NSE8_812 Q&As

Network Security Expert 8 Written Exam

Pass Fortinet NSE8_812 Exam with 100% Guarantee

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

https://www.pass4itsure.com/nse8_812.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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 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.

B. Configure an SD-WAN rule to the DNS server and use the FortiGate interface IPs in the source address.

C. Configure two DNS servers and use DNS servers recommended by the two internet providers.

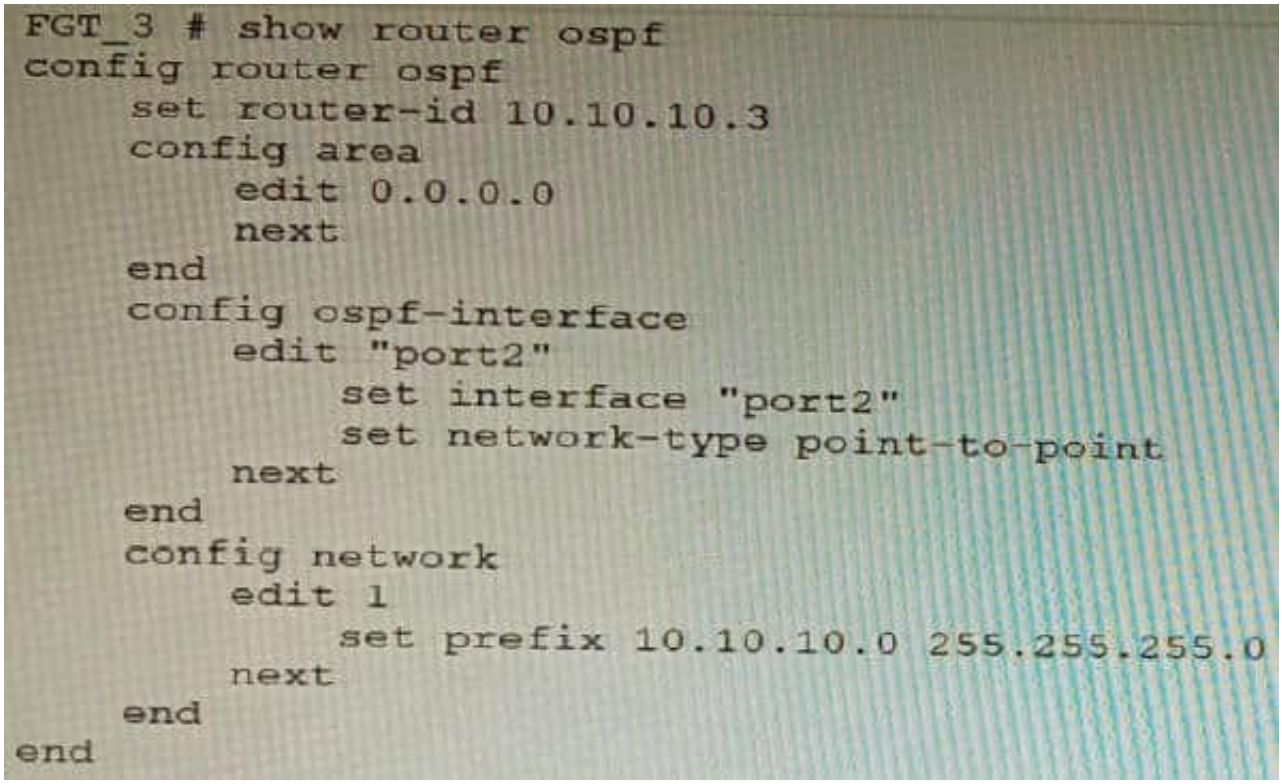
D. Configure local out traffic to use the outgoing interface based on SD-WAN rules with the interface IP and configure an SD-WAN rule to the DNS server.

Correct 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. References: https://docs.fortinet.com/document/fortigate/7.0.0/sd- wan/19662/sd-wan

QUESTION 2

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?

