NSE8_811 Q&As

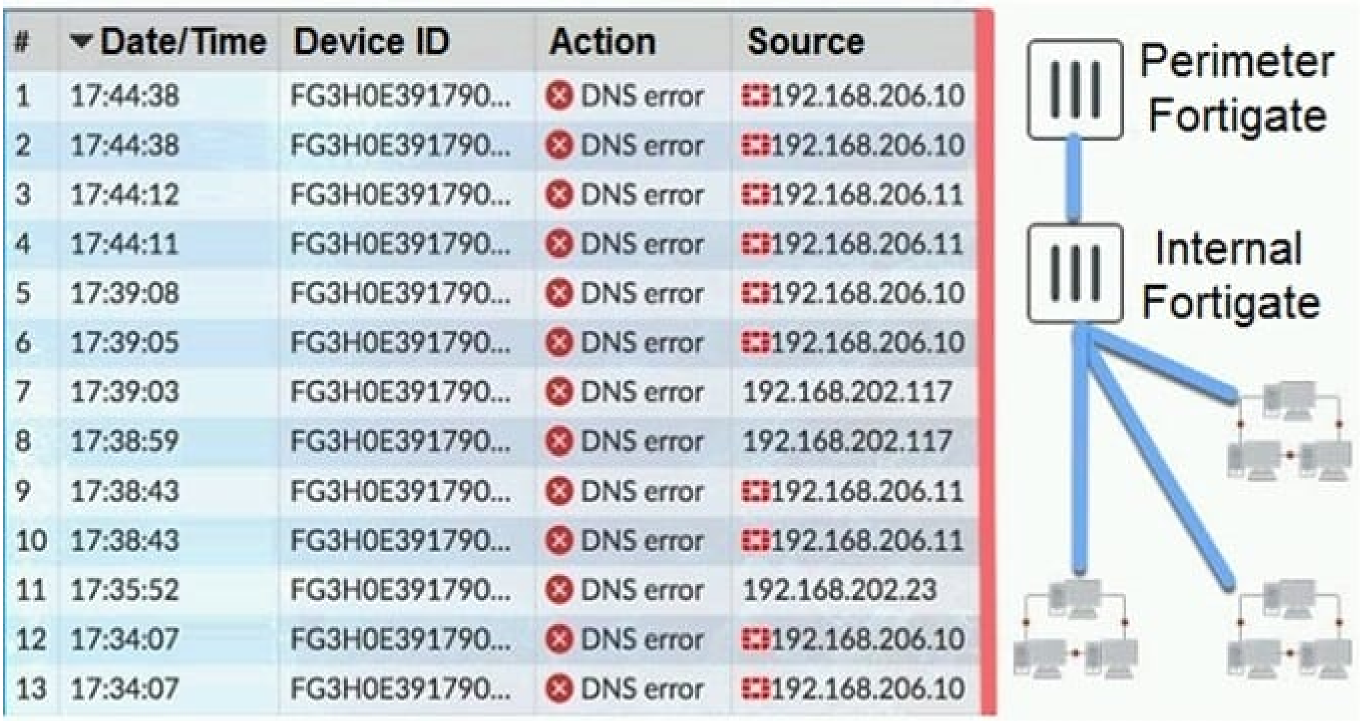
Fortinet NSE 8 Written Exam (NSE8_811)

Pass Fortinet NSE8_811 Exam with 100% Guarantee

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

QUESTION 1

Refer to the exhibit.



#	Date/Time	Device ID	Action	Source
1	17:44:38	FG3H0E391790...	⊗ DNS error	192.168.206.10
2	17:44:38	FG3H0E391790...	⊗ DNS error	192.168.206.10
3	17:44:12	FG3H0E391790...	⊗ DNS error	192.168.206.11
4	17:44:11	FG3H0E391790...	⊗ DNS error	192.168.206.11
5	17:39:08	FG3H0E391790...	⊗ DNS error	192.168.206.10
6	17:39:05	FG3H0E391790...	⊗ DNS error	192.168.206.10
7	17:39:03	FG3H0E391790...	⊗ DNS error	192.168.202.117
8	17:38:59	FG3H0E391790...	⊗ DNS error	192.168.202.117
9	17:38:43	FG3H0E391790...	⊗ DNS error	192.168.206.11
10	17:38:43	FG3H0E391790...	⊗ DNS error	192.168.206.11
11	17:35:52	FG3H0E391790...	⊗ DNS error	192.168.202.23
12	17:34:07	FG3H0E391790...	⊗ DNS error	192.168.206.10
13	17:34:07	FG3H0E391790...	⊗ DNS error	192.168.206.10

