

# JN0-636<sup>Q&As</sup>

Service Provider Routing and Switching Professional (JNCIP-SP)

## Pass Juniper JN0-636 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/jn0-636.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Juniper  
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

Exhibit

```
user@host> show security mka sessions summary
Interface  Member-ID          Type Status Tx Rx CAK Name
ge-0/0/1   E752CAFAE8DDFB82D4EA4BF7
           8951              8888      preceding live 8887
ge-0/0/1   0F2D5171F38EAB16C2E0CB62
           8952              FFFF      fallback active 8959
ge-0/0/1   6B49BD5CF7188F3CD9A29D30
           AAAA              primary in-progress 2439 0
```

Referring to the exhibit, which two statements are true about the CAK status for the CAK named "FFFF"? (Choose two.)

- A. CAK is not used for encryption and decryption of the MACsec session.
- B. SAK is successfully generated using this key.
- C. CAK is used for encryption and decryption of the MACsec session.
- D. SAK is not generated using this key.

Correct Answer: CD

---

**QUESTION 2**

Your company uses non-Juniper firewalls and you are asked to provide a Juniper solution for zero-day malware protection. Which solution would work in this scenario?

- A. Juniper ATP Cloud
- B. Juniper Secure Analytics
- C. Juniper ATP Appliance
- D. Juniper Security Director

Correct Answer: A

Explanation: Juniper ATP Cloud provides zero-day malware protection for non-Juniper firewalls. It's a cloud-based service that analyzes files and network traffic to detect and prevent known and unknown (zero-day) threats. It uses a combination of static and dynamic analysis techniques, as well as machine learning, to detect and block malicious files, even if they are not known to traditional anti-virus software. It also provides real-time visibility and detailed forensics for incident response and remediation.

---

**QUESTION 3**

You issue the command shown in the exhibit.

Which policy will be active for the identified traffic?

- A. Policy p4
- B. Policy p7
- C. Policy p1
- D. Policy p12

Correct Answer: B

---

#### QUESTION 4

Exhibit You have recently configured Adaptive Threat Profiling and notice 20 IP address entries in the monitoring section of the Juniper ATP Cloud portal that do not match the number of entries locally on the SRX Series device, as shown in the exhibit.

```
user@SRX> show service security-intelligence category summary
Category name      :SecProfiling
Status             :Enable
Description        :Security Profiling Data
Update interval   :300s
TTL                :172800s
Feed name          :Proxy_Nodes
Version            :20220812.1
Objects number     :80
Create time        :2022-08-14 11:53:46 UTC
Update time        :2022-08-15 06:11:11 UTC
Update status      :Store succeeded
Expired            :No
Status             :Active
Options            :N/A
user@SRX> show security dynamic-address category-name SecProfiling feed-name
Proxy_Nodes
user@SRX>
```

What is the correct action to solve this problem on the SRX device?

- A. You must configure the DAE in a security policy on the SRX device.
- B. Refresh the feed in ATP Cloud.
- C. Force a manual download of the Proxy\_\_Nodes feed.
- D. Flush the DNS cache on the SRX device.

Correct Answer: C

---

**QUESTION 5**

The monitor traffic interface command is being used to capture the packets destined to and the from the SRX Series device. In this scenario, which two statements related to the feature are true? (Choose two.)

- A. This feature does not capture transit traffic.
- B. This feature captures ICMP traffic to and from the SRX Series device.
- C. This feature is supported on high-end SRX Series devices only.
- D. This feature is supported on both branch and high-end SRX Series devices.

Correct Answer: AD

Explanation: <https://forums.juniper.net/t5/Ethernet-Switching/monitor-traffic-interface/td-p/462528>

---

**QUESTION 6**

You configured a chassis cluster for high availability on an SRX Series device and enrolled this HA cluster with the Juniper ATP Cloud. Which two statements are correct in this scenario? (Choose two.)

