

100% Money Back
Guarantee

Vendor:Juniper

Exam Code:JN0-334

Exam Name:Security-Specialist (JNCIS-SEC)

Version:Demo

QUESTION 1

After performing a software upgrade on an SRX5800 chassis cluster, you notice that node1 is in the primary state and node0 is in the backup state. Your network standards dictate that node0 should be in the primary state.

In this scenario, which command should be used to comply with the network standards?

- A. request chassis cluster failover redundancy-group 254 node 1
- B. request chassis cluster failover redundancy-group 0 node 0
- C. request chassis cluster failover redundancy-group 254 mode 0
- D. request chassis cluster failover redundancy-group 0 node 1

Correct Answer: B

Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-chassis-clusterredundancy-group-failover.html

QUESTION 2

What are two types of attack objects used by IPS on SRX Series devices? (Choose two.)

- A. protocol anomaly-based attacks
- B. spam-based attacks
- C. signature-based attacks
- D. DDoS-based attacks

Correct Answer: AC

QUESTION 3

What is the correct step sequence used when Sky ATP analyzes a file?

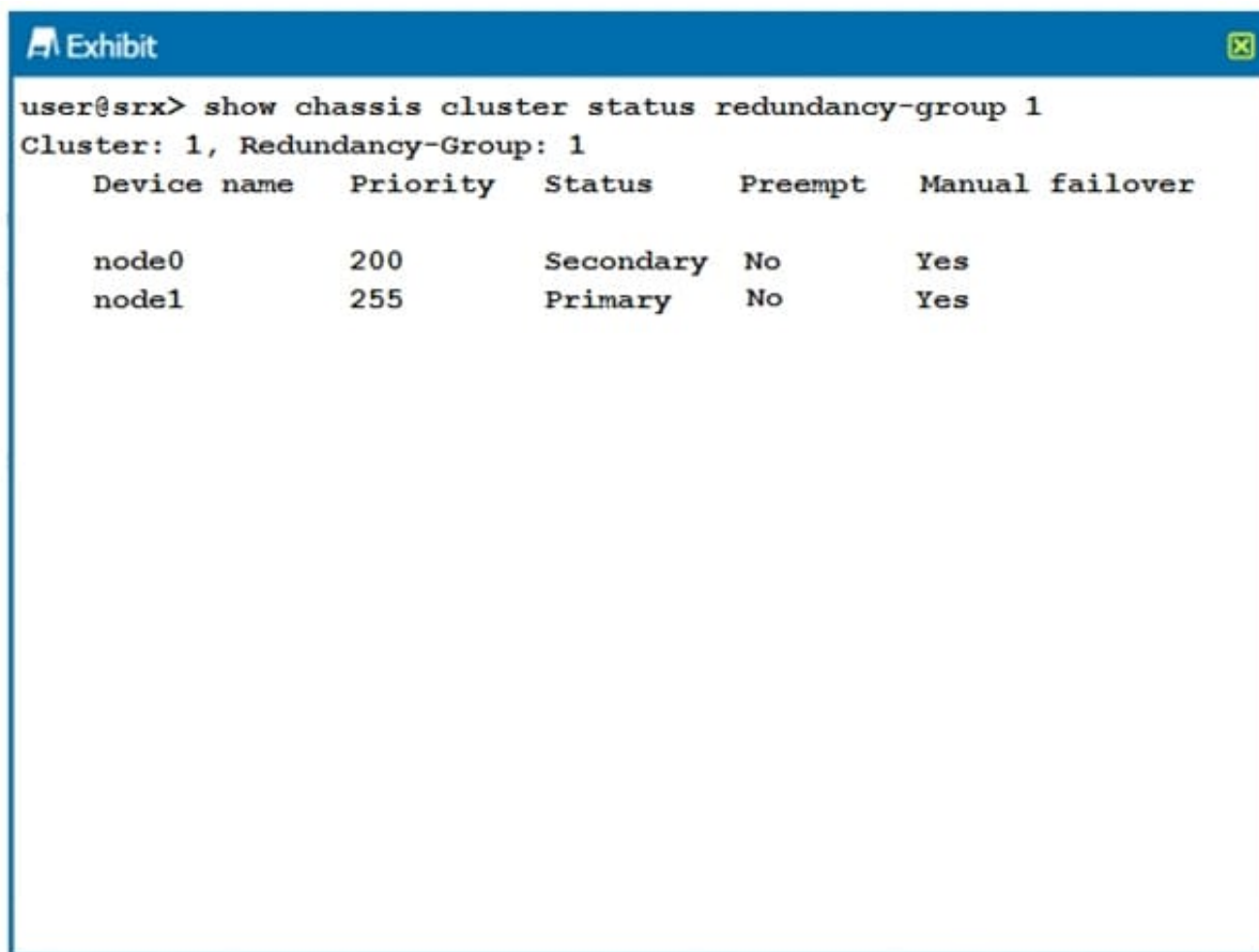
- A. static analysis -> cache lookup -> antivirus scanning -> dynamic analysis
- B. cache lookup -> static analysis -> antivirus scanning -> dynamic analysis
- C. cache lookup -> antivirus scanning -> static analysis -> dynamic analysis
- D. dynamic analysis -> static analysis -> antivirus scanning -> cache lookup

