

Juniper.JN0-336.v2026-09-15.q30

Exam Code:	JN0-336
Exam Name:	Security, Specialist (JNCIS-SEC)
Certification Provider:	Juniper
Free Question Number:	30
Version:	v2026-09-15
# of views:	112
# of Questions views:	353
https://www.freecram.net/torrent/Juniper.JN0-336.v2026-09-15.q30.html	

NEW QUESTION: 1

You are implementing an SRX Series device at a branch office that has low bandwidth and also uses a cloud- based VoIP solution with an outbound policy that permits all traffic.

Which service would you implement at your edge device to prioritize VoIP traffic in this scenario?

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

Answer: (SHOW ANSWER)

The correct answer is D. AppQoS. The requirement is not to block, permit, translate, or inspect SIP signaling; it is to prioritize VoIP traffic on a low-bandwidth branch link. Juniper Application QoS, or AppQoS, is designed exactly for this purpose. Juniper states that AppQoS provides the ability to prioritize and meter application traffic so business-critical or high-priority application traffic receives better service. It can classify traffic by application, assign forwarding classes, rewrite DSCP values, set loss priority, and apply rate limiters.

Option A, AppFW, is wrong because AppFW controls application access; it is used to permit, deny, reject, or log application traffic, not primarily to prioritize voice traffic. Option B, SIP ALG, is wrong because the SIP ALG helps inspect and handle SIP control traffic and related media pinholes, but it is not a QoS prioritization service. Option C, AppQoS, is not the correct SRX edge service being tested here. For cloud-based VoIP under a broad outbound permit rule, AppQoS is the correct service because it can identify the VoIP application and give it better treatment during congestion. Reference topics: AppQoS, application traffic control, VoIP prioritization, DSCP rewrite, forwarding class, rate limiting.

NEW QUESTION: 2

Which two steps are necessary to prepare the Active Directory domain for a JIMS installation? (Choose two.)

- A. Create two limited access user accounts.
- B. Create three limited access user accounts.
- C. Add one full access user account to Active Directory groups.
- D. Add limited access user accounts to Active Directory groups.

Answer: ([SHOW ANSWER](#))

The correct answers are A and D. Preparing Active Directory for JIMS requires creating limited-permission service accounts and assigning those accounts to the required Active Directory groups. Juniper's JIMS deployment guidance states that you must create service accounts so JIMS can read from the defined directory services and identity producers; if PC probing is used, a service account is also required for that function. The same JIMS documentation includes a section named Configure Limited-Permission User Accounts, followed by Add Limited Permission User Accounts to Active Directory Groups.

Option A is correct because the JIMS preparation workflow commonly uses limited-permission accounts for event log access and PC probe access. Juniper identifies accounts such as JIMS-EventLogRemoteAccess and JIMS-PC-Probe in the Active Directory group-membership procedure. Option D is correct because those limited accounts must be added to the proper AD groups, including Event Log Readers and the groups required for remote management or PC probe operation.

Option B is wrong because the tested preparation requirement is not three limited-access accounts. Option C is wrong because JIMS should not be prepared by adding a broad full-access account; the course objective is least-privilege identity collection. Reference topics: JIMS, Active Directory preparation, limited-permission service accounts, Event Log Readers, PC probe account.

NEW QUESTION: 3

You are asked to use Junos Space Security Director to download the latest application signatures in the ApplD database.

In this scenario, which two statements are correct? (Choose two.)

- A. The ApplD database is stored in Junos Space Security Director.
- B. The ApplD database is stored on the managed SRX Series device.
- C. The ApplD database is maintained by a third-party host.
- D. The ApplD database is stored on a local storage server in the management network.

Answer: ([SHOW ANSWER](#))

The correct answers are A and B. In Security Director-managed environments, Security Director can download the signature database and then install the active signature database update on selected managed devices. Juniper's Security Director workflow states that after the signature database is downloaded, you install the active database, select the target devices, and Security Director sends the full or incremental signature database update to those devices. That confirms that Security Director stores and manages the signature database package centrally for deployment.

Option B is also correct because the SRX Series device must have the application signature database installed locally for AppID/AppSecure features such as AppFW, AppTrack, AppQoS, and IDP application matching.

Juniper's AppID documentation states that the application package is installed in the application signature database on the device, and that AppID signature updates enable AppSecure features on the SRX.

Option C is wrong because Juniper provides and maintains the predefined AppID database through Juniper's security download infrastructure, not a third-party host. Juniper explicitly describes the predefined application identification database as provided by Juniper Networks and updated through a subscription service. Option D is wrong because a local storage server can be used only as part of an offline/manual update workflow; it is not where the AppID database normally resides. Reference topics: Security Director, AppID database, application signatures, SRX AppSecure services, signature database installation.

NEW QUESTION: 4

When using Adaptive Threat Profiling, which two deployment modes are available on SRX Series devices?

(Choose two.)

