Fortinet.FCP_ZCS-AD-7.4.v2026-02-18.q13

Exam Code:	FCP_ZCS-AD-7.4
Exam Name:	FCP - Azure Cloud Security 7.4 Administrator
Certification Provider:	Fortinet
Free Question Number:	13
Version:	v2026-02-18
# of views:	647
# of Questions views:	131
https://www.dumpsfiles.com/files/Fortinet/FCP_ZCS-AD-7.4/Fortinet.FCP_ZCS-AD-7.4.v2026-02-18.q13	

NEW QUESTION: 1

Which statement about deploying VMs in a gateway subnet is true?

A. VMs are not allowed in a gateway subnet

B. VMs can be deployed in a gateway subnet only after you deploy the VPN Gateway

C. VMs are required in a gateway subnet

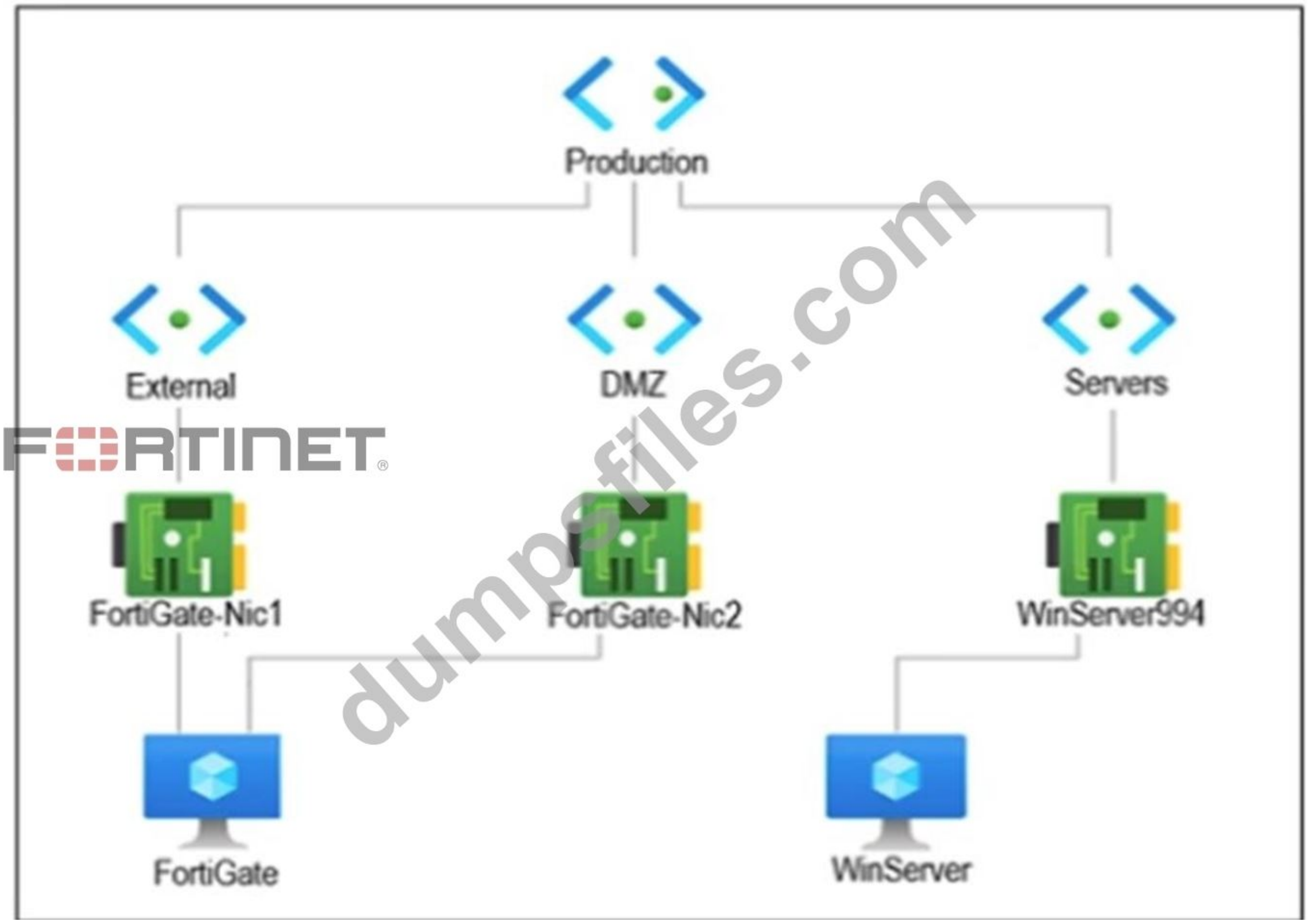
D. VMs are automatically deployed in a gateway subnet

