Free Questions for JN0-335 by vceexamstest

Shared by Bass on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Exhibit

Exhibit

```
[edit services ssl]
user@srx# commit
[edit services ssl proxy]
  'profile Server-Protect'
    Unsupported cert type of server certid: SSL-Proxy
error: configuration check-out failed
[edit services ssl]
user@srx#
```

When trying to set up a server protection SSL proxy, you receive the error shown. What are two reasons for this error? (Choose two.)

Options:

A- The SSL proxy certificate ID is part of a blocklist.

B- The SSL proxy certificate ID does not have the correct renegotiation option set.

C- The SSL proxy certificate ID is for a forwarding proxy.

D- The SSL proxy certificate ID does not exist.

Answer:

A, D

Explanation:

Two possible reasons for this error are that the SSL proxy certificate ID does not exist, or the SSL proxy certificate ID is part of a blocklist. If the SSL proxy certificate ID does not exist, you will need to generate a new certificate. If the SSL proxy certificate ID is part of a blocklist, you will need to contact the source of the blocklist to remove it. Additionally, you may need to check that the SSL proxy certificate ID has the correct renegotiation option set, as this is necessary for proper server protection. For more information, you can refer to the Juniper Security documentation athttps://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/security-ssl-proxy-configuration.html.

Question 2

Question Type: MultipleChoice

You are configuring logging for a security policy.

In this scenario, in which two situations would log entries be generated? (Choose two.)

Options:

A- every 10 minutes

B- at session initialization

C- every 60 seconds

D- at session close

Answer:

B, D

Explanation:

Log entries would be generated in two situations: at session initialization and at session close. At session initialization, the log entry would include details about the connection, such as the source and destination IP addresses, the service being used, and the action taken by the security policy. At session close, the log entry would include details about the connection, such as the duration of the session, the bytes sent/received, and the action taken by the security policy. For more information, you can refer to the Juniper Security documentation athttps://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/security-log-configuration.html.

Question 3

Question Type: MultipleChoice

Your company is using the Juniper ATP Cloud free model. The current inspection profile is set at 10 MB You are asked to configure ATP Cloud so that executable files up to 30 MB can be scanned while at the same time minimizing the change in scan time for other file types.

Which configuration should you use in this scenario?

Options:

A- Use the CLI to create a custom profile and increase the scan limit.

B- Use the ATP Cloud UI to change the default profile to increase the scan limit for all files to 30 MB.

C- Use the CLI to change the default profile to increase the scan limit for all files to 30 MB.

D- Use the ATP Cloud UI to update a custom profile and increase the scan limit for executable files to 30 MB.

Answer:

D

Explanation:

In this scenario, you should use the ATP Cloud UI to create a custom profile and update the scan limit for executable files to 30 MB. This will ensure that executable files up to 30 MB can be scanned, while at the same time minimizing the change in scan time for other file types. To do this, log in to the ATP Cloud UI and go to the Profiles tab. Click the Create button to create a new profile, and then adjust the scan limits for executable files to 30 MB. Once you have saved the custom profile, you can apply it to the desired systems and the new scan limit will be in effect.

Question 4

Question Type: **MultipleChoice**

Exhibit

Exhibit

```
user@SRX# show security policies
pre-id-default-policy {
log {
    session-init;
}
    then {
        session-timeout {
            tcp 30;
            udp 30;
            others 300;
        }
    }
}
```

Which two statements are correct about the configuration shown in the exhibit? (Choose two.)

Options:

A- The session-class parameter in only used when troubleshooting.

B- The others 300 parameter means unidentified traffic flows will be dropped in 300 milliseconds.

C- Every session that enters the SRX Series device will generate an event

D- Replacing the session-init parameter with session-lose will log unidentified flows.

Answer:

B, C

Explanation:

The configuration shown in the exhibit is for a Juniper SRX Series firewall. The session-init parameter is used to control how the firewall processes unknown traffic flows. With the session-init parameter set to 300, any traffic flows that the firewall does not recognize will be dropped after 300 milliseconds. Additionally, every session that enters the device, whether it is known or unknown, will generate an event, which can be used for logging and troubleshooting purposes. The session-lose parameter is used to control how the firewall handles established sessions that are terminated.

Question 5

Question Type: MultipleChoice

You are asked to find systems running applications that increase the risks on your network. You must ensure these systems are processed through IPS and Juniper ATP Cloud for malware and virus protection.

Which Juniper Networks solution will accomplish this task?

Options:

A- JIMS

B- Encrypted Traffic Insights

C- UTM

D- Adaptive Threat Profiling

Answer:

D

Explanation:

Adaptive Threat Profiling (ATP) is a Juniper Networks solution that enables organizations to detect malicious activity on their networks and process it through IPS and Juniper ATP Cloud for malware and virus protection. ATP is powered by Juniper's advanced Machine Learning and Artificial Intelligence (AI) capabilities, allowing it to detect and block malicious activity in real-time. ATP is integrated with Juniper's Unified Threat Management (UTM) and Encrypted Traffic Insights (ETI) solutions, providing an end-to-end network protection solution.

