Vendor: VMware

Exam Code: 6V0-21.25

Exam Name: VMware vDefend Security for VCF 5.x Administrator

Version: DEMO

QUESTION 1
Which following roles are pre-configured in roles and cannot be modified? (Select all that apply)

A. Principal Identity Users
B. External Users
C. Local Users
D. Admin
E. Guest Users
F. Audit
G. Analyst

Answer: DF
Explanation:
In VMware vDefend (NSX), Role-Based Access Control (RBAC) is foundational for securing the management plane and ensuring that users only have the permissions necessary to perform their jobs (the principle of least privilege). The system ships with several built-in roles out-of-the-box.

The Admin (often referred to as Enterprise Admin) and Audit roles are hardcoded, immutable system roles. They are pre-configured to ensure there is always a guaranteed, tamper-proof baseline for system administration and compliance auditing.

The Admin Role: This is the highest level of privilege in the system. It grants full read and write access to every configuration, policy, and system setting within the vDefend environment. Broadcom locks this role to prevent accidental demotion or modification that could potentially lock legitimate administrators out of the system or break underlying integrations (like vCenter or VCF).

The Audit Role: This is a strict read-only role designed exclusively for compliance officers and security auditors. It allows a user to view configurations, logs, and security policies without any ability to make changes. This role is immutable to guarantee to compliance regulatory bodies that the auditor has unimpeded, read-only visibility that cannot be silently modified or restricted by a rogue administrator.

QUESTION 2
In vDefend Malware Detection and Prevention, what technology is the sandbox built on?

A. VMware virtualization
B. Full System Emulation
C. KVM virtualization
D. Dedicated physical hardware

Answer: B
Explanation:
When a file is flagged as suspicious and sent to the vDefend Advanced Threat Prevention (ATP) cloud for dynamic analysis, it is placed inside a sandbox. The sandbox utilized by VMware vDefend is built on Full System Emulation (FSE), a custom architectural approach originally developed by Lastline (which VMware acquired).

This is a critical distinction from traditional sandboxes. Modern, evasive malware is often "sandbox-aware." It will check its environment to see if it is running inside a standard commercial hypervisor (like standard VMware ESXi, Hyper-V, or KVM). If the malware detects virtualization tools, specific drivers, or CPU flags associated with standard hypervisors, it will remain dormant to avoid detection.

Full System Emulation circumvents this by emulating the entire hardware stack--including the CPU, memory, and peripherals--in software. This means the malware cannot detect that it is being watched. Furthermore, because the emulator acts as the virtual CPU, it has visibility into every single instruction the malware attempts to execute and every memory location it attempts to access. This allows vDefend to detect malicious intent even if the malware uses zero-day exploits, highly obfuscated code, or fileless memory techniques.

QUESTION 3
Which vDefend Gateway Firewall feature is ONLY supported on T1 Gateways?

A. Gateway IDRS
B. Stateful Services on A/A Gateways
C. Gateway IDFW
D. L3/L4 Gateway Firewall

Answer: C
Explanation:
In the vDefend routing and security architecture, there is a two-tiered gateway system: Tier-0 (T0) and Tier-1 (T1). Tier-0 gateways handle North-South traffic leaving the data center to the physical network, while Tier-1 gateways handle East-West routing between tenant applications or specific segments.

Gateway Identity Firewall (Gateway IDFW) is a feature that allows administrators to create firewall rules based on Active Directory user identities rather than just IP addresses, but applied at the perimeter of a tenant or application zone. This feature is exclusively supported on Tier-1 Gateways.

The architectural reasoning behind this limitation is proximity to the workload. Tier-1 gateways are deployed closer to the application segments and act as the direct default gateways for the Virtual Machines or Virtual Desktop Infrastructure (VDI) instances where user logins occur. By placing the Identity Firewall enforcement at the T1 layer, vDefend can accurately map user login contexts (via Active Directory and VMware Tools) to specific application zones before the traffic ever reaches the centralized Tier-0 gateway, ensuring granular, tenant-specific, identity-based perimeter security.

