# NSE8_812 Q&As

Network Security Expert 8 Written Exam

## Pass Fortinet NSE8_812 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

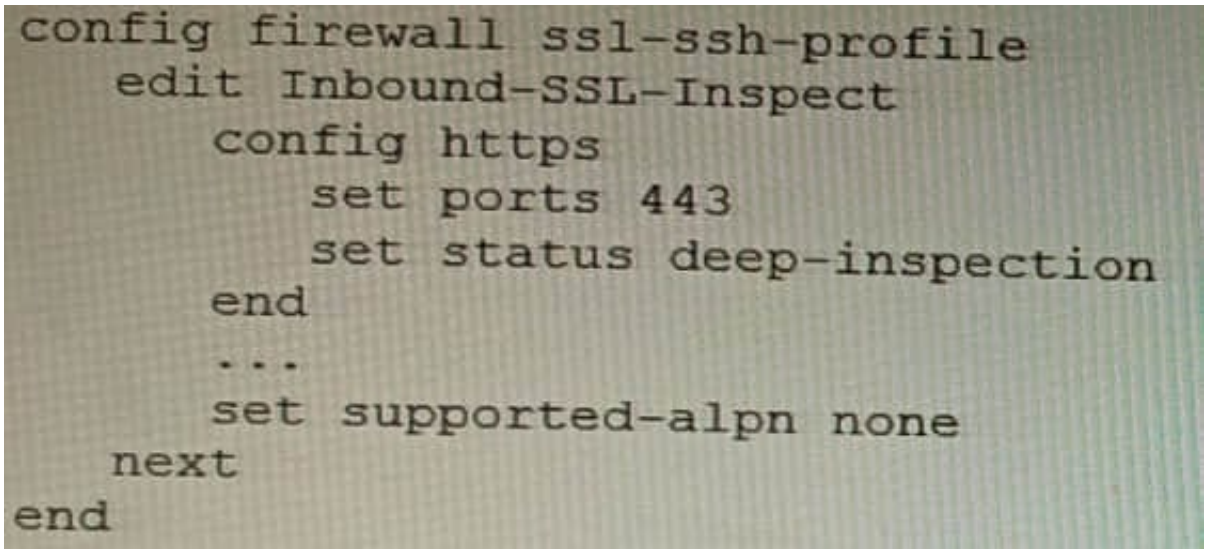
**https://www.pass4itsure.com/nse8_812.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

**QUESTION 1**

Refer to the CLI configuration of an SSL inspection profile from a FortiGate device configured to protect a web server:




Based on the information shown, what is the expected behavior when an HTTP/2 request comes in?

A. FortiGate will reject all HTTP/2 ALPN headers.

B. FortiGate will strip the ALPN header and forward the traffic.

C. FortiGate will rewrite the ALPN header to request HTTP/1.

D. FortiGate will forward the traffic without modifying the ALPN header.

Correct Answer: A

Explanation: Thesupported-alpnparameter is set tohttp1.1in the SSL inspection profile. This means that the FortiGate will only accept HTTP/1.1 traffic. Any HTTP/2 traffic will be rejected.

The following is the relevant documentation from Fortinet:

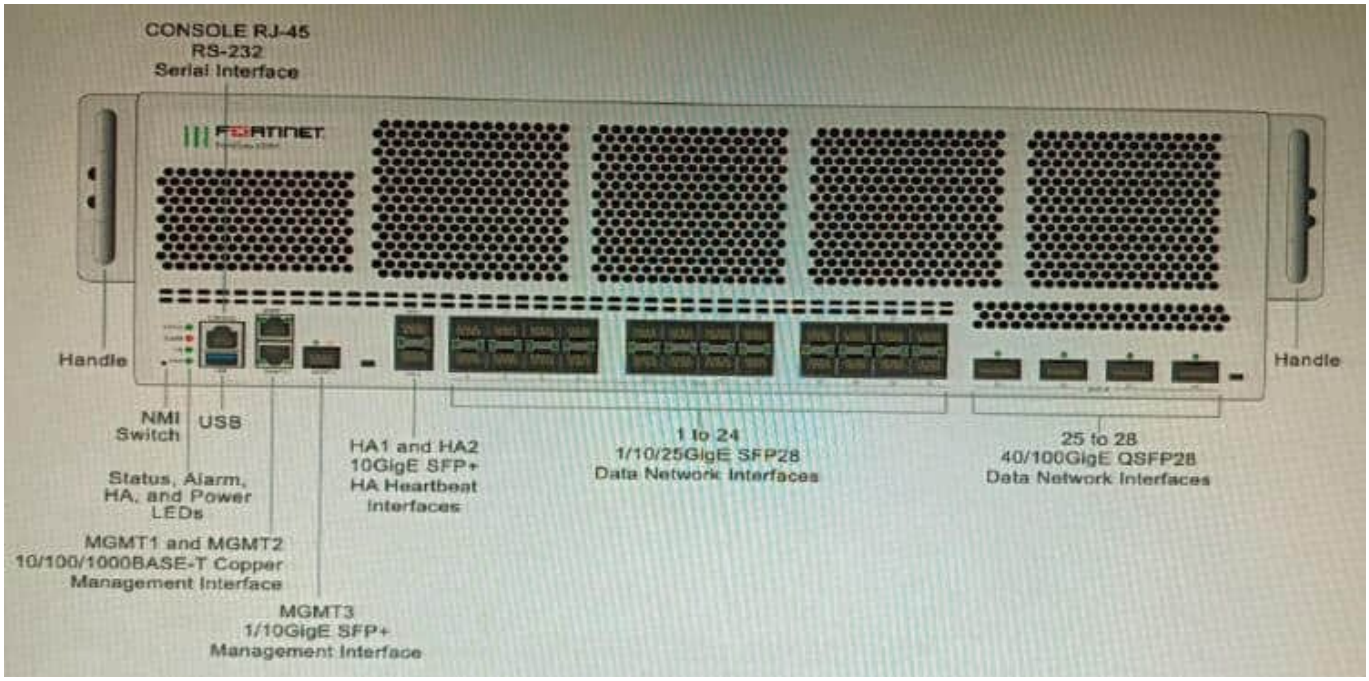
Thesupported-alpnparameter specifies the list of ALPN protocols that the FortiGate will accept. If the client requests a protocol that is not in this list, the FortiGate will reject the connection.

The default value for thesupported-alpnparameter isall. This means that the FortiGate will accept any ALPN protocol that the client requests. To reject all HTTP/2 traffic, set thesupported-alpnparameter tohttp1.1. Source: https://

docs.fortinet.com/document/fortigate/7.0.0/new-features/710924/http-2- support-in-proxy-mode-ssl-inspection

**QUESTION 2**

Refer to the exhibit.




You are deploying a FortiGate 6000F. The device should be directly connected to a switch. In the future, a new hardware module providing higher speed will be installed in the switch, and the connection to the FortiGate must be moved to this higher-speed port.

You must ensure that the initial FortiGate interface connected to the switch does not affect any other port when the new module is installed and the new port speed is defined.

How should the initial connection be made?

A. Connect the switch on any interface between ports 21 to 24

B. Connect the switch on any interface between ports 25 to 28

C. Connect the switch on any interface between ports 1 to 4

D. Connect the switch on any interface between ports 5 to 8.

Correct Answer: C

Explanation: The FortiGate 6000F has 24 1/10/25-Gbps SFP28 data network interfaces (1 to 24). These interfaces are divided into the following interface groups: 1 to 4, 5 to 8, 9 to 12, 13 to 16, 17 to 20, and 21 to 24. The ports 25 to 28 are

40/100-Gbps QSFP28 data network interfaces.

The initial connection should be made to any interface between ports 1 to 4. This is because the ports 21 to 24 are part of the same interface group, and changing the speed of one of these ports will affect the speeds of all of the ports in the

group. The ports 5 to 8 are also part of the same interface group, so they should not be used for the initial connection. The new hardware module that will be installed in the switch will provide higher speed ports. When this module is installed,

the speed of the ports 21 to 24 will be increased. However, this will not affect the ports 1 to 4, because they are not part of the same interface group.