Question 6

Question Type: MultipleChoice

Which two statements are correct about JSA data collection? (Choose two.)

Options:

A- The Event Collector collects information using BGP FlowSpec.

B- The Flow Collector can use statistical sampling

C- The Flow Collector parses logs.

D- The Event Collector parses logs

Answer:

B, D

Explanation:

The Flow Collector can use statistical sampling to collect and store network flow data in the JSA database. The Event Collector collects information from various sources including syslog, SNMP, NetFlow, and BGP FlowSpec. Both the Flow Collector and the Event Collector parse logs to extract useful information from the logs.

Question 7

Question Type: MultipleChoice

You want to use IPS signatures to monitor traffic.

Which module in the AppSecure suite will help in this task?

Options:

A- AppTrack

B- AppQoS

C- AppFW

D- APPID

Answer:

C

Explanation:

The AppFW module in the AppSecure suite provides IPS signatures that can be used to monitor traffic and detect malicious activities. AppFW also provides other security controls such as Web application firewall, URL filtering, and application-level visibility.

Question 8

Question Type: MultipleChoice

Which two statements are correct about chassis clustering? (Choose two.)

Options:

A- The node ID value ranges from 1 to 255.

B- The node ID is used to identify each device in the chassis cluster.

C- A system reboot is required to activate changes to the cluster.

D- The cluster ID is used to identify each device in the chassis cluster.

Answer:

A, B

Explanation:

The node ID value ranges from 1 to 255 and is used to identify each device in the chassis cluster. The cluster ID is also used to identify each device, but it is not part of the node ID configuration. A system reboot is not required to activate changes to the cluster, but it is recommended to ensure that all changes are applied properly.

Question 9

Question Type: MultipleChoice

Which two statements are correct about SSL proxy server protection? (Choose two.)

Options:

A- You do not need to configure the servers to use the SSL proxy the function on the SRX Series device.

B- You must load the server certificates on the SRX Series device.

C- The servers must be configured to use the SSL proxy function on the SRX Series device.

D- You must import the root CA on the servers.

Answer:

B, C

Explanation:

You must load the server certificates on the SRX Series device and configure the servers to use the SSL proxy function on the SRX Series device. This is done to ensure that the SSL proxy is able to decrypt the traffic between the client and server. Additionally, you must import the root CA on the servers in order for the SSL proxy to properly validate the server certificate.

Question 10

Question Type: MultipleChoice

After JSA receives external events and flows, which two steps occur? (Choose two.)

Options:

A- After formatting the data, the data is stored in an asset database.

B- Before formatting the data, the data is analyzed for relevant information.

C- Before the information is filtered, the information is formatted

D- After the information is filtered, JSA responds with active measures

Answer:

B, C

Explanation:

Before formatting the data, the data is analyzed for relevant information. This is done to filter out any irrelevant data and to extract any useful information from the data. After the information is filtered, it is then formatted so that it can be stored in an asset database. After the data has been formatted, JSA will then respond with active measures.

Question 11

Question Type: MultipleChoice

Which two statements are true about the fab interface in a chassis cluster? (Choose two.)

Options:

A- The fab link does not support fragmentation.

B- The physical interface for the fab link must be specified in the configuration.

C- The fab link supports traditional interface features.

D- The Junos OS supports only one fab link.

Answer:

B, C

Explanation:

The physical interface for the fab link must be specified in the configuration. Additionally, the fab link supports traditional interface features such as MAC learning, security policy enforcement, and dynamic routing protocols. The fab link does not support fragmentation and the Junos OS supports up to two fab links.

Question 12

Question Type: MultipleChoice

Which method does the IoT Security feature use to identify traffic sourced from IoT devices?

Options:

A- The SRX Series device streams metadata from the IoT device transit traffic to Juniper ATP Cloud Juniper ATP Cloud.

B- The SRX Series device streams transit traffic received from the IoT device to Juniper ATP Cloud.

C- The SRX Series device identifies IoT devices using their MAC address.

D- The SRX Series device identifies IoT devices from metadata extracted from their transit traffic.

Answer:

D

Explanation:

The metadata is used to identify the type of device, its associated activities and its threat profile. This information is used to determine the appropriate security policy for the device. For more information on loT Security, please refer to the Juniper Security, Specialist (JNCIS-SEC) study guide.

To Get Premium Files for JN0-335 Visit

https://www.p2pexams.com/products/jn0-335

For More Free Questions Visit

https://www.p2pexams.com/juniper/pdf/jn0-335