PassQueen
a.k.a dumpsqueen.com

Check Point Certified Maestro Expert

Checkpoint 156-835

Version Demo

Total Demo Questions: 9

Total Premium Questions: 94

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Splitter cannot be used _____.

A. To connect single port on orchestrator to multiple Appliances

B. To connect single port on Appliance to multiple ports on the orchestrator

C. To connect single port on orchestrator to the same Appliance

D. To connect single port on orchestrator to multiple port on external switch

ANSWER: B

Explanation:

The correct answer is “To connect single port on Appliance to multiple ports on the orchestrator”. In a Maestro deployment, a splitter is intended to fan out a connection from one Orchestrator port toward Security Appliance interfaces; it is not a device for combining or distributing one Appliance interface across multiple Orchestrator ports. The cabling model preserves a defined Orchestrator-to-Appliance relationship and the expected forwarding, redundancy, and interface-mapping behavior of the Maestro fabric. Therefore, the splitter’s supported direction is from the Orchestrator side to the Appliance side, rather than using one Appliance port as a source for several Orchestrator ports. This distinction matters when planning Security Group connectivity: the physical topology must follow the documented port mappings and use supported splitter-cable arrangements so that the Orchestrator can correctly identify and manage the connected appliance interfaces. Check Point’s Maestro documentation describes the platform architecture, Orchestrator role, and supported appliance connectivity model. See the Check Point Quantum Maestro overview and the Maestro Technical Guide.

QUESTION NO: 2

What is the purpose of g_tcpdump command?

A. Collects traffic dump from Sync network

B. The same as tcpdump, just on Scalable Platform

C. Collects traffic dump from CIN network

D. Collects traffic dump from all Active Appliances within Security Group

ANSWER: D

Explanation:

`g_tcpdump` is a Maestro Security Group diagnostic utility that initiates packet captures across the active Security Group Members simultaneously. This distributed capture is important because Maestro distributes connections among multiple appliances; examining traffic on only one member can miss the member that actually processed the connection. The command therefore provides a Security Group-wide view for troubleshooting packet flow, connectivity, and traffic-handling issues while maintaining the context of the individual active appliances. Its output identifies the appliance associated with captured packets, allowing an administrator to correlate a flow with the member processing it. The utility is effectively designed for coordinated, multi-member packet collection in a Maestro Security Group, rather than a capture limited to one dedicated network. Check Point documents `g_tcpdump` as a Maestro command for running `tcpdump` on the applicable active Security Group Members. See the Check Point Maestro Administration Guide: Using g_tcpdump and the Maestro Security Group monitoring documentation.

QUESTION NO: 3

Which Maestro internal networks must be isolated from ordinary production user traffic? Select all that apply.

A. Management network

B. Sync network

C. Chassis Internal Network (CIN)

D. Configured production uplink network

E. External routed VLAN carried through Security Group data ports

ANSWER: A B C

Explanation:

The Management network, Sync network, and Chassis Internal Network (CIN) serve Maestro control, management, and synchronization functions. They must be planned as internal infrastructure networks and not used as ordinary production transit paths. Production traffic should use the Security Group data interfaces and the designated Orchestrator uplink and downlink topology.

The Chassis Internal Network documentation describes the CIN role in a Maestro deployment.

QUESTION NO: 4

An appliance is being evaluated for use as a Maestro Security Group Member. Which interface capabilities are required for the applicable Maestro data interfaces? Select all that apply.

A. 10, 40, or 100 Gbps interface capability

B. Double VLAN tagging support

C. LLDP support

D. A 1 Gbps interface dedicated to production traffic

E. Fibre Channel support

ANSWER: A B C

Explanation:

Supported Maestro appliance interfaces require an applicable 10, 40, or 100 Gbps interface capability, support for double VLAN tagging, and LLDP support. These features are necessary for Maestro connectivity, topology discovery, and its traffic-forwarding design. A dedicated 1 Gbps production interface is not a substitute for a supported Maestro data interface.

Consult the official Check Point documentation portal and the hardware compatibility information for the precise appliance and release.

QUESTION NO: 5

What is the Iterator process?

A. Iterator is the process that simulates distribution in case of Appliance failure

B. Iterator is the process that follows Appliance recovery and simulates what the distribution would have been if the recovered Appliance had been alive.