Answer: A (LEAVE A REPLY)

Azure does not allow the deployment of virtual machines (VMs) in a gateway subnet.The gateway subnet is specifically reserved forAzure VPN Gateway or ExpressRoute Gateway instances, and deploying other resources in it can causegateway deployment or operation failures.

NEW QUESTION: 2

Refer to the exhibit.



You are troubleshooting a network connectivity issue between two VMs that are deployed in Azure.

One VM is a FortiGate that has one interface in the DMZ subnet, which is in the Production VNet.

The other VM is a Windows Server in the Servers subnet, which is also in the Production VNet.

You cannot ping the Windows Server from the FortiGate VM.

What is the reason for this?

A. You have not created a VPN to allow traffic between those subnets

B. By default, Azure does not allow ICMP traffic between subnets

C. The firewall in the Windows VM is blocking the traffic

D. You have not configured a user-defined route for this traffic

Answer: C (LEAVE A REPLY)

The FortiGate VM and the Windows Server VM are in different subnets but within the sameProduction virtual network, which means they can communicateby defaultunless restricted. Azure allows ICMP between subnets, butWindows VMs have ICMP blocked by default in their firewallsettings. Therefore, the likely reason for the ping failure is that theWindows Server's firewall is blocking ICMP (ping) traffic.

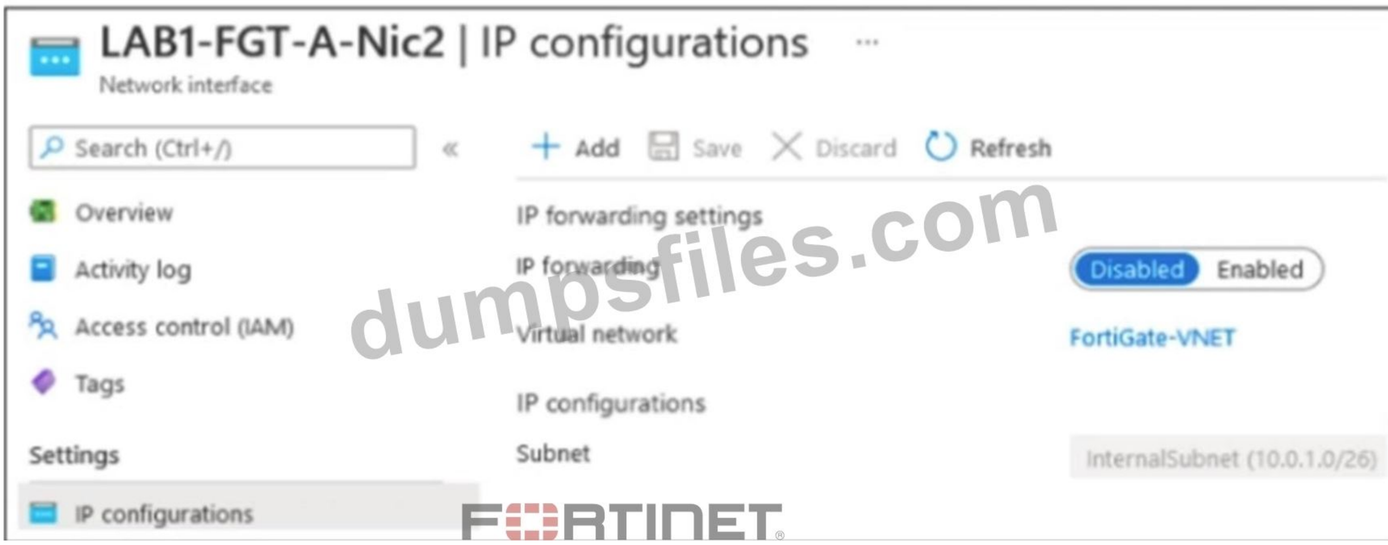
NEW QUESTION: 3

Which role does the local network gateway play in FortiGate to Azure VPN connectivity?