- A. bridge
- B. inline
- C. tap
- D. promiscuous

Answer: (SHOW ANSWER)

The correct answers are B and C. Adaptive Threat Profiling allows SRX Series Firewalls to act either as inline enforcement devices or as tap-based sensors. In an inline deployment, the SRX is directly in the traffic path and can enforce policy actions such as blocking, denying, or adding threat indicators to Security Intelligence feeds for real-time mitigation. In a tap deployment, the SRX observes copied traffic from a TAP/SPAN-style feed and contributes intelligence without being the active forwarding device. Juniper's ATP Cloud documentation states that Adaptive Threat Profiling enables SRX devices to be deployed as sensors on Tap ports, identifying and sharing intelligence to inline devices for real-time enforcement. It also describes a "Tap- based SRX Series Firewall sensor" and contrasts it with an inline device.

Option A, bridge, is not the deployment mode being tested here. Bridge/transparent forwarding is a firewall deployment style, not the named Adaptive Threat Profiling mode. Option D, promiscuous, is also wrong; promiscuous mode is an interface behavior, not the ATP Adaptive Threat Profiling deployment model.

Reference topics: ATP Cloud, Adaptive Threat Profiling, tap sensors, inline enforcement, Security Intelligence feeds.

NEW QUESTION: 5

You need to deploy an SRX Series device in your virtual environment.

In this scenario, what are two benefits of using a cSRX? (Choose two.)

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

Answer: (SHOW ANSWER)

The correct answers are C and D. The cSRX is Juniper's containerized SRX firewall, intended for lightweight virtual and container environments where rapid deployment and high density matter. Juniper's cSRX documentation lists supported security capabilities including basic firewall policy, NAT, Intrusion Detection and Prevention, content security/UTM functions, ATP Cloud, SSL Proxy, AppID, AppFW, and AppTrack.

That supports option C, because cSRX provides SRX security services in a containerized footprint rather than requiring a full VM-based firewall appliance.

Option D is also correct because Juniper identifies the cSRX's small footprint and minimum resource reservation requirements as key benefits; it is designed to scale more densely than VM-based firewall options.

Juniper's Day One cSRX guide specifically identifies faster deployment, a small footprint, and reduced resource consumption as major benefits. Option A is not the best answer for this exam item because the question asks for cSRX deployment benefits, not merely forwarding-mode support. Option B is wrong because the tested cSRX advantage is not a default three-zone configuration. Reference topics: cSRX container firewall, virtual SRX deployment, firewall/NAT/IPS/UTM services, lightweight resource footprint.

NEW QUESTION: 6

You have configured a new site-to-site VPN tunnel. The exhibit shows the security IPsec statistics output for the specific tunnel index from one of the tunnel-end devices.

```
user@srx> show security ipsec statistics index 131073
ESP Statistics:
  Encrypted bytes: 0
  Decrypted bytes: 0
  Encrypted packets: 0
  Decrypted packets: 0
AH Statistics:
  Input bytes: 0
  Output bytes: 0
  Input packets: 0
  Output packets: 0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 83, ESP decryption failures: 79
  Bad headers: 0, Bad trailers: 0
```

Which two statements are correct in this scenario? (Choose two.)

- A. AH is incorrectly configured.
- B. The far-end tunnel device is rebooting.
- C. The ESP configuration is not set up correctly.
- D. No traffic passes through this tunnel.

Answer: C,D ([LEAVE A REPLY](#))

The correct answers are C and D. The exhibit shows ESP encrypted bytes = 0, ESP decrypted bytes = 0, encrypted packets = 0, and decrypted packets = 0. That means no traffic is successfully passing through the IPsec tunnel. Juniper's show security ipsec statistics command displays ESP encrypted/decrypted packet and byte counters, so zero values on these counters indicate that the tunnel is not successfully carrying protected ESP traffic.

Option C is also correct because the output shows ESP authentication failures and ESP decryption failures.

Since ESP is the IPsec protocol responsible for encrypted payload handling, failures in ESP authentication

/decryption point to an ESP/IPsec Phase 2 mismatch or incorrect configuration, such as mismatched authentication algorithm, encryption algorithm, keys, proposal parameters, or incompatible negotiated SA settings. Juniper's IPsec overview explains that Phase 2 negotiates the IPsec SA used to authenticate traffic flowing through the tunnel, so ESP-related failures belong to the IPsec/ESP configuration path rather than AH.

Option A is wrong because the AH counters and AH authentication failures are zero; the evidence is not pointing to AH. Option B is unsupported because the output does not show peer reboot behavior. Reference topics: IPsec VPN, ESP statistics, Phase 2/IPsec SA negotiation, ESP authentication failures, ESP decryption failures.

NEW QUESTION: 7

Which two statements describe how Juniper ATP Cloud improves security? (Choose two.)

- A.** It tracks and logs malicious traffic.
- B.** It offers real-time threat analysis and mitigation.
- C.** It simulates real user environments to trigger malicious code execution.
- D.** It increases performance speeds.

Answer: ([SHOW ANSWER](#))

The correct answers are B and C. Juniper ATP Cloud improves security by delivering cloud-based threat detection, malware analysis, and enforcement integration with SRX Series Firewalls. Juniper describes ATP Cloud as using shared cloud intelligence so customers benefit from new threat intelligence in near real time. It also provides zero-day threat protection, machine-learning-based malware detection, inline malware blocking, and policy actions that can stop malware, quarantine infected systems, prevent data exfiltration, and disrupt lateral movement.

