PASS

Juniper

JN0-335

Security, Specialist (JNCIS-SEC)

Question: 23

What are three capabilities of AppQoS? (Choose three.)

A. re-write DSCP values
B. assign a forwarding class
C. re-write the TTL
D. rate-limit traffic
E. reserve bandwidth

Answer: A,B,E

Explanation:

AppQoS (Application Quality of Service) is a Junos OS feature that provides advanced control and prioritization of application traffic. With AppQoS, you can classify application traffic, assign a forwarding class to the traffic, and apply quality of service (QoS) policies to the traffic. You can also re-write DSCP values and reserve bandwidthfor important applications. However, AppQoS does not re-write the TTL or rate-limit traffic.

Source: Juniper Networks, Security, Specialist (JNCIS-SEC) Study Guide. Chapter 3: AppSecure. Page 66-67.

Question: 24

You are asked to find systems running applications that increase the risks on your network. You must ensure these systems are processed through IPS and Juniper ATP Cloud for malware and virus protection.

Which Juniper Networks solution will accomplish this task?

A. JIMS
B. Encrypted Traffic Insights
C. UTM

D. Adaptive Threat Profiling

Answer: D

Explanation:

Adaptive Threat Profiling (ATP) is a Juniper Networks solution that enables organizations to detect malicious activity on their networks and process it through IPS and Juniper ATP Cloud for malware and virus protection. ATP is powered by Juniperâs advanced Machine Learning and Artificial Intelligence (AI) capabilities, allowing it to detect and block malicious activity in real-time. ATP is integrated with Juniperâs Unified Threat Management (UTM) and Encrypted Traffic Insights (ETI) solutions, providing an end-to-end network protection solution.

Question: 25

Which statement about security policy schedulers is correct?

A. Multiple policies can use the same scheduler.
B. A policy can have multiple schedulers.
C. When the scheduler is disabled, the policy will still be available.
D. A policy without a defined scheduler will not become active

Answer: A

Explanation:

Schedulers can be defined and reused by multiple policies, allowing for more efficient management of policy activation and deactivation. This can be particularly useful for policies that need to be activated during specific time periods, such as business hours or maintenance windows.

Question: 26

Exhibit
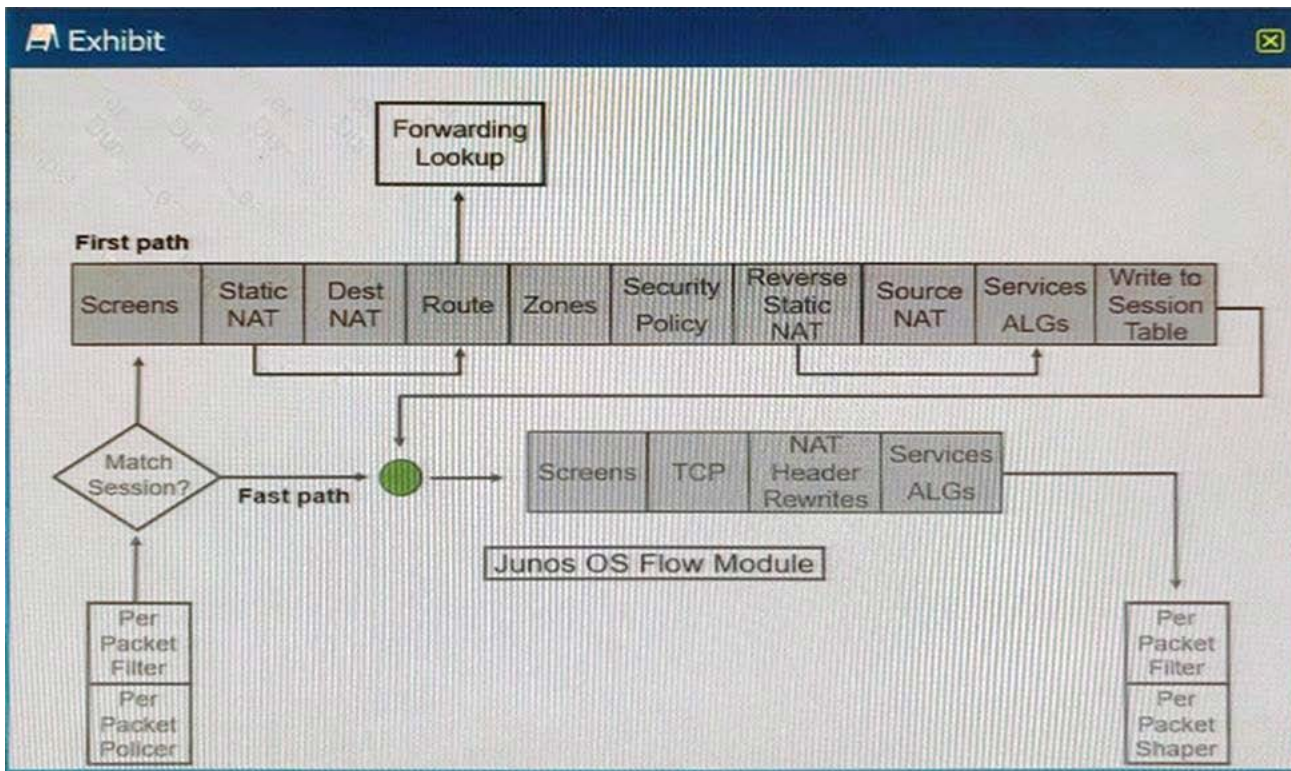
Referring to the SRX Series flow module diagram shown in the exhibit, where is application security processed?

