Exam AZ-700 topic 3 question 19 discussion

×

Switch to a voting comment New

Type your comment...

Submit

flurgen248 1 year, 2 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-monitor?pivots=front-door-standard-premium#waf-logs

Client IP is the IP address of the client that made the request. If there was an X-Forwarded-For header in the request, the client IP address is taken from that header field instead.

There wasn't an X-Forwarded-For header, so it is your IP address. Creating a WAF exclusion would allow you to connect, but that is not the goal. Any connections from a different IP would still get the 403 error.

The answer is No.

upvoted 1 times

daemon101 10 months ago

Agree. The requirement is "You need to ensure that the URL is accessible through the application gateway from any IP address".

upvoted 1 times

Nicolas_UY 1 year, 4 months ago

Selected Answer: B

B. No

Creating a WAF policy exclusion for request headers that contain 137.135.10.24 will not ensure that the URL is accessible through the application gateway from any IP address. Instead, you should check the WAF rules and policy settings to ensure that the IP address or range of IP addresses from which you are trying to access the URL is not being blocked by the WAF. You may also need to check the access control lists (ACLs) and network security groups (NSGs) associated with the application gateway to ensure that traffic from the desired IP addresses is allowed.

upvoted 2 times

DeepMoon 1 year, 7 months ago

Given Answer is Correct:

Disabling a client IP for missing an Accept Header is definitely not the answer.

upvoted 2 times