NSE8_812$^{Q\&As}$

Network Security Expert 8 Written Exam

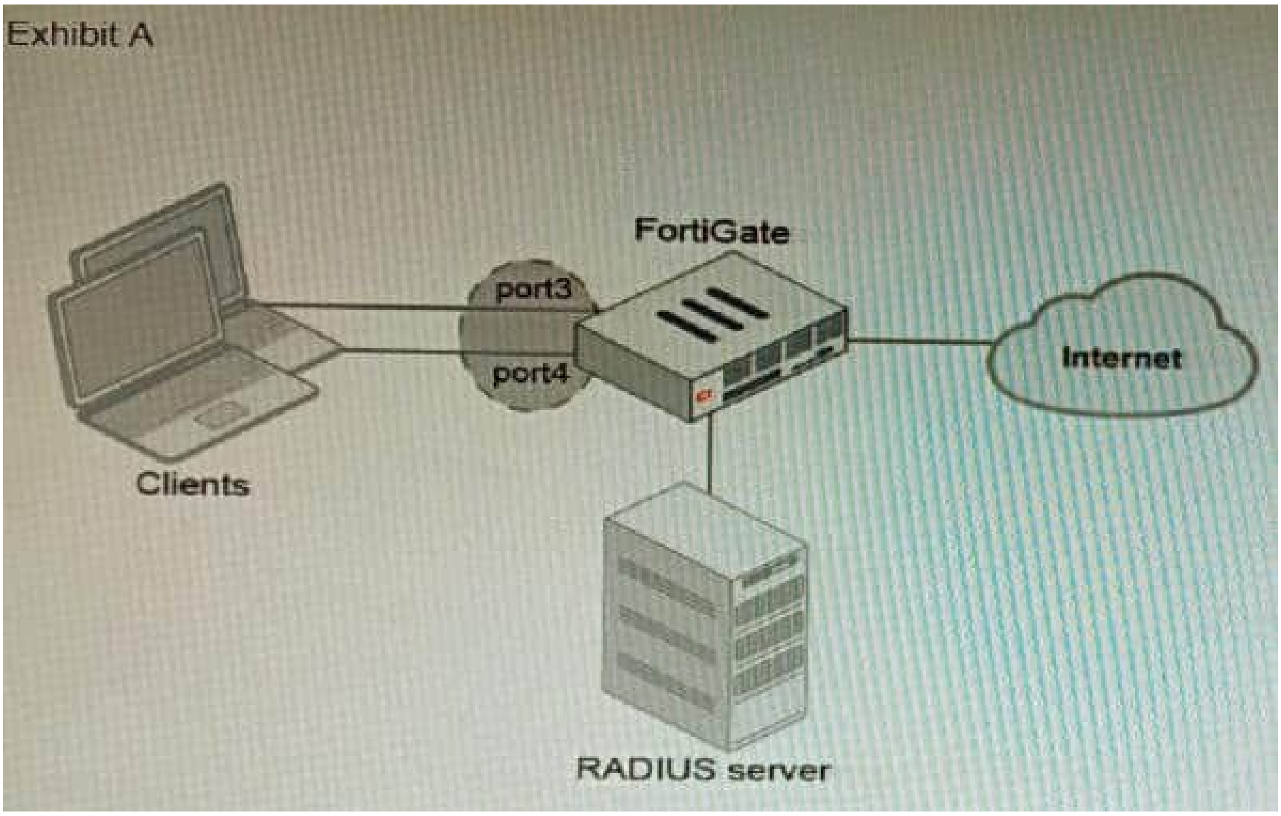
Pass Fortinet NSE8_812 Exam with 100% Guarantee

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

QUESTION 1

Refer to the exhibits.