Option C is also correct because Juniper ATP Cloud uses dynamic analysis, commonly called sandboxing. In this process, a suspicious file is executed in a secure environment while tools monitor its activity. Juniper further explains that ATP Cloud uses deception techniques to make the sandbox appear like a real user environment, including simulated mouse movement, keystrokes, common software packages, realistic network access, stored credentials, and vulnerable OS areas. This encourages evasive malware to execute and reveal malicious behavior.

Option A is weaker and not the best answer because logging alone is not the key ATP Cloud security-improvement mechanism being tested. Option D is wrong because ATP Cloud is a threat-prevention service, not a performance-acceleration technology. Reference topics: ATP Cloud, malware analysis, dynamic sandboxing, machine learning, threat intelligence, inline malware blocking.

NEW QUESTION: 8

You are asked to configure a cluster between SRX1 and SRX2.

Which two commands must be used to accomplish this task? (Choose two.)

- A. user@SRX2# set chassis cluster cluster-id 0 node 1
- B. user@SRX1 > set chassis cluster cluster-id 1 node 0
- C. user@SRX2 > set chassis cluster cluster-id 1 node 1
- D. user@SRX1# set chassis cluster cluster-id 0 node 2

Answer: ([SHOW ANSWER](#))

The correct answers are B and C. To form an SRX chassis cluster, both devices must be assigned the same cluster ID and different node IDs. Juniper states that the cluster ID identifies the cluster, while the node ID identifies the individual node within that cluster. A valid two-node SRX chassis cluster uses node 0 on one chassis and node 1 on the other chassis. Juniper's example shows the operational-mode commands as `set chassis cluster cluster-id 1 node 0 reboot` on the first device and `set chassis cluster cluster-id 1 node 1 reboot` on the second device.

Option A is wrong because cluster-id 0 disables clustering rather than forming a cluster. It also shows configuration-mode prompt #, while this chassis cluster node assignment is performed from operational mode.

Option D is doubly wrong: cluster-id 0 disables clustering, and node 2 is invalid because SRX chassis cluster node IDs are limited to 0 and 1. The exam options omit the reboot keyword, but the only logically valid pair is still SRX1 as node 0 and SRX2 as node 1 under the same nonzero cluster ID. Reference topics: HA Clustering, chassis cluster ID, node ID, operational-mode cluster enablement.

NEW QUESTION: 9

You are asked to set up SSL proxy in SRX Series devices. An SSL proxy profile is already defined for you.

Which two steps are required to complete the setup? (Choose two.)

- A. Reference the SSL proxy profile in a security policy.
- B. Enable host-inbound-traffic HTTPS in the security zone in which SSL proxy is referenced.
- C. Reference the SSL proxy profile in a security zone.
- D. Enable any Layer 7 services in the security policy in which SSL proxy is referenced.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 10

Which two statements are correct about redundant fabric interfaces in a chassis cluster? (Choose two.)

- A. fab0 and fab1 are located on both node0 and node1.
- B. fab0 is located on node0, whereas fab1 is located on node1.
- C. The media type must be the same for each redundant fabric interface.
- D. The media type can be different for each redundant fabric interface.

Answer: ([SHOW ANSWER](#))

The correct answers are B and C. In an SRX chassis cluster, the fabric connection is represented by two logical fabric interfaces: fab0 and fab1. Juniper configuration examples show fab0 assigned to the node0-side fabric member interface and fab1 assigned to the node1-side fabric member interface; for example, Juniper shows fab0 using a node0 interface such as ge-0/0/1 and fab1 using a node1 interface such as ge-7/0/1. That eliminates option A, because fab0 and fab1 are not both independently located on both nodes; they represent the two node sides of the cluster fabric link.

Option C is also correct. Juniper states that only the same type of interfaces can be configured as fabric children, and for dual fabric links both child interface types should match, such as Gigabit Ethernet with Gigabit Ethernet or 10-Gigabit Ethernet with 10-Gigabit Ethernet. Option D is therefore wrong because mixed media types are not supported for the redundant fabric child interfaces. Reference topics: HA Clustering, chassis cluster fabric interfaces, fab0/fab1, redundant fabric links, fabric child interface requirements.

NEW QUESTION: 11

In Juniper high availability (HA) SRX Series device implementations, which interface will be used to exchange session state, configuration files, and ensure session continuity across nodes using the proprietary Trivial Network Protocol?

- A. fab
- B. fxp0
- C. fxp1
- D. swfab

Answer: ([SHOW ANSWER](#))

The correct answer is A. fab. In SRX Series chassis clustering, the fabric interface, shown as fab0/fab1, is the data-plane HA link used between cluster nodes. Juniper states that SRX chassis clusters use the fabric interface for session synchronization and traffic forwarding, and that the fabric link synchronizes dynamic runtime state, including session-state objects created by NAT, ALG, authentication, and IPsec processing.

This is what enables stateful failover and session continuity when traffic processing moves between nodes.

