Fortinet FCP_ZCS_AD-7.4予想試験、FCP_ZCS_AD-7.4認定テキスト

2026年Xhs1991の最新FCP_ZCS_AD-7.4 PDFダンプおよびFCP_ZCS_AD-7.4試験エンジンの無料共有：https://drive.google.com/open?id=16e7zp_Cr4mc-K43rddNGRKXL7vQ-Vxn_

弊社は君のFCP_ZCS_AD-7.4試験に合格させるとともにまた一年の無料の更新のサービスも提供し、もしFCP_ZCS_AD-7.4試験に失敗したら全額で返金いたします。しかしその可能性はほとんどありません。弊社は100%合格率を保証し、購入前にネットでダウンロードしてください。

Fortinet FCP_ZCS_AD-7.4 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• VPN Solutions in Azure: This section of the exam measures skills of a Network Security Engineer and addresses secure connectivity between Azure and on-premises environments. Candidates will review the different site-to-site VPN options available in Azure, configure tunnels between FortiGate devices and Azure VPN gateways, and understand how Azure Virtual WAN enhances global connectivity.
トピック 2	• Azure Route Server Use Cases: This section of the exam measures skills of a Cloud Engineer and explores real-world applications of the Azure Route Server. It includes identifying scenarios where Route Server is used to streamline routing operations, support hybrid connectivity, and improve manageability in complex network topologies.

トピック 3	• Azure Route Server Concepts: This section of the exam measures skills of a Cloud Engineer and covers the basics of Azure Route Server. The focus is on understanding what the Azure Route Server is, how it functions within a virtual network, and how it simplifies the management of dynamic routing by automating route exchange with network virtual appliances.
トピック 4	• High Availability (HA): This section of the exam measures skills of a Network Security Engineer and focuses on maintaining system resilience within Azure. Candidates are required to demonstrate knowledge of setting up FortiGate-based high availability in Azure, configuring Azure-native load balancing, and implementing autoscaling features to ensure continuous service availability and optimal performance.
トピック 5	• Azure Virtual WAN: This section of the exam measures skills of a Cloud Engineer and explains the concept and deployment of Azure Virtual WAN. It focuses on building large-scale, optimized, and automated branch connectivity with Azure regions and services using virtual WAN hubs, improving cloud-based networking efficiency and scalability.
トピック 6	• Fortinet Product Deployment: This section of the exam measures skills of a Network Security Engineer and covers the implementation of Fortinet products within Azure environments. The topics include deploying individual FortiWeb and FortiGate instances, integrating FortiGate with Azure's software-defined networking, and applying best practices for secure and efficient deployments of Fortinet solutions in the cloud.

Fortinet FCP - Azure Cloud Security 7.4 Administrator 認定 FCP_ZCS_AD-7.4 試験問題 (Q26-Q31):

質問 # 26
Your organization is in the process of optimizing its Azure network architecture and wants to dynamically manage and exchange routing information between its virtual networks and on-premises networks.
Which Azure service would help to provide a centralized point for efficient route management and dynamic routing?

- A. Azure ExpressRoute
- B. Azure Virtual WAN
- C. Azure VPN Gateway
- D. Azure Route Server

正解：D

解説：
Azure Route Server enables dynamic route exchange using BGP between your Azure virtual network and network virtual appliances (NVAs) or on-premises networks. It provides a centralized and scalable solution for route management, allowing seamless integration of routing updates without manual configuration changes.

質問 # 27
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. One NSG for each interface
- B. Two virtual NICs
- C. One new route table
- D. One VM Scale set

