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.passapply.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

You want to access the JSON API on FortiManager to retrieve information on an object. In this scenario, which two methods will satisfy the requirement? (Choose two.)

A. Download the WSDL file from FortiManager administration GUI.

B. Make a call with the curl utility on your workstation.

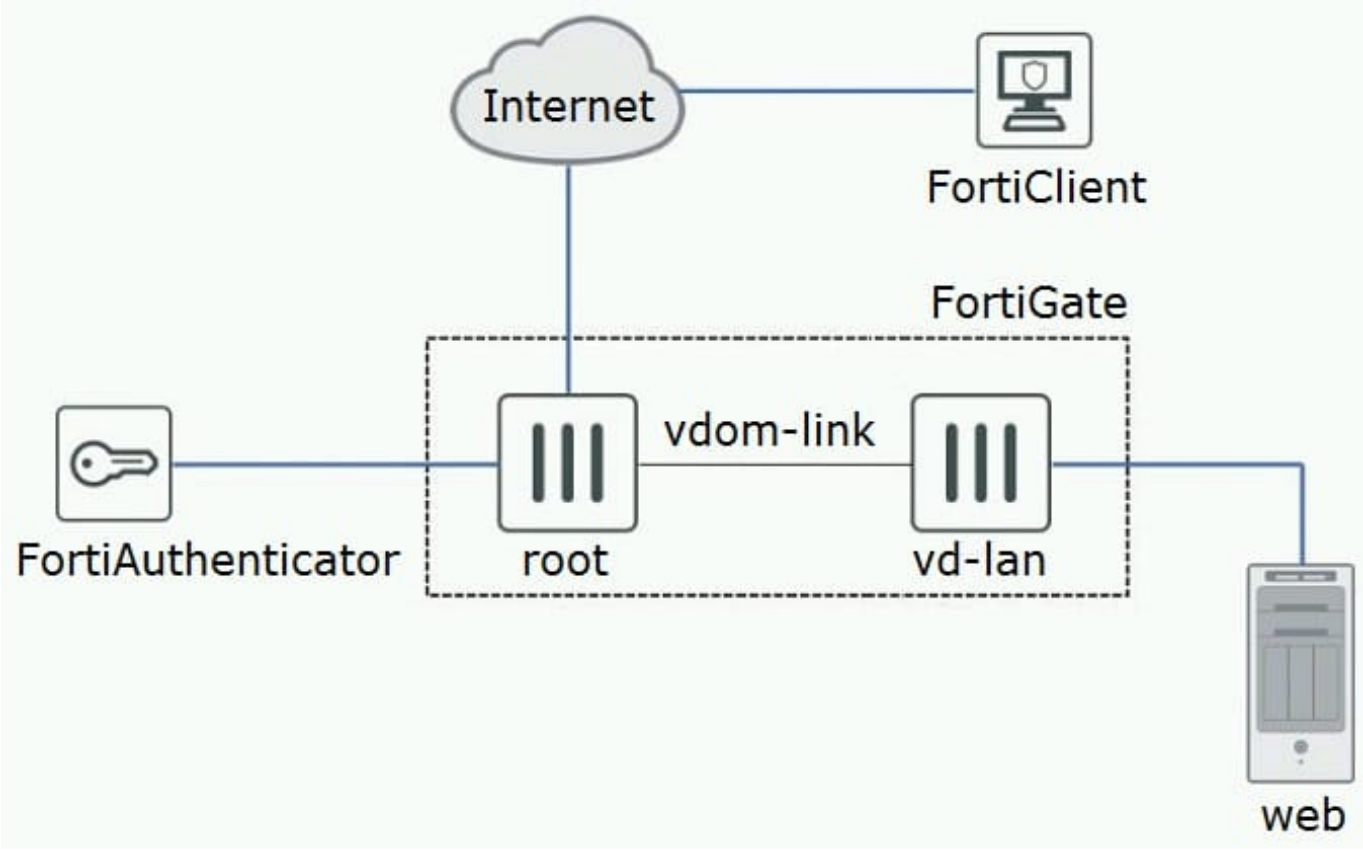
C. Make a call with the SoapUI API tool on your workstation.

