NSE7$^{Q\&As}$

Fortinet Troubleshooting Professional

Pass Fortinet NSE7 Exam with 100% Guarantee

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

https://www.pass2lead.com/nse7.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

A corporate network allows Internet Access to FSSO users only. The FSSO user student does not have Internet access after successfully logged into the Windows AD network. The output of the `diagnose debug authd fsso list\' command does not show student as an active FSSO user. Other FSSO users can access the Internet without problems. What should the administrator check? (Choose two.)

A. The user student must not be listed in the CA\\'s ignore user list.

B. The user student must belong to one or more of the monitored user groups.

C. The student workstation\\'s IP subnet must be listed in the CA\\'s trusted list.

D. At least one of the student\\'s user groups must be allowed by a FortiGate firewall policy.

Correct Answer: BD

QUESTION 2

Examine the partial output from the IKE real time debug shown in the exhibit; then answer the question below.

```
#diagnose debug application ike -1
#diagnose debug enable
ike 0: …..: 75: responder: aggressive mode get 1st message…
…
ike 0: …..:76: incoming proposal:
ike 0: …..:76: proposal id = 0:
ike 0: …..:76:    protocol id= ISAKMP:
ike 0: …..:76:       trans_id = KEY_IKE.
ike 0: …..:76:       encapsulation = IKE/none
ike 0: …..:76:          type= OAKLEY_ENCRYPT_ALG, val=AES_CBC.
ike 0: …..:76:          type= OAKLEY_HASH_ALG, val=SHA2_256.
ike 0: …..:76:          type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: …..:76:          type=OAKLEY_GROUP, val=MODP2048.
ike 0: …..:76: ISAKMP SA lifetime=86400
ike 0: …..:76: my proposal, gw Remote:
ike 0: …..:76: proposal id=1:
ike 0: …..:76:    protocol id= ISAKMP:
ikc 0: …..:76:       trans_id= KEY_IKE.
ike 0: …..:76:       encapsulation = IKE/none
ike 0: …..:76:          type=OAKLEY_ECNRYPT_ALG, val=DES_CBC.
ike 0: …..:76:          type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0: …..:76:          type=AUTH_METHOD, val= PRESHARED_KEY.
ike 0: …..:76:          type=OAKLEY_GROUP, val =MODP2048.
ike 0: …..:76: ISAKMP SA lifetime=86400
ike 0: …..:76: proposal id=1:
ike 0: …..:76:    protocol id= ISAKMP:
ike 0: …..:76:       trans_id= KEY_IKE.
ike 0: …..:76:       encapsulation = IKE/none
ike 0: …..:76:          type=OAKLEY_ENCRYPT_ALG, val=DES_CBC.
ike 0: …..:76:          type= OAKLEY_HASH_ALG, val=SHA2_256.
ike 0: …..:76:          type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: …..:76:          type=OAKLEY_GROUP, val=MODP1536.
ike 0: …..:76: ISAKMP SA lifetime=86400
ike 0: …..:76: negotiation failure
ike Negotiate ISAKMP SA Error: ike 0: …..:76: no SA proposal chosen
```

Why didn\\'t the tunnel come up?

A. IKE mode configuration is not enabled in the remote IPsec gateway.

B. The remote gateway\\'s Phase-2 configuration does not match the local gateway\\'s phase- 2 configuration.

C. The remote gateway\\'s Phase-1 configuration does not match the local gateway\\'s phase- 1 configuration.

D. One IPsec gateway is using main mode, while the other IPsec gateway is using aggressive mode.

Correct Answer: B

QUESTION 3

View the exhibit, which contains the output of diagnose sys session stat, and then answer the question

below.

```
NGFW-1 # diagnose sys session stat
misc info:      session_count=591   setup_rate=0   exp_count=0
clash=162  memory_tension_drop=0  ephemeral=0/65536
removeable=0
delete=0, flush-0, dev_down=0/0
TCP sessions:
        166 in NONE state
        1 in ESTABLISHED state
        3 in SYN_SENT state
        2 in TIME_WAIT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000006
global: ses_limit=0  ses6_limit=0  rt_limit=0  rt6_limit=0
```

![Pass2Lead](https://Pass2Lead.com)
Which statements are correct regarding the output shown? (Choose two.)

