Free Questions for JN0-335 by go4braindumps

Shared by Randolph on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You want to set up JSA to collect network traffic flows from network devices on your network.

Which two statements are correct when performing this task? (Choose two.)

Options:

A- BGP FlowSpec is used to collect traffic flows from Junos OS devices.

B- Statistical sampling increases processor utilization

C- Statistical sampling decreases event correlation accuracy.

D- Superflows reduce traffic licensing requirements.

Answer:

A, C

Explanation:

The two correct statements when performing this task are A. BGP FlowSpec is used to collect traffic flows from Junos OS devices, and C. Statistical sampling decreases event correlation accuracy. BGP FlowSpec is a Junos OS feature that allows network devices to send traffic flow information to a Juniper security device using BGP. This allows the Juniper security device to monitor and collect the traffic flows and analyze them for suspicious activity. Statistical sampling increases processor utilization by selecting only a subset of the data to be analyzed, which can help reduce the amount of data sent to the security device. However, this also decreases the accuracy of event correlation, as some events may be missed due to the sampling. Superflows reduce traffic licensing requirements by offloading the processing of certain traffic flows to the device itself, instead of having it sent to the security device.

Question 2

Question Type: MultipleChoice

What are two types of system logs that Junos generates? (Choose two.)

Options:

A- SQL log files

B- data plane logs

C- system core dump files

D- control plane logs

Answer:

B, D

Explanation:

The two types of system logs that Junos generates are control plane logs and data plane logs. Control plane logs are generated by the Junos operating system and contain system-level events such as system startup and shutdown, configuration changes, and system alarms. Data plane logs are generated by the network protocol processes and contain messages about the status of the network and its components, such as routing, firewall, NAT, and IPS. SQL log files and system core dump files are not types of system logs generated by Junos.

Question 3

Question Type: MultipleChoice

Which two statements are correct about the cSRX? (Choose two.)

Options:

A- The cSRX supports firewall, NAT, IPS, and UTM services.

B- The cSRX only supports Layer 2 'bump-in-the-wire' deployments.

C- The cSRX supports BGP, OSPF. and IS-IS routing services.

D- The cSRX has three default zones: trust, untrust, and management

Answer:

A, D

Explanation:

The two statements that are correct about the cSRX are that it supports firewall, NAT, IPS, and UTM services, and that it has three default zones: trust, untrust, and management. The cSRX is a software-defined security solution that provides comprehensive network security capabilities and is designed for virtualized environments. It supports firewall, NAT, IPS, and UTM services to protect against threats, as well as BGP, OSPF, and IS-IS routing services for routing functionality. Additionally, the cSRX has three default zones: trust, untrust, and management. The trust zone is used to define traffic that is allowed to enter the network, the untrust zone is used to define traffic that should be blocked from entering the network, and the management zone is used to manage the device itself. The cSRX does not support Layer 2 'bump-in-the-wire' deployments.

Question 4

Question Type: MultipleChoice

Which two statements about SRX Series device chassis clusters are true? (Choose two.)

Options:

A- Redundancy group 0 is only active on the cluster backup node.

B- Each chassis cluster member requires a unique cluster ID value.

C- Each chassis cluster member device can host active redundancy groups

D- Chassis cluster member devices must be the same model.

Answer:

B, C

Explanation:

B) Each chassis cluster member requires a unique cluster ID value: This statement is true. Each chassis cluster member must have a unique cluster ID assigned, which is used to identify each device in the cluster.

C) Each chassis cluster member device can host active redundancy groups: This statement is true. Both devices in a chassis cluster can host active redundancy groups, allowing for load balancing and failover capabilities.

The two statements about SRX Series device chassis clusters that are true are that each chassis cluster member requires a unique cluster ID value, and that each chassis cluster member device can host active redundancy groups. A unique cluster ID value is necessary so that all members of the cluster can be identified, and each chassis cluster member device can host active redundancy groups to ensure that the cluster is able to maintain high availability and redundancy. Additionally, it is not necessary for all chassis cluster member devices to be the same model, as long as all devices are running the same version of Junos software.

Question 5

Question Type: **MultipleChoice**

Exhibit

Exhibit

```
user@srx> show security flow session
Session ID: 61524, Policy name: Internet-access/9, Timeout: 48, Valid
  In: 10.10.12.37/37466 --> 10.111.111.254/80;tcp, Conn Tag: 0x0, If: ge-
0/0/0.0, Pkts: 3, Bytes: 1023,
  Out: 10.111.111.254/80 --> 10.10.12.37/9241;tcp, Conn Tag: 0x0, If: ge-
0/0/1.0, Pkts: 0, Bytes: 0,
user@srx> show services application-identification application-system-cache
Application System Cache Configurations:
  application-cache: on
    Cache lookup for security-services: off
    Cache lookup for miscellaneous-services: on
  cache-entry-timeout: 3600 seconds
pic: 0/0
Logical system name: root-logical-system
```

Referring to the exhibit which statement is true?

Options:

A- SSL proxy functions will ignore the session.

B- SSL proxy leverages post-match results.

C- SSL proxy must wait for return traffic for the final match to occur.

D- SSL proxy leverages pre-match result

Answer:

D

Question 6

Question Type: **MultipleChoice**

What are two benefits of using a vSRX in a software-defined network? (Choose two.)

Options:

A- scalability

B- no required software license

C- granular security

D- infinite number of interfaces

Answer:

A, C

Explanation:

Scalability: vSRX instances can be easily added or removed as the needs of the network change, making it a flexible option for scaling in a software-defined network.

Granular Security: vSRX allows for granular security policies to be enforced at the virtual interface level, making it an effective solution for securing traffic in a software-defined network.

The two benefits of using a vSRX in a software-defined network are scalability and granular security. Scalability allows you to increase the number of resources available to meet the demands of network traffic, while granular security provides a level of control and flexibility to your network security that is not possible with a traditional firewall. With a vSRX, you can create multiple levels of security policies, rules, and access control lists to ensure that only authorized traffic can enter and exit your network. Additionally, you would not require a software license to use the vSRX, making it an economical solution for those looking for increased security and flexibility.

Question 7

Question Type: MultipleChoice

Which two devices would you use for DDoS protection with Policy Enforcer? (Choose two.)

Options:

A- vQFX

B- MX

C- vMX

D- QFX

Answer:

B, C

Explanation:

The MX and vMX devices can be used for DDoS protection with Policy Enforcer. Policy Enforcer is a Juniper Networks solution that provides real-time protection from DDoS attacks. It can be used to detect and block malicious traffic, and also provides granular control over user access and policy enforcement. The MX and vMX devices are well-suited for use with Policy Enforcer due to their high-performance hardware and advanced security features.

Question 8

Question Type: MultipleChoice

Which solution enables you to create security policies that include user and group information?

Options:

A- JIMS

B- ATP Appliance

C- Network Director

D- NETCONF

Answer:

A

Explanation:

The solution that enables you to create security policies that include user and group information is JIMS (Juniper Identity Management Service). JIMS collects and maintains a large database of user, device, and group information from Active Directory domains or syslog sources, and enables SRX Series devices to rapidly identify thousands of users in a large, distributed enterprise. With JIMS, you can create security policies that include user and group information, and enforce user-based access control policies to protect network resources.

Question 9

Question Type: MultipleChoice

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?

Options:

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.