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.passapply.com/jn0-636.html

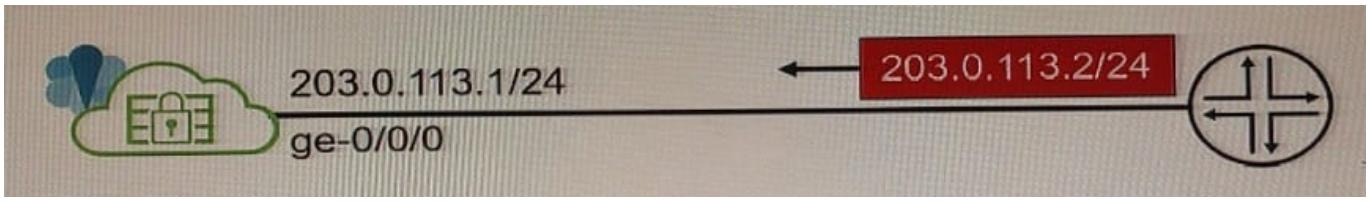
100% Passing Guarantee
100% Money Back Assurance

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

Exhibit



You configure Source NAT using a pool of addresses that are in the same subnet range as the external ge-0/0/0 interface on your vSRX device. Traffic that is exiting the internal network can reach external destinations, but the return traffic is being dropped by the service provider router.

Referring to the exhibit, what must be enabled on the vSRX device to solve this problem?

A. STUN

B. Proxy ARP

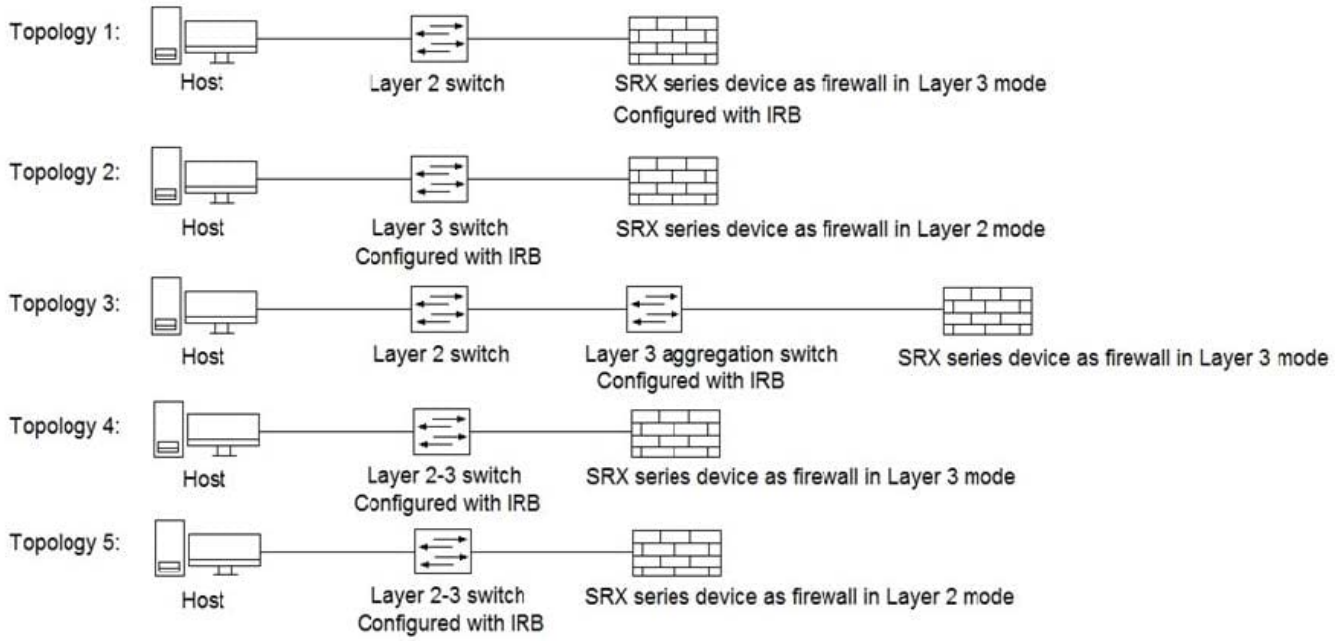
C. Persistent NAT

D. DNS Doctoring

Correct Answer: D

QUESTION 2

Click the Exhibit button.



Referring to the exhibit, which three topologies are supported by Policy Enforcer? (Choose three.)

A. Topology 3

B. Topology 5

C. Topology 2

D. Topology 4

E. Topology 1

Correct Answer: ADE

Reference: https://www.juniper.net/documentation/en_US/junos-space17.2/policy- enforcer/topics/concept/ policy-enforcer-deployment-supported-topologies.html

QUESTION 3

You want to enforce I DP policies on HTTP traffic.

In this scenario, which two actions must be performed on your SRX Series device? (Choose two)

A. Choose an attacks type in the predefined-attacks-group HTTP-All.

B. Disable screen options on the Untrust zone.

C. Specify an action of None.

D. Match on application junos-http.

Correct Answer: AD

Explanation: To enforce IDP policies on HTTP traffic on an SRX Series device, the following actions must be performed:

Choose an attacks type in the predefined-attacks-group HTTP-All: This allows the SRX Series device to match on specific types of attacks that can occur within HTTP traffic. For example, it can match on SQL injection or cross-site scripting

(XSS) attacks.

Match on application junos-http: This allows the SRX Series device to match on HTTP traffic specifically, as opposed to other types of traffic. It is necessary to properly identify the traffic that needs to be protected. Disabling screen options on

the Untrust zone and specifying an action of None are not necessary to enforce IDP policies on HTTP traffic. The first one is a feature used to prevent certain types of attacks, the second one is used to take no action in case of a match.

QUESTION 4

While troubleshooting security policies, you added the count action. Where do you see the result of this action?

A. In the show security policies hit-count command output.

B. In the show security flow statistics command output.

C. In the show security policies detail command output.

D. In the show firewall log command output.

Correct Answer: A

QUESTION 5

What is the purpose of the Switch Microservice of Policy Enforcer?

A. to isolate infected hosts

B. to enroll SRX Series devices with Juniper ATP Cloud

C. to inspect traffic for malware

D. to synchronize security policies to SRX Series devices

Correct Answer: D

Explanation: The Switch Microservice of Policy Enforcer is used to synchronize security policies to SRX Series devices. It receives the policy configuration from the Policy Manager and pushes it to the SRX Series devices. It\\'s responsible for configuring the security policies on the SRX devices, including firewall rules, VPN configurations, and other security features.

The purpose of the Switch Microservice of Policy Enforcer is to synchronize security policies to SRX Series devices. It allows administrators to quickly apply security policies across their network devices, ensuring consistent security settings. Additionally, it can help to prevent unauthorized access and malware propagation.