A. Forwarding Lookup
B. Services ALGs
C. Security Policy
D. Screens

Answer: B

Question: 27

What information does encrypted traffic insights (ETI) use to notify SRX Series devices about known malware sites?

A. certificates
B. dynamic address groups
C. MAC addresses
D. domain names

Answer: D

Explanation:

Encrypted traffic insights (ETI) uses domain names to notify SRX Series devices about known malware sites. ETI is a feature of the SRX Series firewall that can detect and block malware that is hidden in encrypted traffic. It works by analyzing the domain names of the websites that the encrypted traffic is attempting to access. If the domain name matches a known malware site, ETIwill send an alert to the SRX Series device, which can then take appropriate action to block the traffic. ETI is a useful tool for protecting against threats that attempt to evade detection by hiding in encrypted traffic.

Question: 28

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.

Question: 29

You want to deploy a virtualized SRX in your environment.

In this scenario, why would you use a vSRX instead of a cSRX? (Choose two.)

A. The vSRX supports Layer 2 and Layer 3 configurations.
B. Only the vSRX provides clustering.
C. The vSRX has faster boot times.
D. Only the vSRX provides NAT, IPS, and UTM services

Answer: A,C

Explanation:

The vSRX supports both Layer 2 and Layer 3 configurations, while the cSRX is limited to Layer 3 configurations. Additionally, the vSRX has faster boot times, which is advantageous in certain scenarios. The vSRX and cSRX both provide NAT, IPS, and UTM services.

Question: 30

Regarding static attack object groups, which two statements are true? (Choose two.)

A. Matching attack objects are automatically added to a custom group.
B. Group membership automatically changes when Juniper updates the IPS signature database.
C. Group membership does not automatically change when Juniper updates the IPS signature database.
D. You must manually add matching attack objects to a custom group.

Answer: B,D

Question: 31

Which statement regarding Juniper Identity Management Service (JIMS) domain PC probes is true?

