NSE8_811 Q&As

Fortinet NSE 8 Written Exam (NSE8_811)

Pass Fortinet NSE8_811 Exam with 100% Guarantee

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

https://www.leads4pass.com/nse8_811.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A customer is experiencing problems with a legacy L3/L4 firewall device and the IPv6 SIP VoIP traffic. Their device is dropping SIP packets, consequently, it cannot process SIP voice calls.

Which solution will solve the customer\\'s problem?

A. Replace their legacy device with a FortiGate and deploy a FortiVoice to extract information from the body of the IPv6 SIP packet.

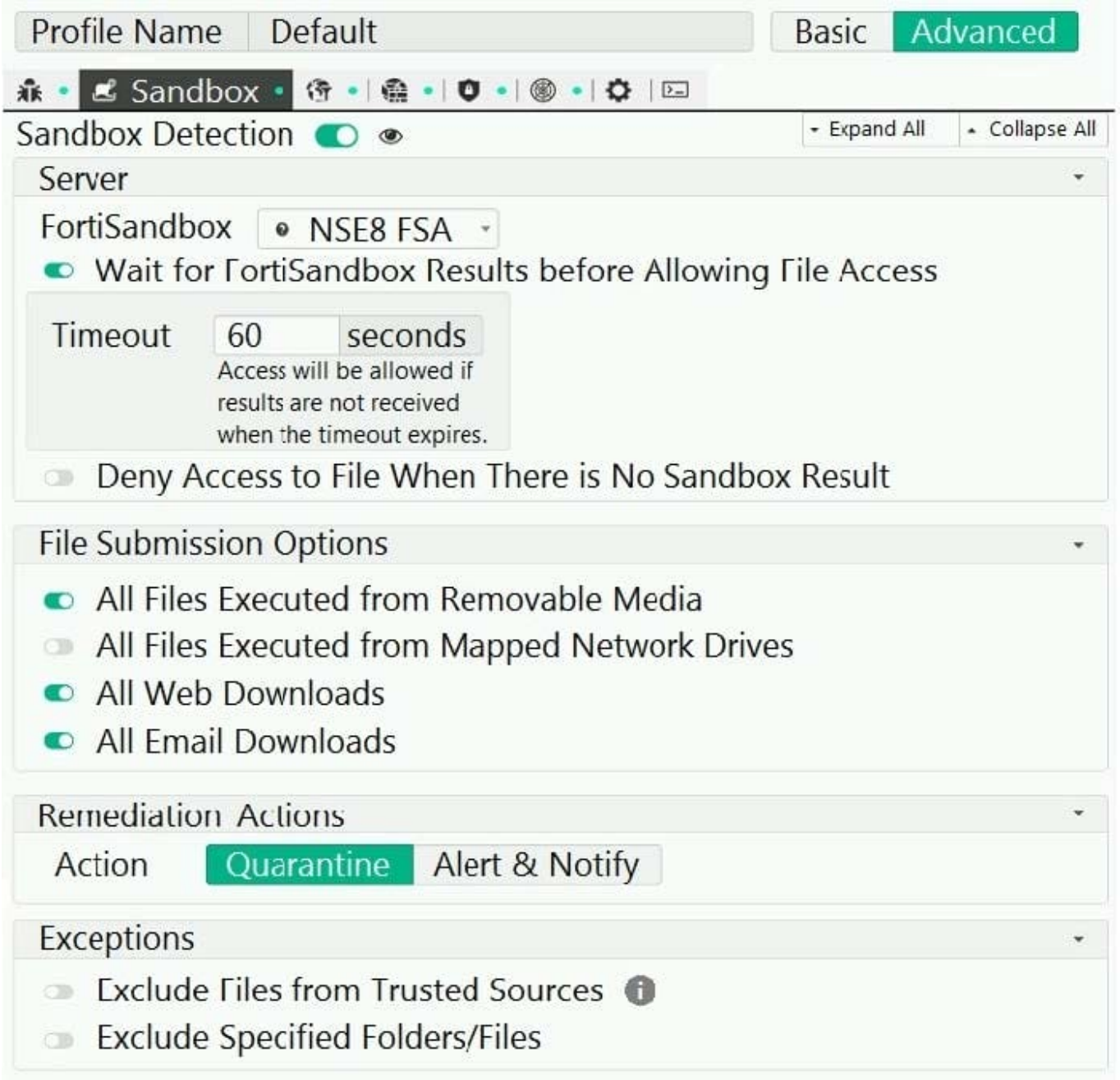
B. Deploy a FortiVoice and enable IPv6 SIP.