QUESTION 4
What best describes an incident in vDefend NDR?

A. It always consists of a single event
B. It may consist of a single event or a number of events that have been correlated
C. It always consists of multiple correlated events
D. An incident always begins and ends with multiple correlated events

Answer: B
Explanation:
To understand Network Detection and Response (NDR), you must understand the hierarchy of security telemetry: Events, Incidents, and Campaigns.

An Event is a single anomaly or triggered detector (e.g., an IDS signature matching, or NTA noticing an unusual DNS query).

An Incident is a formalized alert presented to the security analyst in the NDR dashboard, indicating an actual threat that requires investigation.

While the primary power of vDefend NDR is its Artificial Intelligence engine--which correlates multiple seemingly low-level events (like a port scan followed by a suspicious file download and lateral movement) into a single, high-confidence Incident--an Incident does not strictly require multiple events.

If a single, highly critical event occurs--such as the Malware Prevention engine definitively detonating and confirming a severe piece of zero-day ransomware--the NDR engine will immediately escalate that single event into a full-blown Incident. Therefore, an incident may consist of just one highly critical event, or dozens of lower-level events correlated together over time.

QUESTION 5
Which of the following components can enforce Layer 7 Context Firewall Rules? (Select all that apply)

A. Distributed Firewall
B. Tier 1 Gateway
C. Tier 0 Gateway
D. VMK Interface

Answer: ABC
Explanation:
Layer 7 Context-Aware Firewalling goes beyond traditional Layer 3 (IP Address) and Layer 4 (Port/Protocol) filtering. It involves Deep Packet Inspection (DPI) to identify the actual application (App-ID), URL, or Fully Qualified Domain Name (FQDN) being used (e.g., distinguishing between standard web browsing and an unauthorized file transfer over the same HTTPS port 443).

VMware vDefend is highly versatile and can enforce these advanced Layer 7 context rules across multiple enforcement points in the data center:

Distributed Firewall (DFW) (Option A): Enforces L7 rules directly at the vNIC of the virtual machine. This is ideal for East-West micro-segmentation, stopping a compromised VM from communicating with another VM via an unauthorized application protocol.

Tier-1 Gateway (Option B): Enforces L7 rules at the tenant or application boundary. This is ideal for protecting a specific application zone from other zones within the data center.

Tier-0 Gateway (Option C): Enforces L7 rules at the main edge of the data center. This acts as the primary North-South perimeter firewall, inspecting traffic entering or leaving the physical network.

QUESTION 6
Which statements are true for DFW and Rule processing order based on the information shown in the image? (Select all that apply)

```
[root@vesxi-nsxt-10:~] vsipioctl getconfig -f nic-2292571-eth0-vmware-sfw.2

ruleset mains {

# generation number: 0
```

```
# realization time : 2020-05-21T13:01:48

# FILTER rules

rule 1596 at 1 inout protocol tcp from addrset e70a9a79-c346-48c4-8b9d-
402e97e38a7c to addrset be665396-14d9-4ee4-98b9-9c21ebfl27a port 464
accept;

rule 1596 at 2 inout protocol udp from addrset e70a9a79-c346-48c4-8b9d-
402e97e38a7c to addrset be665396-14d9-4ee4-98b9-9c21ebfl27a port 464
accept;

rule 1595 at 3 inout protocol udp from addrset e70a9a79-c346-48c4-8b9d-
402e97e38a7c to addrset 9edl2e5f-36f4-42a9-a79b-87efc243alef port 53
accept;

rule 1594 at 4 inout protocol udp from addrset e70a9a79-c346-48c4-8b9d-
402e97e38a7c to addrset 59e6aa90-e360-4341-9fb3-b312772b79fb port 123
accept;

rule 2 at 5 inout protocol any from any to any accept;

}
```

A. Rule 1595 will be processed before rule 1596
B. Rule 1594 will be processed after 1595 and 1596
C. Rule 1596 will be the first one to be processed
D. Rule 2 will only be processed if the conditions for the above rules are not met

Answer: BCD
Explanation:
When troubleshooting Distributed Firewall (DFW) enforcement directly on an ESXi host via the CLI, administrators use the vsipioctl command to view the actual data plane rules mapped to a specific VM's virtual NIC.

