Vendor: Juniper

Exam Code: JN0-335

Exam Name: Security, Specialist (JNCIS-SEC)

Version: DEMO

QUESTION 1
Which two statements are true about the vSRX? (Choose two.)

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

Answer: BD
Explanation:
The vSRX is a virtual security appliance that runs on a virtual machine. It provides firewall, VPN, and other security services in a virtualized environment.
The vSRX is based on a version of Junos OS that is optimized for virtualization. It runs on a Linux kernel and uses a KVM hypervisor. It supports VMware ESXi and KVM hypervisors. The vSRX has support for VMXNET3 vNICs, which are high-performance virtual network interfaces provided by VMware. These interfaces can provide higher throughput and lower CPU utilization than other virtual NIC types.

QUESTION 2
Which three statements are correct about fabric interfaces on the SRX5800? (Choose three.)

A. Fabric interfaces must be user-assigned interfaces.
B. Fabric interfaces must have a user-assigned IP address.
C. Fabric interfaces must be same interface type.
D. Fabric interfaces must be on the same Layer 2 segment.
E. Fabric interfaces must be system-assigned interfaces.

Answer: CDE
Explanation:
https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-chassis-cluster-data-plane-interfaces.html

QUESTION 3
You are deploying a new SRX Series device and you need to log denied traffic. In this scenario, which two policy parameters are required to accomplish this task? (Choose two.)

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

Answer: BC
Explanation:
https://supportportal.juniper.net/s/article/SRX-How-to-log-traffic-for-the-default-deny-policy?language=en_US

QUESTION 4
You are asked to reduce the load that the JIMS server places on your Which action should you take in this situation?

A. Connect JIMS to the RADIUS server

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

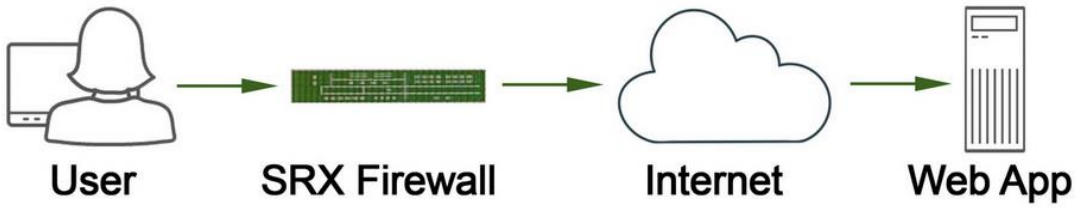
Answer: A
Explanation:
Connect JIMS to the RADIUS server: RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. By connecting JIMS to a RADIUS server, authentication requests can be offloaded from the domain controller to the RADIUS server. This reduces the load on the domain controller because the RADIUS server can handle a portion of the authentication and authorization tasks.

QUESTION 5
Which two statements about unified security policies are correct? (Choose two.)

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

Answer: CD
Explanation:
Unified security policies are security policies that enable you to use dynamic applications as match conditions along with existing 5-tuple or 6-tuple matching conditions. They simplify application-based security policy management at Layer 7 and provide greater control and extensibility to manage dynamic applications traffic.

QUESTION 6
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: AB

QUESTION 7
You have deployed an SRX300 Series device and determined that files have stopped being scanned.
In this scenario, what is a reason for this problem?

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

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

QUESTION 8
Which three statements about SRX Series device chassis clusters are true? (Choose three.)

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

Answer: BCE
Explanation:
1. Chassis cluster member devices synchronize configuration using the control link: This statement is correct because the control link is used for configuration synchronization among other functions.
2. A control link failure causes the secondary cluster node to be disabled: This statement is correct because a control link failure causes the secondary node to become ineligible for primary role and remain in secondary role until the control link is restored.
3. Heartbeat messages verify that the chassis cluster control link is working: This statement is correct because heartbeat messages are sent periodically over the control link to monitor its status.

QUESTION 9
Which two statements are correct about security policy changes when using the policy rematch feature? (Choose two.)

A. When a policy change includes changing the policy's action from permit to deny, all existing sessions are maintained
B. When a policy change includes changing the policy's source or destination address match condition, all existing sessions are dropped.
C. When a policy change includes changing the policy's action from permit to deny, all existing sessions are dropped.
D. When a policy change includes changing the policy's source or destination address match condition, all existing sessions are reevaluated.

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

deactivated, or deleted.

QUESTION 11
You are asked to block malicious applications regardless of the port number being used. In this scenario, which two application security features should be used? (Choose two.)

A. AppFW
B. AppQoE
C. APPID
D. AppTrack

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

QUESTION 11
A client has attempted communication with a known command-and-control server and it has reached the configured threat level threshold.
Which feed will the clients IP address be automatically added to in this situation?

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

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

QUESTION 12
When a security policy is deleted, which statement is correct about the default behavior of active sessions allowed by that policy?

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

Answer: A
Explanation:
When a security policy is deleted, the active sessions allowed by the policy will be dropped. The default behavior is that all active sessions allowed by the policy will be terminated and the traffic will no longer be forwarded. There is no way to mark the active sessions as a legacy flow or to

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

QUESTION 13
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: A
Explanation:
AppTrack: Tracks and reports applications passing through the device.
- Intrusion Detection and Prevention (IDP): Applies appropriate attack objects to applications running on nonstandard ports. Application identification improves IDP performance by narrowing the scope of attack signatures for applications without decoders.
- AppFW: Implements an application firewall using application-based rules.
- AppQoS: Provides quality-of-service (QoS) prioritization based on application awareness

QUESTION 14
Which two statements are correct about the configuration shown in the exhibit? (Choose two.)

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

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

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

QUESTION 15
When trying to set up a server protection SSL proxy, you receive the error shown. What are two reasons for this error? (Choose two.)

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

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

Answer: AD
Explanation:
Two possible reasons for this error are that the SSL proxy certificate ID does not exist, or the SSL proxy certificate ID is part of a blocklist. If the SSL proxy certificate ID does not exist, you will need to generate a new certificate. If the SSL proxy certificate ID is part of a blocklist, you will need to contact the source of the blocklist to remove it. Additionally, you may need to check that the SSL proxy certificate ID has the correct renegotiation option set, as this is necessary for proper server protection.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**