DUMPSARENA

Security, Specialist (JNCIS-SEC)

Juniper JN0-336

Version Demo

Total Demo Questions: 8

Total Premium Questions: 81

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Security Concepts	20
Topic 2, Security Policies	27
Topic 3, IPsec VPNs	12
Topic 4, Security Platforms	22
Total	81

QUESTION NO: 1

Which two statements are correct about IDP policy templates? (Choose two.)

A. They are provided by Juniper Networks.

B. They are not customizable.

C. They are available on a “factory-default config.”

D. They must be installed.

ANSWER: A D

Explanation:

IDP policy templates are predefined policy sets supplied by Juniper Networks to streamline the initial deployment of intrusion detection and prevention protection on SRX Series devices. They provide a practical starting point for common deployment roles and services, such as client protection, server protection, Web server protection, DNS server protection, file server protection, and DMZ services. Because the templates are Juniper-provided baseline policies, administrators can select an appropriate starting point and then adapt it to the organization’s traffic patterns, hosted services, and security requirements. Juniper documents that these predefined templates are obtained as part of the IDP security package content rather than being immediately usable policy configuration in a default device setup. To make the templates available for configuration and use, the administrator downloads the IDP policy-template package and installs it on the device. After installation, the templates can be viewed, copied, customized, and applied through the IDP policy configuration hierarchy. This installation step ensures that the device has the relevant template content before an administrator activates an IDP policy for traffic inspection. See Juniper’s IDP policy templates overview and template installation documentation.

QUESTION NO: 2

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: A

Explanation:

“It supports a maximum of two domains.” is correct for the SRX Series integrated user firewall implementation that uses Microsoft Active Directory as its identity source. The identity-aware firewall correlates authenticated user identities with source IP addresses, enabling policies to match directory users and groups rather than relying only on network addresses. For this integrated Active Directory configuration, Juniper documents a scale limit of two configured domains. This is a platform implementation limit for the identity-source feature, rather than a general limit inherent to Microsoft Active Directory itself.

When configuring the identity source, the administrator supplies domain information and domain-controller connection details so the firewall can collect logon information and obtain directory user and group data. Juniper’s user-firewall documentation describes the Active Directory identity-source workflow and its supported configuration limits, including the domain limit. This capacity guidance is important when planning identity-aware policy deployments across multiple Windows domains: environments requiring identities from more domains must use an architecture or identity integration method that accommodates that scale.

See Juniper’s User Firewall documentation and the Active Directory authentication-source configuration procedure for the integrated user-firewall configuration model and limits.

QUESTION NO: 3

An IPsec VPN peer successfully establishes an IKEv2 SA, but no CHILD_SA is created. The IKE log reports that no matching IPsec proposal was found.

Which configuration area should you examine first?

A. The IKE proposal

B. The IPsec proposal

C. The Dead Peer Detection settings

D. The external interface address

ANSWER: B

Explanation:

You should examine the **IPsec proposal**. An IKEv2 IKE_SA can be established successfully even when the peers cannot agree on the parameters for the CHILD_SA that protects user traffic. The IPsec proposals must have compatible settings, such as the ESP encryption and authentication algorithms, for the IPsec SA negotiation to succeed.

The IKE proposal affects IKE_SA establishment, which has already succeeded. Dead Peer Detection and the external interface configuration can affect tunnel availability, but they do not cause a no-matching-IPsec-proposal error during CHILD_SA negotiation.

QUESTION NO: 4

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

```
{primary:node0}
user@srx> show chassis cluster statistics
Control link statistics:
    Control link 0:
        Heartbeat packets sent: 332
        Heartbeat packets received: 347
        Heartbeat packet errors: 0
Fabric link statistics:
    Child link 0
        Probes sent: 337
        Probes received: 339
    Child link 1
        Probes sent: 0
        Probes received: 0
Services Synchronized:
    Service name                    RTOs sent       RTOs received
    Translation context             0               0
    Incoming NAT                    0               0
    Resource manager                0               0
    DS-LITE create                  0               0
    Session create                  0               0
    IPv6 session create             0               0
    Session close                   0               0
    ...
```

A. Fabric link 0 is working.

B. The control link is working.

C. Fabric link 1 is failing.

D. The control link is failing.

ANSWER: A B

Explanation:

Fabric link 0 is working because its fabric-link statistics show probe packets being transmitted and received. In an SRX chassis cluster, the fabric link carries data-plane traffic between nodes, and the cluster maintains probe counters to monitor the operational state of each fabric child link. Incrementing sent and received probe values demonstrate bidirectional fabric-link monitoring activity for fabric link 0.

The control link is working because the control-link statistics show heartbeat packets sent and received with no heartbeat packet errors. The control link is the cluster's control-plane communications path and is used for heartbeat and state-related coordination between the nodes. Successful bidirectional heartbeats, together with an error count of zero, provide the expected evidence that this link is operational at the time the command output was collected. Junos exposes these counters through the chassis-cluster statistics output specifically to help validate control-link and fabric-link health. See the Juniper show chassis cluster statistics command reference and the SRX chassis cluster overview.

