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

QUESTION 1

Which statement is true about persistent NAT types?

A. The target-host-port parameter cannot be used with IPv4 addresses in NAT46.

B. The target-host parameter cannot be used with IPv6 addressee in NAT64.

C. The target-host parameter cannot be used with IPv4 addresses in NAT46

D. The target-host-port parameter cannot be used with IPv6 addresses in NAT64

Correct Answer: D

Explanation: NAT (Network Address Translation) is a method to map one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. There are different types of NAT, one of them is the persistent NAT which is a type of NAT that allows you to map the same internal IP address to the same external IP address each time a host initiates a connection.

QUESTION 2

Your organization has multiple Active Directory domain to control user access. You must ensure that security polices are passing traffic based upon the user\\'s access rights.

What would you use to assist your SRX series devices to accomplish this task?

A. JIMS

B. Junos Space

C. JSA

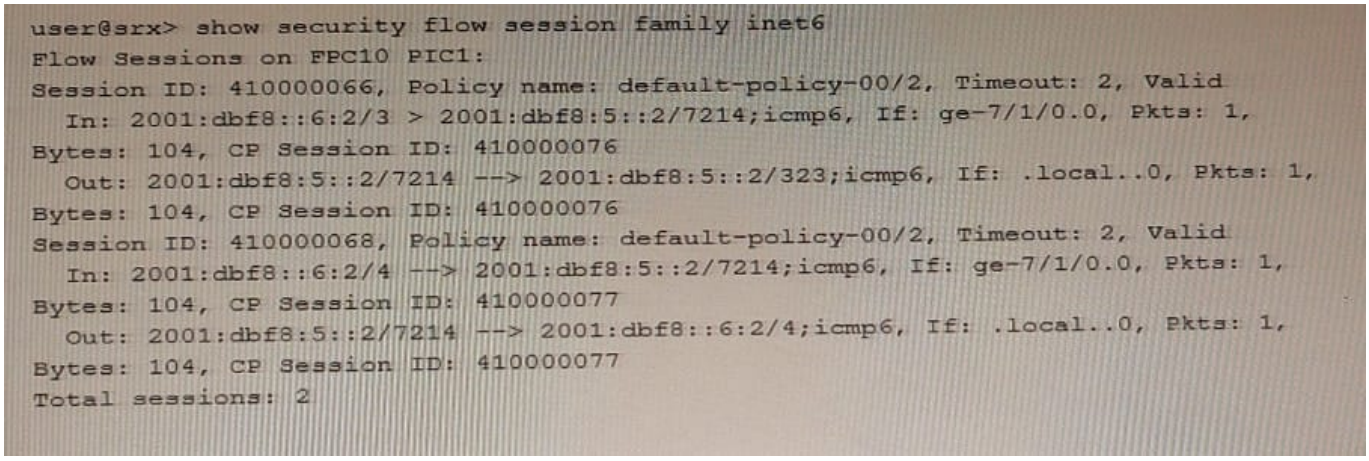
D. JATP Appliance

Correct Answer: A

Explanation: https://www.juniper.net/documentation/en_US/junos/topics/topic- map/security-user-auth-configure-jims.html

QUESTION 3

Exhibit



Which statement is true about the output shown in the exhibit?

A. The SRX Series device is configured with default security forwarding options.

B. The SRX Series device is configured with packet-based IPv6 forwarding options.

C. The SRX Series device is configured with flow-based IPv6 forwarding options.

D. The SRX Series device is configured to disable IPv6 packet forwarding.

Correct Answer: A

QUESTION 4

The monitor traffic interface command is being used to capture the packets destined to and the from the SRX Series device. In this scenario, which two statements related to the feature are true? (Choose two.)

