DUMPSBOSS.

# Security, Specialist (JNCIS-SEC)

## Juniper JN0-335

## Version Demo

**Total Demo Questions: 10**

**Total Premium Questions: 65**

**Buy Premium PDF**

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

## QUESTION NO: 1

Which method does the IoT Security feature use to identify traffic sourced from IoT devices?

**A.** The SRX Series device streams metadata from the IoT device transit traffic to Juniper ATP Cloud Juniper ATP Cloud.

**B.** The SRX Series device streams transit traffic received from the IoT device to Juniper ATP Cloud.

**C.** The SRX Series device identifies IoT devices using their MAC address.

**D.** The SRX Series device identifies IoT devices from metadata extracted from their transit traffic.

## ANSWER: D

**Explanation:**

The metadata is used to identify the type of device, its associated activities and its threat profile. This information is used to determine the appropriate security policy for the device. For more information on IoT Security, please refer to the Juniper Security, Specialist (JNCIS-SEC) study guide.

## QUESTION NO: 2

Which two statements are correct about Juniper ATP Cloud? (Choose two.)

**A.** Once the target threshold is met, Juniper ATP Cloud continues looking for threats from 0 to 5 minutes.

**B.** Once the target threshold is met, Juniper ATP Cloud continues looking for threats levels range from 0 to 10 minutes.

**C.** The threat levels range from 0-10.

**D.** The threat levels range from 0-100.

## ANSWER: A C

**Explanation:**

According to the Juniper Networks JNCIS-SEC Study Guide, Juniper ATP Cloud sets target thresholds for security events and then continuously scans the environment for any activity that exceeds this threshold. Once the threshold is met, Juniper ATP Cloud continues looking for threats for a period of 0 to 5 minutes. The threat levels range from 0 to 10, with 0 being the lowest and 10 being the highest.

## QUESTION NO: 3

Which two statements are true about mixing traditional and unified security policies? (Choose two.)

**A.** When a packet matches a unified security policy, the evaluation process terminates

**B.** Traditional security policies must come before unified security policies

**C.** Unified security policies must come before traditional security policies

**D.** When a packet matches a traditional security policy, the evaluation process terminates

**ANSWER: A D**

## QUESTION NO: 4

Which two statements are correct about security policy changes when using the policy rematch feature? (Choose two.)

**A.** When a policy change includes changing the policy's action from permit to deny, all existing sessions are maintained

**B.** When a policy change includes changing the policy's source or destination address match condition, all existing sessions are dropped.

**C.** When a policy change includes changing the policy's action from permit to deny, all existing sessions are dropped.

**D.** When a policy change includes changing the policy's source or destination address match condition, all existing sessions are reevaluated.

**ANSWER: C D**

**Explanation:**

policy rematch is a feature that enables the device to reevaluate an active session when its associated security policy is modified. The session remains open if it still matches the policy that allowed the session initially. The session is closed if its associated policy is renamed, deactivated, or deleted1.

## QUESTION NO: 5

You are asked to determine how much traffic a popular gaming application is generating on your network.

Which action will you perform to accomplish this task?

**A.** Enable AppQoS on the proper security zones

**B.** Enable APBR on the proper security zones

**C.** Enable screen options on the proper security zones

**D.** Enable AppTrack on the proper security zones.

**ANSWER: D**

**Explanation:**

AppTrack is a feature of Juniper Networks firewall solutions that allows administrators to track applications, users, and the amount of traffic generated by those applications on the network. AppTrack can be enabled on specific security zones of the network to monitor traffic on those zones. This feature can be used to determine how much traffic a popular gaming application is generating on the network. For more information, please refer to the Juniper Networks JNCIS-SEC Study Guide.

Reference: Juniper Networks Security, Specialist (JNCIS-SEC) Study Guide, Chapter 4: AppSecure, page 4-15.

## QUESTION NO: 6

Which two statements are correct about chassis clustering? (Choose two.)

