EXAMTOPICS

-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

When configuring the FortiCASB policy, which three configuration options are available? (Choose three.)

A. Intrusion prevention policies

B. Threat protection policies

C. Data loss prevention policies

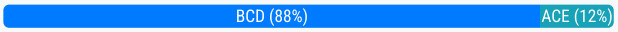
D. Compliance policies

E. Antivirus policies

Suggested Answer: *B, C, D*

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/bf017449-572a-11e9-81a4-00505692583a/forticasb-4.1.0-admin-guide.pdf (62)

Community vote distribution



guihlopes08 Most Recent 3 years, 5 months ago

outdated exam! I took the test yesterday, 3 questions fell out

upvoted 1 times

charruco 3 years, 8 months ago

BCD are correct Policy setting allows you to configure each policy to fit the need of your usage. You can select any type of Policy (Data Analysis, Threat Protection or Compliance) https://docs.fortinet.com/document/forticasb/20.1.0/online-help/482958/policy-configuration

upvoted 1 times

mordechayd 3 years, 11 months ago

according the docs and the study guide

upvoted 3 times

KaX001 3 years, 11 months ago

BCD https://docs.fortinet.com/document/forticasb/20.1.0/online-help/482958/policy-configuration

upvoted 2 times

bigbug 4 years ago

Hi. who did write this exam more recently?

upvoted 1 times

tachy_22 4 years, 1 month ago

BCD is correct FortiCASB offers Data Analysis (DA) policies, Threat Protection policies, Compliance policies, and Customized policies.

upvoted 1 times

kinge2 4 years, 1 month ago

Selected Answer: ACE

Answer is ACE since CWP provide Risk Assessment, Data Analysis, Threat Protection, Intergation and Compliance - page 185 of study guide

upvoted 1 times

kinge2 4 years, 1 month ago

Answer is ACE since CWP provide Risk Assessment, Data Analysis, Threat Protection, Intergation and Compliance - page 185 of study guideThe question is about fortiCASB ,not CWP BCD is the correct answers

upvoted 1 times

mordechayd 3 years, 11 months ago

The question is about fortiCASB ,not CWP BCD is the correct answers

upvoted 2 times

elgato01 4 years, 2 months ago

B, C, D https://docs.fortinet.com/document/forticasb/20.1.0/online-help/482958/policy-configuration

upvoted 3 times

RueDizz 4 years, 4 months ago

This correct

upvoted 1 times

Question #2 *Topic 1*

You have been tasked with deploying FortiGate VMs in a highly available topology on the Amazon Web Services (AWS) cloud. The requirements for your deployment are as follows:
* You must deploy two FortiGate VMs in a single virtual private cloud (VPC), with an external elastic load balancer which will distribute ingress traffic from the internet to both FortiGate VMs in an active-active topology.
* Each FortiGate VM must have two elastic network interfaces: one will connect to a public subnet and other will connect to a private subnet.
* To maintain high availability, you must deploy the FortiGate VMs in two different availability zones.
How many public and private subnets will you need to configure within the VPC?

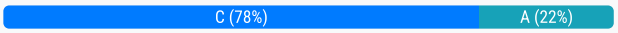
A. One public subnet and two private subnets

B. Two public subnets and one private subnet

C. Two public subnets and two private subnets

D. One public subnet and one private subnet

Suggested Answer: *C*
Reference: https://github.com/fortinet/aws-cloudformation-templates/blob/master/LambdaAA-RouteFailover/6.0/README.md

Community vote distribution


smahah Most Recent 3 years, 6 months ago
"Each subnet must reside entirely within one Availability Zone and cannot span zones" from AWS documentation (https://docs.aws.amazon.com/vpc/latest/userguide/configure-subnets.html). Since we need to deploy in 2 AZs -> 1 pub and 1 priv subnet for each AZ
upvoted 2 times

charruco 3 years, 8 months ago
C. Two public subnets and two private subnets https://github.com/fortinet/aws-cloudformation-templates/blob/master/LambdaAA-RouteFailover/6.0/README.md
upvoted 1 times

elgato01 4 years, 2 months ago
Official documentation: https://docs.fortinet.com/document/fortigate-public-cloud/6.4.0/aws-administration-guide/682830/deploying-and-configuring-fortigate-vm-active-active-ha which takes you here: https://github.com/fortinet/aws-cloudformation-templates/tree/master/LambdaAA-RouteFailover/6.0 where it states that two by two
upvoted 3 times

