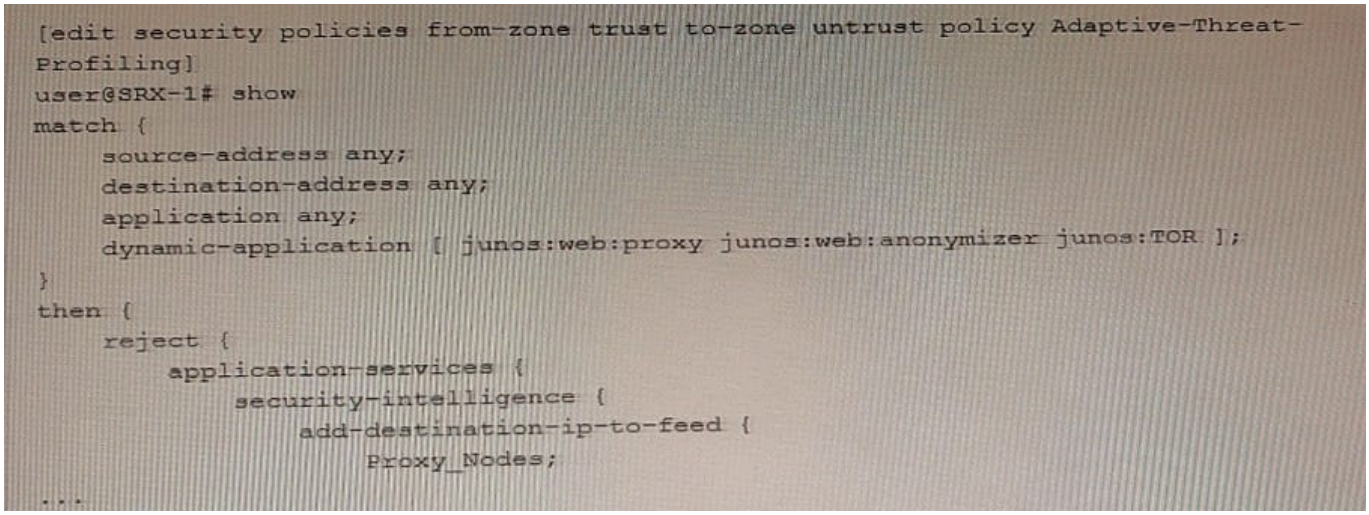
Correct Answer: CDE

https://kb.juniper.net/InfoCenter/index?page=contentandid=TN326andcat=andactp=LISTandshowDr aft=false

---

QUESTION 3

Exhibit



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

A. The SRX-1 device can use the Proxy__Nodes feed in another security policy.

B. You can use the Proxy_Nodes feed as the source-address and destination-address match criteria of another security policy on a different SRX Series device.

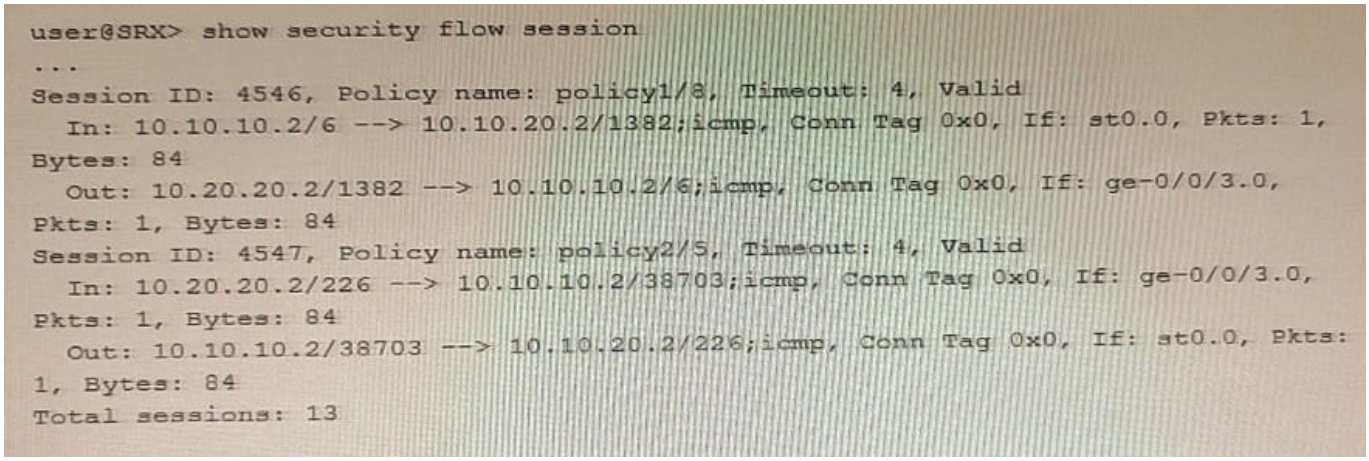
C. The SRX-1 device creates the Proxy_wodes feed, so it cannot use it in another security policy.

D. You can only use the Proxy_Node3 feed as the destination-address match criteria of another security policy on a different SRX Series device.

Correct Answer: AC

QUESTION 4

Exhibit



You are validating bidirectional traffic flows through your IPsec tunnel. The 4546 session represents traffic being sourced from the remote end of the IPsec tunnel. The 4547 session represents traffic that is sourced from the local network destined to the remote network.

Which statement is correct regarding the output shown in the exhibit?

A. The remote gateway address for the IPsec tunnel is 10.20.20.2

B. The session information indicates that the IPsec tunnel has not been established

C. The local gateway address for the IPsec tunnel is 10.20.20.2

D. NAT is being used to change the source address of outgoing packets

Correct Answer: B

QUESTION 5

Your IPsec VPN configuration uses two CoS forwarding classes to separate voice and data traffic. How many IKE security associations are required between the IPsec peers in this scenario?

B. 3

C. 4

D. 2

Correct Answer: A

Explanation: An IKE security association (SA) is a set of parameters that define how the Internet Key Exchange (IKE) protocol will authenticate and establish the secure channel between the IPsec VPN peers. When you configure an IPsec

VPN, one IKE SA is created between the peers, regardless of how many CoS forwarding classes are used to separate the traffic. The SA will be used to negotiate the IPsec SA parameters, such as encryption algorithms and keys.

In this scenario, only 1 IKE security association is required between the IPsec peers, no matter how many CoS forwarding classes are used to separate the voice and data traffic.