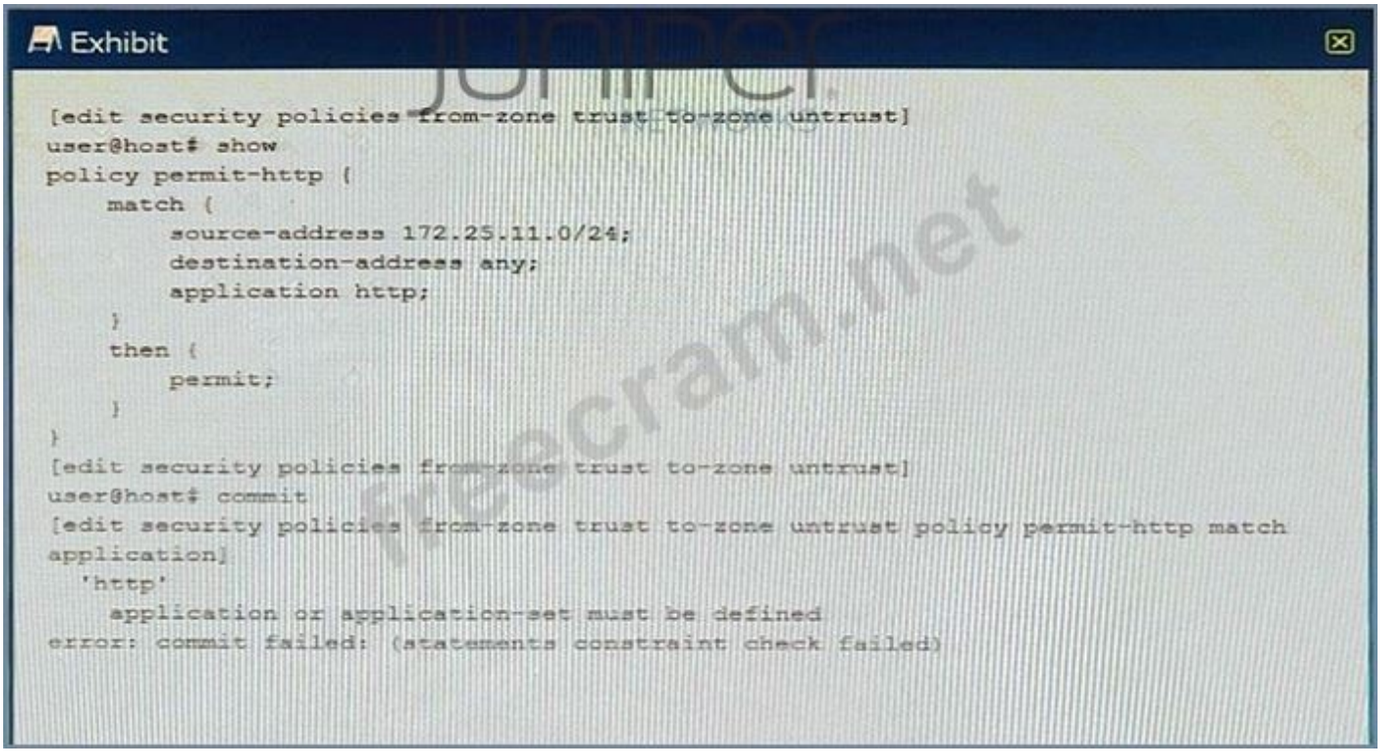
Juniper.JN0-336.v2026-05-09.q48

Exam Code:	JN0-336
Exam Name:	Security, Specialist (JNCIS-SEC)
Certification Provider:	Juniper
Free Question Number:	48
Version:	v2026-05-09
# of views:	107
# of Questions views:	486
https://www.freecram.net/torrent/Juniper.JN0-336.v2026-05-09.q48.html	

NEW QUESTION: 1
Exhibit



You are trying to create a security policy on your SRX Series device that permits HTTP traffic from your private 172 25.11.0/24 subnet to the Internet You create a policy named permit-http between the trust and untrust zones that permits HTTP traffic. When you issue a commit command to apply the 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: (SHOW ANSWER)

The error message indicates that the Junos-http application is not defined, so you need to either create 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.

NEW QUESTION: 2

Click the Exhibit button.

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.

Answer: (SHOW ANSWER)

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. Reference: = Security Intelligence Theory, Firewall Filter Support on Loopback Interface

NEW QUESTION: 3
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: (SHOW ANSWER)
B: 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.
C: 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.
E: 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.

