

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.leads4pass.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

You are creating the CLI script to be used on a new SD-WAN deployment. You will have branches with a different number of internet connections and want to be sure there is no need to change the Performance SLA configuration in case more connections are added to the branch.

The current configuration is:

```
config health-check
  edit "Default_AWS"
    set server "aws.amazon.com"
    set protocol http
    set interval 1000
    set probe-timeout 1000
    set recoverytime 10
  config sla
    edit 1
      set latency-threshold 250
      set jitter-threshold 50
      set packetloss-threshold 5
    next
  end
next
end
```

Which configuration do you use for the Performance SLA members?

- A. set members any
- B. set members 0
- C. current configuration already fulfills the requirement

D. set members all

Correct Answer: A

Explanation: The set members any option will ensure that all of the SD-WAN interfaces are included in the Performance SLA. This is the best option if you want to be sure that the Performance SLA will be triggered even if more connections are added to the branch in the future. The set members 0 option will exclude all of the SD-WAN interfaces from the Performance SLA. This is not a good option because it will prevent the Performance SLA from being triggered even if there is a problem with the network. The current configuration already fulfills the requirement option is incorrect because it does not ensure that all of the SD-WAN interfaces will be included in the Performance SLA. The set members all option will include all of the SD-WAN interfaces in the Performance SLA, but it is not the best option because it is not scalable. If you have a large number of SD-WAN interfaces, this option will cause the Performance SLA to be triggered too often. References: Performance SLA | FortiGate / FortiOS 7.4.0 Configuring Performance SLA | FortiGate / FortiOS 7.4.0

QUESTION 2

Refer to the exhibits.

Exhibit A

```
vd: root/0
name: vpn-hub02-1
version: 2
interface: wan1 7
addr: 10.73.255.67:500 -> 10.73.255.82:500
tun_id: 10.73.255.82/::10.73.255.82
remote_location: 0.0.0.0
created: 82236s ago
peer-id: CN = fgtdc01.example.com
peer-id-auth: yes
assigned IPv4 address: 192.168.73.67/255.255.255.224
auto-discovery: 2 receiver
PPK: no
IKE SA: created 1/1 established 1/1 time 50/50/50 ms
IPsec SA: created 1/2 established 1/2 time 0/25/50 ms
  id/spi: 1 e4f6465bbae7490f/2535d26ef1f21557
  direction: initiator
  status: established 82236-82236s ago = 50ms
  proposal: aes256-sha256
  child: no
  PPK: no
  message-id sent/rcv: 4/1
  lifetime/rekey: 86400/3863
  DPD sent/rcv: 00000000/00000000
  peer-id: CN = fgtdc01.example.com
```

Exhibit B

```
lqr01-brancho1 # diag vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=vpn-hub02-1 ver=2 serial=1 10.73.255.67:0->10.73.255.82:0 tun_id=10.73.255.82
tun_id=:10.73.255.82 dst mtu=1500 dpd-link=on weight=1
bound_if=7 lqwy=static/1 tun=tunnel/255 mode=auto/1 encap=none/536 options{0218}=npu create_dev frag
accept_traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=4 ilast=0 olast=0 adar/2
stat: rxp=1 txp=1500326 rxh=73 txh=273040631
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=vpn-hub02-1 proto=0 sa=1 ref=27 serial=i Auto-negotiate adr
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=3844/0M replaywin=2048
seqno=b1d18 esn=0 replaywin lastseq=000000000 itn=0 qat=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=42902/43200
dec: spi=4da0c1d esp=aes key=32 6495048006e1561c4c5b9d91e5e22c454446438480484a81eebed9f9d3742ef
ah=sha256 key=32 7fb9fce764431ba10b6da80263cd0494d9f5824cc9d5bd26db2c7ffca1d572
enc: spi=f80065a7 esp=aes key=32 df2741a4d69cf6a241fe80b7722e1b13045b89457e7bf29ee171779b556c63cf
ah=sha256 key=32 9e07bf36eca21c4732cf5af4ccdfef7f1dbcb19e7elafe17fe2a77475f2dd2b0fa
dec:pkts/bytes=0/0, enc:pkts/bytes=1456559/316245764
npu_flag=03 npu_rqwy=10.73.255.82 npu_lqwy=10.73.255.67 npu_selid=0 dec_npuid=1 enc_npuid=1
```

