

Juniper.JN0-335.by.Griam.76q

Number: JN0-335
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: JN0-335

Name: Juniper Security, Specialist



Exam A

QUESTION 1

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

Correct Answer: A, B, E

Section:

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 bandwidth for 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 2

You are implementing an SRX Series device at a branch office that has low bandwidth and also uses a cloud-based VoIP solution with an outbound policy that permits all traffic. Which service would you implement at your edge device to prioritize VoIP traffic in this scenario?

- A. AppFW
- B. SIP ALG
- C. AppQoS
- D. AppQoS

Correct Answer: D

Section:

Explanation:

The service that you would implement at your edge device to prioritize VoIP traffic in this scenario is AppQoS. AppQoS is a feature that enables you to allocate bandwidth and prioritize traffic based on application signatures or custom rules. AppQoS can enhance the quality of service and experience for critical or latency-sensitive applications, such as VoIP. You can configure AppQoS policies to assign different classes of service (CoS) values or queue numbers to different applications or traffic flows. You can also define bandwidth limits, guarantees, or bursts for each class or queue. Reference:= [Application Quality of Service Overview], [Configuring Application Quality of Service]

QUESTION 3

Which two functions does Juniper ATP Cloud perform to reduce delays in the inspection of files? (Choose two.)

- A. Juniper ATP Cloud allows the creation of allowlists.
- B. Juniper ATP Cloud uses a single antivirus software package to analyze files.
- C. Juniper ATP Cloud allows end users to bypass the inspection of files.
- D. Juniper ATP Cloud performs a cache lookup on files.

Correct Answer: A, D

Section:

Explanation:

Juniper ATP Cloud is a cloud-based service that provides advanced threat prevention and detection for your network. It integrates with SRX Series firewalls and MX Series routers to analyze files and network traffic for signs of malicious activity. Two functions that Juniper ATP Cloud performs to reduce delays in the inspection of files are:

Juniper ATP Cloud allows the creation of allowlists: Allowlists are lists of trusted files or file hashes that are excluded from scanning by Juniper ATP Cloud. You can create allowlists based on file name, file type, file size, file hash, or sender domain. By using allowlists, you can reduce the number of files that need to be uploaded to Juniper ATP Cloud for analysis and improve the performance and efficiency of your network.

Juniper ATP Cloud performs a cache lookup on files: Cache lookup is a process that checks if a file has been previously scanned by Juniper ATP Cloud and if there is a cached verdict for it. If there is a cached verdict, Juniper ATP Cloud returns it immediately without scanning the file again. If there is no cached verdict, Juniper ATP Cloud uploads the file for analysis. By using cache lookup, you can reduce the time and bandwidth required for scanning files by Juniper ATP Cloud.

QUESTION 4

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

- A. The chassis cluster data plane is connected with revenue ports.
- B. The chassis cluster can contain a maximum of three devices.
- C. The chassis cluster data plane is connected with SPC ports.
- D. The chassis cluster can contain a maximum of two devices.

Correct Answer: A, D

Section:**Explanation:**

Two statements that are correct about SRX Series device chassis clusters are:

The chassis cluster data plane is connected with revenue ports: A chassis cluster is a high-availability feature that groups two identical SRX Series devices into a cluster that acts as a single device. The cluster has two types of links: control links and fabric links. The control links are used for exchanging heartbeat messages and configuration synchronization between the nodes. The fabric links are used for forwarding data traffic between the nodes. The fabric links are connected with revenue ports, which are regular Ethernet interfaces that can also be used for normal traffic when not in cluster mode.

The chassis cluster can contain a maximum of two devices: A chassis cluster can only consist of two nodes: node 0 and node 1. The nodes must be the same model, have the same hardware configuration, run the same software version, and have the same license keys. The nodes share a common configuration and act as backup for each other in case of failure.

QUESTION 5

Which two statements are correct about the Junos IPS feature? (Choose two.)

- A. IPS is integrated as a security service on SRX Series devices.
- B. IPS uses sandboxinQ to detect unknown attacks.
- C. IPS is a standalone platform running on dedicated hardware or as a virtual device.
- D. IPS uses protocol anomaly rules to detect unknown attacks.

Correct Answer: A, D

Section:**Explanation:**

Junos IPS is a feature that provides intrusion prevention and detection services on SRX Series devices. It monitors network traffic and compares it against predefined signatures or custom rules to identify and block malicious or unwanted packets. Two statements that are correct about the Junos IPS feature are:

IPS is integrated as a security service on SRX Series devices: Junos IPS is not a separate platform or device, but a security service that runs on SRX Series firewalls. It can be enabled and configured as part of the security policy on the SRX Series device and applied to specific zones, interfaces, or traffic flows.

IPS uses protocol anomaly rules to detect unknown attacks: Junos IPS uses two types of rules to detect attacks: signature rules and protocol anomaly rules. Signature rules match traffic against known attack patterns or signatures and block them based on predefined actions. Protocol anomaly rules detect deviations from the expected behavior or structure of common protocols, such as TCP, UDP, ICMP, etc. Protocol anomaly rules can help identify unknown or zero-day attacks that may not have a signature yet.

QUESTION 6

You are asked to ensure that if the session table on your SRX Series device gets close to exhausting its resources, that you enforce a more aggressive age-out of existing flows. In this scenario, which two statements are correct? (Choose two.)

- A. The early-ageout configuration specifies the timeout value, in seconds, that will be applied once the low-watermark value is met.
- B. The early-ageout configuration specifies the timeout value, in seconds, that will be applied once the high-watermark value is met.
- C. The high-watermark configuration specifies the percentage of how much of the session table is left before disabling a more aggressive age-out timer.
- D. The high-watermark configuration specifies the percentage of how much of the session table can be allocated before applying a more aggressive age-out timer

Correct Answer: B, D

Section:

Explanation:

The early-ageout configuration specifies the timeout value, in seconds, that will be applied once the high-watermark value is met. The high-watermark configuration specifies the percentage of how much of the session table can be allocated before applying a more aggressive age-out timer. This ensures that the session table does not become full and cause traffic issues, and also ensures that existing flows are aged out quickly when the table begins to get close to being full.

QUESTION 7

Which two sources are used by Juniper Identity Management Service (JIMS) for collecting username and device IP addresses? (Choose two.)

- A. Microsoft Exchange Server event logs
- B. DNS
- C. Active Directory domain controller event logs
- D. OpenLDAP service ports

Correct Answer: B, C

Section:

Explanation:

Juniper Identity Management Service (JIMS) collects username and device IP addresses from both DNS and Active Directory domain controller event logs. DNS is used to resolve hostnames to IP addresses, while Active Directory domain controller event logs are used to get information about user accounts, such as when they last logged in.

QUESTION 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

Correct Answer: D

Section:

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 9

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

- A. JIMS



- B. ATP Appliance
- C. Network Director
- D. NETCONF

Correct Answer: A

Section:

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 10

You want to control when cluster failovers occur.

In this scenario, which two specific parameters would you configure on an SRX Series device? (Choose two.)

- A. hearcbeac-interval
- B. heartbeat-address
- C. hearcbeat-cos
- D. hearcbeac-chreshold

Correct Answer: A, D

Section:

Explanation:

To control when cluster failovers occur, you need to configure two specific parameters on an SRX Series device: heartbeat-interval and heartbeat-threshold. These parameters determine how often the nodes in a cluster exchange heartbeat messages and how many consecutive heartbeats can be missed before a failover is triggered. The heartbeat-interval specifies the time interval in seconds between each heartbeat message. The default value is 1 second and the range is from 0.1 to 10 seconds. The heartbeat-threshold specifies the number of consecutive heartbeats that must be missed before a failover occurs. The default value is 3 and the range is from 2 to 255. Reference:="Configuring Chassis Clustering on SRX Series Devices,Chassis Cluster Redundancy Group Failover

QUESTION 11

You administer a JSA host and want to include a rule that sets a threshold for excessive firewall denies and sends an SNMP trap after receiving related syslog messages from an SRX Series firewall.