C. Iterator is the process that runs on the Orchestrator and calculates a distribution in case of Appliance failure

D. Iterator is the process that runs on the Orchestrator and calculates a distribution in case of Appliance recovery

ANSWER: B

Explanation:

Iterator is the process that follows Appliance recovery and simulates what the distribution would have been if the recovered Appliance had been alive. In a Maestro deployment, appliance availability affects how Security Group Members are distributed across the available appliances. When an appliance returns to service, the system must evaluate the intended distribution state while accounting for the workload and member placement that continued during the outage. The Iterator process performs this recovery-oriented simulation so Maestro can determine the distribution that would have existed had the recovered appliance remained available. This supports an orderly return toward the appropriate operational distribution after recovery, rather than treating the event simply as a new failure calculation. Understanding this distinction is important for Maestro operations: Iterator is specifically associated with the recovery workflow and with modeling the expected distribution in the hypothetical state where the recovered appliance had not been unavailable. Check Point's Maestro documentation describes the platform's appliance and Security Group Member distribution architecture; consult the Maestro Administration Guide and the Check Point documentation portal for the release-specific recovery and distribution procedures.

QUESTION NO: 6

Which design practices improve hardware and path resiliency for a Security Group connected to two Maestro Orchestrators? Select all that apply.

A. Connect redundant appliance downlinks to separate Orchestrators

B. Connect redundant power supplies to independent power feeds

C. Use dedicated out-of-band management connectivity

D. Connect both redundant downlinks to the same Orchestrator

E. Use the Management network as a production transit network

ANSWER: A B C

Explanation:

Each Security Group Member should use redundant downlinks connected to separate Orchestrators so that the loss of one Orchestrator, cable, or connected path does not isolate the member. Redundant power supplies should use independent power feeds to avoid a shared upstream power failure. Dedicated out-of-band management provides an administrative path that is independent from production traffic connectivity.

Connecting both redundant links to ports on only one Orchestrator does not provide Orchestrator-level redundancy. Refer to the Check Point Quantum Maestro overview for Maestro scalability and resiliency architecture.

QUESTION NO: 7

An administrator needs to apply the same Gaia Clish command to every active Security Group Member from the Security Group context. Which Maestro utility is designed for this task?

A. `g_clish`

B. `g_all`

C. `asg perf`

D. `orchd restart`

ANSWER: A

Explanation:

`g_clish` distributes a specified Gaia Clish command to the active members of the current Security Group. This is appropriate for consistent interface, route, or other Gaia configuration tasks that must be performed on all active Security Group Members. `g_all` is instead a general remote-command utility and does not provide the Clish-specific workflow.

See the Check Point documentation portal for the Maestro administration guide applicable to the deployed release.

QUESTION NO: 8

What is the default range of physical ports for downlinks on Orchestrator MHO-170?

A. 3 - 16

B. 17 - 31

C. 25 - 32

D. 1 - 16

ANSWER: B

Explanation:

The default downlink physical-port range on an MHO-170 Orchestrator is **17 - 31**. Maestro uses predefined interface-role ranges on the Orchestrator so that initial Cabling and configuration follow a predictable topology. In the default MHO-170 layout, these ports are allocated for connections from the Orchestrator toward Security Group Members, which are the downlink-facing connections. This default assignment is important during initial deployment because it aligns the physical cabling model with Maestro's expected interface roles and enables consistent connectivity across the Security Group fabric. Administrators can validate the installed appliance's port layout and interface-role configuration before connecting uplinks and Security Group Members, particularly when adapting a deployment to a nonstandard design. The MHO-170 is part of Check Point's Maestro hyperscale platform; its appliance-specific interface mapping should be followed together with the applicable Maestro administration and hardware documentation. See Check Point's Maestro hyperscale network security overview and the Check Point Support Center for the current Maestro hardware documentation and deployment guidance.

QUESTION NO: 9

Which statements accurately describe the scale-out behavior of a Maestro Security Group? Select all that apply.

A. Members operate as one logical Security Group

B. Adding members can increase aggregate inspection capacity

C. The group uses a unified policy-management model

D. The Orchestrator becomes the policy-enforcement gateway

E. Each member requires an unrelated policy rulebase

ANSWER: A B C

Explanation:

A Security Group combines multiple Security Gateway appliances into one logical security system. Adding supported members can increase aggregate inspection capacity, subject to platform limits and actual traffic characteristics. The group uses a unified management and policy model, and remaining members can continue to provide service when a member becomes unavailable. The Orchestrator does not become a Security Gateway merely because additional members are added.

See the Maestro Administration Guide overview.