KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **NSE7_CDS_AR-7.6**

Title : Fortinet NSE 7 - Public Cloud Security 7.6.4 Architect

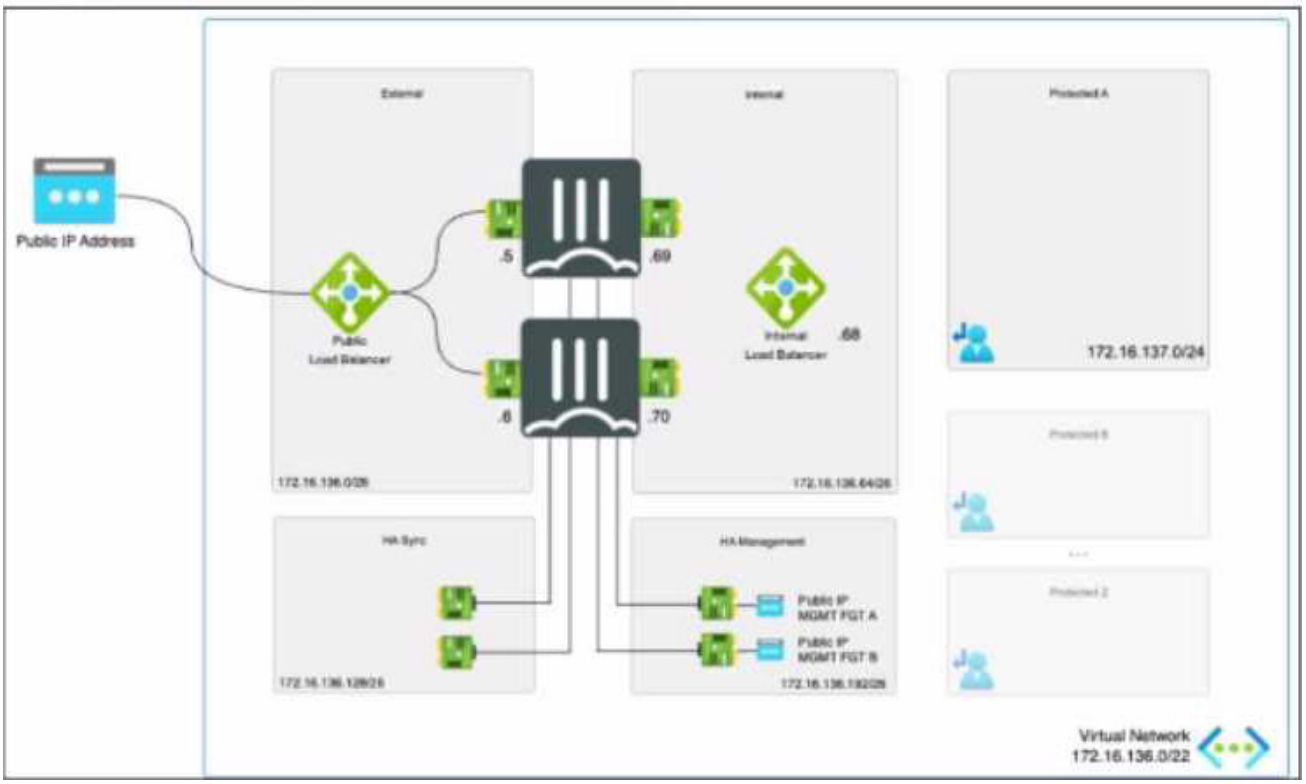
Version : DEMO

1.An administrator would like to use FortiCNP to keep track of sensitive data files located in the Amazon Web Services (AWS) S3 bucket and protect it from malware.
Which FortiCNP feature should the administrator use?
A. FortiCNP Threat Detection policies
B. FortiCNP Risk Management policies
C. FortiCNP Data Scan policies
D. FortiCNP Compliance policies
Answer: C
Explanation:
https://docs.fortinet.com/document/forticnp/22.4.a/online-help/359537/anti-virus-scan-policy

2.You are using Ansible to modify the configuration of several FortiGate VMs.
What is the minimum number of files you need to create, and in which file should you configure the target FortiGate IP addresses?
A. One playbook file for each target and the required tasks, and one inventory file.
B. One .yaml file with the targets IP addresses, and one playbook file with the tasks.
C. One inventory file for each target device, and one playbook file.
D. One text file for all target devices, and one playbook file.
Answer: D
Explanation:
Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:
Based on the FortiOS 7.6 Automation Guide and the provided documentation for Ansible workflows, the following structure is required for managing multiple FortiGate nodes:
Inventory File (The Target List): The inventory is a single file that defines the list of managed nodes. It specifies critical information such as hostnames, connection details, and specifically the IP addresses of the target devices. According to the study guide, this inventory is a text file that lists all the systems you want to manage.
Playbook File (The Task List): You create and edit a separate file that acts as the playbook. This file is written in YAML format and contains the series of tasks that Ansible performs on the managed nodes to reach a desired state.
Minimum File Count: A basic Ansible workflow consists of exactly two files: one inventory file (text) and one playbook file (YAML). By listing the target IP address (e.g., 10.0.206.131) within the inventory text file, the administrator can manage the FortiGate device without needing individual files for every target.
Why other options are incorrect:
Option A & C: Creating a separate playbook or inventory file for each target is inefficient and contradicts the core Ansible workflow, which uses a single inventory to manage multiple hosts.
Option B: While the playbook is a .yaml file, the study guide specifically defines the inventory (where IP addresses are configured) as a text file in the context of the basic workflow.

3.Refer to the exhibit.

HA Topology



The exhibit shows an active-passive high availability FortiGate pair with external and internal Azure load balancers There is no SDN connector used in this solution.
Which configuration must the administrator implement on each FortiGate?
A. Single BGP route to Azure probe IP address.
B. One static route to Azure Lambda IP address.
C. Two static routes to Azure probe IP address.
D. Two BGP routes lo Azure probe IP address.
Answer: C

4.Your DevOps team is evaluating different Infrastructure as Code (IaC) solutions for deploying complex Azure environments.
What is an advantage of choosing Azure Bicep over other IaC tools available?
A. Azure Bicep generates deployment logs that are optimized to improve error handling.
B. Azure Bicep provides immediate support for all Azure services, including those in preview.
C. Azure Bicep requires less frequent schema updates than Azure Resource Manager (ARM) templates.
D. Azure Bicep can reduce deployment costs by limiting resource utilization during testing.
Answer: B

5.You must add an Amazon Web Services (AWS) network access list (NACL) rule to allow SSH traffic to a subnet for temporary testing purposes. When you review the current inbound and outbound NACL rules, you notice that the rules with number 5 deny SSH and telnet traffic to the subnet.
What can you do to allow SSH traffic?
A. You do not have to create any NACL rules because the default security group rule automatically allows SSH traffic to the subnet.

B. You must create a new allow SSH rule anywhere in the network ACL rule base to allow SSH traffic.
C. You must create two new allow SSH rules, each with a number bigger than 5.
D. You must create two new allow SSH rules, each with a number smaller than 5.
Answer: D