正解：A、B

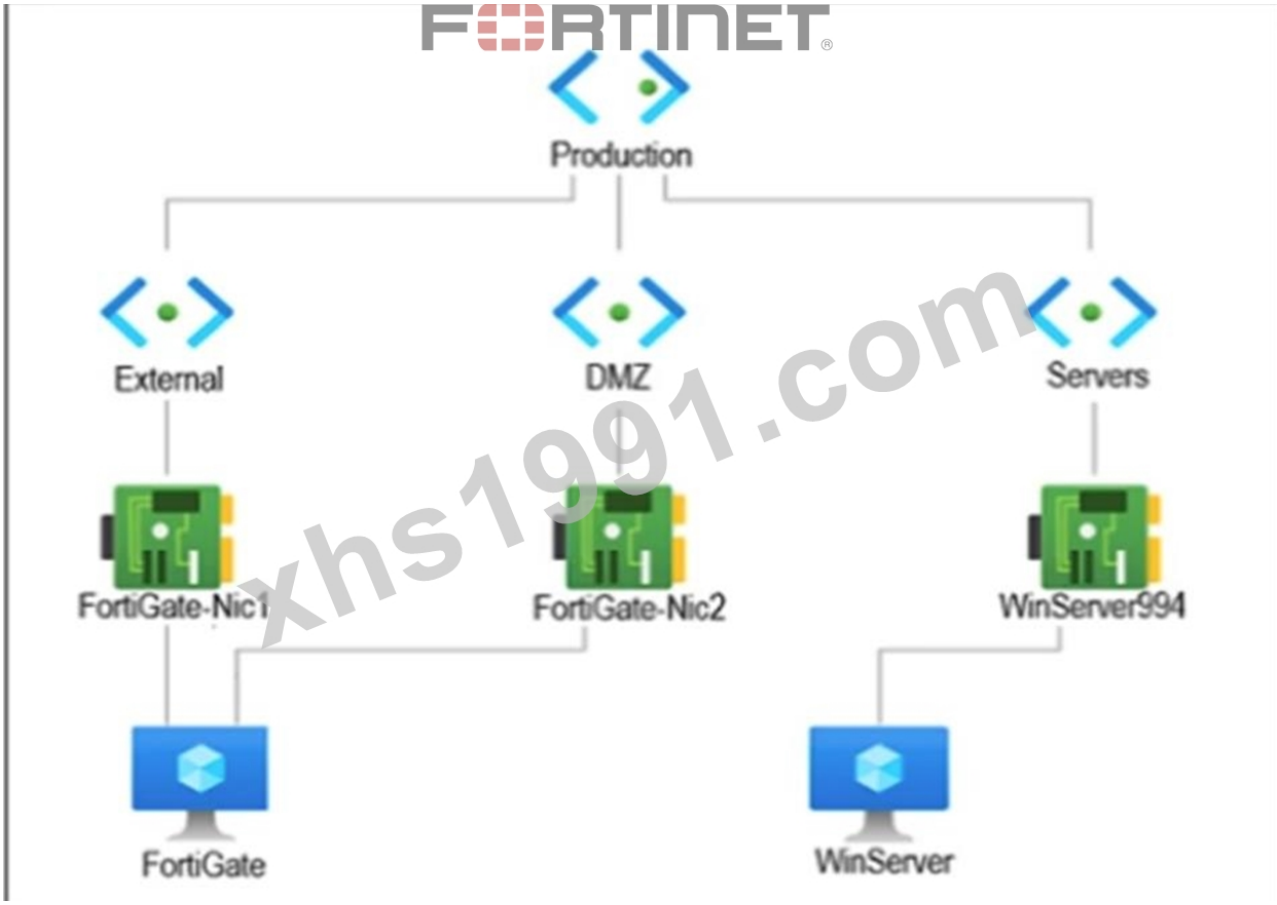
解説：
Two virtual NICs - The FortiGate Azure Marketplace template deploys the VM with at least two network interfaces: one for the external/public interface and one for the internal/private interface.
One NSG for each interface - The deployment creates separate Network Security Groups (NSGs) attached to each NIC to control inbound and outbound traffic as per Fortinet's best practices.

質問 # 28
What capabilities does Azure Virtual WAN offer?
(Choose Three)
Response:

- A. Reduced latency for Azure services
- B. Direct on-premises connection via private links
- C. Centralized network and policy management
- D. Automated route management across VPN, ExpressRoute, and Azure connections
- E. Integrated security with native firewalls and security controls