Exhibit C

```
config vpn ipsec phase1-interface
edit "vpn-hub02-1"
    set interface "wan1"
    set net-device enable
    set mode-cfg enable
    set proposal aes256-sha256
    set add-route disable
    set auto-discovery-receiver enable
    set remote-gw 10.73.255.82
next
end
```

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 3

Refer to the exhibit showing a firewall policy configuration.

```
Policies
config firewall policy
  edit 1
    set name "Dev-To-Cloud-Assets"
    set srcintf "port2"
    set dstintf "port4"
    set srcaddr "Dev-Subnet"
    set dstaddr "Dev-Cloud-Assets"
    set action accept
    set schedule "always"
    set service "ALL"
    set fsso disable
    set groups "Dev-Users"
    set nat enable
  next
  edit 2
    set name "Internet-Access"
    set srcintf "port2"
    set dstintf "port4"
    set srcaddr "All-Internal"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set fsso disable
    set nat enable
  next
end
```

To prevent unauthorized access of their cloud assets, an administrator wants to enforce authentication on firewall policy ID 1. What change does the administrator need to make?

- A.

```
config user setting
    set auth-on-demand always
end
```
- B.

```
config user setting
    set auth-secure-http enable
    set auth-http-basic disable
end
```
- C.

```
config firewall policy
    edit 1
        set ntlm-guest disable
    next
end
```
- D.

```
config firewall policy
    edit 1
        set fssso enable
    next
end
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: C

Explanation: The firewall policy in the exhibit allows all traffic from the internal network to the cloud. To enforce authentication on this traffic, the administrator needs to add the auth- on-demand option to the policy. This option will force all

users to authenticate before they are allowed to access the cloud.

The following is the correct configuration:

```
config firewall policy
```


edit 1

```
set srcintf "internal"
```

```
set dstintf "wan1"
```

```
set srcaddr "all"
```

```
set dstaddr "all"
```

```
set service "all"
```

```
set action accept
```

```
set auth-on-demand enable
```

References:

[Configuring firewall authentication | FortiGate / FortiOS 7.4.0 - Fortinet Document Library](#)

[Firewall policy configuration | FortiGate / FortiOS 7.4.0 - Fortinet Document Library](#)

QUESTION 4

Refer to the exhibits.

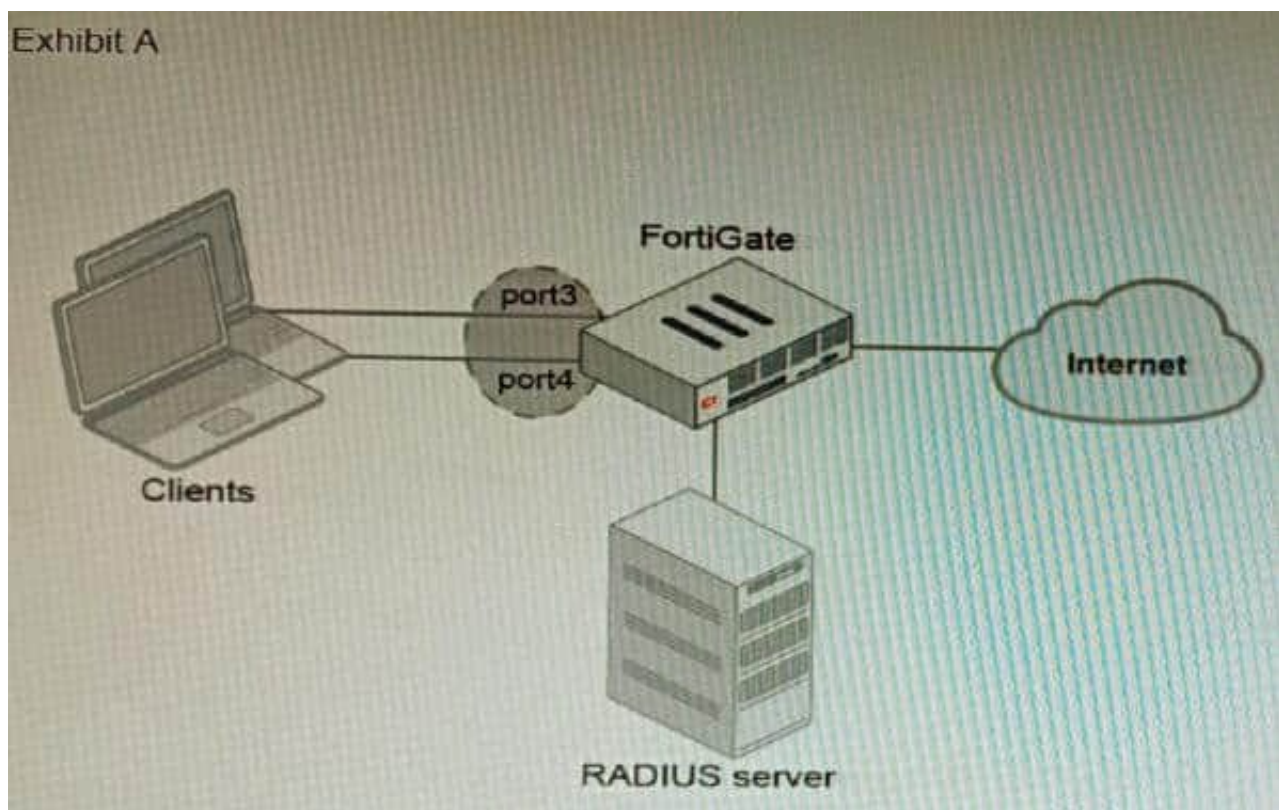


Exhibit B

```
get hardware npu np6 port-list
Chip XAUI Ports Max Cross-chip
Speed offloading
```