NEW QUESTION: 4
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: (SHOW ANSWER)
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-co

NEW QUESTION: 5
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: (SHOW ANSWER)
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.

NEW QUESTION: 6
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: (SHOW ANSWER)
vSRX provides flexible networking capabilities which include support for both Layer 2 (data link) and Layer 3 (network) configurations. This allows it to handle a variety of routing and switching tasks within virtual environments.
Clustering capability, which involves grouping multiple vSRX instances to operate as a single entity for redundancy and high availability, is a feature specific to vSRX. This is critical in environments where continuous uptime and resilience are required.

NEW QUESTION: 7

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-close
B. deny
C. count
D. session-init
Answer: (SHOW ANSWER)

NEW 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
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 9
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.
Answer: (SHOW ANSWER)
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.

Reference: = Configuring Redundant Ethernet Interfaces, [Understanding Redundant Ethernet Interfaces]

NEW QUESTION: 10

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: (SHOW ANSWER)

When using SSL proxy, the servers themselves do not require any special configuration to utilize the SSL proxy function on the SRX device. The SSL proxy operates transparently, intercepting and decrypting SSL/TLS traffic before it reaches the servers.

For the SSL proxy to function effectively, especially in server protection mode where it impersonates the server to the client, it is necessary to load the server's certificates onto the SRX device. This allows the SRX to establish a trusted connection with the client using the server's credentials.

NEW QUESTION: 11

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.

Answer: B,D (LEAVE A REPLY)

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.

Reference: = Juniper Networks Expands Connected Security Portfolio with Encrypted Traffic Analysis for Juniper Advanced Threat Prevention and SecIntel for Mist Wireless, Encrypted Traffic Insights Overview, Configure Encrypted Traffic Insights

NEW QUESTION: 12
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: (SHOW ANSWER)
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.

NEW QUESTION: 13
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 (LEAVE A REPLY)
Encrypted traffic insights (ETI) uses domain names to notify SRX Series devices about known malware sites. ETI is a feature of the SRX Series firewall that can detect and block malware that is hidden in encrypted traffic. It works by analyzing the domain names of the websites that the encrypted traffic is attempting to access. If the domain name matches a known malware site, ETIwill send an alert to the SRX Series device, which can then take appropriate action to block the traffic. ETI is a useful tool for protecting against threats that attempt to evade detection by hiding in encrypted traffic.

NEW QUESTION: 14
You are troubleshooting unexpected issues on your JIMS server due to out of order event log timestamps.
Which action should you take to solve this issue?
A. Enable time synchronization on the client devices.
B. Enable time synchronization on the JIMS server.
C. Enable time synchronization on the domain controllers.
D. Enable time synchronization on the SRX Series devices.
Answer: (SHOW ANSWER)
To solve the issue of out of order event log timestamps on your JIMS server, you should enable time synchronization on the domain controllers. 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 and CSO for identity-based security policies. JIMS relies on the timestamps of the event logs generated by the domain controllers to track user logins, logouts, and IP address changes. If the domain controllers have different or inaccurate clocks, the event logs may have out of order or incorrect timestamps, which can cause JIMS to miss or misinterpret some events and affect its accuracy and performance. Therefore, you should ensure that all the domain controllers in your network are synchronized with a reliable time source, such as an NTP server or a Windows Time service. Reference: = Juniper Identity Management Service User Guide, Juniper Identity Management Service Feature Guide, Configure JIMS Collector to Get Microsoft Event Logs, Considerations for timestamps in centralized logging platforms

NEW QUESTION: 15
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: (SHOW ANSWER)
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.

NEW QUESTION: 16
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: (SHOW ANSWER)
In chassis clustering, the node ID is indeed used to uniquely identify each device within the cluster. This allows for individual addressing and management of devices within the cluster configuration, which is crucial for operations and maintenance.
Typically, activating changes that involve chassis clustering configuration, such as setting or changing the node ID or forming a new cluster, requires a reboot of the devices. This ensures that

all configuration changes are properly applied and that the devices can synchronize their states as part of the cluster.

NEW QUESTION: 17
Which two statements are true about application identification? (Choose two.)
A. Application identification can identity 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.
Answer: A,D (LEAVE A REPLY)
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.
Reference: = [Application Identification Overview], [Application Identification Concepts], [Understanding Signature Rules and Protocol Anomaly Rules]

NEW QUESTION: 18
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.

Answer: (SHOW ANSWER)

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.

