



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.geekcert.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

Your company uses non-Juniper firewalls and you are asked to provide a Juniper solution for zero-day malware protection. Which solution would work in this scenario?

- A. Juniper ATP Cloud
- B. Juniper Secure Analytics
- C. Juniper ATP Appliance
- D. Juniper Security Director

Correct Answer: A

Explanation: Juniper ATP Cloud provides zero-day malware protection for non-Juniper firewalls. It's a cloud-based service that analyzes files and network traffic to detect and prevent known and unknown (zero-day) threats. 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. It also provides real-time visibility and detailed forensics for incident response and remediation.

QUESTION 2

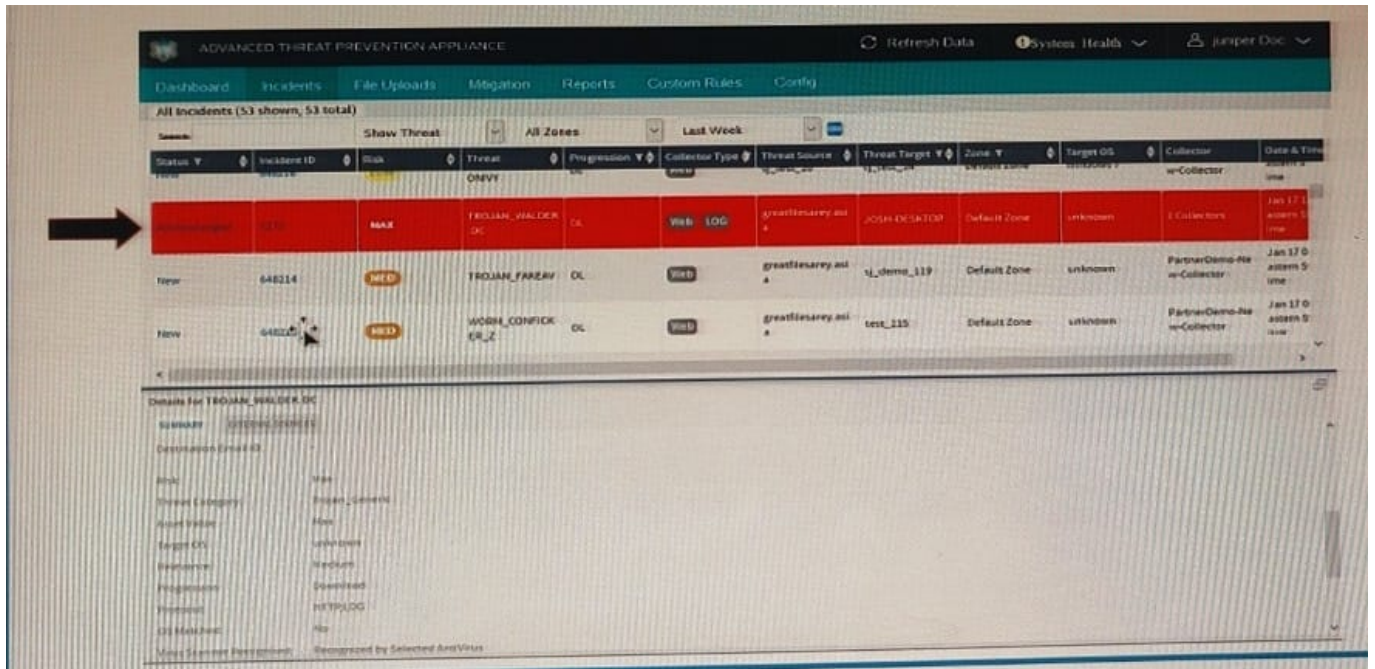
You want to identify potential threats within SSL-encrypted sessions without requiring SSL proxy to decrypt the session contents. Which security feature achieves this objective?

- A. infected host feeds
- B. encrypted traffic insights
- C. DNS security
- D. Secure Web Proxy

Correct Answer: C

QUESTION 3

Exhibit



The highlighted incident (arrow) shown in the exhibit shows a progression level of "Download" in the kill chain. What are two appropriate mitigation actions for the selected incident? (Choose two.)

- A. Immediate response required: Block malware IP addresses (download server or CnC server)
- B. Immediate response required: Wipe infected endpoint hosts.
- C. Immediate response required: Deploy IVP integration (if configured) to confirm if the endpoint has executed the malware and is infected.
- D. Not an urgent action: Use IVP to confirm if machine is infected.

Correct Answer: BD

QUESTION 4

Which two log format types are supported by the JATP appliance? (Choose two.)

- A. YAML
- B. XML
- C. CSV
- D. YANG

Correct Answer: BC

Explanation: https://www.juniper.net/documentation/en_US/release-independent/jatp/topics/topic-map/jatp-custom-log-ingestion.html



QUESTION 5

Exhibit

```
[edit security ike gateway advpn-gateway]
user@srx# show
ike-policy advpn-policy;
address 192.168.3.1;
local-identity distinguished-name;
remote-identity distinguished-name container O=Juniper;
external-interface ge-0/0/3.0;
version v2-only;
[edit interfaces]
user@srx# show st0
unit 0 {
    family inet {
        address 10.100.100.1/24;
    }
}
```

Referring to the exhibit, a spoke member of an ADVPN is not functioning correctly. Which two commands will solve this problem? (Choose two.)

- A.

```
[edit interfaces]
user@srx# set st0.0 multipoint
```
- B.

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

```
[edit security ike gateway advpn-gateway]
user@srx# set local-identity inet advpn
```
- D.

```
[edit security ike gateway advpn-gateway]
user@srx# set advpn partner disable
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Correct Answer: C



VCE & PDF

GeekCert.com

<https://www.geekcert.com/jn0-636.html>

2024 Latest geekcert JN0-636 PDF and VCE dumps Download

[Latest JN0-636 Dumps](#)

[JN0-636 VCE Dumps](#)

[JN0-636 Braindumps](#)