![Pass2Lead logo](https://Pass2Lead.com)
JN0-635^{Q&As}

Security, Professional

Pass Juniper JN0-635 Exam with 100% Guarantee

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

https://www.pass2lead.com/jn0-635.html

100% Passing Guarantee
100% Money Back Assurance

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

![Pass2Lead](https://Pass2Lead.com)
QUESTION 1

You are asked to implement the session cache feature on an SRX5400.

In this scenario, what information does a session cache entry record? (Choose two.)

A. The type of processing to do for ingress traffic

B. The type of processing to do for egress traffic

C. To which SPU the traffic of the session should be forwarded

D. To which NPU the traffic of the session should be forwarded

Correct Answer: BC

Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-packet-basedforwarding.html

QUESTION 2

Click the Exhibit button.

```
user@srx> show chassis cluster interfaces
Control link status: Up

Control interfaces:
    Index      Interface        Monitored-Status      Internal-SA      Security
     0         em0              Up                    Disabled         Enabled

Fabric link status: Up

...
```

Referring to the exhibit, which statement is true?

A. ARP security is securing data across the control interface

B. IPsec is securing data across the control interface

C. SSH is securing data across the control interface

D. MACsec is securing data across the control interface

Correct Answer: D

Reference: https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/ show-chassis-cluster-interfaces.html

![Pass2Lead](https://Pass2Lead.com)
QUESTION 3

In a Juniper ATP Appliance, what would be a reason for the mitigation rule to be in the failed-remove state?

A. The Juniper ATP Appliance received a commit error message from the SRX Series device

B. The Juniper ATP Appliance received an unknown error message from the SRX Series device

C. The Juniper ATP Appliance was not able to communicate with the SRX Series device

D. The Juniper ATP Appliance was not able to obtain the config lock

Correct Answer: D

Reference: https://www.juniper.net/documentation/en_US/release-independent/jatp/topics/topic-map/jatpmitigation-and-reporting.html

---

QUESTION 4

Click the Exhibit button.

```
user@srx> show log flow-trace
Apr 3 02:10:28 02:10:28.045090:CID-0:THREAD_ ID-01:RT: <10.10.101.10/60858->
10.10.102.10/22; 6, 0x0> matched filter filter-1:
...
Apr 3 02:10:28 02:10:28.045100:CID-0:THREAD_ID-01:RT: no session found, start
first path. in tunnel-0x0, from_cp_flag-0
...
Apr 3 02:10:28 02:10:28.045104:CID-0:THREAD_ID-01:RT: flow first create session
...
...
Apr 3 02:10:28 02:10:28.045143:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.10) from trust (ge-0/0/4 0 in 0) to ge-0/0/5.0, Next-hop: 10.10.102.10
...
Apr 3 02:10:28 02:10:28.045158:CID-0:THREAD_ID-01:RT: flow_first_policy search:
policy search from zone trust-> zone dmz (0x0 0xedba0016,0x16)
...
Apr 3 02:10:28 02:10:28.045191:CID-0:THREAD_ID-01:RT: packet dropped, denied by
policy
...
Apr 3 02:10:28 02:10:28.045192:CID-0:THREAD_ID-01:RT: denied by policy default-
policy-logical-system-00(2), dropping Pkt
...
Apr 3 02:10:28 02:10:28.0451 92:CID-0.THREAD_ID-01:RT: packet dropped, policy
deny
```

The exhibit shows a snippet of a security flow trace. A user cannot open an SSH session to a server. Which action will solve the problem?

A. Create a security policy that matches the traffic parameters

B. Edit the source NAT to correct the translated address

C. Create a route entry to direct traffic into the configured tunnel

D. Create a route to the desired server

Correct Answer: A

QUESTION 5

Which Junos security feature is used for signature-based attack prevention?

A. RADIUS

B. AppQoS

C. IPS

D. PIM

Correct Answer: C

QUESTION 6

You have set up Security Director with Policy Enforcer and have configured 12 third-party feeds and a Sky ATP feed. You are also injecting 16 feeds using the available open API. You want to add another compatible feed using the available open API, but Policy Enforcer is not receiving the new feed.