Thusi26 4 years, 2 months ago
A should be correct if you think logically. After a Failover FortiGate B needs to send out the traffic through the samen Internal / external IP / subnet.
upvoted 1 times

Gallego 4 years, 2 months ago
C is correct. You need 1 private and 1 public subnet for each AZ. You need to deploy it in 2 AZ's (same VPC) so you need 2 private and 2 public
upvoted 1 times

rteo82 4 years, 2 months ago
C is correct https://github.com/fortinet/aws-cloudformation-templates/blob/master/LambdaAA-RouteFailover/6.0/README.md
upvoted 1 times

RueDizz 4 years, 4 months ago
A. One public subnet and two private subnets
upvoted 2 times

Question #3 *Topic 1*

You are deploying Amazon Web Services (AWS) GuardDuty to monitor malicious or unauthorized behaviors related to AWS resources. You will also use the
Fortinet aws-lambda-guardduty script to translate feeds from AWS GuardDuty findings into a list of malicious IP addresses. FortiGate can then consume this list as an external threat feed.
Which Amazon AWS services must you subscribe to in order to use this feature?

A. GuardDuty, CloudWatch, S3, Inspector, WAF, and Shield.

B. GuardDuty, CloudWatch, S3, and DynamoDB.

C. Inspector, Shield, GuardDuty, S3, and DynamoDB.

D. WAF, Shield, GuardDuty, S3, and DynamoDB.

Suggested Answer: *B*
Official Answer: B

Community vote distribution
B (71%) A (29%)

charruco Most Recent 3 years, 8 months ago
B You must subscribe to GuardDuty, CloudWatch, S3, and DynamoDB. https://docs.fortinet.com/document/fortigate-public-cloud/6.4.0/aws-administration-guide/908646/populating-threat-feeds-with-guardduty
upvoted 1 times

LJCF 4 years, 2 months ago
"GuardDuty, CloudWatch, S3, and DynamoDB." https://docs.fortinet.com/document/fortigate-public-cloud/6.4.0/aws-administration-guide/908646/populating-threat-feeds-with-guardduty
upvoted 2 times

Spippolo 4 years, 2 months ago
https://docs.fortinet.com/document/fortigate-public-cloud/6.4.0/aws-administration-guide/908646/populating-threat-feeds-with-guardduty
upvoted 2 times

hippo2048 4 years, 3 months ago
Ans. B AWS GuardDuty is a managed threat detection service that monitors malicious or unauthorized behaviors/activities related to AWS resources. GuardDuty provides visibility of logs called "findings", and Fortinet provides a Lambda script called "aws-lambda-guardduty", which translates feeds from AWS GuardDuty findings into a list of malicious IP addresses in an S3 location, which a FortiGate-VM can consume as an external threat feed after being configured to point to the list's URL. To use this feature, you must subscribe to "GuardDuty, CloudWatch, S3, and DynamoDB." https://docs.fortinet.com/document/fortigate-public-cloud/6.4.0/aws-administration-guide/908646/populating-threat-feeds-with-guardduty
upvoted 2 times

RueDizz 4 years, 4 months ago
Selected Answer: A
A. GuardDuty, CloudWatch, S3, Inspector, WAF, and Shield. Explanation/Reference: Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/ed901ad2-4424-11e9-94bf-00505692583a/FortiOS_6.2.0_AWS_Cookbook.pdf
upvoted 2 times

RueDizz 4 years, 4 months ago
A. GuardDuty, CloudWatch, S3, Inspector, WAF, and Shield. Explanation/Reference: Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/ed901ad2-4424-11e9-94bf-00505692583a/FortiOS_6.2.0_AWS_Cookbook.pdfAns is B To use this feature, you must subscribe to GuardDuty, CloudWatch, S3, and DynamoDB https://docs.fortinet.com/document/fortigate-public-cloud/6.4.0/aws-administration-guide/908646/populating-threat-feeds-with-guardduty
upvoted 2 times

rteo82 4 years, 2 months ago
Ans is B To use this feature, you must subscribe to GuardDuty, CloudWatch, S3, and DynamoDB https://docs.fortinet.com/document/fortigate-public-cloud/6.4.0/aws-administration-guide/908646/populating-threat-feeds-with-guardduty
upvoted 2 times