Which JSA rule type satisfies this requirement?

- A. common
- B. offense
- C. flow
- D. event

Correct Answer: D

Section:

Explanation:

To include a rule that sets a threshold for excessive firewall denies and sends an SNMP trap after receiving related syslog messages from an SRX Series firewall, you need to use an event rule type in JSA. An event rule type allows you to create custom rules based on the events that are collected and normalized by JSA from various sources, such as firewalls, routers, switches, servers, and so on. You can define the conditions, tests, and actions for an event rule, such as matching a specific event name, setting a threshold for the number of occurrences, and sending an SNMP trap to a specified host. Reference:="Creating a Custom Rule,Customizing the SNMP Trap Output

QUESTION 12

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

- A. The DNS ALG supports DDNS.

- B. The DNS ALG supports VPN tunnels.
- C. The DNS ALG performs DNS doctoring.
- D. The DNS ALG does not support NAT.

Correct Answer: A, C

Section:

Explanation:

The DNS ALG is an application layer gateway that handles data associated with locating and translating domain names into IP addresses. It runs on port 53 and monitors DNS query and reply packets. Two statements about the DNS ALG that are correct are:

The DNS ALG supports DDNS: DDNS is Dynamic DNS, which is a method of updating DNS records in real time to reflect changes in network configurations or hostnames. The DNS ALG can process DDNS messages differently from DNS messages and perform address translation in the query part of the message.

The DNS ALG performs DNS doctoring: DNS doctoring is a technique of modifying the DNS reply packets to replace the original IP addresses with translated IP addresses that are suitable for the destination network. This allows the clients to access servers that are located behind NAT devices or in different networks.

QUESTION 13

You want to be alerted if the wrong password is used more than three times on a single device within five minutes.

Which Juniper Networks solution will accomplish this task?

- A. Adaptive Threat Profiling
- B. Juniper Secure Analytics
- C. Juniper Identity Management Service
- D. Intrusion Prevention System

Correct Answer: B

Section:

Explanation:

The Juniper Networks solution that will accomplish the task of alerting if the wrong password is used more than three times on a single device within five minutes is Juniper Secure Analytics (JSA). JSA is a security intelligence platform that collects, analyzes, and correlates network data from various sources, such as firewalls, routers, switches, servers, and applications. JSA can detect and respond to threats, anomalies, and vulnerabilities in real time using rules, offenses, reports, and dashboards. JSA can also integrate with JIMS (Juniper Identity Management Service) to obtain user identity information from Active Directory domains or syslog sources. JSA can use this information to create custom rules that trigger offenses or alerts based on user behavior or activity, such as failed login attempts or password changes.

QUESTION 14

While working on an SRX firewall, you execute the `show security policies policy-name <name> detail` command.

Which function does this command accomplish?

- A. It displays details about the default security policy.
- B. It identifies the different custom policies enabled.
- C. It shows the system log files for the local SRX Series device.
- D. It shows policy counters for a configured policy.

Correct Answer: D

Section:

Explanation:

The function that the `show security policies policy-name <name> detail` command accomplishes is showing policy counters for a configured policy. Policy counters are statistics that indicate how many times a policy has been matched by traffic and what actions have been taken by the policy. Policy counters can help you monitor and troubleshoot the performance and effectiveness of your security policies. The `show security policies policy-name <name> detail` command displays detailed information about a specific policy, such as its source zone, destination zone, description, state, hit count, byte count, packet count, action count, and session count.

QUESTION 15



Your JIMS server is unable to view event logs.

Which two actions would you take to solve this issue? (Choose two.)

- A. Enable the correct host-inbound-traffic rules on the SRX Series devices.
- B. Enable remote event log management within Windows Firewall on the necessary Exchange servers.
- C. Enable remote event log management within Windows Firewall on the necessary domain controllers.
- D. Enable remote event log management within Windows Firewall on the JIMS server.

Correct Answer: B, C

Section:

Explanation:

If your JIMS server is unable to view event logs, two actions that you would take to solve this issue are:

Enable remote event log management within Windows Firewall on the necessary Exchange servers: JIMS (Juniper Identity Management Service) is a Windows service that collects user, device, and group information from Active Directory domains or syslog sources and provides it to SRX Series devices for identity-based security policies. JIMS relies on the event logs generated by the domain controllers and Exchange servers to track user logins, logouts, and IP address changes. If the Windows Firewall on the Exchange servers blocks the remote event log management, JIMS cannot access the event logs and obtain the user identity information. Therefore, you need to enable remote event log management within Windows Firewall on the Exchange servers that are configured as event sources in JIMS.

Enable remote event log management within Windows Firewall on the necessary domain controllers: Similarly, if the Windows Firewall on the domain controllers blocks the remote event log management, JIMS cannot access the event logs and obtain the user identity information. Therefore, you need to enable remote event log management within Windows Firewall on the domain controllers that are configured as event sources in JIMS.

QUESTION 16

Which two statements are correct about the fab interface in a chassis cluster? (Choose two.)

- A. Real-time objects (RTOs) are exchanged on the fab interface to maintain session synchronization.
- B. In an active/active configuration, inter-chassis transit traffic is sent over the fab interface.
- C. The fab interface enables configuration synchronization.
- D. Heartbeat signals sent on the fab interface monitor the health of the control plane link.

Correct Answer: A, B

Section:

Explanation:

The fab interface is a fabric link that connects the two nodes in a chassis cluster. A chassis cluster is a high-availability feature that groups two identical SRX Series devices into a cluster that acts as a single device. The fab interface has two functions:

Real-time objects (RTOs) are exchanged on the fab interface to maintain session synchronization: RTOs are data structures that store information about active sessions, such as source and destination IP addresses, ports, protocols, and security policies. RTOs are exchanged between the nodes on the fab interface to ensure that both nodes have the same session information and can take over the traffic in case of a failover.

In an active/active configuration, inter-chassis transit traffic is sent over the fab interface: In an active/active configuration, both nodes in a cluster can process traffic for different redundancy groups (RGs). RGs are collections of interfaces or services that fail over together from one node to another. If traffic needs to transit from one RG to another RG that is active on a different node, it is sent over the fab interface.

QUESTION 17

On an SRX Series firewall, what are two ways that Encrypted Traffic Insights assess the threat of the traffic? (Choose two.)

- A. It decrypts the file in a sandbox.
- B. It validates the certificates used.
- C. It decrypts the data to validate the hash.
- D. It reviews the timing and frequency of the connections.

Correct Answer: B, D

Section:

Explanation:

Encrypted Traffic Insights is a feature that enables the SRX Series firewall and the ATP Cloud to detect malicious threats that are hidden in encrypted traffic without decrypting the traffic. It does so by analyzing the metadata and connection patterns of the encrypted sessions. Two ways that Encrypted Traffic Insights assess the threat of the traffic are:

It validates the certificates used: The SRX Series firewall extracts the server certificate from the encrypted session and compares its signature with a blocklist of known malicious certificates provided by ATP Cloud. If there is a match, the session is blocked and reported as a threat.

It reviews the timing and frequency of the connections: The SRX Series firewall sends the connection details, such as source and destination IP addresses, ports, protocols, and timestamps, to ATP Cloud. ATP Cloud applies behavior analysis and machine learning algorithms to detect anomalous or suspicious patterns of connections, such as high frequency, low duration, or unusual timing.

