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.passapply.com/jn0-635.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You have the NAT rule, shown in the exhibit, applied to allow communication across an IPsec tunnel between your two sites with identical networks. Which statement is correct in this scenario?

A. The NAT rule with translate the source and destination addresses.

B. The NAT rule will only translate two addresses at a time.

C. The NAT rule in applied to the N/A routing instance.

D. 10 packets have been processed by the NAT rule.

Correct Answer: A

QUESTION 2

You are asked to configure an IPsec VPN between two SRX Series devices that allows for processing of

CoS on the intermediate routers.

What will satisfy this requirement?

A. route-based VPN

B. OpenVPN

C. remote access VPN

D. policy-based VPN

Correct Answer: A

Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/secuirty-cos-basedipsec-vpns.html

QUESTION 3

You are connecting two remote sites to your corporate headquarters site; you must ensure that all traffic is

secured and

only uses a single Phase 2 SA for both sites.

In this scenario, which VPN should be used?

A. An IPsec group VPN with the corporate firewall acting as the hub device.

B. Full mesh IPsec VPNs with tunnels between all sites.

C. A hub-and-spoke IPsec VPN with the corporate firewall acting as the hub device.

D. A full mesh Layer 3 VPN with the corporate firewall acting as the hub device.

Correct Answer: A

Reference: https://www.juniper.net/us/en/local/pdf/app-notes/3500202-en.pdf

QUESTION 4

Click the Exhibit button.

```
user@host> telnet 172.20.202.10
Connected to 172.20.202.10.
Escape character is '^]'.
remote-device (ttyp1)
login:

user@srx> show security flow session application telnet
Session ID: 68748, Policy name: FBF-Internet/11, Timeout: 1722, Valid
 In: 172.20.201.10/55530 --> 172.20.202.10/23;tcp, Conn Tag: 0x0, If: ge-
0/0/5.0,
Pkts: 28, Bytes: 1624,
 Out: 172.20.202.10/23 --> 172.20.201.10/55530;tcp, Conn Tag: 0x0, If:
ge-0/0/1.0, Pkts: 22, Bytes: 1418,
Total sessions: 1
```

You are implementing a new branch site and want to ensure Internet traffic is sent directly to your ISP and other traffic is sent to your company headquarters. You have configured filter-based forwarding to accomplish this objective. You verify proper functionality using the outputs shown in the exhibit.

Which two statements are true in this scenario? (Choose two.)