D. Make a call with the Web browser on your workstation.

Correct Answer: AC

QUESTION 2

Refer to the exhibit.



The exhibit shows a topology where a FortiGate is split into two VDOMs, root and vd-lan. The root VDOM provides external SSL-VPN access, where the users are authenticated by a FortiAuthenticator. The vd-lan VDOM provides internal access to a Web server.

For the remote users to access the internal Web server, there are a few requirements as follows:

All traffic must come from the SSL-VPN.

The vd-lan VDOM only allows authenticated traffic to the Web server.

Users must only authenticate once, using the SSL-VPN portal.

SSL-VPN uses RADIUS-based authentication.

Given these requirements and the topology shown in the exhibit, which two statements are true? (Choose

two.)

A. vd-lan connects to FortiAuthenticator as a regular FSSO client.

B. root is configured for FSSO while vd-lan is configured for RSSO.

C. root sends "RADIUS Accounting Messages" to FortiAuthenticator

D. vd-lan receives authentication messages from root using FSSO.

Correct Answer: AC

QUESTION 3

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 4

Refer to the exhibit.

```
FS448D-A (LAG-1) # show
config switch trunk
    edit "LAG-1"
        set mode lacp-active
        set mclag-icl enable
        set members "port13" "port14"
    next
end

FS448D-B (LAG-2) # show
config switch trunk
    edit "LAG-2"
        set mode lacp-active
        set mclag-icl enable
        set members "port13" "portl4"
    next
end

FortiGate-A # show switch-controller managed-switch
config switch-controller managed-switch
    edit FS448D-A
        config ports
            edit "LAG-3"
                set type trunk
                set mode lacp-active
                set mclag enable
                set members "port15"
            next
        end
    next
    edit FS448D-B
        config ports
            edit "LAG-3"
                set type trunk
                set mode lacp-active
                set mclag enable
                set members "port15"
            next
        end
    next
end
```

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

A. LAG-3 on switches on FS448D-A and FS448D-B may be connected to a single 802.3ad trunk on another device.

B. LAG-1 and LAG-2 should be connected to a 4-port single 802.3ad trunk on another device.

C. port13 and port14 on FS448D-A should be connected to port13 and port14 on FS448D-B.

D. LAG-1 and LAG-2 should be connected to a single 4-port 802.3ad interface on the FortiGate-A.

Correct Answer: AC

QUESTION 5

A customer wants to use a central RADIUS server for management authentication when connecting to the FortiGate GUI and to provide different levels of access for different types of employees.

Which three actions are required to provide the requested functionality? (Choose three.)

A. Create a wildcard administrator on the FortiGate.

B. Enable radius-vdom-override in the CLI.

C. Create multiple administrator profiles with matching RADIUS VSAs.

D. Enable accprofile-override in the CLI.

E. Set the RADIUS authentication type to MS-CHAPv2.

Correct Answer: ACD

QUESTION 6

FortiMail is configured with the protected domain "internal.lab".

Which two envelope addresses will need an access control rule to relay e-mail sent for unauthenticated users? (Choose two.)

A. MAIL FROM: training@internal.lab; RCPT TO: student@internal.lab

B. MAIL FROM: student@internal.lab; RCPT TO: student@fortinet.com

C. MAIL FROM: training@fortinet.com; RCPT TO: student@fortinet.com

D. MAIL FROM: student@fortinet.com; RCPT TO: student@internal.lab

Correct Answer: BC

QUESTION 7

A company has just deployed a new FortiMail in gateway mode. The administrator is asked to strengthen e-mail

protection by applying the policies shown below.

E-mails can only be accepted if a valid e-mail account exists. Only authenticated users can send e-mails out.

Which two actions will satisfy the requirements? (Choose two.)

