Exam Code: JN0-335

Exam Name: Security, Specialist

Website: **www.VCEplus.io - www.VCEup.com**

Question No: 1

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: BC

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 database2.

Question No: 2

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

Answer: BC

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 No: 3

You are asked to reduce the load that the JIMS server places on your 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.

Answer: D

Explanation:

JIMS server is a Juniper Identity Management Service that collects user identity information from different authentication sources for SRX Series devices12. 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 No: 4

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.

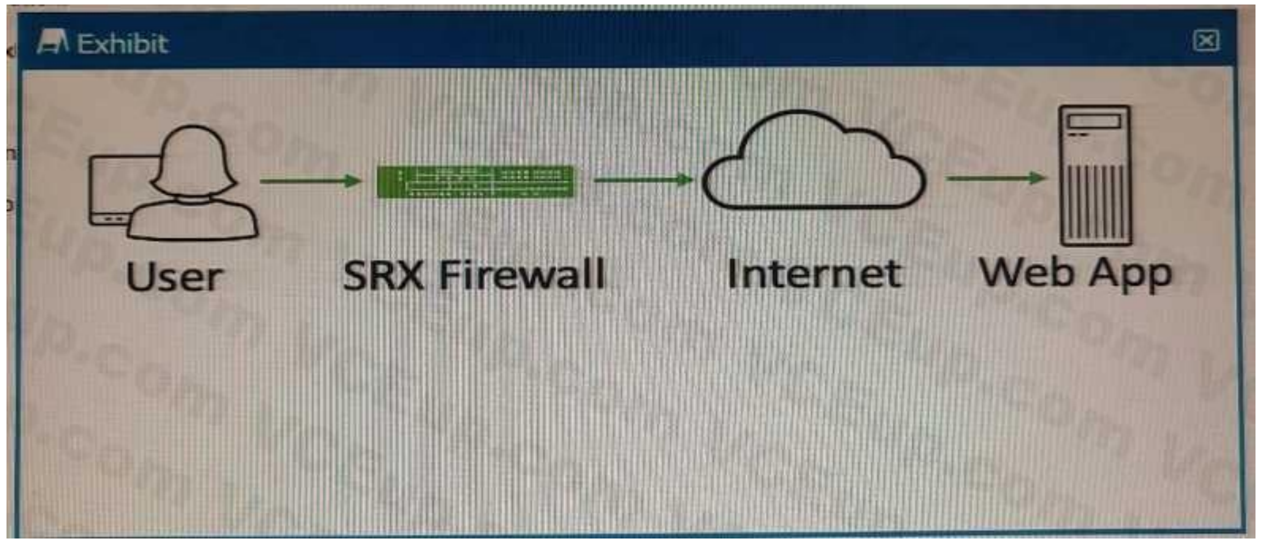
D. APPID results are used to determine the final security policy

Answer: CD

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 conditions12. They simplify applicationbased security policy management at Layer 7 and provide greater control and extensibility to manage dynamic applications traffic3

Question No: 5

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

Answer: BC

Explanation:

1. Client protection proxy: This statement is correct 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 server4.

2. Server protection proxy: This statement is correct because a reverse proxy can also be called a server protection proxy since it protects the web server’s identity and location from the user4.

Question No: 6

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.

Answer: D

Explanation:

You have exceeded the maximum files submission for your SRX platform size: This statement is correct 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 size3. For example, SRX320 has a limit of 10 files per minute3.

Question No: 7

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.

Answer: BCE

Explanation:

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

2. A control link failure causes the secondary cluster node to be disabled: This statement is correct 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.

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

Question No: 8

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

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

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

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

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

Answer: CD

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

Question No: 9

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. AppQoE

C. APPID

D. AppTrack

Answer: AC

Explanation: you can block applications and users based on network access policies, users and their job roles, time, and application signatures2. You can also use Juniper Advanced Threat Prevention (ATP) to find and block commodity and zero-day cyberthreats within files, IP traffic, and DNS requests1

Question No: 10

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 clients 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

Answer: D

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 No: 11

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

Answer: A

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.

Reference: Juniper Networks Security, Specialist (JNCIS-SEC) Study Guide, Chapter 3: Security Policies, page 3-9.

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 No: 12

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

Which action will you perform to accomplish this task?

A. Enable AppQoS on the proper security zones

B. Enable APBR on the proper security zones

C. Enable screen options on the proper security zones

D. Enable AppTrack on the proper security zones.

Answer: D

Explanation:

AppTrack is a feature of Juniper Networks firewall solutions that allows administrators to track applications, users, and the amount of traffic generated by those applications on the network.

AppTrack can be enabled on specific security zones of the network to monitor traffic on those zones.

This feature can be used to determine how much traffic a popular gaming application is generating on the network. For more information, please refer to the Juniper Networks JNCIS-SEC Study Guide.

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

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 No: 13

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.

Answer: D

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.

Reference: Juniper Networks Security, Specialist (JNCIS-SEC) Study Guide, Chapter 6: SSL Proxy, page 6-9.

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 No: 14

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.

Answer: AB

Explanation:

Reference: Juniper Networks Security, Specialist (JNCIS-SEC) Study Guide, Chapter 7: Intrusion Prevention System, page 7-5.

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 No: 15

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.

Answer: CD

Explanation:

Question No: 16

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.

Answer: BD

Explanation:

Reference: Juniper Networks Security, Specialist (JNCIS-SEC) Study Guide, Chapter 1: Introduction to Junos Security, page 1-8.