Option B, fxp0, is wrong because fxp0 is the out-of-band management interface, not the chassis-cluster synchronization path. Option C, fxp1, is tempting but wrong for this question: fxp1 is the control-link interface used for control-plane cluster functions such as heartbeats and cluster control communication, not the main session-state synchronization path. Option D, swfab, is not the standard SRX chassis-cluster fabric interface name used for this function. Juniper's clustering

configuration examples specifically define fab0 and fab1 as the interfaces used for the fabric connection and data-plane RTO/session synchronization.

NEW QUESTION: 12

You are establishing an IPsec VPN and must ensure that payload data is encrypted. In this scenario, which IPsec security protocol should you configure?

- A. SHA-1
- B. ESP
- C. AH
- D. PFS

Answer: (SHOW ANSWER)

The correct answer is B. ESP. In IPsec, the security protocol responsible for encrypting protected traffic is Encapsulating Security Payload (ESP). Juniper defines ESP as the IPsec protocol used for encrypting the IP packet and authenticating its contents. In practical SRX VPN design, ESP is the normal protocol selected when confidentiality is required because it can provide encryption, packet integrity, authentication, and anti-replay protection depending on the configured IPsec proposal.

Option A, SHA-1, is incorrect because SHA-1 is an authentication/hash algorithm, not an IPsec security protocol and not a payload encryption mechanism. Option C, AH, is incorrect because Authentication Header validates packet source and integrity but does not encrypt payload data. AH is therefore unsuitable when the requirement explicitly says payload data must be encrypted. Option D, PFS, is incorrect because Perfect Forward Secrecy is a key-exchange property used during Phase 2 rekeying; it strengthens key independence but does not itself encrypt packets. In Junos IPsec configuration logic, the security protocol decision is between ESP and AH, and encryption requires ESP. Reference topics: IPsec VPN, ESP, AH, IPsec security protocols, payload confidentiality, IPsec proposal design.

NEW QUESTION: 13

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: C,D (LEAVE A REPLY)

The correct answers are C and D. Static attack object groups are manually defined groups. Juniper states that custom attack groups are static in nature because the attacks are explicitly specified in the group; therefore, those attack groups do not change when the security database is updated. This is the key difference between static groups and dynamic groups. Dynamic groups use matching criteria and can automatically update membership when the signature database changes, but static groups do not behave that way.

Option C is correct because updating the IPS/IDP signature database does not automatically add or remove members from a static attack group. Option D is correct because the administrator must explicitly add the desired attack objects to the custom static group. Option A describes dynamic matching behavior, not static group behavior. Option B is also dynamic-group behavior; Juniper Security Director documentation says dynamic group membership is automatically updated during signature updates based on the group's matching criteria. Static groups are intentionally deterministic: they include only the attacks manually selected by the administrator. Reference topics: IDP attack objects, static attack groups, custom attack groups, dynamic attack groups, IPS signature database updates.

NEW QUESTION: 14

Which statement is correct about Active Directory as an identity source for identity-aware security policies?

- A.** It supports a maximum of two domains.
- B.** It supports logical systems.
- C.** It supports 20 Active Directory servers per domain.
- D.** It tracks non-Windows Active Directory users.

Answer: ([SHOW ANSWER](#))

The correct answer is A. It supports a maximum of two domains. Juniper's Active Directory identity-source configuration guidance states that an SRX Series Firewall using the integrated user firewall/Active Directory identity source can be configured for a maximum of two domains. That is the exact limit relevant to this question. The same Juniper configuration page separately states that a maximum of 10 domain controllers can be configured, which directly eliminates option C because the supported figure is not 20 Active Directory servers per domain.

Option B is wrong because Active Directory identity source is not presented as a logical-systems feature in the JNCIS-SEC identity-aware firewall context. Option D is wrong because the primary Active Directory mechanism reads Windows domain controller event logs and uses WMI/DCOM plus LDAP to build IP-to- user and group mappings. Juniper describes the SRX as reading and monitoring the Windows event log on the domain controller, then using LDAP to obtain user/group information. Non-domain or non-Windows cases typically require alternate authentication behavior such as captive portal, not native Active Directory event- log tracking.

Reference topics: Identity-Aware Security Policies, Active Directory identity source, integrated user firewall, domain limits, domain controllers, WMIC, LDAP mapping.

NEW QUESTION: 15

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

- A.** If no match exists in cache, the remaining analysis features are processed with the cumulative threat score transmitted to the SRX Series device.
- B.** If a match exists in cache, that threat score is sent to the SRX Series device and the analysis continues.

- C.** If a match exists in cache, that threat score is sent to the SRX Series device and the analysis stops.
- D.** If no match exists in cache, the first analysis feature to generate a threat score is transmitted to the SRX Series device.

Answer: ([SHOW ANSWER](#))

The correct answers are A and C. Juniper ATP Cloud uses a malware-analysis pipeline. When a file is submitted, the first step is a cache lookup based on the file hash. Juniper explains that if the file has already been analyzed, the stored verdict is returned to the SRX Series Firewall and there is no need to re-analyze the file. That directly supports C and eliminates B, because analysis does not continue when a cached verdict is found.

If the cache lookup does not return a verdict, the remaining ATP Cloud analysis techniques are used. Juniper describes the pipeline model in which each analysis technique creates a verdict number, and those verdicts are combined into a final verdict score from 0 to 10. That final threat score is what the SRX compares against ATP Cloud policy settings to permit or block the session. Option D is wrong because ATP Cloud does not simply return the first score generated by any one feature.