A. It manages the encryption keys for the VPN connection

B. It represents the Azure VPN Gateway in the FortiGate configuration
C. It defines the IP addresses of the on-premises network
D. It is responsible for load balancing traffic between FortiGate and Azure
Answer: C (LEAVE A REPLY)
Thelocal network gatewayin Azure represents theon-premises VPN device(such as FortiGate) and defines theon-premises public IP addressand theaddress prefixesof the on-premises network. This is essential for configuring site-to-site VPN connections from Azure to FortiGate.

NEW QUESTION: 4
Refer to the exhibit.



The exhibit shows some of the properties of a virtual NIC that is used by a FortiGate VM deployed in Azure.
The virtual NIC shown is connected to a subnet (10.0.1.0/26) with several VMs that will be accessing the internet through the FortiGate VM.
Which statement is true for this scenario?
A. The NIC in the exhibit needs to be assigned a public IP address.
B. The VMs in the 10.0.1.0/26 subnet can access the internet through FortiGate.
C. You must change the default gateway on the VMs in the Internal Subnet for this to work.
D. The parameters of the virtual NIC are not configured correctly.
Answer: C (LEAVE A REPLY)
For VMs in the10.0.1.0/26subnet to access the internetthrough the FortiGate VM, theirdefault gateway must be changedto the internal IP address of the FortiGate's NIC in that subnet (e.g.,LAB1-FGT-A-Nic2).
This ensures traffic is routedthrough FortiGate for inspection and NAT, rather than directly using Azure's default system routes.

NEW QUESTION: 5
What is a key advantage of the branch-to-hub to hub-to-branch topology in an Azure virtual WAN?

A. Increased security through isolated connections between branches and hubs
B. Enhanced scalability enables communication between branch offices
C. Load balancing enabled by the simultaneous connection of each branch to multiple hubs
D. Improved branch-to-branch communication for faster data transfer
Answer: (SHOW ANSWER)
Thebranch-to-hub to hub-to-branchtopology in Azure Virtual WAN enablesefficient branch-to-branch communicationby routing traffic through connected hubs. This improvesdata transfer speed and reliability between branches without needing direct connections between all sites, simplifying management while maintaining performance.

NEW QUESTION: 6
Why would you use a user-defined route in Azure?
A. To manage user authentication and access control
B. To have the traffic from the other VMs inspected by FortiGate
C. To allow inbound management access to FortiGate VMs
D. To allow communication between FortiGate VMs on two subnets in the same VNET
Answer: B (LEAVE A REPLY)
Auser-defined route (UDR)in Azure is used toredirect trafficfrom other VMsthrough a FortiGate VM for inspection. By modifying the routing table, you ensure that outbound or inter-subnet traffic issent to the FortiGate as the next hop, enablingtraffic filtering, logging, and security enforcement.

NEW QUESTION: 7
When you deploy a single FortiGate VM using the available template from the Azure Marketplace, several other resources are also created.
Which two resources, among others, are created during the process? (Choose two.)
A. Two virtual NICs
B. One NSG for each interface
C. One VM Scale set
D. One new route table
Answer: A,B (LEAVE A REPLY)
Two virtual NICs - The FortiGate Azure Marketplace template deploys the VM with at least two network interfaces: one for the external/public interface and one for the internal/private interface.
One NSG for each interface - The deployment creates separate Network Security Groups (NSGs) attached to each NIC to control inbound and outbound traffic as per Fortinet's best practices.

