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.passapply.com/nse8_812.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

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 exhibits.

Exhibit A

	FORTIAP 431F
Hardware	
Hardware Type	Indoor AP
Number of Radios	3 + 1 BLE
Number of Antennas	5 Internal + 1 BLE Internal
Antenna Type and Peak Gain	PIFA: 4 dBi for 2.4 GHz, 5 dBi for 5 GHz
Maximum Data Rate	Radio 1: up to 1147 Mbps Radio 2: up to 2402 Mbps Radio 3: scan only
Bluetooth Low Energy Radio	Bluetooth scanning and iBeacon advertisement @ 6 dBm max TX power
Interfaces	1× 100/1000/2500 Base-T RJ45, 1 × 10/100/1000 Base-T RJ45, 1x Type A USB, 1x RS-232 RJ45 Serial Port
Power over Ethernet (PoE)	• 802.3at PoE default • 1 port powered by 802.3at or 2 ports powered by 802.3af - Full System functionality + USB support
Maximum Tx Power (Conducted)	Radio 1: 2.4 GHz 24 dBm / 251 mW (4 chains combined)* Radio 2: 5 GHz 23 dBm / 200 mW (4 chains combined)* Radio 3: NA
Environment	
Power Supply	SP-FAP400-PA-XX or GPI-130
Power Consumption (Max)	24.5 W
Directives	Low Voltage Directive • RoHS
UL2043 Plenum Material	No
Mean Time Between Failures	>10 Years
Surge Protection Built In	Yes
Hit-less PoE Failover	Yes

Exhibit B

	FORTISWITCH 224E-POE	FORTISWITCH 124E-FPOE	FORTISWITCH 248E-FPOE
Hardware Specifications			
Total Network Interfaces	24x GE RJ45 ports and 4x GE SFP ports	24x GE RJ45 and 4x GE SFP	48x GE RJ45 ports and 4x GE SFP ports
Dedicated Management 10/100 Port	1	0	1
RJ-45 Serial Console Port	1	1	1
Form Factor	1 RU Rack Mount	1 RU Rack Mount	1 RU Rack Mount
Power over Ethernet (PoE) Ports	12 (802.3af/802.3at)	24 (802.3af/at)	48 (802.3af/802.3at)
PoE Power Budget	180 W	370 W	740 W
Mean Time Between Failures	> 10 years	> 10 years	> 10 years
Retail Price	$1,000	$1,250	$1,500

A customer wants to deploy 12 FortiAP 431F devices on high density conference center, but they do not currently have any PoE switches to connect them to. They want to be able to run them at full power while having network redundancy From the FortiSwitch models and sample retail prices shown in the exhibit, which build of materials would have the lowest cost, while fulfilling the customer\\'s requirements?

