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.pass2lead.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

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.

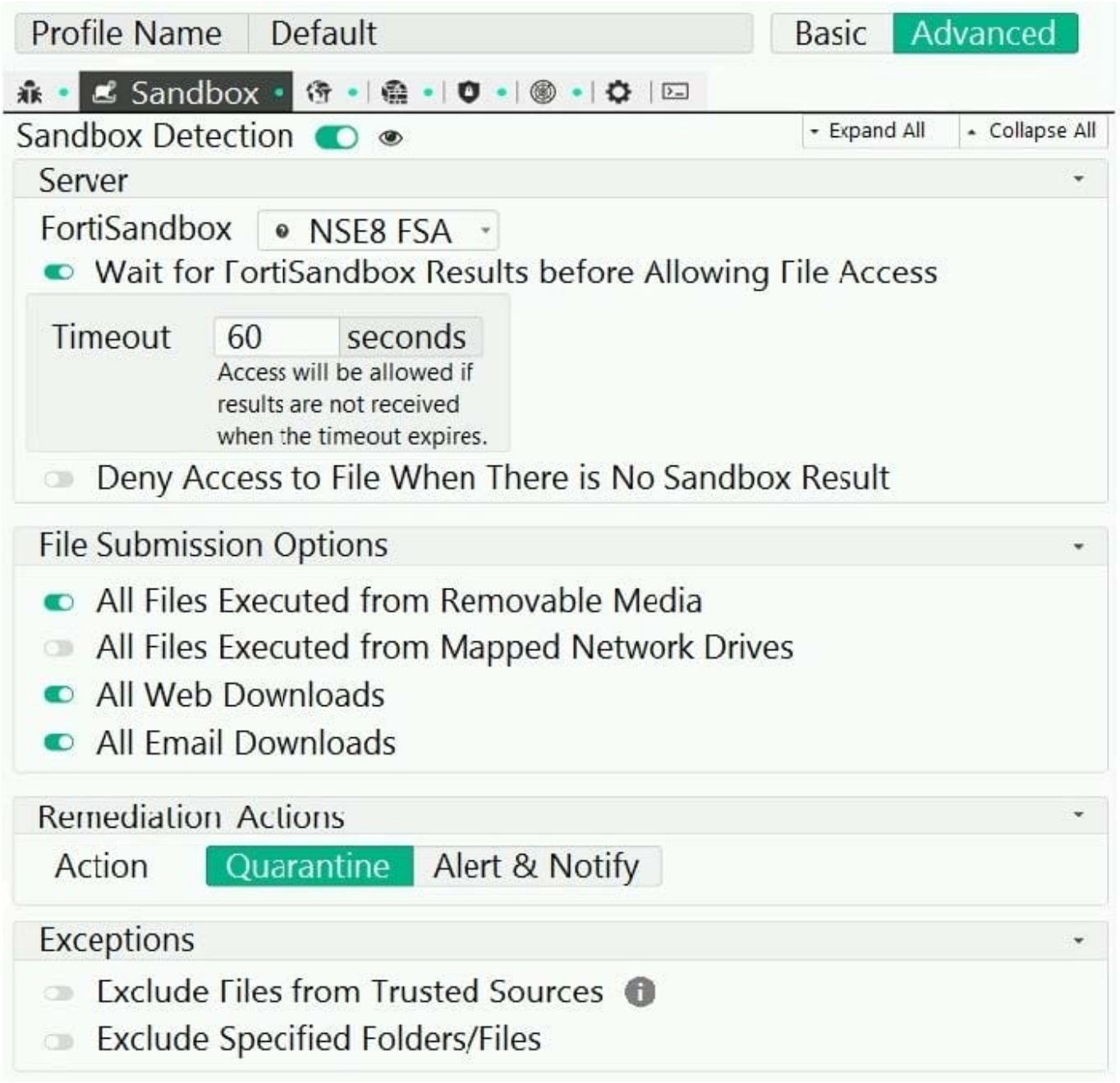
B. The FortiWeb must receive an HTTP 200 response code from the server.