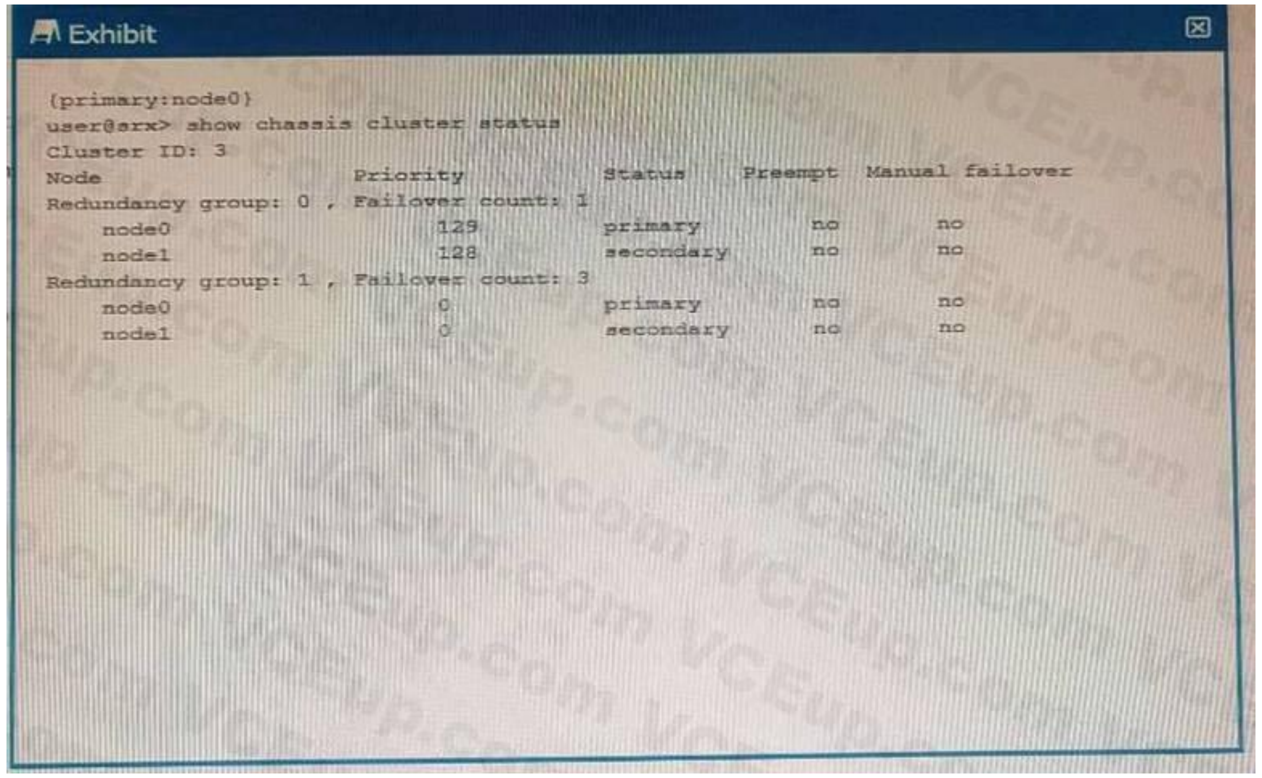
The vSRX is a virtual security appliance that runs on a virtual machine. It provides firewall, VPN, and other security services in a virtualized environment.

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 No: 17

Exhibit



Exhibit

```
{primary:node0}
user@srx> show chassis cluster status
Cluster ID: 3
Node                    Priority           Status     Preempt  Manual failover
Redundancy group: 0 , Failover count: 1
    node0                    129           primary        no         no
    node1                    128           secondary      no         no
Redundancy group: 1 , Failover count: 3
    node0                    0             primary        no         no
    node1                    0             secondary      no         no
```

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

A. Redundancy group 1 is in an ineligible state.

B. Node1 is the active node for the control plane

C. There are no issues with the cluster.

D. Redundancy group 0 is in an ineligible state.

Answer: A

Explanation:

Question No: 18

You want to manually failover the primary Routing Engine in an SRX Series high availability cluster pair.

Which step is necessary to accomplish this task?

A. Issue the set chassis cluster disable reboot command on the primary node.

B. Implement the control link recover/ solution before adjusting the priorities.

C. Manually request the failover and identify the secondary node

D. Adjust the priority in the configuration on the secondary node.

Answer: A

Explanation:

In order to manually failover the primary Routing Engine in an SRX Series high availability cluster pair, you must issue the command "set chassis cluster disable reboot" on the primary node. This command will disable the cluster and then reboot the primary node, causing the secondary node to take over as the primary node. This is discussed in greater detail in the Juniper Security, Specialist (JNCIS-SEC) Study Guide (page 68).

Question No: 19

You want to permit access to an application but block application sub-Which two security policy features provide this capability? (Choose two.)

A. URL filtering

B. micro application detection

C. content filtering

D. APPID

Answer: AB

Explanation:

The two security policy features that provide the capability to permit access to an application but block its sub-applications are URL filtering and micro application detection. URL filtering allows you to create policies that permit or block access to certain websites or webpages based on URL patterns.

Micro application detection is a more sophisticated approach that can identify and block specific applications, even if they are embedded within other applications or websites. According to the Juniper Networks Certified Internet Specialist (JNCIS-SEC) Study Guide [1], “micro application detection is the most accurate way to detect and control applications.” Content filtering and APPID are more general approaches and are not as effective in providing the level of granularity needed to block sub-applications.

Question No: 20

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 No: 21

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: BC

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 No: 22

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

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

B. Traditional security policies must come before unified security policies

C. Unified security policies must come before traditional security policies

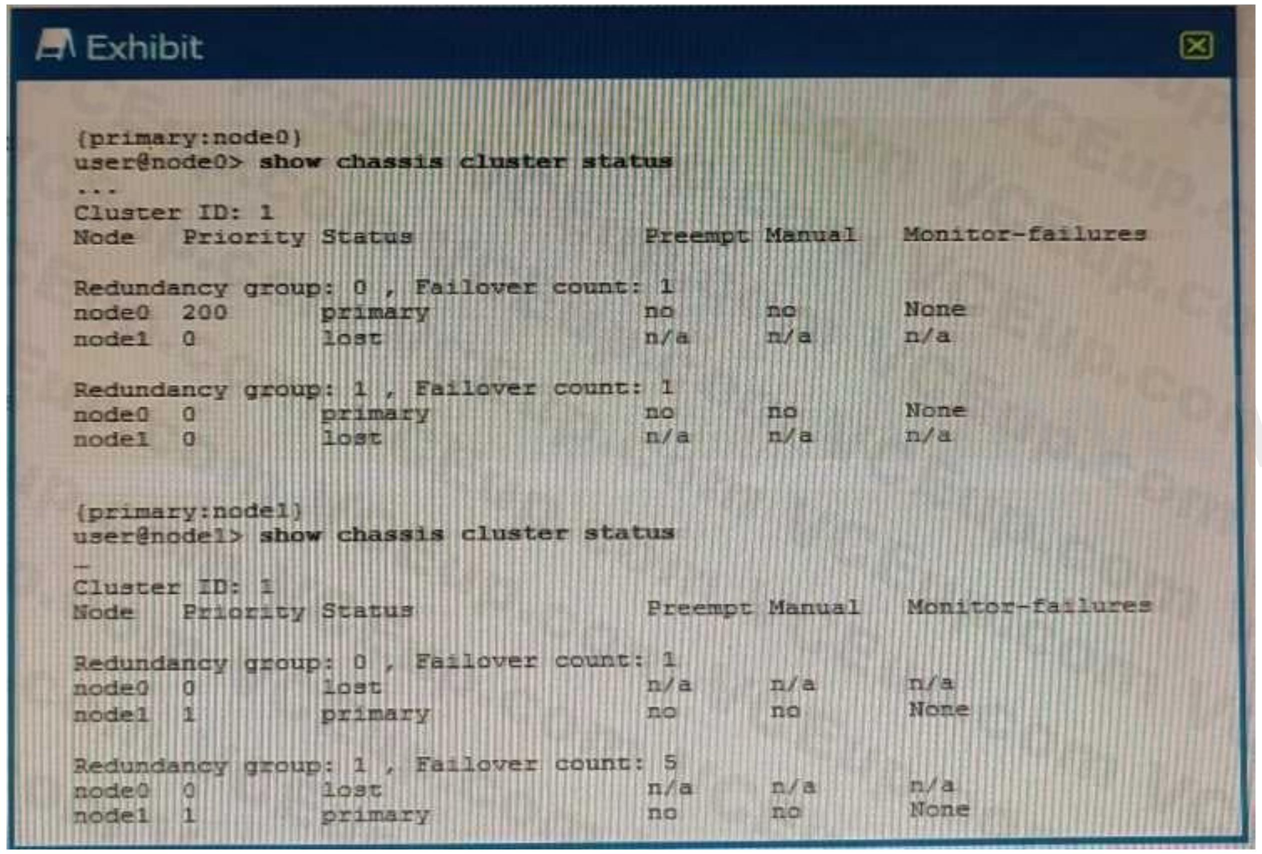
D. When a packet matches a traditional security policy, the evaluation process terminates