A. 1x FortiSwitch 248EFPOE

B. 2x FortiSwitch 224E-POE

C. 2x FortiSwitch 248E-FPOE

D. 2x FortiSwitch 124E-FPOE

Correct Answer: C

Explanation: The customer wants to deploy 12 FortiAP 431F devices on a high density conference center, but they do not have any PoE switches to connect them to. They want to be able to run them at full power while having network redundancy. PoE switches are switches that can provide both data and power to connected devices over Ethernet cables, eliminating the need for separate power adapters or outlets. PoE switches are useful for deploying devices such as wireless access points, IP cameras, and VoIP phones in locations where power outlets are scarce or inconvenient. The FortiAP 431F is a wireless access point that supports PoE+ (IEEE 802.3at) standard, which can deliver up to 30W of power per port. The FortiAP 431F has a maximum power consumption of 25W when running at full power. Therefore, to run 12 FortiAP 431F devices at full power, the customer needs PoE switches that can provide at least 300W of total PoE power budget (25W x 12). The customer also needs network redundancy, which means that they need at least two PoE switches to connect the FortiAP devices in case one switch fails or loses power. From the FortiSwitch models and sample retail prices shown in the exhibit, the build of materials that has the lowest cost while fulfilling the customer\\'s requirements is 2x FortiSwitch 248E- FPOE. The FortiSwitch 248E-FPOE is a PoE switch that has 48 GE ports with PoE+ capability and a total PoE power budget of 370W. It also has 4x 10 GE SFP+ uplink ports for high-speed connectivity. The sample retail price of the FortiSwitch 248E-FPOE is $1,995, which means that two units will cost $3,990. This is the lowest cost among the other options that can meet the customer\\'s requirements. Option A is incorrect because the FortiSwitch 248EFPOE is a non-PoE switch that has no PoE capability or power budget. It cannot provide power to the FortiAP devices over Ethernet cables. Option B is incorrect because the FortiSwitch 224E-POE is a PoE switch that has only 24 GE ports with PoE+ capability and a total PoE powerbudget of 185W. It cannot provide enough ports or power to run 12 FortiAP devices at full power. Option D is incorrect because the FortiSwitch 124E-FPOE is a PoE switch that has only 24 GE ports with PoE+ capability and a total PoE power budget of 185W. It cannot provide enough ports or power to run 12 FortiAP devices at full power. References: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSwitch_Secure_Access_Series.pdfhttps://www.fortinet.com/content/dam/fortine t/assets/data-sheets/FortiAP_400_Series.pdf

QUESTION 3

A customer with a FortiDDoS 200F protecting their fibre optic internet connection from incoming traffic sees that all the traffic was dropped by the device even though they were not under a DoS attack. The traffic flow was restored after it was rebooted using the GUI. Which two options will prevent this situation in the future? (Choose two)

A. Change the Adaptive Mode.

B. Create an HA setup with a second FortiDDoS 200F

C. Move the internet connection from the SFP interfaces to the LC interfaces

D. Replace with a FortiDDoS 1500F

Correct Answer: BD

B is correct because creating an HA setup with a second FortiDDoS 200F will provide redundancy in case one of the devices fails. This will prevent all traffic from being dropped in the event of a failure.

D is correct because the FortiDDoS 1500F has a larger throughput capacity than the FortiDDoS 200F. This means that

it will be less likely to drop traffic even under heavy load.

The other options are incorrect. Option A is incorrect because changing the Adaptive Mode will not prevent the device from dropping traffic. Option C is incorrect because moving the internet connection from the SFP interfaces to the LC

interfaces will not change the throughput capacity of the device.

References:

FortiDDoS 200F Datasheet | Fortinet Document Library FortiDDoS 1500F Datasheet | Fortinet Document Library High Availability (HA) on FortiDDoS | FortiDDoS / FortiOS 7.0.0 - Fortinet Document Library

QUESTION 4

On a FortiGate Configured in Transparent mode, which configuration option allows you to control Multicast traffic passing through the?