C. Deploy a FortiVoice and enable an IPv6 SIP session helper.

D. Replace their legacy device with a FortiGate and configure it to extract information from the body of the IPv6 SIP packet.

Correct Answer: A

QUESTION 2



Anti-Virus Real-Time Protection is enabled without any exclusions.

Referring to the exhibit, which two behaviors will the FortiClient endpoint have after receiving the profile update from the FortiClient EMS? (Choose two.)

A. Access to a downloaded file will always be allowed after 60 seconds when the FortiSandbox is reachable.

B. The user will not be able to access a downloaded file for a maximum of 60 seconds if it is not a virus and the FortiSandbox is reachable.

C. Files executed from a mapped network drive will not be inspected by the FortiClient endpoint AntiVirus engine.

D. If the Real-Time Protection does not detect a virus, the user will be able to access a downloaded file when the FortiSandbox is unreachable.

Correct Answer: AB

QUESTION 3

Consider the following VDOM configuration:

```
config global
    config system vdom-link
        edit vlink2
    end
config system interface
        edit vlink20
            set vdom nat
    next
        edit vlink21
            set vdom transparent
end
```

In which two ways can you establish communication between an existing NAT VDOM and a new transparent VDOM? (Choose two.)

A. Set the set ip 10.10.10.1 command to vlink2l.

B. Set the set ip 10.10.10.1 command to vlink20.

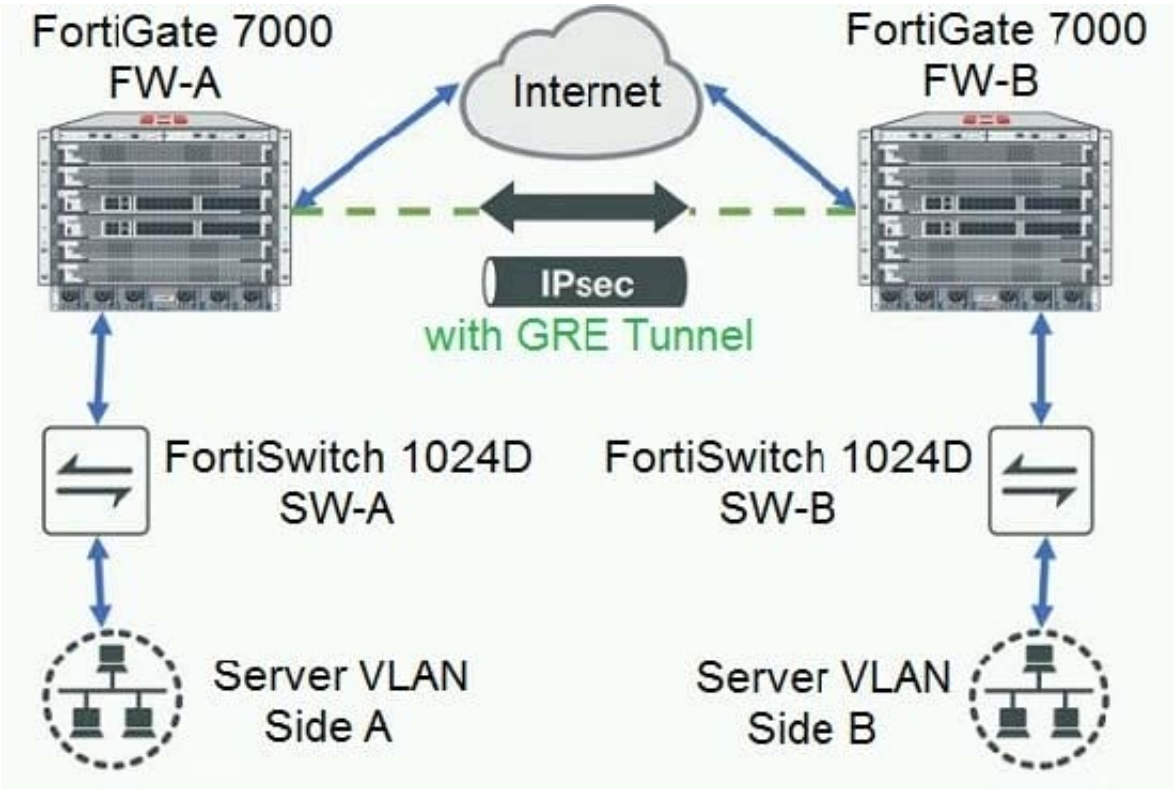
C. Set type ppp to the vdom-link, vlink2.

