NSE6_FWB-6.4$^{\text{Q\&As}}$

Fortinet NSE 6 - FortiWeb 6.4

Pass Fortinet NSE6_FWB-6.4 Exam with 100% Guarantee

QUESTION 1

Which statement about local user accounts is true?

A. They are best suited for large environments with many users.

B. They cannot be used for site publishing.

C. They must be assigned, regardless of any other authentication.

D. They can be used for SSO.

Correct Answer: B

QUESTION 2

What role does FortiWeb play in ensuring PCI DSS compliance?

A. PCI specifically requires a WAF

B. Provides credit card processing capabilities

C. Provide ability to securely process cash transactions

D. Provides load balancing between multiple web servers

Correct Answer: A

FortiWeb helps you meet all PCI requirements, but PCI now specifically recommends using a WAF, and developing remediations against the top 10 vulnerabilities, according to OWASP.

QUESTION 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.

Correct Answer: B

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 4

How does your FortiWeb configuration differ if the FortiWeb is upstream of the SNAT device instead of downstream of the SNAT device?

A. You must enable the "Use" X-Forwarded-For: option.

B. FortiWeb must be set for Transparent Mode

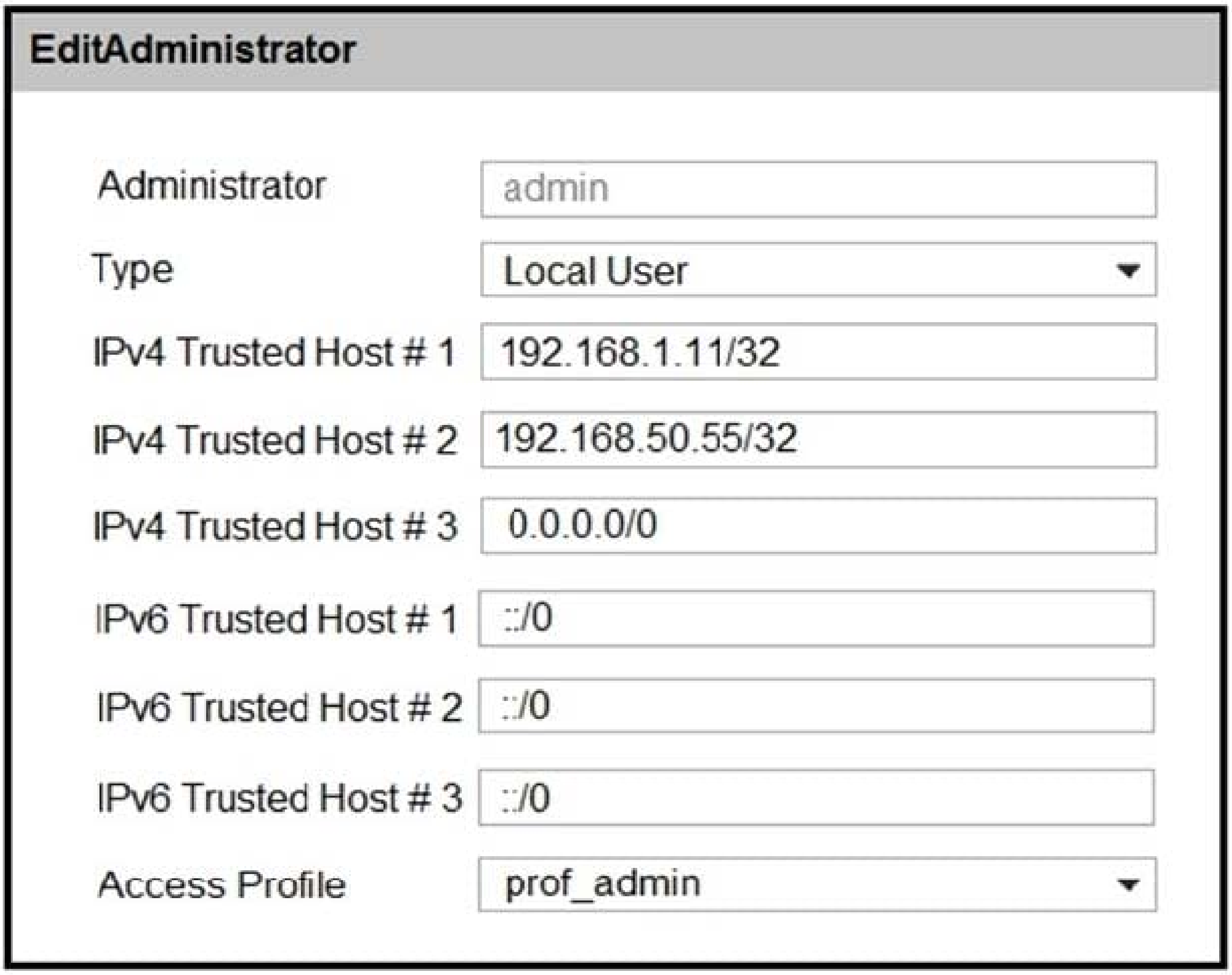
C. No special configuration required

D. You must enable "Add" X-Forwarded-For: instead of the "Use" X-Forwarded-For: option.

Correct Answer: D

QUESTION 5

Refer to the exhibit.



EditAdministrator

Administrator	admin
Type	Local User
IPv4 Trusted Host # 1	192.168.1.11/32
IPv4 Trusted Host # 2	192.168.50.55/32
IPv4 Trusted Host # 3	0.0.0.0/0
IPv6 Trusted Host # 1	::/0
IPv6 Trusted Host # 2	::/0
IPv6 Trusted Host # 3	::/0
Access Profile	prof_admin

There is only one administrator account configured on FortiWeb. What must an administrator do to restrict any brute force attacks that attempt to gain access to the FortiWeb management GUI?

A. Delete the built-in administrator user and create a new one.

B. Configure IPv4 Trusted Host # 3 with a specific IP address.

C. The configuration changes must be made on the upstream device.

D. Change the Access Profile to Read_Only.

Correct Answer: B

Reference: https://docs.fortinet.com/document/fortiweb/6.1.1/administration-guide/397469/preventing-brute-force-logins