PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 7Public Cloud Security 7.6.4 Architect

Fortinet NSE7_CDS_AR-7.6

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Refer to the exhibit.

After the initial Terraform configuration in Microsoft Azure, the terraform plan command is run.

Which two statements about running the terraform plan command are true? (Choose two.)

A. The terraform plan command will deploy the rest of the resources except the service principle details.

B. You cannot run the terraform apply command before the terraform plan command.

C. The terraform plan command makes terraform do a dry run.

D. You must run the terraform init command once, before the terraform plan command.

ANSWER: C D

Explanation:

The `terraform plan` command performs a preview, or dry run, of the actions Terraform proposes to take to reconcile the declared configuration with the current state and provider-managed infrastructure. It evaluates resource definitions, dependencies, variables, and the current state, then presents the planned additions, changes, or deletions without creating or modifying Azure resources. This lets an administrator validate the expected deployment safely before approving it with `terraform apply`.

Terraform working directories must be initialized with `terraform init` before planning. Initialization prepares the directory by installing the provider plugins required by the configuration, configuring the backend used for state when applicable, and initializing referenced modules. Therefore, in the initial workflow, running `terraform init` before `terraform plan` is required. Initialization is normally performed once for an unchanged working directory, though it should be run again when provider, module, or backend configuration changes. HashiCorp documents the plan workflow at Terraform plan command and initialization requirements at Terraform init command.

QUESTION NO: 2

An administrator deploys a FortiGate-VM in an AWS VPC to inspect outbound traffic from private application subnets. The FortiGate-VM has an external interface in a public subnet and an internal interface in a private subnet. The FortiGate-VM can reach the internet, but the application instances cannot.

Which route-table configuration is required for the application instances to use FortiGate-VM for internet access?

A. Add a default route from the application subnet to the FortiGate-VM internal network interface.

B. Add a default route from the application subnet directly to the internet gateway.

C. Add a default route from the FortiGate-VM public subnet to its internal network interface.

D. Add a default route from the application subnet to the virtual private gateway.

ANSWER: A

Explanation:

The route table associated with each private application subnet must contain a default route that uses the FortiGate-VM internal network interface as its target. The FortiGate-VM external subnet must have a default route to the internet gateway so that traffic forwarded and source-NATed by FortiGate-VM can reach the internet.

Routing the private application subnet directly to the internet gateway would bypass FortiGate-VM. A route from the public subnet to the FortiGate-VM internal interface would not provide the required return path to the internet.