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 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

You must create a High Availability deployment with two FortiWebs in Amazon Web Services (AWS); each on different Availability Zones (AZ) from the same region. At the same time, each FortiWeb should be able to deliver content from the Web servers of both of the AZs.

Which deployment would fulfill this requirement?

A. Configure the FortiWebs in Active-Active HA mode and use AWS Elastic Load Balancer (ELB) for the internal Web servers.

B. Use AWS Elastic Load Balancer (ELB) for both the FortiWebs in standalone mode and the internal Web servers in an ELB sandwich.

C. Configure the FortiWebs in Active-Active HA mode and use AWS Route 53 to load balance the internal Web servers.

D. Use AWS Route 53 to load balance the FortiWebs in standalone mode and use AWS Virtual Private Cloud (VPC) Peering to load balance the internal Web servers.

Correct Answer: B

QUESTION 4

A FortiGate with the default configuration shown below is deployed between two IP telephones. FortiGate receives the INVITE request shown in the exhibit from Phone A (internal) to Phone B (external).

NVITE sip:PhoneB@172.20.120.30 SIP/2.0 Via: SIP/2.0/UDP 10.31.101.20:5060 From: PhoneA To: PhoneB Call-ID: 314159@10.31.101.20 CSeq: 1 INVITE Contact: sip:PhoneA@10.31.101.20 v=0 o=PhoneA 5462346 332134 IN IP4 10.31.101.20 c=IN IP4 10.31.101.20 m=audio 49170 RTP 0 3

Which two statements are correct after the FortiGate receives the packet? (Choose two.)

A. NAT takes place only in the SIP application layer.

B. A pinhole will be opened to accept traffic sent to the FortiGate WAN IP address.

C. NAT takes place at both the network and SIP application layers.

D. A pinhole is not required to accept traffic sent to the FortiGate WAN IP address.

Correct Answer: BC

QUESTION 5

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 6

A legacy router has been replaced by a FortiGate device. The FortiGate has inherited the management IP address of the router and now the network administrator needs to remove the router from the FortiSIEM configuration.

Which two statements about this operation are true? (Choose two.)

A. FortiSIEM will move the router device into the Decommission folder.

B. The router will be completely deleted from the FortiSIEM database.

C. By default, FortiSIEM can only parser event logs for FortiGate devices.

D. FortiSIEM will discover a new device for the FortiGate with the same IP.

Correct Answer: AD

QUESTION 7

A company has just rolled out new remote sites and now you need to deploy a single firewall policy to all of these sites to allow Internet access using FortiManager. For this particular firewall policy, the source address object is called LAN,

but its value will change according to the site the policy is being installed.

Which statement about creating the object LAN is correct?

