JN0-634 Q&As

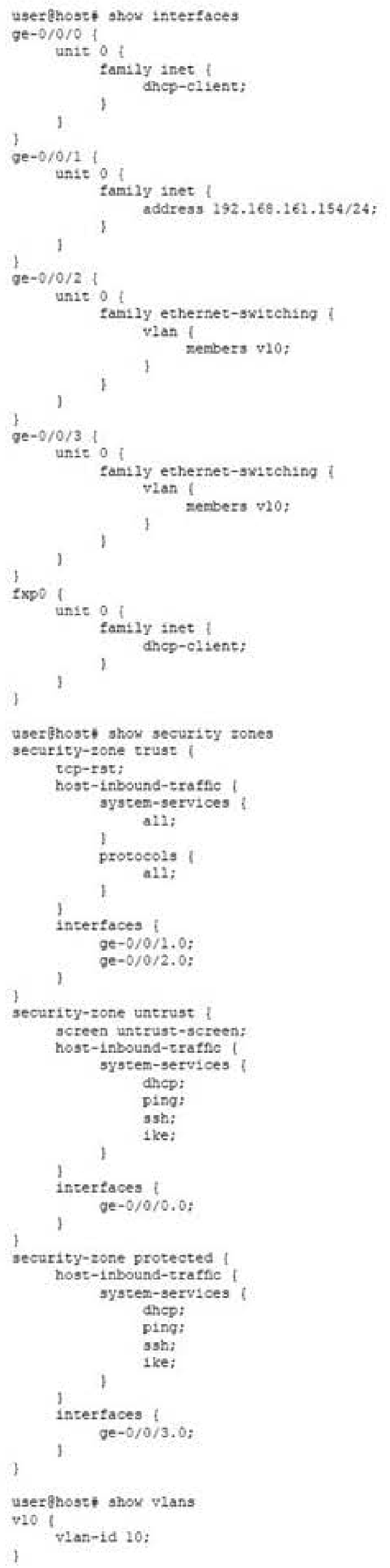
Security, Professional (JNCIP-SEC)

Pass Juniper JN0-634 Exam with 100% Guarantee

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

QUESTION 1

Click the Exhibit button.



```
user@host# show interfaces
ge-0/0/0 {
     unit 0 {
          family inet {
               dhcp-client;
          }
     }
}
ge-0/0/1 {
     unit 0 {
          family inet {
               address 192.168.161.154/24;
          }
     }
}
ge-0/0/2 {
     unit 0 {
          family ethernet-switching {
               vlan {
                    members v10;
               }
          }
     }
}
ge-0/0/3 {
     unit 0 {
          family ethernet-switching {
               vlan {
                    members v10;
               }
          }
     }
}
fxp0 {
     unit 0 {
          family inet {
               dhcp-client;
          }
     }
}

user@host# show security zones
security-zone trust {
     tcp-rst;
     host-inbound-traffic {
          system-services {
               all;
          }
          protocols {
               all;
          }
     }
     interfaces {
          ge-0/0/1.0;
          ge-0/0/2.0;
     }
}
security-zone untrust {
     screen untrust-screen;
     host-inbound-traffic {
          system-services {
               dhcp;
               ping;
               ssh;
               ike;
          }
     }
     interfaces {
          ge-0/0/0.0;
     }
}
security-zone protected {
     host-inbound-traffic {
          system-services {
               dhcp;
               ping;
               ssh;
               ike;
          }
     }
     interfaces {
          ge-0/0/3.0;
     }
}

user@host# show vlans
v10 {
     vlan-id 10;
}
```

You have enabled mixed mode on an SRX Series device. You are unable to commit the configuration shown in the exhibit.

What is the problem in this scenario?

A. A Layer 3 interface has not been configured on VLAN v10.

B. The trust zone cannot contain both Layer 2 and Layer 3 interfaces.

C. STP is not enabled under the host-inbound-traffic system services hierarchy on the trust and protected security zones.

D. An IRB interface has not been configured.

Correct Answer: B

QUESTION 2

The Software-Defined Secure Networks Policy Enforcer contains which two components? (Choose two.)

A. SRX Series device

B. Sky ATP

C. Policy Controller

D. Feed Connector

Correct Answer: CD

QUESTION 3

Your manager has identified that employees are spending too much time posting on a social media site. You are asked to block user from posting on this site, but they should still be able to access any other site on the Internet.