Reference: = Configuring Chassis Clustering on SRX Series Devices, SRX Series Chassis Cluster Configuration Overview, Connecting SRX Series Firewalls to Create a Chassis Cluster

NEW QUESTION: 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: (SHOW ANSWER)

Micro application detection is a feature that enables more granular control over applications by identifying and taking action on sub-features or specific behaviors within an application. For example, allowing access to Facebook while blocking Facebook Chat.

Application Identification (APPID) is a feature that identifies and controls applications based on their traffic patterns and characteristics. APPID can be configured to recognize not only the main application but also its various subcomponents, allowing for precise control over what is allowed or blocked.

NEW QUESTION: 20

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.

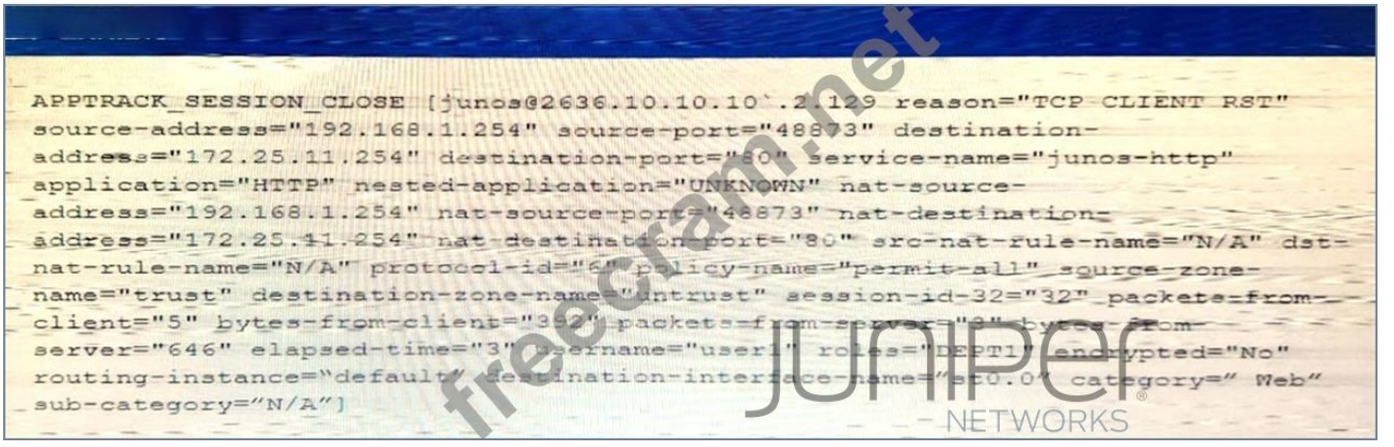
C. Use the CLI to change the default profile to increase the scan limit for all files to 30 MB.

D. Use the ATP Cloud UI to update a custom profile and increase the scan limit for executable files to 30 MB.

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 21
Click the Exhibit button.



Which two statements about the log output shown in the exhibit are correct? (Choose two)
A. AppTrack is enabled on the untrust zone.
B. AppTrack is enabled on the trast zone.
C. Traffic destined to the HTTP server is placed in an IPsec tunnel
D. Source NAT is performed
Answer: (SHOW ANSWER)

NEW QUESTION: 22
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: (SHOW ANSWER)
In many threat intelligence and evaluation systems, including Juniper ATP Cloud, the threat levels are often scored on a scale to provide a quick reference of the potential risk associated with a threat. A common range for these threat levels is from 0 to 10, with 0 representing minimal or no threat and 10 representing a severe threat.

Alternatively, some systems may use a more granular scoring system ranging from 0 to 100, providing a more nuanced assessment of threat levels. This range allows for finer differentiation between the levels of threat severity.

NEW QUESTION: 23
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. AppTrack
B. AppQoE
C. APPID
D. AppFW
Answer: (SHOW ANSWER)

NEW QUESTION: 24
On an SRX5800, which port is used for chassis cluster out-of-band management?
A. Txp0
B. user-defined
C. ge-0/0/0
D. fxp1
Answer: (SHOW ANSWER)

NEW QUESTION: 25
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: (SHOW ANSWER)
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.

NEW QUESTION: 26
You are preparing a proposal for a new customer who has submitted the following requirements for a vSRX deployment:
-- globally distributed,
-- rapid provisioning,
-- scale based on demand,
-- and low CapEx.

Which solution satisfies these requirements?