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

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

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

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

A. Option A

B. Option B

C. Option C

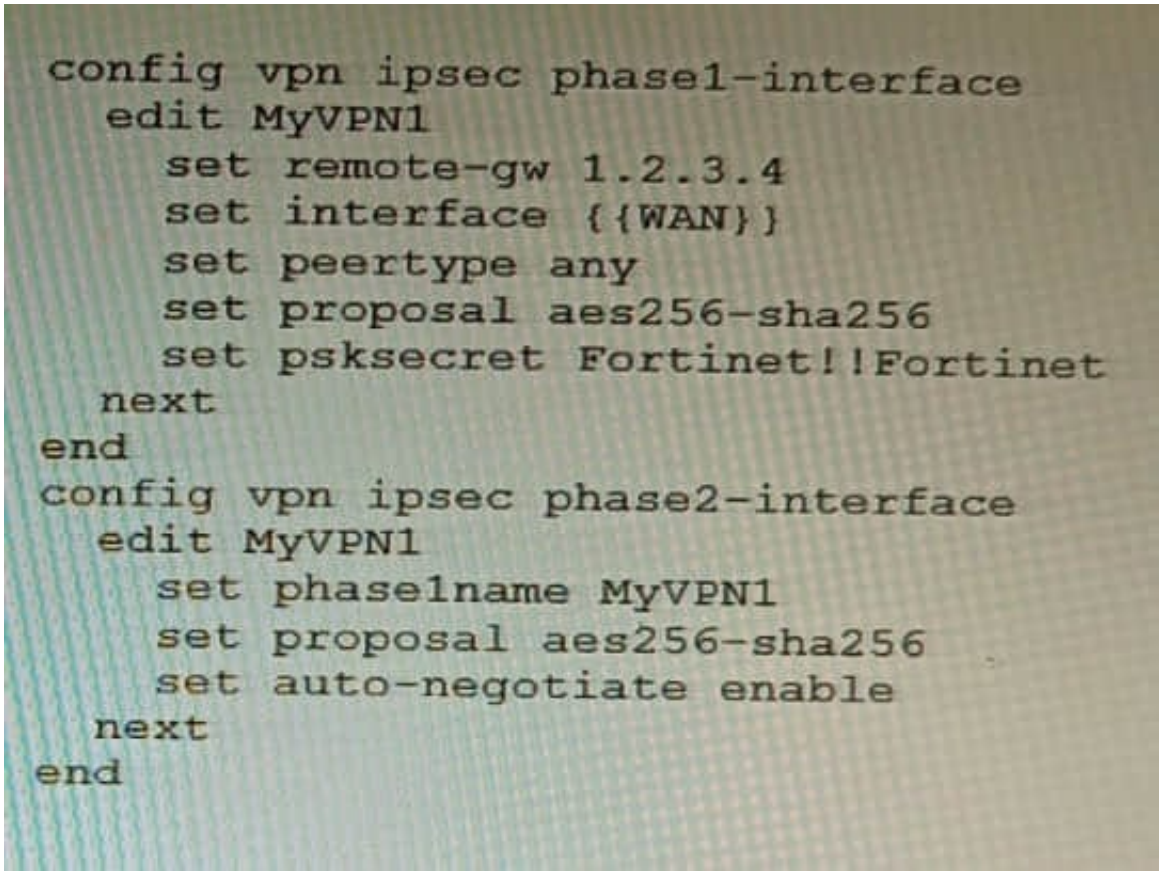
D. Option D

Correct 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 thecurrent 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.
References:https://docs.fortinet.com/document/ fortigate/7.0.0/administration- guide/358640/basic-ospf-example

QUESTION 3

Refer to the exhibit.



FortiManager is configured with the Jinja Script under CLI Templates shown in the exhibit.

Which two statements correctly describe the expected behavior when running this template? (Choose two.)

A. The Jinja template will automatically map the interface with "WAN" role on the managed FortiGate.

B. The template will work if you change the variable format to $(WAN).

C. The template will work if you change the variable format to {{ WAN }}.

D. The administrator must first manually map the interface for each device with a meta field.

E. The template will fail because this configuration can only be applied with a CLI or TCL script.

Correct Answer: DE

Explanation: D. The administrator must first manually map the interface for each device with a meta field.