Therefore, the initial connection should be made to any interface between ports 1 to 4, in order to ensure that the FortiGate interface connected to the switch does not affect any other port when the new module is installed and the new port

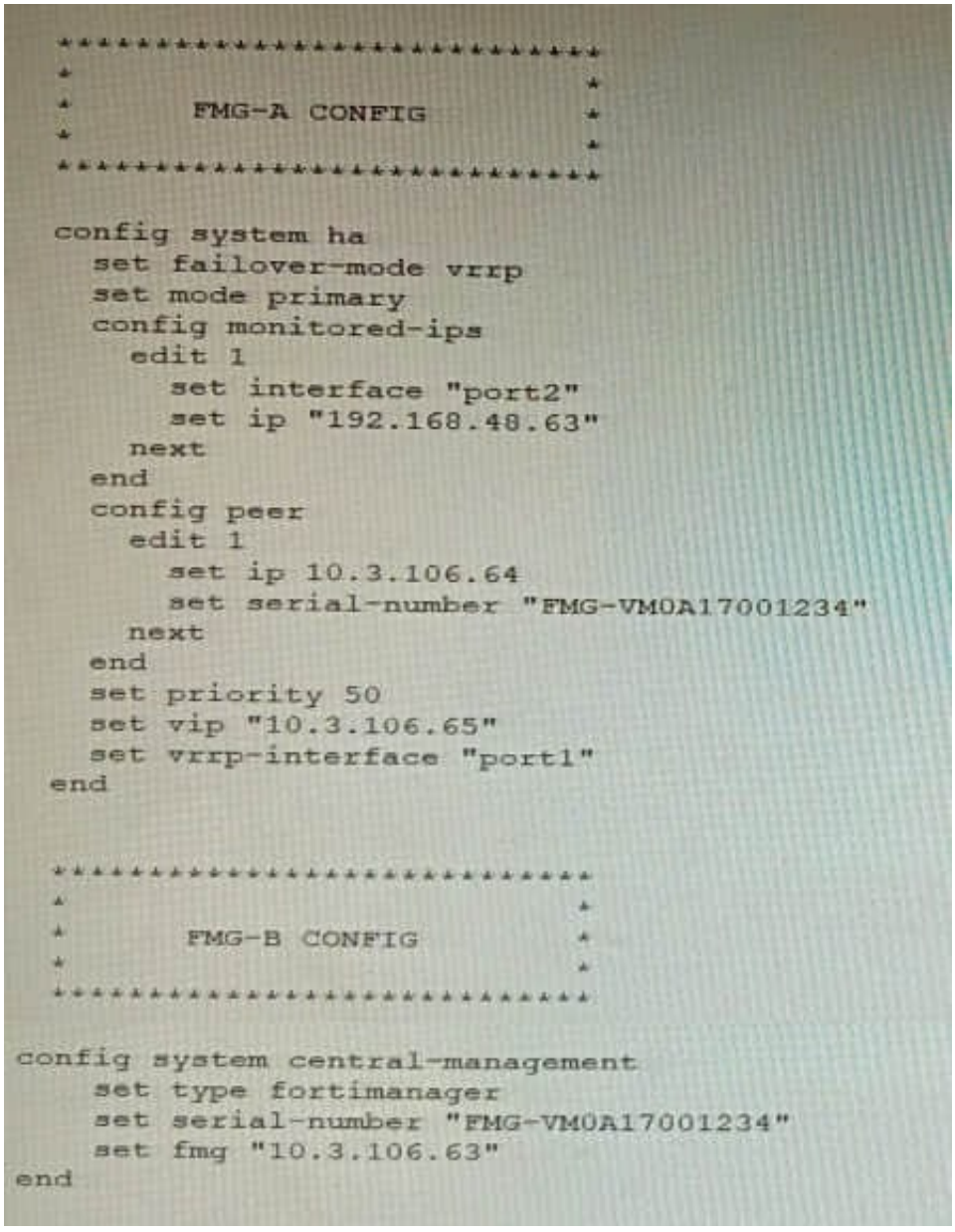
speed is defined.

Reference:

FortiGate 6000F Front Panel Interfaces: https://docs.fortinet.com/document/fortigate- 6000/hardware/fortigate-6000f-system-guide/827055/front-panel-interfaces

**QUESTION 3**

Refer to the exhibit showing FortiGate configurations



FortiManager VM high availability (HA) is not functioning as expected after being added to an existing deployment.

The administrator finds that VRRP HA mode is selected, but primary and secondary roles are greyed out in the GUI The managed devices never show online when FMG-B becomes primary, but they will show online whenever the FMG-A

becomes primary.

What change will correct HA functionality in this scenario?

