Microsoft Discussions

Exam AZ-900 All Questions

View all questions & answers for the AZ-900 exam

Go to Exam

EXAM AZ-900 TOPIC 1 QUESTION 262 DISCUSSION

Actual exam question from Microsoft's AZ-900

Question #: 262

Topic #: 1

[All AZ-900 Questions]

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your Azure environment contains multiple Azure virtual machines.

You need to ensure that a virtual machine named VM1 is accessible from the Internet over HTTP.

Solution: You modify an Azure firewall.

Does this meet the goal?

A. Yes

B. No

Show Suggested Answer

by NoNotSpam at *Nov. 7, 2019, 6:27 p.m.*

Comments

Type your comment...

Submit

foreverlearner Highly Voted 4 years, 5 months ago

You can either modify a firewall or modify a NSG. For basic allow/deny traffic, NSG is enough. But the same can be achieved with Firewall as well.
"The Azure Firewall service complements network security group functionality. Together, they provide better "defense-in-depth" network security. Network security groups provide distributed network layer traffic filtering to limit traffic to resources within virtual networks in each subscription. Azure Firewall is a fully stateful, centralized network firewall as-a-service, which provides network- and application-level protection across different subscriptions and virtual networks."
https://docs.microsoft.com/en-us/azure/firewall/firewall-faq

upvoted 51 times

Chris0105 3 years, 6 months ago

You are right. see as well question #133, so it must be firewall or NSG. I actually thought it was just NSG - seems I am wrong.

upvoted 3 times

thebadfella 3 years, 2 months ago

Guys, forget about the question for a moment and look at your on-prem infra, you need to whitelist in FW first for any legitmate inbound access. So answer is "YES"

upvoted 3 times

lehoang15tuoi 3 years, 10 months ago

Your logic is not clear. To put it simply, both Firewall and NSG can be used to block traffic. Think of them like 2 gates on the same walkway. You open one and close one, can you pass through both? The NSG default rule is blocking all inbound traffic, so if you don't do anything with it, it doesn't matter what you do with the firewall.

upvoted 15 times

Mozbius_ 2 years, 10 months ago

EXACTLY my chain of thought. But then again... They didn't specify that a NSG has been set up (NSG's are not set by default when you create a vm...) so the only thing that could prevent a vm from communicating on port 80 is the firewall...

upvoted 3 times

PhilB1000 Highly Voted 4 years, 8 months ago

https://docs.microsoft.com/en-us/azure/firewall/firewall-faq#what-is-the-difference-between-network-security-groups-nsgs-and-azure-firewall
What is the difference between Application Gateway WAF and Azure Firewall?

The Web Application Firewall (WAF) is a feature of Application Gateway that provides centralized inbound protection of your web applications from common exploits and vulnerabilities. Azure Firewall provides inbound protection for non-HTTP/S protocols (for example, RDP, SSH, FTP), outbound network-level protection for all ports and protocols, and application-level protection for outbound HTTP/S.

upvoted 14 times

if10w Most Recent 1 week, 3 days ago

Modifying an Azure firewall alone will not ensure that VM1 is accessible from the Internet over HTTP. While an Azure firewall can control and filter network traffic, you also need to configure other components to allow HTTP access.

Here are the steps you should take:

Network Security Group (NSG):
Ensure that there is an NSG associated with the subnet or network interface of VM1.
Add an inbound security rule to allow HTTP traffic (port 80).
Public IP Address:
Ensure that VM1 has a public IP address assigned to it.
VM's Firewall Settings:
Ensure that the Windows Firewall on VM1 allows inbound HTTP traffic.
These steps, combined with any necessary Azure firewall rules, will ensure that VM1 is accessible over HTTP from the Internet.

If you need more detailed instructions on any of these steps, feel free to ask!

upvoted 1 times

Nathan12345 1 month, 3 weeks ago

Selected Answer: A

can modify in firewall

upvoted 1 times

Alsari 3 months ago

Selected Answer: B

Modifying an Azure firewall alone does not meet the goal. To ensure that VM1 is accessible from the Internet over HTTP, you should modify the Network Security Group (NSG) associated with VM1 to allow inbound traffic on port 80 (HTTP). Additionally, you need to ensure that the VM has a public IP address and that any necessary routing or load balancing configurations are correctly set.