QUESTION 18

Click the Exhibit button.




```

user@host> show configuration policy-options
  prefix-list manager-ip {
    10.0.0.0/8;
    192.168.4.254/32;
  }
user@host> show configuration firewall
  filter manager-ip {
    term block_non_manager {
      from {
        source-address {
          0.0.0.0/0;
        }
        source-prefix-list {
          manager-ip except;
        }
        protocol tcp;
        destination-port [ ssh https telnet http ];
      }
      then {
        discard;
      }
    }
    term accept_everything_else {
      then accept;
    }
  }
user@host> show configuration interfaces lo0
unit 0 {
  family inet {
    filter {
      input manager-ip;
    }
  }
}

```



You are validating the configuration template for device access. The commands in the exhibit have been entered to secure IP access to an SRX Series device. Referring to the exhibit, which two statements are true? (Choose two.)

- A. The device manager can access the device from 192.168.11.248.
- B. The loopback interface blocks invalid traffic on its entry into the device.
- C. The loopback interface blocks invalid traffic on its exit from the device.
- D. The device manager can access the device from 10.253.1.2.

Correct Answer: B, D

Section:

Explanation:

The commands in the exhibit show how to configure a firewall filter on the loopback interface (lo0) of an SRX Series device. The loopback interface is a gateway for all the control traffic that enters the Routing Engine of the device. The firewall filter can be used to monitor and protect this control traffic from various attacks. Two statements that are true based on the exhibit are:

The loopback interface blocks invalid traffic on its entry into the device: The firewall filter applied on lo0 has a term that matches any packet with an invalid source address (such as 0.0.0.0/8 or 127.0.0.0/8) and discards it. This prevents spoofing or DoS attacks using invalid source addresses.

The device manager can access the device from 10.253.1.2: The firewall filter applied on lo0 has a term that matches any packet with a source address of 10.253.1.2 and accepts it. This allows the device manager to access the device from this IP address using protocols such as SSH, Telnet, HTTP, or HTTPS.

QUESTION 19

Click the Exhibit button.

```
user@srx> show chassis cluster status redundancy-group 1
```

```
Cluster: 1, Redundancy-Group: 1
```

Device name	Priority	Status	Preempt
Manual failover			
node0	0	Secondary	No
node1	200	Primary	No

Which two statements describe the output shown in the exhibit? (Choose two.)

- A. Redundancy group 1 experienced an operational failure.
- B. Redundancy group 1 was administratively failed over.
- C. Node 0 is controlling traffic for redundancy group 1.
- D. Node 1 is controlling traffic for redundancy group 1.

Correct Answer: B, D

Section:

Explanation:

The output shown in the exhibit displays the status of a chassis cluster redundancy group (RG) on an SRX Series device. A chassis cluster RG is a collection of objects, such as interfaces or services, that fail over together from one node to another in case of a failure or manual intervention. A chassis cluster RG can be primary on one node and backup on another node at any given time. Two statements that describe the output shown in the exhibit are:

Redundancy group 1 was administratively failed over: The output shows that redundancy group 1 has "Manual failover" set to "Yes". This indicates that redundancy group 1 was manually switched from one node to another using the request chassis cluster failover redundancy-group command.

Node 1 is controlling traffic for redundancy group 1: The output shows that node 1 has "Status" set to "Primary" for redundancy group 1. This means that node 1 is active and controlling traffic for redundancy group 1.

QUESTION 20

What are two requirements for enabling AppQoE? (Choose two.)

- A. You need two SRX Series device endpoints.
- B. You need two SRX Series or MX Series device endpoints.
- C. You need an APPID feature license.
- D. You need to configure AppQoS for reverse traffic.

Correct Answer: B, C

Section:

Explanation:

AppQoS is a feature that enables you to monitor and optimize the quality of experience for applications on your network. It uses application-aware routing and dynamic path selection to choose the best path for each application based on predefined or custom SLA profiles. AppQoS also provides visibility and reporting on application performance and network conditions. Two requirements for enabling AppQoS are:

You need two SRX Series or MX Series device endpoints: AppQoS can be configured between two SRX Series device endpoints or between an SRX Series device and an MX Series device in a hub-and-spoke or full mesh topology. The devices must run the same version of Junos OS and have the same AppQoS configuration.

You need an APPID feature license: AppQoS requires an APPID feature license to be installed on the SRX Series device. The APPID feature license enables application identification and classification, which are essential for AppQoS to work.

QUESTION 21

How does Juniper ATP Cloud protect a network from zero-day threats?

- A. It uses a cache lookup.
- B. It uses antivirus software.
- C. It uses dynamic analysis.
- D. It uses known virus signatures.

Correct Answer: C

Section:

Explanation:

Juniper ATP Cloud is a cloud-based service that provides advanced threat prevention and detection for your network. It integrates with SRX Series firewalls and MX Series routers to analyze files and network traffic for signs of malicious activity. Juniper ATP Cloud protects a network from zero-day threats by using dynamic analysis, which is a method of executing files in a sandbox environment and observing their behavior and network interactions. Dynamic analysis can uncover unknown malware that may evade static analysis or signature-based detection methods.

QUESTION 22

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.

Correct Answer: B, C

Section:

Explanation:

static attack object groups are predefined groups of attack objects that are included in Juniper's IPS signature database. These groups do not change automatically when Juniper updates the database.

QUESTION 23

You are deploying a new SRX Series device and you need to log denied traffic.

In this scenario, which two policy parameters are required to accomplish this task? (Choose two.)

- A. session-init



- B. session-close
- C. deny
- D. count

Correct Answer: B, C

Section:

Explanation:

you need to create a global firewall rulebase that matches RT_FLOW_SESSION_DENY events². To do this, you need to specify two policy parameters: deny and session-close³.

QUESTION 24

You are asked to reduce the load that the JIMS server places on your network. Which action should you take in this situation?

- A. Connect JIMS to the RADIUS server
- B. Connect JIMS to the domain Exchange server
- C. Connect JIMS to the domain SQL server.
- D. Connect JIMS to another SRX Series device.

Correct Answer: D

Section:

Explanation:

JIMS server is a Juniper Identity Management Service that collects user identity information from different authentication sources for SRX Series devices^{1,2}. It can connect to SRX Series devices and CSO platform in your network¹.

JIMS server is a service that protects corporate resources by authenticating and restricting user access based on roles². It connects to SRX Series devices and CSO platform to provide identity information for firewall policies¹. To reduce the load that JIMS server places on your network, you should connect JIMS to another SRX Series device¹. This way, you can distribute the identity information among multiple SRX Series devices and reduce network traffic.

QUESTION 25

Which two statements about unified security policies are correct? (Choose two.)