A. Change the FortiManager IP address on the managed FortiGate to 10.3.106.65.

B. Make the monitored IP to match on both FortiManager devices.

C. Unset the primary and secondary roles in the FortiManager CLI configuration so VRRP will decide who is primary.

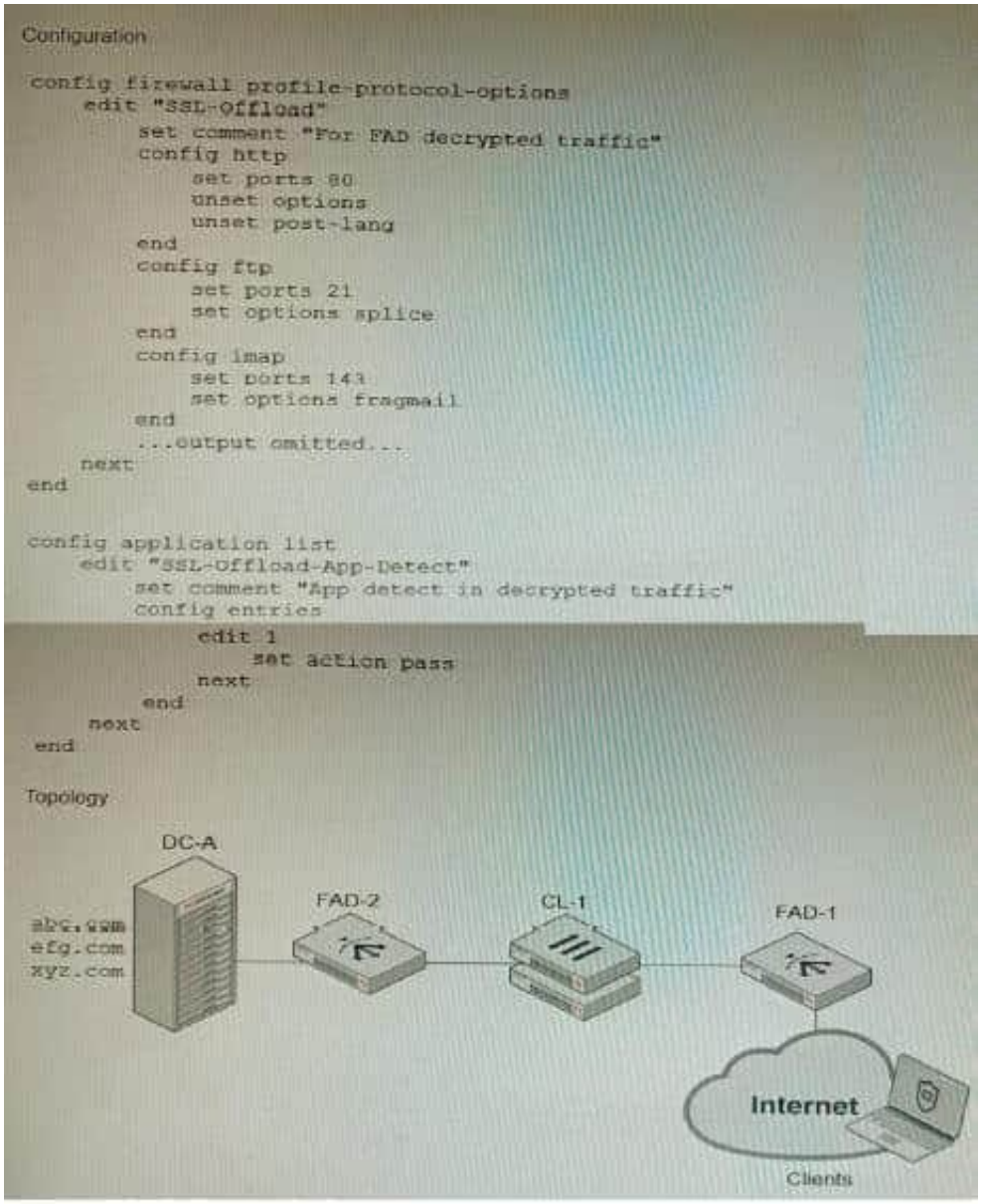
D. Change the priority of FMG-A to be numerically lower for higher preference

Correct Answer: B

Explanation: B is correct because the monitored IP must match on both FortiManager devices for HA to function properly. This is explained in the FortiManager Administration Guide under High Availability > Configuring HA options > Configuring HA options using the GUI. References:
https://docs.fortinet.com/document/fortimanager/7.4.0/administration-guide/568591/highavailabilityhttps://docs.fortinet.com/document/fortimanager/7.4.0/administration- guide/568591/high-availability/568592/configuring-ha-options

**QUESTION 4**

Refer to the exhibits.