正解：C、D、E

質問 # 29
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

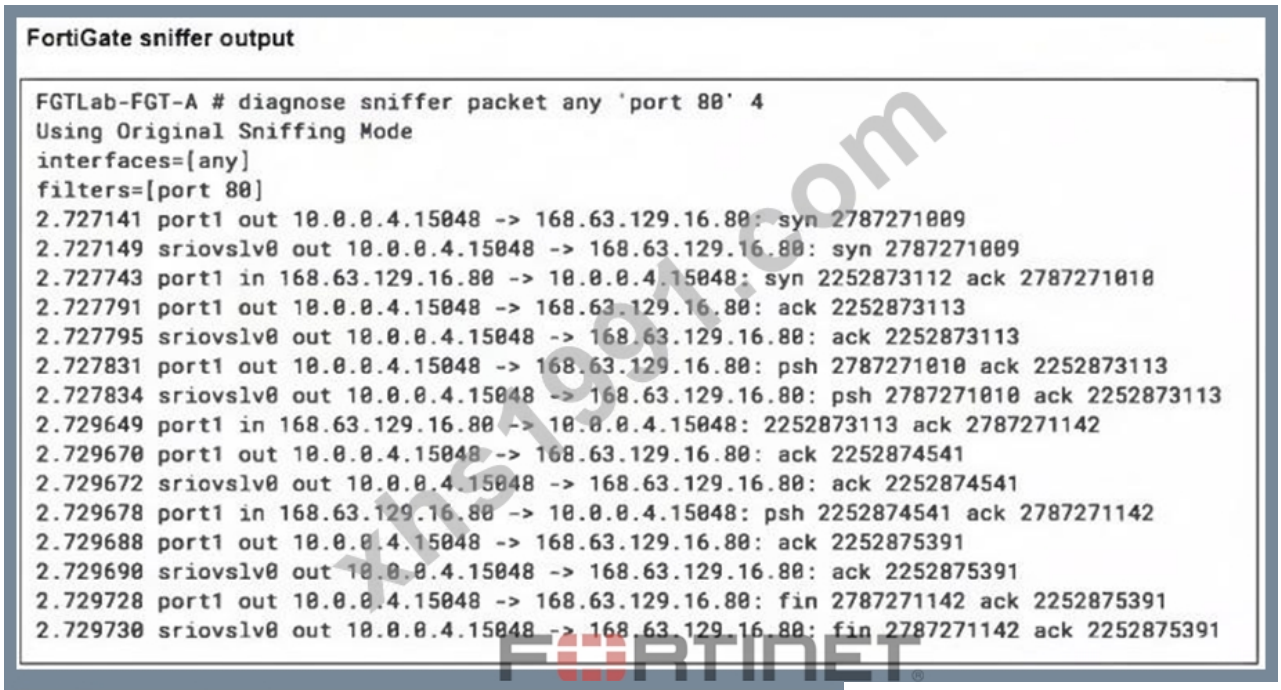
Server in the Servers subnet, which is also in the Production VNet. You cannot ping the Windows Server from the FortiGate VM. What is the reason for this?

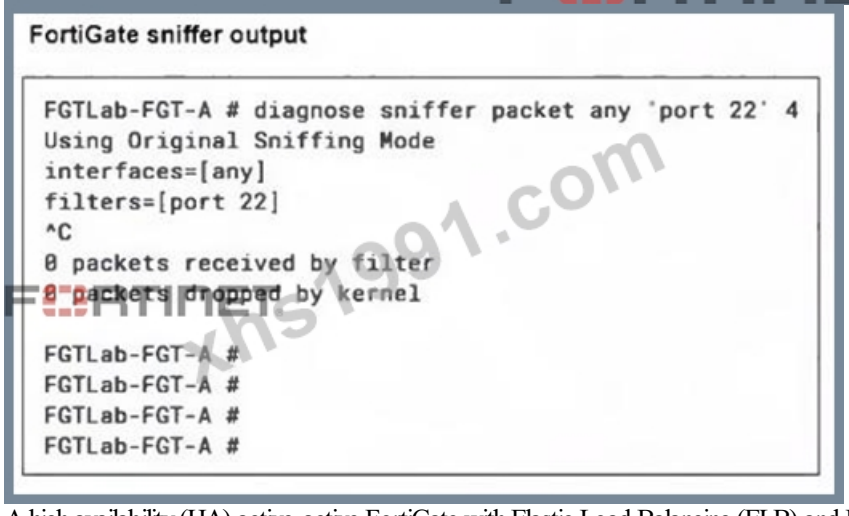
- A. You have not configured a user-defined route for this traffic
- B. You have not created a VPN to allow traffic between those subnets
- C. By default, Azure does not allow ICMP traffic between subnets
- D. The firewall in the Windows VM is blocking the traffic

正解：D

解説：
The FortiGate VM and the Windows Server VM are in different subnets but within the same Production virtual network, which means they can communicate by default unless restricted. Azure allows ICMP between subnets, but Windows VMs have ICMP blocked by default in their firewall settings. Therefore, the likely reason for the ping failure is that the Windows Server's firewall is blocking ICMP (ping) traffic.

質問 # 30
Refer to the exhibits.





A high availability (HA) active-active FortiGate with Elastic Load Balancing (ELB) and Internal Load Balancing (ILB) was deployed with a default setup to filter traffic to a Linux server running Apache server.
Ports 80 and 22 are open on the Linux server, and on FortiGate a VIP and firewall policy are configured to allow traffic through ports 80 and 22. Traffic on port 80 is successful, but traffic on port 22 is not detected by FortiGate.
What configuration changes could you perform to allow SSH traffic?

- A. Configure a customized port under the Frontend IP configuration
- B. Add a new Inbound NAT rule
- C. Add a new Azure load balancing rule
- D. Include the Linux server in the back-end pool options

正解：B

解説：
Since port 80 traffic is reaching the FortiGate (as shown in the sniffer output) but port 22 traffic is not, the issue lies before the FortiGate, at the Azure Load Balancer level. Azure Load Balancers require an Inbound NAT rule to forward specific ports (like SSH on port 22) to a specific backend VM. Creating a new Inbound NAT rule for port 22 will allow SSH traffic to be properly routed to the FortiGate VM.

質問 # 31
.....