The expected behavior is cumulative/final scoring across the remaining analysis pipeline.

Reference topics:

Juniper ATP Cloud, malware analysis pipeline, cache lookup, verdict number, threat score, SRX enforcement.

NEW QUESTION: 16

You want to configure the SSL proxy feature on your SRX Series Firewall.

Which two actions must you perform to accomplish this task? (Choose two.)

- A.** Enable the SSL ALG.
- B.** Create an SSL proxy profile.
- C.** Create an SSL application object.
- D.** Associate an SSL proxy profile with a security policy.

Answer: ([SHOW ANSWER](#))

The correct answers are B and D. On SRX Series Firewalls, SSL proxy is configured by creating an SSL proxy profile and then applying that profile to the relevant security policy as an application service. Juniper's SSL proxy configuration overview lists the required workflow: configure certificates and CA profile material, configure the SSL proxy profile, create a security policy matching the traffic to be inspected, and apply the SSL proxy profile to that security policy. Juniper further states that SSL proxy is enabled as an application service within a security policy, where the policy match criteria identify the traffic and the SSL proxy profile is applied to that traffic.

Option A is wrong because enabling the SSL ALG is not the required control point for SSL proxy. SSL proxy is a decryption/inspection service applied through policy, not simply an ALG toggle. Option C is wrong because creating a separate SSL application object is not the mandatory SSL proxy configuration action. The policy can match the desired traffic and then invoke SSL proxy

through then permit application-services ssl- proxy profile-name. Juniper's example explicitly shows applying the SSL proxy profile under the security policy action.

Reference topics: SSL Proxy, SSL forward proxy, SSL proxy profiles, security policy application-services, encrypted traffic inspection.

Valid JN0-336 Dumps shared by EduDump.com for Helping Passing JN0-336 Exam!

EduDump.com now offer the **newest JN0-336 exam dumps**, the EduDump.com JN0-336 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com JN0-336 dumps with Test Engine here:

<https://www.edudump.com/exams/Juniper/JN0-336/premium/> (70 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 17

Which two services would an SRX Series device use to connect to an LDAP server for identity-aware security policies? (Choose two.)

- A. Active Directory
- B. TACACS+
- C. RADIUS
- D. JIMS

Answer: ([**SHOW ANSWER**](#)**)**

NEW QUESTION: 18

What are two properties negotiated during IKE Phase 2? (Choose two.)

- A. routing protocol
- B. tunneling protocol
- C. aggressive mode
- D. Perfect Forward Secrecy

Answer: B,D ([**LEAVE A REPLY**](#)**)**

The correct answers are B and D. IKE Phase 2 negotiates the IPsec security associations used to protect actual user data through the VPN tunnel. Juniper explains that after Phase 1 establishes a secure authenticated channel, Phase 2 negotiates SAs for the data transmitted through the IPsec tunnel. A Phase 2 proposal includes the IPsec security protocol, which is either ESP or AH, along with selected encryption and authentication algorithms. In the wording of this question, that maps to the tunnel/security protocol property.

Option D, Perfect Forward Secrecy, is also correct because Phase 2 proposals can specify a Diffie-Hellman group when PFS is desired. PFS forces a new DH key exchange for Phase 2 keys so that compromise of earlier keying material does not expose later IPsec encryption keys. Option A is wrong because routing protocols are not negotiated by IKE Phase 2; routing is handled separately over or toward the tunnel interface.

Option C is wrong because aggressive mode is an IKEv1 Phase 1 exchange mode, not a Phase 2 property.

Juniper specifically states that Phase 2 always uses quick mode in IKEv1. Reference topics: IKE Phase 2, IPsec SA negotiation, ESP/AH, Perfect Forward Secrecy, quick mode.

NEW QUESTION: 19

Which two services would an SRX Series device use to connect to an LDAP server for identity-aware security policies? (Choose two.)

- A. Active Directory
- B. TACACS+
- C. RADIUS
- D. JIMS

Answer: ([SHOW ANSWER](#))

The correct answers are A and D. For identity-aware security policies, Junos can obtain user identity information from supported identity sources such as Active Directory and Juniper Identity Management Service (JIMS). Active Directory is the direct identity-source option where the SRX integrates with Microsoft Windows Active Directory and uses directory information for user and group mapping. Juniper's identity-aware firewall documentation states that the firewall obtains user information from identity sources including Active Directory and JIMS, and then uses that identity data in policy decisions.

JIMS is also correct because it centralizes identity collection and provides SRX enforcement points with user, device, IP address, and group-mapping information. Juniper describes JIMS as providing SRX firewalls with high-scale identity data so they can make user-firewall policy decisions. Option B, TACACS+, is wrong because TACACS+ is primarily an administrative authentication, authorization, and accounting protocol, not the LDAP identity-source service used for identity-aware firewall mappings. Option C, RADIUS, is also wrong in this context because RADIUS can authenticate users, but it is not the LDAP directory integration service being tested here. Reference topics: Identity-Aware Firewall, Active Directory identity source, JIMS, LDAP user/group mapping, SRX authentication table.