Exhibit A



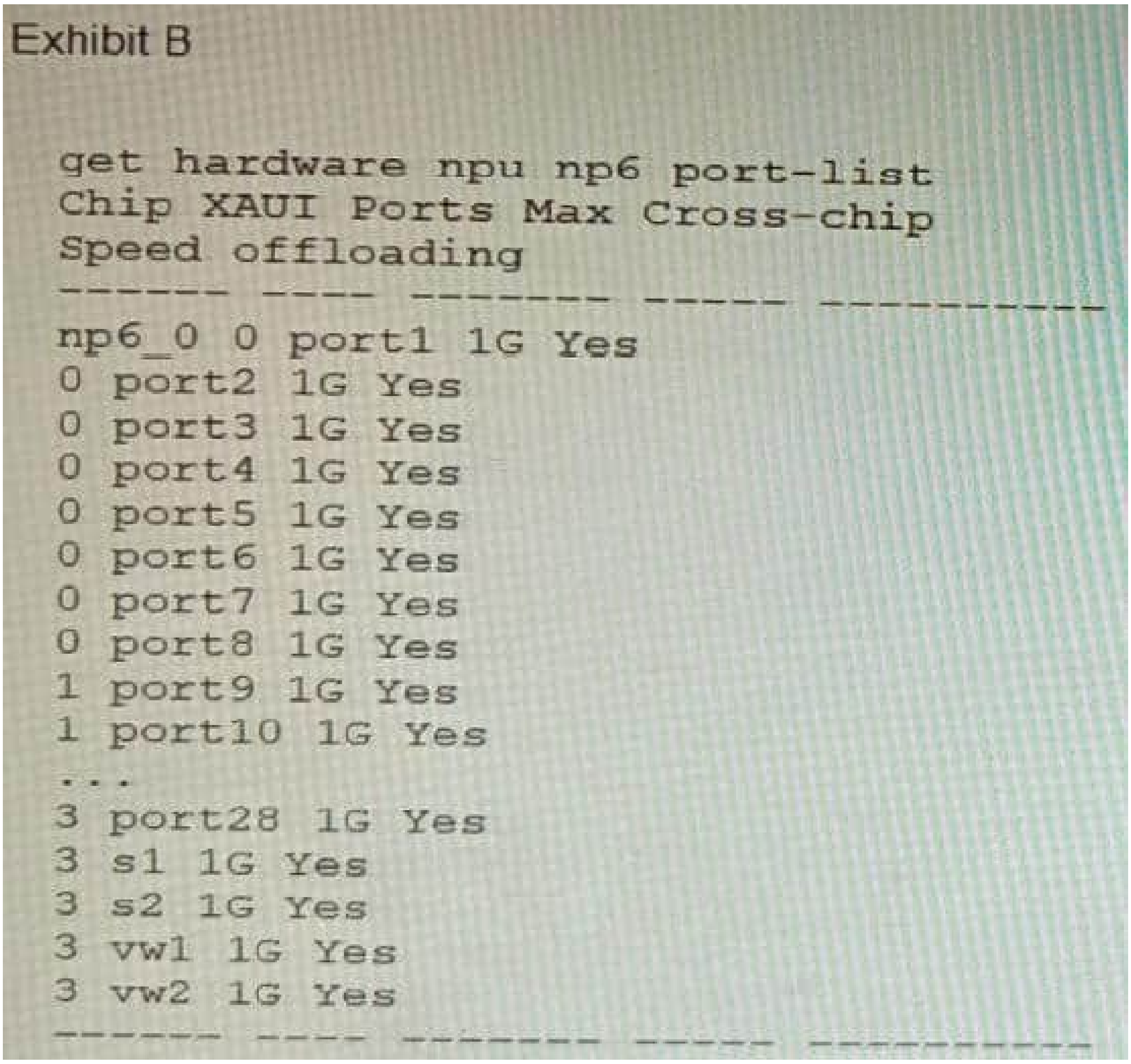


Exhibit B

```
get hardware npu np6 port-list
Chip XAUI Ports Max Cross-chip
Speed offloading
------ ---- ------- ----- ----------
np6_0 0 port1 1G Yes
0 port2 1G Yes
0 port3 1G Yes
0 port4 1G Yes
0 port5 1G Yes
0 port6 1G Yes
0 port7 1G Yes
0 port8 1G Yes
1 port9 1G Yes
1 port10 1G Yes
...
3 port28 1G Yes
3 s1 1G Yes
3 s2 1G Yes
3 vw1 1G Yes
3 vw2 1G Yes
------ ---- ------- ----- ----------
```

A customer is looking for a solution to authenticate the clients connected to a hardware switch interface of a FortiGate 400E.