A. This feature does not capture transit traffic.

B. This feature captures ICMP traffic to and from the SRX Series device.

C. This feature is supported on high-end SRX Series devices only.

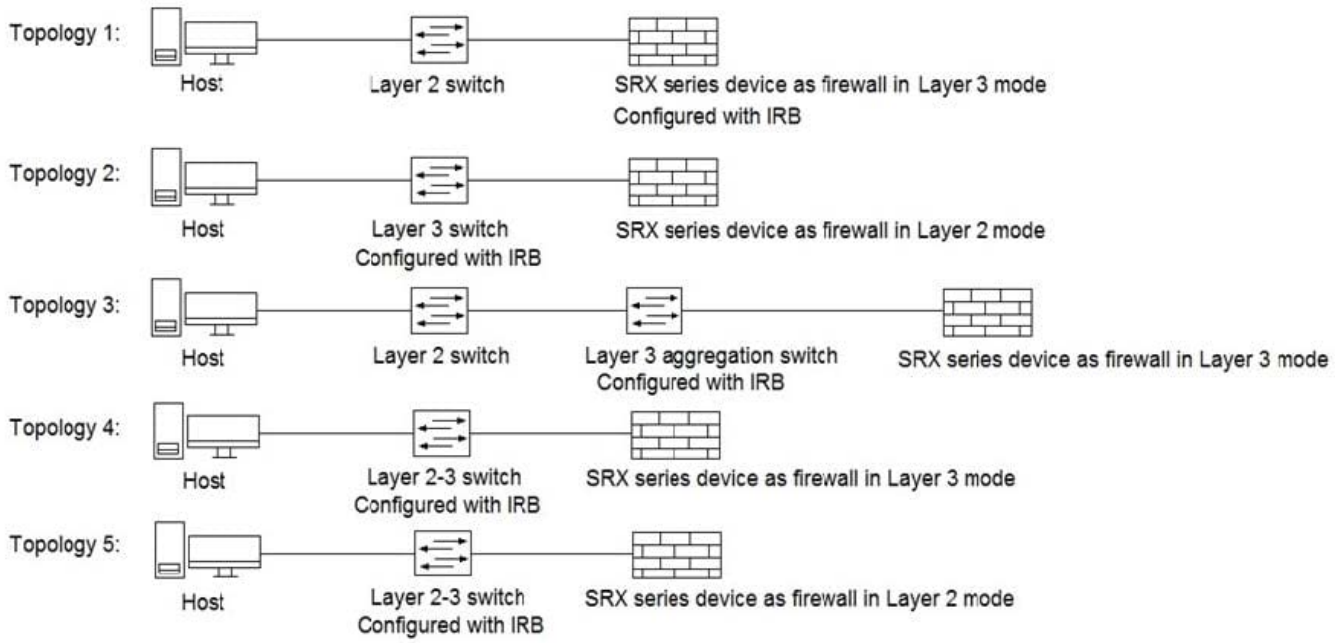
D. This feature is supported on both branch and high-end SRX Series devices.

Correct Answer: AD

Explanation: https://forums.juniper.net/t5/Ethernet-Switching/monitor-traffic-interface/td- p/462528

QUESTION 5

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 6

You are connecting two remote sites to your corporate headquarters site; you must ensure that all traffic is secured and only uses a single Phase 2 SA for both sites.

In this scenario, which VPN should be used?

A. An IPsec group VPN with the corporate firewall acting as the hub device.

B. Full mesh IPsec VPNs with tunnels between all sites.

C. A hub-and-spoke IPsec VPN with the corporate firewall acting as the hub device.

D. A full mesh Layer 3 VPN with the corporate firewall acting as the hub device.

Correct Answer: A

Explanation: https://www.juniper.net/us/en/local/pdf/app-notes/3500202-en.pdf

QUESTION 7

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 8

You want to identify potential threats within SSL-encrypted sessions without requiring SSL proxy to decrypt the session contents. Which security feature achieves this objective?

A. infected host feeds

B. encrypted traffic insights

C. DNS security

D. Secure Web Proxy

Correct Answer: C

QUESTION 9

To analyze and detect malware, Juniper ATP Cloud performs which two functions? (Choose two.)

A. cache lookup: to see if the file is seen already and known to be malicious

B. antivirus scan: with a single vendor solution to see if the file contains any potential threats

C. dynamic analysis: to see what happens if you execute the file in a real environment

D. static analysis: to see what happens if you execute the file in a real environment

Correct Answer: AC

Explanation: Juniper ATP Cloud performs cache lookup to see if the file is seen already and known to be malicious and dynamic analysis to see what happens if you execute the file in a real environment.

QUESTION 10

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.