NEW QUESTION: 20

Which two statements are correct about fabric interfaces on an SRX Series Firewall? (Choose two.)

- A. In an active/active configuration, inter-chassis traffic uses the fab link.
- B. In an active/passive configuration, inter-chassis traffic uses the fab link.
- C. The node ID is reflected in the fabric interface name.
- D. The cluster ID is reflected in the fabric interface name.

Answer: ([SHOW ANSWER](#))

The correct answers are A and B. In SRX chassis clustering, the fabric link, represented by fab interfaces, is the data-plane connection between the two cluster nodes. Juniper describes the fabric as the back-to-back data connection used when traffic on one node must be processed on the other node or must exit through an interface on the other node; session-state information also

passes over the fabric. This is especially visible in active/active clustering, where ingress and egress interfaces can reside on different nodes and transit traffic must cross the fabric link. Option B is also correct because the fabric link still exists in active/passive clustering for cluster data-plane synchronization and inter-node state handling, even though active/passive designs minimize fabric transit traffic because only one node normally forwards traffic at a time. Juniper specifically states that active/passive mode minimizes traffic over the fabric link, not that the fabric link is unused.

Options C and D are not the intended answers. The cluster is identified by a configured cluster ID, and each chassis is identified by a node ID, but the fabric interface names themselves are not where the cluster ID is reflected. Reference topics: HA Clustering, fabric link, active/active clustering, active/passive clustering, session synchronization, inter-node traffic.

NEW QUESTION: 21

What are two ways to help reduce false positives for an IDP rule? (Choose two.)

- A. Change the rule to a lower severity action.
- B. Remove the attack object from the rule.
- C. Create an exempt rule.
- D. Configure a terminal rule at the end of the rule base.

Answer: ([SHOW ANSWER](#))

The correct answers are B and C. IDP false positives occur when legitimate traffic matches an attack signature or attack object incorrectly. One valid way to reduce false positives is to remove the problematic attack object from the IDP rule, especially when that object is not relevant to the protected application, server role, or traffic direction. Juniper defines attack objects as the items specified in IDP rules to identify malicious activity, so removing an irrelevant or noisy attack object directly reduces unwanted matches.

Option C is also correct because Juniper specifically recommends using an exempt rulebase when an IDP rule uses an attack object group containing attack objects that produce false positives or irrelevant log records.

Exempt rules can exclude a specific source, destination, or source/destination pair from matching an IDP rule, preventing unnecessary alarms.

Option A is wrong because changing the action to a lower severity response does not reduce the false positive; it only changes what happens after the false match occurs. Option D is wrong because a terminal rule at the end of the rule base does not prevent earlier false-positive matches. Reference topics: IDP, attack objects, exempt rulebase, false-positive tuning, IDP rule matching.

NEW QUESTION: 22

Using Junos Space Security Director, you want to configure a unique firewall policy for a specific SRX Series device.

Which firewall policy rules would satisfy the requirement?

- A. all devices policy prerules

- B. group policy prerules
- C. device policy rules
- D. all devices policy postrules

Answer: ([SHOW ANSWER](#))

The correct answer is C. device policy rules. In Junos Space Security Director, policy scope matters. A rule intended for one specific SRX Series device must be placed in a device policy, because Juniper defines a device policy as a firewall policy created per device and used when you want to push a unique firewall policy configuration per device. Security Director also distinguishes this from group policies, which are shared with multiple devices, and from all-devices policy rules, which are global in scope rather than device-specific.

Option A is wrong because all-devices prerules are global rules evaluated before device-specific rules; they are not intended for a unique single-device exception. Option B is wrong because group policy prerules apply to devices within a group, not to one individually targeted SRX firewall. Option D is wrong because all-devices postrules are still globally scoped, even though they occur later in policy order. The clean Security Director design is to use device policy rules when the policy must apply only to one SRX device. Reference topics: Security Director, firewall policy hierarchy, device policy, group policy, all-devices prerules/postrules.

NEW QUESTION: 23

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 correct answer is B. count. In Junos security policy configuration, count is the policy parameter used for accounting and tabular operational visibility. Juniper's security policy configuration rules state that accounting and auditing elements can be specified with count and log, while logging itself is enabled at either session-init or session-close.

The operational result is visible through commands such as show security policies hit-count, which displays a table of policy hit counters, including fields such as index, from-zone, to-zone, policy name, policy count, and action. Juniper defines this command as displaying the number of times a security policy rule matches traffic, and the sample output is explicitly tabular. Option A, permit, is an action, not a counter or logging/accounting parameter. Option C, session-init, logs at the beginning of a session, and option D, session-close, logs at session teardown. Those two parameters generate logs, but they do not provide the tabular policy-count view being asked about. Reference topics: security policy accounting, count parameter, hit-count, operational-mode policy monitoring, session-init/session-close logging.

NEW QUESTION: 24

Which three actions does Junos Space Security Director perform during the device discovery process?

(Choose three.)

- A. It imports the device's active device configuration.
- B. it reboots the device.
- C. It imports device status information.
- D. It adds a local superuser account to the device configuration.
- E. It connects to the device using SSH.