Referring to the exhibits, which two conditions allow authentication to the client devices before assigning an IP address? (Choose two.)

A. FortiGate devices with NP6 and hardware switch interfaces cannot support 802.1X authentication.

B. Devices connected directly to ports 3 and 4 can perform 802 1X authentication.

C. Ports 3 and 4 can be part of different switch interfaces.

D. Client devices must have 802 1X authentication enabled

Correct Answer: BD

Explanation: The customer wants to deploy a solution to authenticate the clients connected to a hardware switch interface of a FortiGate 400E device. A hardware switch interface is an interface that combines multiple physical interfaces into one logical interface, allowing them to act as a singleswitch with one IP address and one set of security policies. The customer wants to use 802.1X authentication for this solution, which is a standard protocol for port-based network access control (PNAC) that authenticates clients based on their credentials before granting them access to network resources. One condition that allows authentication to the client devices before assigning an IP address is that devices connected directly to ports 3 and 4 can perform 802.1X authentication. This is because ports 3 and 4 are part of the hardware switch interface named "lan", which has an IP address of 10.10.10.254/24 and an inbound SSL inspection profile named "sslinspection". The inbound SSL inspection profile enables the FortiGate device to intercept and inspect SSL/TLS traffic from clients before forwarding it to servers, which allows it to apply security policies and features such as antivirus, web filtering, application control, etc. However, before performing SSL inspection, the FortiGate device needs to authenticate the clients using 802.1X authentication, which requires the clients to send their credentials (such as username and password) to the FortiGate device over a secure EAP (Extensible Authentication Protocol) channel. The FortiGate device then verifies the credentials with an authentication server (such as RADIUS or LDAP) and grants or denies access to the clients based on the authentication result. Therefore, devices connected directly to ports 3 and 4 can perform 802.1X authentication before assigning an IP address. Another condition that allows authentication to the client devices before assigning an IP address is that client devices must have 802.1X authentication enabled. This is because 802.1X authentication is a mutual process that requires both the client devices and the FortiGate device to support and enable it. The client devices must have 802.1X authentication enabled in their network settings, which allows them to initiate the authentication process when they connect to the hardware switch interface of the FortiGate device. The client devices must also have an 802.1X supplicant software installed, which is a program that runs on the client devices and handles the communication with the FortiGate device using EAP messages. The client devices must also have a trusted certificate installed, which is used to verify the identity of the FortiGate device and establish a secure EAP channel. Therefore, client devices must have 802.1X authentication enabled before assigning an IP address. References: https:// docs.fortinet.com/document/fortigate/7.0.0/administration- guide/19662/hardware-switchinterfaceshttps://docs.fortinet.com/document/fortigate/7.0.0/administration- guide/19662/802-1x-authentication

QUESTION 2

What is the benefit of using FortiGate NAC LAN Segments?

