

- Expert Verified, Online, Free.

**■** MENU Q

**G** 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 231 DISCUSSION**

Actual exam question from Microsoft's AZ-900

Question #: 231

Topic #: 1

[All AZ-900 Questions]

**HOTSPOT** -

To complete the sentence, select the appropriate option in the answer area.

Hot Area:

### **Answer Area**

Application rules Network Address Translation (NAT) rules Network rules Service tags

in Azure Firewall enables users on the internet to access a server on a virtual network.

**Show Suggested Answer** 

by 8 Mev4953 at Sept. 28, 2021, 5:17 p.m.

#### **Comments**

Type your comment...

**Submit** 



Georges Highly Voted 1 3 years and

🗾 o jeuro ugo If you configure network rules and application rules, then network rules are applied in priority order before application rules. NAT rules are applied in priority before network rules. I would go with NAT. https://docs.microsoft.com/en-us/azure/firewall/rule-processing upvoted 14 times ■ Jason71 (Highly Voted 1 3 years ago Got this on the 19/10/2021 exam! upvoted 6 times ■ NoursBear Most Recent ② 2 months, 4 weeks ago It sounds like an inbound request so going for DNAT upvoted 1 times 😑 🏜 varinder82 5 months ago Final Answer: Network Rules upvoted 1 times 🖃 🏜 azirila 1 year, 9 months ago basic knowlegde firewal upvoted 1 times □ ♣ TonyghostR05 2 years ago NAT same as SC-900 upvoted 1 times 😑 📤 Eleftheriia 2 years, 9 months ago The following might be helpful: "Azure Virtual Network NAT is a network address translation service running in Azure. With Azure Virtual Network NAT, you can provide secure outbound connectivity to virtual instances in a private subnet so they can connect outside your virtual network." upvoted 3 times ■ mufflon 2 years, 10 months ago Inbound traffic refers to information coming-in to a network. The question is about incoming traffic. https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat-policy upvoted 2 times 🖃 📤 Ajaykrish 2 years, 10 months ago got it on 29-Nov-2021 👍 🤚 🏴 upvoted 2 times E kruize99 2 years, 11 months ago Answer is NAT. NAT takes priority before network rules for inbound traffic: https://docs.microsoft.com/enus/azure/firewall/rule-processing#dnat-rules-and-network-rules upvoted 2 times ■ MasoudK 2 years, 11 months ago there are two connectivity: inbound and outbound. DNAT is for filtering inbound traffic and not internet access(outbound). So I would go for Network rule. upvoted 4 times MasoudK 3 years ago Network Address Translation (NAT) rules that define destination IP addresses and ports to translate inbound requests. Question is access from Internet to a az resource(VM) sounds like an outbound request. I agree with Network rules upvoted 2 times Removed] 2 years, 6 months ago I agree. I think it is Network Rules. NAT is to keep connection internally or to have a private network connect to internet but does not allow internal connection from the internet. NAT makes no sense here. NAT is supposed to protect internal networks from outside connections (internet). upvoted 2 times mufflon 2 years, 10 months ago Inbound traffic refers to information coming-in to a network. The question is about incoming traffic. https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat-policy upvoted 1 times E TTAKU 3 years ago

it should be "Network Rules", https://docs.microsoft.com/en-us/azure/firewall/rule-processing

upvoted 3 times

😑 📤 Gorilla5 3 years ago

I guess answer is correct. This is from website you have pasted link into"Inbound Internet connectivity can be enabled by configuring Destination Network Address Translation (DNAT) as described in Tutorial: Filter inbound traffic with Azure Firewall DNAT using the Azure portal. NAT rules are applied in priority before network rules"

upvoted 1 times

### ■ Mev4953 3 years ago

It is answer from 194.

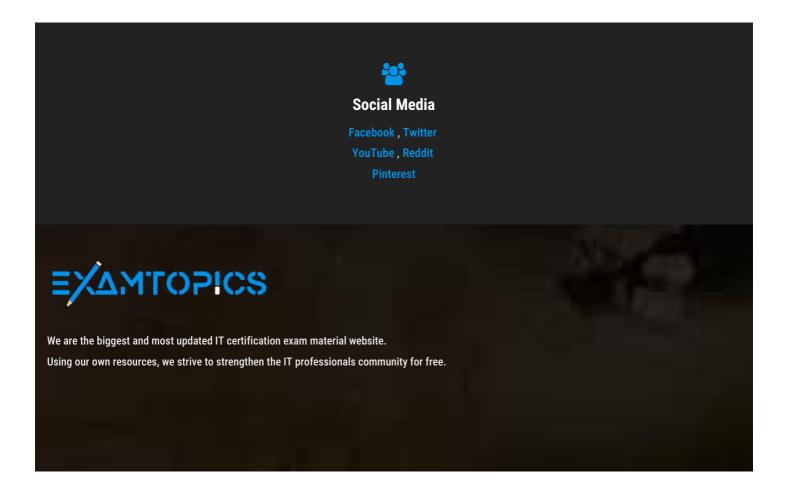
Perimeter

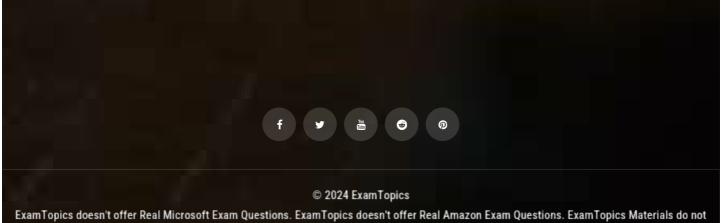
- Use distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for end users.
- Use perimeter firewalls to identify and alert on malicious attacks against your network.

But it doesnt match with this. According to this answer, it should be Perimeter Layer

upvoted 1 times

## Start Learning 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.