A.
```
config system settings
    set multicast-skip-policy disable
end
```

B.
```
config system settings
    set multicast-forward enable
end
```

C.
```
config system settings
    set multicast-forward disable
end
```

D.
```
config system settings
    set multicast-skip-policy enable
end
```

A. Option A

B. Option B

C. Option C

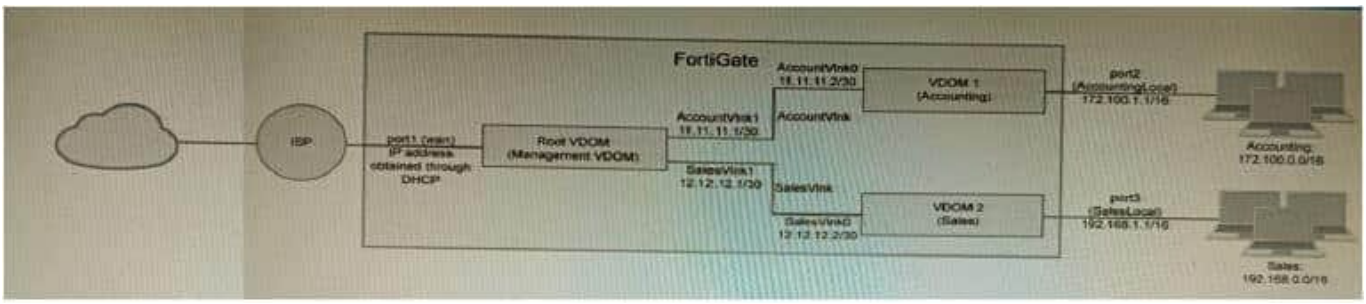
D. Option D

Correct Answer: C

Explanation: To control multicast traffic passing through a FortiGate configured in transparent mode, you can use multicast policies. Multicast policies allow you to filter multicast traffic based on source and destination addresses, protocols, and interfaces. You can also apply securityprofiles to scan multicast traffic for threats and violations. References:https://docs.fortinet.com/document/fortigate/6.2.14/cookbook/968606/configurin g-multicast-forwarding

QUESTION 5

Refer to the exhibit.



A customer has deployed a FortiGate 300E with virtual domains (VDOMs) enabled in the multi-VDOM mode. There are three VDOMs: Root is for management and internet access, while VDOM 1 and VDOM 2 are used for segregating internal traffic. AccountVInk and SalesVInk are standard VDOM links in Ethernet mode.

Given the exhibit, which two statements below about VDOM behavior are correct? (Choose two.)

A. You can apply OSPF routing on the VDOM link in either PPP or Ethernet mode

B. Traffic on AccountVInk and SalesVInk will not be accelerated.

C. The VDOM links are in Ethernet mode because they have IP addressed assigned on both sides.

D. Root VDOM is an Admin type VDOM, while VDOM 1 and VDOM 2 are Traffic type VDOMs.

E. OSPF routing can be configured between VDOM 1 and Root VDOM without any configuration changes to AccountVInk

Correct Answer: AD

A. You can apply OSPF routing on the VDOM link in either PPP or Ethernet mode. This is because VDOM links can be configured in either PPP or Ethernet mode, and OSPF routing can be configured on both types of links. D. Root VDOM is

an Admin type VDOM, while VDOM 1 and VDOM 2 are Traffic type VDOMs. This is because the Root VDOM is the default VDOM, and it is used for management and internet access. VDOM 1 and VDOM 2 are traffic type VDOMs, which are

used for segregating internal traffic.

The other options are not correct.

B. Traffic on AccountVInk and SalesVInk will not be accelerated. This is because VDOM links are not accelerated by default. However, you can configure acceleration on VDOM links if you want.

C. The VDOM links are in Ethernet mode because they have IP addressed assigned on both sides. This is not necessarily true. The VDOM links could be in PPP mode even if they have IP addresses assigned on both sides. E. OSPF routing

can be configured between VDOM 1 and Root VDOM without any configuration changes to AccountVInk. This is correct. OSPF routing can be configured between any two VDOMs, even if they are not directly connected. In this case, the

OSPF routing would be configured on the AccountVInk link.

QUESTION 6

Refer to the exhibits.