A. It provides support for multiple DHCP servers within the same VLAN.

B. It provides physical isolation without changing the IP address of hosts.

C. It provides support for IGMP snooping between hosts within the same VLAN

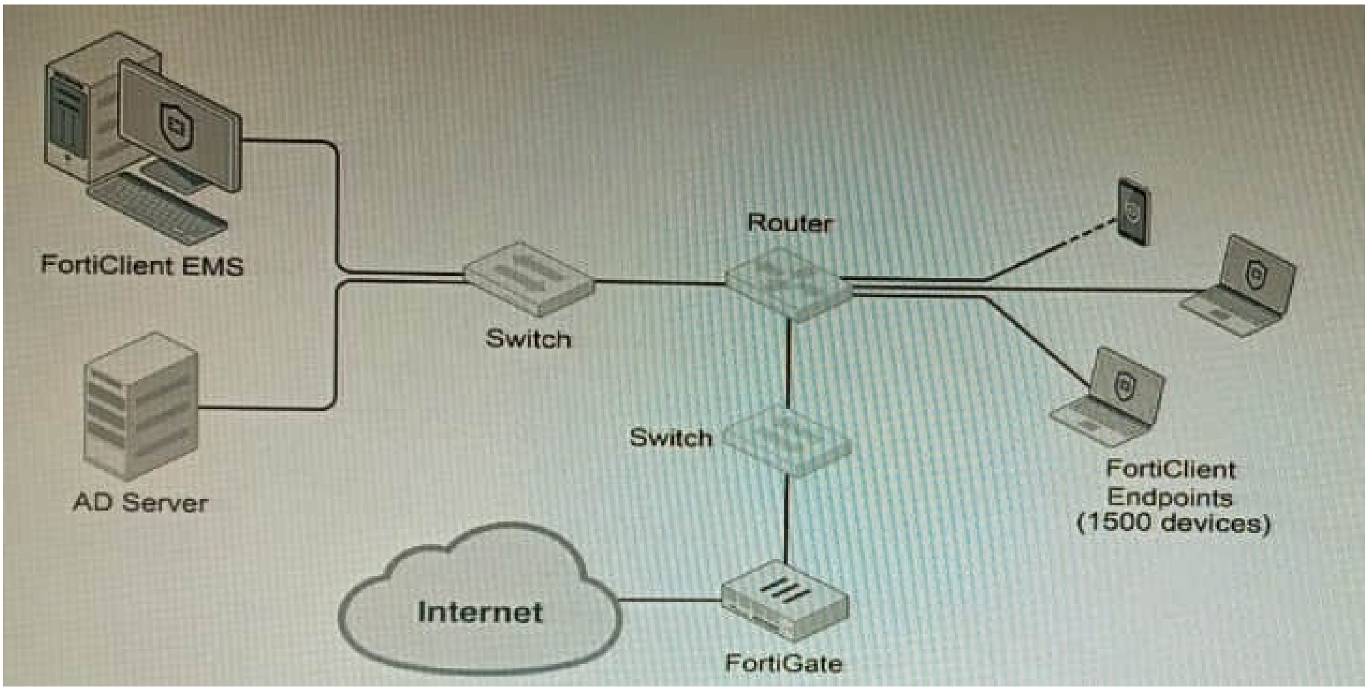
D. It allows for assignment of dynamic address objects matching NAC policy.

Correct Answer: D

Explanation: FortiGate NAC LAN Segments are a feature that allows users to assign different VLANs to different LAN segments without changing the IP address of hosts or bouncing the switch port. This provides physical isolation while maintaining firewall sessions and avoiding DHCP issues. One benefit of using FortiGate NAC LAN Segments is that it allows for assignment of dynamic address objects matching NAC policy. This means that users can create firewall policies based on dynamic address objects that match the NAC policy criteria, such as device type, OS type, MAC address, etc. This simplifies firewall policy management and enhances security byapplying different security profiles to different types of devices. References: https://docs.fortinet.com/document/fortigate/7.0.0/new-features/856212/nac-lan-segments- 7-0-1

QUESTION 3

Refer to the exhibit.



A customer wants FortiClient EMS configured to deploy to 1500 endpoints. The deployment will be integrated with FortiOS and there is an Active Directory server.

Given the configuration shown in the exhibit, which two statements about the installation are correct? (Choose two.)

A. If no client update time is specified on EMS, the user will be able to choose the time of installation if they wish to delay.

B. A client can be eligible for multiple enabled configurations on the EMS server, and one will be chosen based on first priority

C. You can only deploy initial installations to Windows clients.

D. You must use Standard or Enterprise SQL Server rather than the included SQL Server Express

E. The Windows clients only require "File and Printer Sharing0 allowed and the rest is handled by Active Directory group policy

Correct Answer: AE

A is correct because if no client update time is specified on EMS, the user will be able to choose the time of installation if they wish to delay. This is because the FortiClient EMS server will not force the installation on the client. E is correct

because the Windows clients only require "File and Printer Sharing" allowed and the rest is handled by Active Directory group policy. This is because the Active Directory group policy will configure the Windows clients to automatically install

FortiClient and the FortiClient EMS server will only need to push the initial configuration to the clients.

