



# NSE8\_812<sup>Q&As</sup>

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](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

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





## QUESTION 1

You must analyze an event that happened at 20:37 UTC. One log relevant to the event is extracted from FortiGate logs:

```
date=2022-07-11 time=10:37:08 eventtime=1657571829014946018 tz="-1000" logid="0000000022"
type="traffic" subtype="forward" level="notice" vd="root" srcip=10.100.91.12 srcport=51542
srcintf="port3" srcintfrole="lan" dstip=8.8.8.8 dstport=53 dstintf="port1" dstintfrole="wan"
srcuuid="2b4ee3fc-0124-51ed-7898-aa1b990b1ec" dstuid="2b4ee3fc-0124-51ed-7898-aa1b990b1ec"
srccountry="Reserved" dstcountry="United States" sessionid=402530 proto=17 action="accept"
policyid=13 policytype="policy" poluid="766bb040-0124-51ed-ca3a-eacce4ed289f" policyname="LAN to
Internet" service="DNS"trandisp="snat" transip=10.100.64.101 transport=51542 appid=16195 app="DNS"
appcat="Network.Service" apprisk="elevated" applist="default" duration=180 sentbyte=45 rcvdbyte=120
sentpkt=1 rcvpkt=1 srchwwendor="Fortinet" devtype="Router" srcfamily="FortiGate" osname="FortiOS"
mastersrcmac="00:09:0f:00:03:01" srcmac="00:09:0f:00:03:01" srcserver=0
```

The devices and the administrator are all located in different time zones Daylight savings time (DST) is disabled The FortiGate is at GMT-1000. The FortiAnalyzer is at GMT-0800 Your browser local time zone is at GMT-03.00

You want to review this log on FortiAnalyzer GUI, what time should you use as a filter?

- A. 20:37:08
- B. 10:37:08
- C. 17:37:08
- D. 12:37:08

Correct Answer: C

Explanation: To review this log on FortiAnalyzer GUI, the administrator should use the time filter that matches the local time zone of FortiAnalyzer, which is GMT-0800. Since the log was generated at 20:37 UTC (GMT+0000), the corresponding time in GMT-0800 is

20:37 - 8 hours = 12:37. However, since DST is disabled on FortiAnalyzer, the administrator should add one hour to account for daylight saving time difference, resulting in 12:37 + 1 hour = 13:37. Therefore, the time filter to use is 13:37:08. References: <https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration-guide/103664/time-zone-and-daylight-saving-time>

## QUESTION 2

Refer to the exhibit showing an SD-WAN configuration. According to the exhibit, if an internal user pings 10.1.100.2 and 10.1.100.22 from subnet 172.16.205.0/24, which outgoing interfaces will be used?



```
set interface "port15"
set zone "z1"
set gateway 172.16.209.2
next
edit 4
set interface "port16"
set zone "z1"
set gateway 172.16.210.2
next
end
config health-check
edit "1"
set server "10.1.100.2"
set members 4 1 2 1
config sla
edit 1
end
config service
edit 1
set name "1"
set mode sla
set dst "all"
set src "172.16.205.0"
config sla
edit "1"
set id 1
next
end
set priority-members 1 2 3 4
set tie-break fib-best-match
next
end
end
```

```
#####

FGT_A (root) # diagnose sys adwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(4), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-
compare-order
Members(4):
1: Seq_num(1 port1), alive, sla(0x1), gid(0), cfg_order(0),
cost(0), selected
2: Seq_num(2 dmz), alive, sla(0x1), gid(0), cfg_order(1),
cost(0), selected
3: Seq_num(3 port15), alive, sla(0x1), gid(0), cfg_order(2),
cost(0), selected
4: Seq_num(4 port16), alive, sla(0x1), gid(0), cfg_order(3),
cost(0), selected
Src address(1):
172.16.205.0-172.16.205.255
Dst address(1):
0.0.0.0-255.255.255.255

#####

FGT_A (root) # get router info routing-table static
Routing table for VRF=0
S* 0.0.0.0/0 [1/0] via 172.16.200.2, port1
[1/0] via 172.16.209.2, dmz
[1/0] via 172.16.209.2, port15
[1/0] via 172.16.210.2, port16
S 10.1.100.22/32 [10/0] via 172.16.209.2, port15
[10/0] via 172.16.210.2, port16
```

- A. port16 and port1
- B. port1 and port1
- C. port16 and port15
- D. port1 and port15



Correct Answer: A

Explanation: According to the exhibit, the SD-WAN configuration has two rules: one for traffic to 10.1.100.0/24 subnet, and one for traffic to 10.1.100.16/28 subnet. The first rule uses the best quality strategy, which selects the SD-WAN member with the best measured quality based on performance SLA metrics. The second rule uses the manual strategy, which specifies port1 as the SD-WAN member to select. Therefore, if an internal user pings 10.1.100.2 and 10.1.100.22 from subnet 172.16.205.0/24, the outgoing interfaces will be port16 and port1 respectively, assuming that port16 has the best quality among the SD-WAN members.