Answer: AD

Explanation:

Question No: 23

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.

Answer: C

Explanation:

Question No: 24

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

Answer: CD

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.

Question No: 25

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.

Answer: AC

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 No: 26

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

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

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

C. The threat levels range from 0-10.

D. The threat levels range from 0-100.

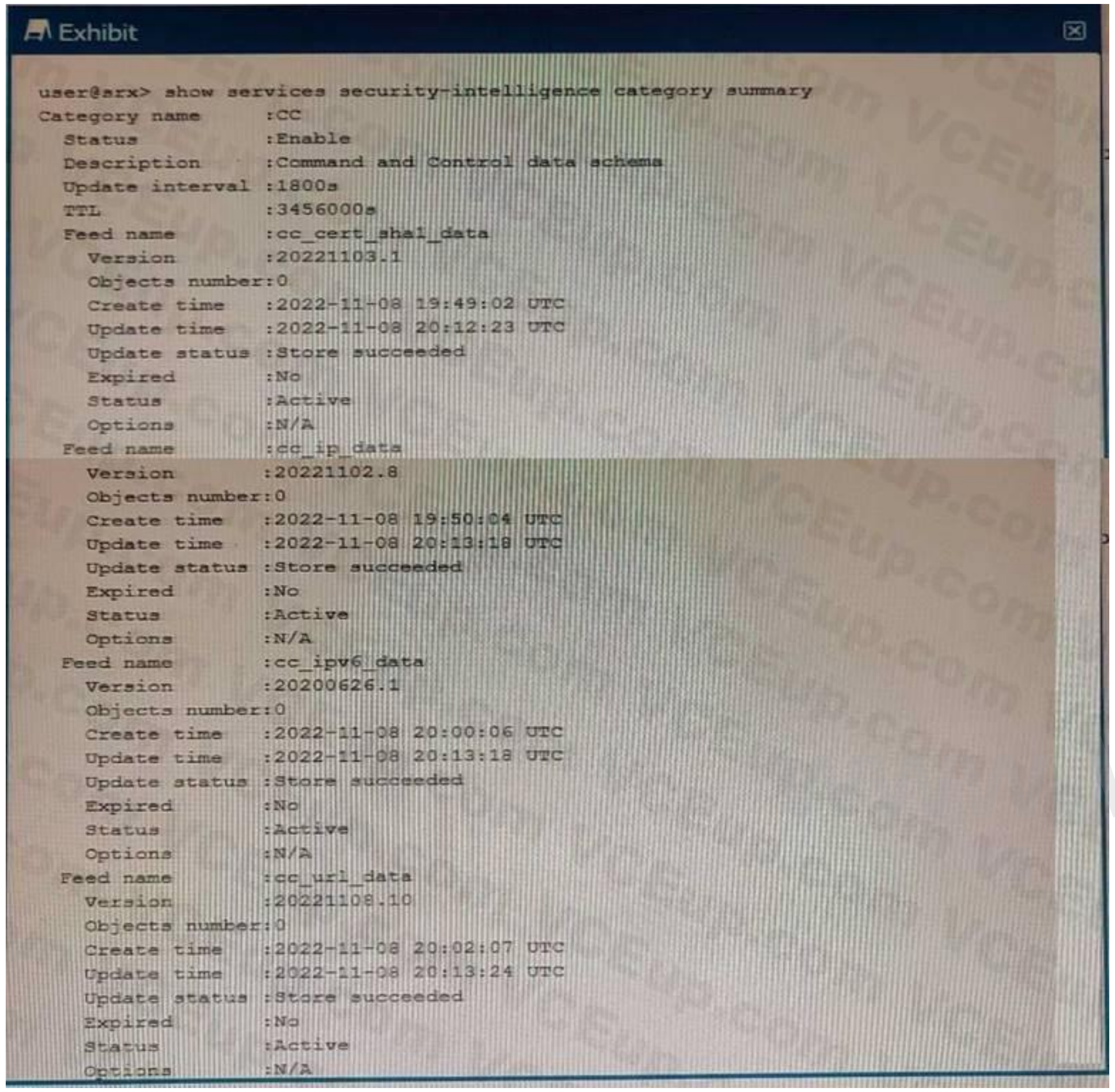
Answer: AC

Explanation:

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

Question No: 27

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.

Answer: C

Explanation:

According to the Juniper Networks JNCIS-SEC Study Guide, when you set up your command-andcontrol (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 No: 28

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.

Answer: AD

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 No: 29

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.

Answer: C

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 No: 30

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.