- A. You must use different license keys on both cluster nodes.
- B. When enrolling your devices, you only need to enroll one node.
- C. You must set up your HA cluster after enrolling your devices with Juniper ATP Cloud
- D. You must use the same license key on both cluster nodes.

Correct Answer: BD

When enrolling your devices, you only need to enroll one node: The Juniper ATP Cloud automatically recognizes the HA configuration and applies the same license and configuration to both nodes of the cluster.

You must use the same license key on both cluster nodes: The HA cluster needs to share the same license key in order to be recognized as a single device by the Juniper ATP Cloud.

You must set up your HA cluster before enrolling your devices with Juniper ATP Cloud. And it is not necessary to use different license keys on both cluster nodes because the HA cluster shares the same license key.

---

**QUESTION 7**

You must implement an IPsec VPN on an SRX Series device using PKI certificates for authentication. As part of the implementation, you are required to ensure that the certificate submission, renewal, and retrieval processes are handled

automatically from the certificate authority.

In this scenario, which statement is correct.

- A. You can use CRL to accomplish this behavior.

- B. You can use SCEP to accomplish this behavior.
- C. You can use OCSP to accomplish this behavior.
- D. You can use SPKI to accomplish this behavior.

Correct Answer: B

Certificate Renewal The renewal of certificates is much the same as initial certificate enrollment except you are just replacing an old certificate (about to expire) on the VPN device with a new certificate. As with the initial certificate request, only

manual renewal is supported. SCEP can be used to re-enroll local certificates automatically before they expire. Refer to Appendix D for more details.

## QUESTION 8

Exhibit

```
Aug 1 11:28:23 11:28:23.434801:CID-0:THREAD_ID-01:RT:<172.20.101.10/59009->
>10.0.1.129/22;6,0x0> matched filter TestFilter:
Aug 1 11:28:23 11:28:23.434805:CID-0:THREAD_ID-01:RT:packet [64] ipid = 36644,
@0xef3edece
Aug 1 11:28:23 11:28:23.434810:CID-0:THREAD_ID-01:RT:---- flow_process_pkt:
(thd 1): flow_ctxt type 15, common flag 0x0, mbuf 0x6918b800, rtbl_idx = 0
Aug 1 11:28:23 11:28:23.434817:CID-0:THREAD_ID-01:RT:ge-0/0/4.0:
172.20.101.10/59009->10.0.1.129/22, tcp, flag 2 syn
Aug 1 11:28:23 11:28:23.434819:CID-0:THREAD_ID-01:RT:find flow: table
0x206a60a0, hash 43106(0xffff), sa 172.20.101.10, da 10.0.1.129, sp 59009, dp
22, proto 6, tok 9, conn-tag 0x00000000
Aug 1 11:28:23 11:28:23.434822:CID-0:THREAD_ID-01:RT:no session found, start
first path. in_tunnel - 0x0, from_cp_flag - 0
Aug 1 11:28:23 11:28:23.434826:CID-0:THREAD_ID-01:RT:flow_first_create_session
Aug 1 11:28:23 11:28:23.434834:CID-0:THREAD_ID-01:RT:flow_first_in_dst_nat: in
<ge-0/0/4.0>, out <N/A> dst_adr 10.0.1.129, sp 59009, dp 22
Aug 1 11:28:23 11:28:23.434835:CID-0:THREAD_ID-01:RT:chose interface ge-0/0/4.0
as incoming nat if.
Aug 1 11:28:23 11:28:23.434838:CID-0:THREAD_ID-01:RT:flow_first_rule_dst_xlate:
DST no-xlate: 0.0.0.0(0) to 10.0.1.129(22)
```

The exhibit shows a snippet of a security flow trace.

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

- A. This packet arrived on interface ge-0/0/4.0.
- B. Destination NAT occurs.
- C. The capture is a packet from the source address 172.20.101.10 destined to 10.0.1.129.
- D. An existing session is found in the table.

Correct Answer: CD

**QUESTION 9**

You are asked to allocate security profile resources to the interconnect logical system for it to work properly. In this scenario, which statement is correct?

