

Exam Questions FCSS_NST_SE-7.4

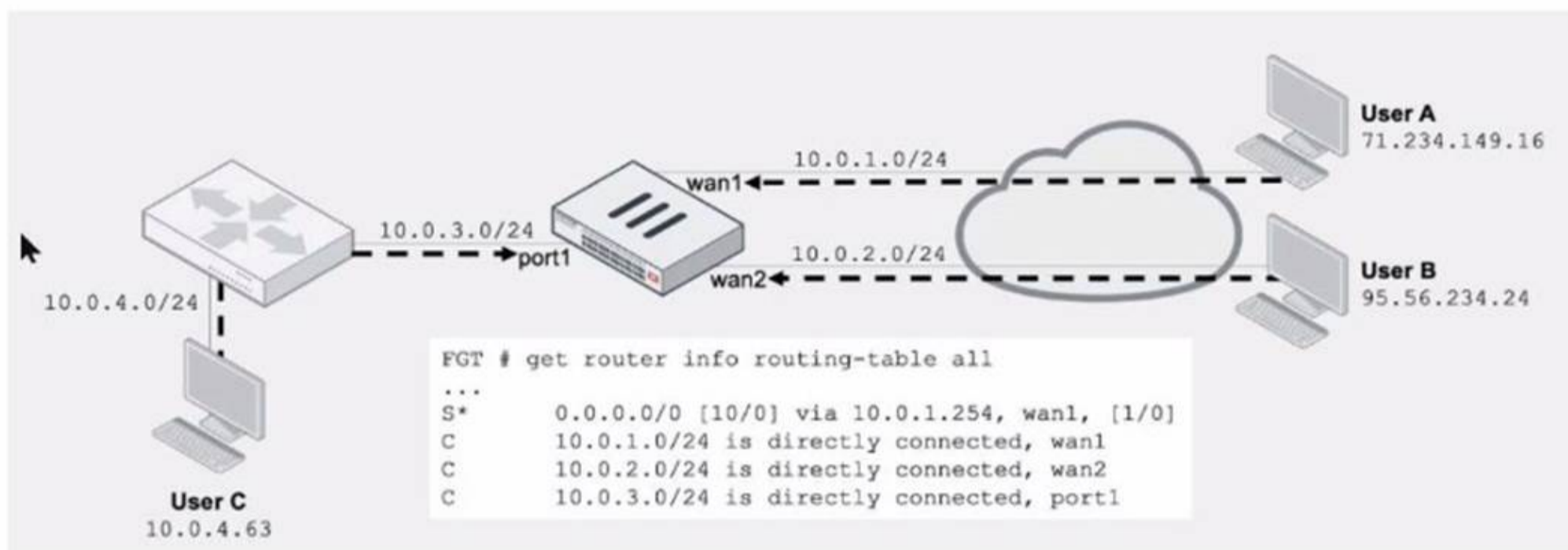
FCSS - Network Security 7.4 Support Engineer

https://www.2passeasy.com/dumps/FCSS_NST_SE-7.4/



NEW QUESTION 1

Refer to the exhibit.



Assuming a default configuration, which three statements are true? (Choose three.)

- A. Strict RPF is enabled by default.
- B. User B: Fai
- C. There is no route to 95.56.234.24 using wan2 in the routing table.
- D. User A: Pas
- E. The default static route through wan1 passes the RPF check regardless of the source IP address.
- F. User B: Pas
- G. FortiGate will use asymmetric routing using wan1 to reply to traffic for 95.56.234.24.
- H. User C: Fai
- I. There is no route to 10.0.4.63 using port1 in the routing table.

Answer: BDE

NEW QUESTION 2

Exhibit.

Name
Remote

Comments
Comments 0/255

Network

IP Version

IPv4 IPv6

Remote Gateway

Static IP Address

IP Address

10.0.10.1

Interface

port1

Local Gateway

☐

Mode Config

☐

NAT Traversal

Enable Disable Forced

Keepalive Frequency

10

Dead Peer Detection

Disable On Idle On Demand

Refer to the exhibit, which contains a screenshot of some phase 1 settings.

The VPN is not up. To diagnose the issue, the administrator enters the following CLI commands on an SSH session on FortiGate:

```
diagnose vpn ike log-filter dst-addr4 10.0.10.1
diagnose debug application ike -1
```

However, the IKE real-time debug does not show any output. Why?

- A. The administrator must also run the command `diagnose debug enable`.
- B. The debug shows only error message
- C. If there is no output, then the phase 1 and phase 2 configurations match.
- D. The log-filter setting is incorrect
- E. The VPN traffic does not match this filter.
- F. Replace `diagnose debug application ike -1` with `diagnose debug application ipsec -1`.

Answer: A

NEW QUESTION 3

An administrator wants to capture encrypted phase 2 traffic between two FortiGate devices using the built-in sniffer.

If the administrator knows that there is no NAT device located between both FortiGate devices, which command should the administrator run?