Exhibit A

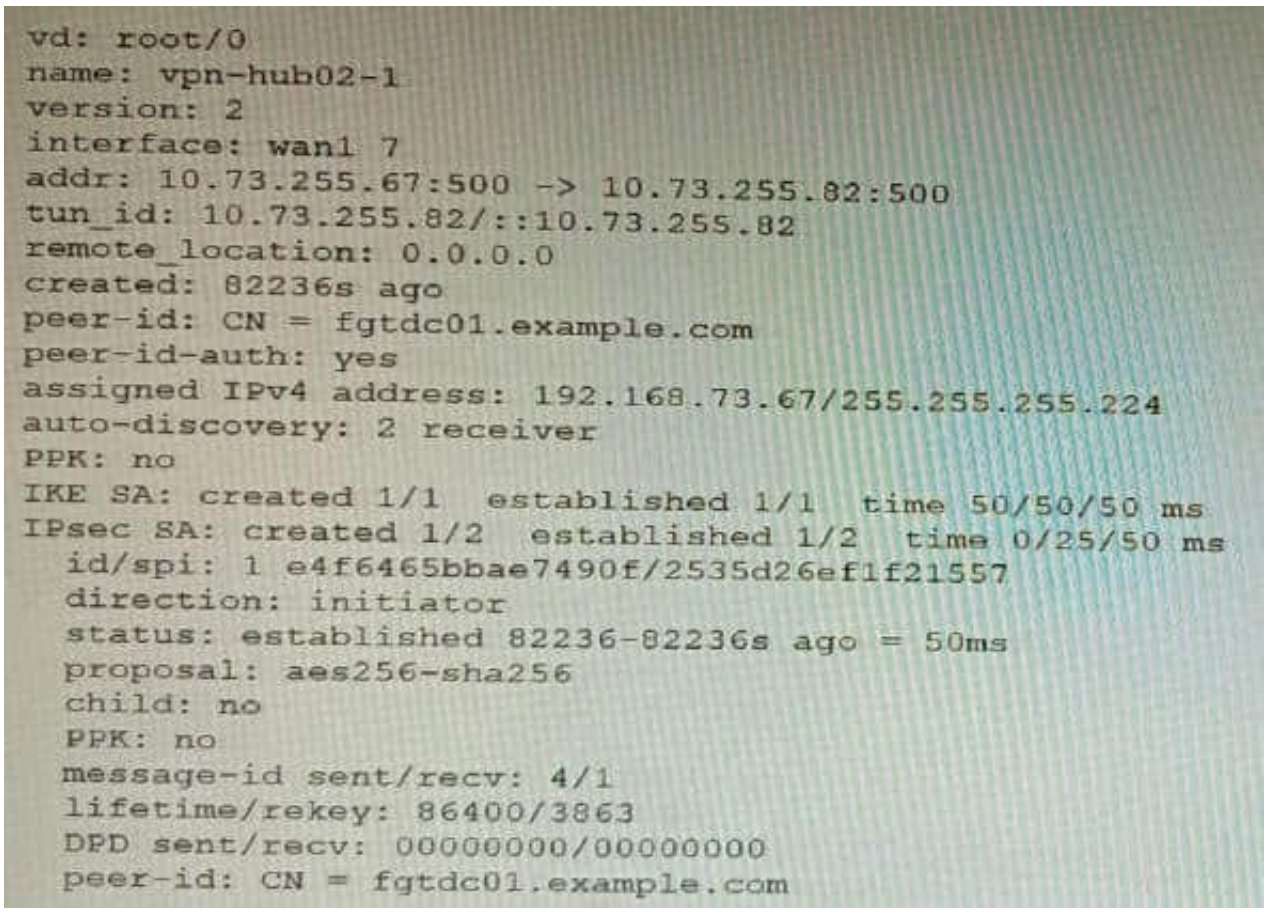


Exhibit B

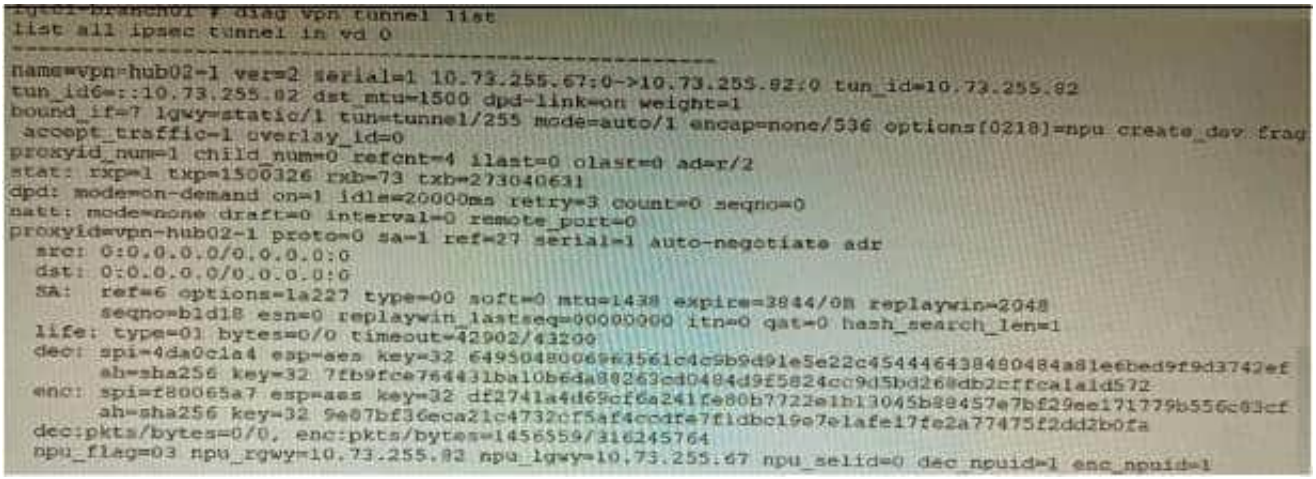
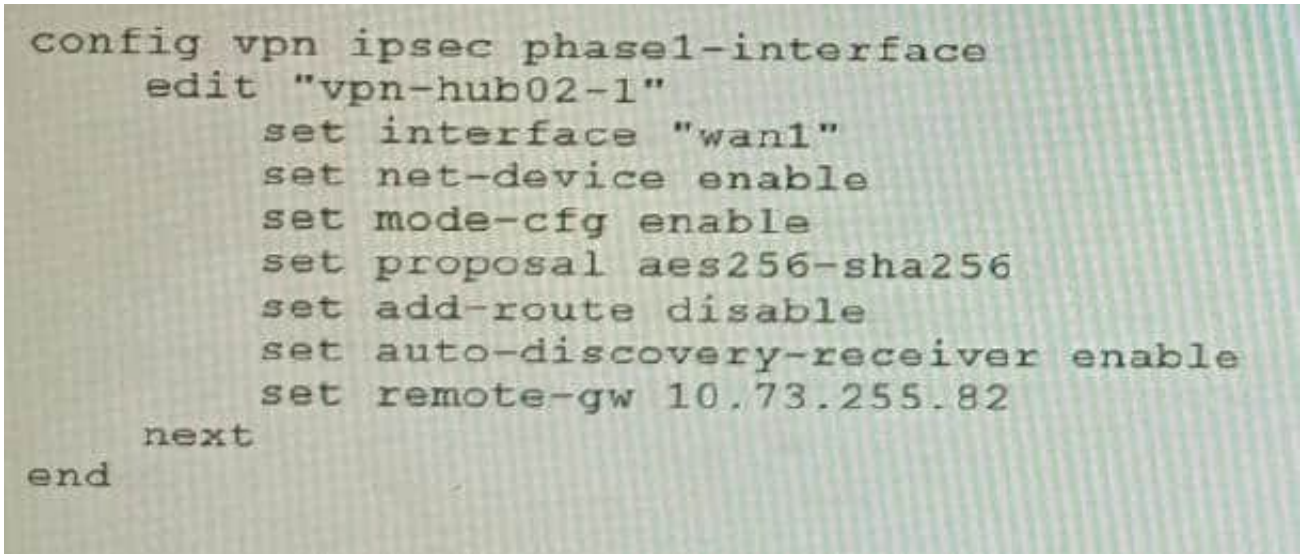


Exhibit C



A customer is trying to set up a VPN with a FortiGate, but they do not have a backup of the configuration. Output during a troubleshooting session is shown in the exhibits A and B and a baseline VPN configuration is shown in Exhibit C Referring to the exhibits, which configuration will restore VPN connectivity?