You have deployed several perimeter FortiGate devices with internal segmentation FortiGate devices behind them. All FortiGate devices are logging to FortiAnalyzer. When you search the logs in FortiAnalyzer for denied traffic, you see numerous log messages, as shown in the exhibit, on your perimeter FortiGate device only.

Which two actions will reduce the number of these log messages? (Choose two.)

A. Disable DNS events logging from FortiGate in the config log fortianalyzer filter section.

B. Apply an application control profile to the perimeter FortiGate devices that does not inspect DNS traffic to the outbound firewall policy.

C. Remove DNS signatures from the IPS profile applied to the outbound firewall policy.

D. Configure the internal FortiGate devices to communicate to FortiGuard using port 8888.

Correct Answer: AD

QUESTION 2

A customer is looking for a way to remove javascripts, macros and hyperlinks from documents traversing the network without affecting the integrity of the content. You propose to use the Content disarm and reconstruction (CDR) feature of the FortiGate.

Which two considerations are valid to implement CDR in this scenario? (Choose two.)

A. The inspection mode of the FortiGate is not relevant for CDR to operate.

B. CDR is supported on HTTPS, SMTPS, and IMAPS if deep inspection is enabled.

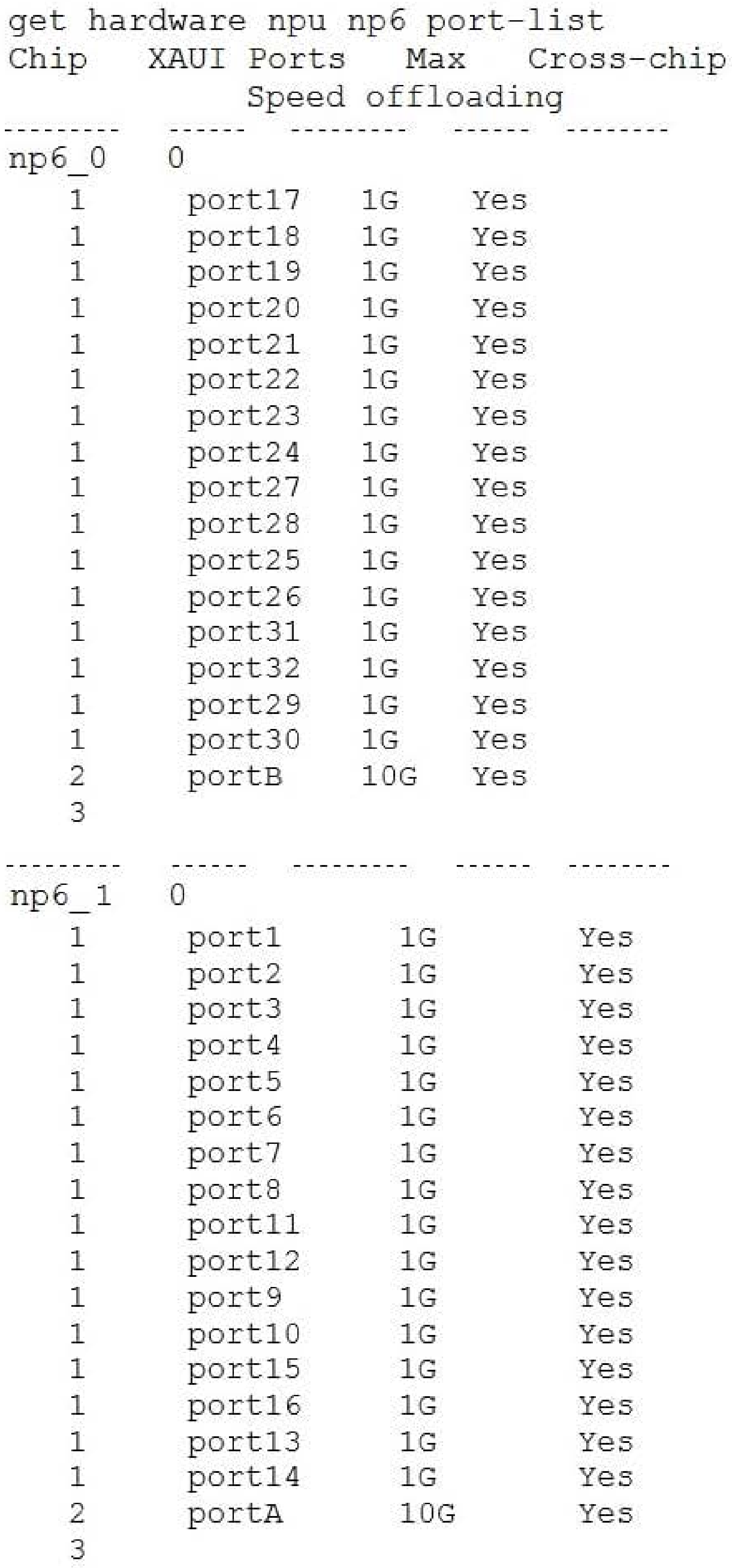
C. CDR can only be performed on Microsoft Office Document and PDF files.