What is the problem in this scenario?

A. You must wait 48 hours for the feed to update

B. You cannot add more than 16 feeds through the available open API

C. You have reached the maximum limit of 29 total feeds

D. You cannot add more than 16 feeds with the available open API

Correct Answer: C

Reference: https://www.juniper.net/documentation/en_US/release-independent/sky-atp/informationproducts/ pathway-pages/sky-atp-admin-guide.pdf page 110

QUESTION 7

In which two ways are tenant systems different from logical systems? (Choose two.)

A. Tenant systems have higher scalability than logical systems

B. Tenant systems have less scalability than logical systems

C. Tenant systems have fewer routing features than logical systems

D. Tenant systems have more routing features than logical systems

Correct Answer: AC

Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/tenant-systemsoverview.html#:~:text=Although%20similar%20to%20logical%20systems,administrative%20domain % 20for%

![Pass2Lead](https://Pass2Lead.com)
QUESTION 8

You are asked to secure your network against TOR network traffic.

Which two Juniper products would accomplish this task? (Choose two.)

A. Contrail Edge

B. Contrail Insights

C. Juniper Sky ATP

D. Juniper ATP Appliance

Correct Answer: CD

QUESTION 9

Click the Exhibit button.

![Pass2Lead](https://Pass2Lead.com)
```
  [edit interfaces]
user@new-site-gateway# show st0
unit 0 {
    family inet {
        address 10.0.0.2/30;
        }
}

  [edit interfaces]
user@new-site-gateway# show ge-0/0/2
unit 0 {
family inet {
dhcp ;

  [edit security zones]
user@new-site-gateway# show security-zone untrust
interfaces {
    ge-0/0/2.0 {
        host-inbound-traffic {
          system-services {
                ike;
                dhcp;
            }
          }
      }
}
  [edit security ike]
user@new-site-gateway# show
policy ike-pol-1 {
        mode main;
        proposal-set standard;
        pre- shared- key ascii - text "  $9$6st6CpOhSeX7V1RwYZG69A"; ## SECRET-
DATA
        }
gateway gate-1 {
    ike-policy ike-pol-1;
    address 203.0.113.5;
    local-identity hostname "srxl@srx.juniper.net";
    external-interface ge-0/0/2.0;
}
```

Your company has purchased a competitor and now must connect the new network to the existing one. The competitor\\'s gateway device is receiving its ISP address using DHCP. Communication between the two sites must be secured; however, obtaining a static public IP address for the new site gateway is not an option at this time. The company has several requirements for this solution:

A site-to-site IPsec VPN must be used to secure traffic between the two sites; The IKE identity on the new site gateway device must use the hostname option; and Internet traffic from each site should exit through

its local Internet connection.

The configuration shown in the exhibit has been applied to the new site\\'s SRX, but the secure tunnel is not

working.

In this scenario, what configuration change is needed for the tunnel to come up?

A. Remove the quotes around the hostname

B. Bind interface st0 to the gateway

C. Change the IKE policy mode to aggressive

D. Apply a static address to ge-0/0/2

Correct Answer: C

QUESTION 10

You have noticed a high number of TCP-based attacks directed toward your primary edge device. You are asked to configure the IDP feature on your SRX Series device to block this attack. Which two IDP attack objects would you configure to solve this problem? (Choose two.)

A. Network

B. Signature

C. Protocol anomaly

D. host

Correct Answer: BC

QUESTION 11

You have configured static NAT for a webserver in your DMZ. Both internal and external users can reach the webserver using the webserver\\'s IP address. However, only internal users can reach the webserver using the webserver\\'s DNS name. When external users attempt to reach the webserver using the webserver\\'s DNS name, an error message is received.

Which action would solve this problem?