A. The session utilizes one routing instance

B. The ge-0/0/5 and ge-0/0/1 interfaces must reside in a single security zone

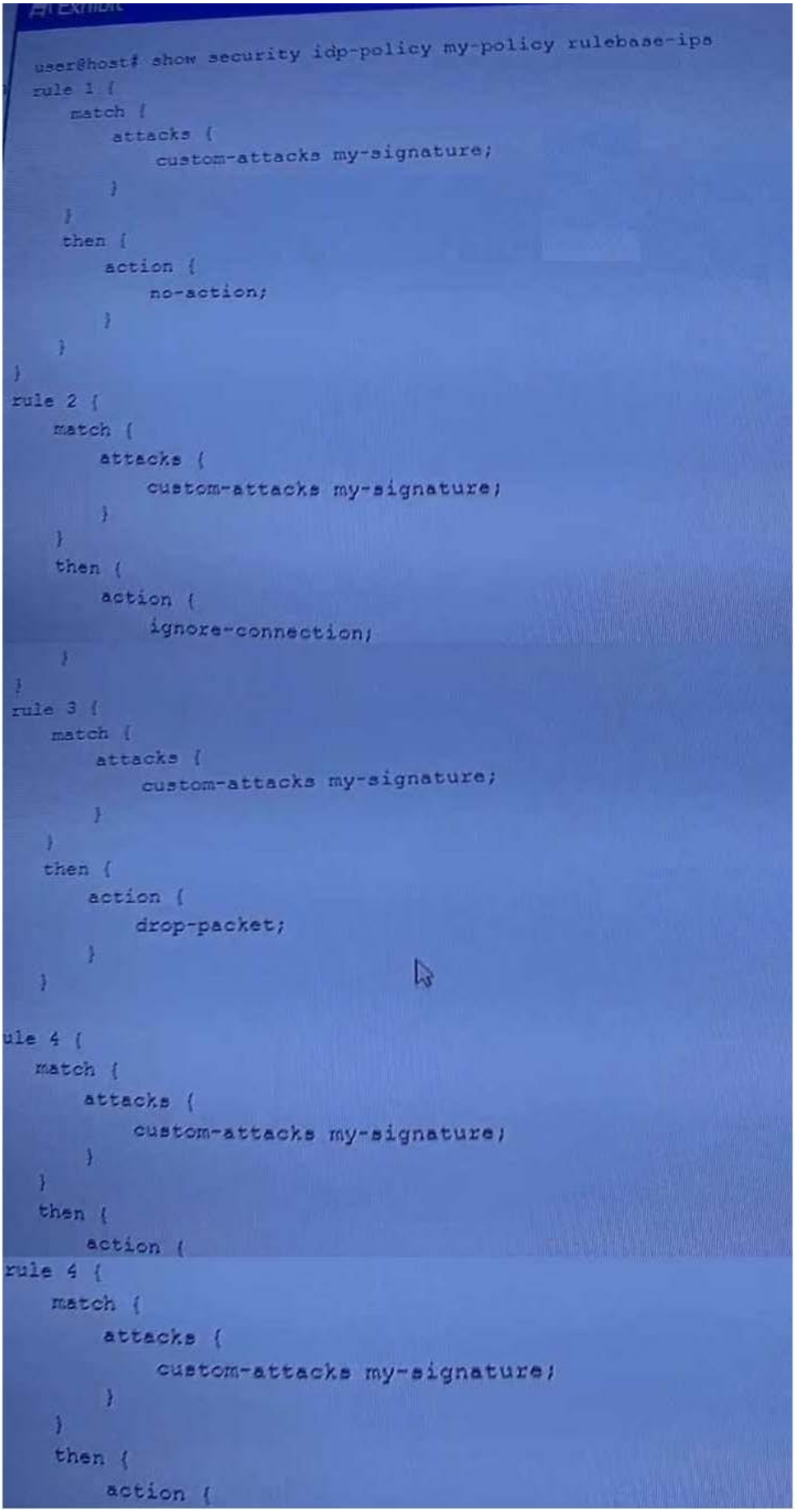
C. The ge-0/0/5 and ge-0/0/1 interfaces can reside in different security zones

D. The session utilizes two routing instances

Correct Answer: AC

QUESTION 5

Exhibit.



```
user@host# show security idp-policy my-policy rulebase-ips
rule 1 {
    match {
        attacks {
            custom-attacks my-signature;
        }
    }
    then {
        action {
            no-action;
        }
    }
}
rule 2 {
    match {
        attacks {
            custom-attacks my-signature;
        }
    }
    then {
        action {
            ignore-connection;
    }
}
rule 3 {
    match {
        attacks {
            custom-attacks my-signature;
        }
    }
    then {
        action {
            drop-packet;
        }
    }

ule 4 {
    match {
        attacks {
            custom-attacks my-signature;
        }
    }
    then {
        action {
rule 4 {
    match {
        attacks {
            custom-attacks my-signature;
        }
    }
    then {
        action {
```

A hub member of an ADVPN is not functioning correctly. Referring the exhibit, which action should you take to solve the problem?

