JN0-636 Q&As

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.pass2lead.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

```
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 2

What are two valid modes for the Juniper ATP Appliance? (Choose two.)

A. flow collector

B. event collector

C. all-in-one

D. core

Correct Answer: AC

Explanation: The Juniper ATP Appliance supports two valid modes of operation:

Flow Collector: This mode allows the Juniper ATP Appliance to collect and analyze network flow data to detect malicious activity.

All-in-One: This mode allows the Juniper ATP Appliance to perform both flow collection and event collection. It includes all the features of the Flow Collector and Event Collector mode.

Event collector and core are not valid modes for the Juniper ATP Appliance, the first one is focused on collecting events and the second one is a term that\\'s not related to the appliance.

QUESTION 3

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

Exhibit

```
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 4

You opened a support ticket with JTAC for your Juniper ATP appliance. JTAC asks you to set up access to the device using the reverse SSH connection. Which three setting must be configured to satisfy this request? (Choose three.)

A. Enable JTAC remote access

B. Create a temporary root account.

C. Enable a JATP support account.

D. Create a temporary admin account.

E. Enable remote support.

Correct Answer: CDE

https://kb.juniper.net/InfoCenter/index?page=contentandid=TN326andcat=andactp=LISTandshowDr aft=false

QUESTION 5

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 junos:TOR ];
}
then {
    reject {
        application-services {
            security-intelligence {
                add-destination-ip-to-feed {
                    Proxy_Nodes;
...
```

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

A. The SRX-1 device can use the Proxy__Nodes feed in another security policy.

B. You can use the Proxy_Nodes feed as the source-address and destination-address match criteria of another security policy on a different SRX Series device.

C. The SRX-1 device creates the Proxy_wodes feed, so it cannot use it in another security policy.

D. You can only use the Proxy_Node3 feed as the destination-address match criteria of another security policy on a different SRX Series device.

Correct Answer: AC

QUESTION 6

What are two important function of the Juniper Networks ATP appliance solution? (Choose two.).

A. Statistics

B. Analysis

C. Detection

D. Filtration

Correct Answer: BC

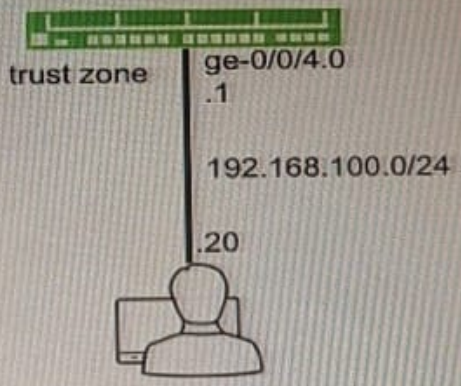
Explanation: https://www.juniper.net/us/en/products-services/security/advanced-threat- prevention/

QUESTION 7

Exhibit

```
[edit]
user@SRX# show interfaces ge-0/0/4
unit 0 {
    family inet {
        address 192.168.100.1/32;
    }
}

[edit security zones]
user@SRX# show security-zone trust
host-inbound-traffic {
    system-services {
        netconf;
    }
}
interfaces {
    ge-0/0/4.0 {
        host-inbound-traffic {
            system-services {
                ssh;
            }
        }
    }
}
```



You are not able to ping the default gateway of 192.168 100 1 (or your network that is located on your SRX Series firewall. Referring to the exhibit, which two commands would correct the configuration of your SRX Series device? (Choose two.)

A.
```
[edit security zones security-zone trust]
user@SRX# set interfaces ge-0/0/4.0 host-inbound-traffic system-services ping
```

B.
```
[edit interfaces ge-0/0/4]
user@SRX# replace pattern 32 with 24
```

C.
```
[edit security zones security-zone trust]
user@SRX# set host-inbound-traffic system-services ping
```

D.
```
[edit security zones security-zone trust]
user@SRX# set host-inbound-traffic system-services ping except
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: C

QUESTION 8

Which three type of peer devices are supported for Cos-Based IPsec VPN?

