DUMPSBOSS.

Fortinet NSE 6 - FortiWeb 6.1

Fortinet NSE6_FWB-6.1

Version Demo

Total Demo Questions: 5

Total Premium Questions: 30

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Which regex expression is the correct format for redirecting the URL http://www.example.com?

A. www\.example\.com

B. www.example.com

C. www\example\com

D. www/.example/.com

ANSWER: B

Explanation:

\1://www.company.com/\2/\3

Reference: https://learn.akamai.com/en-us/webhelp/edge-redirector/edge-redirector-guide/GUID-0C22DFC2-DCC4-42AF-BDB2-9537FBEE03FD.html

QUESTION NO: 2

A client is trying to start a session from a page that would normally be accessible only after the client has logged in.

When a start page rule detects the invalid session access, what can FortiWeb do? (Choose three.)

A. Display an access policy message, then allow the client to continue

B. Redirect the client to the login page

C. Allow the page access, but log the violation

D. Prompt the client to authenticate

E. Reply with a 403 Forbidden HTTP error

ANSWER: B C E

Explanation:

Reference: https://help.fortinet.com/fweb/607/Content/FortiWeb/fortiweb-admin/specify_urls_to_initiate.htm

QUESTION NO: 3

How does FortiWeb protect against defacement attacks?

A. It keeps a complete backup of all files and the database.

B. It keeps hashes of files and periodically compares them to the server.

C. It keeps full copies of all files and directories.

D. It keeps a live duplicate of the database.

ANSWER: B

Explanation:

The anti-defacement feature examines a web site's files for changes at specified time intervals. If it detects a change that could indicate a defacement attack, the FortiWeb appliance can notify you and quickly react by automatically restoring the web site contents to the previous backup.

Reference: https://help.fortinet.com/fweb/551/Content/FortiWeb/fortiweb-admin/anti_defacement.htm

QUESTION NO: 4

When is it possible to use a self-signed certificate, rather than one purchased from a commercial certificate authority?

A. If you are a small business or home office

B. If you are an enterprise whose employees use only mobile devices

C. If you are an enterprise whose resources do not need security

D. If you are an enterprise whose computers all trust your active directory or other CA server

ANSWER: C

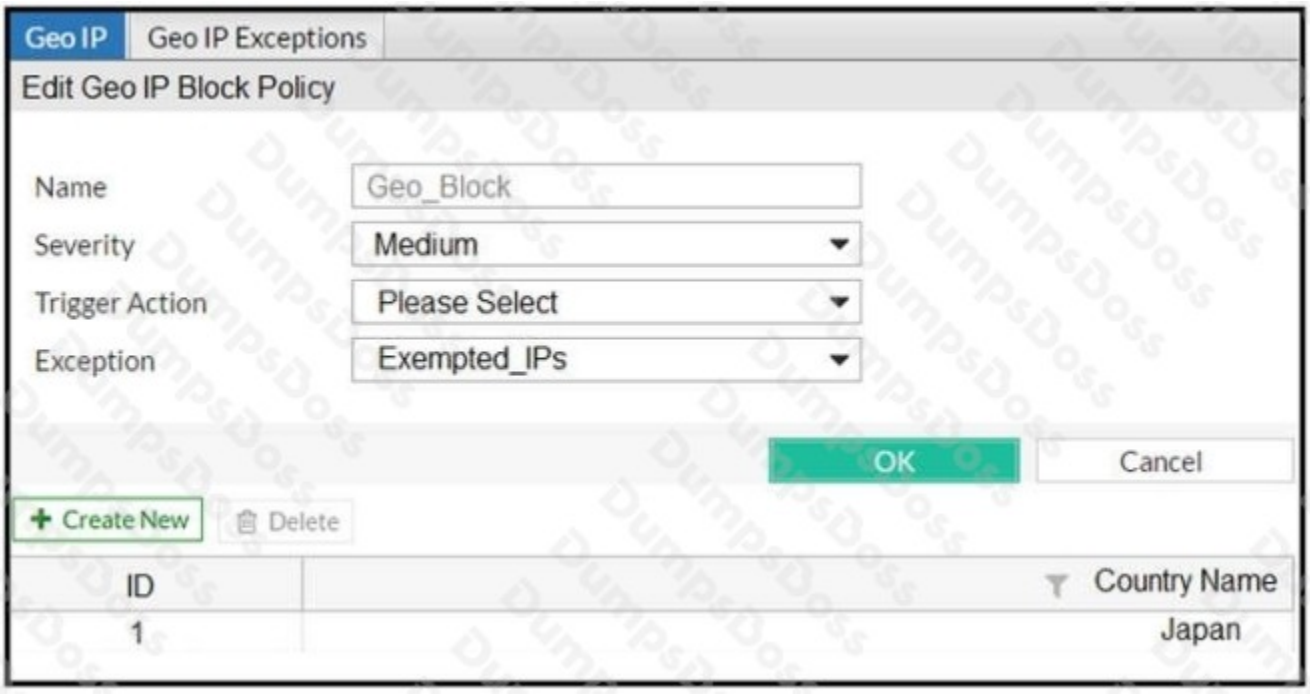
Explanation:

This can include SSL/TLS certificates, code signing certificates, and S/MIME certificates. The reason why they're considered different from traditional certificate-authority signed certificates is that they're created, issued, and signed by the company or developer who is responsible for the website or software being signed. This is why self-signed certificates are considered unsafe for public-facing websites and applications.

Reference: https://sectigostore.com/page/what-is-a-self-signed-certificate/

QUESTION NO: 5

Refer to the exhibit.



FortiWeb is configured to block traffic from Japan to your web application server. However, in the logs, the administrator is seeing traffic allowed from one particular IP address which is geo-located in Japan.

What can the administrator do to solve this problem? (Choose two.)

A. Manually update the geo-location IP addresses for Japan.

B. If the IP address is configured as a geo reputation exception, remove it.

C. Configure the IP address as a blacklisted IP address.

D. If the IP address is configured as an IP reputation exception, remove it.

ANSWER: A C

Explanation:

IP reputation leverages many techniques for accurate, early, and frequently updated identification of compromised and malicious clients so you can block attackers before they target your servers.

IP blacklisting is a method used to filter out illegitimate or malicious IP addresses from accessing your networks. Blacklists are lists containing ranges of or individual IP addresses that you want to block. Reference:
https://docs.fortinet.com/document/fortiweb/6.3.5/administration-guide/137271/blacklisting-whitelisting-clients
https://www.imperva.com/learn/application-security/ip-blacklist/