

Practice Exam Questions

JUNIPER
NETWORKS



JN0-335

Security, Specialist (JNCIS-SEC)



EXAMKILLER

Help Pass Your Exam At First Try

Juniper

Exam JN0-335

Security, Specialist (JNCIS-SEC)

Version: 3.0

[Total Questions: 65]

Question No : 1

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: B,C

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

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

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

Question No : 2

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

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

Answer: D

Explanation: JIMS server is a Juniper Identity Management Service that collects user identity information from different authentication sources for SRX Series devices¹². It can connect to SRX Series devices and CSO platform in your network¹.

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

reduce network traffic.

Question No : 3

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

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

Answer: B,C

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

Question No : 4

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

Which step is necessary to accomplish this task?

- A. Issue the set chassis cluster disable reboot command on the primary node.
- B. Implement the control link recover/ solution before adjusting the priorities.
- C. Manually request the failover and identify the secondary node
- D. Adjust the priority in the configuration on the secondary node.

Answer: A

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

Question No : 5

Which two statements are correct about SSL proxy server protection? (Choose two.)

- A. You do not need to configure the servers to use the SSL proxy the function on the SRX Series device.
- B. You must load the server certificates on the SRX Series device.
- C. The servers must be configured to use the SSL proxy function on the SRX Series device.
- D. You must import the root CA on the servers.

Answer: B,C

Explanation: You must load the server certificates on the SRX Series device and configure the servers to use the SSL proxy function on the SRX Series device. This is done to ensure that the SSL proxy is able to decrypt the traffic between the client and server. Additionally, you must import the root CA on the servers in order for the SSL proxy to properly validate the server certificate.

Question No : 6

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

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

Answer: C,D

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

Question No : 7

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: A,C

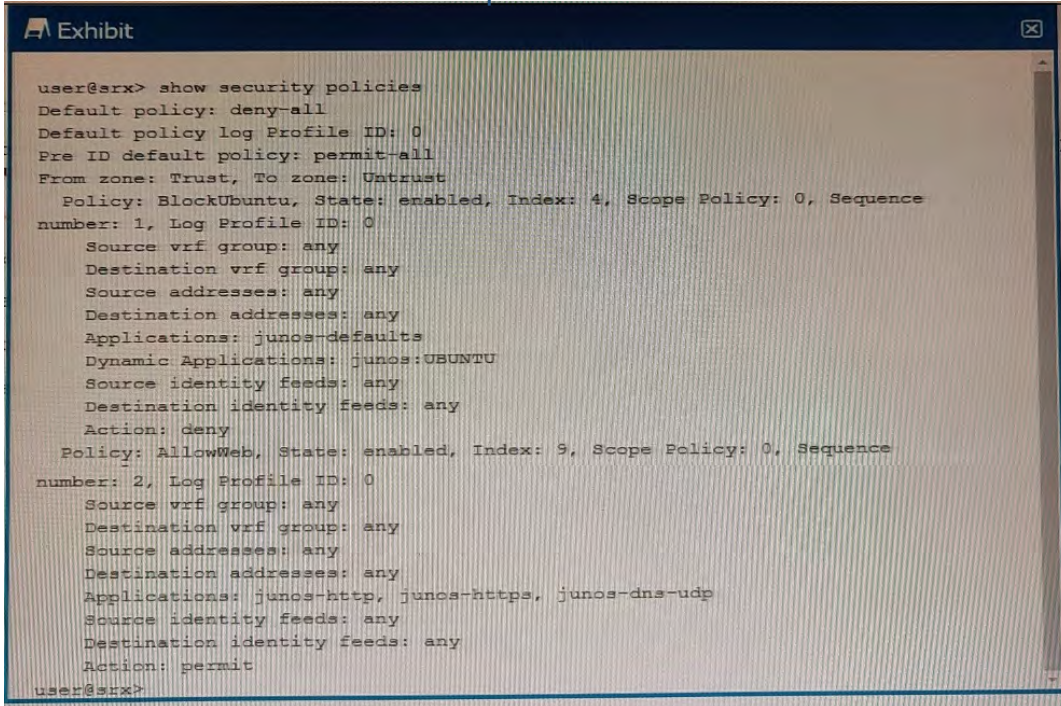
Explanation:

- ✍ Scalability: vSRX instances can be easily added or removed as the needs of the network change, making it a flexible option for scaling in a software-defined network.
- ✍ Granular Security: vSRX allows for granular security policies to be enforced at the virtual interface level, making it an effective solution for securing traffic in a software-defined network.

The two benefits of using a vSRX in a software-defined network are scalability and granular security. Scalability allows you to increase the number of resources available to meet the demands of network traffic, while granular security provides a level of control and flexibility to your network security that is not possible with a traditional firewall. With a vSRX, you can create multiple levels of security policies, rules, and access control lists to ensure that only authorized traffic can enter and exit your network. Additionally, you would not require a software license to use the vSRX, making it an economical solution for those looking for increased security and flexibility.

Question No : 8

Exhibit



```

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

```

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

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

- A. Move the Blockubuntu policy after the Allowweb policy.
- B. Configure the Blockubuntu policy with the junos-https application parameter.
- C. Change the default policy to permit-all.
- D. Configure the Allowweb policy to have a dynamic application of any.

Answer: B

Question No : 9

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: A,B

Explanation: The two security policy features that provide the capability to permit access to an application but block its sub-applications are URL filtering and micro application

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

Question No : 10

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

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

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 No : 11

Exhibit


```

Exhibit
{primary:node0}
user@srx> show chassis cluster status
Cluster ID: 3
Node
Redundancy group: 0 , Failover count: 1
node0
node1
Redundancy group: 1 , Failover count: 3
node0
node1

```

| Node | Priority | Status | Preempt | Manual failover |
|-------|----------|-----------|---------|-----------------|
| node0 | 129 | primary | no | no |
| node1 | 128 | secondary | no | no |
| node0 | 0 | primary | no | no |
| node1 | 0 | secondary | no | no |

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

- A. Redundancy group 1 is in an ineligible state.
- B. Node1 is the active node for the control plane
- C. There are no issues with the cluster.
- D. Redundancy group 0 is in an ineligible state.

Answer: A

Question No : 12

You enable chassis clustering on two devices and assign a cluster ID and a node ID to each device.

In this scenario, what is the correct order for rebooting the devices?

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

Answer: C

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

devices must be rebooted to ensure the proper configuration is applied.

Question No : 13

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

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

Answer: B,D

Explanation: The two types of system logs that Junos generates are control plane logs and data plane logs. Control plane logs are generated by the Junos operating system and contain system-level events such as system startup and shutdown, configuration changes, and system alarms. Data plane logs are generated by the network protocol processes and contain messages about the status of the network and its components, such as routing, firewall, NAT, and IPS. SQL log files and system core dump files are not types of system logs generated by Junos.

Question No : 14

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

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

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

Answer: A,C

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