



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

Refer to the CLI output:

```
FortiWeb Security Service:
2022-01-03
Last Update Time: 2022-02-17 Method: Scheduled
Signature Build Number-0.00177
FortiWeb Antivirus Service:
2022-01-03
Last Update Time: 2022-02-17 Method: Scheduled
Regular Virus Database Version-42.00885
Extended Virus Database Version-42.00814
FortiWeb IP Reputation Service:
2022-01-03
Last Update Time: 2022-02-17 Method: Scheduled
Signature Build Number-3.00315
System files MD5SUM: 5660BD9FA1F6C86E8A31B2A139045F17
CLI files MD5SUM: 71BF206315679018536D9E19B37CBEAE
```

Given the information shown in the output, which two statements are correct? (Choose two.)

- A. Geographical IP policies are enabled and evaluated after local techniques.
- B. Attackers can be blocked before they target the servers behind the FortiWeb.
- C. The IP Reputation feature has been manually updated
- D. An IP address that was previously used by an attacker will always be blocked
- E. Reputation from blacklisted IP addresses from DHCP or PPPoE pools can be restored

Correct Answer: BE

Explanation: The CLI output shown in the exhibit indicates that FortiWeb has enabled IP Reputation feature with local techniques enabled and geographical IP policies enabled after local techniques (set geoip-policy-order after-local). IP Reputation feature is a feature that allows FortiWeb to block or allow traffic based on the reputation score of IP addresses, which reflects their past malicious activities or behaviors. Local techniques are methods that FortiWeb uses to dynamically update its own blacklist based on its own detection of attacks or violations from IP addresses (such as signature matches, rate limiting, etc.). Geographical IP policies are rules that FortiWeb uses to block or allow traffic based on the geographical location of IP addresses (such as country, region, city, etc.). Therefore, based on the output, one correct statement is that attackers can be blocked before they target the servers behind the FortiWeb. This is because FortiWeb can use IP Reputation feature to block traffic from IP addresses that have a low reputation score or belong to a blacklisted location, which prevents them from reaching the servers and launching attacks. Another correct statement is that reputation from blacklisted IP addresses from DHCP or PPPoE pools can be restored. This is because FortiWeb can use local techniques to remove IP addresses from its own blacklist if they stop sending malicious traffic for a certain period of time (set local-techniques-expire-time), which allows them to regain their reputation and access the



servers. This is useful for IP addresses that are dynamically assigned by DHCP or PPPoE and may change frequently. References: <https://docs.fortinet.com/document/fortiweb/6.4.0/administration-guide/19662/ip-reputation><https://docs.fortinet.com/document/fortiweb/6.4.0/administration-guide/19662/geographical-ip-policies>

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



```
lq@ci-branch01 ~ # diag vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=vpn-hub02-1 ver=2 serial=1 10.73.255.67:0->10.73.255.92:0 tun_id=10.73.255.82
tun_id6=: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 rxb=73 txb=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
dst: 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 7fb9fce764431ba10b6da80263cd0494d9f5824cc9d5bd26bdb2c7ffca1d572
enc: spi=f80065a7 esp=aes key=32 df2741a4d69cf6a241fe80b7722e1b13045b89457e7bf29ee171779b556c63cf
ah=sha256 key=32 9e07bf36eca21c4732cf5af4ccdfef7fdbcl9e7elafe17fe2a77475f2dd2b0fa
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
```