A. AWS

B. Network Director

C. Juniper ATP Cloud

D. VMWare ESXi

Answer: (SHOW ANSWER)

The solution that satisfies the requirements for a vSRX deployment is AWS. AWS (Amazon Web Services) is a cloud computing platform that provides on-demand services such as infrastructure, platform, software, and database as a service. AWS is globally distributed, meaning that it has data centers in multiple regions around the world. AWS also allows rapid provisioning, meaning that you can launch vSRX instances in minutes using preconfigured Amazon Machine Images (AMIs) or custom templates. AWS also enables scaling based on demand, meaning that you can adjust the number and size of vSRX instances according to your network traffic and performance needs. AWS also has low CapEx (capital expenditure), meaning that you only pay for what you use and do not need to invest in hardware or maintenance costs.

Reference: = vSRX Deployment Guide for AWS, Understand vSRX Virtual Firewall with AWS, What Is Amazon Web Services?

NEW QUESTION: 27

Click the Exhibit button.

```
user@host> show chassis cluster status redundancy-group 1
Cluster: 1, Redundancy-Group: 1
Device name     Priority     Status      Prempt  Manual  failover
node0           0            Secondary   No      No
node1           200          Primary     No      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.

Answer: (SHOW ANSWER)

The output indicates that node1 has a priority of 200 and is marked as "Primary," which means it is currently the active node controlling traffic for redundancy group 1. The "Primary" status designates that this node is handling the traffic for the specified redundancy group.

According to the exhibit, node0 is listed with a priority of 0 and is marked as "Secondary." This status indicates that node0 is currently not controlling traffic for redundancy group 1, serving instead in a standby role ready to take over should node1 fail or become unavailable.

NEW QUESTION: 28

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

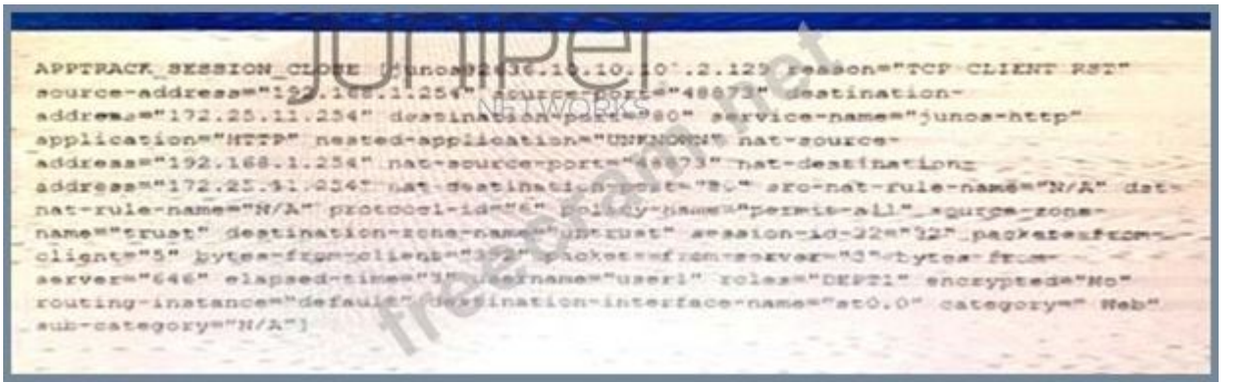
A. When a packet matches a unified security policy, the evaluation process terminates

B. Unified security policies must come before traditional security policies
C. When a packet matches a traditional security policy, the evaluation process terminates
D. Traditional security policies must come before unified security policies