**A.** The node ID value ranges from 1 to 255.

**B.** The node ID is used to identify each device in the chassis cluster.

**C.** A system reboot is required to activate changes to the cluster.

**D.** The cluster ID is used to identify each device in the chassis cluster.

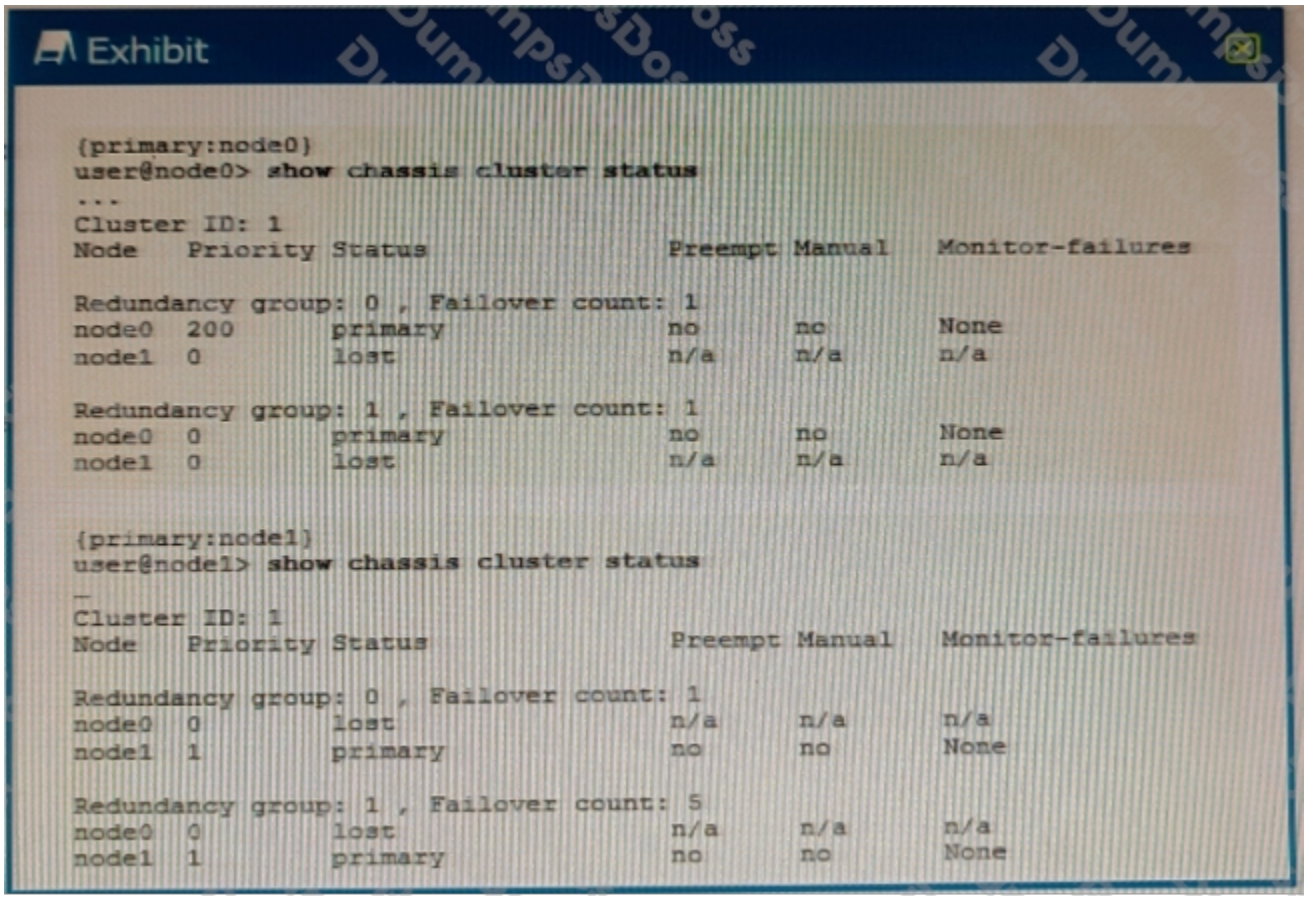
## ANSWER: A B

**Explanation:**

The node ID value ranges from 1 to 255 and is used to identify each device in the chassis cluster. The cluster ID is also used to identify each device, but it is not part of the node ID configuration. A system reboot is not required to activate changes to the cluster, but it is recommended to ensure that all changes are applied properly.

## QUESTION NO: 7

Exhibit




Referring to the exhibit, what do you determine about the status of the cluster.

**A.** Both nodes determine that they are in a primary state.

**B.** Node 1 is down

**C.** Node 2 is down.

**D.** There are no issues with the cluster.

**ANSWER: C**

## QUESTION NO: 8

You are experiencing excessive packet loss on one of your two WAN links route traffic from the degraded link to the working link

Which AppSecure component would you use to accomplish this task?

