

Three User-Friendly Formats of PassTestking Fortinet NSE8_812 Updated Practice Materials



P.S. Free & New NSE8_812 dumps are available on Google Drive shared by PassTestking: https://drive.google.com/open?id=1ExPEjE7-95xSWQKMYy_vU1uehAZ-DKK4

According to the needs of all people, the experts and professors in our company designed three different versions of the NSE8_812 study materials for all customers. The three versions are very flexible for all customers to operate. According to your actual need, you can choose the version for yourself which is most suitable for you to preparing for the coming exam. All the NSE8_812 Study Materials of our company can be found in the three versions. It is very flexible for you to use the three versions of the NSE8_812 study materials to preparing for your coming exam.

As you all know that practicing with the wrong preparation material will waste your valuable money and many precious study hours. So you need to choose the most proper and verified preparation material with caution. Preparation material for the Fortinet NSE 8 - Written Exam (NSE8_812) (NSE8_812) exam questions from PassTestking helps to break down the most difficult concepts into easy-to-understand examples. Also, you will find that all the included questions are based on the last and updated NSE8_812 Exam Dumps version. We are sure that using NSE8_812 Exam Questions preparation material will support you in passing the NSE8_812 exam with confidence.

>> NSE8_812 Valid Test Papers <<

Exam Dumps NSE8_812 Collection - Dump NSE8_812 Collection

With the help of our NSE8_812 test material, users will learn the knowledge necessary to obtain the Fortinet certificate and be competitive in the job market and gain a firm foothold in the workplace. Our NSE8_812 quiz guide' reputation for compiling has created a sound base for our beautiful future business. We are clearly concentrated on the international high-end market, thereby committing our resources to the specific product requirements of this key market sector, as long as cater to all the users who wants to get the test Fortinet certification.

Fortinet NSE 8 - Written Exam (NSE8_812) Sample Questions (Q29-Q34):

NEW QUESTION # 29

Refer to the exhibit.

```

FGT_3 # show router ospf
config router ospf
  set router-id 10.10.10.3
  config area
    edit 0.0.0.0
    next
  end
  config ospf-interface
    edit "port2"
      set interface "port2"
      set network-type point-to-point
    next
  end
  config network
    edit 1
      set prefix 10.10.10.0 255.255.255.0
    next
  end
end

```

You are operating an internal network with multiple OSPF routers on the same LAN segment. FGT_3 needs to be added to the OSPF network and has the configuration shown in the exhibit. FGT_3 is not establishing any OSPF connection. What needs to be changed to the configuration to make sure FGT_3 will establish OSPF neighbors without affecting the DR/BDR election?

```

config router ospf
  config ospf-interface
    edit "port2"
      set priority 255
      set network-type broadcast
    next
  end
end

```

- A.

```

config router ospf
  config ospf-interface
    edit "port2"
      set priority 0
      set network-type broadcast
    next
  end
end

```

- B.

```

config router ospf
  config ospf-interface
    edit "port2"
      set priority 255
      set network-type point-to-multipoint
    next
  end
end

```

- C.

```

config router ospf
  config ospf-interface
    edit "port2"
      set priority 0
      set network-type point-to-multipoint
    next
  end
end

```

- D.

