Free Questions for JN0-335

Shared by Mills on 06-03-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

How does Juniper ATP Cloud protect a network from zero-day threats?

Options:

A- It uses a cache lookup.

B- It uses antivirus software.

C- It uses dynamic analysis.

D- It uses known virus signatures.

Answer:

C

Explanation:

Juniper ATP Cloud is a cloud-based service that provides advanced threat prevention and detection for your network. It integrates with SRX Series firewalls and MX Series routers to analyze files and network traffic for signs of malicious activity. Juniper ATP Cloud protects a network from zero-day threats by using dynamic analysis, which is a method of executing files in a sandbox environment and observing their behavior and network interactions. Dynamic analysis can uncover unknown malware that may evade static analysis or signature-based detection methods.

Question 2

Question Type: MultipleChoice

Which two sources are used by Juniper Identity Management Service (JIMS) for collecting username and device IP addresses? (Choose two.)

Options:

A- Microsoft Exchange Server event logs

B- DNS

C- Active Directory domain controller event logs

D- OpenLDAP service ports

Answer:

B, C

Explanation:

Juniper Identity Management Service (JIMS) collects username and device IP addresses from both DNS and Active Directory domain controller event logs. DNS is used to resolve hostnames to IP addresses, while Active Directory domain controller event logs are used to get information about user accounts, such as when they last logged in.

Question 3

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 4

Question Type: MultipleChoice

You want to control when cluster failovers occur.

In this scenario, which two specific parameters would you configure on an SRX Series device? (Choose two.)

Options:

A- hearcbeac-interval
B- heartbeac-address
C- hearcbeat-cos
D- hearcbeac-chreshold

Answer:

A, D

Explanation:

To control when cluster failovers occur, you need to configure two specific parameters on an SRX Series device: heartbeat-interval and heartbeat-threshold. These parameters determine how often the nodes in a cluster exchange heartbeat messages and how many consecutive heartbeats can be missed before a failover is triggered. The heartbeat-interval specifies the time interval in seconds between each heartbeat message. The default value is 1 second and the range is from 0.1 to 10 seconds. The heartbeat-threshold specifies the number of consecutive heartbeats that must be missed before a failover occurs. The default value is 3 and the range is from 2 to 255.Reference:=Configuring Chassis Clustering on SRX Series Devices,Chassis Cluster Redundancy Group Failover

Question 5

Question Type: MultipleChoice

You want to permit access to an application but block application sub-Which two security policy features provide this capability? (Choose two.)

Options:

A- URL filtering

B- micro application detection

C- content filtering

D- APPID

Answer:

A, B

Explanation:

The two security policy features that provide the capability to permit access to an application but block its sub-applications are URL filtering and micro application detection. URL filtering allows you to create policies that permit or block access to certain websites or webpages based on URL patterns. Micro application detection is a more sophisticated approach that can identify and block specific applications, even if they are embedded within other applications or websites. According to the Juniper Networks Certified Internet Specialist (JNCIS-SEC) Study Guide[1], ''micro application detection is the most accurate way to detect and control applications.'' Content filtering and APPID are more general approaches and are not as effective in providing the level of granularity needed to block sub-applications.

Question 6

Question Type: MultipleChoice

Which statement defines the function of an Application Layer Gateway (ALG)?

Options:

A- The ALG uses software processes for permitting or disallowing specific IP address ranges.

B- The ALG uses software that is used by a single TCP session using the same port numbers as the application.

C- The ALG contains protocols that use one application session for each TCP session.

D- The ALG uses software processes for managing specific protocols.

Answer:

D

Explanation:

The statement that defines the function of an Application Layer Gateway (ALG) is: The ALG uses software processes for managing specific protocols. An ALG is a security component that operates at the application layer (layer 7) of the OSI model and handles data associated with certain application protocols, such as SIP, FTP, RTSP, etc. An ALG acts as a proxy or intermediary between the client and the server applications and performs various functions, such as address and port translation, resource allocation, application response control, and synchronization of data and control traffic. An ALG can also inspect and modify the application payload to enable firewall or NAT traversal, prevent spoofing or DoS attacks, or enforce granular security policies based on application-specific commands.Reference:=Application-level gateway - Wikipedia,What Is an Application Layer Gateway (ALG)? | F5,What is ALG ** Application Layer Gateway | 3CX

Question 7

Question Type: MultipleChoice

On an SRX Series firewall, what are two ways that Encrypted Traffic Insights assess the threat of the traffic? (Choose two.)

Options:

A- It decrypts the file in a sandbox.

B- It validates the certificates used.

C- It decrypts the data to validate the hash.

D- It reviews the timing and frequency of the connections.

Answer:

B, D

Explanation:

Encrypted Traffic Insights is a feature that enables the SRX Series firewall and the ATP Cloud to detect malicious threats that are hidden in encrypted traffic without decrypting the traffic. It does so by analyzing the metadata and connection patterns of the encrypted sessions. Two ways that Encrypted Traffic Insights assess the threat of the traffic are:

It validates the certificates used: The SRX Series firewall extracts the server certificate from the encrypted session and compares its signature with a blocklist of known malicious certificates provided by ATP Cloud. If there is a match, the session is blocked and reported as a threat.

It reviews the timing and frequency of the connections: The SRX Series firewall sends the connection details, such as source and destination IP addresses, ports, protocols, and timestamps, to ATP Cloud. ATP Cloud applies behavior analysis and machine learning algorithms to detect anomalous or suspicious patterns of connections, such as high frequency, low duration, or unusual timing.