VMware

6V0-21.25

VMware vDefend Security for VCF 5.x Administrator

Questions & Answers (Demo)

Version: 4.0

Question: 1

The VMware vDefend Management cluster is deployed by default with how many nodes?

A. One

B. Two

C. Three

D. Four

Answer: C

Explanation:

VMware vDefend (formerly NSX) architecture utilizes a Management Plane that is highly available. For production environments, the NSX Management cluster is deployed with exactly three nodes. This ensures high availability (HA) and fault tolerance for the management and control planes. If one node fails, the cluster maintains quorum and operations continue uninterrupted. While a single node can be deployed for lab or proof-of-concept environments, the default standard for a highly available production cluster is three nodes.

Question: 2

What would best describe DGA activity?

A. Trying to connect to randomly generated domains to obfuscate C2 traffic

B. Intercepting packets to steal sensitive data

C. Logging keystrokes to capture user credentials

D. Exploiting vulnerabilities in web applications through SQL injection

Answer: A

Explanation:

DGA stands for Domain Generation Algorithm. It is a technique used by malware (such as ransomware or botnets) to periodically generate a large number of domain names that serve as rendezvous points with their Command and Control (C2) servers. By rapidly changing the domains they attempt to connect to, attackers obfuscate their traffic and make it highly difficult for static blocklists or basic firewall rules to stop the communication. VMware vDefend's Network Traffic Analysis (NTA) features specific detectors to identify this anomalous DNS behavior associated with DGA.

Question: 3

Which of the following does the Applied To field impact?

A. Per VM vNIC rule count

B. System wide rule count

C. ESX host rule count

D. NSX Manager rule count

Answer: A

Explanation:

In the VMware vDefend Distributed Firewall (DFW), the "Applied To" field is a critical optimization feature. By default, DFW rules are applied to all workloads (Applied To: DFW). However, when you specify specific groups in the "Applied To" field, the rule is only pushed down to the specific vNICs of the virtual machines residing in those groups. This drastically reduces the size of the rule table maintained in memory on the ESXi host for each specific vNIC (the per VM vNIC rule count), improving hypervisor performance and ensuring that workloads only process rules relevant to their network traffic.

Question: 4

Which of the following are optional CNI Plugin functionalities? (Select all that apply)

A. East-West service load balancing

B. Pod network connectivity

C. NetworkPolicy enforcement

D. IP address management (IPAM)

Answer: A, C, D

Explanation:

When integrating container orchestration (like Kubernetes) with VMware vDefend, a Container Network Interface (CNI) plugin (such as Antrea) is utilized. The fundamental, non-optional requirement of a CNI is providing basic pod network connectivity (Option B). However, advanced features like East-West service load balancing (kube-proxy replacement), enforcing Kubernetes NetworkPolicies (security), and handling IP Address Management (IPAM) are considered optional or configurable functionalities depending on the specific CNI implementation and how the cluster is architected to integrate with vDefend.

Question: 5

Which of the following are vDefend Advanced Threat Prevention capabilities? (Select all that apply)

A. Intrusion Detection/Protection Systems (IDS/IPS)

B. Network Traffic Analysis (NTA)

C. Gateway Firewall

D. Network Detection and Response (NDR)

E. Malware Analysis/Sandboxing

Answer: A, B, D, E

Explanation:

VMware vDefend Advanced Threat Prevention (ATP) is a suite of security features designed to move beyond traditional L4-L7 stateful firewalling. It specifically encompasses advanced inspection and anomaly detection tools. These include Distributed and Gateway IDS/IPS (signature-based threat detection), Network Traffic Analysis (NTA - behavioral anomaly detection), Network Detection and Response (NDR - correlating events into actionable campaigns/incidents), and Malware Prevention (which includes file extraction, static analysis, and dynamic sandboxing). The Gateway Firewall (Option C) is considered a foundational firewalling capability rather than an "Advanced Threat Prevention" specific feature.