The other options are incorrect. Option B is incorrect because a client can only be eligible for one enabled configuration on the EMS server. Option C is incorrect because you can deploy initial installations to both Windows and macOS clients.

Option D is incorrect because you can use the included SQL Server Express to deploy FortiClient EMS.

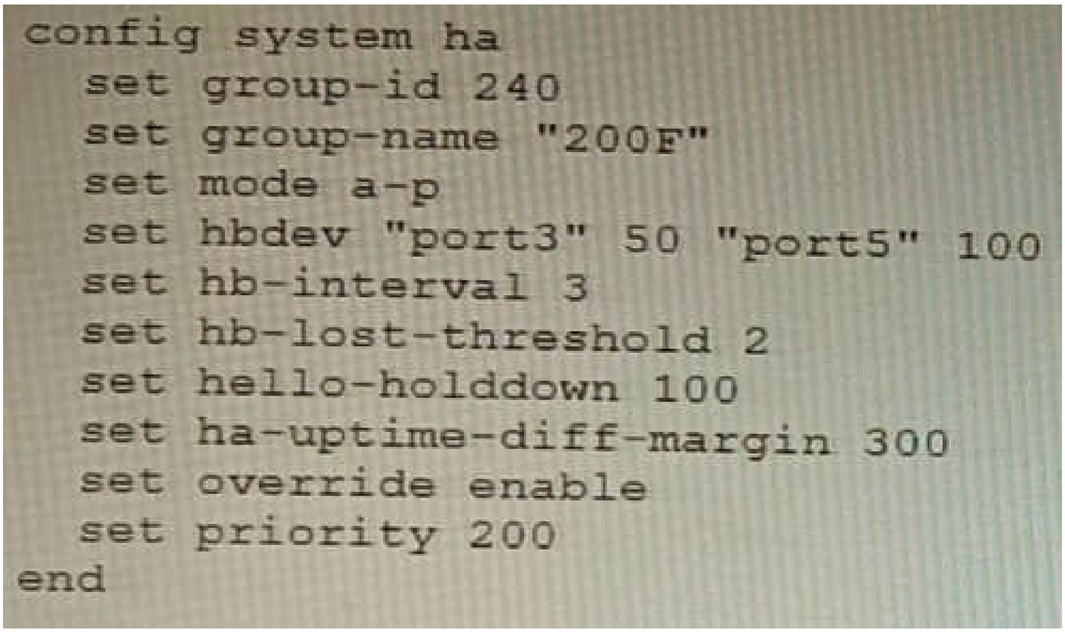
References:

Deploying FortiClient EMS | FortiClient / FortiOS 7.4.0 - Fortinet Document Library Configuring FortiClient EMS | FortiClient / FortiOS 7.4.0 - Fortinet Document Library

FortiClient EMS installation requirements | FortiClient / FortiOS 7.4.0 - Fortinet Document Library

QUESTION 4

An HA topology is using the following configuration:



```
config system ha
    set group-id 240
    set group-name "200F"
    set mode a-p
    set hbdev "port3" 50 "port5" 100
    set hb-interval 3
    set hb-lost-threshold 2
    set hello-holddown 100
    set ha-uptime-diff-margin 300
    set override enable
    set priority 200
end
```

Based on this configuration, how long will it take for a failover to be detected by the secondary cluster member?

A. 600ms

B. 200ms

C. 300ms

D. 100ms

Correct Answer: B

Explanation: The HA heartbeat interval is 100ms, and the number of lost heartbeats before a failover is detected is 2. So, it will take 2 * 100ms = 200ms for a failover to be detected by the secondary cluster member.