- A. Unified security policies require an advanced feature license.
- B. Unified security policies are evaluated after global security policies.
- C. Traffic can initially match multiple unified security policies.
- D. APPID results are used to determine the final security policy

Correct Answer: C, D

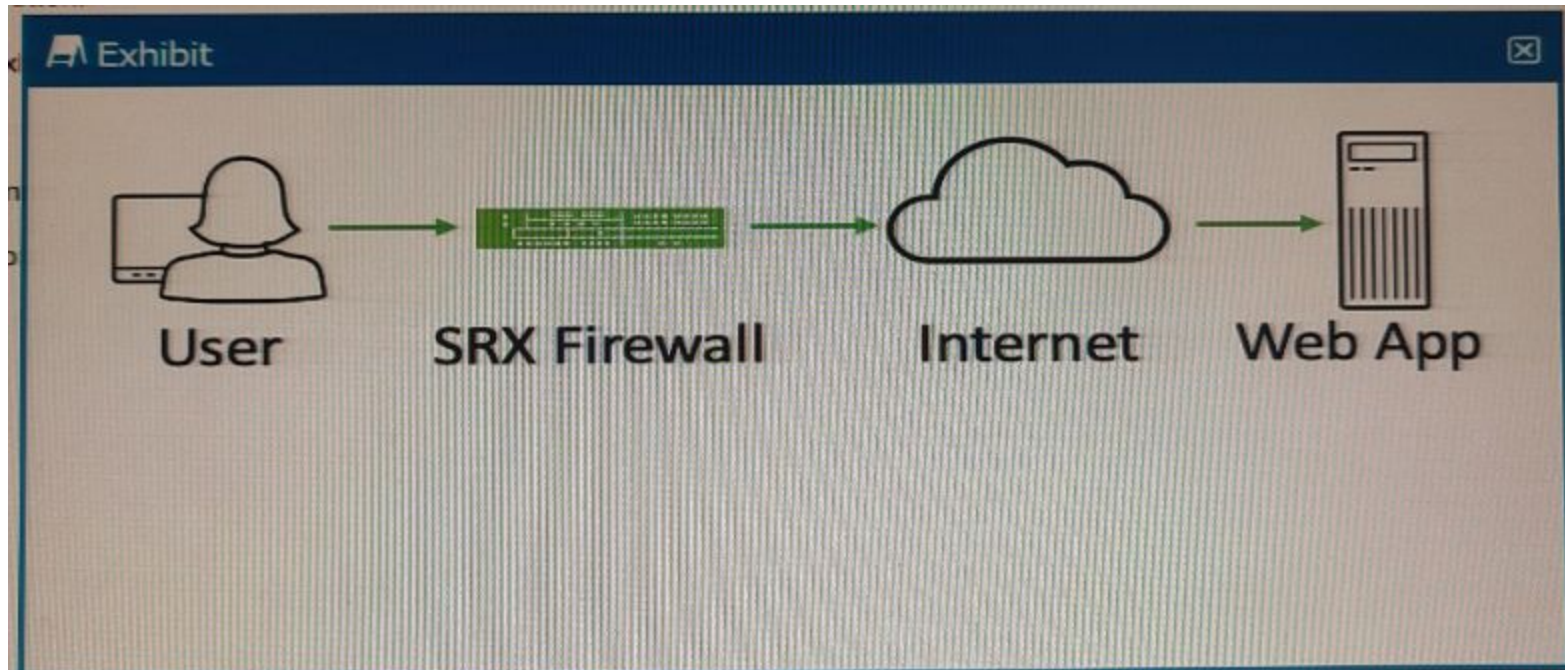
Section:

Explanation:

Unified security policies are security policies that enable you to use dynamic applications as match conditions along with existing 5-tuple or 6-tuple matching conditions^{1,2}. They simplify application-based security policy management at Layer 7 and provide greater control and extensibility to manage dynamic applications traffic³.

QUESTION 26

Exhibit



Referring to the exhibit, which two statements describe the type of proxy used? (Choose two.)

- A. forward proxy
- B. client protection proxy
- C. server protection proxy
- D. reverse proxy

Correct Answer: B, C

Section:

Explanation:

B) Client protection proxy: This statement is incorrect because a forward proxy can also be called a client protection proxy since it protects the user's identity and computer information from the web server.

C) Server protection proxy: This statement is incorrect because a reverse proxy can also be called a server protection proxy since it protects the web server's identity and location from the user.

QUESTION 27

You have deployed an SRX300 Series device and determined that files have stopped being scanned.

In this scenario, what is a reason for this problem?

- A. The software license is a free model and only scans executable type files.
- B. The infected host communicated with a command-and-control server, but it did not download malware.
- C. The file is too small to have a virus.
- D. You have exceeded the maximum files submission for your SRX platform size.

Correct Answer: D

Section:

Explanation:

You have exceeded the maximum files submission for your SRX platform size: This statement is incorrect because file scanning on SRX300 Series device has a limit on the number of files that can be submitted per minute based on the platform size. For example, SRX320 has a limit of 10 files per minute.

QUESTION 28

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



- A. Chassis cluster control links must be configured using RFC 1918 IP addresses.
- B. Chassis cluster member devices synchronize configuration using the control link.
- C. A control link failure causes the secondary cluster node to be disabled.
- D. Recovery from a control link failure requires that the secondary member device be rebooted.
- E. Heartbeat messages verify that the chassis cluster control link is working.

Correct Answer: B, C, E

Section:

Explanation:

B) Chassis cluster member devices synchronize configuration using the control link: This statement is incorrect because the control link is used for configuration synchronization among other functions.

C) A control link failure causes the secondary cluster node to be disabled: This statement is incorrect because a control link failure causes the secondary node to become ineligible for primary role and remain in secondary role until the control link is restored.

E) Heartbeat messages verify that the chassis cluster control link is working: This statement is incorrect because heartbeat messages are sent periodically over the control link to monitor its status.

QUESTION 29

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.

Correct Answer: C, D

Section:

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 deleted.¹

QUESTION 30

You are asked to block malicious applications regardless of the port number being used.

In this scenario, which two application security features should be used? (Choose two.)

- A. AppFW
- B. AppQoS
- C. APPID
- D. AppTrack

Correct Answer: A, C

Section:

Explanation:

you can block applications and users based on network access policies, users and their job roles, time, and application signatures.² You can also use Juniper Advanced Threat Prevention (ATP) to find and block commodity and zero-day cyberthreats within files, IP traffic, and DNS requests.¹

QUESTION 31

A client has attempted communication with a known command-and-control server and it has reached the configured threat level threshold.

Which feed will the client's IP address be automatically added to in this situation?

- A. the command-and-control cloud feed



- B. the allowlist and blocklist feed
- C. the custom cloud feed
- D. the infected host cloud feed

Correct Answer: D

Section:

Explanation:

Infected hosts are internal hosts that have been compromised by malware and are communicating with external C&C servers³. Juniper ATP Cloud provides infected host feeds that list internal IP addresses or subnets of infected hosts along with a threat level³. Once the Juniper ATP Cloud global threshold for an infected host is met, that host is added to the infected host feed and assigned a threat level of 10 by the cloud⁴. You can also configure your SRX Series device to block traffic from these IP addresses using security policies⁴.

QUESTION 32

When a security policy is deleted, which statement is correct about the default behavior of active sessions allowed by that policy?

- A. The active sessions allowed by the policy will be dropped.
- B. The active sessions allowed by the policy will be marked as a legacy flow and will continue to be forwarded.
- C. The active sessions allowed by the policy will be reevaluated by the cached
- D. The active sessions allowed by the policy will continue

Correct Answer: A

Section:

Explanation:

When a security policy is deleted, the active sessions allowed by the policy will be dropped. The default behavior is that all active sessions allowed by the policy will be terminated and the traffic will no longer be forwarded. There is no way to mark the active sessions as a legacy flow or to reevaluate them by the cached rules. According to Juniper Networks Security, Specialist (JNCIS-SEC) Study Guide, when a security policy is deleted, the active sessions allowed by that policy will be dropped. This behavior is the default behavior of the device. There is no way to mark the active sessions as a legacy flow or to re-evaluate them against cached rules. The device will terminate the active sessions and will no longer forward traffic for those sessions.

QUESTION 33

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.

Correct Answer: D

Section:

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.

AppTrack is a feature of the Junos OS that provides visibility into the applications and users on your network. It tracks the usage of applications and provides detailed reports on the amount of traffic generated by each application. By enabling AppTrack on the proper security zones, you can determine how much traffic a popular gaming application is generating on your network.