Answer: (SHOW ANSWER)

NEW QUESTION: 29
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.
Answer: (SHOW ANSWER)
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.
Reference: = [Security Policies Overview], [Security Policy Processing Overview]

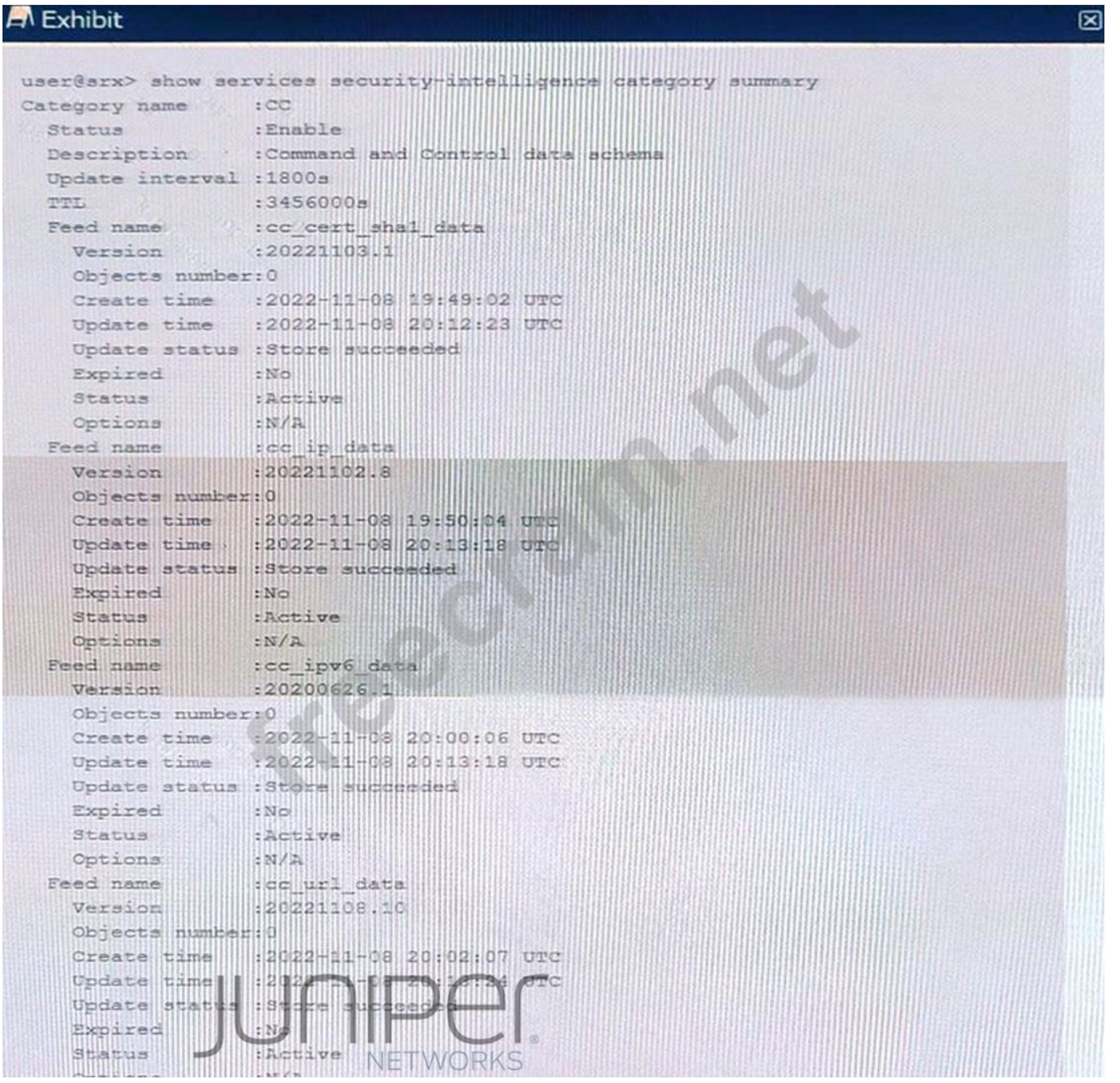
NEW QUESTION: 30
Which two statements are true about the fab interface in a chassis cluster? (Choose two.)
A. The fab link does not support fragmentation.
B. The physical interface for the fab link must be specified in the configuration.
C. The fab link supports traditional interface features.
D. The Junos OS supports only one fab link.
Answer: (SHOW ANSWER)
The fabric link, used for data traffic synchronization between cluster nodes, is designed to handle packets at full size. It does not support packet fragmentation, which means that packets should be sized appropriately to avoid issues related to packet size limitations on the fab interface.
For chassis clustering, the specific physical interfaces used as fabric links (fab links) must be explicitly defined in the configuration. This specification is crucial to ensure proper data flow between nodes for state synchronization and other clustering functions.

NEW QUESTION: 31
Click the Exhibit button.



Which two statements about the log output shown in the exhibit are correct? (Choose two?
A. AppTrack is enabled on the trost zone:
B. AppTrack is enabled on the untrust zone
C. Source NAT is performed
D. Traffic destined to the HTTP server is placed in an IPsec tunnel
Answer: (SHOW ANSWER)

NEW QUESTION: 32
Exhibit



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: (SHOW ANSWER)

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.

NEW QUESTION: 33
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: (SHOW ANSWER)
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.

NEW QUESTION: 34
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. heartbeat-interval
B. heartbeat-address
C. heartbeat-cos
D. heartbeat-threshold
Answer: (SHOW ANSWER)
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

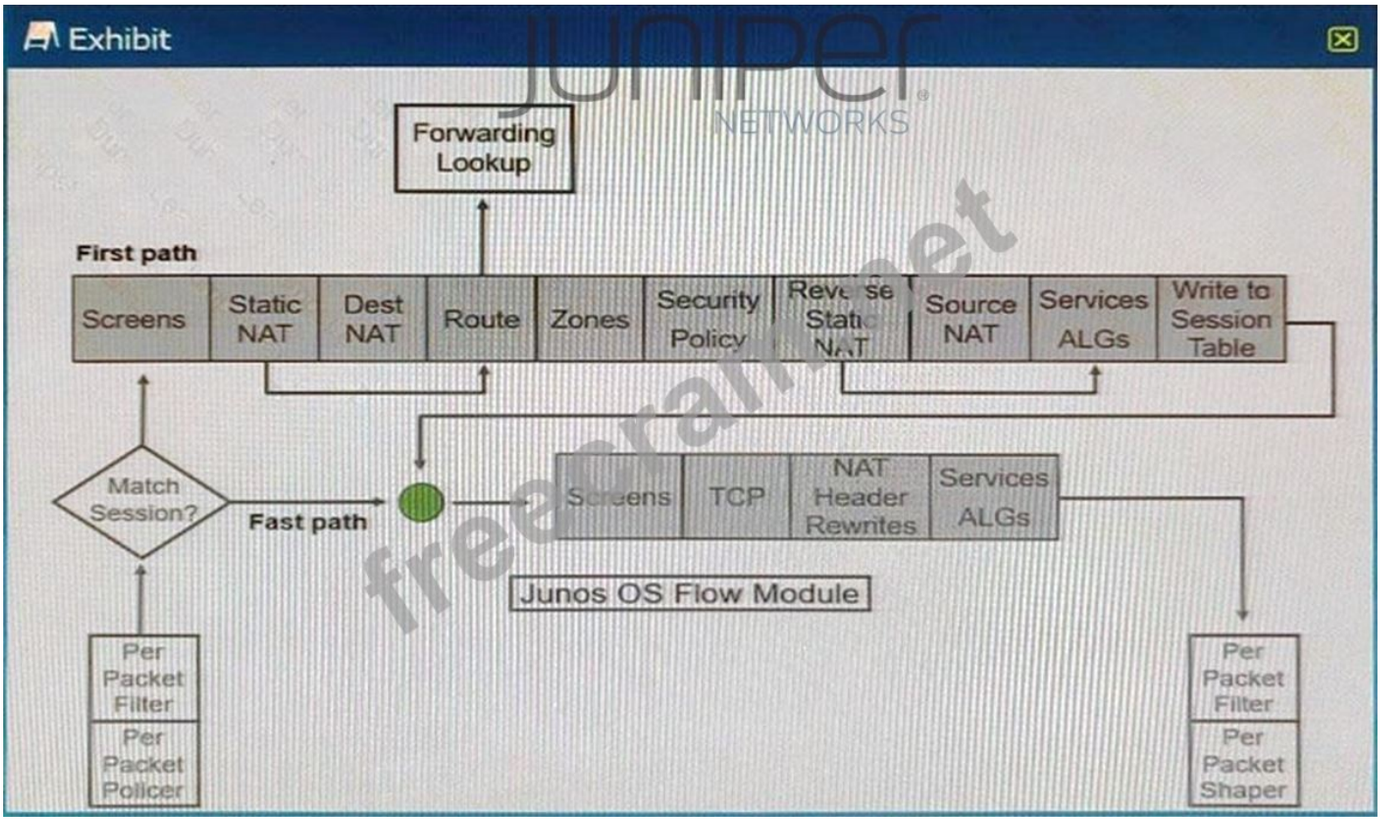
NEW QUESTION: 35
Which two statements about unified security policies are correct? (Choose two.)
A. Unified security policies require an advanced feature license.
B. Traffic can initially match multiple unified security policies.