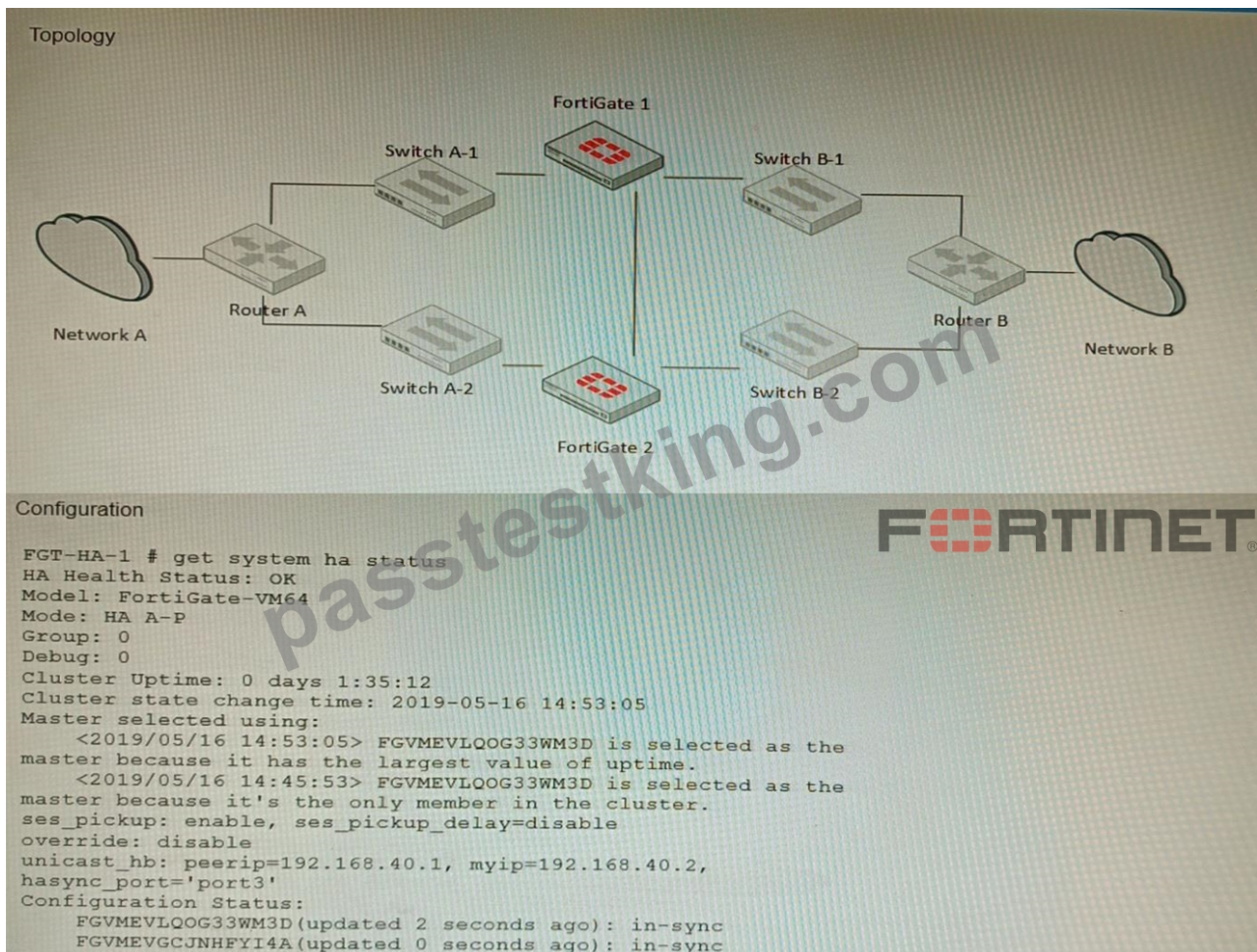
Answer: B

Explanation:

The OSPF configuration shown in the exhibit is using the default priority value of 1 for the interface port1. This means that FGT_3 will participate in the DR/BDR election process with the other OSPF routers on the same LAN segment. However, this is not desirable because FGT_3 is a new device that needs to be added to the OSPF network without affecting the existing DR/BDR election. Therefore, to make sure FGT_3 will establish OSPF neighbors without affecting the DR/BDR election, the priority value of the interface port1 should be changed to 0. This will prevent FGT_3 from becoming a DR or BDR and allow it to form OSPF adjacencies with the current DR and BDR. Option B shows the correct configuration that changes the priority value to 0. Option A is incorrect because it does not change the priority value. Option C is incorrect because it changes the network type to point-to-point, which is not suitable for a LAN segment with multiple OSPF routers. Option D is incorrect because it changes the area ID to 0.0.0.1, which does not match the area ID of the other OSPF routers on the same LAN segment. Reference: <https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/358640/basic-ospf-example>

NEW QUESTION # 30

Refer to the exhibits.



The exhibits show a FortiGate network topology and the output of the status of high availability on the FortiGate. Given this information, which statement is correct?

- A. The cluster members are on the same network and the IP addresses were statically assigned.
- B. The ethertype values of the HA packets are 0x8890, 0x8891, and 0x8892
- C. The cluster mode can support a maximum of four (4) FortiGate VMs
- **D. FGVMEVLQOG33WM3D and FGVMEVGCJNHFYI4A share a virtual MAC address.**

Answer: D

Explanation:

The output of the status of high availability on the FortiGate shows that the cluster mode is active-passive, which means that only one FortiGate unit is active at a time, while the other unit is in standby mode. The active unit handles all traffic and also sends HA heartbeat packets to monitor the standby unit. The standby unit becomes active if it stops receiving heartbeat packets from the active unit, or if it receives a higher priority from another cluster unit. In active-passive mode, all cluster units share a virtual MAC address for each interface, which is used as the source MAC address for all packets forwarded by the cluster. References:

<https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103439/high-availability-with-two-fortigates>

NEW QUESTION # 31

Refer to the exhibits.

GUI Access

GUI Access

Site title: FortiAuthenticator

GUI idle timeout: 480 minutes (1-480 mins)

Maximum HTTP header length: 4 (4-16 KB)

HTTPS Certificate: Default-Server-Certificate | CN=Default-Server-Certificate-7D895AD8

☐ HTTP Strict Transport Security (HSTS) Expiry: 180 (0-730 days)

Certificate authority type: Local CA Trusted CA

CA certificate that issued the server certificate: Fortinet_CA1_Root | emailAddress=support@fortinet.com

☒ Allow all hosts/domain names

Public IP/FQDN for FortiToken Mobile: 100.64.1.76

Configuration

```
FG-1 # show system ftm-push
config system ftm-push
    set server-cert "self-sign"
    set server "10.0.1.150"
    set status enable
end
```

```
FG-1# show system interface port1
config system interface
    edit "port1"
        set vdom "root"
        set ip 100.64.1.41 255.255.255.0
        set allowaccess ping
        set type physical
        set alias "WAN"
        set role wan
        set snmp-index 1
    next
end
```

Topology

An administrator has configured a FortiGate and Forti Authenticator for two-factor authentication with FortiToken push notifications for their SSL VPN login. Upon initial review of the setup, the administrator has discovered that the customers can manually type in their two-factor code and authenticate but push notifications do not work. Based on the information given in the exhibits, what must be done to fix this?

