

DUMPS ARENA

Security, Professional (JNCIP-SEC)

Juniper JN0-634

Version Demo

Total Demo Questions: 10

Total Premium Questions: 65

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

You have configured a log collector VM and Security Director. System logging is enabled on a branch SRX Series device, but security logs do not appear in the monitor charts.

How would you solve this problem?

- A. Configure a security policy to forward logs to the collector.
- B. Configure application identification on the SRX Series device.
- C. Configure security logging on the SRX Series device.
- D. Configure J-Flow on the SRX Series device.

ANSWER: C**QUESTION NO: 2**

Your network includes SRX Series devices at the headquarters location. The SRX Series devices at this location are part of a high availability chassis cluster and are expected to support several UTM features.

Which two statements related to this environment are true? (Choose two.)

- A. UTM features can be configured on either of the nodes within the cluster.
- B. The chassis cluster must be configured for active/active mode.
- C. UTM features must be configured on the primary node within the cluster.
- D. The chassis cluster must be configured for active/backup mode.

ANSWER: A D**QUESTION NO: 3**

Click the Exhibit button.



- Referring to the exhibit, the host has been automatically blocked from communicating on the network because a malicious file was downloaded. You cleaned the infected host and changed the investigation status to Resolved – Fixed. What does Sky ATP do if the host then attempts to download a malicious file that would result in a threat score of 10?
- A. Sky ATP does not log the connection attempt and an SRX Series device does not allow the host to communicate on the network.
 - B. Sky ATP logs the connection attempt and an SRX Series device does not allow the host to communicate on the network.
 - C. Sky ATP logs the connection attempt and an SRX Series device allows the host to communicate on the network.
 - D. Sky ATP does not log the connection attempt and an SRX Series device allows the host to communicate on the network.

ANSWER: C

QUESTION NO: 4

You are configuring transparent mode on an SRX Series device. You must permit IP-based traffic only, and BPDUs must be restarted to the VLANs from which they originate.

Which configuration accomplishes these objectives?

- A. `bridge {block-non-ip-all;bpdu-vlan-flooding;}`
- B. `bridge {block-non-ip-all;bypass-non-ip-unicast;no-packet-flooding;}`
- C. `bridge {bypass-non-ip-unicast;bpdu-vlan-flooding;}`

D. bridge {block-non-ip-all;bypass-non-ip-unicast;bpdu-vlan-flooding;}

ANSWER: A

Explanation:

https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/family-ethernet-s

QUESTION NO: 5

Which IDP rule configuration will send an RST to any new session that meets the action criteria?

- A. ip-action block
- B. action close-client-and-server
- C. ip-action close
- D. action drop-connection

ANSWER: C

Explanation:

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-idp-policy-rules-and-rulebases.h

QUESTION NO: 6

You are implementing user authentication on your network using an SRX Series device and want to ensure that there are redundant forms of authentication for users to access the network. You have configured the device with the integrated user firewall and user role firewall features. You are testing failover methods using the default priority values.

In this scenario, which two statements are true? (Choose two.)

- A. If the user fails local authentication, then the Junos OS will attempt to authenticate the user with a user role firewall.
- B. If the user fails user role firewall authentication, then the Junos OS will attempt to authenticate the user with an integrated user firewall.
- C. If the user fails integrated user firewall authentication, then the Junos OS will attempt to authenticate with a user role firewall.
- D. If the user fails local authentication, then the Junos OS will attempt to authenticate the user with an integrated user firewall.

ANSWER: C D**QUESTION NO: 7**

Which two parameters are required to match in an IDP rule for the terminal option to take effect? (Choose two.)

- A. attacks custom-attacks
- B. attacks predefined-attacks
- C. application
- D. source-address

ANSWER: A B**Explanation:**

The IDP rulebase includes the option to mark a rule as a terminal rule. When a terminal rule matches source, destination, and service, IDP applies the rule and terminates rule matching. It does not matter whether the traffic matches the attack objects.

https://www.juniper.net/documentation/en_US/idp5.1/topics/concept/intrusion-detection-prevention-secu

QUESTION NO: 8

Using the Policy Controller API, which configuration would post Sky ATP with PE mode to the Policy Enforcer controller configuration?

- A. "configs": {"sdsn": false"cloudonly": true}
- B. "configs": {"sdsn": false"cloud": false}
- C. "configs": {"sdsn": true"cloudonly": false}
- D. "configs": {"sdsn": false"cloud": true}

ANSWER: C**Explanation:**

Based on the mode you have selected in the Policy Enforcer UI, you can specify the configuration using the Config API as follows:

Cloud only or cloud feeds mode—You can configure Policy Enforcer in the cloud only or cloud feeds mode as follows: “configs”: {“sdsn”: false “cloudonly”: true} Sky ATP mode—You can configure Policy Enforcer in the Sky ATP mode as follows: “configs”: {“sdsn”: false “cloudonly”: false} Sky ATP with Policy Enforcer mode—You can configure Policy Enforcer in the Sky ATP with Policy Enforcer mode as follows: “configs”: {“sdsn”: true “cloudonly”: false}

https://www.juniper.net/documentation/en_US/release-independent/policy-enforcer/topics/concept/policy-contro

QUESTION NO: 9

Your network includes SRX Series devices at all headquarter, data center, and branch locations. The headquarter and data center locations use high-end SRX Series devices, and the branch locations use branch SRX Series devices. You are asked to deploy IPS on the SRX Series devices using one of the available IPS deployment modes.

In this scenario, which two statements are true? (Choose two.)

- A. Inline tap mode provides enforcement.
- B. Inline tap mode can be used at all locations.
- C. Integrated mode can be used at all locations.
- D. Integrated mode provides enforcement.

ANSWER: C D**QUESTION NO: 10**

You are using the integrated user firewall feature on an SRX Series device.

Which three parameters are stored in the Active Directory authentication table? (Choose three.)

- A. IP address
- B. MAC address
- C. group mapping
- D. username
- E. password

ANSWER: A C D