The Jinja template in the exhibit is expecting a meta field calledWANto be set on the managed FortiGate. This meta field will specify which interface on the FortiGate should be assigned the "WAN" role. If the meta field is not set, then the

template will fail. E. The template will fail because this configuration can only be applied with a CLI or TCL script.

The Jinja template in the exhibit is trying to configure the interface role on the managed FortiGate. This type of configuration can only be applied with a CLI or TCL script. The Jinja template will fail because it is not a valid CLI or TCL script.

QUESTION 4

You are responsible for recommending an adapter type for NICs on a FortiGate VM that will run on an ESXi Hypervisor. Your recommendation must consider performance as the main concern, cost is not a factor. Which adapter type for the NICs will you recommend?

A. Native ESXi Networking with E1000

B. Virtual Function (VF) PCI Passthrough

C. Native ESXi Networking with VMXNET3

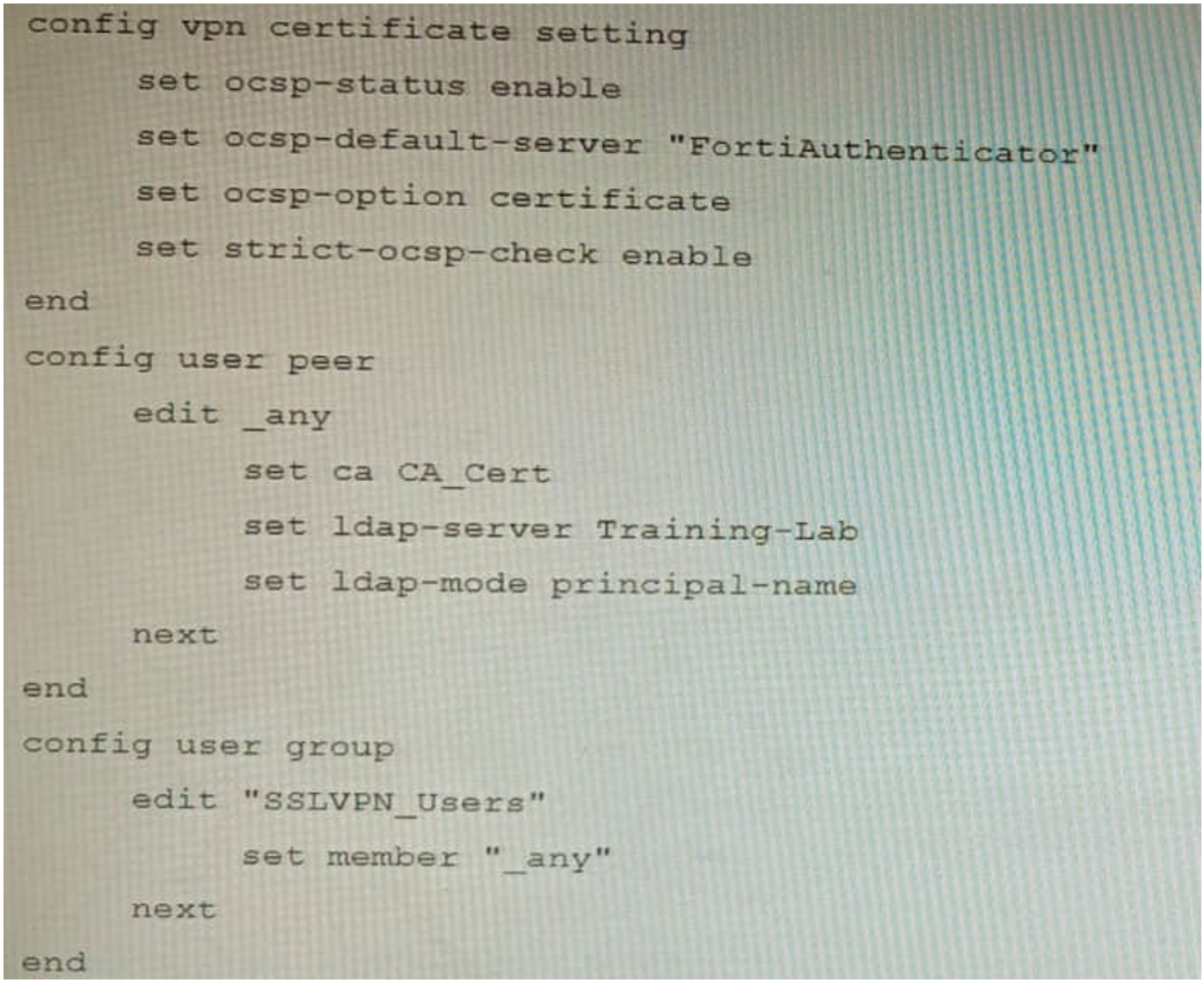
D. Physical Function (PF) PCI Passthrough

