PassQueen
a.k.a dumpsqueen.com

VMware vDefend Security for VCF 5.x Administrator

VMware 6V0-21.25

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, VMware Products and Solutions	11
Topic 2, Install, Configure, Setup	9
Topic 3, Troubleshooting and Repair	3
Total	23

QUESTION NO: 1

Which of the following must be done in order to detect DNS anomalies with NTA? (Select all that apply)

A. Do nothing, it works out of the box

B. Configure a L4 TCP/UDP port 53 allow rule

C. Configure a L7 APPID DNS rule allow rule

D. Enable the DNS Tunneling and DGA detectors

ANSWER: C

Explanation:

Configuring a L7 APPID DNS rule allow rule is required because Network Traffic Analysis needs Layer 7 visibility into DNS traffic to inspect DNS-specific protocol content. An application-aware DNS rule identifies the traffic as DNS based on protocol characteristics and directs it through the appropriate inspection path, allowing the NTA service to extract DNS telemetry such as query names, response behavior, and other protocol attributes. That telemetry provides the context used by DNS-focused analytics to identify anomalous activity, including patterns associated with DNS tunneling and domain-generation algorithms. Merely permitting traffic by port does not establish application-level DNS classification, since DNS can use different transports and ports and port-based policy does not provide the same protocol context. The DNS App ID rule should be applied to the relevant source, destination, and traffic direction so that the DNS flows to be monitored are visible to the distributed firewall and NTA analysis pipeline. VMware's vDefend documentation describes distributed firewall application identification and the Network Traffic Analysis capabilities that use observed network-traffic context for detection. See the VMware vDefend documentation and the VMware NSX product documentation resources.

QUESTION NO: 2

An administrator wants a security policy to apply automatically when newly deployed virtual machines are assigned the tag **App=Web**.

Which two configuration actions support this requirement? (Select two)

A. Create a group with a membership criterion for the App=Web tag

B. Use the tag-based group in the Distributed Firewall rule

C. Add each new virtual machine address to an IP set

D. Place the tagged virtual machines in the firewall exclusion list

E. Create a separate firewall rule for each newly deployed virtual machine

ANSWER: A B

Explanation:

A dynamic group can use a tag membership criterion so that workloads are added when the required tag is assigned. The Distributed Firewall rule must then use that group as the relevant source, destination, or both, depending on the intended policy direction. Adding a virtual machine to an IP set or manually editing the rule for every deployment does not provide automatic tag-based policy assignment.