oefenmaar 4 years, 5 months ago

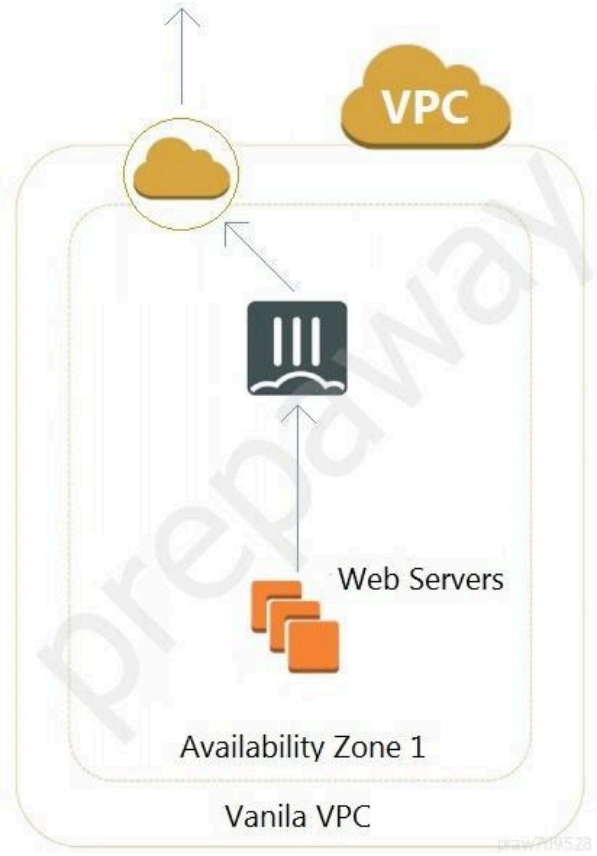
https://docs.fortinet.com/document/fortigate-public-cloud/7.0.0/aws-administration-guide/908646/populating-threat-feeds-with-guardduty To use this feature, you must subscribe to GuardDuty, CloudWatch, S3, and DynamoDB.

upvoted 4 times

Question #4 *Topic 1*

Refer to the exhibit. A customer has deployed an environment in Amazon Web Services (AWS) and is now trying to send outbound traffic from the Web servers to the Internet. The FortiGate policies are configured to allow all outbound traffic; however, the traffic is not reaching the FortiGate internal interface.

What are two possible reasons for this behavior? (Choose two.)



A. The web servers are not configured with the default gateway.

B. The Internet gateway (IGW) is not added to VPC (virtual private cloud).

C. AWS source and destination checks are enabled on the FortiGate interfaces.

D. AWS security groups may be blocking the traffic.

Suggested Answer: *C, D*

Official Answer: CD

Community vote distribution

CD (86%) AD (14%)

charruco 3 years, 8 months ago

CD are correct

upvoted 1 times

cciesam 3 years, 8 months ago

Ans - CD

upvoted 2 times

Nkay17 3 years, 10 months ago

I think it must be AC A- Default gateway needs to be applied to get the traffic reach Fortinet for Internet as there is no default route available by default. C- Src/Dst is enabled by default. So it has to enabled unless you are delpoying via CF template. B - Not required as the Nating will be done via EIP D- Default Outbound NSG allows internet

upvoted 1 times

Nkay17 3 years, 10 months ago

AD - since traffic is not reaching fortinet means that the traffic is denied prior

upvoted 1 times

kinge2 4 years, 1 month ago

Answer is CD

upvoted 3 times

elgato01 4 years, 2 months ago

C and D Check if check is enable (Public_Cloud_6.4_Study_Guide Page 67), by default is enable in AWS and in Azure is disable; and of course the SG has to be checked to make sure that the service/port is allowed is allowed

upvoted 3 times

Spippolo 4 years, 2 months ago

You need to check if source/destination are enabled. Public_Cloud_6.4_Study_Guide Page 67

upvoted 3 times

rteo82 4 years, 2 months ago

A and D is correct. C is incorrect, Public_Cloud_6.4_Study_Guide Page 67 n AWS, the source/destination check feature is enabled by default. And is correct behaviour.