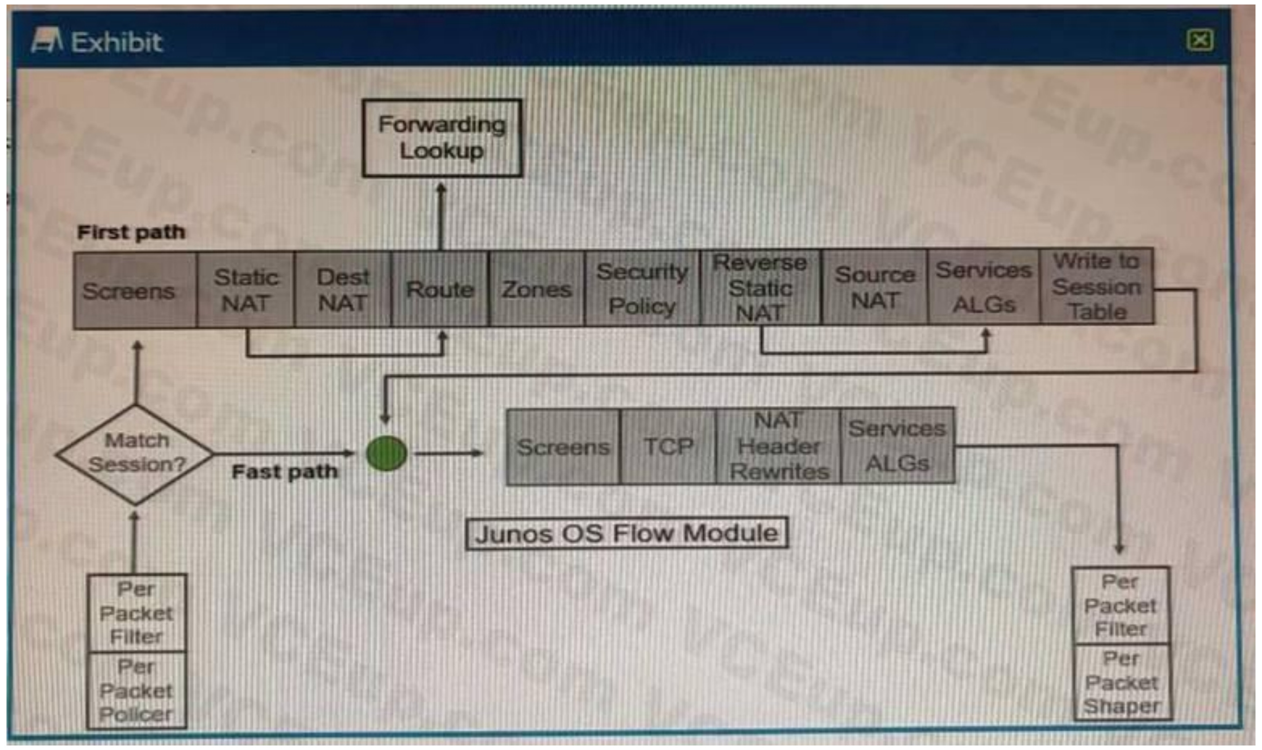
Answer: AD

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 No: 31

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

Explanation:

Question No: 32

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

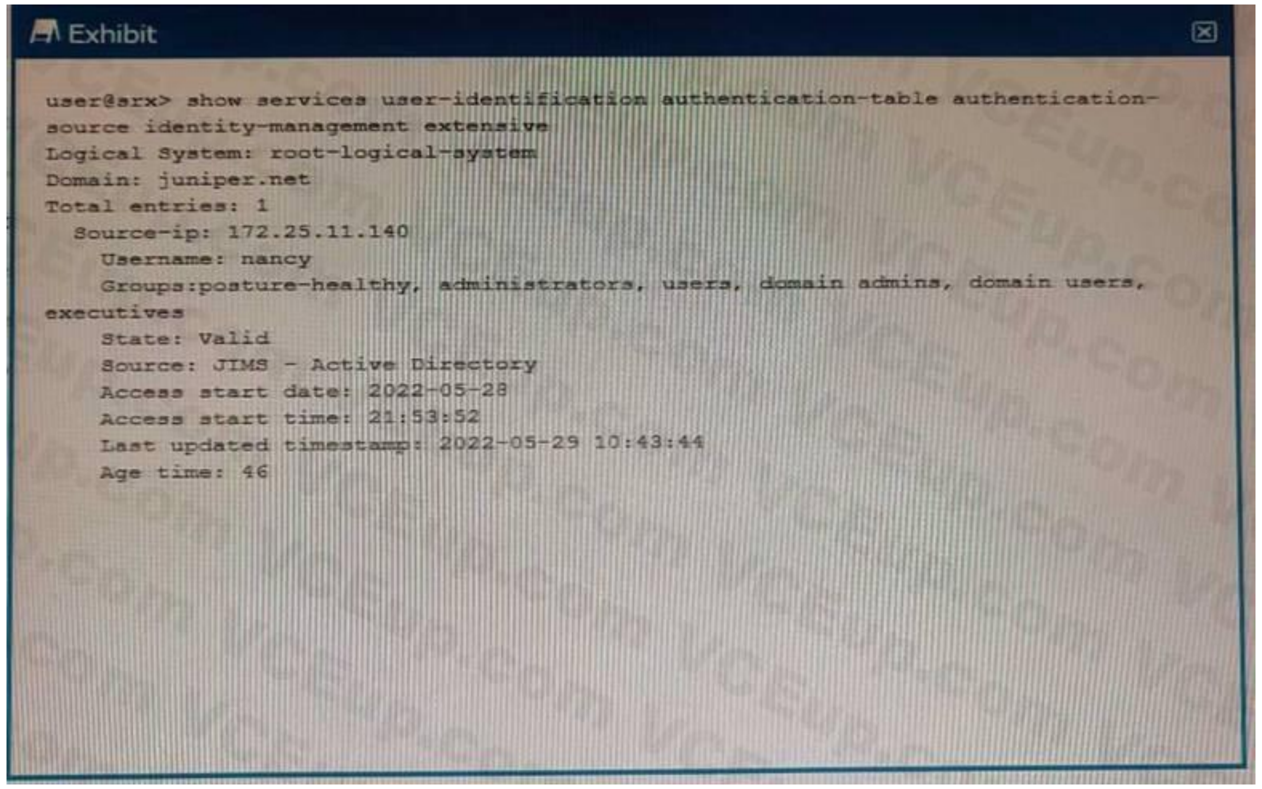
Answer: AC

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 No: 33

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.

Answer: C

Explanation:

Question No: 34

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

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

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

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

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

Answer: D

Explanation:

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

Question No: 35

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

A. The fab link does not support fragmentation.

B. The physical interface for the fab link must be specified in the configuration.

C. The fab link supports traditional interface features.

D. The Junos OS supports only one fab link.

Answer: BC

Explanation:

The physical interface for the fab link must be specified in the configuration. Additionally, the fab link supports traditional interface features such as MAC learning, security policy enforcement, and dynamic routing protocols. The fab link does not support fragmentation and the Junos OS supports up to two fab links.

Question No: 36

After JSA receives external events and flows, which two steps occur? (Choose two.)

A. After formatting the data, the data is stored in an asset database.

B. Before formatting the data, the data is analyzed for relevant information.

C. Before the information is filtered, the information is formatted

D. After the information is filtered, JSA responds with active measures

Answer: BC

Explanation:

Before formatting the data, the data is analyzed for relevant information. This is done to filter out any irrelevant data and to extract any useful information from the data. After the information is filtered, it is then formatted so that it can be stored in an asset database. After the data has been formatted, JSA will then respond with active measures.

Question No: 37

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: BC

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.

Question No: 38

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

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

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

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

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

Answer: AB

Explanation:

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

Question No: 39

You want to use IPS signatures to monitor traffic.

Which module in the AppSecure suite will help in this task?

A. AppTrack

B. AppQoS

C. AppFW

D. APPID

Answer: C

Explanation:

The AppFW module in the AppSecure suite provides IPS signatures that can be used to monitor traffic and detect malicious activities. AppFW also provides other security controls such as Web application firewall, URL filtering, and application-level visibility.

