Vendor: Fortinet

Exam Code: FCP_ZCS_AD-7.4

Exam Name: FCP - Azure Cloud Security 7.4 Administrator

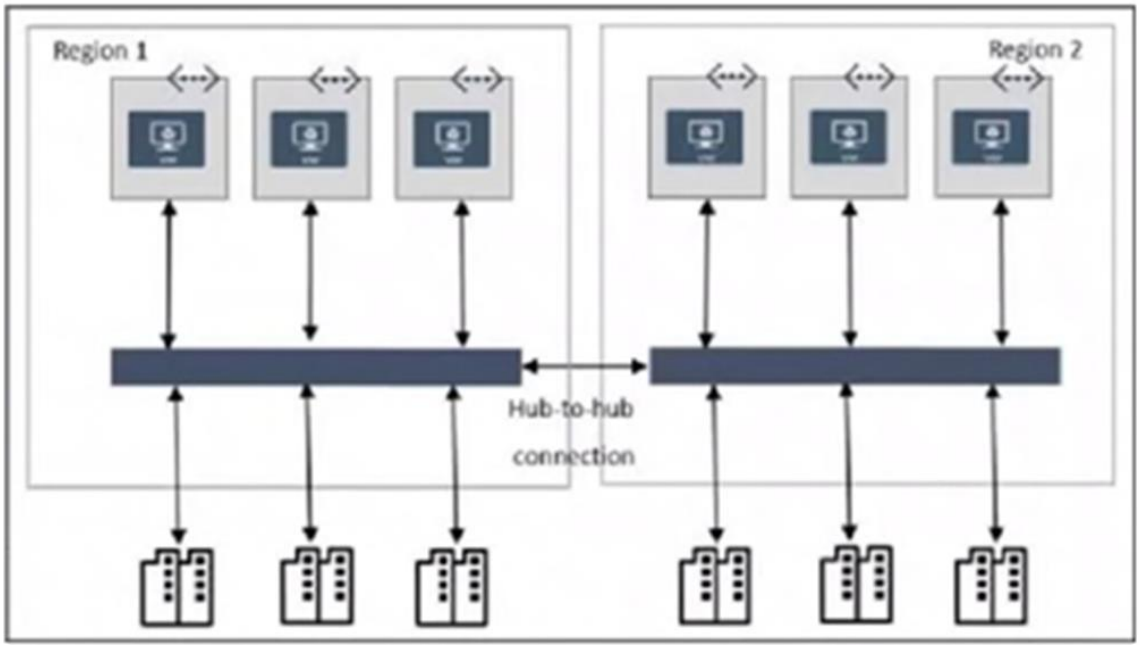
Version: DEMO

QUESTION 1
Which additional features does Azure Firewall Premium offer compared to Azure Firewall Standard?

A. Content filtering and threat intelligence integration
B. Antivirus detection and AI prevention capabilities
C. Advanced DDoS protection and VPN diagnostics
D. Enhanced URL filtering and web categories

Answer: C
Explanation:
Azure Firewall Premium includes advanced features not available in the Standard tier, such as enhanced URL filtering and web categories, TLS inspection, IDPS (intrusion detection and prevention system), and support for private certificate authorities. These enable more granular and secure traffic inspection and control.

QUESTION 2
Refer to the exhibit. Your organization is planning the implementation of a complex hub-to-spoke solution to meet automated large-scale branch connectivity with multiple regions, offering a diverse range of connectivity options.



Which Azure networking service can deliver a solution?

A. Azure SD-WAN
B. Azure Virtual WAN
C. Azure VPN Gateway
D. Azure Firewall Manager

Answer: B
Explanation:
Azure Virtual WAN is designed for large-scale, automated, and global branch connectivity,

supporting hub-and-spoke architectures across multiple regions. It enables centralized routing, hub-to-hub connectivity, and integrates with VPN, ExpressRoute, and SD-WAN solutions, making it ideal for complex, multi-region deployments as shown in the diagram.

QUESTION 3
You are deploying a site-to-site IPsec VPN connection between your on-premise subnet and your Azure VNets.
What is the most important advantage for using FortiGate at both ends of the tunnel?

