Free Questions for JN0-335 by braindumpscollection

Shared by Gonzales on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which two functions does Juniper ATP Cloud perform to reduce delays in the inspection of files? (Choose two.)

Options:

A- Juniper ATP Cloud allows the creation of allowlists.

B- Juniper ATP Cloud uses a single antivirus software package to analyze files.

C- Juniper ATP Cloud allows end users to bypass the inspection of files.

D- Juniper ATP Cloud performs a cache lookup on files.

Answer:

A, D

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. Two functions that Juniper

ATP Cloud performs to reduce delays in the inspection of files are:

Juniper ATP Cloud allows the creation of allowlists: Allowlists are lists of trusted files or file hashes that are excluded from scanning by Juniper ATP Cloud. You can create allowlists based on file name, file type, file size, file hash, or sender domain. By using allowlists, you can reduce the number of files that need to be uploaded to Juniper ATP Cloud for analysis and improve the performance and efficiency of your network.

Juniper ATP Cloud performs a cache lookup on files: Cache lookup is a process that checks if a file has been previously scanned by Juniper ATP Cloud and if there is a cached verdict for it. If there is a cached verdict, Juniper ATP Cloud returns it immediately without scanning the file again. If there is no cached verdict, Juniper ATP Cloud uploads the file for analysis. By using cache lookup, you can reduce the time and bandwidth required for scanning files by Juniper ATP Cloud.

Question 2

Question Type: MultipleChoice

You are implementing an SRX Series device at a branch office that has low bandwidth and also uses a cloud-based VoIP solution with an outbound policy that permits all traffic.

Which service would you implement at your edge device to prioritize VoIP traffic in this scenario?

Options:

A- AppFW

B- SIP ALG

C- AppQoE

D- AppQoS

Answer:

D

Explanation:

The service that you would implement at your edge device to prioritize VoIP traffic in this scenario is AppQoS. AppQoS is a feature that enables you to allocate bandwidth and prioritize traffic based on application signatures or custom rules. AppQoS can enhance the quality of service and experience for critical or latency-sensitive applications, such as VoIP. You can configure AppQoS policies to assign different classes of service (CoS) values or queue numbers to different applications or traffic flows. You can also define bandwidth limits, guarantees, or bursts for each class or queue.Reference:= [Application Quality of Service Overview], [Configuring Application Quality of Service]

Question 3

Question Type: MultipleChoice

You need to deploy an SRX Series device in your virtual environment.

In this scenario, what are two benefits of using a CSRX? (Choose two.)

Options:

A- The cSRX supports Layer 2 and Layer 3 deployments.

B- The cSRX default configuration contains three default zones: trust, untrust, and management.

C- The cSRX supports firewall, NAT, IPS, and UTM services.

D- The cSRX has low memory requirements.

Answer:

C, D

Explanation:

Two benefits of using a cSRX in your virtual environment are:

The cSRX supports firewall, NAT, IPS, and UTM services: The cSRX is a containerized version of the SRX Series firewall that runs as a Docker container on Linux hosts. It provides the same features and functionality as the SRX Series physical firewalls, such as firewall,

NAT, IPS, and UTM services. The cSRX can protect your virtual workloads and applications from various threats and attacks.

The cSRX has low memory requirements: The cSRX is designed to be lightweight and efficient, with low memory and CPU requirements. The cSRX can run on as little as 1 GB of RAM and 1 vCPU, making it suitable for resource-constrained environments.

Question 4

Question Type: MultipleChoice

You want to show tabular data for operational mode commands.

In this scenario, which logging parameter will provide this function?

Options:

A- permit

B- count

C- session-init

D- session-close

Answer:

B

Explanation:

The logging parameter that will provide the function of showing tabular data for operational mode commands is count. The count parameter displays the number of packets and bytes that match a security policy and the action taken by the policy. The count parameter can be used with the show security policies hit-count command to display the policy counters in a tabular format. The count parameter can also be used with the show security flow session command to display the session counters in a tabular format.Reference:=show security policies hit-count,show security flow session

Question 5

Question Type: MultipleChoice

Which sequence does an SRX Series device use when implementing stateful session security policies using Layer 3 routes?