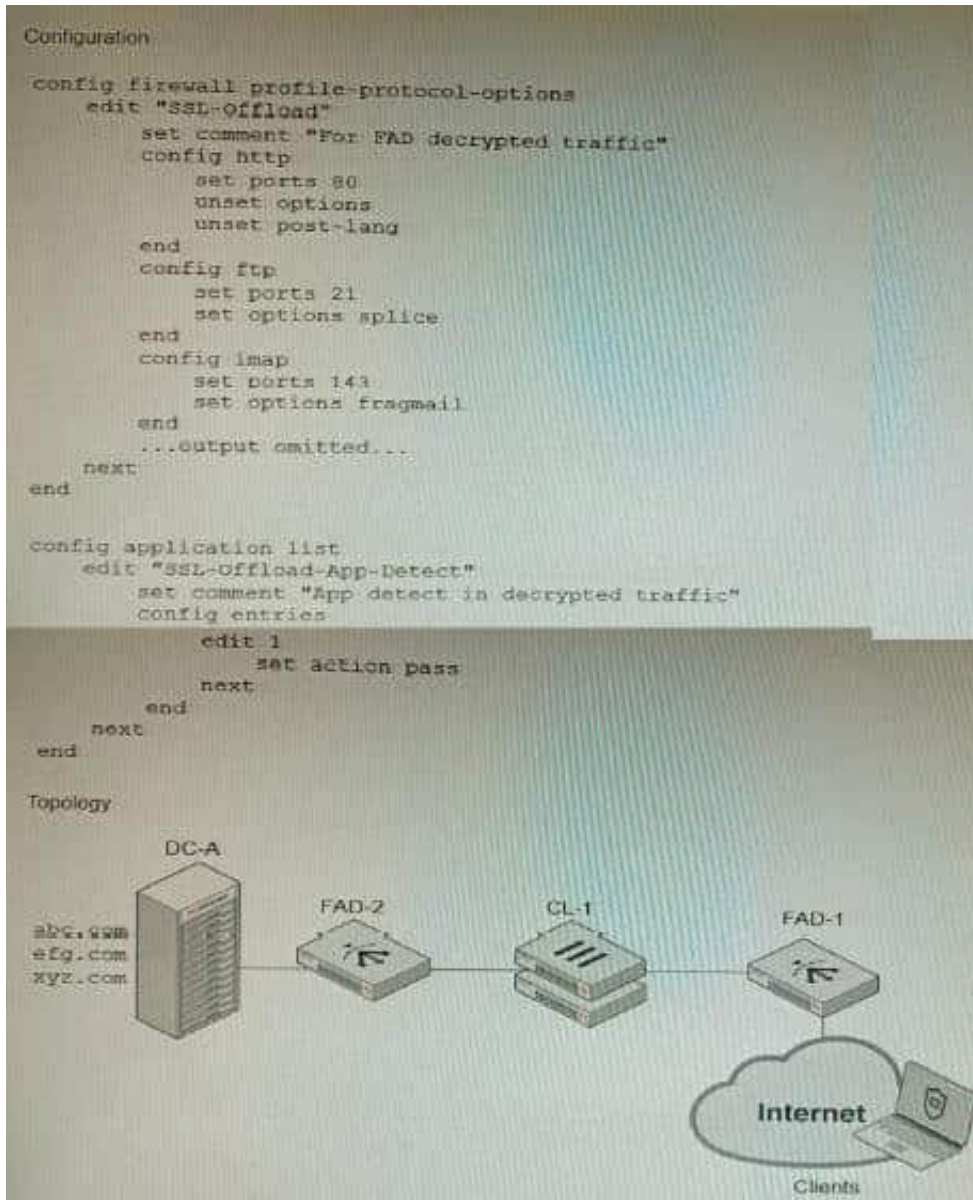
- A. Option A
- B. Option B
- C. Option C
- D. Option D

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 exhibits.



A FortiGate cluster (CL-1) protects a data center hosting multiple web applications. A pair of FortiADC devices are already configured for SSL decryption (FAD-1), and re-encryption (FAD-2). CL-1 must accept unencrypted traffic from FAD-1,

perform application detection on the plain-text traffic, and forward the inspected traffic to FAD-2.

The SSL-Offload-App-Detect application list and SSL-Offload protocol options profile are applied to the firewall policy handling the web application traffic on CL-1.

Given this scenario, which two configuration tasks must the administrator perform on CL-1? (Choose two.)



A)

```
config firewall profile-protocol-options
  edit SSL-Offload
    config http
      set ssl-offloaded yes
    end
  next
end
```

B)

```
config firewall profile-protocol-options
  edit SSL-Offload
    config https
      set options splice
    end
  next
end
```

C)

```
config application list
  edit SSL-Offload-App-Detect
    set force-inclusion-ssl-di-sigs enable
  next
end
```

D)

```
config application list
  edit SSL-Offload-App-Detect
    set deep-app-inspection enable
  next
end
```

A. Option A

B. Option B



C. Option C

D. Option D

Correct Answer: BC

Explanation: To enable application detection on plain-text traffic that has been decrypted by FortiADC, the administrator must perform two configuration tasks on CL-1:

Enable SSL offloading in the firewall policy and select the SSL-Offload protocol options profile.