A. Disable Web filtering

B. Use DNS doctoring

C. Modify the security policy

D. Use destination NAT instead of static NAT

Correct Answer: B

Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-dns-algs.html

QUESTION 12

You have designed the firewall filter shown in the exhibit to limit SSH control traffic to yours SRX Series

![Pass2Lead](https://Pass2Lead.com)
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

Reference: https://www.juniper.net/documentation//en_US/junos/topics/concept/firewall-filter-ex-series-evaluationunderstanding.html

---

QUESTION 13

Click the Exhibit button.

```
user@srx> show security flow session destination-prefix 172.31.15.1
destination-port 22 extensive
Session ID: 19867, Status: Normal
Flags: 0x40/0x0/0x8003
Policy name: internet-trust/5
Source NAT pool: Null, Application: junos-ssh/22
Dynamic application: junos:UNKNOWN,
Encryption: Unknown
Application traffic control rule-set: INVALID, Rule: INVALID
Maximum timeout: 1800, Current timeout: 1766
Session State: Valid
Start time: 598746, Duration: 45
   In: 10.10.101.10/61179 --> 172.31.15.1/22;tcp,
 Conn Tag: 0x0, Interface: ge-0/0/4.0,
    Session token: 0x7, Flag: 0x1021
    Route: 0x110010, Gateway: 10.10.101.10, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 18, Bytes: 3261
   Out: 172.31.15.1/22 --> 10.10.101.10/61179;tcp,
 Conn Tag: 0x0, Interface; ge-0/0/3.0,
   Session token: 0x9, Flag: 0x1020
   Route: 0x120010, Gateway: 172.18.1.2, Tunnel: 0
   Port sequence: 0, FIN sequence: 0,
   FIN state: 0,
   Pkts: 16, Bytes: 3773
 Total sessions: 1
```

Given the command output shown in the exhibit, which two statements are true? (Choose two.)

A. The host 172.31.15.1 is directly connected to interface ge-0/0/3.0

B. Traffic matching this session has been received since the session was established

C. The host 10.10.101.10 is directly connected to interface ge-0/0/4.0

D. Network Address Translation is applied to this session

Correct Answer: BC

QUESTION 14

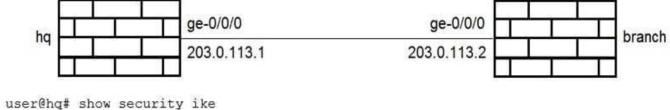What are two important function of the Juniper Networks ATP appliance solution? (Choose two.).

A. Statistics

B. Analysis

C. Detection

D. Filtration

Correct Answer: BC

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

QUESTION 15

Click the Exhibit button.


```
user@hq# show security ike
...
gateway ike_gtw-branch {
      ike-policy ike-policy-branch;
      dynamic hostname branch.abc.com;
      external-interface ge-0/0/0;
      local-address 203.0.113.1;
}
```

The IKE policy and proposal are configured properly on both devices as shown in the exhibit. Which configuration snippet will complete the IKE configuration on the branch SRX Series device?

A. [edit security ike]
   user@srx# show gateway ike_gtw_hq
   ike-policy ike-policy-hq;
   dynamic hostname branch.abc.com;
   external-interface ge-0/0/0;
   local-address 203.0.113.2;

B. [edit security ike]
   user@srx# show gateway ike_gtw_hq
   ike-policy ike-policy-hq;
   dynamic hostname hq.abc.com;
   external-interface ge-0/0/0;
   local-address 203.0.113.2;

C. [edit security ike]
   user@srx# show gateway ike_gtw_hq
   ike-policy ike-policy-hq;
   local-identity hostname hq.abc.com;
   external-interface ge-0/0/0;
   local-address 203.0.113.2;

D. [edit security ike]
   user@srx# show gateway ike_gtw_hq
   ike-policy ike-policy-hq;
   local-identity hostname branch.abc.com;
   external-interface ge-0/0/0;
   local-address 203.0.113.2;

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: D

Latest JN0-635 Dumps   JN0-635 Practice Test   JN0-635 Braindumps