A. High-end SRX Series device

B. cSRX

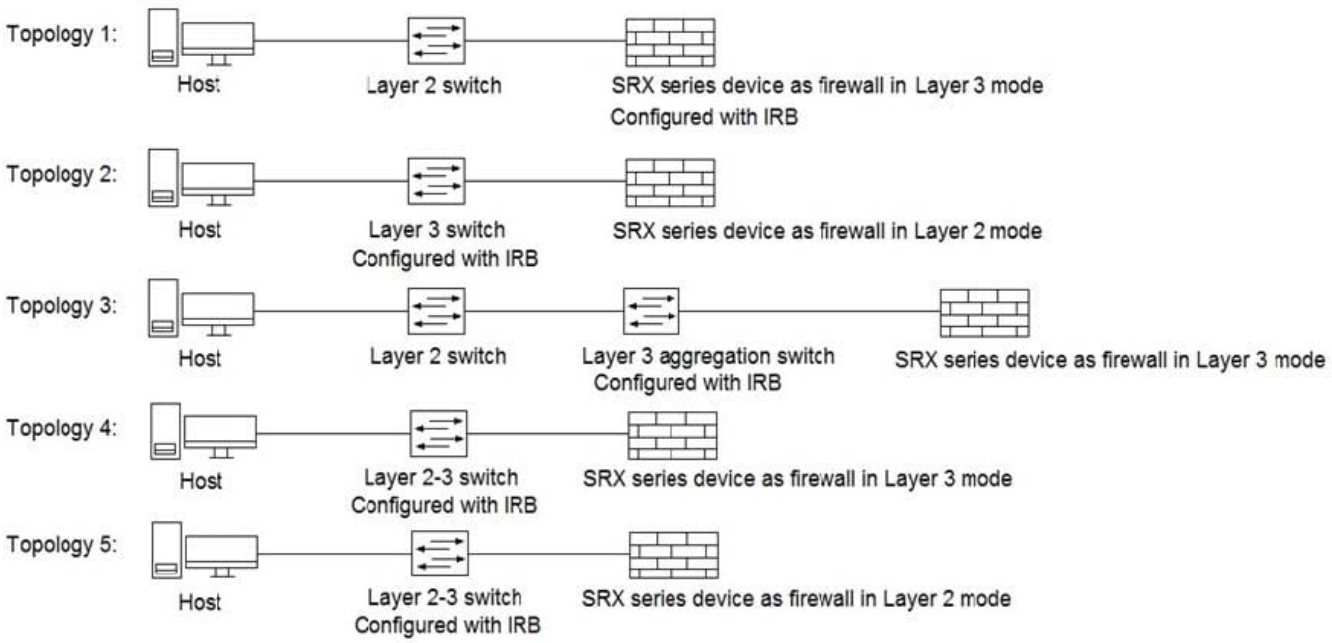
C. vSRX

D. Branch-end SRX Series devics

Correct Answer: ACD

QUESTION 9

Click the Exhibit button.



Referring to the exhibit, which three topologies are supported by Policy Enforcer? (Choose three.)

A. Topology 3

B. Topology 5

C. Topology 2

D. Topology 4

E. Topology 1

Correct Answer: ADE

Reference: https://www.juniper.net/documentation/en_US/junos-space17.2/policy- enforcer/topics/concept/ policy-enforcer-deployment-supported-topologies.html

QUESTION 10

Exhibit

Exhibit

```
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.
```

You are using traceoptions to verify NAT session information on your SRX Series device. Referring to the exhibit, which two statements are correct? (Choose two.)

A. This is the last packet in the session.

B. The SRX Series device is performing both source and destination NAT on this session.

C. This is the first packet in the session.

D. The SRX Series device is performing only source NAT on this session.

Correct Answer: AB

QUESTION 11

You are connecting two remote sites to your corporate headquarters site. You must ensure that all traffic is secured and sent directly between sites In this scenario, which VPN should be used?

A. IPsec ADVPN

B. hub-and-spoke IPsec VPN

C. Layer 2 VPN

D. full mesh Layer 3 VPN with EBGP

Correct Answer: A

Explanation: IPsec ADVPN (Auto-Discovery VPN) is a VPN that enables the creation of a full mesh VPN topology among a set of remote sites. It allows the remote sites to discover one another automatically and establish IPsec VPN tunnels among themselves. It is useful when you need to connect multiple remote sites to your corporate headquarters site, and ensure that all traffic is secured and sent directly between sites. ADVPN allows for the creation of a hub-and-spoke topology, which is not suitable for this case. Layer 2 VPN can be used for point to point connectivity but does not secure the traffic. Also, A full mesh Layer 3 VPN with EBGP is a good option for this scenario but it is more complex than ADVPN, and it requires more configuration.

QUESTION 12

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.

QUESTION 13

Your IPsec VPN configuration uses two CoS forwarding classes to separate voice and data traffic. How many IKE security associations are required between the IPsec peers in this scenario?

B. 3

C. 4

D. 2

Correct Answer: A

Explanation: An IKE security association (SA) is a set of parameters that define how the Internet Key Exchange (IKE) protocol will authenticate and establish the secure channel between the IPsec VPN peers. When you configure an IPsec

VPN, one IKE SA is created between the peers, regardless of how many CoS forwarding classes are used to separate the traffic. The SA will be used to negotiate the IPsec SA parameters, such as encryption algorithms and keys.

In this scenario, only 1 IKE security association is required between the IPsec peers, no matter how many CoS forwarding classes are used to separate the voice and data traffic.

QUESTION 14

You have designed the firewall filter shown in the exhibit to limit SSH control traffic to yours SRX Series device without affecting other traffic. Which two statement are true in this scenario? (Choose two.)

A. The filter should be applied as an output filter on the loopback interface.

B. Applying the filter will achieve the desired result.

C. Applying the filter will not achieve the desired result.

D. The filter should be applied as an input filter on the loopback interface.

Correct Answer: CD

Explanation: https://www.juniper.net/documentation//en_US/junos/topics/concept/firewall- filter-ex-series-evaluation-understanding.html

---

QUESTION 15

You are asked to download and install the IPS signature database to a device operating in chassis cluster mode. Which statement is correct in this scenario?

A. You must download and install the IPS signature package on the primary node.

B. The first synchronization of the backup node and the primary node must be performed manually.

C. The first time you synchronize the IPS signature package from the primary node to the backup node, the primary

node must be rebooted.

D. The IPS signature package must be downloaded and installed on the primary and backup nodes.

Correct Answer: D