Options:

A- An SRX Series device will perform a security policy search before conducting a longest-match Layer 3 route table lookup.

B- An SRX Series device performs a security policy search before implementing an ALG security check on the longest-match Layer 3 route.

C- An SRX Series device will conduct a longest-match Layer 3 route table lookup before performing a security policy search.

D- An SRX Series device conducts an ALG security check on the longest-match route before performing a security policy search.

Answer:

C

Explanation:

The sequence that an SRX Series device uses when implementing stateful session security policies using Layer 3 routes is:

An SRX Series device will conduct a longest-match Layer 3 route table lookup before performing a security policy search: When an SRX Series device receives a packet, it first looks up the destination IP address in the routing table and finds the longest matching route to forward the packet. Then, it performs a security policy search based on the source zone, destination zone, source address, destination address, protocol, and application of the packet. If there is a matching policy that allows the packet, it creates or updates a session entry for the packet and applies any security services configured in the policy.

Question 6

Question Type: MultipleChoice

Which two statements are true about application identification? (Choose two.)

Options:

A- Application identification can identity nested applications that are within Layer 7.

B- Application identification cannot identify nested applications that are within Layer 7.

C- Application signatures are the same as IDP signatures.

D- Application signatures are not the same as IDP signatures.

Answer:

A, D

Explanation:

Application identification is a feature that enables SRX Series devices to identify and classify network traffic based on application signatures or custom rules. Application identification can enhance security, visibility, and control over network applications. Two statements that are true about application identification are:

Application identification can identify nested applications that are within Layer 7: Nested applications are applications that run within another application protocol, such as HTTP or SSL. For example, Facebook or YouTube are nested applications within HTTP. Application identification can identify nested applications by inspecting the application payload and matching it against predefined or custom signatures.

Application signatures are not the same as IDP signatures: Application signatures are patterns of bytes or strings that uniquely identify an application protocol or a nested application. IDP signatures are patterns of bytes or strings that indicate an attack or an exploit against a vulnerability. Application signatures are used for application identification and classification, while IDP signatures are used for intrusion detection and prevention.

Question 7

Question Type: **MultipleChoice**

Which two statements are correct about a policy scheduler? (Choose two.)

Options:

A- A policy scheduler can only be applied when using the policy-rematch feature.

B- A policy scheduler can be dynamically activated based on traffic flow volumes.

C- A policy scheduler can be defined using a daily schedule.

D- A policy scheduler determines the time frame that a security policy is actively evaluated.

Answer:

C, D

Explanation:

A policy scheduler is a feature that allows a security policy to be activated or deactivated for a specified time period. You can define schedulers for a single or recurrent time slot within which a policy is active. Two statements that are correct about a policy scheduler are:

A policy scheduler can be defined using a daily schedule: You can configure a scheduler to be active every day for a certain time interval, such as from 8:00 AM to 5:00 PM. You can also exclude specific days from the daily schedule, such as weekends or holidays.

A policy scheduler determines the time frame that a security policy is actively evaluated: When you associate a scheduler with a security policy, the policy is only available for policy lookup during the time frame specified by the scheduler. When the scheduler is off, the policy is inactive and cannot be matched by any traffic.

Question 8

Question Type: MultipleChoice

On which three Hypervisors is vSRX supported? (Choose three.)

Options:

A- VMware ESXi

B- Citrix Hypervisor

C- Hyper-V

D- KVM

E- Oracle VM

Answer:

A, C, D

Explanation:

vSRX is a virtual firewall that runs as a software instance on a hypervisor. A hypervisor is a software layer that allows multiple virtual machines to run on a single physical host. vSRX supports three hypervisors: VMware ESXi, Hyper-V, and KVM. VMware ESXi is a hypervisor that runs on x86 servers and supports various operating systems and applications. Hyper-V is a hypervisor that runs on Windows Server and supports Windows and Linux virtual machines. KVM (Kernel-based Virtual Machine) is a hypervisor that runs on Linux and supports Linux, Windows, and other operating systems.