A. [edit interfaces] root@vSRX-1# delete st0.0 multipoint

B. [edit interfaces] user@hub-1# delete ipsec vpn advpn-vpn traffic-selector

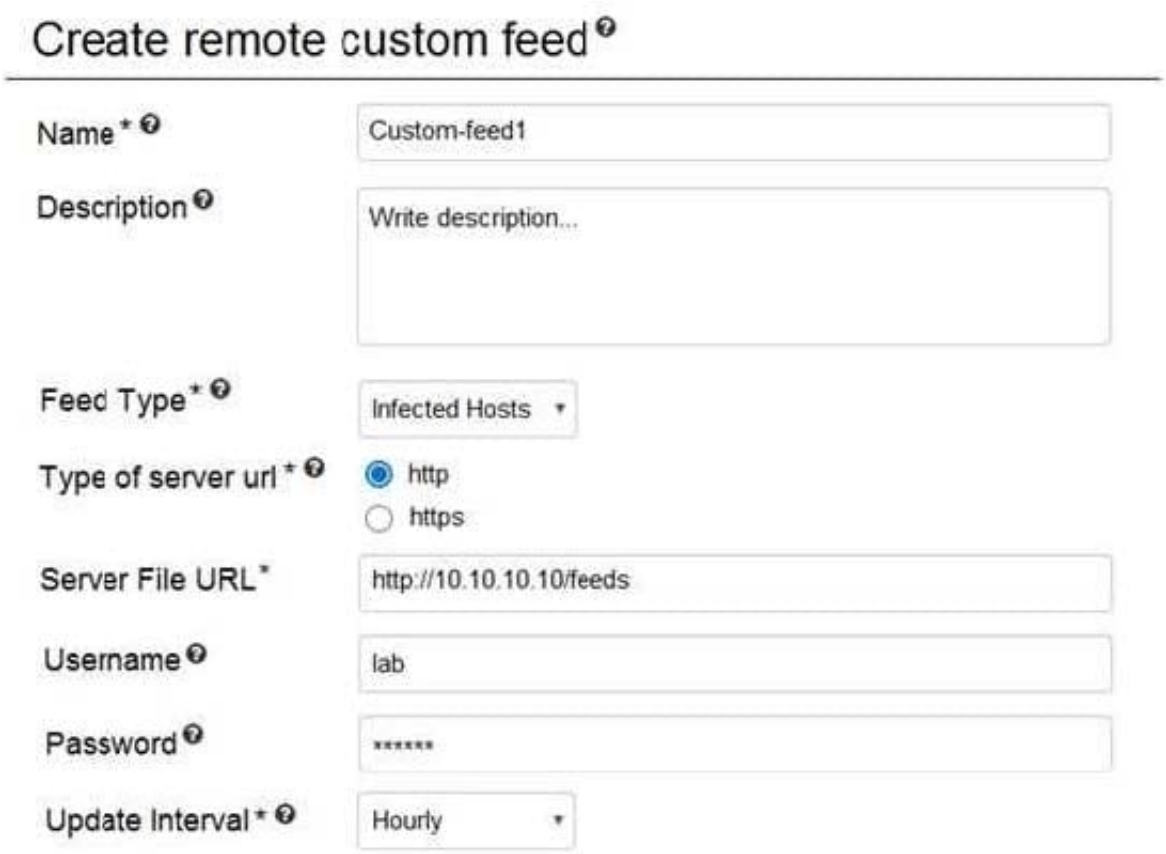
C. [edit security] user@hub-1# set ike gateway advpn-gateway advpn suggester disable

D. [edit security] user@hub-1# delete ike gateway advpn-gateway advpn partner

Correct Answer: B

QUESTION 6

Click the Exhibit button.



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

A. Events based on this third-party feed will not affect a host\\'s threat score

B. SRX Series devices will block traffic based on this third-party feed

C. SRX Series devices will not block traffic based on this third-party feed

D. Events based on this third-party feed will affect a host\\'s threat score

Correct Answer: AB

Reference: https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/skyatp-integrated-feeds.html

QUESTION 7

You are trying to get a SSH honeypot set up on a Juniper ATP Appliance collector. The collector is running on hardware with two physical interfaces and two physical CPU cores. The honeypot feature is not working.

Which statement is true in this scenario?

A. The collector must have at least three physical interfaces

B. The collector must have at least four physical cores

C. The collector must have at least four physical interfaces

D. The collector must have at least six physical cores

Correct Answer: A

QUESTION 8

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 9

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 10

Your SRX Series device does not see the SYN packet. What is the default action in this scenario?

A. The device will forward the subsequent packets and the session will be established

B. The device will forward the subsequent packets and the session will not be established

C. The device will drop the subsequent packets and the session will not be established

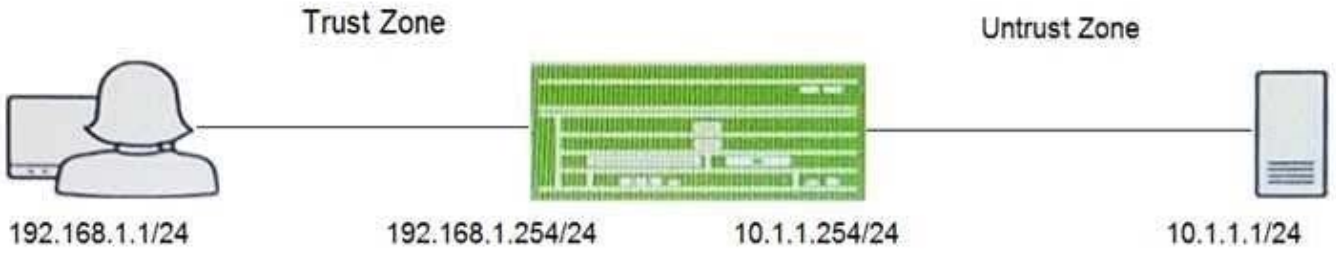
D. The device will drop the subsequent packets and the session will be established