Question No: 40

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

Answer: BD

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 No: 41

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

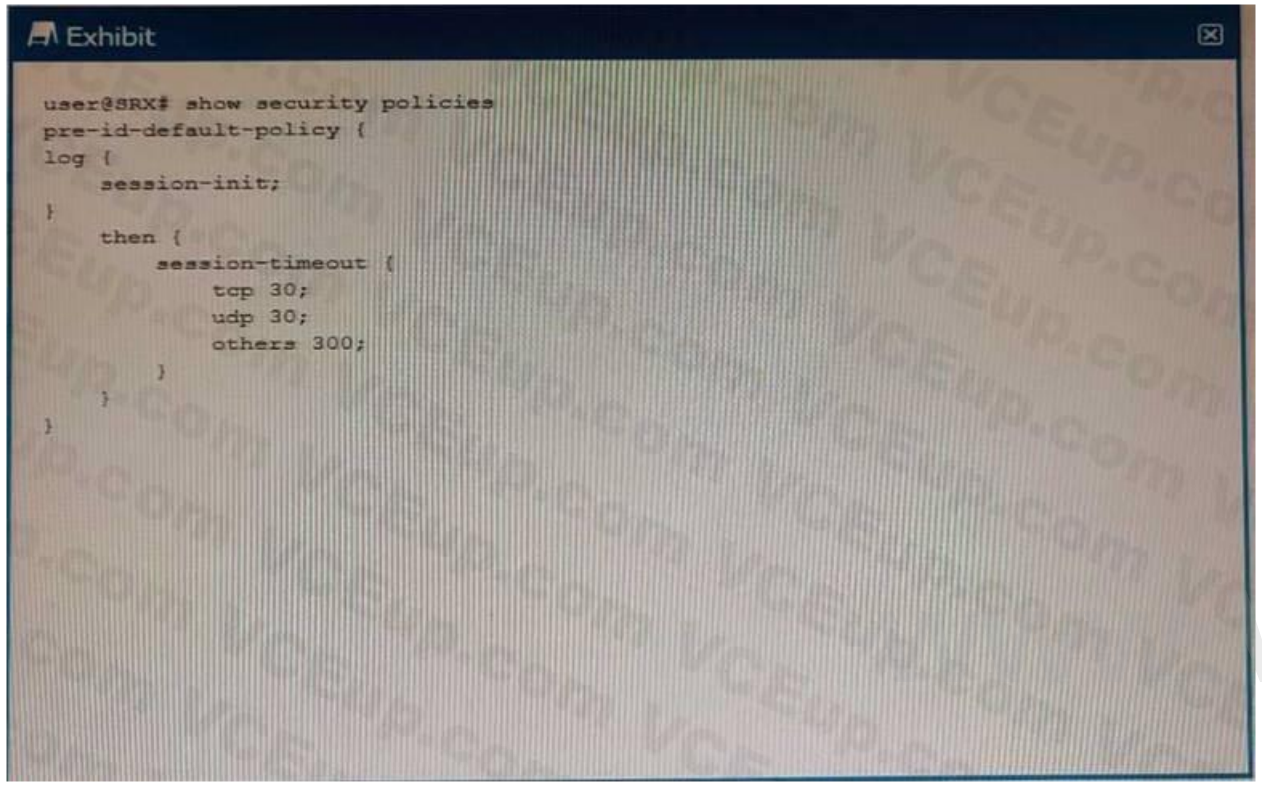
Answer: D

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 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 No: 42

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: BC

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 No: 43

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 Ul 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 Ul to update a custom profile and increase the scan limit for executable files to 30 MB.

Answer: D

Explanation:

In this scenario, you should use the ATP Cloud Ul 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 Ul 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 No: 44