```
-----
np6_0 0 port1 1G Yes
0 port2 1G Yes
0 port3 1G Yes
0 port4 1G Yes
0 port5 1G Yes
0 port6 1G Yes
0 port7 1G Yes
0 port8 1G Yes
1 port9 1G Yes
1 port10 1G Yes
...
3 port28 1G Yes
3 s1 1G Yes
3 s2 1G Yes
3 vw1 1G Yes
3 vw2 1G Yes
-----
```

A customer is looking for a solution to authenticate the clients connected to a hardware switch interface of a FortiGate 400E.

Referring to the exhibits, which two conditions allow authentication to the client devices before assigning an IP address? (Choose two.)

- A. FortiGate devices with NP6 and hardware switch interfaces cannot support 802.1X authentication.
- B. Devices connected directly to ports 3 and 4 can perform 802 1X authentication.
- C. Ports 3 and 4 can be part of different switch interfaces.
- D. Client devices must have 802 1X authentication enabled

Correct Answer: BD

Explanation: The customer wants to deploy a solution to authenticate the clients connected to a hardware switch interface of a FortiGate 400E device. A hardware switch interface is an interface that combines multiple physical interfaces into one logical interface, allowing them to act as a single switch with one IP address and one set of security policies. The customer wants to use 802.1X authentication for this solution, which is a standard protocol for port-based network access control (PNAC) that authenticates clients based on their credentials before granting them access to

network resources. One condition that allows authentication to the client devices before assigning an IP address is that devices connected directly to ports 3 and 4 can perform 802.1X authentication. This is because ports 3 and 4 are part of the hardware switch interface named "lan", which has an IP address of 10.10.10.254/24 and an inbound SSL inspection profile named "sslinspection". The inbound SSL inspection profile enables the FortiGate device to intercept and inspect SSL/TLS traffic from clients before forwarding it to servers, which allows it to apply security policies and features such as antivirus, web filtering, application control, etc. However, before performing SSL inspection, the FortiGate device needs to authenticate the clients using 802.1X authentication, which requires the clients to send their credentials (such as username and password) to the FortiGate device over a secure EAP (Extensible Authentication Protocol) channel. The FortiGate device then verifies the credentials with an authentication server (such as RADIUS or LDAP) and grants or denies access to the clients based on the authentication result. Therefore, devices connected directly to ports 3 and 4 can perform 802.1X authentication before assigning an IP address. Another condition that allows authentication to the client devices before assigning an IP address is that client devices must have 802.1X authentication enabled. This is because 802.1X authentication is a mutual process that requires both the client devices and the FortiGate device to support and enable it. The client devices must have 802.1X authentication enabled in their network settings, which allows them to initiate the authentication process when they connect to the hardware switch interface of the FortiGate device. The client devices must also have an 802.1X supplicant software installed, which is a program that runs on the client devices and handles the communication with the FortiGate device using EAP messages. The client devices must also have a trusted certificate installed, which is used to verify the identity of the FortiGate device and establish a secure EAP channel. Therefore, client devices must have 802.1X authentication enabled before assigning an IP address.

References: [https:// docs.fortinet.com/document/fortigate/7.0.0/administration- guide/19662/hardware-switchinterfaces](https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/19662/hardware-switchinterfaces)[https://docs.fortinet.com/document/fortigate/7.0.0/administration- guide/19662/802-1x-authentication](https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/19662/802-1x-authentication)

QUESTION 5

A customer's cybersecurity department needs to implement security for the traffic between two VPCs in AWS, but these belong to different departments within the company. The company uses a single region for all their VPCs.

Which two actions will achieve this requirement while keeping separate management of each department's VPC? (Choose two.)

- A. Create a transit VPC with a FortiGate HA cluster, connect to the other two using VPC peering, and use routing tables to force traffic through the FortiGate cluster.
- B. Create an IAM account for the cybersecurity department to manage both existing VPC, create a FortiGate HA Cluster on each VPC and IPSEC VPN to force traffic between the VPCs through the FortiGate clusters
- C. Migrate all the instances to the same VPC and create IAM accounts for each department, then implement a new subnet for a FortiGate auto-scaling group and use routing tables to force the traffic through the FortiGate cluster.
- D. Create a VPC with a FortiGate auto-scaling group with a Transit Gateway attached to the three VPC to force routing through the FortiGate cluster

Correct Answer: AD

Explanation: To implement security for the traffic between two VPCs in AWS, while keeping separate management of each department's VPC, two possible actions are: Create a transit VPC with a FortiGate HA cluster, connect to the other two using VPC peering, and use routing tables to force traffic through the FortiGate cluster. This option allows the cybersecurity department to manage the transit VPC and apply security policies on the FortiGate cluster, while the other departments can manage their own VPCs and instances. The VPC peering connections enable direct communication between the VPCs without using public IPs or gateways. The routing tables can be configured to direct all inter-VPC traffic to the transit VPC. Create a VPC with a FortiGate auto-scaling group with a Transit Gateway attached to the three VPCs to force routing through the FortiGate cluster. This option also allows the cybersecurity department to manage the security VPC and apply security policies on the FortiGate cluster, while the other departments can manage their own VPCs and instances. The Transit Gateway acts as a network hub that connects multiple VPCs and on-premises networks. The routing tables can be configured to direct all inter-VPC traffic to the security VPC. References:

<https://docs.fortinet.com/document/fortigate-public-cloud/7.2.0/aws-administration-guide/506140/connecting-a-local-fortigate-to-an-aws-vpc-vpn> <https://docs.fortinet.com/document/fortigate-public-cloud/7.0.0/sd-wan-architecture-forenterprise/166334/sd-wan-configuration>

[Latest NSE8_812 Dumps](#)

[NSE8_812 PDF Dumps](#)

[NSE8_812 Braindumps](#)