A. There are 0 ephemeral sessions.

B. All the sessions in the session table are TCP sessions.

C. No sessions have been deleted because of memory pages exhaustion.

D. There are 166 TCP sessions waiting to complete the three-way handshake.

Correct Answer: AD

QUESTION 4

View the exhibit, which contains the output of a real-time debug, and then answer the question below.

```
# diagnose debug application urlfilter -1
# diagnose debug enable

msg="received a request /tmp/.ipsengine_498_0_0.url.socket, addr_len=37:
d=www.fortinet.com:80
id=83, vfname='root', vfid=0, profile='default', type=0, client=10.0.1.10,
url_source=1, url="/"
msg="Found it in cache.   URL cat=52" IP cat=52user="N/A" src=10.0.1.10
sport=60348 dst=66.171.121.44 dport=80 service="http" hostname="
www.fortinet.com" url="/" matchType=prefix
action=10(ftgd-block) wf-act=3(BLOCK) user="N/A" src=10.0.1.10 sport=60348
dst=66.171.121.44
dport=80 service="http" cat=52 cat desc="Information Technology"
hostname="fortinet.com"
url="/"
```

Which of the following statements is true regarding this output? (Choose two.)

A. This web request was inspected using the root web filter profile.

B. FortiGate found the requested URL in its local cache.

C. The requested URL belongs to category ID 52.

D. The web request was allowed by FortiGate.

Correct Answer: BC

QUESTION 5

An administrator has configured a FortiGate device with two VDOMs: root and internal. The administrator has also created and inter-VDOM link that connects both VDOMs. The objective is to have each VDOM advertise some routes to the other VDOM via OSPF through the inter-VDOM link. What OSPF configuration settings must match in both VDOMs

to have the OSPF adjacency successfully forming? (Choose three.)

A. Router ID.

B. OSPF interface area.

C. OSPF interface cost.

D. OSPF interface MTU.

E. Interface subnet mask.

Correct Answer: BDE

QUESTION 6

When does a RADIUS server send an Access-Challenge packet?

A. The server does not have the user credentials yet.

B. The server requires more information from the user, such as the token code for two- factor authentication.

C. The user credentials are wrong.

D. The user account is not found in the server.

Correct Answer: B

QUESTION 7

Examine the output of the \\'diagnose debug rating\\' command shown in the exhibit; then answer the question below.


```
# diagnose debug rating
Locale        : english
License       : Contract
Expiration    : Wed Mar 27 17:00:00 20xx
-=- Server List (Mon Apr 16 15:32:55 20xx) -=-
IP                 Weight    RTT    Flags   TZ    Packets    Curr Lost    Total Los
69.195.205.101     10        45             -5    262432     0            846
69.195.205.102     10        46             -5    329072     0            6806
209.222.147.43     10        75             -5    71638      0            275
96.45.33.65        20        71             -8    36875      0            92
208.91.112.196     20        103    DI      -8    34784      0            1070
208.91.112.198     20        107    D       -8    35170      0            1533
80.85.69.41        60        144            0     33728      0            120
62.209.40.73       71        226            1     33797      0            192
121.111.236.180    150       197            9     33754      0            145
69.195.205.103     45        44     F       -5    26410      26226        26227
```

Which statement are true regarding the output in the exhibit? (Choose two.)

A. There are three FortiGuard servers that are not responding to the queries sent by the FortiGate.

![Pass2Lead logo](https://Pass2Lead.com)
B. The TZ value represents the delta between each FortiGuard server\\'s time zone and the FortiGate\\'s time zone.

