Leads4Pass

JN0-633 ^{Q&As}

Security, Professional (JNCIP-SEC)

Pass Juniper JN0-633 Exam with 100% Guarantee

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

https://www.leads4pass.com/jn0-633.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

You are deploying a standalone SRX650 in transparent mode for evaluation purposes in a potential client\\'s network. The client will need to access the device to modify security policies and perform other various configurations. Where would you configure a Layer 3 interface to meet this requirement?

A. fxp0.0

B. vlan.1

C. irb.1

D. ge-0/0/0.0

Correct Answer: C

QUESTION 2

You are asked to ensure that your IPS engine blocks attacks. You must ensure that your system continues to drop additional malicious traffic without additional IPS processing for up to 30 minutes. You must ensure that the SRX Series device does send a notification packet when the traffic is dropped.

Which statement is correct?

A. Use the IP-Block action.

B. Use the Drop Packet action.

C. Use the Drop Connection action.

D. Use the IP-Close action.

Correct Answer: D

QUESTION 3

-- Exhibit -[edit forwarding-options] user@srx240# show packet-capture {

 file filename my-packet-capture;

 maximum-capture-size 1500; } -- Exhibit -

Referring to the exhibit, you are attempting to perform a packet capture on an SRX240 to troubleshoot an SSH issue in your network. However, no information appears in the packet capture file.

Which firewall filter must you apply to the necessary interface to collect data for the packet capture?

A. user@srx240# show filter pkt-capture { term pkt-capture-term {

 from {

protocol tcp;

port ssh;

}

then packet-mode;

}

term allow-all {

then accept;

}

}

[edit firewall family inet]

B. user@srx240# show filter pkt-capture { term pkt-capture-term {

from {

protocol tcp;

port ssh;

}

then {

count packet-capture;

}

}

term allow-all {

then accept;

}

}

[edit firewall family inet]

C. user@srx240# show filter pkt-capture { term pkt-capture-term {

from {

protocol tcp;

port ssh;

}

```
then {

routing-instance packet-capture;

}

}

term allow-all {

then accept;

}

}
[edit firewall family inet]
```

D. user@srx240# show

```
filter pkt-capture {

term pkt-capture-term {

from {

protocol tcp;

port ssh;

}

then {

sample;

accept;

}

}

term allow-all {

then accept;

}

}
[edit firewall family inet]
```
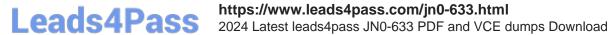
Correct Answer: D

QUESTION 4

Click the Exhibit button.

[edit security idp-policy test] user@host# show rulebase-ips {

 rule R3 {

 match {

 source-address any;

 destination-address any;

 attacks {

predefined-attacks FTP:USER:ROOT;

 }

 }

 then {

 action {

recommended;

 }

 }

 terminal;

 }

 rule R4 {

 match {

 source-address any;

 destination-address any;

 attacks {

predefined-attacks HTTP:HOTMAIL:FILE-UPLOAD;

 }

 }

 then {

 action { recommended; } } } }

You have just committed the new IDP policy shown in the exhibit. However, you notice no action is taken on traffic matching the R4 IDP rule. Which two actions will resolve the problem? (Choose two.)

A. Change the R4 rule to match on a predefined attack group.

B. Insert the R4 rule above the R3 rule.

C. Delete the terminal statement from the R3 rule.

D. Change the IPS rulebase to an exempt rulebase.

Correct Answer: C

QUESTION 5

You have initiated the download of the IPS signature database on your SRX Series device.

Which command would you use to confirm the download has completed?

A. request security idp security-package install

B. request security idp security-package download

C. request security idp security-package install status

D. request security idp security-package download status

Correct Answer: D

[JN0-633 PDF Dumps](#)   [JN0-633 Practice Test](#)   [JN0-633 Study Guide](#)