D. Set type ethernet to the vdom-link, vlink2.

Correct Answer: BD

QUESTION 4

Refer to the exhibit.



You have two data centers with a FortiGate 7000-series chassis connected by VPN. All traffic flows over an established generic routing encapsulation (GRE) tunnel between them. You are troubleshooting traffic that is traversing between Server VLAN A and Server VLAN B. The performance is lower than expected and you notice all traffic is only going through the FPM in slot 3 while nothing through the FPM in slot 4.

Referring to the exhibit, which statement is true?

A. Removing traffic shaping from the firewall policy allowing this traffic will allow for load-balancing to the other module.

B. Changing the algorithm to take source IP, destination IP and port into account will load balance this traffic to the other module.

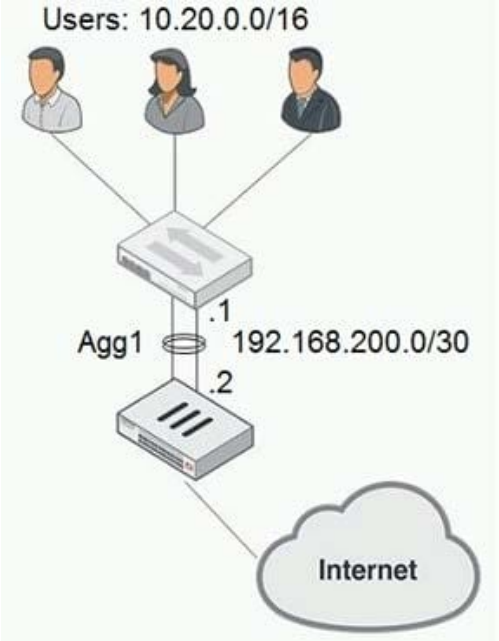
C. There is no way to load-balance the traffic in this scenario.

D. Configuring a load-balance flow-rule in the CLI will load-balance this traffic.

Correct Answer: D

QUESTION 5

Refer to the exhibit.




```
config system interface
    edit "Agg1"
        set ip 192.168.200.2 255.255.255.252
        set type aggregate
        set member port1 port2
        set vdom "root"
        set weight 1
        set lacp-mode passive
        set min-links 1
        set algorithm L2
    next
end
```

You created an aggregate interface between a FortiGate and a switch consisting of two 1 Gbps links as shown in the exhibit. However, the maximum bandwidth never exceeds 1 Gbps and employees are reporting that the network is slow. After troubleshooting, you notice that only one member interface is being used. The configuration for the aggregate interface is shown in the exhibit.

In this scenario, which command will solve this problem?