Answer: ([SHOW ANSWER](#))

The correct answers are A, C, and E. During Security Director device discovery, Junos Space first finds and connects to the managed device, then synchronizes the device inventory and configuration into the Junos Space database. Juniper's Security Director documentation states that discovery uses a discovery profile containing target information, authentication credentials, probes, and SSH fingerprints. During discovery, Junos Space connects to the physical device and retrieves the running configuration and status information. It also states that Junos Space uses SSH, with optional ping and SNMP, to discover network devices.

Option B is wrong because device discovery is not a reboot operation. Rebooting would be disruptive and is not part of onboarding a managed SRX into Security Director. Option D is wrong because discovery does not automatically inject a local superuser into the SRX configuration. Security Director authenticates using credentials supplied in the discovery profile; it does not create privileged local accounts as a discovery action.

The tested workflow is management-plane discovery: connect, authenticate, retrieve inventory/status, and import configuration state. Reference topics: Security Director, device discovery, discovery profiles, SSH, running configuration import, device status synchronization.

NEW QUESTION: 25

Which two statements are correct about the security associations of an IPsec VPN? (Choose two.)

- A. IPsec security associations are established during IKEv1 Phase 2 negotiations.
- B. IKEv1 security associations are established during IKEv1 Phase 2 negotiations.
- C. IPsec security associations are established during IKEv1 Phase 1 negotiations.
- D. IKEv1 security associations are established during IKEv1 Phase 1 negotiations.

Answer: ([SHOW ANSWER](#))

The correct answers are A and D. In IKEv1-based IPsec VPNs, there are two distinct negotiation phases.

IKEv1 Phase 1 establishes the secure and authenticated IKE channel between peers. That means the IKE SA is built during Phase 1. Juniper describes Phase 1 as the negotiation of proposals for how to authenticate and secure the channel, including encryption algorithms, authentication algorithms, Diffie-Hellman group, and authentication method.

IKEv1 Phase 2 then uses that secure channel to negotiate the IPsec SAs that protect actual user traffic through the VPN. Juniper states that Phase 2 negotiates security associations to secure the

data traversing the IPsec tunnel, and that the Phase 2 proposal includes the security protocol, such as ESP or AH, plus the selected encryption and authentication algorithms. Option B is wrong because IKEv1 SAs are not established in Phase

2; Phase 2 creates IPsec SAs. Option C is wrong because Phase 1 does not create the data-plane IPsec SA; it creates the secure IKE control channel used for Phase 2 negotiation.

Reference topics: IPsec VPN, IKEv1 Phase 1, IKE SA, IKEv1 Phase 2, IPsec SA, ESP/AH proposals.

NEW QUESTION: 26

Referring to the exhibit, what should you do to ensure that Juniper ATP Cloud detects malware in HTTPS traffic?



- A. Manually configure and apply an SSL proxy profile.
- B. Lower the threat score.
- C. Configure a new device profile that includes encrypted traffic.
- D. Change the action to redirect the encrypted traffic to a decryption device.

Answer: A ([LEAVE A REPLY](#))

The correct answer is A. Manually configure and apply an SSL proxy profile. HTTPS traffic is encrypted, so ATP Cloud cannot extract and submit downloaded files for malware analysis unless the SRX can decrypt the SSL/TLS session first. Juniper's ATP Cloud documentation states that to detect malware in HTTPS traffic, you must configure the SSL inspection CA used for SSL forward proxy, and the ATP Cloud policy workflow specifically includes configuring an SSL proxy profile to inspect HTTPS traffic. Juniper's example shows the SSL proxy profile being created with a root CA and then applied so HTTPS sessions can be inspected before advanced anti-malware processing occurs.

Option B is wrong because lowering the threat score only changes the enforcement threshold after a file verdict is returned; it does not solve the inability to inspect encrypted payloads. Option C is wrong because changing the ATP device profile alone does not decrypt HTTPS traffic. The exhibit already shows a malware profile and HTTP file-download configuration, but HTTPS malware detection still requires SSL proxy.

Option D is wrong because Junos ATP Cloud integration does not require redirecting encrypted traffic to a separate decryption appliance for this task. The SRX performs SSL forward proxy locally, then advanced anti-malware can inspect extracted content. Reference topics: ATP Cloud, HTTPS malware inspection, SSL forward proxy, SSL inspection CA, advanced anti-malware policy.

NEW QUESTION: 27

You are asked to ensure that traffic that matches an IDP policy is not impacted until administrators have a chance to evaluate it.

In this scenario, which IP action should be configured for the policy?

- A. ip-block
- B. ip-notify
- C. ip-connection-rate-limit
- D. ip-close

Answer: ([SHOW ANSWER](#))

The correct answer is B. ip-notify. When administrators want visibility without enforcement impact, ip-notify is the correct IP action. Juniper Security Director documentation defines IP Notify as an IP action that does not take any action against future traffic but logs the event. That is exactly the requirement in the question:

traffic matching the IDP condition must not be blocked, closed, or rate-limited until administrators have reviewed the events and decided whether enforcement is appropriate.