A.
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 1
        set authmethod signature
        set certificate "BR01FGTLOCAL"
        set peer "vpn-hub02-1_peer"
    next
end
```

B.
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 2
        set net-device enable
        set psksecret fortinet
    next
end
```

C.
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 2
        set authmethod signature
        set npu-offload disable
        set certificate "BR01FGTLOCAL"
        set peer "vpn-hub02-1_peer"
    next
end
```

D.
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 2
        set authmethod signature
        set certificate "BR01FGTLOCAL"
        set peer "vpn-hub02-1_peer"
    next
end
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: C

Explanation: The output in Exhibit A shows that the VPN tunnel is not established because the peer IP address is incorrect. The output in Exhibit B shows that the peer IP address is 192.168.1.100, but the baseline VPN configuration in Exhibit C shows that the peer IP address should be 192.168.1.101. To restore VPN connectivity, you need to change the peer IP address in the VPN tunnel configuration to 192.168.1.101. The correct configuration is shown below: config vpn ipsec phase1-interface edit "wan" set peer-ip 192.168.1.101 set peer-id 192.168.1.101 set dhgrp 1 set auth-mode psk set psk SECRET_PSK next end Option A is incorrect because it does not change the peer IP address. Option B is incorrect because it changes the peer IP address to 192.168.1.100, which is the incorrect IP address. Option D is incorrect because it does not include the necessary configuration for the VPN tunnel.

QUESTION 7

What is the benefit of using FortiGate NAC LAN Segments?

A. It provides support for multiple DHCP servers within the same VLAN.

B. It provides physical isolation without changing the IP address of hosts.

C. It provides support for IGMP snooping between hosts within the same VLAN

D. It allows for assignment of dynamic address objects matching NAC policy.

Correct Answer: D

Explanation: FortiGate NAC LAN Segments are a feature that allows users to assign different VLANs to different LAN segments without changing the IP address of hosts or bouncing the switch port. This provides physical isolation while maintaining firewall sessions and avoiding DHCP issues. One benefit of using FortiGate NAC LAN Segments is that it allows for assignment of dynamic address objects matching NAC policy. This means that users can create firewall policies based on dynamic address objects that match the NAC policy criteria, such as device type, OS type, MAC address, etc. This simplifies firewall policy management and enhances security byapplying different security profiles to different types of devices. References: https://docs.fortinet.com/document/fortigate/7.0.0/new-features/856212/nac-lan-segments- 7-0-1

QUESTION 8

Refer to the exhibit.

You have deployed a security fabric with three FortiGate devices as shown in the exhibit. FGT_2 has the following configuration:

```
config system csf
set fabric-object-unification local
end
```

FGT_1 and FGT_3 are configured with the default setting. Which statement is true for the synchronization of fabric-objects?

A. Objects from the FortiGate FGT_2 will be synchronized to the upstream FortiGate.

B. Objects from the root FortiGate will only be synchronized to FGT__2.

C. Objects from the root FortiGate will not be synchronized to any downstream FortiGate.

D. Objects from the root FortiGate will only be synchronized to FGT_3.

Correct Answer: C

Explanation: The fabric-object-unification setting on FGT_2 is set to local, which means that objects will not be synchronized to any other FortiGate devices in the security fabric. The default setting for fabric-object-unification is default, which

means that objects will be synchronized from the root FortiGate to all downstream FortiGate devices. Since FGT_2 is not the root FortiGate and the fabric-object-unification setting is set to local, objects from the root FortiGate will not be

synchronized to FGT_2.

Reference:

Synchronizing objects across the Security Fabric:

https://docs.fortinet.com/document/fortigate/6.4.0/administration- guide/880913/synchronizing-objects-across-the-security-fabric

QUESTION 9

You are deploying a FortiExtender (FEX) on a FortiGate-60F. The FEX will be managed by the FortiGate. You anticipate high utilization. The requirement is to minimize the overhead on the device for WAN traffic.

Which action achieves the requirement in this scenario?

A. Add a switch between the FortiGate and FEX.

B. Enable CAPWAP connectivity between the FortiGate and the FortiExtender.

C. Change connectivity between the FortiGate and the FortiExtender to use VLAN Mode

D. Add a VLAN under the FEX-WAN interface on the FortiGate.

Correct Answer: C

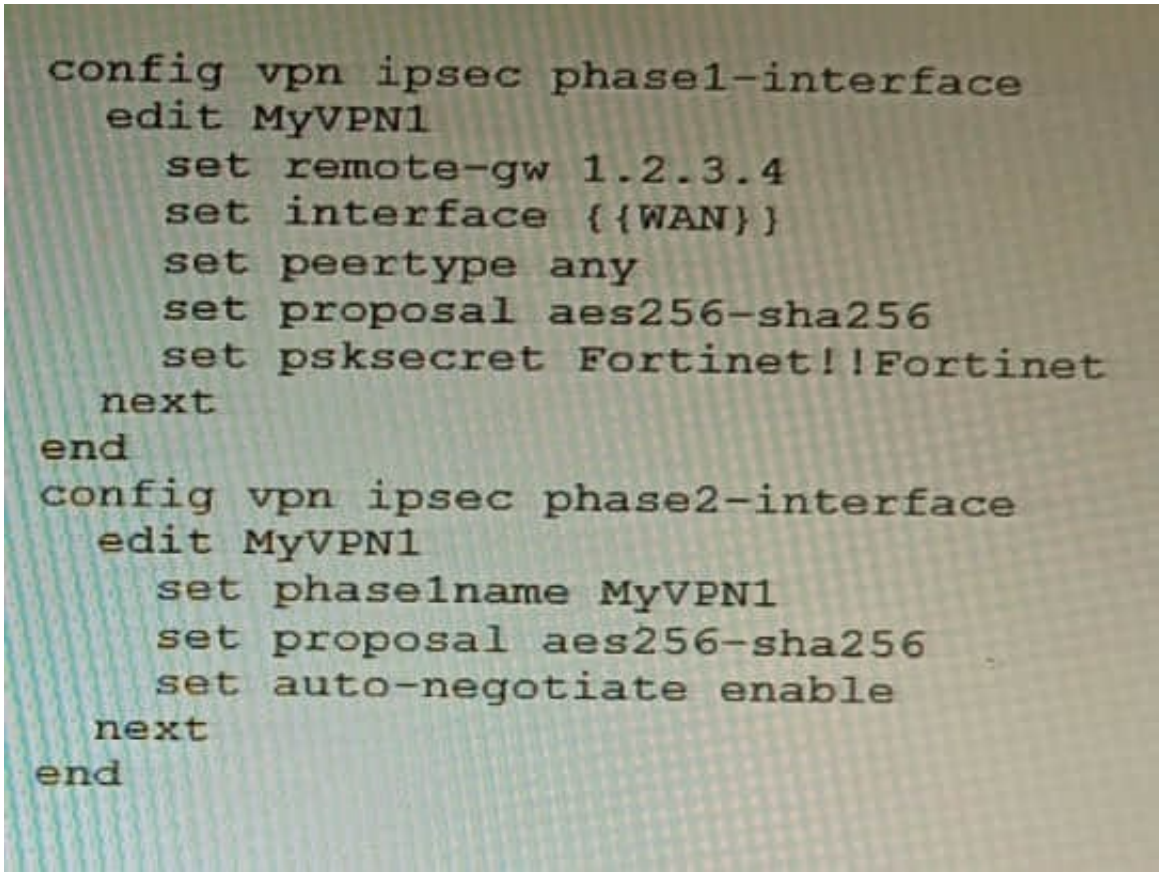
Explanation: VLAN Mode is a more efficient way to connect a FortiExtender to a FortiGate than CAPWAP Mode. This is because VLAN Mode does not require the FortiExtender to send additional control traffic to the FortiGate. The other options are not correct.

A. Add a switch between the FortiGate and FEX. This will add overhead to the network, as the switch will need to process the traffic. B. Enable CAPWAP connectivity between the FortiGate and the FortiExtender. This will increase the overhead on the FortiGate, as it will need to process additional control traffic.

D. Add a VLAN under the FEX-WAN interface on the FortiGate. This will not affect the overhead on the FortiGate.

QUESTION 10

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.

Latest NSE8_812 Dumps NSE8_812 Practice Test NSE8_812 Study Guide