Vendor: Juniper

Exam Code:JN0-634

Exam Name: Security, Professional (JNCIP-SEC)

Version: Demo

QUESTION 1

Which Junos security feature is used for signature-based attack prevention?

A. RADIUS

B. AppQoS

C. IPS

D. PIM

Correct Answer: C

QUESTION 2

SRX Series devices with AppSecure support which three custom signatures? (Choose three.)

A. MAC address-based mapping

B. latency detection mapping

C. IP protocol-based mapping

D. ICMP-based mapping

E. Layer 7-based signatures

Correct Answer: CDE

QUESTION 3

You have set up Sky ATP with the SRX Series devices in your network. However, your SRX Series devices are unable to communicate with the Sky ATP cloud because the communication is being blocked by a gateway network device.

Which two actions should you take to solve the problem? (Choose two.)

A. Open destination port 443 inbound from the Internet on the gateway network device.

B. Open destination port 8080 outbound from the Internet on the gateway network device.

C. Open destination port 443 outbound from the Internet on the gateway network device.

D. Open destination port 8080 inbound from the Internet on the gateway network device.

Correct Answer: CD

QUESTION 4

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

QUESTION 5

Click the Exhibit button.

```
[edit security policies global policy int-FW]
user@host# show
match {
     source-address any;
     destination-address any;
     application any;
}
then {
     permit;
}

user@host> show security user-identification local-authentication-table all

user@host>
```

You have configured integrated user firewall on the SRX Series devices in your network. However, you noticed that no users can access the servers that are behind the SRX Series devices.

Referring to the exhibit, what is the problem?

A. The Kerberos service is not configured correctly on the Active Directory server.

B. There are no authentication entries in the SRX Series device for the users.

C. The security policy on the SRX Series device is configured incorrectly.

D. The SAML service is not configured correctly on the Active Directory server.

Correct Answer: C

QUESTION 6

To which three UTM components would the custom-objects parameter apply? (Choose three.)

A. Sky ATP

B. antispam

C. content filtering

D. antivirus

E. Web filtering

Correct Answer: BCE

QUESTION 7

You are scanning files that are being transferred from the Internet to hosts on your internal network with Sky ATP. However, you notice that files that are 1 GB in size are not being scanned by Sky ATP.

In this scenario, which two statements are true? (Choose two.)

A. The Sky ATP failback option is set to permit.

B. The Sky ATP engine or the SRX Series device is too busy.

C. The 1 GB file size is larger than the scan size limit for Sky ATP.

D. The Sky ATP policy on the SRX Series device is misconfigured.

Correct Answer: CD

QUESTION 8

Using the Policy Controller API, which configuration would post Sky ATP with PE mode to the Policy Enforcer controller configuration?

"configs": {

A. "sdsn": false "cloudonly": true }

B. "configs": { "sdsn": false "cloud": false } "configs": {

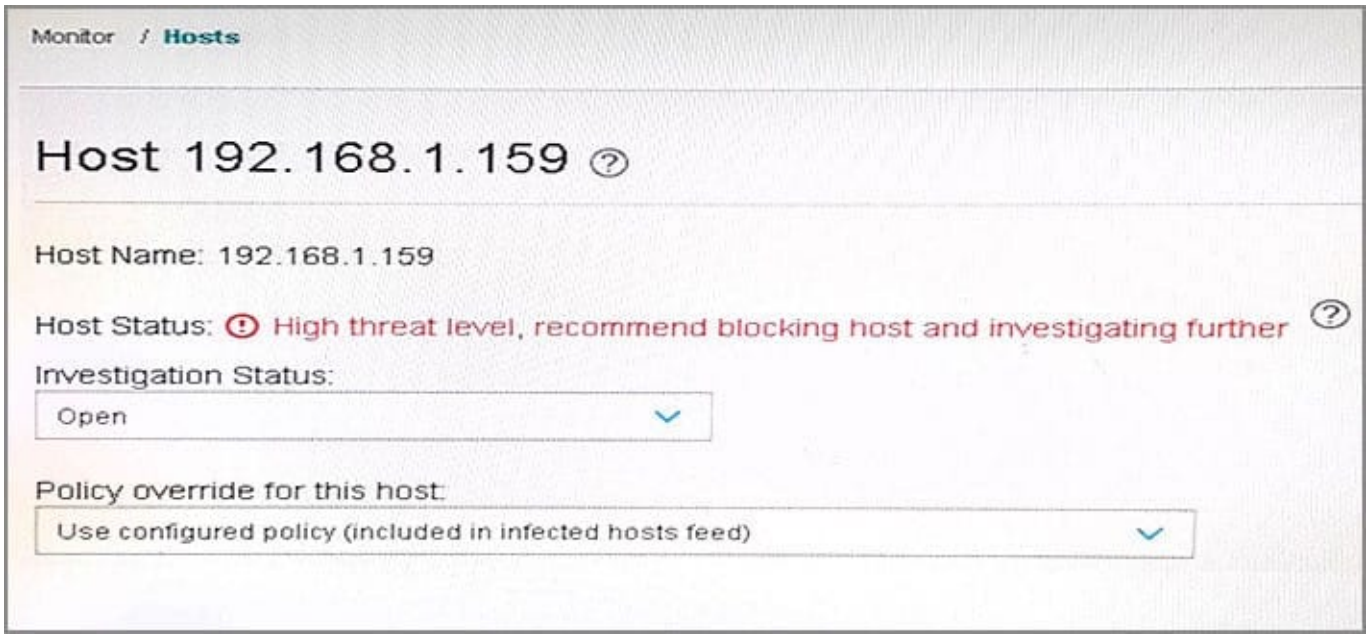
C. "sdsn": true "cloudonly": false }

D. "configs": { "sdsn": false "cloud": true }

Correct Answer: C

QUESTION 9

Click the Exhibit button.



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 10

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 11

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 12

You want to review AppTrack statistics to determine the characteristics of the traffic being monitored. Which operational mode command would accomplish this task on an SRX Series device?

A. show services application-identification statistics applications

B. show services application-identification application detail

C. show security application-tracking counters

D. show services security-intelligence statistics

Correct Answer: A