QUESTION NO: 5

Which three different objects would be created, modified, cloned, and deleted in the Shared Objects workspace of Junos Space Security Director? (Choose three.)

A. geo IP

B. IP address

C. audit logs

D. policy enforcement groups

E. policy rules

ANSWER: A B D

Explanation:

The Shared Objects workspace in Junos Space Security Director is intended for defining reusable configuration elements that can be referenced throughout security-policy configuration. **geo IP** belongs in this workspace because geographic IP data can be used to define location-based matches for security policies. Managing it centrally lets administrators consistently use geographic regions or countries wherever that match criterion is required.

IP address is also a Shared Objects item because Security Director uses address objects to represent individual hosts, networks, ranges, or related address definitions. These reusable address definitions can then be selected in policy source and destination fields instead of repeatedly entering raw IP information. Central object management makes updates available wherever the object is referenced.

policy enforcement groups are shared definitions used to organize endpoints or other enforcement targets for policy-enforcement workflows. Creating, modifying, cloning, and deleting these groups from a common workspace supports consistent application across the managed environment. The shared-object model is specifically designed to centralize such reusable definitions rather than tying them to one individual policy instance.

Juniper Security Director documentation is available from the Security Director documentation portal, and Juniper's product documentation index provides additional release-specific Security Director references at Juniper Documentation.

QUESTION NO: 6

An administrator inserts a new deny policy above an existing permit policy on an SRX Series device. New connections are denied as expected, but several connections established before the policy change continue to pass traffic.

What should the administrator do to apply the new policy to those existing connections?

A. Clear the existing sessions.

B. Enable policy hit counting.

C. Configure session-close logging.

D. Move the deny policy below the permit policy.

ANSWER: A

Explanation:

The administrator should **clear the existing sessions**. SRX Series devices are stateful firewalls and make the security-policy decision when the first packet of a new session is processed. Subsequent packets belonging to that established session are matched against the session table and do not undergo a new security-policy lookup for every packet.

Committing the new policy correctly affects new sessions, which explains why newly initiated connections are denied. Moving the policy to another position or enabling policy hit counting does not re-evaluate sessions that are already established. Clearing the relevant sessions forces subsequent traffic to create new sessions and undergo policy evaluation against the updated rule set.

QUESTION NO: 7

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: C D

Explanation:

The cSRX supports firewall, NAT, IPS, and UTM services because it delivers the SRX security feature set in a containerized form factor for virtualized and cloud-native environments. This allows security policy enforcement to be deployed close to containerized workloads while retaining core next-generation firewall functions. Juniper documents cSRX support for stateful firewall policies and NAT, as well as advanced security capabilities that include intrusion prevention and content-security services. Consequently, cSRX can provide meaningful traffic inspection and threat-prevention controls rather than functioning only as a lightweight packet-forwarding container.

The cSRX has low memory requirements because it is specifically designed for high-density deployments in which a full virtual-machine firewall would consume unnecessary compute and memory resources. A container-based architecture reduces per-instance overhead and enables faster instantiation, making cSRX suitable for elastic environments where security instances may be created or removed alongside application workloads. Its small footprint is therefore a practical deployment benefit, particularly when many isolated workloads require firewall enforcement on shared infrastructure. Juniper describes cSRX as a containerized firewall for cloud environments and documents its resource-oriented deployment characteristics in its cSRX documentation. See Juniper's cSRX overview and the cSRX features documentation.

QUESTION NO: 8

What is a function of the Juniper Identity Management Service?

A. encrypting user e-mail

B. logging malicious code sent through ingress and egress ports

C. encrypting network data traffic

D. maintaining a centralized authentication table

ANSWER: D

Explanation:

Juniper Identity Management Service (JIMS) is used to supply identity information to SRX Series firewalls for identity-aware policy enforcement. Its key function is maintaining a centralized authentication table: JIMS collects user-to-IP address mappings and associated group membership from supported identity sources, including Microsoft Active Directory environments and domain controllers. It then distributes this information to SRX devices so that firewall policies can use authenticated usernames and directory groups as match criteria rather than relying solely on IP addresses.

This centralized model is particularly useful where users receive dynamic addresses or move between network locations. Once JIMS has correlated an IP address with a user and that user's group relationships, the SRX firewall can apply the appropriate access policy based on organizational identity. The authentication entries held and shared by JIMS provide the identity context required for user-based and group-based security controls. This makes JIMS an identity-information collection and distribution component for the Identity-Aware Firewall feature. Juniper's documentation describes JIMS as collecting and distributing user identity information, while identity-aware policies use authenticated user and group data to control traffic. See the JIMS Overview and Juniper's Identity-Aware Security Policies documentation.