D. Files processed by CDR can have the original copy quarantined on the FortiGate.

Correct Answer: CD

QUESTION 3

Refer to the exhibit.



```
get hardware npu np6 port-list
Chip    XAUI Ports    Max    Cross-chip
                Speed offloading
--------  -----  --------  -----  -------
np6_0    0
    1      port17   1G    Yes
    1      port18   1G    Yes
    1      port19   1G    Yes
    1      port20   1G    Yes
    1      port21   1G    Yes
    1      port22   1G    Yes
    1      port23   1G    Yes
    1      port24   1G    Yes
    1      port27   1G    Yes
    1      port28   1G    Yes
    1      port25   1G    Yes
    1      port26   1G    Yes
    1      port31   1G    Yes
    1      port32   1G    Yes
    1      port29   1G    Yes
    1      port30   1G    Yes
    2      portB    10G   Yes
    3

--------  -----  --------  -----  -------
np6_1    0
    1      port1      1G        Yes
    1      port2      1G        Yes
    1      port3      1G        Yes
    1      port4      1G        Yes
    1      port5      1G        Yes
    1      port6      1G        Yes
    1      port7      1G        Yes
    1      port8      1G        Yes
    1      port11     1G        Yes
    1      port12     1G        Yes
    1      port9      1G        Yes
    1      port10     1G        Yes
    1      port15     1G        Yes
    1      port16     1G        Yes
    1      port13     1G        Yes
    1      port14     1G        Yes
    2      portA      10G       Yes
    3
```

You are trying to configure Link-Aggregation Group (LAG), but ports A and B do not appear on the list of member options.

Referring to the exhibit, which statement is correct in this situation?