- A. The NAT resources must be defined in the security profile for the interconnect logical system.
- B. No resources are needed to be allocated to the interconnect logical system.
- C. The resources must be calculated based on the amount of traffic that will flow between the logical systems.
- D. The flow-session resource must be defined in the security profile for the interconnect logical system.

Correct Answer: D

Explanation: The flow-session resource is needed in order to ensure adequate and secure communication between the two logical systems.

---

**QUESTION 10**

You are configuring transparent mode on an SRX Series device. You must permit IP-based traffic only, and BPDUs must be restricted to the VLANs from which they originate.

Which configuration accomplishes these objectives?

- A. 

```
bridge {  
  block-non-ip-all;  
  bypass-non-ip-unicast;  
  no-packet-flooding;  
}
```
- B. 

```
bridge {  
  block-non-ip-all;  
  bypass-non-ip-unicast;  
  bpdu-vlan-flooding;  
}
```
- C. 

```
bridge {  
  bypass-non-ip-unicast;  
  bpdu-vlan-flooding;  
}
```
- D. 

```
bridge {  
  block-non-ip-all;  
  bpdu-vlan-flooding;  
}
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: D

[https://www.juniper.net/documentation/us/en/software/junos/multicast-l2/topics/ref/statement/family-ethernet-switching-edit-interfaces-qfx-series.html#statement-name-statement\\_\\_d26608e73](https://www.juniper.net/documentation/us/en/software/junos/multicast-l2/topics/ref/statement/family-ethernet-switching-edit-interfaces-qfx-series.html#statement-name-statement__d26608e73)

---

## QUESTION 11

Exhibit

```
May 23 05:20:34 Vendor-Id: 0 Attribute Type:Reply-Message(18) Value:string-type
Length:36
May 23 05:20:34 authd_radius_parse_message:generic-type:18
May 23 05:20:34 Vendor-Id: 0 Attribute Type:Reply-Message(18) Value:string-type
Length:15
May 23 05:20:34 authd_radius_parse_message:generic-type:18
May 23 05:20:34 Framework - module(radius) return: FAILURE
```

You configure a traceoptions file called radius on your returns the output shown in the exhibit What is the source of the problem?

- A. An incorrect password is being used.
- B. The authentication order is misconfigured.
- C. The RADIUS server IP address is unreachable.
- D. The RADIUS server suffered a hardware failure.

Correct Answer: D

---

#### QUESTION 12

Exhibit Referring to the exhibit, which three statements are true? (Choose three.)