A. JIMS domain PC probes analyze domain controller security event logs at60-mmute intervals by default.
B. JIMS domain PC probes are triggered if no username to IP address mapping is found in the domain security event log.
C. JIMS domain PC probes are triggered to map usernames to group membership information.
D. JIMS domain PC probes are initiated by an SRX Series device to verify authentication table information.
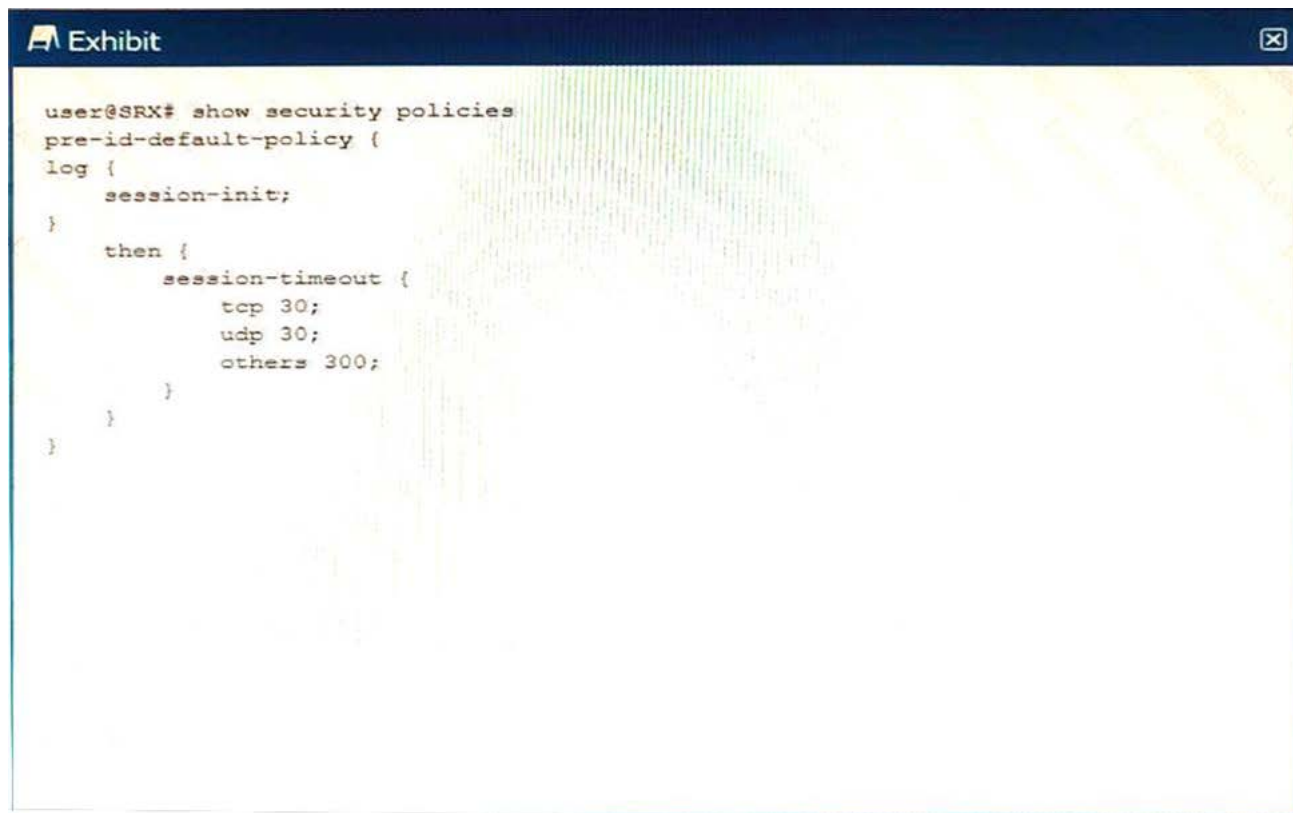
Answer: B

Explanation:

Juniper Identity Management Service (JIMS) domain PC probes are used to map usernames to IP addresses in the domain security event log. This allows for the SRX Series device to verify authentication table information, such as group membership. The probes are triggered whenever a username to IP address mapping is not found in the domain security event log. By default, the probes are executed at 60-minute intervals.

Question: 32

Exhibit


```
user@SRX# show security policies
pre-id-default-policy {
log {
    session-init;
}
    then {
        session-timeout {
            tcp 30;
            udp 30;
            others 300;
        }
    }
}
```

Which two statements are correct about the configuration shown in the exhibit? (Choose two.)

A. The session-class parameter in only used when troubleshooting.
B. The others 300 parameter means unidentified traffic flows will be dropped in 300 milliseconds.
C. Every session that enters the SRX Series device will generate an event
D. Replacing the session-init parameter with session-lose will log unidentified flows.

Answer: B,C

Explanation:

The configuration shown in the exhibit is for a Juniper SRX Series firewall. The session-init parameter is used to control how the firewall processes unknown traffic flows. With the session-init parameter set to 300, any traffic flows that the firewall does not recognize will be dropped after 300 milliseconds. Additionally, every session that enters the device, whether it is known or unknown, will generate an event, which can be used for logging and troubleshooting purposes. The session-lose parameter is used to control how the firewall handles established sessions that are terminated.

Question: 33

Which two statements are true about the vSRX? (Choose two.)

A. It does not have VMXNET3 vNIC support.
B. It has VMXNET3 vNIC support.
C. UNIX is the base O
D. Linux is the base O

Answer: B

Question: 34

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

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: 35

Which two statements are correct about SSL proxy server protection? (Choose two.)

A. You do not need to configure the servers to use the SSL proxy the function on the SRX Series device.
B. You must load the server certificates on the SRX Series device.
C. The servers must be configured to use the SSL proxy function on the SRX Series device.
D. You must import the root CA on the servers.

Answer: B,C

Explanation:

You must load the server certificates on the SRX Series device and configure the servers to use the SSL proxy function on the SRX Series device. This is done to ensure that the SSL proxy is able to decrypt the traffic between the client and server. Additionally, you must import the root CA on the servers in order for the SSL proxy to properly validate the server certificate.

SAMPLE QUESTIONS

These questions are for demo purpose only. **Full version** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.

Exam Dumps: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.

Practice Tests: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.

Updated Content: Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.

Technical Support: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.