A.
```
config system interface
edit Agg1
   set algorithm L4
end
```

B.
```
config system interface
edit Agg1
   set weight 2
end
```

C.
```
config system interface
edit Agg1
   set lacp-mode active
end
```

D.
```
config system interface
edit Agg1
   set min-links 2
end
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 6

An organization has one central site and three remote sites. A FortiSIEM has been installed on the central site and now all devices across the remote sites must be centrally monitored by the FortiSIEM at the central site.

Which action will reduce the WAN usage by the monitoring system?

A. Enable SD-WAN FEC (Forward Error Correction) on the FortiGate at the remote site.

B. Install both Supervisor and Collector on each remote site.

C. Install local Collectors on each remote site.

D. Disable real-time log upload on the remote sites.

Correct Answer: C

QUESTION 7

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.

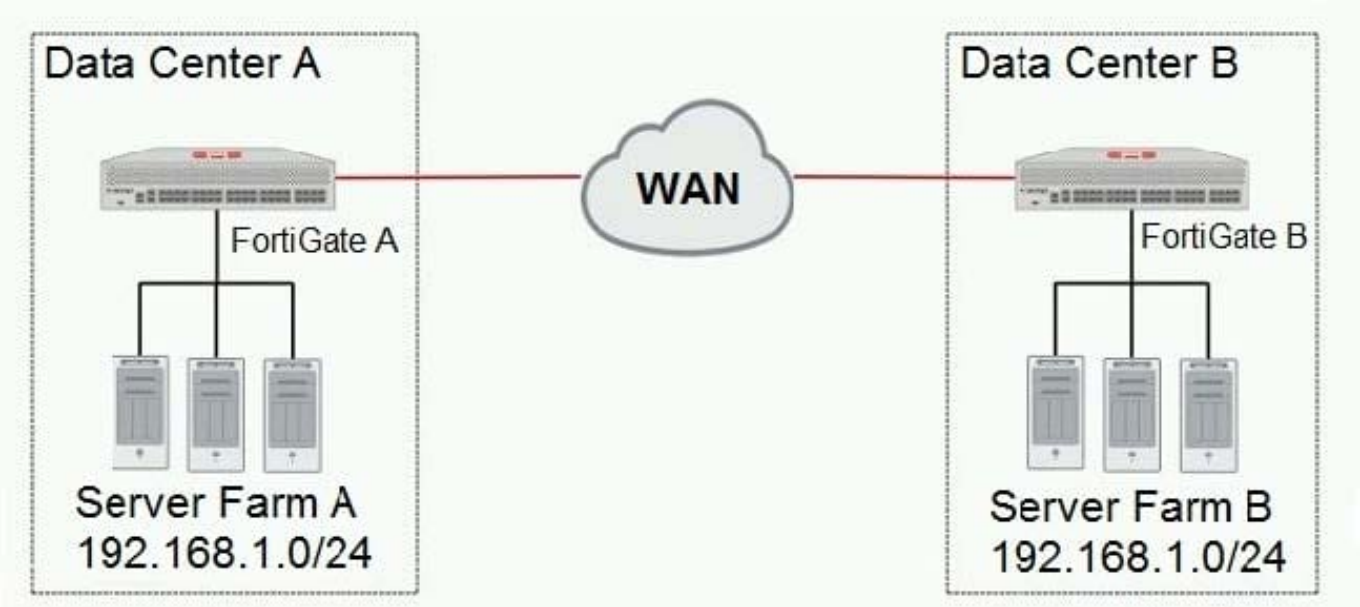
C. CDR can only be performed on Microsoft Office Document and PDF files.

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

Correct Answer: CD

QUESTION 8

Refer to the exhibit.



A company has two data centers (DC) connected using a Layer 3 network. Servers in farm A need to connect to servers in farm B as though they were all in the same Layer 2 segment.

Referring to the exhibit, what is configured on the FortiGate devices on each DC to allow this connectivity?

A. Create an IPsec tunnel with VXLAN encapsulation.

B. Create an IPsec tunnel with VLAN encapsulation.

C. Create an IPsec tunnel with transport-mode encapsulation.

D. Create an IPsec tunnel with tunnel-mode encapsulation.

Correct Answer: A

QUESTION 9

In a FortiGate 5000 series, two FortiControllers are working as an SLBC cluster in a-p mode. The configuration shown below is applied.

```
config load-balance session-setup
    set tcp-ingress enable
end
```

Which statement is true on how new TCP sessions are handled by the Distributor Processor (DP)?

A. The new session added in the DP session table is automatically deleted, if the traffic is denied by the processing worker.

B. No new session is added in the DP session table until the processing worker accepts the traffic.

C. A new session added in the DP session table remains in the table even if the traffic is denied by the processing worker.

D. A new session added in the DP session table remains in the table only if traffic is accepted by the processing worker.

Correct Answer: C

QUESTION 10

You are asked to implement a single FortiGate 5000 chassis using Session-aware Load Balance Cluster (SLBC) with Active-Passive FortiControllers. Both FortiControllers have the configuration shown below, with the rest of the configuration set to the default values.

```
config system ha
    set mode dual
    set password fortinetnse8
    set group-id 5
    set chassis-id 1
    set minimize-chassis-failover enable
    set hbdev "b1"
end
```

Both FortiControllers show Master status. What is the problem in this scenario?

A. The b1 interface of the two FortiControllers do not see each other.

B. The management interface of both FortiControllers was connected on the same network.

C. The chassis ID settings on FortiController on slot 2 should be set to 2.

D. The priority should be set higher for FortiController on slot-1.

Correct Answer: A