```

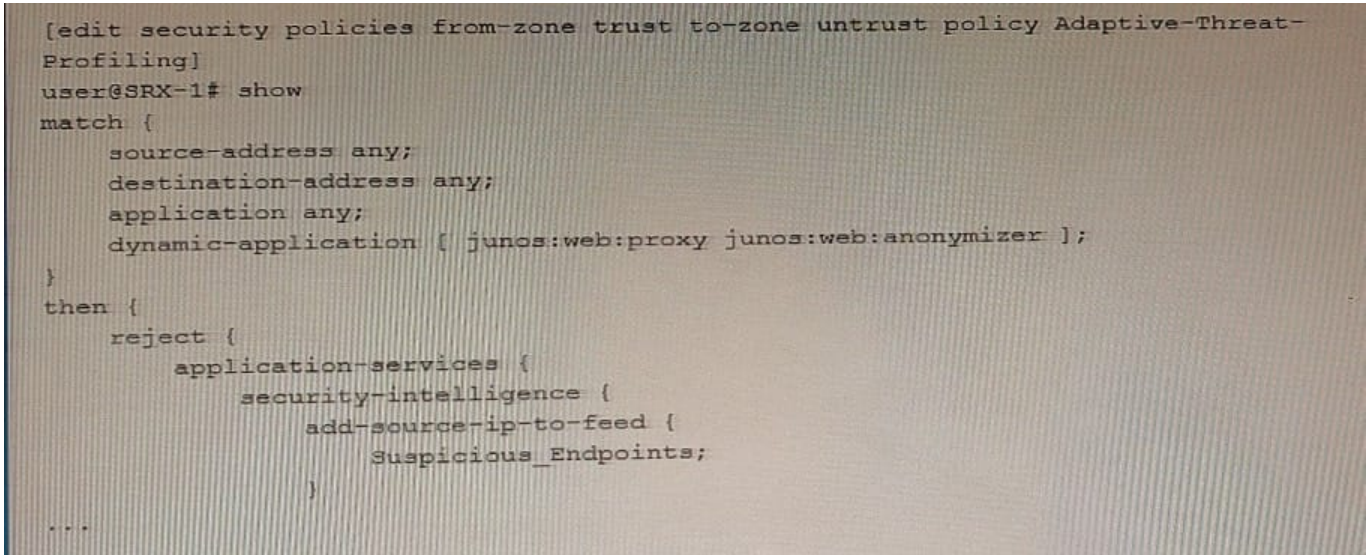
user@srx> show log flow-log
Apr 13 17:46:17 17:46:17.316930:CID-0:THREAD_ID-01:RT:<10.10.101.10/65131-
>10.10.102.1/22;6,0x0> matched filter F1:
Apr 13 17:46:17 17:46:17.317009:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.1) from trust (ge-0/0/4.0 in 0) to ge-0/0/5.0, Next-hop: 10.10.102.1
Apr 13 17:46:17 17:46:17.317016:CID-0:THREAD_ID-
01:RT:flow_first_policy_search: policy search from zone trust-> zone dmz
(0x0,0xfe6b0016,0x16)
Apr 13 17:46:17 17:46:17.317019:CID-0:THREAD_ID-01:RT:Policy lkup: vsys 0
zone(8:trust) -> zone(9:dmz) scope:0
Apr 13 17:46:17 17:46:17.317020:CID-0:THREAD_ID-01:RT: 10.10.101.10/65131 ->
10.10.102.1/22 proto 6
Apr 13 17:46:17 17:46:17.317031:CID-0:THREAD_ID-01:RT: permitted by policy
trust-to-dmz(8)
Apr 13 17:46:17 17:46:17.317031:CID-0:THREAD_ID-01:RT: packet passed,
Permitted by policy.
Apr 13 17:46:17 17:46:17.317038:CID-0:THREAD_ID-01:RT: choose interface ge-
0/0/5.0(P2P) as outgoing phy if
Apr 13 17:46:17 17:46:17.317042:CID-0:THREAD_ID-01:RT:is_loop_pak: Found loop
on ifp ge-0/0/5.0, addr: 10.10.102.1, rtt_idx: 0 addr_type:0x3.
Apr 13 17:46:17 17:46:17.317044:CID-0:THREAD_ID-
01:RT:flow_first_loopback_check: Setting interface: ge-0/0/5.0 as loop ifp.
Apr 13 17:46:17 17:46:17.317213:CID-0:THREAD_ID-01:RT:
flow_first_create_session
Apr 13 17:46:17 17:46:17.317215:CID-0:THREAD_ID-01:RT: flow_first_in_dst_nat:
0/0/5.0 as incoming nat if.
call flow_route_lookup(): src_ip 10.10.101.10, x_dst_ip 10.10.102.1, in ifp
ge-0/0/5.0, out ifp N/A sp 65131, dp 22, ip_proto 6, tos 0
Apr 13 17:46:17 17:46:17.317227:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.1) from dmz (ge-0/0/5.0 in 0) to .local..0, Next-hop: 10.10.102.1
Apr 13 17:46:17 17:46:17.317228:CID-0:THREAD_ID-
01:RT:flow_first_policy_search: policy search from zone dmz-> zone junos-host
(0x0,0xfe6b0016,0x16)
Apr 13 17:46:17 17:46:17.317230:CID-0:THREAD_ID-01:RT:Policy lkup: vsys 0
zone(9:dmz) -> zone(2:junos-host) scope:0
Apr 13 17:46:17 17:46:17.317230:CID-0:THREAD_ID-01:RT: 10.10.101.10/65131 ->
10.10.102.1/22 proto 6
Apr 13 17:46:17 17:46:17.317236:CID-0:THREAD_ID-01:RT: packet dropped, denied
by policy
Apr 13 17:46:17 17:46:17.317237:CID-0:THREAD_ID-01:RT: denied by policy deny-
ssh(9), dropping pkt
Apr 13 17:46:17 17:46:17.317237:CID-0:THREAD_ID-01:RT: packet dropped, policy
deny.
    