NEW QUESTION: 8
A Linux server was deployed in a protected subnet with a dynamic IP address. A FortiGate VM in the internal subnet provides traffic filtering to it. and you must implement a firewall policy using the IP address of the Linux server.
Which feature could help integrate FortiGate using Linux server tags?
A. Targets Management

B. Microsoft Entra ID
C. Software-defined network (SDN) connector
D. Service Fabric Cluster
Answer: C (LEAVE A REPLY)
TheSoftware-defined network (SDN) connectorallows FortiGate to dynamically pull metadata such astags, IP addresses, and resource groupsfrom Azure resources. This enablesautomatic policy updatesbased on dynamic IP changes, such as those of a Linux server in a protected subnet.

NEW QUESTION: 9
What is a requirement when you deploy a FortiGate active-active cluster in Azure?
A. You must assign the public IP address to an Azure load balancer.
B. You must use unicast FGCP to synchronize the configurations.
C. You must configure both load balancers to allow administrative access.
D. You must configure all FortiGate VMs with three or more interfaces.
Answer: (SHOW ANSWER)
In anactive-active FortiGate clusterdeployment in Azure, you must assign thepublic IP address to an Azure load balancer. This is required because Azure does not support multiple VMs sharing a single public IP directly. TheAzure Load Balancerhandles inbound traffic and distributes it to the active FortiGate instances.

NEW QUESTION: 10
In the context of Azure Route Server, what is a primary function of the route server subnet?
A. Providing DNS resolution for on-premises networks
B. Hosting virtual machines for routing propagation purposes
C. Serving as the hub for the exchange of routing information
D. Acting as a dedicated subnet to host network virtual appliances (NVAs) with routing propagation capabilities
Answer: C (LEAVE A REPLY)
Theroute server subnetin Azure is adedicated subnetthat hosts theAzure Route Server, which functions as thehub for dynamic routing information exchangebetween Azure virtual networks and BGP-enabled network virtual appliances (NVAs) or on-premises routers. It enables seamless and centralized route propagation.

NEW QUESTION: 11
What characterizes the branch-to-branch topology in an Azure virtual WAN?
A. Improved scalability for branch offices connecting to Azure
B. Enhanced security through centralized traffic management
C. Increased redundancy through multiple connections to the central hub
D. Simplified network architecture with reduced hub dependencies
Answer: A (LEAVE A REPLY)

Thebranch-to-branch topologyin Azure Virtual WAN is characterized bydirect connectivity between branchesthrough the Virtual WAN backbone, whichreduces dependency on centralized hubs. This results in asimplified network architecture, lowering latency and optimizing routing between branch locations.

NEW QUESTION: 12

What is a key distinction between Azure Firewall and FortiGate VM in terms of their primary functions?

A. Azure Firewall is a cloud-native network security service, while FortiGate VM is a network virtual appliance (NVA) that provides comprehensive security functions.

B. Azure Firewall focuses on network traffic inspection, while FortiGate VM is primarily a web application firewall.

C. Azure Firewall is designed exclusively for application layer filtering, while FortiGate VM is suitable for both on-premises and cloud environments.

D. Azure Firewall and FortiGate VM have identical primary functions, and no features differentiation.

Answer: (SHOW ANSWER)

Azure Firewallis acloud-native, fully managednetwork security servicedesigned to control and log network traffic using Azure policies. In contrast, theFortiGate VMis anetwork virtual appliance (NVA)that delivers comprehensive security features, including firewalling, IPS, antivirus, VPN, and application control, suitable forboth on-premises and cloud deployments.

NEW QUESTION: 13

After integrating a FortiGate VM with Azure Route Server, you detect that routes are not propagating successfully.

What initial step could you perform to diagnose the root cause?

A. Examine the Azure Microsoft Entra ID permissions associated with the FortiGate VM to ensure that correct authentication is being used for BGP peering

B. Monitor the network latency between the FortiGate VM and Azure Route Server to identify potential communication delays affecting route propagation

C. Verify that the FortiGate VM is running the latest firmware version

D. Verify the BGP peering status on both the FortiGate VM and Azure Route Server

Answer: (SHOW ANSWER)

Thefirst and most direct diagnostic stepis toverify the BGP peering statuson both theFortiGate VM and Azure Route Server. If BGP peering is not established or is in an idle or down state, route propagation will fail. This check confirms whether the two systems are communicating and exchanging routes as expected.