A. It minimizes the need for encryption in transit
B. It allows scaling based on performance and capacity requirements
C. It provides consistent security policies and configurations
D. It reduces the need for troubleshooting due to FortiGate automatic configuration

Answer: C
Explanation:
Using FortiGate at both ends of a site-to-site IPsec VPN tunnel provides the advantage of applying consistent security policies, configurations, and management tools across both the on-premises and Azure environments. This simplifies policy enforcement, improves operational efficiency, and ensures uniform threat protection.

QUESTION 4
Your organization is planning to deploy FortiWeb in Azure to provide a web application security solution to its web servers. One of the requirements is to have granular control of the number of vCPUs and memory assigned to this resource.
Which cloud model could meet this requirement?

A. Software-as-a-Service (SaaS)
B. Platform-as-a-Service (PaaS)
C. Function-as-a-Service (FaaS)
D. Infrastructure-as-a-Service (IaaS)

Answer: D
Explanation:
Infrastructure-as-a-Service (IaaS) allows you to deploy FortiWeb as a virtual machine in Azure, giving you granular control over vCPU and memory allocation. This model provides full flexibility over the compute resources and network configuration, which is essential for deploying and scaling security appliances like FortiWeb.

QUESTION 5
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: A
Explanation:
Azure Firewall is a cloud-native, fully managed network security service designed to control and log network traffic using Azure policies. In contrast, the FortiGate VM is a network virtual appliance (NVA) that delivers comprehensive security features, including firewalling, IPS, antivirus, VPN, and application control, suitable for both on-premises and cloud deployments.

QUESTION 6
Refer to the exhibits, which show the outputs of two commands taken on a Windows VM running in Azure.

IP address configuration

```
C:\windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix  . : 12htgkvlwy3e1kwr2zeco.cloudapp.net
Link-local IPv6 Address . . . . . : fe80::51f1:1be4:a33b:d868%2
IPv4 Address. . . . . . . . . . . : 10.0.1.4
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 10.0.1.1
```

Trace output

```
C:\windows\system32>tracert 10.0.2.4

Tracing route to 10.0.2.4 over a maximum of 30 hops
  1     <1 ms     <1 ms     <1 ms  10.0.2.4

Trace complete.
```

Which statement is true about the device with the IP address 10.0.2.4?

A. It is reachable through FortiGate in transparent mode
B. It is provided by Azure for routing traffic among subnets
C. It is on the same VNET as the Windows VM
D. It is on the same subnet as the Windows VM

Answer: C
Explanation:
The trace output shows only one hop to reach 10.0.2.4, indicating that the destination is in the same Azure virtual network (VNet) as the Windows VM. Since the VM's IP is 10.0.1.4 and the destination is 10.0.2.4, they are in different subnets, but Azure allows direct routing between subnets within the same VNet without additional hops.

QUESTION 7
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
Explanation:
Azure does not allow the deployment of virtual machines (VMs) in a gateway subnet. The gateway subnet is specifically reserved for Azure VPN Gateway or ExpressRoute Gateway instances, and deploying other resources in it can cause gateway deployment or operation failures.

QUESTION 8
What is a limitation of the Network Security Groups (NSGs) in Azure?

A. NSGs allow the filtering of inbound traffic only.
B. NSGs are applied only to vNICs.
C. NSGs operate at the application layer, limiting their effectiveness in the network layer.
D. NSGs cannot be applied to individual virtual machines.

Answer: B
Explanation:
A limitation of NSGs is that they are applied only at the subnet level or to network interfaces (vNICs), not directly to other resources like load balancers or application gateways. This means granular application-layer filtering is not supported, and NSGs primarily operate at Layers 3 and 4.

QUESTION 9
In Microsoft Entra ID, what is the primary administrative unit that represents an organization and its relationship with Microsoft's cloud services?

A. Microsoft Entra tenant
B. Microsoft Entra subscription
C. Microsoft Entra organization
D. Microsoft Entra domain

Answer: A
Explanation:
A Microsoft Entra tenant is the primary administrative unit that represents an organization within Microsoft's identity platform. It defines the boundary for identity management, access control, and resource governance, and serves as the core entity that connects the organization to Microsoft's cloud services such as Azure and Microsoft 365.

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**