Correct Answer: C

Reference: https://www.juniper.net/documentation/en_US/release-independent/sky-atp/informationproducts/pathway-

QUESTION 4

Click the Exhibit button.



The exhibit shows a terminal window with a blue header bar labeled "Exhibit". The terminal prompt is "user@srx>". The command entered is "show chassis cluster status redundancy-group 1". The output is as follows:

```
Cluster: 1, Redundancy-Group: 1
  Device name  Priority  Status    Preempt  Manual failover
  node0       200     Secondary No        Yes
  node1       255     Primary  No        Yes
```

Which two statements describe the output shown in the exhibit? (Choose two.)

- A. Node 0 is passing traffic for redundancy group 1.
- B. Redundancy group 1 experienced an operational failure.
- C. Redundancy group 1 was administratively failed over.
- D. Node 1 is passing traffic for redundancy group1.

Correct Answer: CD

QUESTION 5

What are two valid JIMS event log sources? (Choose two.)

- A. Microsoft Windows Server 2012 audit logs
- B. Microsoft Active Directory server event logs
- C. Microsoft Exchange Server event logs
- D. Microsoft Active Directory audit logs

Correct Answer: BC

QUESTION 6

Which statement is true about JATP incidents?

- A. Incidents have an associated threat number assigned to them.
- B. Incidents are sorted by category, followed by severity.
- C. Incidents consist of all the events associated with a single threat.
- D. Incidents are always automatically mitigated.

Correct Answer: C

QUESTION 7

When working with network events on a Juniper Secure Analytics device, flow records come from which source?

- A. tap port
- B. SPAN
- C. switch
- D. mirror

Correct Answer: B

Reference: https://www.juniper.net/documentation/en_US/jsa7.3.1/jsa-arch-deployment-guide/topics/concept/jsa-ad-jsa-events-and-flows.html

QUESTION 8

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 9

You are configuring a client-protection SSL proxy profile. Which statement is correct in this scenario?

- A. A server certificate is not used but a root certificate authority is used.
- B. A server certificate and root certificate authority are not used.
- C. A server certificate is used but a root certificate authority is not used.
- D. A server certificate and a root certificate authority are both used.