**A.** AppFW

**B.** AppQoE

**C.** AppQoS

**D.** APBR

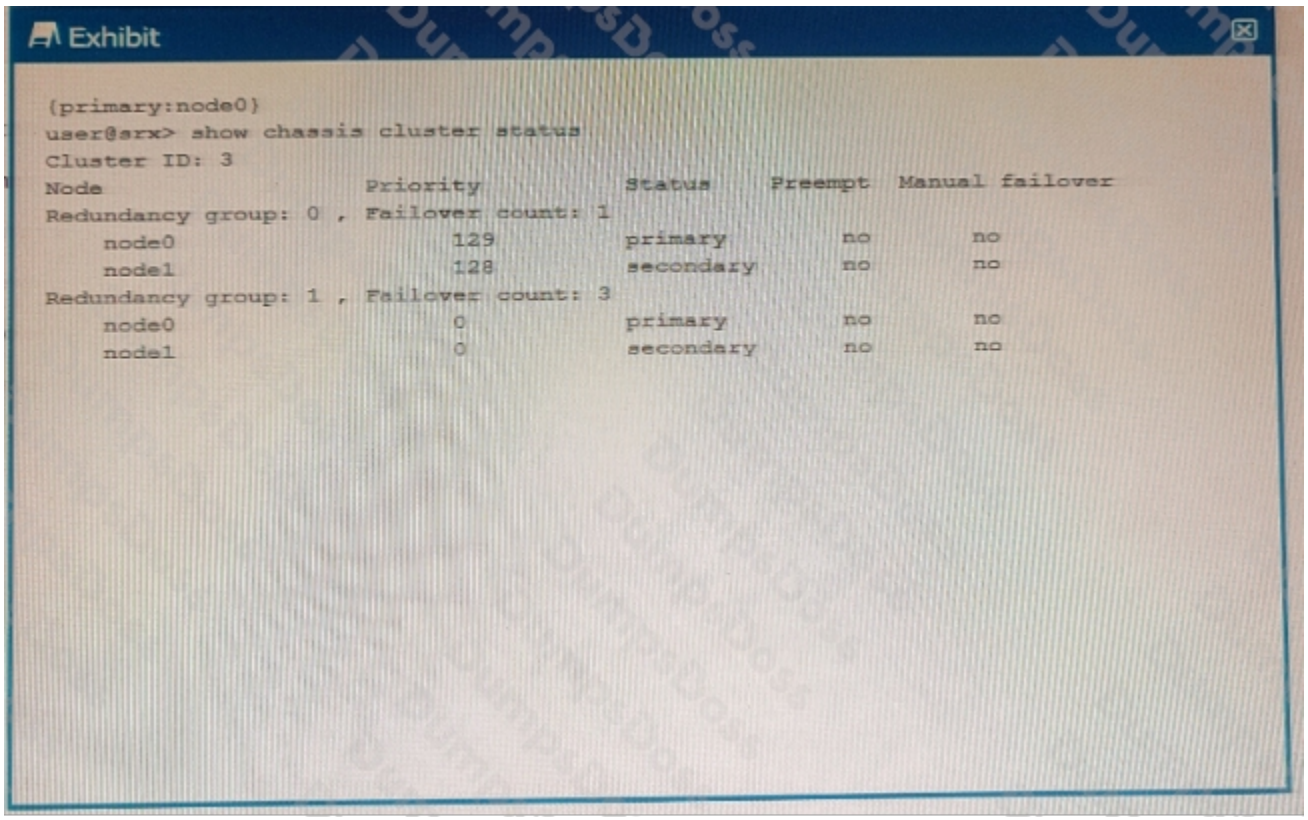
**ANSWER: D**

**Explanation:**

APBR (Application Path-Based Routing) is an AppSecure component which can be used to route traffic from the degraded link to the working link in order to reduce packet loss. APBR is a policy-based routing solution that allows you to configure rules to direct traffic to the most appropriate path, based on application, user, or network metrics.

## QUESTION NO: 9

Exhibit




Using the information from the exhibit, which statement is correct?

**A.** Redundancy group 1 is in an ineligible state.

**B.** Node1 is the active node for the control plane

**C.** There are no issues with the cluster.

**D.** Redundancy group 0 is in an ineligible state.

**ANSWER: A**

## QUESTION NO: 10

Your manager asks you to provide firewall and NAT services in a private cloud.

Which two solutions will fulfill the minimum requirements for this deployment? (Choose two.)

**A.** a single vSRX

**B.** a vSRX for firewall services and a separate vSRX for NAT services

**C.** a cSRX for firewall services and a separate cSRX for NAT services

**D.** a single cSRX

## ANSWER: B C

**Explanation:**

A single vSRX or cSRX cannot provide both firewall and NAT services simultaneously. To meet the minimum requirements for this deployment, you need to deploy a vSRX for firewall services and a separate vSRX for NAT services (option B), or a cSRX for firewall services and a separate cSRX for NAT services (option C). This is according to the Juniper Networks Certified Security Specialist (JNCIS-SEC) Study Guide.