upvoted 1 times

rteo82 4 years, 2 months ago

A and D is correct. C is incorrect, Public_Cloud_6.4_Study_Guide Page 67 n AWS, the source/destination check feature is enabled by default. And is correct behaviour.If the check is enabled, IP addresses that are different from the assigned IP address of the interface are NOT allowed

upvoted 1 times

smahah Most Recent 3 years, 6 months ago

If the check is enabled, IP addresses that are different from the assigned IP address of the interface are NOT allowed

upvoted 1 times

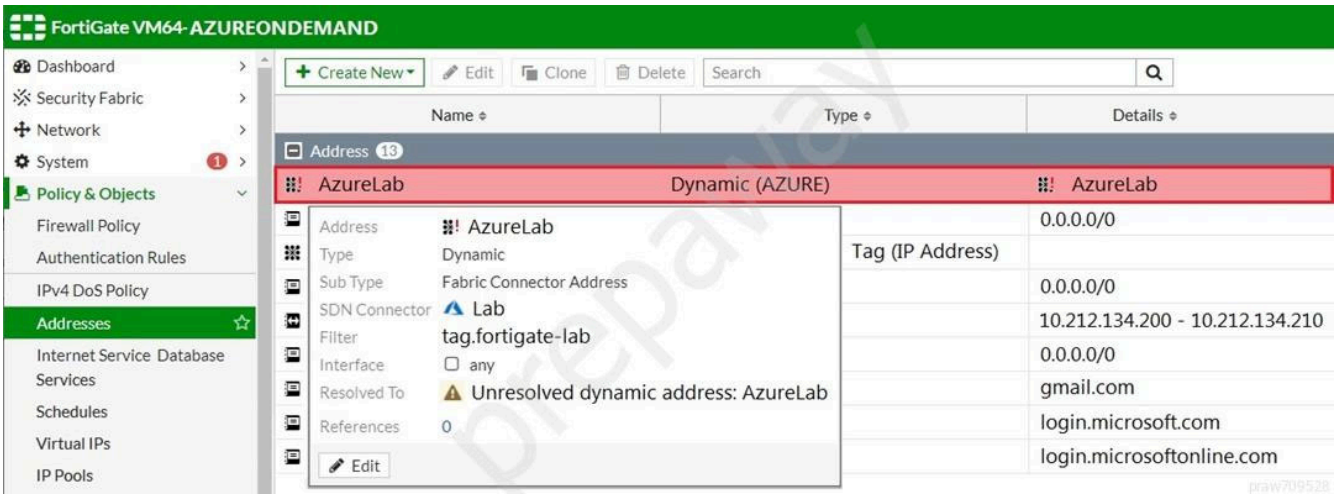
RueDizz 4 years, 4 months ago

A. The web servers are not configured with the default gateway. D. AWS security groups may be blocking the traffic.

upvoted 2 times

Question #5 *Topic 1*

Refer to the exhibit. Your senior administrator successfully configured a FortiGate fabric connector with the Azure resource manager, and created a dynamic address object on the FortiGate VM to connect with a windows server in Microsoft Azure. However, there is now an error on the dynamic address object, and you must resolve the issue.
How do you resolve this issue?



A. Run diagnose debug application azd -l on FortiGate.

B. In the Microsoft Azure portal, set the correct tag values for the windows server.

C. In the Microsoft Azure portal, access the windows server, obtain the private IP address, and assign the IP address under the FortiGate-VM AzureLab address object.

D. Delete the address object and recreate a new address object with the type set to FQDN.

Suggested Answer: *A*
Reference: https://docs.fortinet.com/document/fortigate-public-cloud/6.2.0/azure-administration-guide/985498/troubleshooting-azure-fabric-connector

Community vote distribution
B (62%) C (25%) A (12%)

FortiLeo Most Recent 3 years, 5 months ago
It can't be B now because the filter for the tag is not correct. It should be this format: tag. = and on the screenshot there's a dash.
upvoted 1 times

derrickf 3 years, 6 months ago
They have updated the exam to reflect -1 -- "Run diagnose debug application azd -1 on FortiGate." Although I am still not sure this would be the correct answer.
upvoted 1 times

pojkofd00m 3 years, 6 months ago
Answer must be A, probably a typo from the dump. Will come back and update after passing the certification if I have the question. If not, should be BPlz, we'll greatly appreciate your contribution
upvoted 1 times

pojkofd00m 3 years, 6 months ago
Answer must be A, probably a typo from the dump. Will come back and update after passing the certification if I have the question. If not, should be B
upvoted 1 times

bigbug 3 years, 6 months ago
Plz, we'll greatly appreciate your contribution
upvoted 1 times