C. FortiGate will send the FortiGuard queries to the server with highest weight.

D. A server\\'s round trip delay (RTT) is not used to calculate its weight.

Correct Answer: BC

QUESTION 8

A FortiGate\\'s portl is connected to a private network. Its port2 is connected to the Internet. Explicit web proxy is enabled in port1 and only explicit web proxy users can access the Internet. Web cache is NOT enabled. An internal web proxy user is downloading a file from the Internet via HTTP. Which statements are true regarding the two entries in the FortiGate session table related with this traffic? (Choose two.)

A. Both session have the local flag on.

B. The destination IP addresses of both sessions are IP addresses assigned to FortiGate\\'s interfaces.

C. One session has the proxy flag on, the other one does not.

D. One of the sessions has the IP address of port2 as the source IP address.

Correct Answer: AD

QUESTION 9

An administrator has configured two FortiGate devices for an HA cluster. While testing the HA failover, the administrator noticed that some of the switches in the network continue to send traffic to the former primary unit. The administrator decides to enable the setting link- failed-signal to fix the problem. Which statement is correct regarding this command?

A. Forces the former primary device to shut down all its non-heartbeat interfaces for one second while the failover occurs.

B. Sends an ARP packet to all connected devices, indicating that the HA virtual MAC address is reachable through a new master after a failover.

C. Sends a link failed signal to all connected devices.

D. Disables all the non-heartbeat interfaces in all the HA members for two seconds after a failover.

Correct Answer: A

QUESTION 10

What does the dirty flag mean in a FortiGate session?

A. Traffic has been blocked by the antivirus inspection.

B. The next packet must be re-evaluated against the firewall policies.

![Pass2Lead logo](https://Pass2Lead.com)
C. The session must be removed from the former primary unit after an HA failover.

D. Traffic has been identified as from an application that is not allowed.

Correct Answer: B

QUESTION 11

A FortiGate is rebooting unexpectedly without any apparent reason. What troubleshooting tools could an administrator use to get more information about the problem? (Choose two.)

A. Firewall monitor.

B. Policy monitor.
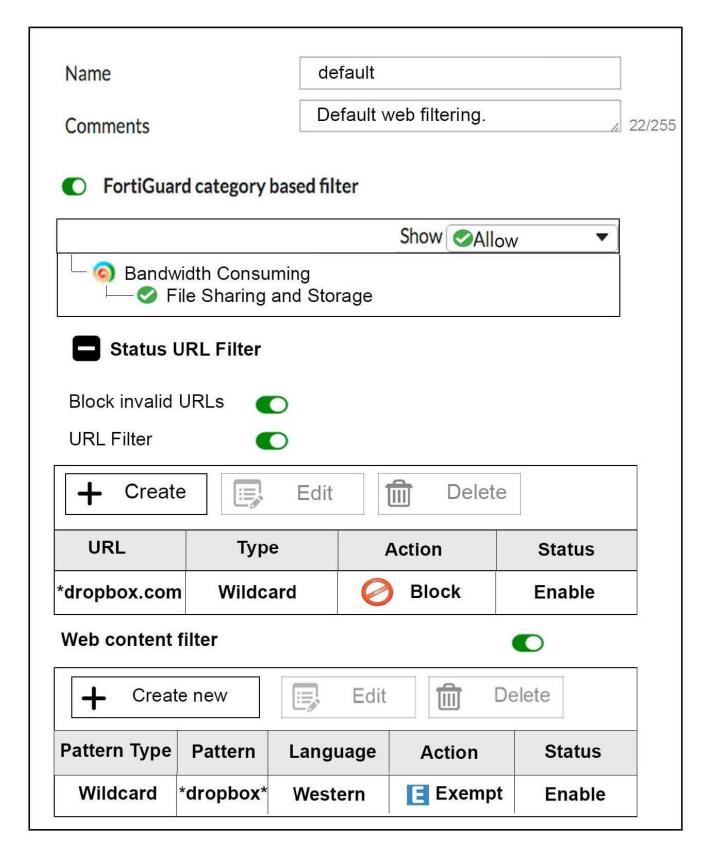
C. Logs.

D. Crashlogs.

Correct Answer: CD

QUESTION 12

View the exhibit, which contains a partial web filter profile configuration, and then answer the question

below.