C. Unified security policies are evaluated after global security policies.
D. APPID results are used to determine the final security policy
Answer: (SHOW ANSWER)

NEW QUESTION: 36
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
Answer: (SHOW ANSWER)
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

NEW QUESTION: 37
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: (SHOW ANSWER)
- 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.

NEW QUESTION: 38
Exhibit



Referring to the SRX Series flow module diagram shown in the exhibit, where is application security processed?
A. Screens
B. Services ALGs
C. Security Policy
D. Forwarding Lookup
Answer: (SHOW ANSWER)

NEW QUESTION: 39
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

Answer: (SHOW ANSWER)

An offense rule in JSA is designed to aggregate multiple events or log entries based on specified criteria into a single offense, which can then trigger responses such as notifications or actions like sending an SNMP trap. This type of rule is well-suited for scenarios where you need to monitor for patterns or rates of events, such as excessive firewall denies, and take action when these exceed defined thresholds.

Offense rules can analyze both event and flow data, making them highly versatile for comprehensive security monitoring.

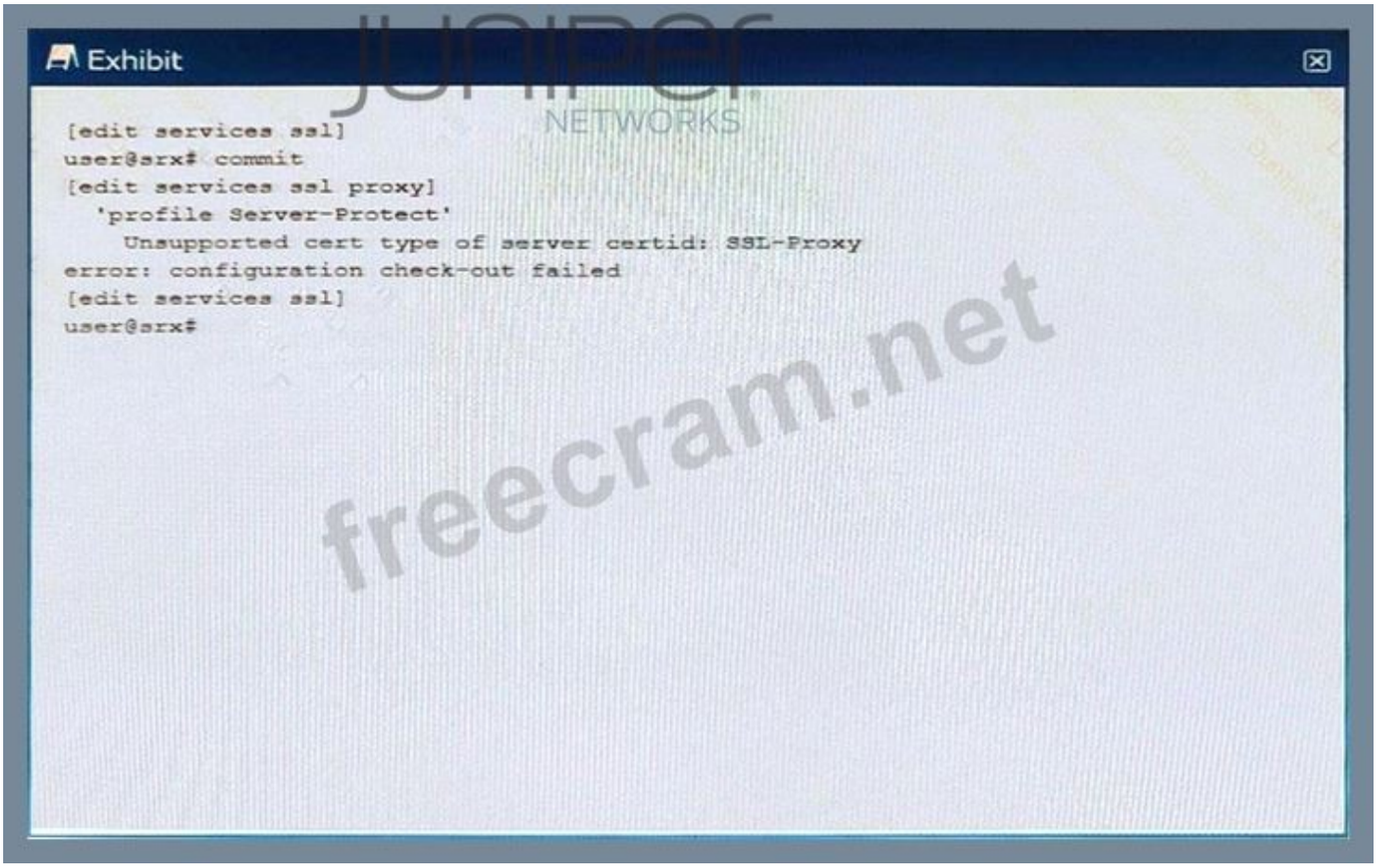
NEW QUESTION: 40

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.
Answer: (SHOW ANSWER)
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.
Reference: = Firewall Filter Support on Loopback Interface, [MX/SRX] The behavior of firewall filters that are applied on the loopback interfaces in virtual routers

NEW QUESTION: 41
Exhibit



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: B,D (LEAVE A REPLY)

The error message shown in the exhibit regarding the SSL proxy setup indicates an issue with the type of server certificate being used. The error explicitly states, "Unsupported cert type of server certid." Here are two plausible reasons for this error based on the options provided:

Option B. The SSL proxy certificate ID does not have the correct renegotiation option set.

This option points to a configuration issue related to the properties or capabilities of the certificate, such as renegotiation, which if not set correctly according to the expected requirements of the SSL proxy, might lead to the certificate being unsupported. Renegotiation settings are critical in ensuring secure connections, and mismatches in configuration can result in errors.