charruco 3 years, 8 months ago

B is correct The answer A is incorrect because has a typo "l", The right command is "-1" not "l" diagnose debug application azd -1 https://docs.fortinet.com/document/fortigate-public-cloud/6.2.0/azure-administration-guide/985498/troubleshooting-azure-fabric-connector

upvoted 1 times

mordechayd 3 years, 11 months ago

B. In the Microsoft Azure portal, set the correct tag values for the windows server. A not resolving the issue,just debugging the API communication between fw and azure graph D. Meaning nothing (its cannot resolve the problem) C. Wrong way to the solution

upvoted 4 times

dsmse 4 years ago

"A" is the correct answer. You must solve the problem in the right way and through the right analysis. The purpose is that the connector receives the information dynamically and if the synchronization is failing, the analyst must correct the problem so that the information is correctly synchronized with the environment. https://docs.fortinet.com/document/fortigate-public-cloud/6.0.0/configuring-fabric-connnector-for-fortigate-on-azure-stack/833052/troubleshooting

upvoted 1 times

tachy_22 4 years, 1 month ago

FortiOS_6.4_Azure_Administration_Guide.pdf You can use the diagnose sys sdn status command to view the status of your SDN connectors. You can check if API calls are made successfully by running the following commands in the CLI: diagnose debug enable diagnose debug application azd -1 I think is A

upvoted 3 times

kinge2 4 years, 1 month ago

The answer is C as you cannot execute the command azd -l on the Fortigate firewall. Also this link indicate that the error is missing object in Azure AD - https://docs.fortinet.com/document/fortigate/6.2.0/new-features/432538/fsso-dynamic-address-subtype-6-2-2

upvoted 1 times

elgato01 4 years, 2 months ago

Selected Answer: A

Very tricky question, it is telling you that the object was configured successfully, however if we take option C, the address object will be added as static, and maybe i need it to be dynamic, because it may change, so option C would defeat the purpose of SDN Fabric Connector address, however option A seems more realistic, as i would do a debug to see where the problem is, however this would not fix the issue, but it will guide me in the right direction, hopefully. So, option C it is the temporary fix and A would look much realistic.

upvoted 1 times

elgato01 4 years, 2 months ago

Very tricky question, it is telling you that the object was configured successfully, however if we take option C, the address object will be added as static, and maybe i need it to be dynamic, because it may change, so option C would defeat the purpose of SDN Fabric Connector address, however option A seems more realistic, as i would do a debug to see where the problem is, however this would not fix the issue, but it will guide me in the right direction, hopefully. So, option C it is the temporary fix and A would look much realistic.Actually is option B, from the Labs the guy didnt assign the tag to the windows server and when you try to call the object it says unable to resolve, so Option B, final answer.One more point, it says that the connector is successfully connected, which it is true, one thing is the Fabric connector and another thing is the dynamic object, so final option according to the mistake made by the instructor in the Labs from the Azure part, Option B final.

upvoted 1 times

elgato01 4 years, 2 months ago

Actually is option B, from the Labs the guy didnt assign the tag to the windows server and when you try to call the object it says unable to resolve, so Option B, final answer.One more point, it says that the connector is successfully connected, which it is true, one thing is the Fabric connector and another thing is the dynamic object, so final option according to the mistake made by the instructor in the Labs from the Azure part, Option B final.

upvoted 4 times

elgato01 4 years, 2 months ago

Actually is option B, from the Labs the guy didnt assign the tag to the windows server and when you try to call the object it says unable to resolve, so Option B, final answer.

upvoted 4 times

elgato01 4 years, 2 months ago

One more point, it says that the connector is successfully connected, which it is true, one thing is the Fabric connector and another thing is the dynamic object, so final option according to the mistake made by the instructor in the Labs from the Azure part, Option B final.

upvoted 3 times

hippo2048 4 years, 3 months ago

A is incorret, the debug command will only show the error not resolve the issue. B is incorrect, the admin has setup it with suecess D is incorrect, as the type should be Fabric Connectoraddress C seems the correct answer