A. Create a new object called LAN and enable per-device mapping.

B. Create a new object called LAN and promote it to the global database.

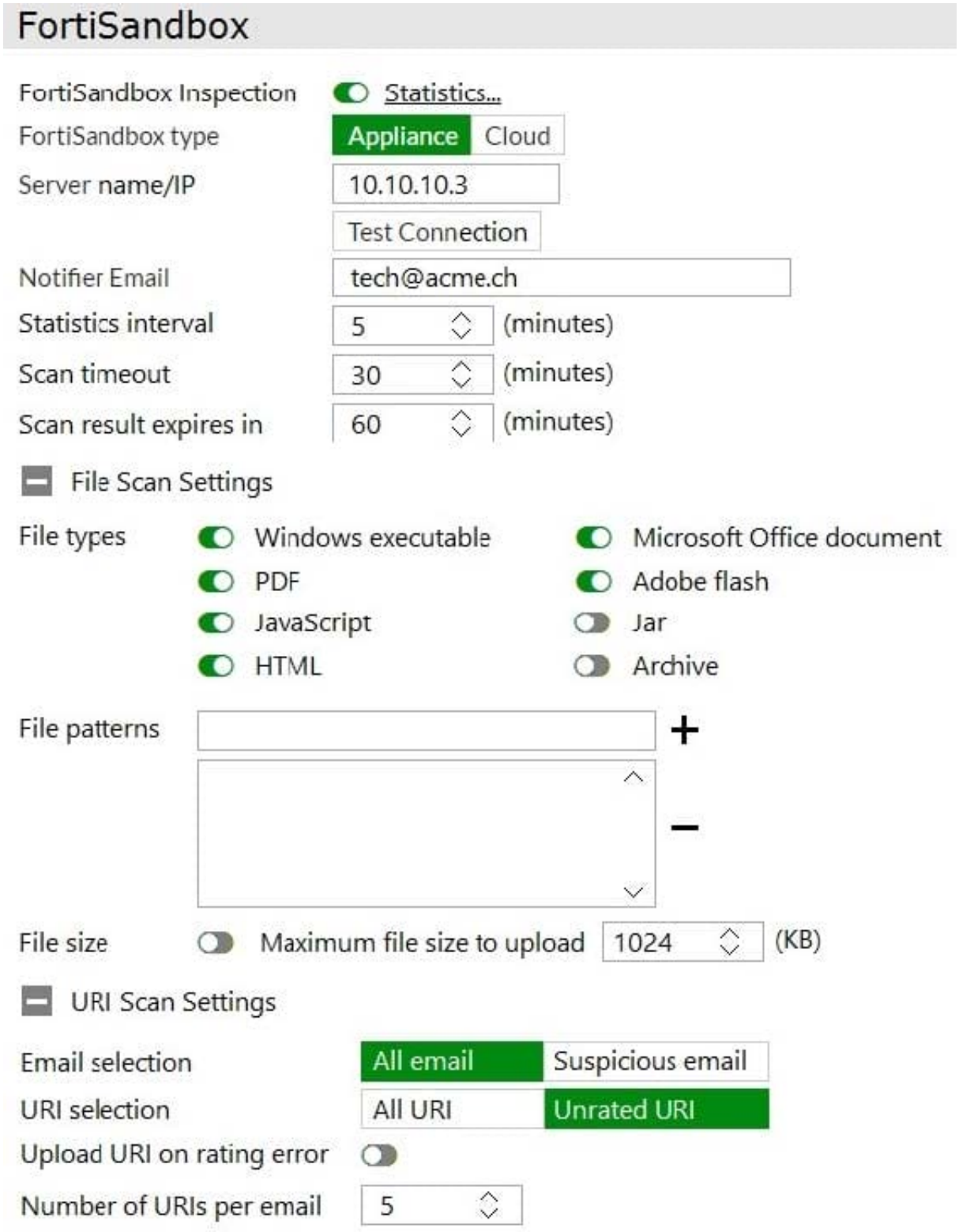
C. Create a new object called LAN and use it as a variable on a TCL script.

D. Create a new object called LAN and set meta-fields per remote site.

Correct Answer: A

QUESTION 8

Refer to the exhibit.



You have installed a FortiSandbox and configured it in your FortiMail. Referring to the exhibit, which two statements are correct? (Choose two.)

A. If FortiMail is not able to obtain the results from the FortiGuard queries, URIs will not be checked by the FortiSandbox.

B. FortiMail will cache the results for 30 minutes

C. If the FortiSandbox with IP 10.10.10.3 is not available, the e-mail will be checked by the FortiCloud Sandbox.

D. FortiMail will wait up to 30 minutes to obtain the scan results.

Correct Answer: AD

QUESTION 9

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

QUESTION 10

You want to manage a FortiGate with the FortiCloud service. The FortiGate shows up in your list of devices on the FortiCloud Web site, but all management functions are either missing or grayed out.

Which statement is correct in this scenario?

A. The management tunnel mode on the managed FortiGate must be changed to normal.

B. The managed FortiGate is running a version of FortiOS that is either too new or too old for FortiCloud.

C. The managed FortiGate requires that a FortiCloud management license be purchased and applied.

D. You must manually configure system central-management on the FortiGate CLI and set the management type to fortiguard.

Correct Answer: D