Option D. The SSL proxy certificate ID does not exist.

If the certificate ID being referred to in the SSL proxy profile does not exist in the device's certificate store or is incorrectly referenced, the system will be unable to apply the configuration, leading to an error during the commit operation. This situation would typically result in an error indicating that the system can't find or recognize the specified certificate ID.

NEW QUESTION: 42

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: (SHOW ANSWER)
Statistical sampling involves collecting a representative subset of data rather than examining all traffic.
While this method decreases processor utilization by reducing the volume of data that must be analyzed and stored, it can also lead to decreased accuracy in event correlation because not all events are captured.
Superflows in JSA are aggregated flow records that represent summaries of multiple flow records. This aggregation reduces the number of flows that need to be processed and stored, which can help in managing licensing requirements related to the volume of traffic being analyzed, especially in environments with high traffic volumes.

NEW QUESTION: 43
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: (SHOW ANSWER)
You can specify the source IP address or a range of IP addresses to exclude certain traffic originating from specific network segments or devices. This is useful for whitelisting traffic from known, secure sources that are otherwise triggering false positives in the IPS system.
Similarly, you can specify the destination IP address or a range of addresses to exclude traffic destined for particular network hosts or segments. This helps in reducing false positives for traffic directed towards trusted internal resources or specific external services that are known to be safe.

NEW QUESTION: 44
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: B,D (LEAVE A REPLY)

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.

NEW QUESTION: 45
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: (SHOW ANSWER)
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.

NEW QUESTION: 46
Click the Exhibit button.

