



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.passapply.com/jn0-636.html>

100% Passing Guarantee
100% Money Back Assurance

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

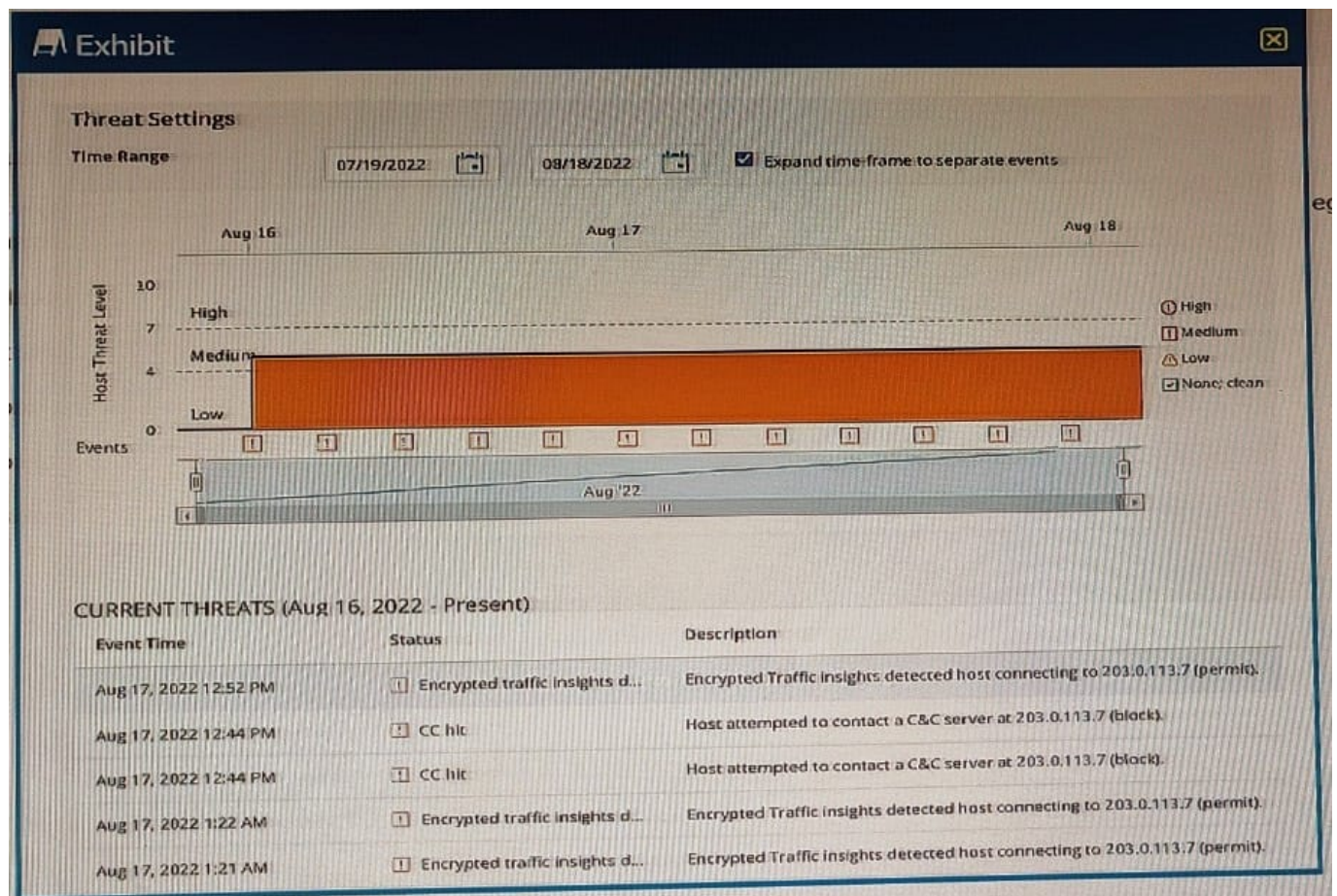
- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers





QUESTION 1

Exhibit You are using ATP Cloud and notice that there is a host with a high number of ETI and CandC hits sourced from the same investigation and notice that some of the events have not been automatically mitigated. Referring to the exhibit, what is a reason for this behavior?



- A. The CandC events are false positives.
- B. The infected host score is globally set below a threat level of 5.
- C. The infected host score is globally set above a threat level of 5.
- D. The ETI events are false positives.

Correct Answer: D

QUESTION 2

SRX Series device enrollment with Policy Enforcer fails To debug further, the user issues the following command show configuration services security--intelligence url

`https : //cloudfeeds . argon . juniperaecurity . net/api/manifeat. xml`



and receives the following output:

What is the problem in this scenario?

- A. The device is directly enrolled with Juniper ATP Cloud.
- B. The device is already enrolled with Policy Enforcer.
- C. The SRX Series device does not have a valid license.
- D. Junos Space does not have matching schema based on the

Correct Answer: C

QUESTION 3

While troubleshooting security policies, you added the count action. Where do you see the result of this action?

- A. In the show security policies hit-count command output.
- B. In the show security flow statistics command output.
- C. In the show security policies detail command output.
- D. In the show firewall log command output.

Correct Answer: A

QUESTION 4

Which two modes are supported on Juniper ATP Cloud? (Choose two.)

- A. global mode
- B. transparent mode
- C. private mode
- D. Layer 3 mode

Correct Answer: AC

Explanation: Juniper ATP Cloud supports two main modes of operation:

Global mode: In this mode, the Juniper ATP Cloud service analyzes all files and network traffic that pass through the cloud-based service. It uses a combination of static and dynamic analysis techniques, as well as machine learning, to detect

and block malicious files, even if they are not known to traditional anti-virus software. Private mode: In this mode, the Juniper ATP Cloud service analyzes only the files and network traffic that are specifically uploaded or submitted for analysis

by the user. It uses the same analysis techniques as in global mode, but the user has more control over which files and



network traffic are analyzed and can be used to analyze files that are behind the firewall.

QUESTION 5

Exhibit You have recently configured Adaptive Threat Profiling and notice 20 IP address entries in the monitoring section of the Juniper ATP Cloud portal that do not match the number of entries locally on the SRX Series device, as shown in the exhibit.

```
user@SRX> show service security-intelligence category summary
Category name      :SecProfiling
Status             :Enable
Description        :Security Profiling Data
Update interval    :300s
TTL                :172800s
Feed name          :Proxy_Nodes
Version            :20220812.1
Objects number:80
Create time        :2022-08-14 11:53:46 UTC
Update time        :2022-08-15 06:11:11 UTC
Update status      :Store succeeded
Expired            :No
Status             :Active
Options            :N/A
user@SRX> show security dynamic-address category-name SecProfiling feed-name
Proxy_Nodes
user@SRX>
```

What is the correct action to solve this problem on the SRX device?

- A. You must configure the DAE in a security policy on the SRX device.
- B. Refresh the feed in ATP Cloud.
- C. Force a manual download of the Proxy_Nodes feed.
- D. Flush the DNS cache on the SRX device.

Correct Answer: C

[Latest JN0-636 Dumps](#)

[JN0-636 PDF Dumps](#)

[JN0-636 VCE Dumps](#)