



# JN0-634<sup>Q&As</sup>

Security, Professional (JNCIP-SEC)

**Pass Juniper JN0-634 Exam with 100% Guarantee**

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

<https://www.geekcert.com/jn0-634.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

Click the Exhibit button.

Monitor / Hosts

Host 192.168.1.159 ?

Host Name: 192.168.1.159

Host Status: ? High threat level, recommend blocking host and investigating further ?

Investigation Status:

Open

Policy override for this host:

Use configured policy (included in infected hosts feed)

Referring to the exhibit, the host has been automatically blocked from communicating on the network because a malicious file was downloaded. You cleaned the infected host and changed the investigation status to Resolved ?Fixed.

What does Sky ATP do if the host then attempts to download a malicious file that would result in a threat score of 10?

- A. Sky ATP does not log the connection attempt and an SRX Series device does not allow the host to communicate on the network.
- B. Sky ATP logs the connection attempt and an SRX Series device does not allow the host to communicate on the network.
- C. Sky ATP logs the connection attempt and an SRX Series device allows the host to communicate on the network.
- D. Sky ATP does not log the connection attempt and an SRX Series device allows the host to communicate on the network.

Correct Answer: C

### QUESTION 2

Which statement about transparent mode on an SRX340 is true?

- A. You must reboot the device after configuring transparent mode.
- B. Security policies applied to transparent mode zones require Layer 2 address matching.
- C. Screens are not supported in transparent mode security zones.



D. All interfaces on the device must be configured with the ethernet-switching protocol family.

Correct Answer: A

---

### QUESTION 3

You are creating an IPS policy with multiple rules. You want traffic that matches rule 5 to silently be dropped, along with any future packets that match the appropriate attributes of the incoming traffic.

In this scenario, which ip-action parameter should you use?

- A. ip-block
- B. ip-close
- C. log-create
- D. timeout

Correct Answer: A

---

### QUESTION 4

You have configured a log collector VM and Security Director. System logging is enabled on a branch SRX Series device, but security logs do not appear in the monitor charts.

How would you solve this problem?

- A. Configure a security policy to forward logs to the collector.
- B. Configure application identification on the SRX Series device.
- C. Configure security logging on the SRX Series device.
- D. Configure J-Flow on the SRX Series device.

Correct Answer: C

---

### QUESTION 5

Click the Exhibit button.



```
<12>1 2016-02-18T01:32:50.391Z utm-srx550-b RT_UTM - WEBFILTER_URL_BLOCKED
[junos@2636.1.1.1.2.86 source-address="192.0.2.3" source-port="32056"
destination-address="198.51.100.2" destination-port="80" category="cat1"
reason="BY_BLACK_LIST" profile="uf1" url="www.example.com" obj="/"
username="N/A" roles="N/A] WebFilter: ACTION="URL Blocked" 192.0.2.3(32056) -
>198.51.100.2(80) CATEGORY="cat1" REASON="BY_BLACK_LIST" PROFILE="uf1"
URL=www.example.com OBJ=/ username N/A roles N/A
```

A customer submits a service ticket complaining that access to <http://www.example.com/> has been blocked.

Referring to the log message shown in the exhibit, why was access blocked?

- A. All illegal source port was utilized.
- B. The URI matched a profile entry.
- C. The user/role permissions were exceeded.
- D. There was a website category infraction.

Correct Answer: B

[Latest JN0-634 Dumps](#)

[JN0-634 Study Guide](#)

[JN0-634 Braindumps](#)