You have implemented SSL client protection proxy. Employees are receiving the error shown in the exhibit.

How do you solve this problem?

A. Load a known good, but expired. CA certificate onto the SRX Series device.

B. Install a new SRX Series device to act as the client proxy

C. Reboot the SRX Series device.

D. Import the existing certificate to each client device.

Answer: (SHOW ANSWER)

SSL client protection proxy is a feature that allows you to decrypt and inspect the SSL traffic from clients to servers. To do this, you need to install a certificate authority (CA) certificate on the SRX Series device and import the same certificate to each client device. This way, the SRX Series device can act as a proxy between the client and the server and perform security checks on the decrypted traffic. If the client device does not have the certificate installed, it will receive an error message like the one shown in the exhibit. Reference: = JNCIS-SEC Certification, Open Learning - Security, Specialist (JNCIS-SEC), SSL Proxy Configuration

NEW QUESTION: 47

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: (SHOW ANSWER)

In the exhibit, the SRX Firewall could be acting as a forward proxy, managing outbound internet requests from internal users or clients within a private network to the internet. Forward proxies are commonly used to control and monitor outbound traffic, provide content caching to improve load times, and enforce company policies.

The scenario can also imply a reverse proxy setup where the SRX Firewall might be configured to direct incoming requests from the internet to the web application. Reverse proxies are used to balance load, enhance security, manage SSL encryption, and provide additional caching functionalities for inbound traffic to servers.

NEW QUESTION: 48

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: (SHOW ANSWER)

A single vSRX instance is capable of handling both firewall and NAT services simultaneously. This solution provides a streamlined and resource-efficient way to secure and manage network traffic within a private cloud environment.

Similar to the vSRX, a single cSRX can also provide both firewall and NAT services. The cSRX, being a containerized version of the SRX, is particularly suited for environments where high

density and microservices architectures are used, offering high performance in a compact form factor.