DUMPSARENA

VMware Certified Advanced ProfessionalVMware Cloud Foundation 9.0 Networking

VMware 3V0-25.25

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, VMware Cloud Foundation Networking Architecture and Technologies	1
Topic 2, VMware Cloud Foundation Networking Design	3
Topic 3, VMware Cloud Foundation Networking Implementation	12
Topic 4, VMware Cloud Foundation Networking Troubleshooting and Optimization	7
Total	23

QUESTION NO: 1

An administrator creates a distributed firewall rule to deny all outbound traffic from a compromised virtual machine. The rule is published successfully, but traceflow shows that traffic from the virtual machine continues without distributed firewall enforcement. Other virtual machines on the same segment are evaluated by the distributed firewall as expected.

Which configuration should the administrator verify first?

A. Verify whether the virtual machine is included in the distributed firewall exclusion list.

B. Verify that the segment is associated with the correct overlay transport zone.

C. Verify that the Tier-1 Gateway Firewall has a matching deny rule.

D. Verify that the virtual machine belongs to an additional NSX group.

ANSWER: A

Explanation:

The administrator should verify whether the compromised virtual machine is included in the NSX distributed firewall exclusion list. Virtual machines in the exclusion list bypass distributed firewall processing, so a newly published rule cannot affect their traffic.

The segment transport zone controls segment availability rather than firewall applicability. A Tier-1 Gateway Firewall rule would not explain why traffic from this individual virtual machine bypasses distributed firewall enforcement. Adding the virtual machine to another group does not override an exclusion-list entry.

QUESTION NO: 2

An administrator creates a VLAN-backed segment for workloads that require access to a physical VLAN. The physical VLAN is available only through the second uplink on every ESXi host. The segment currently uses the default teaming policy, which has the first uplink configured as active.

Which action would ensure that traffic for the VLAN-backed segment uses the correct physical uplink?

A. Enable ECMP on the Tier-0 Gateway.

B. Create a named teaming policy with the second uplink active and apply it to the segment.

C. Change the default teaming policy for all transport nodes.

D. Connect the segment to an additional Tier-1 Gateway.

ANSWER: B

Explanation:

The administrator should create a named teaming policy with the second uplink configured as active and apply that policy to the VLAN-backed segment. A named teaming policy allows an individual segment to use a different uplink assignment from the transport node's default uplink policy.

Changing the default policy would affect other segments that rely on it. Configuring ECMP affects routed traffic forwarding and does not select an ESXi host uplink for a VLAN segment. Adding an additional Tier-1 Gateway does not correct the physical uplink mapping.