Correct Answer: C

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

QUESTION 11

Click the Exhibit button.



A user reports trouble when using SSH to a server outside your organization. The traffic traverses an SRX Series device that is performing NAT and applying security policies.

Referring to the exhibit, which configuration will allow you to see the bidirectional flow through the SRX Series device?

A.
```
[edit security flow traceoptions]
file tracefile;
flag basic-datapath;
packet-filter MATCH-TRAFFIC-OUT {
     source-prefix 192.168.1.1/32;
     destination-prefix 192.168.1.254/32;
}
packet-filter MATCH-TRAFFIC-IN {
     source-prefix 10.1.1.1/32;
     destination-prefix 10.1.1.254./32;
}
```

B.
```
[edit security flow traceoptions]
file tracefile;
flag basic-datapath;
packet-filter MATCH-TRAFFIC-OUT {
     source-prefix 192.168.1.1/32;
     destination-prefix 192.168.1.254/32;
}
```

C.
```
[edit security flow traceoptions]
file tracefile;
flag basic-datapath;
packet-filter MATCH-TRAFFIC {
     source-prefix 192.168.1.1/32;
     destination-prefix 10.1.1.1/32;
}
```

D.
```
[edit security flow traceoptions]
file tracefile;
flag basic-datapath;
packet-filter MATCH-TRAFFIC-OUT {
     source-prefix 192.168.1.1/32;
     destination-prefix 10.1.1.1/32;
}
packet-filter MATCH-TRAFFIC-IN {
     source-prefix 10.1.1.1/32;
     destination-prefix 192.168.1.1./32;
}
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: D

QUESTION 12

Click the Exhibit button.

```
user@srx> show security macsec connections
Interface name: ge-0/0/0
      CA name: ca1
      Cipher suite: GCM-AES-128          Encryption: on
      Key server offset: 0               Include SCI: no
      Replay protect: off                Replay window: 0
            Outbound secure channels
                  SC Id: 02:00:00:01:01:04/1
                  Outgoing packet number: 1
                  Secure associations
                  AN: 3 Status: inuse Create time: 00:01:43
            Inbound secure channels
                  SC Id: 02:00:00:02:01:04/1
                  Secure associations
                  AN: 3 Status: inuse Create time: 00:01:43
```

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

A. Data is transmitted across the link in plaintext

B. The link is not protected against man-in-the-middle attacks

C. The link is protected against man-in-the-middle attacks

D. Data is transmitted across the link in cyphertext

Correct Answer: BD

QUESTION 13

When would you use the port-overloading-factor 1 setting?

A. to enable the port-overloading

B. to disable the port-overloading

C. to map ports with 1:1 ratio for port-overloading

D. to set the maximum port-overloading capacity to 65,536

Correct Answer: C

Reference: https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/ security-edit-port-overloading-interface-source-nat.html

QUESTION 14

You are asked to set up notifications if one of your collector traffic feeds drops below 100 kbps.

Which two configuration parameters must be set to accomplish this task? (Choose two.)

A. Set a traffic SNMP trap on the JATP appliance

B. Set a logging notification on the JATP appliance

C. Set a general triggered notification on the JATP appliance

D. Set a traffic system alert on the JATP appliance

Correct Answer: BD

QUESTION 15

You have a webserver and a DNS server residing in the same internal DMZ subnet. The public Static NAT addresses for the servers are in the same subnet as the SRX Series devices internet-facing interface. You implement DNS doctoring to ensure remote users can access the webserver.

Which two statements are true in this scenario? (Choose two.)

A. The DNS doctoring ALG is not enabled by default.

B. The Proxy ARP feature must be configured.

C. The DNS doctoring ALG is enabled by default.

D. The DNS CNAME record is translated.

Correct Answer: BC