```

- A. The packet's destination is to an interface on the SRX Series device.
- B. The packet's destination is to a server in the DMZ zone.
- C. The packet originated within the Trust zone.
- D. The packet is dropped before making an SSH connection.
- E. The packet is allowed to make an SSH connection.

Correct Answer: ACD

**QUESTION 13**

Exhibit



```
[edit security policies from-zone trust to-zone untrust policy Adaptive-Threat-Profiling]
user@SRX-1# show
match {
    source-address any;
    destination-address any;
    application any;
    dynamic-application [ junos:web:proxy junos:web:anonymizer ];
}
then {
    reject {
        application-services {
            security-intelligence {
                add-source-ip-to-feed {
                    Suspicious_Endpoints;
                }
            }
        }
    }
}
...
```

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

- A. The `Suspicious_Endpoint` feed is only usable by the SRX-1 device.
- B. You must manually create the `Suspicious_Endpoint` feed in the Juniper ATP Cloud interface.
- C. The `Suspiciou3_Endpoint` feed is usable by any SRX Series device that is a part of the same realm as SRX-1
- D. Juniper ATP Cloud automatically creates the `Suopi\cioua_Endpoints` feed after you commit the security policy.

Correct Answer: AC

---

**QUESTION 14**

Exhibit

```
Profile: xyz-profile3
  Server address: 192.168.30.188
  Authentication port: 1645
  Preauthentication port: 1810
  Accounting port: 1646
  Status: UNREACHABLE
Profile: xyz-profile2
  Server address: 192.168.30.190
  Authentication port: 1812
  Preauthentication port: 1810
  Accounting port: 1813
  Status: DOWN ( 60 seconds )
Profile: xyz-profile11
  Server address: 2001:DB8:0:f101::2
  Authentication port: 1645
  Preauthentication port: 1810
  Accounting port: 1646
  Status: UP
Profile: xyz-profile7
  Server address: 192.168.30.191
  Authentication port: 1812
  Preauthentication port: 1810
  Accounting port: 1813
  Status: DOWN ( 30 seconds )
```

The show network-access aaa radius-servers command has been issued to solve authentication issues.

Referring to the exhibit, to which two authentication servers will the SRX Series device continue to send requests? (Choose TWO)

- A. 2001:DB8:0:f101::2
- B. 192.168.30.191
- C. 192.168.30.190
- D. 192.168.30.188

Correct Answer: BD

#### QUESTION 15

Regarding IPsec CoS-based VPNs, what is the number of IPsec SAs associated with a peer based upon?

- A. The number of traffic selectors configured for the VPN.
- B. The number of CoS queues configured for the VPN.
- C. The number of classifiers configured for the VPN.
- D. The number of forwarding classes configured for the VPN.

Correct Answer: D

Explanation: In IPsec CoS-based VPNs, the number of IPsec Security Associations (SAs) associated with a peer is based on the number of forwarding classes configured for the VPN. The forwarding classes are used to classify and prioritize different types of traffic, such as voice and data traffic. Each forwarding class requires a separate IPsec SA to be established between the peers, in order to provide the appropriate level of security and quality of service for each type of traffic.

[Latest JN0-636 Dumps](#)

[JN0-636 PDF Dumps](#)

[JN0-636 Exam Questions](#)