A. Configure recipient address verification.

B. Configure inbound recipient policies.

C. Configure outbound recipient policies.

D. Configure access control rules.

Correct Answer: AD

QUESTION 8

Refer to the exhibit.

```
config vpn certificate setting
      set ocsp-status enable
      set ocsp-default-server "FAC"
      set strict-ocsp-check enable
end
config user peer
   edit _any_
      set ca CA_Cert
      set ldap-server Training-Lab
      set ldap-mode principal-name
   next
end
config user group
   edit "SSLVPN_Users"
      set member "_any_"
   next
end
```

A FortiGate device is configured to authenticate SSL VPN users using digital certificates. A partial FortiGate configuration is shown in the exhibit.

Referring to the exhibit, which two statements about this configuration are true? (Choose two.)

A. The authentication will fail if the user certificate does not contain the user principal name (UPN) information.

B. The authentication will fail if the user certificate does not contain the CA_Cert string in the CA field.

C. The authentication will fail if the OCSP server is down.

D. OCSP is used to verify that the user-signed certificate has not expired.

Correct Answer: AC

QUESTION 9

Refer to the exhibit.

```
FGR # show firewall policy6
config firewall policy6
    edit 1
        set name "internet-ipv6"
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "fd00:acd5:87a4:890d::10/128"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set users "nse8user"
        set profile-type group
        set profile-group "nse8-pfg"
        set nat enable
    next
end

FGR # show firewall policy
config firewall policy
    edit 1
        set name "Internet"
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set logtraffic all
        set fsso disable
        set users "nse8user"
        set webfilter-profile "nse8-wf"
        set dnsfilter-profile "nse8-wf-dns"
        set profile-protocol-options "nse8-po"
        set ssl-ssh-profile "certificate-inspection"
        set nat enable
next
end

FGR # show firewall profile-group nse8-pfg
config firewall profile-group
    edit "nse8-pfg"
        set webfilter-profile "nse8-wf"
        set dnsfilter-profile "nse8-wf-dns"
        set profile-protocol-options "nse8-po"
        set ssl-ssh-profile "certificate-inspection"
    next
end
```

Referring to the firewall polices shown in exhibit, which two statements are true? (Choose two.)

A. The IPv4 policy is allowing security profile groups.

B. The IPv6 traffic for nse8user is filtered using the DNS profile.

C. The IPv4 traffic for nse8user is filtered using the DNS profile.

D. The Web traffic for nse8user is being filtered differently in IPv4 and IPv6.

Correct Answer: BC

QUESTION 10

Refer to the exhibit.

```
ike 0:Dial-Up_0:30:Dial-Up:5: IPsec SA selectors #src=1 #dst=1
ike 0:Dial-Up_0:30:Dial-Up:5: src 0 7 0:0.0.0.0-255.255.255.255:0
ike 0:Dial-Up_0:30:Dial-Up:5: dst 0 7 0:10.10.10.0-10.10.10.255:0
ike 0:Dial-Up_0:30:Dial-Up:5: add dynamic IPsec SA selectors
ike 0:Dial-Up_1:2: moving route 10.10.10.0/255.255.255.0 oif Dial-Up_1(23) metric 15 priority 0 to 0:DialUp_0:5
ike 0:Dial-Up_1:2: del route 10.10.10.0/255.255.255.0 oif Dial-Up_1(23) metric 15 priority 0
ike 0:Dial-Up_1: deleting
ike 0:Dial-Up_1: flushing
ike 0:Dial-Up_1: deleting IPsec SA with SPI fa6915c1
ike 0:Dial-Up_1:Dial-Up: deleted IPsec SA with SPI fa6915c1, SA count: 0
ike 0:Dial-Up_1: sending SNMP tunnel DOWN trap for Dial-Up
ike 0:Dial-Up_1:Dial-Up: delete
```

A FortiGate is configured for a dial-up IPsec VPN to allow multiple remote FortiGate devices to connect to it. However, FortiGate A and B have problems connecting to the VPN. Only one of them can be connected at a time. If site B tries to connect while site A is connected, site A is disconnected. The IKE real-time debug shows the output in the exhibit when site A is disconnected.

Referring to the exhibit, which configuration setting should be executed in the dial-up configuration to allow both VPNs to be connected at the same time?

A. set route-overlap allow

B. set single-source disable

C. set enforce-unique-id disable

D. set add-route enable

Correct Answer: A