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

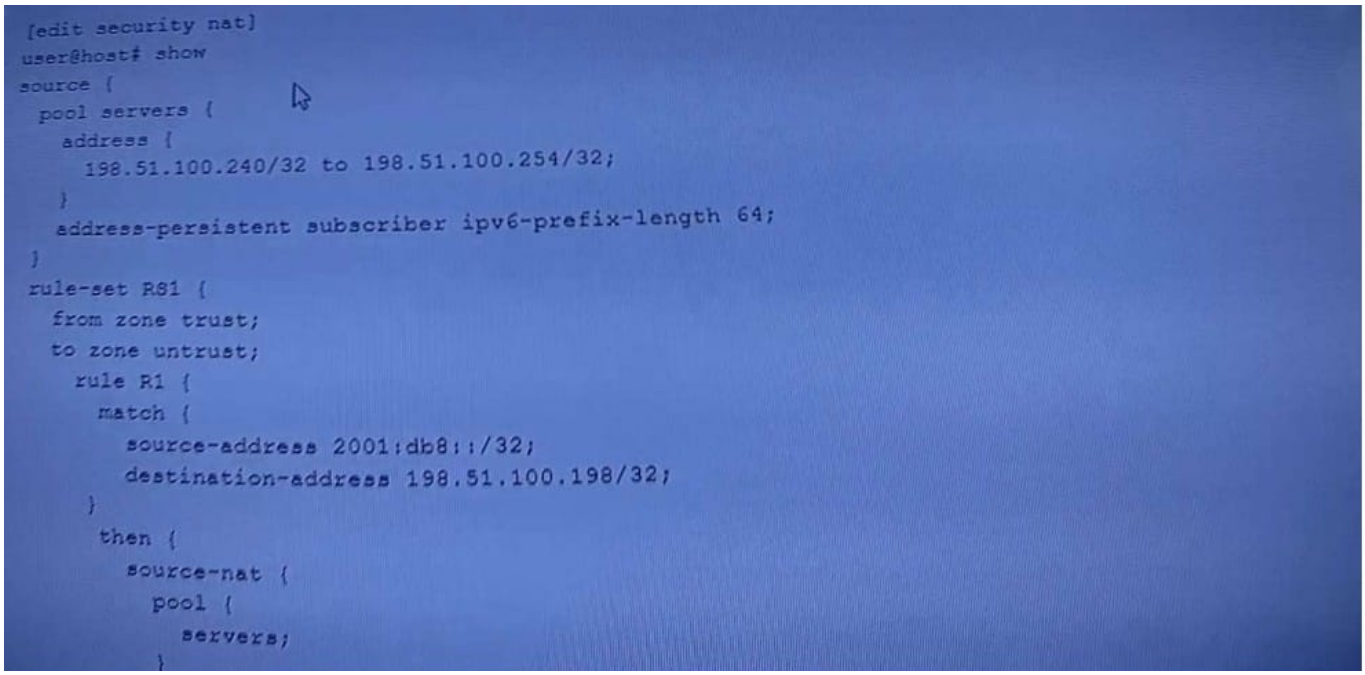
100% Passing Guarantee
100% Money Back Assurance

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.



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

A. The configured solution allows IPv6 to IPv4 translation.

B. The configured solution allows IPv4 to IPv6 translation.

C. The IPv6 address is invalid.

D. External hosts cannot initiate contact.

Correct Answer: AC

QUESTION 2

Click the Exhibit button.

```
Communicate with JATP server...
error: [Error] Failed to communicate with JATP server when retrieving
registration status.
Please make sure you are able to connect to JATP server. If this issue still
remains, please contact JTAC for help.
```

When attempting to enroll an SRX Series device to JATP, you receive the error shown in the exhibit. What is the cause of the error?

A. The fxp0 IP address is not routable

B. The SRX Series device certificate does not match the JATP certificate

C. The SRX Series device does not have an IP address assigned to the interface that accesses JATP

D. A firewall is blocking HTTPS on fxp0

Correct Answer: C

Reference: https://kb.juniper.net/InfoCenter/index? page=contentandid=KB33979andcat=JATP_SERIESandactp=LIST

QUESTION 3

You are not able to activate the SSH honeypot on the all-in-one Juniper ATP appliance. What would be a cause of this problem?