Name	default
Comments	Default web filtering. 22/255

FortiGuard category based filter

Show ✅Allow ▼

- ◎ Bandwidth Consuming
  - ✅ File Sharing and Storage

Status URL Filter

Block invalid URLs ⬤

URL Filter ⬤

+ Create	Edit	🗑 Delete

URL	Type	Action	Status
*dropbox.com	Wildcard	🚫 Block	Enable

Web content filter ⬤

+ Create new	Edit	🗑 Delete

Pattern Type	Pattern	Language	Action	Status
Wildcard	*dropbox*	Western	E Exempt	Enable

Which action will FortiGate take if a user attempts to access www.dropbox.com, which is categorized as File Sharing and Storage?

A. FortiGate will exempt the connection based on the Web Content Filter configuration.

B. FortiGate will block the connection based on the URL Filter configuration.

C. FortiGate will allow the connection based on the FortiGuard category based filter configuration.

D. FortiGate will block the connection as an invalid URL.

Correct Answer: B

QUESTION 13

An administrator wants to capture ESP traffic between two FortiGates using the built-in sniffer. If the administrator knows that there is no NAT device located between both FortiGates, what command should the administrator execute?

A. diagnose sniffer packet any `udp port 500\\'

B. diagnose sniffer packet any `udp port 4500\\'

C. diagnose sniffer packet any `esp\\'

D. diagnose sniffer packet any `udp port 500 or udp port 4500\\'

Correct Answer: C

QUESTION 14

A FortiGate has two default routes: All Internet traffic is currently using port1. The exhibit shows partial information for one sample session of Internet traffic from an internal user:

```
config router static
    edit 1
        set gateway 10.200.1.254
        set priority 5
        set device "port1"
    next
    edit2
        set gateway 10.200.2.254
        set priority 10
        set device "port2"
    next
end
```

```
# diagnose sys session list
Session info: proto=6 proto_state=01 duration =17 expire=7 timeout=3600
flags= 00000000 sockflag=00000000 sockport=0 av idx=0 use=3
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty none app_ntf
statistic (bytes/packets/allow_err): org=575/7/1 reply=23367/19/1 tuples=2
origin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907-
>54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80-
>10.200.1.1:64907(10.0.1.10:64907)
pos/(before, after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000294 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

What would happen with the traffic matching the above session if the priority on the first default route (IDd1) were changed from 5 to 20?

A. Session would remain in the session table and its traffic would keep using port1 as the outgoing interface.

B. Session would remain in the session table and its traffic would start using port2 as the outgoing interface.

C. Session would be deleted, so the client would need to start a new session.

D. Session would remain in the session table and its traffic would be shared between port1 and port2.

Correct Answer: A

QUESTION 15

View the exhibit, which contains the output of a BGP debug command, and then answer the question below.

```
# get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
3 BGP AS-PATH entries
0 BGP community entries

Neighbor      V   AS     MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down    State/PfxRcd
10.125.0.60   4   65060  1698     1756     103     0    0     03:02:49            1
10.127.0.75   4   65075  2206     2250     102     0    0     02:45:55            1
10.200.3.1    4   65501  101      115      0       0    0     never         Active

Total number of neighbors 3
```

Which of the following statements about the exhibit are true? (Choose two.)

A. For the peer 10.125.0.60, the BGP state of is Established.

B. The local BGP peer has received a total of three BGP prefixes.

C. Since the BGP counters were last reset, the BGP peer 10.200.3.1 has never been down.

D. The local BGP peer has not established a TCP session to the BGP peer 10.200.3.1.

Correct Answer: BC

NSE7 PDF Dumps   NSE7 Practice Test   NSE7 Exam Questions