Option A, ip-block, is wrong because it blocks future packets matching the IP action rule. That would immediately impact traffic. Option C, ip-connection-rate-limit, is wrong because it limits the connection rate and therefore changes traffic behavior before administrators complete evaluation. Option D, ip-close, is also wrong because it closes matching future sessions by sending reset packets to the client and server, which is disruptive. In a safe evaluation or tuning phase, the proper approach is to log and observe first, then move to stronger actions such as block, close, or rate-limit only after the detected condition has been validated.

Reference topics: IDP IP actions, ip-notify, event logging, non-disruptive evaluation mode, IDP policy tuning.

NEW QUESTION: 28

Which two statements about proxy IDs are correct? (Choose two.)

- A. Proxy IDs cannot override default Junos behavior.
- B. By default, for a route-based IPsec VPN, a Junos security device sets the proxy ID to 0.0.0.0/0.
- C. Proxy IDs must match on both peers for a Phase 2 tunnel to establish.
- D. Proxy IDs are created during IKE Phase 1.

Answer: ([SHOW ANSWER](#))

The correct answers are B and C. In Junos route-based IPsec VPNs, the default proxy ID is broad: local 0.0.0.0

/0, remote 0.0.0.0/0, and service any. This default behavior allows routed traffic entering the secure tunnel interface to determine what is protected by the VPN rather than requiring a narrow policy-based encryption domain. Juniper's IPsec VPN configuration guidance also states that proxy IDs are used in Phase 2 negotiations, and that a proxy ID mismatch is one of the common causes of Phase 2 failure. For interoperability with some third-party VPN peers, Juniper notes that proxy IDs may need to be manually configured to match the peer.

Option A is wrong because proxy IDs can override default route-based behavior when manually configured, especially when a peer requires specific local and remote protected subnets. Option D is wrong because proxy IDs are not created during IKE Phase 1. Phase 1 builds the secure IKE channel; proxy IDs belong to Phase 2

/IPsec SA negotiation, where the peers agree on traffic selectors for encrypted traffic. Reference topics: IPsec VPN, route-based VPNs, proxy IDs, Phase 2 negotiation, traffic selectors, third-party VPN interoperability.

NEW QUESTION: 29

How does the SSL proxy service identify SSL traffic?

- A. by examining the URL
- B. by using AppID results
- C. by examining the destination port
- D. by reading the server certificate

Answer: (SHOW ANSWER)

The correct answer is B. by using AppID results. Junos SSL proxy does not identify SSL/TLS sessions by assuming that encrypted traffic always uses TCP/443. That would be technically weak because SSL/TLS can run on nonstandard ports, and non-SSL applications can also use common HTTPS ports. Juniper's SSL proxy documentation explains that SSL proxy works with application security services and that AppID is used in the encrypted-traffic inspection workflow. In earlier wording from Juniper AppSecure material, SSL proxy uses application identification services to determine whether a session is SSL encrypted; in current Junos documentation, SSL proxy and AppID are tightly linked so encrypted sessions can be identified, decrypted, inspected, and then re-encrypted for enforcement.

Option A is wrong because the URL is inside the HTTP payload, and in HTTPS much of the meaningful HTTP content is encrypted before SSL proxy inspection occurs. Option C is wrong because destination port is only a rough hint, not a reliable detection method. Option D is wrong because certificates are used in the SSL

/TLS handshake and proxy trust model, but the service's traffic classification relies on AppID results, not merely reading the server certificate. Reference topics: SSL Proxy, AppID, encrypted session detection, SSL

/TLS inspection, application security services.

NEW QUESTION: 30

Your manager asks you to update your SRX Series device's IDP security package. You perform the required steps; however, when you attempt to install the package, you receive an error.

```
user@srx> request security idp security-package install
error: Security Package installation disabled temporarily due to invalid license.
```

Referring to the exhibit, which two statements are correct about this error? (Choose two.)

- A. IDP stops inspecting traffic.
- B. The IDP license has expired.
- C. IDP continues to inspect traffic only using the installed signatures.
- D. The IDP license is missing/not installed.

Answer: (SHOW ANSWER)

The correct answers are B and C. The exhibit shows the command `request security idp security-package install` failing with: "Security package installation disabled temporarily due to invalid license." In the IDP update workflow, the SRX must have a valid IDP/AppSecure-related license to install updated security packages. Juniper's support guidance for an expired IDP license states that if the IDP license expires, attacks continue to be inspected, but IDP update installation is not allowed. That maps directly to this exhibit: the existing IDP engine and currently installed attack database can continue to inspect traffic, but the device cannot install the newer downloaded package until licensing is corrected.

Option A is wrong because expiration does not immediately stop all IDP inspection; it prevents installing new updates. Option D is not the best answer because the specific operational behavior shown is consistent with an invalid/expired license condition after attempting a package install, not proof that no license was ever installed. The practical remediation is to validate the installed license, renew or reinstall the correct IDP license, then retry the security-package installation. Reference topics: IDP licensing, security-package download/install, attack database updates, installed signature inspection behavior.

Valid JN0-336 Dumps shared by EduDump.com for Helping Passing JN0-336 Exam!

EduDump.com now offer the **newest JN0-336 exam dumps**, the EduDump.com JN0-336 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com JN0-336 dumps with Test Engine here:

<https://www.edudump.com/exams/Juniper/JN0-336/premium/> (70 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)