A. The collector must have a minimum of two interfaces.

B. The collector must have a minimum of three interfaces.

C. The collector must have a minimum of five interfaces.

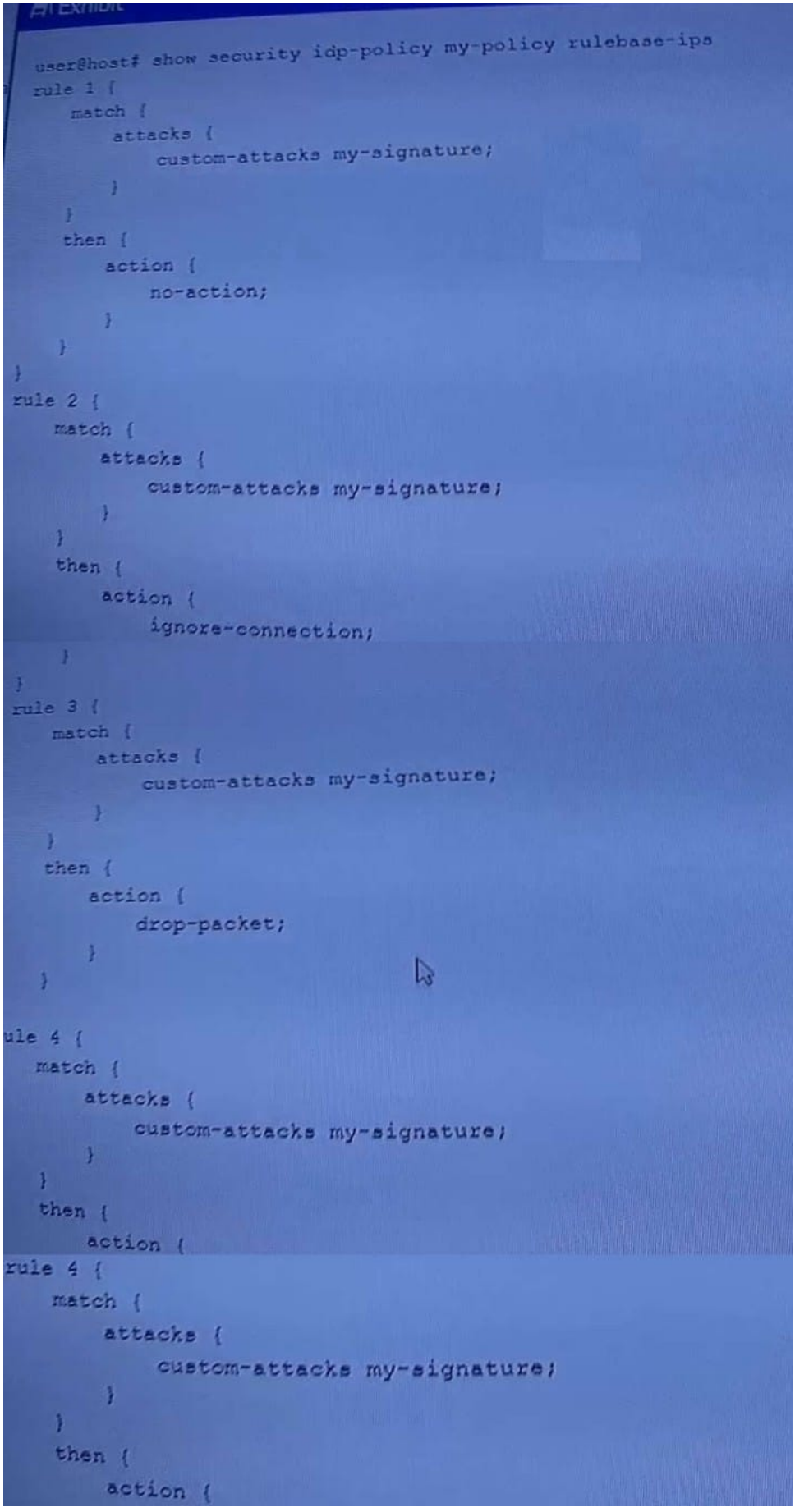
D. The collector must have a minimum of four interfaces.

Correct Answer: D

Explanation: https://www.juniper.net/documentation/en_US/release- independent/jatp/topics/task/configuration/jatp-traffic-collectorsetting-ssh-honeypot- detection.html

QUESTION 4

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 5

You are required to deploy a security policy on an SRX Series device that blocks all known Tor network IP addresses. Which two steps will fulfill this requirement? (Choose two.)

A. Enroll the devices with Juniper ATP Appliance.

B. Enroll the devices with Juniper ATP Cloud.

C. Enable a third-party Tor feed.

D. Create a custom feed containing all current known MAC addresses.

Correct Answer: AB

Explanation: To block all known Tor network IP addresses on an SRX Series device, the following steps must be taken:

Enroll the devices with Juniper ATP Appliance or Juniper ATP Cloud: both of these services provide threat intelligence feeds that include known IP addresses associated with the Tor network. By enrolling the SRX Series device, the device

will have access to the latest Tor network IP addresses, and it can then use this information to block traffic from those IP addresses. Creating a custom feed containing all current known MAC addresses, is not a valid option since Tor network

uses IP addresses, MAC addresses are not used to identify the Tor network.

Enable a third-party Tor feed may be used but it\\'s not necessary as Juniper ATP Appliance and Juniper ATP Cloud already provide the same feature.