upvoted 1 times

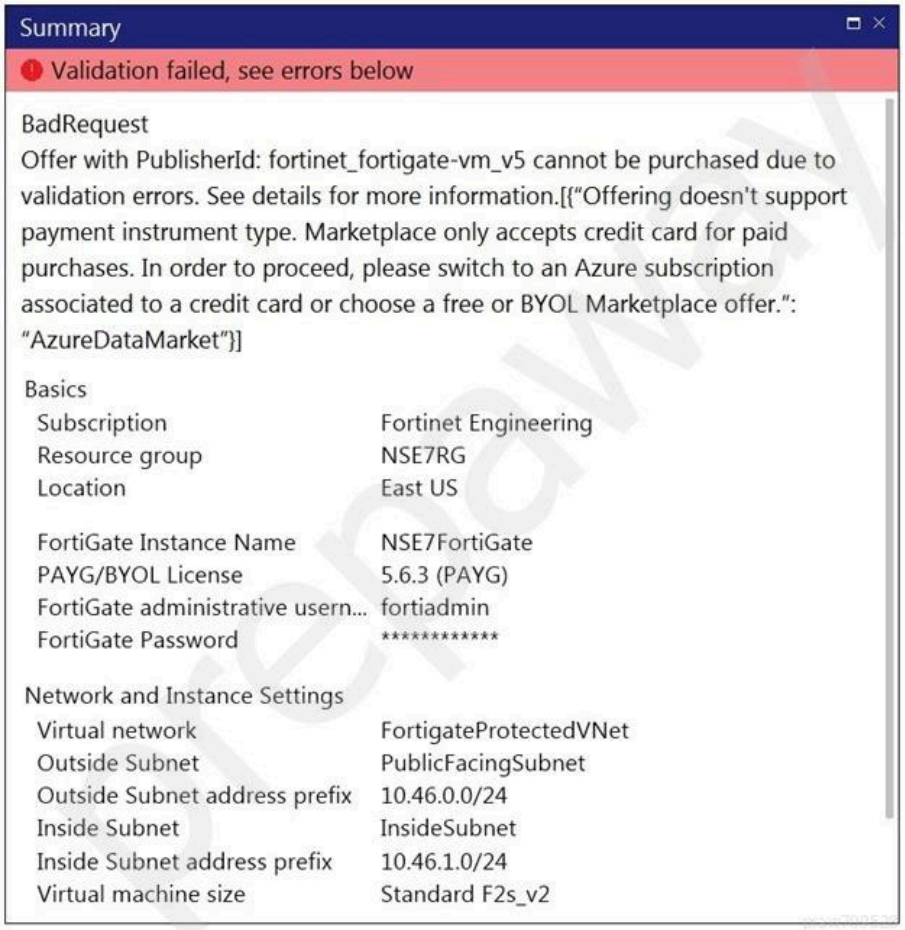
RueDizz 4 years, 4 months ago

C. In the Microsoft Azure portal, access the windows server, obtain the private IP address, and assign the IP address under the FortiGate-VM AzureLab address object.

upvoted 1 times

Question #6 *Topic 1*

Refer to the exhibit. You are deploying a FortiGate-VM in Microsoft Azure using the PAYG/On-demand licensing model. After you configure the FortiGate-VM, the validation process fails, displaying the error shown in the exhibit.
What caused the validation process to fail?



A. You selected the incorrect resource group.

B. You selected the Bring Your Own License (BYOL) licensing mode.

C. You selected the PAYG/On-demand licensing model, but did not select correct virtual machine size.

D. You selected the PAYG/On-demand licensing model, but did not associate a valid Azure subscription.

Suggested Answer: *B*
Reference: https://docs.fortinet.com/document/fortiweb-public-cloud/6.4.0/deploying-auto-scaling-on-azure/9139/frequently-asked-questions

Community vote distribution
D (87%) A (13%)

charruco Most Recent 3 years, 8 months ago
D is correct
upvoted 1 times

charruco 3 years, 8 months ago
D is correct, the issue is related to the Azure subscription and payment. Answer B does not make sense. Fortigate supports (BYOL) licensing mode.
https://docs.fortinet.com/document/fortigate-public-cloud/6.2.0/azure-administration-guide/752225/order-types
upvoted 1 times

dadeadfreak 3 years, 10 months ago
the issue is with the payment, D is the correct answer
upvoted 3 times

tachy_22 4 years, 1 month ago

D is correct

upvoted 3 times

abusdns 4 years, 1 month ago

Option D, Azure subcription error

upvoted 3 times

elgato01 4 years, 2 months ago

Option D, this is a license error associated with the azure subscription

upvoted 3 times

LJCF 4 years, 2 months ago

As an error displayed, the payment method is wrong. D is the correct answer.