A. The FortiGate interfaces are defective and require replacement.

B. The FortiGate model does not have an Integrated Switch Fabric (ISF).

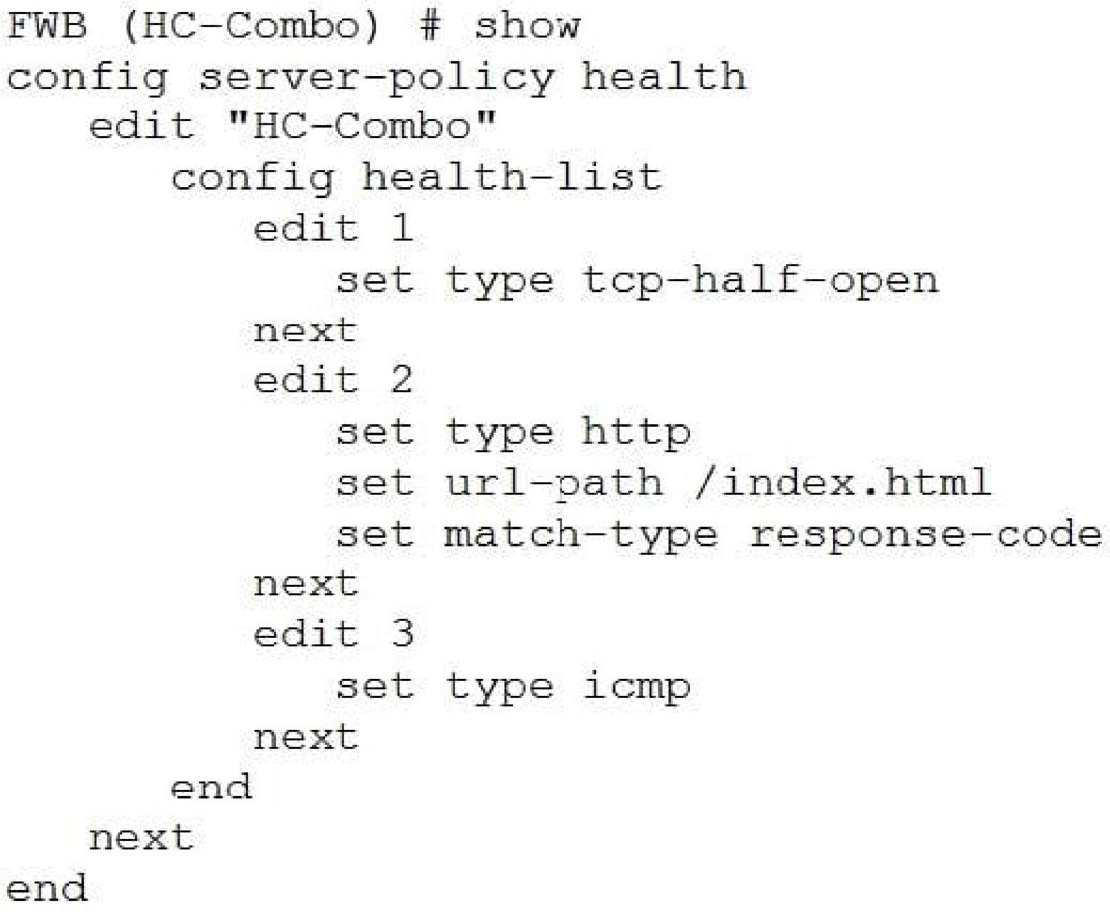
C. The FortiGate model being used does not support LAG.

D. The FortiGate SFP+ slot does not have the correct module.

Correct Answer: B

QUESTION 4

Refer to the exhibit.



```
FWB (HC-Combo) # show
config server-policy health
    edit "HC-Combo"
        config health-list
            edit 1
                set type tcp-half-open
            next
            edit 2
                set type http
                set url-path /index.html
                set match-type response-code
            next
            edit 3
                set type icmp
            next
        end
    next
end
```

You created a custom health-check for your FortiWeb deployment. Given the output shown in the exhibit, which statement is true?

A. The FortiWeb must receive an RST packet from the server.

B. The FortiWeb must receive an HTTP 200 response code from the server.

C. The FortiWeb must match the hash value of the page index.html.

D. The FortiWeb must receive an ICMP Echo Request from the server.

Correct Answer: B

QUESTION 5

A FortiGate is used as a VPN hub for a number of remote spoke VPN units (Group A) spokes using a phase 1 main mode dial-up tunnel and pre-shared keys. You are asked to establish VPN connectivity for a newly acquired organization\\'s sites for which new devices will be provisioned Group B spokes.

Both existing Group A and new Group B spoke units are dynamically addressed through a single public IP Address on the hub. You are asked to ensure that spokes from Group B have different access permissions than the existing VPN spokes units Group A.

Which two solutions meet the requirements for the new spoke group? (Choose two.)

A. Implement a new phase 1 dial-up main mode tunnel with a different pre-shared key than the Group A spokes.

B. Implement a new phase 1 dial-up main mode tunnel with certificate authentication.

C. Implement a new phase 1 dial-up main mode tunnel with pre-shared keys and XAuth.

D. Implement separate phase 1 dial-up aggressive mode tunnels with a distinct peer ID.

Correct Answer: CD