A FortiGate cluster (CL-1) protects a data center hosting multiple web applications. A pair of FortiADC devices are already configured for SSL decryption (FAD-1), and re-encryption (FAD-2). CL-1 must accept unencrypted traffic from FAD-1,

perform application detection on the plain-text traffic, and forward the inspected traffic to FAD-2.

The SSL-Offload-App-Detect application list and SSL-Offload protocol options profile are applied to the firewall policy handling the web application traffic on CL-1.

Given this scenario, which two configuration tasks must the administrator perform on CL-1? (Choose two.)

A)

```
config firewall profile-protocol-options
    edit SSL-Offload
        config http
            set ssl-offloaded yes
        end
    next
end
```

B)

```
config firewall profile-protocol-options
    edit SSL-Offload
        config https
            set options splice
        end
    next
end
```

C)

```
config application list
    edit SSL-Offload-App-Detect
        set force-inclusion-ssl-di-sigs enable
    next
end
```

D)

```
config application list
    edit SSL-Offload-App-Detect
        set deep-app-inspection enable
    next
end
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: BC

Explanation: To enable application detection on plain-text traffic that has been decrypted by FortiADC, the administrator must perform two configuration tasks on CL-1:

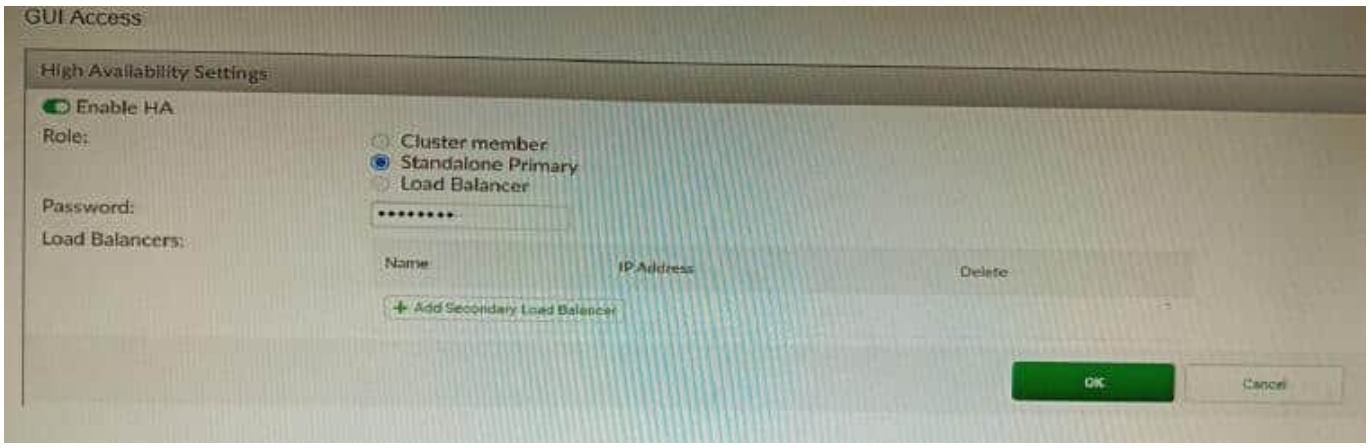
Enable SSL offloading in the firewall policy and select the SSL-Offload protocol options profile.

Enable application control in the firewall policy and select the SSL-Offload-App- Detect application list. References:

https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103438/application- detection-on-ssl-offloaded-traffic

**QUESTION 5**

Refer to the exhibit, which shows the high availability configuration for the FortiAuthenticator (FAC1).




Based on this information, which statement is true about the next FortiAuthenticator (FAC2) member that will join an HA cluster with this FortiAuthenticator (FAC1)?

A. FAC2 can only process requests when FAC1 fails.

B. FAC2 can have its HA interface on a different network than FAC1.

C. The FortiToken license will need to be installed on the FAC2.

D. FSSO sessions from FAC1 will be synchronized to FAC2.

Correct Answer: D

Explanation: When FortiAuthenticator operates in cluster mode, it provides active-passive failover and synchronization of all configuration and data, including FSSO sessions, between the cluster members. Therefore, if FAC1 is the active unit and FAC2 is the standby unit, any FSSO sessions from FAC1 will be synchronized to FAC2. If FAC1 fails, FAC2 will take over the active role and continue to process the FSSO sessions. References:https://docs.fortinet.com/document/ fortiauthenticator/6.1.2/administration- guide/122076/high-availability