In the output provided, the at X statement strictly dictates the top-to-bottom processing order established by the hypervisor kernel:

Option B is True: Rule 1594 is explicitly designated at 4. Therefore, it will process sequentially after rules 1596 (which are at 1 and at 2) and rule 1595 (which is at 3).

Option C is True: Rule 1596 is designated at 1, meaning it is at the very top of the ruleset sequence and will be evaluated against the traffic packet first.

Option D is True: Rule 2 is designated at 5 and uses the logic any from any to any. This makes it the "catch-all" or default rule at the very bottom of the data plane flow table. The vNIC will only evaluate and hit this rule if the traffic packet fails to match the specific conditions of rules 1 through 4.

QUESTION 7
Which of the following are true regarding Antrea? (Select all that apply)

A. Antrea Agent runs on every Worker Node
B. Antrea integration allows support of mixed rules of Virtual Machines and Kubernetes objects

C. Antrea Agent computes NetworkPolicies from K8s and publishes the results to the Antrea Controller
D. Antrea Agent runs on every node of the management cluster

Answer: AB
Explanation:
Antrea is VMware's Kubernetes-native Container Network Interface (CNI) utilized for micro-segmenting container pods.

Option A is True: Architecturally, Antrea deploys an antrea-agent component on every single Kubernetes Worker Node (typically as a DaemonSet). This agent is responsible for programming the Open vSwitch (OVS) datapath on that specific node to enforce pod routing and security policies.

Option B is True: A massive advantage of integrating Antrea with vDefend (NSX) is unified security. The vDefend management plane synchronizes Kubernetes inventory (Pods, Namespaces). This allows security administrators to write "mixed" Distributed Firewall rules within a single policy framework-- for example, permitting traffic from a traditional Virtual Machine (e.g., a DB server) directly to a Kubernetes Pod (e.g., a Web frontend) using dynamic tagging.

QUESTION 8
NestDB is a central Database deployed on all three NSX Managers nodes responsible for storing the user intent.

A. True
B. False

Answer: B
Explanation:
This statement is False because "NestDB" is a fabricated term. In the VMware vDefend (NSX) architecture, the highly available, distributed database responsible for securely storing management plane data, configurations, and user intent across the three NSX Manager nodes is called CorfuDB (or simply Corfu).

CorfuDB is an open-source, strongly consistent, distributed data store developed by VMware. It ensures that if an administrator logs into Manager Node A and creates a security policy, that intent is instantly and resiliently replicated to Manager Nodes B and C.

QUESTION 9
Which of the following API actions are not valid?

A. GET
B. POST
C. UPDATE
D. DELETE

Answer: C
Explanation:
The VMware vDefend REST API strictly adheres to standard HTTP protocols and syntax. When interacting with an API endpoint to manipulate a security object, you must use standard HTTP verbs (methods).

Valid HTTP verbs include GET (to retrieve or read data), POST (to create new data), PUT (to replace data), PATCH (to partially modify data), and DELETE (to remove data).

While "Update" is a concept (represented by the letter 'U' in CRUD), UPDATE is NOT a valid HTTP verb or API action. If you attempt to send an HTTP request with the method UPDATE to the vDefend Manager, the API gateway will reject it with an error (typically a 405 Method Not Allowed or 400 Bad Request).

QUESTION 10
What of the following is true regarding Distributed Firewall logging?