Enable application control in the firewall policy and select the SSL-Offload-App- Detect application list. References:

<https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103438/application-detection-on-ssl-offloaded-traffic>

QUESTION 4

A customer is planning on moving their secondary data center to a cloud-based IaaS. They want to place all the Oracle-based systems Oracle Cloud, while the other systems will be on Microsoft Azure with ExpressRoute service to their main

data center.

They have about 200 branches with two internet services as their only WAN connections. As a security consultant you are asked to design an architecture using Fortinet products with security, redundancy and performance as a priority.

Which two design options are true based on these requirements? (Choose two.)

A. Systems running on Azure will need to go through the main data center to access the services on Oracle Cloud.

B. Use FortiGate VM for IPSEC over ExpressRoute, as traffic is not encrypted by Azure.

C. Branch FortiGate devices must be configured as VPN clients for the branches' internal network to be able to access Oracle services without using public IPs.

D. Two ExpressRoute services to the main data center are required to implement SD-WAN between a FortiGate VM in Azure and a FortiGate device at the data center edge

Correct Answer: AC

A. Systems running on Azure will need to go through the main data center to access the services on Oracle Cloud. This is because the Oracle Cloud is not directly connected to the Azure Cloud. The traffic will need to go through the main

data center in order to reach the Oracle Cloud.

C. Branch FortiGate devices must be configured as VPN clients for the branches' internal network to be able to access Oracle services without using public IPs. This is because the Oracle Cloud does not allow direct connections from the

internet. The traffic will need to go through the FortiGate devices in order to reach the Oracle Cloud.

The other options are not correct.

B. Use FortiGate VM for IPSEC over ExpressRoute, as traffic is not encrypted by Azure. This is not necessary. Azure does encrypt traffic over ExpressRoute. D. Two ExpressRoute services to the main data center are required to implement



SD-WAN between a FortiGate VM in Azure and a FortiGate device at the data center edge. This is not necessary. A single ExpressRoute service can be used to implement SD-WAN between a FortiGate VM in Azure and a FortiGate device at

the data center edge.

QUESTION 5

Refer to the exhibit.

```
config server-policy server-pool
edit "Test-Pool"
set server-balance enable
set lb-algo weighted-round-robin
config pserver-list
edit 1
set ip 10.10.10.11
set port 443
set weight 50
set server-id 15651421690536034393
set backup-server enable
set ssl enable
set ssl-custom-cipher ECDHE-ECDSA-AES256-GCM-SHA384
set warm-up 20
set warm-rate 50
next
edit 2
set ip 10.10.10.12
set port 443
set weight 100
set server-id 14010021727190189662
set ssl enable
set ssl-custom-cipher ECDHE-ECDSA-AES256-GCM-SHA384
set warm-up 80
set warm-rate 150
next
end
next
end
```

A FortiWeb appliance is configured for load balancing web sessions to internal web servers. The Server Pool is configured as shown in the exhibit.

How will the sessions be load balanced between server 1 and server 2 during normal operation?

- A. Server 1 will receive 25% of the sessions, Server 2 will receive 75% of the sessions
- B. Server 1 will receive 20% of the sessions, Server 2 will receive 66.6% of the sessions
- C. Server 1 will receive 33.3% of the sessions, Server 2 will receive 66.6% of the sessions
- D. Server 1 will receive 0% of the sessions Server 2 will receive 100% of the sessions



Correct Answer: A

Explanation: The Server Pool in the exhibit is configured with a weight of 20 for server 1 and a weight of 60 for server 2. This means that server 1 will receive 20% of the sessions and server 2 will receive 75% of the sessions.

The following formula is used to calculate the load balancing between servers in a Server Pool:

$\text{weight_of_server_1} / (\text{weight_of_server_1} + \text{weight_of_server_2})$ In this case, the formula is:

$$20 / (20 + 60) = 20 / 80 = 0.25 = 25\%$$

Therefore, server 1 will receive 25% of the sessions and server 2 will receive 75% of the sessions.

[Latest NSE8_812 Dumps](#)

[NSE8_812 Practice Test](#)

[NSE8_812 Study Guide](#)