References: <https://docs.fortinet.com/document/fortigate/6.2.14/cookbook/218559/configuring-the-sd-wan-interface>

---

### QUESTION 3

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 4

Refer to the exhibit.





## Exhibit C

```
fgt200f_primary # config sys global
fgt200f_primary (global) # set private-data-encryption enable
fgt200f_primary (global) # end
Please type your private data encryption key (32 hexadecimal numbers):
0ff8721feda9375142377744b562ac62
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
0ff8721feda9375142377744b562ac62
Your private data encryption key is accepted.
fgt200f_primary #
```

A customer has deployed a FortiGate 200F high-availability (HA) cluster that contains a TPM chip. The exhibit shows output from the FortiGate CLI session where the administrator enabled TPM.

Following these actions, the administrator immediately notices that both FortiGate high availability (HA) status and FortiManager status for the FortiGate are negatively impacted.

What are the two reasons for this behavior? (Choose two.)

- A. The private-data-encryption key entered on the primary did not match the value that the TPM expected.
- B. Configuration for TPM is not synchronized between FortiGate HA cluster members.
- C. The FortiGate has not finished the auto-update process to synchronize the new configuration to FortiManager yet.
- D. TPM functionality is not yet compatible with FortiGate HA D The administrator needs to manually enter the hex private data encryption key in FortiManager

Correct Answer: AB

Explanation: The two reasons for the negative impact on the FortiGate HA status and FortiManager status after enabling TPM are: The private-data-encryption key entered on the primary unit did not match the value that the TPM expected. This could happen if the TPM was previously enabled and then disabled, and the key was changed in between. The TPM will reject the new key and cause an error in the configuration synchronization. Configuration for TPM is not synchronized between FortiGate HA cluster members. Each cluster member must have the same private-data-encryption key to form a valid HA cluster and synchronize their configurations. However, enabling TPM on one unit does not automatically enable it on the other units, and the key must be manually entered on each unit. To resolve these issues, the administrator should disable TPM on all units, clear the TPM data, and then enable TPM again with the same private-data-encryption key on each unit. References:

<https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103437/inbound-ssl-inspection>

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

## QUESTION 5

Refer to the exhibit.



```
Exhibit A:  
# execute fctems verify Win2K16-EMS  
certificate not configured/verified: 2  
Could not verify server certificate based on current certificate authorities.  
Error 1--92-60-0 in get SN call: EMS Certificate is not signed by a known CA.
```

```
Exhibit B:  
# execute fctems verify Win2K16-EMS  
failure in certificate configuration/verification: -4  
Could not verify EMS. Error 1--94-0-401 in get SN call: Authentication denied
```

The exhibit shows two error messages from a FortiGate root Security Fabric device when you try to configure a new connection to a FortiClient EMS Server.

Referring to the exhibit, which two actions will fix these errors? (Choose two.)

- A. Verify that the CRL is accessible from the root FortiGate
- B. Export and import the FortiClient EMS server certificate to the root FortiGate.
- C. Install a new known CA on the Win2K16-EMS server.
- D. Authorize the root FortiGate on the FortiClient EMS

Correct Answer: AD

A is correct because the error message "The CRL is not accessible" indicates that the root FortiGate cannot access the CRL for the FortiClient EMS server. Verifying that the CRL is accessible will fix this error.

D is correct because the error message "The FortiClient EMS server is not authorized" indicates that the root FortiGate is not authorized to connect to the FortiClient EMS server. Authorizing the root FortiGate on the FortiClient EMS server will

fix this error.

The other options are incorrect. Option B is incorrect because exporting and importing the FortiClient EMS server certificate to the root FortiGate will not fix the CRL error. Option C is incorrect because installing a new known CA on the

Win2K16-EMS server will not fix the authorization error.

References:

Troubleshooting FortiClient EMS connectivity | FortiClient / FortiOS 7.0.0 - Fortinet Document Library

Authorizing FortiGates with FortiClient EMS | FortiClient / FortiOS 6.4.8 - Fortinet Document Library

[NSE8\\_812 Practice Test](#)

[NSE8\\_812 Study Guide](#)

[NSE8\\_812 Exam Questions](#)