Correct Answer: D

QUESTION 10

Click the Exhibit button.

```
[edit]
user@srx# show security idp
idp-policy base-policy {
    rulebase-exempt {
        rule R1 {
            match {
                from-zone trust;
                source-address internal-devices;
                to-zone any;
                destination-address any;
                attacks {
                    predefined-attacks FTP:USER:ROOT;
                }
            }
        }
    }
}
active-policy base-policy;
```

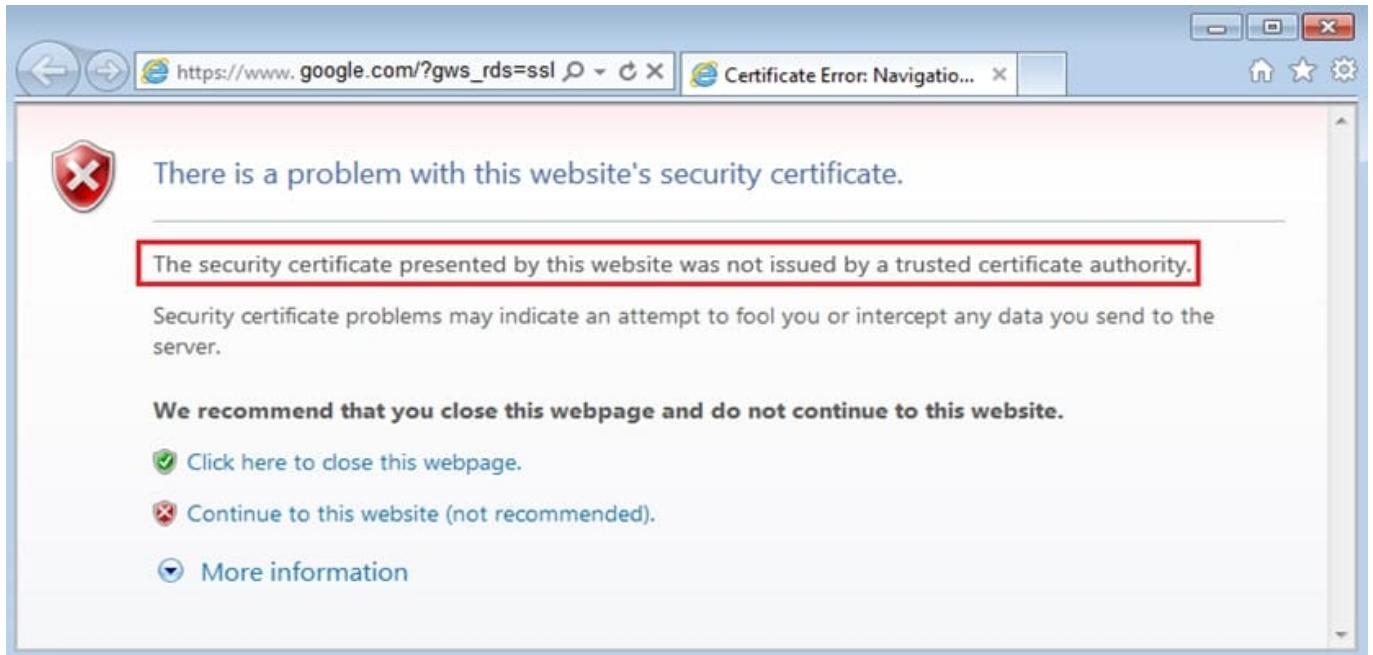
Referring to the exhibit, which statement is true?

- A. IDP blocks root users.
- B. IDP closes the connection on matched sessions.
- C. IDP ignores the connection on matched sessions.
- D. IDP blocks all users.

Correct Answer: C

QUESTION 11

Click the Exhibit button.



You have implemented SSL proxy client protection. After implementing this feature, your users are complaining about the warning message shown in the exhibit.

Which action must you perform to eliminate the warning message?

- A. Configure the SRX Series device as a trusted site in the client Web browsers.
- B. Regenerate the SRX self-signed CA certificate and include the correct organization name.
- C. Import the SRX self-signed CA certificate into the client Web browsers.
- D. Import the SRX self-signed CA certificate into the SRX certificate public store.

Correct Answer: C

QUESTION 12

Which feature is used when you want to permit traffic on an SRX Series device only at specific times?

- A. scheduler
- B. pass-through authentication
- C. ALGs
- D. counters

Correct Answer: A

