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.geekcert.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 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.

QUESTION 2

Your Source NAT implementation uses an address pool that contains multiple IPv4 addresses Your users report that when they establish more than one session with an external application, they are prompted to authenticate multiple times External hosts must not be able to establish sessions with internal network hosts.

What will solve this problem?

A. Disable PAT.

B. Enable destination NAT.

C. Enable persistent NAT

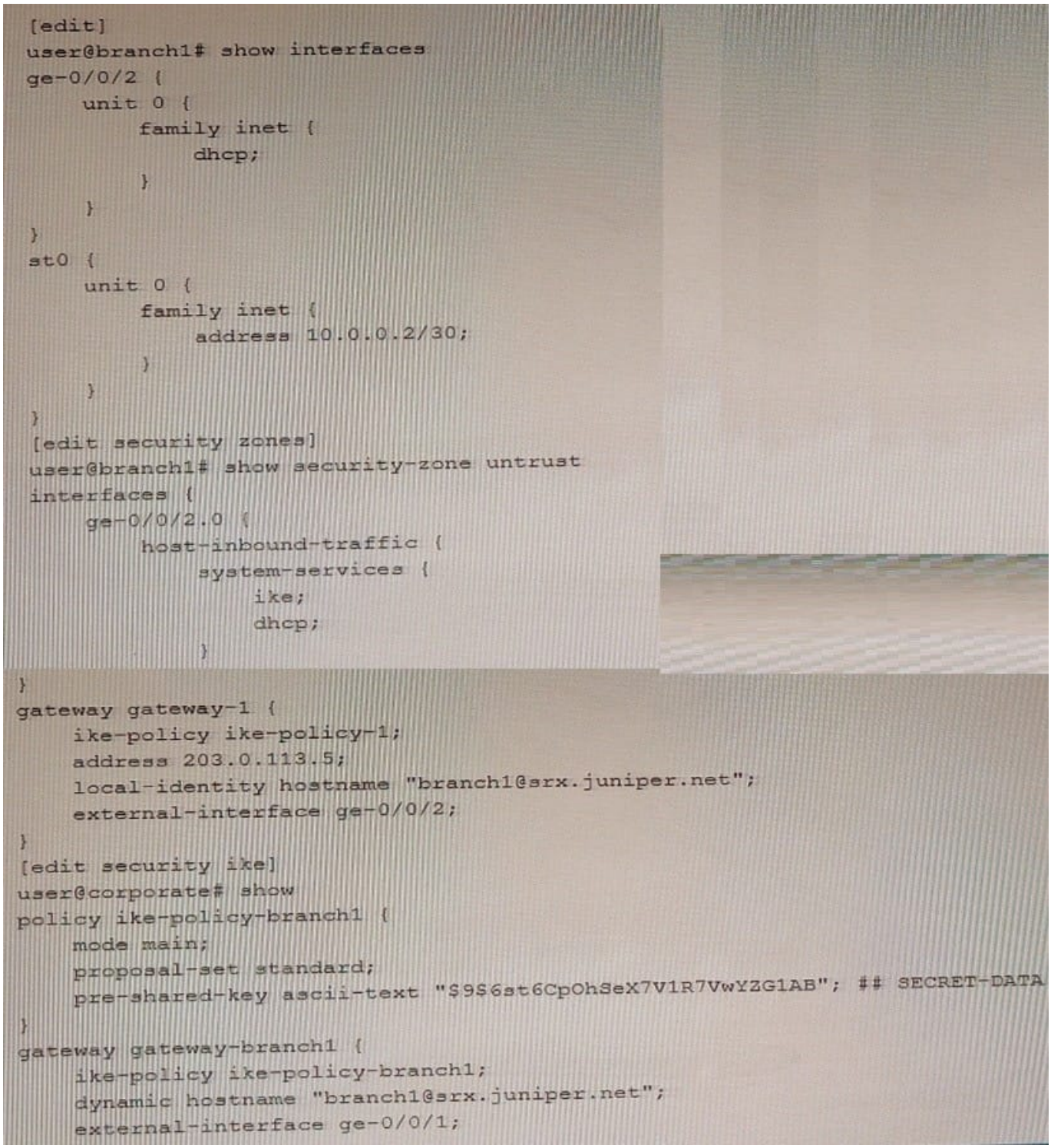
D. Enable address persistence.

Correct Answer: D

Explanation: The solution to this problem is to enable address persistence. This will ensure that the same external IP address is used for multiple sessions between an internal host and an external host. This will result in only one authentication being required, as the same external IP address will be used for all sessions.

QUESTION 3

Exhibit



You are trying to configure an IPsec tunnel between SRX Series devices in the corporate office and branch1. You have committed the configuration shown in the exhibit, but the IPsec tunnel is not establishing. In this scenario, what would solve this problem.

A. Add multipoint to the st0.0 interface configuration on the branch1 device.

B. Change the IKE proposal-set to compatible on the branch1 and corporate devices.

C. Change the local identity to inet advpn on the branch1 device.

D. Change the IKE mode to aggressive on the branch1 and corporate devices.

Correct Answer: C

QUESTION 4

In Juniper ATP Cloud, what are two different actions available in a threat prevention policy to deal with an infected host? (Choose two.)

A. Send a custom message

B. Close the connection.

C. Drop the connection silently.

D. Quarantine the host.

Correct Answer: BD

Explanation: In Juniper ATP Cloud, a threat prevention policy allows you to define how the system should handle an infected host. Two of the available actions are:

Close the connection: This action will close the connection between the infected host and the destination to which it is trying to connect. This will prevent the host from communicating with the destination and will stop any malicious activity.

Quarantine the host: This action will isolate the infected host from the network by placing it in a quarantine VLAN. This will prevent the host from communicating with other devices on the network, which will prevent it from spreading malware

or exfiltrating data.

Sending a custom message is used to notify the user and administrator of the action taken. Drop the connection silently is not an action available in Juniper ATP Cloud.

QUESTION 5

You issue the command shown in the exhibit.

Which policy will be active for the identified traffic?

A. Policy p4

B. Policy p7

C. Policy p1

D. Policy p12

Correct Answer: B

JN0-636 Practice Test JN0-636 Exam Questions JN0-636 Braindumps