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

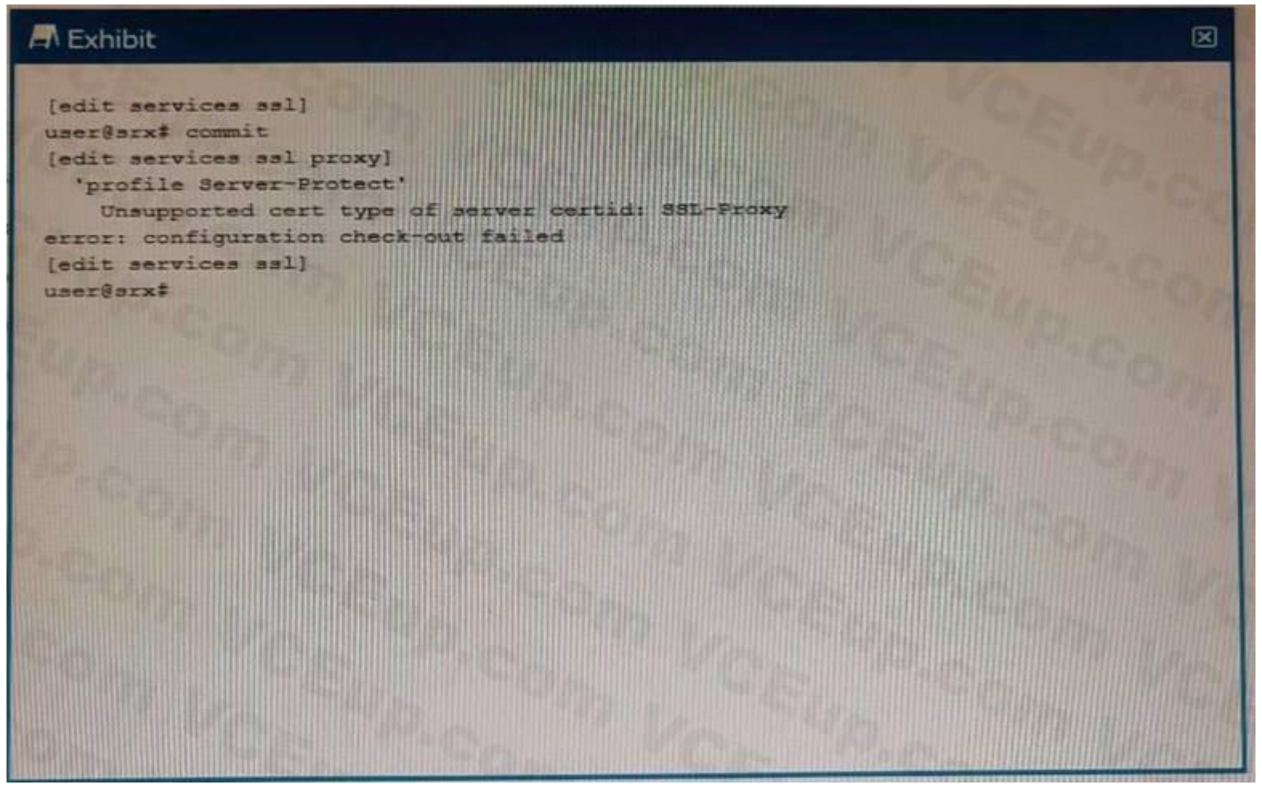
Answer: BD

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 No: 45

Exhibit



```
[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.

Answer: AD

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/configurationstatement/ security-ssl-proxy-configuration.html.

Question No: 46

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.

Answer: CD

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/releaseindependent/ security/jnpr-security-srx-series/information-products/topic-collection/jnpr-securitysrx- resources.html#id-jnpr-security-srx-resources-atp-cloud.

Question No: 47

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.

Reference: Security, Specialist (JNCIS-SEC) Study Guide. Chapter 5: Security Policies.

Question No: 48

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

Answer: B

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.

Reference: Juniper Networks. JNCIS-SEC Study Guide: Chapter 8, Intrusion Prevention System (IPS).

Question No: 49

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: ABE

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 No: 50

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 aggress.ve 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

Answer: BD

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 No: 51

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

Answer: BC

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 No: 52

You are experiencing excessive packet loss on one of your two WAN links route traffic from the degraded link to the working link Which AppSecure component would you use to accomplish this task?

A. AppFW

B. AppQoE

C. AppQoS

D. APBR

Answer: D

Explanation:

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

Question No: 53

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

A. JIMS

B. ATP Appliance

C. Network Director

D. NETCONF

Answer: A

Explanation:

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

Question No: 54

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

A. vQFX

B. MX

C. vMX

D. QFX

Answer: BC

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 highperformance hardware and advanced security features.

Question No: 55

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

Answer: AC

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.

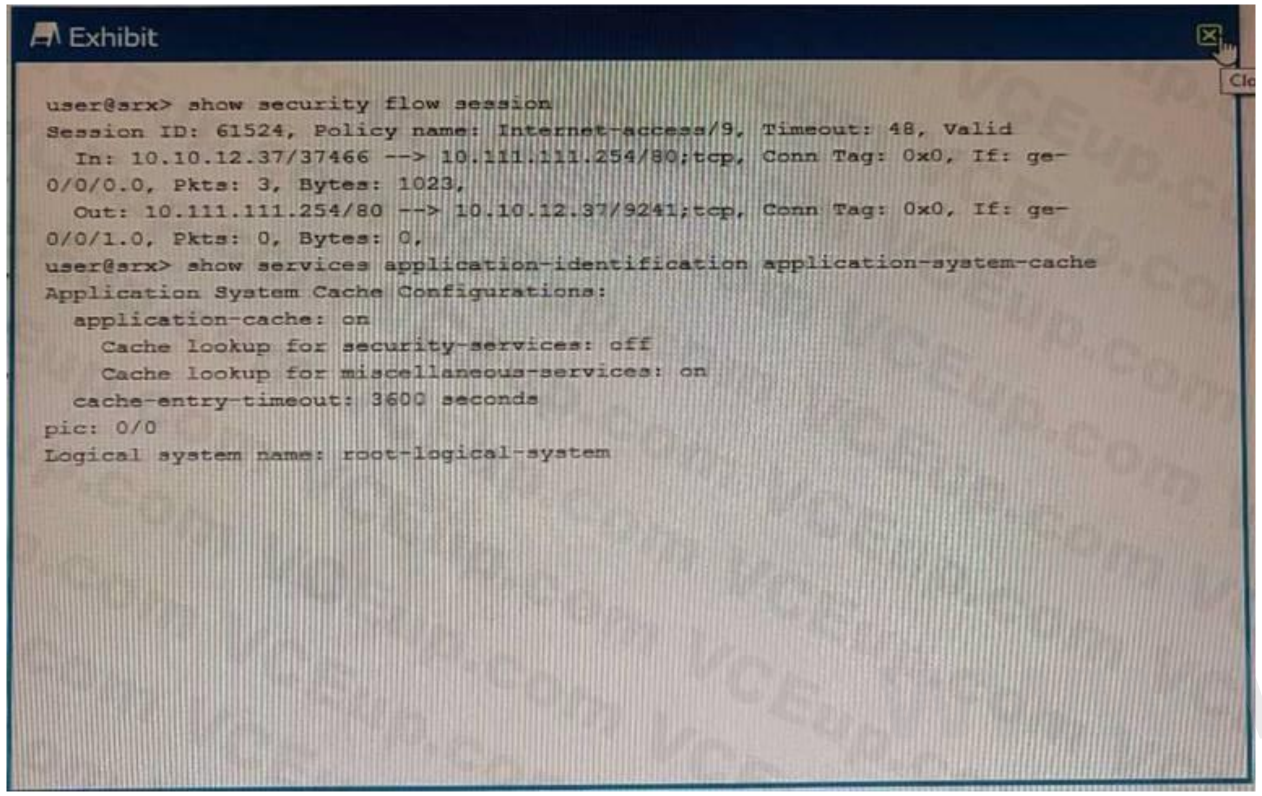
Granular Security: vSRX allows for granular security policies to be enforced at the virtual interface level, making it an effective solution for securing traffic in a software-defined network.

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 No: 56

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

Answer: D

Explanation:

Question No: 57

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: BC

Explanation:

1. 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.

2. 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 No: 58

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

Answer: AD

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 softwaredefined 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 No: 59

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

Answer: BD

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 No: 60

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.

Answer: AC

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 No: 61

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

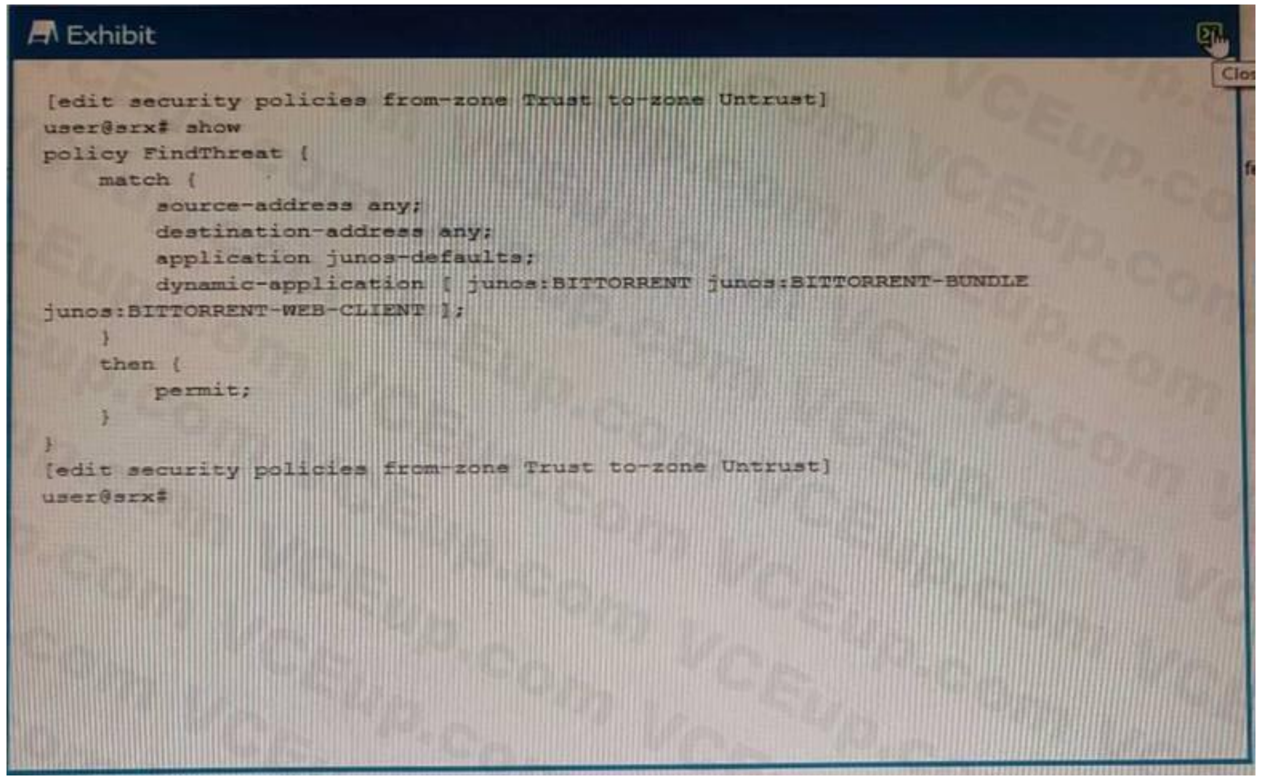
Answer: D

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, 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 No: 62

Exhibit



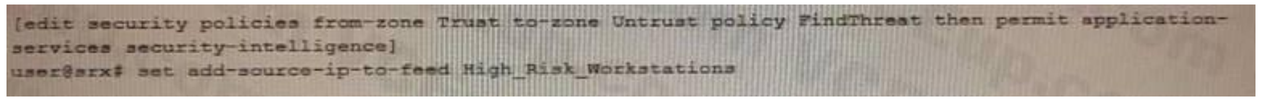
Exhibit