upvoted 3 times

Marcal 1 year, 5 months ago

No, modifying an Azure firewall would not meet the goal of ensuring that a virtual machine named VM1 is accessible from the Internet over HTTP. To achieve this goal, you would need to configure the network security group (NSG) associated with VM1 to allow inbound traffic on port 80 (HTTP).

upvoted 2 times

BengalTigers 1 year, 7 months ago

B. No.

Modifying an Azure firewall alone will not ensure that a virtual machine named VM1 is accessible from the Internet over HTTP. Instead, you need to configure the network security group (NSG) associated with the VM1's network interface to allow inbound traffic on port 80 (HTTP) from the Internet. Additionally, you may also need to configure any applicable Azure load balancer, DNS, or public IP settings to ensure proper connectivity.

upvoted 3 times

zellck 1 year, 9 months ago

Selected Answer: A

A is the answer.

upvoted 1 times

jokerbase 2 years, 5 months ago

Follow this article:
https://adamtheautomator.com/azure-firewall/
We can choose Azure Firewall or NSG. It's also working together. We also can create a VM without NSG. Almost the example they created the VM with NSG because it's free. Azure Firewall is not free. That's all.

upvoted 3 times

MS_Learner 2 years, 8 months ago

Got Feb 10, 2022, this question came in a way where they list 4 options, so I choose Azure firewall.

upvoted 2 times

mikamozg 2 years, 11 months ago

Firewall, WAF and NSG
Application rules aren't applied for inbound connections. So if you want to filter inbound HTTP/S traffic, you should use Web Application Firewall (WAF). Or alternatively you can tweak NSG because by default everything is closed on NSG once it is created and assigned to vnet, subnet or vnic.
Below is tutorial how to setup firewall and vnet, but if you go through you will see that all conversation is about outbound trafic not inbound may be because Azure Firewall application rules aren't applied for inbound connections. So we left with WAF or NSG.
https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal

upvoted 1 times

> **mikamozg** 2 years, 11 months ago
>
> in addition if you go through the deploy guide you will see that making changes to firewall is not enough you always need to do additional things like create default route in ip tables or create default route in VM in order to direct traffic to firewall. so answering to test question making changes on Firewall is not enough.
>
> upvoted 1 times
>
> > **mikamozg** 2 years, 11 months ago
> >
> > https://docs.microsoft.com/en-us/azure/virtual-machines/windows/nsg-quickstart-portal
> > You open a port, or create an endpoint, to a virtual machine (VM) in Azure by creating a network filter on a subnet or a VM network interface. You place these filters, which control both inbound and outbound traffic, on a network security group attached to the resource that receives the traffic.
> >
> > upvoted 1 times
> >
> > > **mikamozg** 2 years, 11 months ago
> > >
> > > everytime you search for the correct answer or solution NSG comes up:
> > > https://docs.microsoft.com/en-us/answers/questions/182838/need-to-enable-ports-80-and-443-along-with-inbound.html
> > >
> > > upvoted 1 times

manfredw 3 years, 2 months ago

correct

upvoted 1 times

stefano1856 3 years, 4 months ago

In Microsoft Learning Path is stated :
Azure Firewall provides Inbound protection for non-HTTP/S protocols (for example, RDP, SSH, and FTP)
https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/7-combine-services-complete-solution#:~:text=Azure%20Firewall%20provides,and%20FTP

upvoted 2 times

Eka22 3 years, 5 months ago

hey guys...in my opinion the answer is correct it should be YES. In simple words , NSGs allow authentic ends to communicate and doesn't care about the data exchange, on the other hand, Azure Firewall does the same thing as NSG but, it also checks the data transfer. So the best suitable here to use is Azure Firewall.

upvoted 1 times

Kavitw 3 years, 6 months ago

correct answer

upvoted 1 times

CARIOCA 3 years, 6 months ago

This question is very divided in the feedback after all what would be the answer and which justified it?

upvoted 1 times

Tas006 3 years, 6 months ago

Answer is A. This question came out on the 05.03.2021

upvoted 2 times

Load full discussion...

Using our own resources, we strive to strengthen the IT professionals community for free.

ExamTopics doesn't offer Real Microsoft Exam Questions. ExamTopics doesn't offer Real Amazon Exam Questions. ExamTopics Materials do not contain actual questions and answers from Cisco's Certification Exams.

CFA Institute does not endorse, promote or warrant the accuracy or quality of ExamTopics. CFA® and Chartered Financial Analyst® are registered trademarks owned by CFA Institute.