- A. On FG-1 CLI, the ftm-push server setting must point to 100.64.141.
- B. On FAC-1, the FortiToken public IP setting must point to 100.64.1.41
- **C. FAC-1 must have an internet routable IP address for push notifications.**
- D. On FG-1 port1, the ftm access protocol must be enabled.

Answer: C

Explanation:

FortiToken push notifications require that the FortiAuthenticator has an internet routable IP address. This is because the FortiAuthenticator uses this IP address to send push notifications to the FortiGate.

The other options are not correct. Enabling the ftm access protocol on FG-1 port1 is not necessary for push notifications to work. The ftm-push server setting on FG-1 CLI should already point to the FortiAuthenticator's IP address. The FortiToken public IP setting on FAC-1 is not relevant to push notifications.

Here is a table that summarizes the different options:

Option	Description
Enable the ftm access protocol on FG-1 port1	Not necessary for push notifications to work.
Set the ftm-push server setting on FG-1 CLI to the FortiAuthenticator's IP address	Already done.
Set the FortiToken public IP setting on FAC-1 to 100.64.141	Not relevant to push notifications.
Set the FortiAuthenticator's IP address to an internet routable IP address	Necessary for push notifications to work.

NEW QUESTION # 32

SD-WAN is configured on a FortiGate. You notice that when one of the internet links has high latency the time to resolve names using DNS from FortiGate is very high.

You must ensure that the FortiGate DNS resolution times are as low as possible with the least amount of work.

What should you configure?

- A. Configure two DNS servers and use DNS servers recommended by the two internet providers.
- B. Configure local out traffic to use the outgoing interface based on SD-WAN rules with a manual defined IP associated to a loopback interface and configure an SD-WAN rule from the loopback to the DNS server.
- C. Configure an SD-WAN rule to the DNS server and use the FortiGate interface IPs in the source address.
- **D. Configure local out traffic to use the outgoing interface based on SD-WAN rules with the interface IP and configure an SD-WAN rule to the DNS server.**

Answer: D

Explanation:

SD-WAN is a feature that allows users to optimize network performance and reliability by using multiple WAN links and applying rules based on various criteria, such as latency, jitter, packet loss, etc. One way to ensure that the FortiGate DNS resolution times are as low as possible with the least amount of work is to configure local out traffic to use the outgoing interface based on SD-WAN rules with the interface IP and configure an SD-WAN rule to the DNS server. This means that the FortiGate will use the best WAN link available to send DNS queries to the DNS server according to the SD-WAN rule, and use its own interface IP as the source address. This avoids NAT issues and ensures optimal DNS performance. Reference:

<https://docs.fortinet.com/document/fortigate/7.0.0/sd-wan/19662/sd-wan>

NEW QUESTION # 33

Refer to the exhibits.

FortiSandbox

FortiSandbox

FortiSandbox Inspection

☒ Statistics...

FortiSandbox type:

Appliance
 Cloud
 Enhanced Cloud

Server name/IP:

fortisandboxcloud.com

Test Connection

Notification email:

Statistics interval:

5
 (minutes)

Scan timeout:

30
 (minutes)

Scan result expires in:

60
 (minutes)

AV Profile

AntiVirus Profile

FortiSandbox

Scan mode:

Submit and wait for result
 Submit only

☒ Attachment analysis

Malicious/Virus	Action: --Default--	+ New...	Edit...
High risk	Action: --Default--	+ New...	Edit...
Medium risk	Action: --Default--	+ New...	Edit...
Low risk	Action: --Default--	+ New...	Edit...
No Result	Action: --None--	+ New...	Edit...

☐ URL analysis

Malicious/Virus	Action: --Default--	+ New...	Edit...
High risk	Action: --Default--	+ New...	Edit...
Medium risk	Action: --Default--	+ New...	Edit...
Low risk	Action: --Default--	+ New...	Edit...
No Result	Action: --None--	+ New...	Edit...

Create

Cancel

You must integrate a FortiMail and FortiSandbox Enhanced Cloud solution for a customer who is concerned about the e-mails being delayed for too long.

According to the configuration shown in the exhibits, which would be an expected behavior?

- A. If an attachment is sent to the FortiSandbox while the job queue is full, the e-mail might be delayed for up to 30 minutes, then e-mail will be relayed to the mail server.
- B. FortiMail will ignore the timeout value if content disarm and reconstruction (CDR) is enabled.
- **C. FortiMail will relay valid e-mails to the mail server as soon as it is done with other local inspections.**
- D. FortiMail will not wait for results but only for attachments that have been already submitted to the FortiSandbox in the last 60 minutes.

Answer: C

NEW QUESTION # 34

.....

BONUS!!! Download part of PassTestking NSE8_812 dumps for free: https://drive.google.com/open?id=1ExPeJ7E-95xSWOKMYy_vU1uehAZ-DKK4