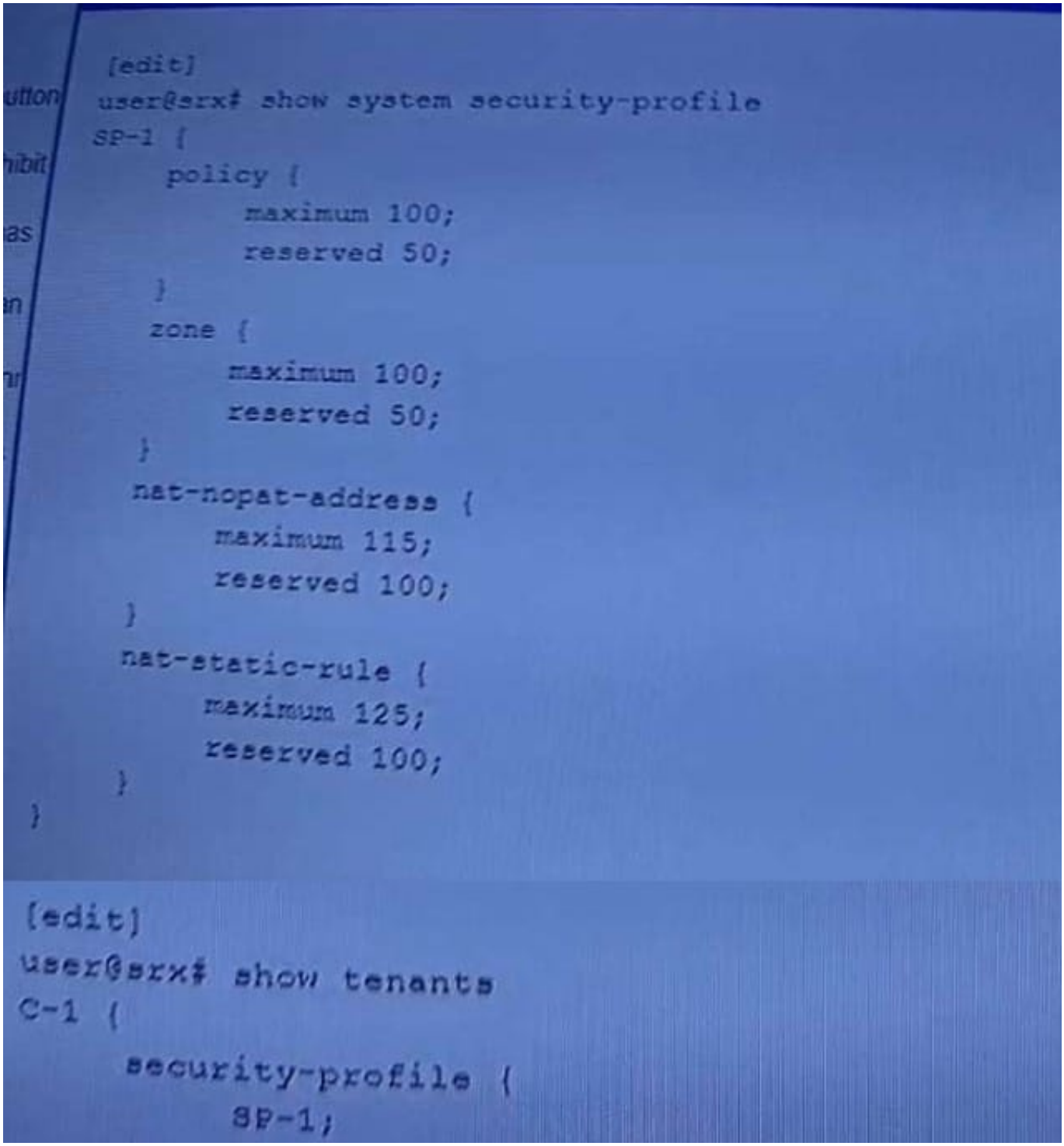
E. Enable remote support.

Correct Answer: CDE

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

QUESTION 11

Exhibit.



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

A. The c-1 TSYS has a reservation for the security flow resource.

B. The c-1 TSYS can use security flow resources up to the system maximum.

C. The c-1 TSYS cannot use any security flow resources.

D. The c-1 TSYS has no reservation for the security flow resource.

Correct Answer: CD

Explanation: https://www.juniper.net/documentation/en_US/junos/topics/topic- map/security-profile-logical-system.html

QUESTION 12

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 13

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 14

Which two types of source NAT translations are supported in this scenario? (Choose two.)

A. translation of IPv4 hosts to IPv6 hosts with or without port address translation

B. translation of one IPv4 subnet to one IPv6 subnet with port address translation

C. translation of one IPv6 subnet to another IPv6 subnet without port address translation

D. translation of one IPv6 subnet to another IPv6 subnet with port address translation

Correct Answer: AD

QUESTION 15

Exhibit

```
user@SRX> show security flow session
...
Session ID: 4546, Policy name: policy1/8, Timeout: 4, Valid
  In: 10.10.10.2/6 --> 10.10.20.2/1382;icmp, Conn Tag 0x0, If: st0.0, Pkts: 1,
Bytes: 84
  Out: 10.20.20.2/1382 --> 10.10.10.2/6;icmp, Conn Tag 0x0, If: ge-0/0/3.0,
Pkts: 1, Bytes: 84
Session ID: 4547, Policy name: policy2/5, Timeout: 4, Valid
  In: 10.20.20.2/226 --> 10.10.10.2/38703;icmp, Conn Tag 0x0, If: ge-0/0/3.0,
Pkts: 1, Bytes: 84
  Out: 10.10.10.2/38703 --> 10.10.20.2/226;icmp, Conn Tag 0x0, If: st0.0, Pkts:
1, Bytes: 84
Total sessions: 13
```

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