QUESTION 34

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

- A. JIMS domain PC probes analyze domain controller security event logs at 60-minute 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.

Correct Answer: B

Section:

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 35

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

Correct Answer: B, C

Section:

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 36

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

Correct Answer: A, D

Section:

QUESTION 37

You are asked to implement IPS on your SRX Series device.

In this scenario, which two tasks must be completed before a configuration will work? (Choose two.)

- A. Download the IPS signature database.
- B. Enroll the SRX Series device with Juniper ATP Cloud.
- C. Install the IPS signature database.
- D. Reboot the SRX Series device.

Correct Answer: A, C

Section:**Explanation:**

The two tasks that must be completed before a configuration for IPS on an SRX Series device will work are downloading the IPS signature database and installing the IPS signature database. The Security, Specialist (JNCIS-SEC) Study guide provides further information on how to download and install the IPS signature database. Enrolling the SRX Series device with Juniper ATP Cloud is not necessary to make a configuration work, and rebooting the SRX Series device is not required either.

QUESTION 38

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.

Correct Answer: A, C

Section:**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 39

Exhibit



```
user@srx> show services security-intelligence category summary
```

```
Category name      :CC
Status             :Enable
Description        :Command and Control data schema
Update interval    :1800s
TTL                :3456000s
Feed name          :cc_cert_sha1_data
Version            :20221103.1
Objects number:0
Create time        :2022-11-08 19:49:02 UTC
Update time        :2022-11-08 20:12:23 UTC
Update status      :Store succeeded
Expired            :No
Status             :Active
Options            :N/A
Feed name          :cc_ip_data
Version            :20221102.8
Objects number:0
Create time        :2022-11-08 19:50:04 UTC
Update time        :2022-11-08 20:13:18 UTC
Update status      :Store succeeded
Expired            :No
Status             :Active
Options            :N/A
Feed name          :cc_ipv6_data
Version            :20200626.1
Objects number:0
Create time        :2022-11-08 20:00:06 UTC
Update time        :2022-11-08 20:13:18 UTC
Update status      :Store succeeded
Expired            :No
Status             :Active
Options            :N/A
Feed name          :cc_url_data
Version            :20221108.10
Objects number:0
Create time        :2022-11-08 20:02:07 UTC
Update time        :2022-11-08 20:13:24 UTC
Update status      :Store succeeded
Expired            :No
Status             :Active
Options            :N/A
```



You just finished setting up your command-and-control (C&C) category with Juniper ATP Cloud. You notice that all of the feeds have zero objects in them.

Which statement is correct in this scenario?

- A. The security intelligence policy must be configured; on a unified security policy
- B. Use the commit full command to start the download.
- C. No action is required, the feeds take a few minutes to download.
- D. Set the maximum C&C entries within the Juniper ATP Cloud GUI.

Correct Answer: C

Section:

Explanation:

According to the Juniper Networks JNCIS-SEC Study Guide, when you set up your command-and-control (C&C) category with Juniper ATP Cloud, all of the feeds will initially have zero objects in them. This is normal, as it can take a few minutes for the feeds to download. No action is required in this scenario and you will notice the feeds start to populate with objects once the download is complete.

QUESTION 40

Your network uses a single JSA host and you want to implement a cluster.
In this scenario, which two statements are correct? (Choose two.)

- A. The software versions on both primary and secondary hosts
- B. The secondary host can backup multiple JSA primary hosts.
- C. The primary and secondary hosts must be configured with the same storage devices.
- D. The cluster virtual IP will need an unused IP address assigned.

Correct Answer: A, D

Section:

Explanation:

According to the Juniper Networks JNCIP-SEC Study Guide, when setting up a cluster with a single JSA host, both the primary and secondary hosts must have the same software version installed. Additionally, an unused IP address must be assigned to the cluster virtual IP. The primary and secondary hosts do not need to be configured with the same storage devices, and the secondary host cannot be used to backup multiple JSA primary hosts.

QUESTION 41

You enable chassis clustering on two devices and assign a cluster ID and a node ID to each device.
In this scenario, what is the correct order for rebooting the devices?

- A. Reboot the secondary device, then the primary device.
- B. Reboot only the secondary device since the primary will assign itself the correct cluster and node ID.
- C. Reboot the primary device, then the secondary device.
- D. Reboot only the primary device since the secondary will assign itself the correct cluster and node ID.

Correct Answer: C

Section:

Explanation:

when enabling chassis clustering on two devices, the correct order for rebooting them is to reboot the primary device first, followed by the secondary device. It is not possible for either device to assign itself the correct cluster and node ID, so both devices must be rebooted to ensure the proper configuration is applied.

QUESTION 42

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

- A. SRX chassis clustering supports active/passive and active/active for the data plane.



- B. SRX chassis clustering only supports active/passive for the data plane.
- C. SRX chassis clustering supports active/passive for the control plane.
- D. SRX chassis clustering supports active/active for the control plane.

Correct Answer: A, D

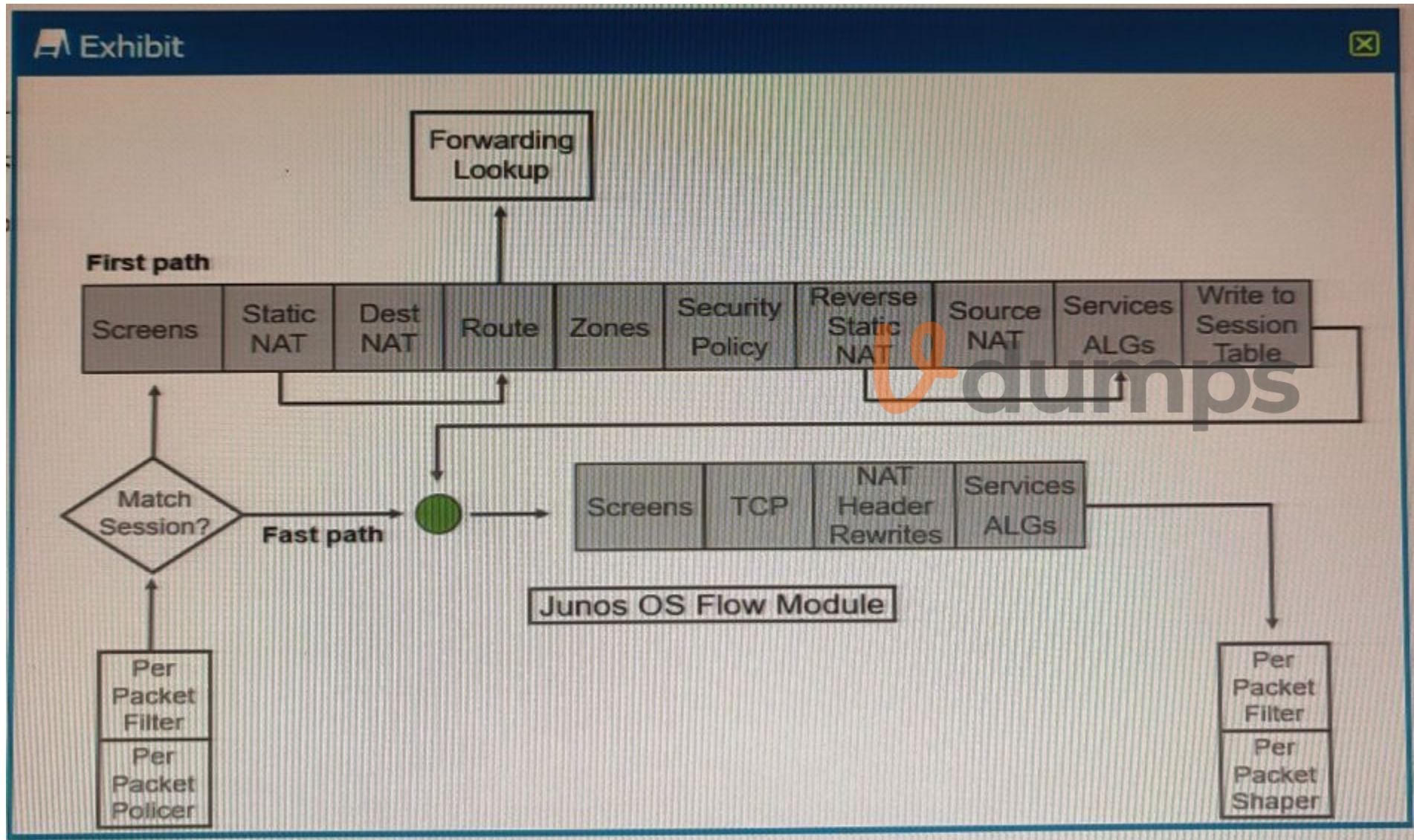
Section:

Explanation:

SRX chassis clustering supports active/passive and active/active for the data plane. In an active/active configuration, both cluster members process and forward traffic, which increases throughput and provides redundancy. For the control plane, SRX chassis clustering supports active/active, meaning that both cluster members can process and forward control traffic, providing redundancy and improved scalability

QUESTION 43

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

Correct Answer: B

Section:

QUESTION 44

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

Correct Answer: A, C

Section:

Explanation:

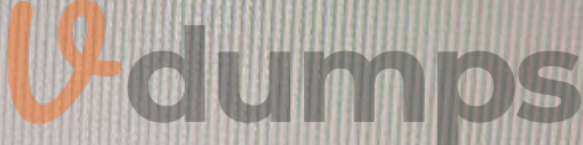
The vSRX supports both Layer 2 and Layer 3 configurations, while the cSRX is limited to Layer 3 configurations. Additionally, the vSRX has faster boot times, which is advantageous in certain scenarios. The vSRX and cSRX both provide NAT, IPS, and UTM services.

QUESTION 45

Exhibit




```
Exhibit ✕
user@srx> show services user-identification authentication-table authentication-
source identity-management extensive
Logical System: root-logical-system
Domain: juniper.net
Total entries: 1
  Source-ip: 172.25.11.140
    Username: nancy
    Groups:posture-healthy, administrators, users, domain admins, domain users,
executives
    State: Valid
    Source: JIMS - Active Directory
    Access start date: 2022-05-28
    Access start time: 21:53:52
    Last updated timestamp: 2022-05-29 10:43:44
    Age time: 46
```



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

- A. Nancy logged in to the juniper.net Active Directory domain.
- B. The IP address of Nancy's client PC is 172.25.11.
- C. The IP address of the authenticating domain controller is 172.25.11.140.
- D. Nancy is a member of the Active Directory sales group.

Correct Answer: C

Section:

QUESTION 46

Which two statements are correct about JSA data collection? (Choose two.)

- A. The Event Collector collects information using BGP FlowSpec.
- B. The Flow Collector can use statistical sampling
- C. The Flow Collector parses logs.
- D. The Event Collector parses logs

Correct Answer: B, D

Section:

Explanation:

The Flow Collector can use statistical sampling to collect and store network flow data in the JSA database. The Event Collector collects information from various sources including syslog, SNMP, NetFlow, and BGP FlowSpec. Both the Flow Collector and the Event Collector parse logs to extract useful information from the logs.

QUESTION 47

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

Correct Answer: D

Section:

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 Juniper's advanced Machine Learning and Artificial Intelligence (AI) capabilities, allowing it to detect and block malicious activity in real-time. ATP is integrated with Juniper's Unified Threat Management (UTM) and Encrypted Traffic Insights (ETI) solutions, providing an end-to-end network protection solution.

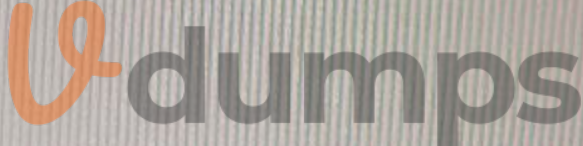
QUESTION 48

Exhibit




```
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 is 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.

Correct Answer: B, C

Section:

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 49

Your company is using the Juniper ATP Cloud free model. The current inspection profile is set at 10 MB. You are asked to configure ATP Cloud so that executable files up to 30 MB can be scanned while at the same time minimizing the change in scan time for other file types.

Which configuration should you use in this scenario?

- A. Use the CLI to create a custom profile and increase the scan limit.
- B. Use the ATP Cloud UI to change the default profile to increase the scan limit for all files to 30 MB.
- C. Use the CLI to change the default profile to increase the scan limit for all files to 30 MB.
- D. Use the ATP Cloud UI to update a custom profile and increase the scan limit for executable files to 30 MB.

Correct Answer: D

Section:

Explanation:

In this scenario, you should use the ATP Cloud UI to create a custom profile and update the scan limit for executable files to 30 MB. This will ensure that executable files up to 30 MB can be scanned, while at the same time minimizing the change in scan time for other file types. To do this, log in to the ATP Cloud UI and go to the Profiles tab. Click the Create button to create a new profile, and then adjust the scan limits for executable files to 30 MB. Once you have saved the custom profile, you can apply it to the desired systems and the new scan limit will be in effect.

QUESTION 50

You are configuring logging for a security policy.

In this scenario, in which two situations would log entries be generated? (Choose two.)

- A. every 10 minutes
- B. at session initialization
- C. every 60 seconds
- D. at session close

Correct Answer: B, D

Section:

Explanation:


Log entries would be generated in two situations: at session initialization and at session close. At session initialization, the log entry would include details about the connection, such as the source and destination IP addresses, the service being used, and the action taken by the security policy. At session close, the log entry would include details about the connection, such as the duration of the session, the bytes sent/received, and the action taken by the security policy. For more information, you can refer to the Juniper Security documentation at https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/security-log-configuration.html.

QUESTION 51

Exhibit