In this scenario, which AppSecure feature will accomplish this task?

A. AppQoS

B. AppTrack

C. APpFW

D. APBR

Correct Answer: C

QUESTION 4

Your network includes SRX Series devices at the headquarters location. The SRX Series devices at this location are part of a high availability chassis cluster and are configured for IPS. There has been a node failover.

In this scenario, which statement is true?

A. Existing sessions continue to be processed by IPS because of table synchronization.

B. Existing sessions are no longer processed by IPS and become firewall sessions.

C. Existing session continue to be processed by IPS as long as GRES is configured.

D. Existing sessions are dropped and must be reestablished so IPS processing can occur.

Correct Answer: A

QUESTION 5

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 6

Your network includes SRX Series devices at all headquarter, data center, and branch locations. The headquarter and data center locations use high-end SRX Series devices, and the branch locations use branch SRX Series devices. You are asked to deploy IPS on the SRX Series devices using one of the available IPS deployment modes.

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

A. Inline tap mode provides enforcement.

B. Inline tap mode can be used at all locations.

C. Integrated mode can be used at all locations.

D. Integrated mode provides enforcement.

Correct Answer: CD

QUESTION 7

Which AppSecure feature identifies applications that are present in traffic?

A. AppID

B. AppTrack

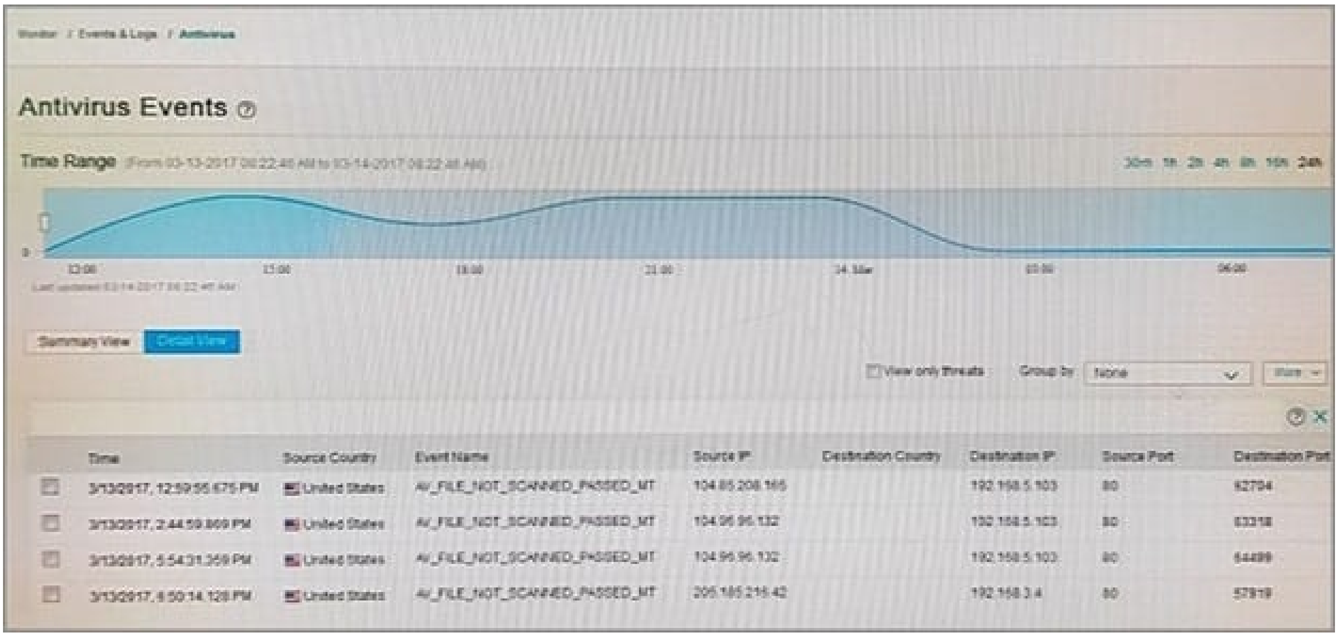
C. AppFW

D. AppQoS

Correct Answer: A

QUESTION 8

Click the Exhibit button.