Correct Answer: C

Explanation: The FortiGate VM is a virtual firewall appliance that can run on various hypervisors, such as ESXi, Hyper-V, KVM, etc. The adapter type for NICs on a FortiGate VM determines the performance and compatibility of the network interface cards with the hypervisor and the physical network. There are different adapter types available for NICs on a FortiGate VM, such as E1000, VMXNET3, SR-IOV, etc. If performance is the main concern and cost is not a factor, one option is to use native ESXi networking with VMXNET3 adapter type for NICs on a FortiGate VM that will run on an ESXi hypervisor. VMXNET3 is a paravirtualized network interface card that is optimized for performance in virtual machines and supports features such as multiqueue support, Receive Side Scaling (RSS), Large Receive Offload (LRO), IPv6 offloads, and MSI/MSI-X interrupt delivery. Native ESXi networking means that the FortiGate VM uses the standard virtual switch (vSwitch) or distributed virtual switch (dvSwitch) provided by the ESXi hypervisor to connect to the physical network. This option can provide high performance and compatibility for NICs on a FortiGate VM without requiring additional hardware or software components. References:
https://docs.fortinet.com/document/fortigate/7.0.0/vm-installation- for-vmware-esxi/19662/installing-fortigate-vm-on-vmware- esxihttps://docs.fortinet.com/document/fortigate/7.0.0/vm-installationfor-vmware- esxi/19662/networking

QUESTION 5

An administrator has configured a FortiGate device to authenticate SSL VPN users using digital certificates. A FortiAuthenticator is the certificate authority (CA) and the Online Certificate Status Protocol (OCSP) server. Part of the FortiGate configuration is shown below:



```
config vpn certificate setting
    set ocsp-status enable
    set ocsp-default-server "FortiAuthenticator"
    set ocsp-option certificate
    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
```

Based on this configuration, which two statements are true? (Choose two.)

A. OCSP checks will always go to the configured FortiAuthenticator

B. The OCSP check of the certificate can be combined with a certificate revocation list.

C. OCSP certificate responses are never cached by the FortiGate.

D. If the OCSP server is unreachable, authentication will succeed if the certificate matches the CA.

Correct Answer: BD

B is correct because the OCSP check of the certificate can be combined with a certificate revocation list (CRL). This

means that the FortiGate will check the OCSP server to see if the certificate has been revoked, and it will also check the CRL to see if the certificate has been revoked. D is correct because if the OCSP server is unreachable, authentication will succeed if the certificate matches the CA. This is because the FortiGate will fall back to using the CRL if the OCSP server is unreachable. The other options are incorrect. Option A is incorrect because OCSP checks can go to other OCSP servers, not just the FortiAuthenticator. Option C is incorrect because OCSP certificate responses can be cached by the FortiGate. References: Configuring SSL VPN authentication using digital certificates | FortiGate / FortiOS 7.2.0 - Fortinet Document Library Online Certificate Status Protocol (OCSP) | FortiGate / FortiOS 7.2.0 - Fortinet Document Library Certificate Revocation Lists (CRLs) | FortiGate / FortiOS 7.2.0 - Fortinet Document Library