upvoted 2 times

Spippolo 4 years, 2 months ago

D. is correct.

upvoted 1 times

hippo2048 4 years, 3 months ago

the issue is with the payment and license type, D is the correct answer

upvoted 3 times

hippo2048 4 years, 3 months ago

the issue is with the payment and license type, D is the correct answerYes agree. D is correct. A is incorrect, Subscriptions is higher tier management level of resource group. https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-setup-guide/organize-resources

upvoted 3 times

rteo82 4 years, 2 months ago

Yes agree. D is correct. A is incorrect, Subscriptions is higher tier management level of resource group. https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-setup-guide/organize-resources

upvoted 2 times

RueDizz 4 years, 4 months ago

A. You selected the incorrect resource group.

upvoted 2 times

Question #7 *Topic 1*

An Amazon Web Services (AWS) auto-scale FortiGate cluster has just experienced a scale-down event, terminating a FortiGate in availability zone C.
This has now black-holed the private subnet in this availability zone.
What action will the worker node automatically perform to restore access to the black-holed subnet?

A. The worker node applies a route table from a non-black-holed subnet to the black-holed subnet.

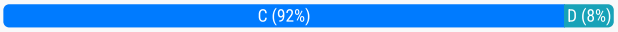
B. The worker node moves the virtual IP of the terminated FortiGate to a running FortiGate on the worker node's private subnet interface.

C. The worker node modifies the route table applied to the black-holed subnet changing its default route to point to a running FortiGate on the worker node's private subnet interface.

D. The worker node migrates the subnet to a different availability zone.

Suggested Answer: *C*
Official Answer: C

Community vote distribution



charruco Most Recent 3 years, 8 months ago
C is correct! C. The worker node modifies the route table applied to the black-holed subnet changing its default route to point to a running FortiGate on the worker node's private subnet interface.
upvoted 1 times

cciesam 3 years, 8 months ago
Ans - C
upvoted 3 times

kinge2 4 years, 1 month ago
C is correct
upvoted 2 times

abusdns 4 years, 1 month ago
C is correct
upvoted 2 times

elgato01 4 years, 2 months ago
Option C, Official documentation, failover process on a single AZ, https://github.com/fortinet/aws-cloudformation-templates/blob/main/FGCP/7.0/SingleAZ/README.md#failover-process || Outbound failover is provided by reassigning the secondary IP addresses of ENI1\port2 from FortiGate 1's private interface to FortiGate 2's private interface. ##Additionally any route targets referencing FortiGate 1's private interface will be updated to reference FortiGate 2's private interface.##
upvoted 3 times

goCisco 4 years, 2 months ago
Answer is B https://github.com/fortinet/aws-cloudformation-templates/tree/master/LambdaAA-RouteFailover/6.0
upvoted 1 times

goCisco 4 years, 2 months ago
Answer is B https://github.com/fortinet/aws-cloudformation-templates/tree/master/LambdaAA-RouteFailover/6.0Sorry, it should be C. Because the route table on the black-holed subnet is updated for its default route to point to the working FG. https://github.com/fortinet/aws-cloudformation-templates/tree/master/LambdaAA-RouteFailover/6.0
upvoted 1 times

goCisco 4 years, 2 months ago
Sorry, it should be C. Because the route table on the black-holed subnet is updated for its default route to point to the working FG. https://github.com/fortinet/aws-cloudformation-templates/tree/master/LambdaAA-RouteFailover/6.0
upvoted 2 times

RueDizz 4 years, 4 months ago
D. The worker node migrates the subnet to a different availability zone.
upvoted 1 times

Question #8 *Topic 1*

Which two statements about the Amazon Cloud Services (AWS) network access control lists (ACLs) are true? (Choose two.)

A. Network ACLs are stateless, and inbound and outbound rules are used for traffic filtering.

B. Network ACLs are stateful, and inbound and outbound rules are used for traffic filtering.

C. Network ACLs must be manually applied to virtual network interfaces.

D. Network ACLs support allow rules and deny rules.

Suggested Answer: *A, D*

Reference: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

Community vote distribution

AD (100%)

charruco Most Recent 3 years, 8 months ago

AD Correct! https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html Network ACLs are stateless. Security groups are stateful.

upvoted 1 times

charruco 3 years, 8 months ago

AD Correct! https://aws.amazon.com/premiumsupport/knowledge-center/security-network-acl-vpc-endpoint/ -Network ACLs are stateless. You must define rules for both outbound and inbound traffic.

upvoted 1 times

cciesam 3 years, 8 months ago

Ans - AD

upvoted 3 times

kinge2 4 years, 1 month ago

they are corretc

upvoted 2 times

elgato01 4 years, 2 months ago

Options A and D, Official documentation under Network ACL basics: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

upvoted 2 times

Spippolo 4 years, 2 months ago

Public Cloud Security 6.4 Study Guide (pag. 88) A, D.

upvoted 2 times

Question #9 *Topic 1*

When an organization deploys a FortiGate-VM in a high availability (HA) (active/active) architecture in Microsoft Azure, they need to determine the default timeout values of the load balancer probes.
In the event of failure, how long will Azure take to mark a FortiGate-VM as unhealthy, considering the default timeout values?

