Get Free VMware 6V0-21.25 Dumps PDF Questions

Why risk failure? Download updated VMware vDefend Security for VCF 5.x Administrator exam PDF questions today. Practice with real 6V0-21.25 dumps and verified answers designed to help you ace your certification quickly using PrepBolt 6V0-21.25 exam pdf questions and answers.

Thank you for Downloading 6V0-21.25 exam PDF Demo

https://prepbolt.com/6V0-21.25.html

Question 1

Question Type: MultipleChoice

Which of the following is not an available option for membership criteria selection when creating group of type Antrea?

Options:

A- K8s Namespace
B- Antrea Egress
C- K8s NetworkPolicy
D- K8s Service

Answer:

C

Explanation:

When integrating Kubernetes via the Antrea CNI, vDefend allows administrators to dynamically group container workloads to apply broad security policies. You can group these workloads by native Kubernetes metadata attributes, specifically their K8s Namespace, the K8s Service they belong to, or their Antrea Egress IP bindings.

However, you cannot use a K8s NetworkPolicy as a grouping criterion. A NetworkPolicy is the actual security rule/enforcement intent applied to the pods, not an identity attribute or label of the pod itself. Grouping by a rule to apply another rule creates a logical conflict, so it is not an available option in the vDefend UI.

Question 2

Question Type: MultipleChoice

Which of the following is NOT a feature of the VMware vDefend Gateway Firewall?

Options:

A- Implemented on Edge Node

B- Layer 7 APP-ID
C- Guest Introspection
D- TLS Decryption

Answer:

C

Explanation:

To answer this, you must separate Gateway features (perimeter) from Distributed features (hypervisor).

Guest Introspection (Option C) is an API framework that uses VMware Tools to look inside the Guest Operating System of a Virtual Machine (used for Identity Firewall user logons or agentless Anti-Virus). Because it interacts directly with the local VM OS, it is strictly a Distributed/Hypervisor-level feature.

The Gateway Firewall sits far away on the Edge Node (Option A). It does not have Guest Introspection capabilities because it cannot directly talk to the OS of a VM. Instead, it relies on network-level features like Layer 7 App-ID (Option B) and TLS Decryption (Option D) to secure North-South traffic.

==========

Question 3

Question Type: MultipleChoice

vDefend firewall provides support to VMs connected to which of the following?

Options:

A- VMs connected to Overlay Networks
B- VMs connected to VLAN Networks
C- VMs connected to DvPG Networks
D- All of the above

Answer:

D

Explanation:

A massive architectural advantage of the VMware vDefend Distributed Firewall (DFW) is that its enforcement mechanism is entirely decoupled from the underlying network topology. Because the firewall rules are enforced directly at the hypervisor kernel level (specifically at the virtual NIC of the VM) before the traffic even hits the virtual switch, it is completely agnostic to how that traffic is eventually transported.

Therefore, DFW seamlessly supports and protects VMs whether they are connected to modern NSX Geneve Overlay Networks, traditional NSX-backed VLAN Networks, or even standard vSphere Distributed Port Groups (DvPG Networks) that have no routing overlay.

==========

Question 4

Question Type: MultipleChoice

If you want to run Gateway IDS/IPS, what is the minimum Edge Form Factor size supported to run this feature?

Options:

A- Medium
B- X-Large
C- Small
D- Large

Answer:

D

Explanation:

Gateway IDS/IPS is an incredibly resource-intensive service. Unlike basic stateful firewall rules that just check IP headers and ports, Gateway IDS/IPS performs complex Deep Packet Inspection (DPI) against thousands of threat signatures for heavy North-South perimeter traffic. Furthermore, it often handles TLS Inspection (Decryption), which requires massive CPU and memory allocations.

Because of these heavy computational requirements, VMware restricts the deployment of Gateway IDS/IPS to Edge Nodes deployed with a minimum form factor size of Large. Deploying this service on Small or Medium Edge nodes is unsupported, as they lack the compute resources and would immediately bottleneck data center traffic.

==========

Question 5

Question Type: MultipleChoice

Which one of the following is NOT one of the use-cases of Distributed Intrusion Detection and Prevention?

Options:

A- Provide routing capability for an air-gapped network to securely access the internet
B- Enable software-based IDS/IPS for Critical applications
C- Prevent lateral movement of attackers by blocking vulnerabilities
D- Achieve regulatory compliance requirements for PCI-DSS, HIPAA, SOX

Answer:

A

Explanation:

VMware vDefend Distributed IDS/IPS is a highly specialized, software-based inspection engine designed specifically to detect and block malicious payloads (exploits) moving laterally (East-West) between virtual machines. Because it operates at the vNIC level, it is perfect for achieving regulatory compliance (Option D), protecting critical internal apps (Option B), and stopping lateral movement (Option C).

However, it is not a router. Providing internet access routing to an air-gapped network is a fundamental routing and NAT function (typically handled by a Tier-0/Tier-1 Gateway or a physical perimeter firewall), completely unrelated to the Deep Packet Inspection signature-matching functions of the Distributed IDS engine.

==========

Thank You for trying 6V0-21.25 PDF Demo

To try our 6V0-21.25 practice exam software visit link below

https://prepbolt.com/6V0-21.25.html

Start Your 6V0-21.25 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your 6V0-21.25 preparation with actual exam questions.