```
Exhibit [X]
[edit services ssl]
user@srx# commit
[edit services ssl proxy]
  'profile Server-Protect'
    Unsupported cert type of server certid: SSL-Proxy
error: configuration check-out failed
[edit services ssl]
user@srx#
```



When trying to set up a server protection SSL proxy, you receive the error shown. What are two reasons for this error? (Choose two.)

- A. The SSL proxy certificate ID is part of a blocklist.
- B. The SSL proxy certificate ID does not have the correct renegotiation option set.
- C. The SSL proxy certificate ID is for a forwarding proxy.
- D. The SSL proxy certificate ID does not exist.

Correct Answer: A, D

Section:

Explanation:

Two possible reasons for this error are that the SSL proxy certificate ID does not exist, or the SSL proxy certificate ID is part of a blocklist. If the SSL proxy certificate ID does not exist, you will need to generate a new certificate. If the SSL proxy certificate ID is part of a blocklist, you will need to contact the source of the blocklist to remove it. Additionally, you may need to check that the SSL proxy certificate ID has the correct renegotiation option set, as this is necessary for proper server protection. For more information, you can refer to the Juniper Security documentation at https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/security-ssl-proxy-configuration.html.

QUESTION 52

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

- A. Dynamic analysis is always performed to determine if a file contains malware.
- B. If the cache lookup determines that a file contains malware, performed to verify the results.
- C. Dynamic analysis is not always necessary to determine if a file contains malware.
- D. If the cache lookup determines that a file contains malware, static analysis is not performed to verify the results.

Correct Answer: C, D

Section:

Explanation:

Dynamic analysis is not always necessary to determine if a file contains malware, as the ATP Cloud uses a cache lookup to quickly identify known malicious files. If the cache lookup determines that a file contains malware, static analysis is not performed to verify the results. This information can be found on the Juniper website here: https://www.juniper.net/documentation/en_US/release-independent/security/jnpr-security-srx-series/information-products/topic-collection/jnpr-security-srx-resources.html#id-jnpr-security-srx-resources-atp-cloud.

QUESTION 53

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

Correct Answer: A

Section:

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 54

You are asked to create an IPS-exempt rule base to eliminate false positives from happening. Which two configuration parameters are available to exclude traffic from being examined? (Choose two.)

- A. source port
- B. source IP address
- C. destination IP address
- D. destination port

Correct Answer: B

Section:

Explanation:

To exclude traffic from being examined by IPS, you can use the source IP address and/or destination port as criteria for the exemption. This is achieved by configuring an IPS-exempt rule base that includes specific exemption rules based on these criteria.

QUESTION 55

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

- A. vQFX
- B. MX
- C. vMX

D. QFX

Correct Answer: B, C

Section:

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 56

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

- A. scalability
- B. no required software license
- C. granular security
- D. infinite number of interfaces

Correct Answer: A, C

Section:

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 57

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?

- 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

Correct Answer: D

Section:

QUESTION 58

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.

Correct Answer: B, C

Section:

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 59

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

- 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

Correct Answer: A, D

Section:

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 60

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

- A. SQL log files
- B. data plane logs
- C. system core dump files
- D. control plane logs

Correct Answer: B, D

Section:

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 61

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.)

- 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.

Correct Answer: A, C

Section:

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 62

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

Correct Answer: D

Section:

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, ETI will 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 63

Exhibit




```
[edit security policies from-zone Trust to-zone Untrust]
user@srx# show
policy FindThreat {
  match {
    source-address any;
    destination-address any;
    application junos-defaults;
    dynamic-application [ junos:BITTORRENT junos:BITTORRENT-BUNDLE
junos:BITTORRENT-WEB-CLIENT ];
  }
  then {
    permit;
  }
}
[edit security policies from-zone Trust to-zone Untrust]
user@srx#
```



You are asked to track BitTorrent traffic on your network. You need to automatically add the workstations to the High_Risk_Workstations feed and the servers to the BitTorrent_Servers feed automatically to help mitigate future threats.

Which two commands would add this functionality to the FindThreat policy? (Choose two.)

A)

```
[edit security policies from-zone Trust to-zone Untrust policy FindThreat then permit application-
services security-intelligence]
user@srx# set add-source-ip-to-feed High_Risk_Workstations
```

B)

```
[edit security policies from-zone Trust to-zone Untrust policy FindThreat then permit application-
services security-intelligence]
user@srx# set add-source-identity-to-feed High_Risk_Workstations
```

C)

```
[edit security policies from-zone Trust to-zone Untrust policy FindThreat then permit application-
services security-intelligence]
user@srx# set add-destination-identity-to-feed BitTorrent_Servers
```

D)


```
[edit security policies from-zone Trust to-zone Untrust policy FindThreat then permit application-  
services security-intelligence]  
user@srx# set add-destination-ip-to-feed BitTorrent_Servers
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Correct Answer: C

Section:

QUESTION 64

Which two types of SSL proxy are available on SRX Series devices? (Choose two.)

- A. Web proxy
- B. client-protection
- C. server-protection
- D. DNS proxy

Correct Answer: B, C

Section:

Explanation:

Based on SSL proxy is a feature that allows SRX Series devices to decrypt and inspect SSL/TLS traffic for security purposes. According to SRX Series devices support two types of SSL proxy:

Client-protection SSL proxy also known as forward proxy --- The SRX Series device resides between the internal client and outside server. It decrypts and inspects traffic from internal users to the web.

Server-protection SSL proxy also known as reverse proxy --- The SRX Series device resides between outside clients and internal servers. It decrypts and inspects traffic from web users to internal servers.

QUESTION 65

Click the Exhibit button.

```

[edit services]
user@srx# show
security-intelligence {
  profile ATP_Infected-Hosts {
    category Infected-Hosts;
    rule Rule-1 {
      match {
        threat-level 8;
      }
      then {
        action {
          block {
            drop;
          }
        }
      }
    }
  }
}

```



Referring to the exhibit, what will the SRX Series device do in this configuration?

- A. Packets from the infected hosts with a threat level of 8 will be dropped and a log message will be generated.
- B. Packets from the infected hosts with a threat level of 8 or above will be dropped and a log message will be generated.
- C. Packets from the infected hosts with a threat level of 8 or above will be dropped and no log message will be generated.
- D. Packets from the infected hosts with a threat level of 8 will be dropped and no log message will be generated.

Correct Answer: C

Section:

Explanation:

The exhibit shows a configuration snippet for security intelligence on an SRX Series device. Security intelligence is a feature that allows you to block or monitor traffic from malicious sources based on threat intelligence feeds from Juniper ATP Cloud or other providers. The configuration defines a profile for ATP Infected-Hosts, which is a feed that contains IP addresses of hosts that are infected with malware and communicate with command-and-control servers. The configuration also defines a rule for threat level 8, which is a parameter that indicates the severity of the threat. Based on this configuration, the SRX Series device will do the following:

Packets from the infected hosts with a threat level of 8 or above will be dropped: The action block-and-drop under the rule means that the device will block any traffic from the infected hosts that have a threat level equal to or higher than 8. This will prevent the hosts from sending or receiving malicious commands or data.

No log message will be generated: The absence of any log option under the rule means that the device will not generate any log message for the blocked traffic. This may reduce the load on the device and the logging server, but it may also limit the visibility and analysis of the security events.

QUESTION 66

Which two statements are correct about a reth LAG? (Choose two.)

- A. Links must have the same speed and duplex setting.
- B. Links must use the same cable type

- C. You must have a 'minimum-links' statement value of two.
- D. You should have two or more interfaces.

Correct Answer: A, D

Section:

Explanation:

A reth LAG is a redundant Ethernet link aggregation group that combines multiple physical interfaces into a single logical interface in a chassis cluster. A reth LAG provides load balancing and redundancy for traffic within or between redundancy groups. Two statements that are correct about a reth LAG are:

Links must have the same speed and duplex setting: To form a reth LAG, the physical interfaces must have the same speed and duplex setting. This ensures that the links can operate at the same capacity and avoid performance issues or errors.

You should have two or more interfaces: To create a reth LAG, you need to have at least two physical interfaces. One interface should be connected to node 0 and the other interface should be connected to node 1. You can also have more than two interfaces in a reth LAG for increased bandwidth and redundancy.

QUESTION 67

Which two statements are true about application identification? (Choose two.)

- A. Application identification can identify nested applications that are within Layer 7.
- B. Application identification cannot identify nested applications that are within Layer 7.
- C. Application signatures are the same as IDP signatures.
- D. Application signatures are not the same as IDP signatures.

Correct Answer: A, D

Section:

Explanation:

Application identification is a feature that enables SRX Series devices to identify and classify network traffic based on application signatures or custom rules. Application identification can enhance security, visibility, and control over network applications. Two statements that are true about application identification are:

Application identification can identify nested applications that are within Layer 7: Nested applications are applications that run within another application protocol, such as HTTP or SSL. For example, Facebook or YouTube are nested applications within HTTP. Application identification can identify nested applications by inspecting the application payload and matching it against predefined or custom signatures.

Application signatures are not the same as IDP signatures: Application signatures are patterns of bytes or strings that uniquely identify an application protocol or a nested application. IDP signatures are patterns of bytes or strings that indicate an attack or an exploit against a vulnerability. Application signatures are used for application identification and classification, while IDP signatures are used for intrusion detection and prevention.