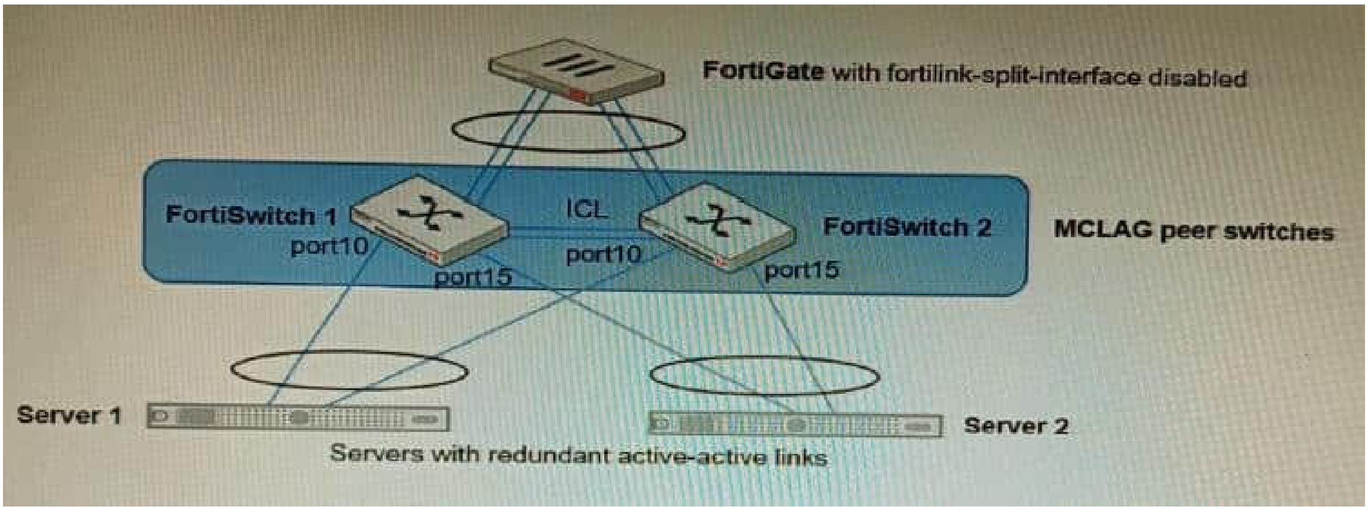
Reference:

FortiGate High Availability:

https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/647723/link- monitoring-and-ha-failover-time

QUESTION 5

Refer to the exhibit.


FortiGate with fortilink-split-interface disabled
FortiSwitch 1
port10
port15
ICL
port10
FortiSwitch 2
port15
MCLAG peer switches
Server 1
Server 2
Servers with redundant active-active links

You have been tasked with replacing the managed switch Forti Switch 2 shown in the topology. Which two actions are correct regarding the replacement process? (Choose two.)

A. After replacing the FortiSwitch unit, the automatically created trunk name does not change

B. CLAG-ICL needs to be manually reconfigured once the new switch is connected to the FortiGate

C. After replacing the FortiSwitch unit, the automatically created trunk name changes.

D. MCLAG-ICL will be automatically reconfigured once the new switch is connected to the FortiGate.

Correct Answer: AB

A is correct because the automatically created trunk name is based on the MAC address of the FortiSwitch unit. When the FortiSwitch unit is replaced, the MAC address will change, but the trunk name will not change. B is correct because CLAG-ICL is a manually configured link aggregation group. When the FortiSwitch unit is replaced, the CLAG-ICL configuration will need to be manually reconfigured on the new FortiSwitch unit. The other options are incorrect. Option C is incorrect because the automatically created trunk name does not change when the FortiSwitch unit is replaced. Option D is incorrect because MCLAG-ICL is a manually configured link aggregation group and will not be automatically reconfigured when the FortiSwitch unit is replaced. References: Configuring link aggregation on FortiSwitches | FortiSwitch / FortiOS 7.0.4 - Fortinet Document Library Managing FortiLink | FortiGate / FortiOS 7.0.4 - Fortinet Document Library