JN0-334 Q&As

Security-Specialist (JNCIS-SEC)

Pass Juniper JN0-334 Exam with 100% Guarantee

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

https://www.geekcert.com/jn0-334.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Click the Exhibit button.

```
user@srx> show configuration services
advanced-anti-malware {
  policy TPP {
    http {
      inspection-profile default profile;
      action block;
      notification {
        log;
      }
    }
    verdict-threshold 7;
    fallback-options {
      action permit;
      notification {
        log;
      }
    }
    default-notification {
        log;
    }
    whitelist-notification {
        log;
    }
    blacklist-notification {
        log;
    }
  }
}

user@srx> show configuration security policies
from-zone Client to-zone Internet {
  policy Rule-1 {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit (
        application-services {
          advanced-anti-malware-policy TPP;
        }
      }
    }
  }
}
```

You have deployed Sky ATP to protect your network from attacks so that users are unable to download malicious files. However, after a user attempts to download a malicious file, they are still able to communicate through the SRX Series device.

Referring to the exhibit, which statement is correct?

A. Change the security policy from a standard security policy to a unified security policy.

B. Remove the fallback options in the advanced anti-malware policy.

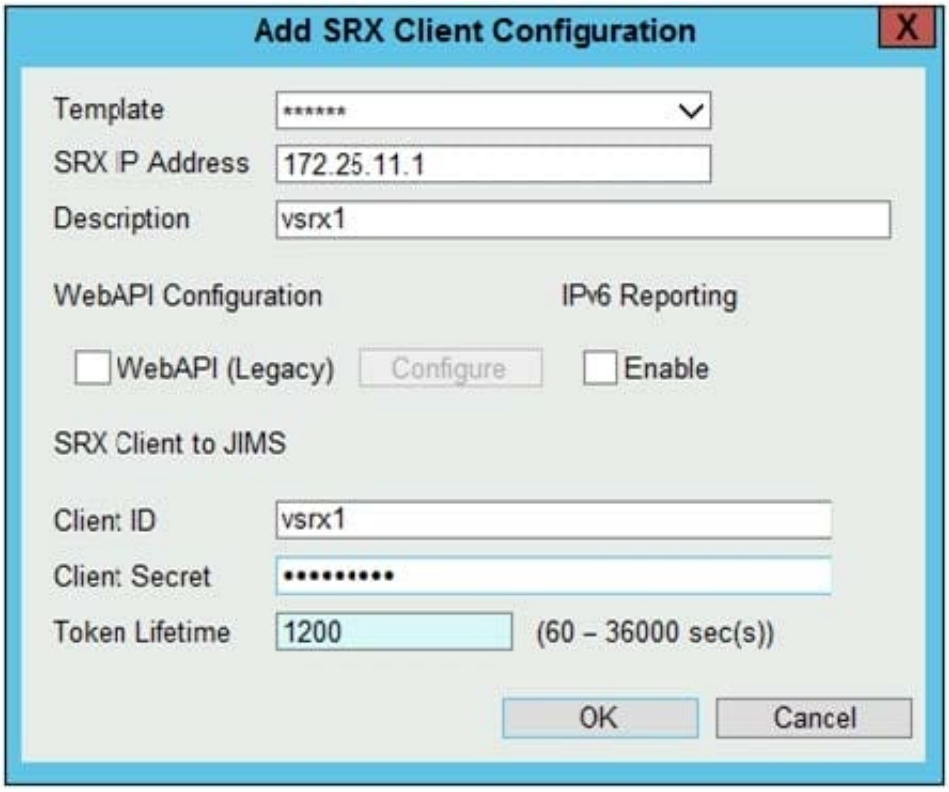
C. Configure a security intelligence policy and apply it to the security policy.

D. Lower the verdict threshold in the advanced anti-malware policy.

Correct Answer: C

QUESTION 2

Click the Exhibit button.



Referring to the exhibit, which two values in the JIMS SRX client configuration must match the values configured on the SRX client? (Choose two.)

A. IPv6 Reporting

B. Client ID

C. Client Secret

D. Token Lifetime

Correct Answer: BC

Reference: https://www.juniper.net/documentation/en_US/jims/topics/task/configuration/jims-srxconfiguring.html

QUESTION 3

You want to use Sky ATP to protect your network; however, company policy does not allow you to send any files to the cloud.

Which Sky ATP feature should you use in this situation?

A. Only use on-premises local Sky ATP server anti-malware file scanning.

B. Only use cloud-based Sky ATP file hash lookups.

C. Only use on-box SRX anti-malware file scanning.

D. Only use cloud-based Sky ATP file blacklists.

Correct Answer: B

QUESTION 4

You must block the lateral spread of Remote Administration Tools (RATs) that use SMB to propagate within the network, using the JATP solution.

Which action would accomplish this task?

A. Configure a new anti-virus configuration rule.

B. Configure whitelist rules

C. Configure YARA rules.

D. Configure the SAML settings.

Correct Answer: C

QUESTION 5

Click the Exhibit button.

```
user@srx> show security flow session
Session ID: 19068, Policy name: trust-to-untrust/15, Timeout: 1800, Valid
Resource information : FTP ALG, 1, 0
  In: 172.20.104.10/58479 --> 172.18.1.2/21;tcp, Conn Tag: 0x0, If: ge-0/0/3.0,
Pkts: 42, Bytes: 1796,
  Out: 172.18.1.2/21 --> 172.20.104.10/58479;tcp, Conn Tag: 0x0, If: ge-0/0/4.0,
Pkts: 43, Bytes: 2739,
```

Which two statements are true about the session shown in the exhibit? (Choose two.)

A. Two security policies are required for bidirectional traffic flow.

B. The ALG was enabled by manual configuration.

C. The ALG was enabled by default.

D. One security policy is required for bidirectional traffic flow.

Correct Answer: AB