A. Broadcom recommends logging all the DFW rules, as it does not have any CPU overhead
B. VMware Cloud Foundation logging tools are the only supported remote log server supported
C. The Firewall logs are first sent to the management plane to sanitize any Personally Identifiable Information
D. Logging can be enabled on per rule basis

Answer: D
Explanation:
Logging is critical for security operations and compliance, but it must be managed carefully. In vDefend, logging is exceptionally granular: it is enabled on a strict per-rule basis.

Why Option D is true and Option A is false: If an administrator enabled logging globally for every single rule (including high-volume infrastructure traffic like DNS or basic allowed web traffic), the ESXi hosts would generate a massive flood of syslog traffic. This causes significant CPU overhead, network congestion, and fills up log server storage rapidly. Best practice is to only enable logging on "Drop/Deny" rules, or on specific "Allow" rules governing highly critical applications.

(Option B is false because standard syslog protocols are used, supporting third-party tools like Splunk or QRadar. Option C is false because the ESXi host sends syslogs directly to the logging server; hair-pinning logs through the Management Plane would cause an architecture bottleneck).

QUESTION 11
On which node does the vDefend local control plane (LCP) reside?

A. NSX Manager appliance
B. vCenter appliance
C. NSX Controller appliance
D. ESXi host

Answer: D
Explanation:
The VMware vDefend (NSX) control plane is divided into two distinct components to ensure maximum scalability and resiliency: the Central Control Plane (CCP) and the Local Control Plane (LCP).

Central Control Plane (CCP): This resides logically on the NSX Manager cluster. It computes the overall network and security topology based on the administrator's intent.

Local Control Plane (LCP): This resides directly on every individual ESXi host (and Edge Node) as a daemon/service (specifically the nsx-proxy and netcpa agents). The CCP pushes the calculated state down to the LCP on the host. The LCP is then responsible for programming

those specific rules directly into the host's Data Plane (the hypervisor kernel modules). By keeping an LCP on the ESXi host, the host can continue to enforce security rules and route traffic even if it temporarily loses connectivity to the central NSX Managers.

QUESTION 12
Which component is responsible for maintaining the flow state table for active traffic flows?

A. Management Plane
B. Data Plane
C. Central Control Plane
D. Local Control Plane

Answer: B
Explanation:
In the software-defined networking stack, the planes have very specific, separated duties.

The Management Plane handles user UI/API input, and the Control Plane computes the topology. However, neither of these planes actually touch or inspect the network packets.

The Data Plane (which resides directly in the ESXi hypervisor kernel at the virtual switch/vNIC layer) is the engine that physically moves, inspects, drops, or forwards network traffic. Because the Distributed Firewall is stateful, it must track every active connection (TCP handshakes, sequence numbers, UDP timers) to allow return traffic automatically. This real-time, high-speed tracking occurs exclusively within the Data Plane, which maintains the active Flow State Table in the hypervisor's memory.

QUESTION 13
Which of the following are valid Network Traffic Analysis detectors in vDefend ATP? (Select all that apply)

A. DNS tunneling
B. Unusual traffic pattern
C. Password brute force
D. Vertical port scan

Answer: AB
Explanation:
VMware vDefend Network Traffic Analysis (NTA) focuses on behavioral anomalies and advanced evasive techniques rather than simple, noisy, signature-based events.
DNS Tunneling (Option A): This is a highly sophisticated detector. Attackers often encapsulate stolen data or Command & Control (C2) instructions inside standard DNS queries (because DNS is rarely blocked by firewalls). NTA uses Deep Packet Inspection (DPI) to detect this anomalous payload hiding in port 53.
Unusual Traffic Pattern (Option B): NTA uses machine learning to baseline normal East-West traffic in your data center. If a web server that normally only talks to a database server suddenly starts transferring gigabytes of data to an unknown internal workstation, this detector flags the anomaly.
(Note: Basic password brute force and simple vertical port scans are traditionally handled by the standard IDS/IPS signature engines, whereas NTA focuses on deeper, protocol-level anomalies and AI-driven deviations).

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**