```
[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.

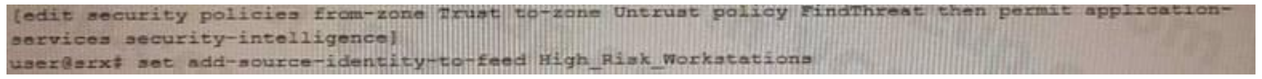
Which two commands would add this functionality to the FindThreat policy? (Choose two.)

A)



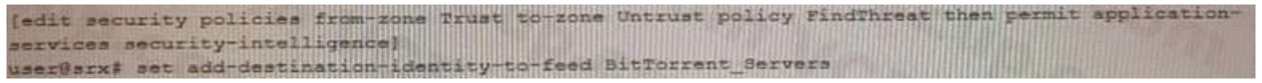
```
[edit security policies from-zone Trust to-zone Untrust policy FindThreat then permit application-
services security-intelligence]
user@srx# set add-source-ip-to-feed High_Risk_Workstations
```

B)



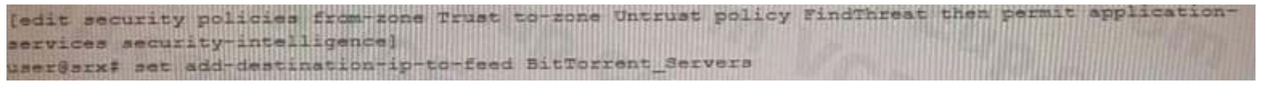
```
[edit security policies from-zone Trust to-zone Untrust policy FindThreat then permit application-
services security-intelligence]
user@srx# set add-source-identity-to-feed High_Risk_Workstations
```

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

Answer: C

Explanation:

Question No: 63

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

Answer: BC

Explanation:

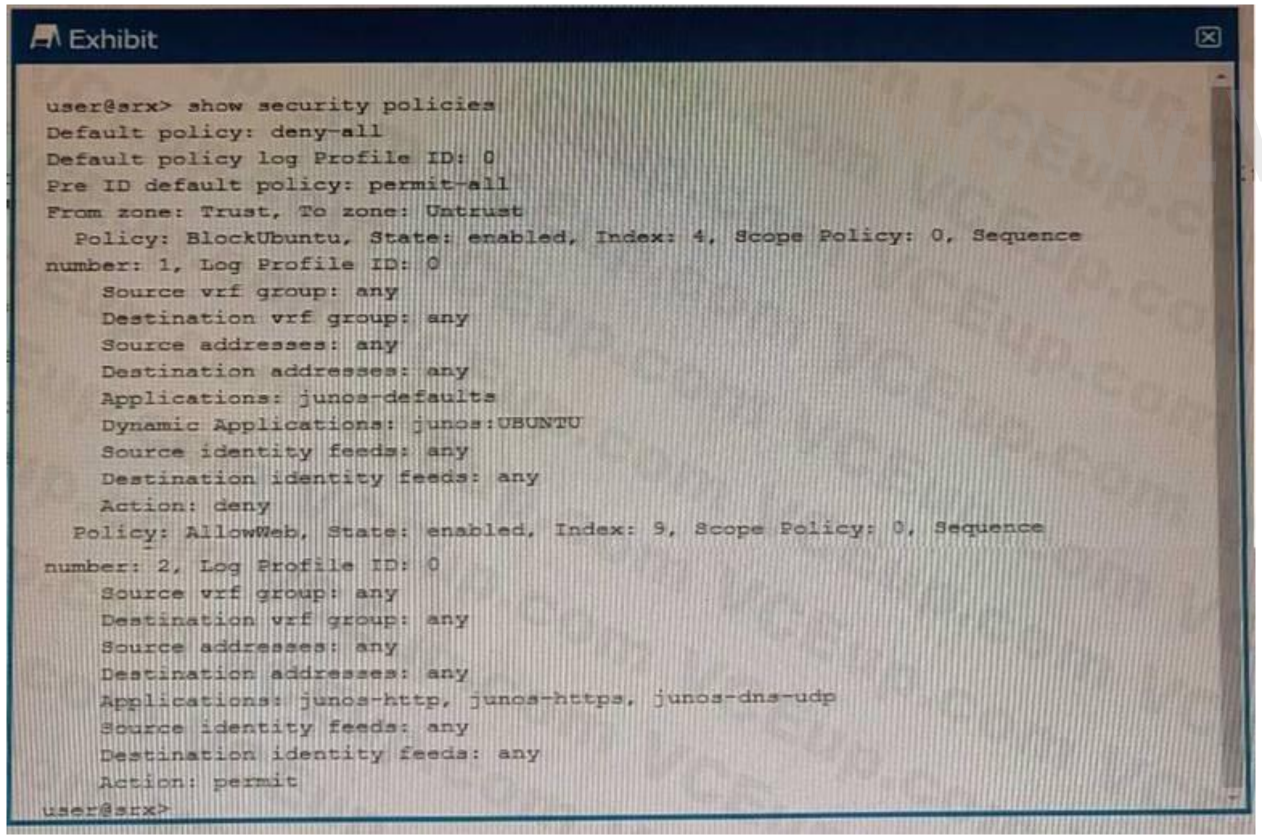
Based on SSL proxy is a feature that allows SRX Series devices to decrypt and inspect SSL/TLS traffic for security purposes. According to SRX Series devices support two types of SSL proxy:

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 No: 64

Exhibit



```
user@srx> show security policies
Default policy: deny-all
Default policy log Profile ID: 0
Pre ID default policy: permit-all
From zone: Trust, To zone: Untrust
  Policy: BlockUbuntu, State: enabled, Index: 4, Scope Policy: 0, Sequence
number: 1, Log Profile ID: 0
    Source vrf group: any
    Destination vrf group: any
    Source addresses: any
    Destination addresses: any
    Applications: junos-defaults
    Dynamic Applications: junos:UBUNTU
    Source identity feeds: any
    Destination identity feeds: any
    Action: deny
  Policy: AllowWeb, State: enabled, Index: 9, Scope Policy: 0, Sequence
number: 2, Log Profile ID: 0
    Source vrf group: any
    Destination vrf group: any
    Source addresses: any
    Destination addresses: any
    Applications: junos-http, junos-https, junos-dns-udp
    Source identity feeds: any
    Destination identity feeds: any
    Action: permit
user@srx>
```

You are asked to ensure that servers running the Ubuntu OS will not be able to update automatically by blocking their access at the SRX firewall. You have configured a unified security policy named Blockuburrtu, but it is not blocking the updates to the OS.

Referring to the exhibit which statement will block the Ubuntu OS updates?

A. Move the Blockubuntu policy after the Allowweb policy.

B. Configure the Blockubuntu policy with the junos-https application parameter.

C. Change the default policy to permit-all.

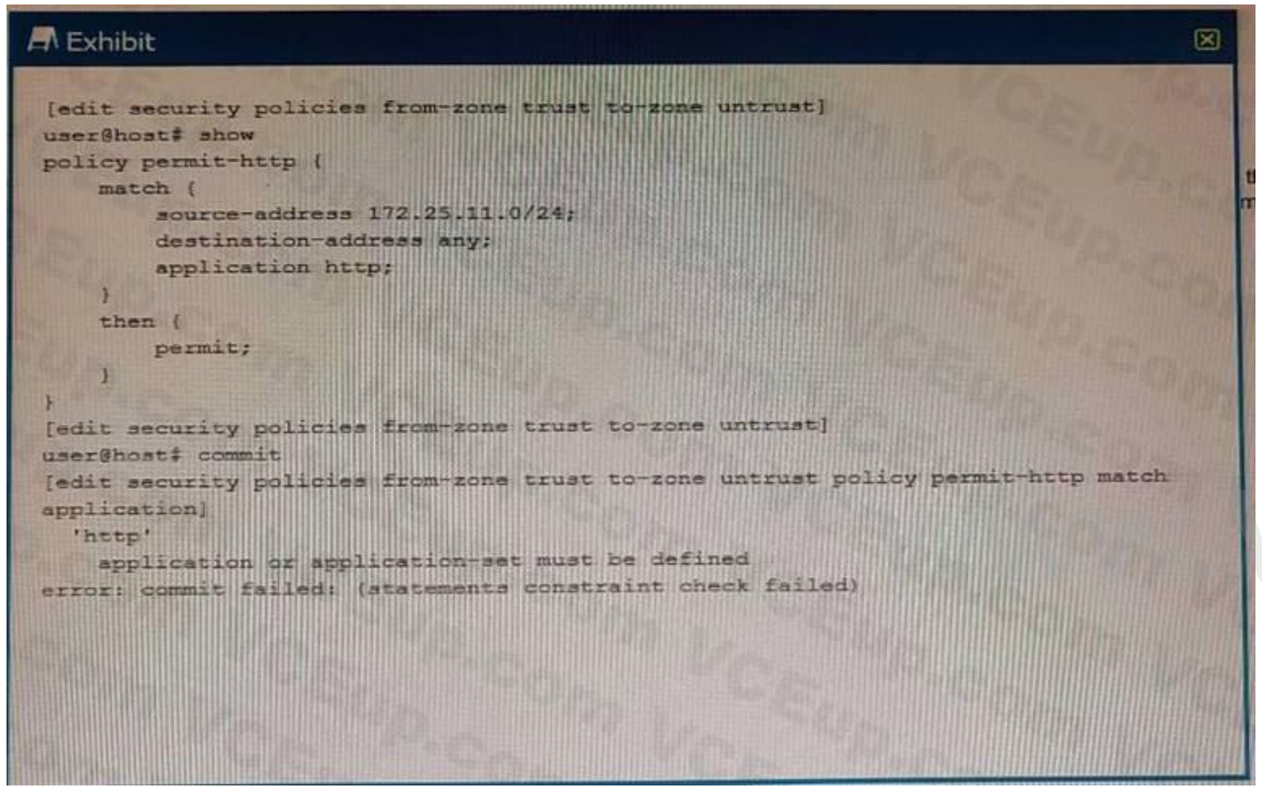
D. Configure the Allowweb policy to have a dynamic application of any.

Answer: B

Explanation:

Question No: 65

Exhibit



```
[edit security policies from-zone trust to-zone untrust]
user@host# show
policy permit-http {
    match {
        source-address 172.25.11.0/24;
        destination-address any;
        application http;
    }
    then {
        permit;
    }
}
[edit security policies from-zone trust to-zone untrust]
user@host# commit
[edit security policies from-zone trust to-zone untrust policy permit-http match
application]
  'http'
    application or application-set must be defined
error: commit failed: (statements constraint check failed)
```

You are trying to create a security policy on your SRX Series device that permits HTTP traffic fromyour private 172 25.11.0/24 subnet to the Internet You create a policy named permit-http betweenthe trust and untrust zones that permits HTTP traffic. When you issue a commit command to applythe configuration changes, the commit fails with the error shown in the exhibit.

Which two actions would correct the error? (Choose two.)

A. Issue the rollback 1 command from the top of the configuration hierarchy and attempt the commit again.

B. Execute the Junos commit full command to override the error and apply the configuration.

C. Create a custom application named http at the [edit applications] hierarchy.

D. Modify the security policy to use the built-in Junos-http applications.

Answer: CD

Explanation:

The error message indicates that the Junos-http application is not defined, so you need to eithercreate a custom application or modify the security policy to use the built-in Junos-http application.

Doing either of these will allow you to successfully commit the configuration.