Monitor / Events & Logs / Antivirus
Antivirus Events
Time Range (From 03-13-2017 08:22:46 AM to 03-14-2017 08:22:46 AM)
30m 1h 2h 4h 8h 16h 24h
0
12:00
15:00
18:00
21:00
14. Mar
03:00
06:00
Last updated 03-14-2017 08:22:46 AM
Summary View
Detail View
View only threats
Group by
None
More

	Time	Source Country	Event Name	Source IP	Destination Country	Destination IP	Source Port	Destination Port
□	3/13/2017, 12:59:55.675 PM	United States	AV_FILE_NOT_SCANNED_PASSED_MT	104.85.208.165		192.168.5.103	80	62704
□	3/13/2017, 2:44:59.869 PM	United States	AV_FILE_NOT_SCANNED_PASSED_MT	104.96.96.132		192.168.5.103	80	63318
□	3/13/2017, 5:54:31.359 PM	United States	AV_FILE_NOT_SCANNED_PASSED_MT	104.96.96.132		192.168.5.103	80	64489
□	3/13/2017, 6:50:14.128 PM	United States	AV_FILE_NOT_SCANNED_PASSED_MT	205.185.216.42		192.168.3.4	80	57919

Security Director is reporting the events shown in the exhibit.

If the fallback parameter is set to pass traffic, what would cause the events?

A. The files are too large for the antivirus engine to process.

B. The files are not scanned because they were permitted by a security policy.

C. The files are not scanned because they are the wrong file format.

D. The antivirus engine is unable to re-encrypt the files.

Correct Answer: A

QUESTION 9

Which three components are part of the AppSecure services suite? (Choose three.)

A. IDP

B. Sky ATP

C. AppQoS

D. AppFW

E. Web filtering

Correct Answer: ACD

QUESTION 10

After using Security Director to add a new firewall policy rule on an SRX Series device, you notice that the hit count on the policy is not increasing. Upon further investigation, you find that the devices listed in the new rule are able to communicate as expected. Your firewall policy consists of hundreds of rules.

Using only Security Director, how do you find the rule that is allowing the communication to occur in this scenario?

A. Generate a Top Firewall Rules report.

B. Generate a Policy Analysis report.

C. Generate a Top Source IPs report.

D. Generate a Top Firewall Events report.

Correct Answer: D

QUESTION 11

Which browser is supported by Security Director with Logging and Reporting?

A. Firefox

B. Agora

C. PowerBrowser

D. Mosaic

Correct Answer: A

QUESTION 12

What is the correct application mapping sequence when a user goes to Facebook for the first time through an SRX Series device?

A. first packet > process packet > check application system cache > classify application > process packet > match and identify application

B. first packet > check application system cache > process packet > classify application > match and identify application

C. first packet > check application system cache > classify application > process packet > match and identify application

D. first packet > process packet > check application system cache > classify application > match and identify application

Correct Answer: D

QUESTION 13

You are using IDP on your SRX Series device and are asked to ensure that the SRX Series device has the latest IDP database, as well as the latest application signature database.

In this scenario, which statement is true?

A. The application signature database cannot be updated on a device with the IDP database installed.

B. You must download each database separately.

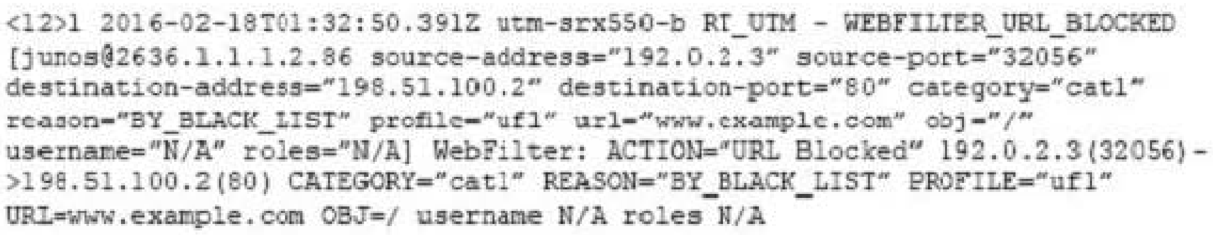
C. The IDP database includes the latest application signature database.

D. You must download the application signature database before installing the IDP database.

Correct Answer: C

QUESTION 14

Click the Exhibit button.



```
<12>1 2016-02-18T01:32:50.391Z utm-srx550-b RT_UTM - WEBFILIER_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.cxample.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 15

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