A. Less than 10 seconds

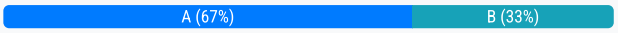
B. 30 seconds

C. 20 seconds

D. 16 seconds

Suggested Answer: *A*
Official Answer: A

Community vote distribution



rac_sp Most Recent 3 years, 6 months ago
It is less than 10 seconds. First it is ACTIVE ACTIVE configuration, so Azure Load balancer as soon as detect the failure mark the device as unhealthy. I´d recommend you mark this question and send do feedback in the exam if you face it. FINALLY if you check the LAB recorded in the oficial NSE course from Fortinet Portal, the instructor does test the LOAD BALANCE and clearly states that the Fortigate machine ACTIVE ACTIVE HA becomes unhealty in less than 10 seconds in case of failure, of if the official instructors says that recorded who am I to disagree ?
upvoted 1 times

charruco 3 years, 8 months ago
A. Less than 10 seconds
upvoted 1 times

charruco 3 years, 8 months ago
Answer A In my opinion, the question is related to Azure "take an action" https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview -If your application produces a time-out response just before the next probe arrives, the detection of the events will take 5 seconds plus the duration of the application time-out when the probe arrives. You can assume the detection to take slightly over 5 seconds. -If your application produces a time-out response just after the next probe arrives, the detection of the events won't begin until the probe arrives and times out, plus another 5 seconds. You can assume the detection to take just under 10 seconds. Assume the reaction to a time-out response will take a minimum of 5 seconds and a maximum of 10 seconds to react to the change.
upvoted 1 times

mordechayd 3 years, 11 months ago
https://github.com/fortinet/azure-templates/blob/main/FortiGate/Active-Active-ELB-ILB/azuredeploy.json#L580 its an a-a architecture and the default TCP probe is 5x2 (every 5 seconds X 2 Intervals for failover)
upvoted 3 times

kinge2 4 years ago
Selected Answer: A
Any manipulation of UDRs or public IP addresses for active-passive solutions take 30 seconds to be applied after failover is initiated, whereas Azure load balancers can send probes as often as every five seconds and will stop forwarding traffic after two failures
upvoted 1 times

kinge2 4 years ago
Any manipulation of UDRs or public IP addresses for active-passive solutions take 30 seconds to be applied after failover is initiated, whereas Azure load balancers can send probes as often as every five seconds and will stop forwarding traffic after two failuresThe question is related to "FTG Active/Active architecture"
upvoted 1 times

charruco 3 years, 8 months ago
The question is related to "FTG Active/Active architecture"
upvoted 1 times

dsmse 4 years ago

"A" is the best answer. From 6 to 10 seconds... https://docs.fortinet.com/document/fortigate-public-cloud/6.0.0/use-case-high-availability-for-fortigate-on-azure/224311/basic-concepts Remembering: FortiGate Scenario (HA Active/Active)

upvoted 1 times

tachy_22 4 years, 1 month ago

HA Failover: * 30 seconds -- 2 minutes is Active -Passive * less 10 seconds is Active - Active I think is A.

upvoted 1 times

elgato01 4 years, 2 months ago

Another tricky question, option B would look the best fit hier, Azure official documentation under HTTP/HTTPS probe. it says that how much time would it take to mark a fortigate vm down, here is assuming that we are probing the vm over its http/https server. https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview

upvoted 1 times

Spippolo 4 years, 2 months ago

B. https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview

upvoted 1 times

hippo2048 4 years, 3 months ago

B, 30 seconds. The default health monitoring tests the three servers every 30 seconds for a healthy HTTP response with a 30 second timeout for each request. https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-probe-overview

upvoted 1 times

RueDizz 4 years, 4 months ago

B. 30 seconds

upvoted 1 times