QUESTION 68

Which sequence does an SRX Series device use when implementing stateful session security policies using Layer 3 routes?

- A. An SRX Series device will perform a security policy search before conducting a longest-match Layer 3 route table lookup.
- B. An SRX Series device performs a security policy search before implementing an ALG security check on the longest-match Layer 3 route.
- C. An SRX Series device will conduct a longest-match Layer 3 route table lookup before performing a security policy search.
- D. An SRX Series device conducts an ALG security check on the longest-match route before performing a security policy search.

Correct Answer: C

Section:

Explanation:

The sequence that an SRX Series device uses when implementing stateful session security policies using Layer 3 routes is:

An SRX Series device will conduct a longest-match Layer 3 route table lookup before performing a security policy search: When an SRX Series device receives a packet, it first looks up the destination IP address in the routing table and finds the longest matching route to forward the packet. Then, it performs a security policy search based on the source zone, destination zone, source address, destination address, protocol, and application of the packet. If there is a matching policy that allows the packet, it creates or updates a session entry for the packet and applies any security services configured in the policy.

QUESTION 69

You want to show tabular data for operational mode commands.
In this scenario, which logging parameter will provide this function?

- A. permit
- B. count
- C. session-init
- D. session-close

Correct Answer: B

Section:

Explanation:

The logging parameter that will provide the function of showing tabular data for operational mode commands is count. The count parameter displays the number of packets and bytes that match a security policy and the action taken by the policy. The count parameter can be used with the show security policies hit-count command to display the policy counters in a tabular format. The count parameter can also be used with the show security flow session command to display the session counters in a tabular format. Reference:=show security policies hit-count,show security flow session

QUESTION 70

You need to deploy an SRX Series device in your virtual environment.
In this scenario, what are two benefits of using a cSRX? (Choose two.)

- A. The cSRX supports Layer 2 and Layer 3 deployments.
- B. The cSRX default configuration contains three default zones: trust, untrust, and management.
- C. The cSRX supports firewall, NAT, IPS, and UTM services.
- D. The cSRX has low memory requirements.

Correct Answer: C, D

Section:

Explanation:

Two benefits of using a cSRX in your virtual environment are:

The cSRX supports firewall, NAT, IPS, and UTM services: The cSRX is a containerized version of the SRX Series firewall that runs as a Docker container on Linux hosts. It provides the same features and functionality as the SRX Series physical firewalls, such as firewall, NAT, IPS, and UTM services. The cSRX can protect your virtual workloads and applications from various threats and attacks.

The cSRX has low memory requirements: The cSRX is designed to be lightweight and efficient, with low memory and CPU requirements. The cSRX can run on as little as 1 GB of RAM and 1 vCPU, making it suitable for resource-constrained environments.

QUESTION 71

How does the SSL proxy detect if encryption is being used?

- A. It uses application identity services.
- B. It verifies the length of the packet
- C. It queries the client device.
- D. It looks at the destination port number.

Correct Answer: D

Section:

Explanation:

The SSL proxy can detect if encryption is being used by looking at the destination port number of the packet. If the port number is 443, then the proxy can assume that the packet is being sent over an encrypted connection. If the port number is different, then the proxy can assume that the packet is not encrypted. For more information, please refer to the Juniper Networks JNCIS-SEC Study Guide.

The SSL proxy is a security feature that provides visibility and control over SSL/TLS encrypted traffic. When SSL proxy is enabled, it intercepts SSL/TLS traffic and decrypts it to allow visibility into the content of the encrypted traffic. However, before decrypting the traffic, the SSL proxy must first determine if the traffic is encrypted.



To detect if encryption is being used, the SSL proxy looks at the destination port number. If the destination port number is a known SSL/TLS port (e.g., TCP port 443), the SSL proxy assumes that encryption is being used and intercepts the traffic. If the destination port is not a known SSL/TLS port, the SSL proxy does not intercept the traffic and allows it to pass through the device unmodified.

QUESTION 72

Which two statements are correct when considering IPS rule base evaluation? (Choose two.)

- A. IPS evaluates rules concurrently.
- B. IPS applies the most severe action to traffic matching multiple rules,
- C. IPS evaluates rules sequentially
- D. IPS applies the least severe action to traffic matching multiple rules.

Correct Answer: A, B

Section:

Explanation:

The Intrusion Prevention System (IPS) is a feature that provides protection against network-based threats. The IPS uses a rule base to evaluate network traffic and apply actions based on the rules that match the traffic.

When evaluating the rule base, the IPS evaluates the rules concurrently (option A). This means that the IPS can apply multiple rules to the same traffic simultaneously.

If multiple rules match the same traffic, the IPS applies the most severe action (option B). This means that if there are conflicting actions specified in different rules, the IPS will apply the action that has the highest severity.

For example, if one rule specifies a 'drop' action and another rule specifies a 'log' action for the same traffic, the IPS will drop the traffic because dropping has a higher severity than logging.

QUESTION 73

You have implemented a vSRX in your VMware environment. You want to implement a second vSRX Series device and enable chassis clustering.

Which two statements are correct in this scenario about the control-link settings? (Choose two.)

- A. In the vSwitch security settings, accept promiscuous mode.
- B. In the vSwitch properties settings, set the VLAN ID to None.
- C. In the vSwitch security settings, reject forged transmits.
- D. In the vSwitch security settings, reject MAC address changes.



Correct Answer: C, D

Section:

QUESTION 74

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 OS.
- D. Linux is the base OS.

Correct Answer: B, D

Section:

Explanation:

The vSRX is a virtual security appliance that runs on a virtual machine. It provides firewall, VPN, and other security services in a virtualized environment.

The vSRX is based on a version of Junos OS that is optimized for virtualization. It runs on a Linux kernel and uses a KVM hypervisor. It supports VMware ESXi and KVM hypervisors.

The vSRX has support for VMXNET3 vNICs, which are high-performance virtual network interfaces provided by VMware. These interfaces can provide higher throughput and lower CPU utilization than other virtual NIC types.

QUESTION 75

Exhibit


```
Exhibit
{primary:node0}
user@node0> show chassis cluster status
...
Cluster ID: 1
Node  Priority Status          Preempt Manual  Monitor-failures

Redundancy group: 0 , Failover count: 1
node0  200    primary          no      no      None
node1  0       lost             n/a     n/a     n/a

Redundancy group: 1 , Failover count: 1
node0  0       primary          no      no      None
node1  0       lost             n/a     n/a     n/a

{primary:node1}
user@node1> show chassis cluster status
...
Cluster ID: 1
Node  Priority Status          Preempt Manual  Monitor-failures

Redundancy group: 0 , Failover count: 1
node0  0       lost             n/a     n/a     n/a
node1  1       primary          no      no      None

Redundancy group: 1 , Failover count: 5
node0  0       lost             n/a     n/a     n/a
node1  1       primary          no      no      None
```

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.

Correct Answer: C

Section:

QUESTION 76

Which two features are configurable on Juniper Secure Analytics (JSA) to ensure that alerts are triggered when matching certain criteria? (Choose two.)

- A. building blocks
- B. assets
- C. events
- D. tests

Correct Answer: C, D

Section:

Explanation:

The two configurable features on Juniper Secure Analytics (JSA) that can be used to ensure that alerts are triggered when matching certain criteria are events and tests. Events refer to the collection of data from different sources, while tests are used to define the criteria for which an alert is triggered. For example, you can use events to collect data from a firewall and tests to define criteria such as IP address, port number, and the type of

traffic. The Security, Specialist (JNCIS-SEC) Study guide provides further information on how to configure these features on JSA.