- A. `diagnose sniffer packet any 'udp port 500'`
- B. `diagnose sniffer packet any 'ip proto 50'`
- C. `diagnose sniffer packet any 'udp port 4500'`
- D. `diagnose sniffer packet any 'ah'`

Answer: B

NEW QUESTION 4

Refer to the exhibit, which shows a truncated output of a real-time LDAP debug.

```
# diagnose debug application fnbamd -l
# diagnose debug enable
fnbamd_fsm.c[1274] handle_req-Rcvd auth req 8781845 for jsmith in Lab opt=27 prot=0
fnbamd_ldap.c[637] resolve_ldap_FQDN-Resolved address 10.10.181.10, result 10.10.181.10
fnbamd_ldap.c[232] start_search_dn-base:'DC=TAC,DC=ottawa,DC=fortinet,DC=com' filter:sAMAccountName=jsmith
fnbamd_ldap.c[1351] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[1833] poll_ldap_servers-Continue pending for req 8781845
fnbamd_ldap.c[266] get_all_dn-Found DN 1:CN=John Smith,CN=Users,DC=TAC,DC=ottawa,DC=fortinet,DC=com
```

What two conclusions can you draw from the output? (Choose two.)

- A. The name of the configured LDAP server is Lab.
- B. The user is authenticating using CN=John Smith.
- C. FortiOS is able to locate the user in step 3 (Bind Request) of the LDAP authentication process.
- D. FortiOS is performing the second step (Search Request) in the LDAP authentication process.

Answer: BD

NEW QUESTION 5

Exhibit.

Edit Web Filter Profile

Bandwidth Consuming 6

Freeware and Software Downloads	Allow
File Sharing and Storage	Block
30% 93	

Allow users to override blocked categories

Static URL Filter

Block invalid URLs ☐

URL Filter ☒

+ Create New

Edit

Delete

Search

URL	Type	Action	Status
*dropbox.com	Wildcard	Allow	Enable
1			

Block malicious URLs discovered by FortiSandbox ☐

Content Filter ☒

+ Create New

Edit

Delete

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

Refer to the exhibit, which shows a partial web fillet profile configuration.

Which action does FortiGate take if a user attempts to access [www. dropbox. com](https://www.dropbox.com), which is categorized as File Sharing and Storage?

- A. FortiGate allows the connection, based on the URL Filter configuration.
B. FortiGate blocks the connection as an invalid URL.
C. FortiGate exempts the connection, based on the Web Content Filter configuration.
D. FortiGate blocks the connection, based on the FortiGuard category based filter configuration.

Answer: D

NEW QUESTION 6

Which statement about parallel path processing is correct (PPP)?

- A. PPP chooses from a group of parallel options to identify the optimal path for processing a packet.
- B. Only FortiGate hardware configurations affect the path that a packet takes.
- C. PPP does not apply to packets that are part of an already established session.
- D. Software configuration has no impact on PPP.

Answer: A

NEW QUESTION 7

Which two statements about conserve mode are true? (Choose two.)

- A. FortiGate enters conserve mode when the system memory reaches the configured extreme threshold.
- B. FortiGate starts taking the configured action for new sessions requiring content inspection when the system memory reaches the configured red threshold.
- C. FortiGate exits conserve mode when the system memory goes below the configured green threshold.
- D. FortiGate starts dropping all new sessions when the system memory reaches the configured red threshold.

Answer: BC

NEW QUESTION 8

Which statement about protocol options is true?

- A. Protocol options allow administrators to configure a maximum number of sessions for each configured protocol.
- B. Protocol options give administrators a streamlined method to instruct FortiGate to block all sessions corresponding to disabled protocols.
- C. Protocol options allow administrators to configure the Any setting for all enabled protocols, which provides the most efficient use of system resources.
- D. Protocol options allow administrators to configure which Layer 4 port numbers map to upper-layer protocols, such as HTTP, SMTP, FTP, and so on.

Answer: D

NEW QUESTION 9

Refer to the exhibit, which shows the output of get router info bgp summary.

```
get router info bgp summary

VRF 0 BGP router identifier 172.16.1.254, local AS number 65100
BGP table version is 3
2 BGP AS-PATH entries
0 BGP community entries

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ  OutQ Up/Down  State/PfxRcd
100.64.1.254   4      100     18     20       3    0    0 00:02:55        1
100.64.2.254   4      100      0      0       0    0    0 never        Active

Total number of neighbors 2
```

Which two statements are true? (Choose two.)

- A. The local FortiGate has received one prefix from BGP neighbor 100.64.1.254.
- B. The TCP connection with BGP neighbor 100.64.2.254 was successful.
- C. The local FortiGate has received 18 packets from a BGP neighbor.
- D. The local FortiGate is still calculating the prefixes received from BGP neighbor 100.64.2.264

Answer: AC

NEW QUESTION 10

Refer to the exhibit.

```
# diagnose sys top
Run Time: 0 days, 0 hours and 18 minutes
OU, ON, 1S, 95I, 0WA, 0HI, 0SI, 0ST; 16063, 12523F
      pyfcgid      248      S      2.9      3.8      9
      newcli       251      R      0.1      1.0      5
merged_daemons  185      S      0.1      0.7      6
      miglogd      177      S      0.0      6.8      0
      pyfcgid      249      S      0.0      3.0      2
      pyfcgid      246      S      0.0      2.8      5
      reportd      197      S      0.0      2.7      2
      cmdbsvr      113      S      0.0      2.4      7
```

Which three pieces of information does the diagnose sys top command provide? (Choose three.)

- A. The miglogd daemon is running on CPU core ID 0.
- B. The diagnose sys top command has been running for 18 minutes.
- C. The miglogd daemon would be on top of the list, if the administrator pressed m on the keyboard.
- D. The cmdbsvr process is occupying 2.4% of the total user memory space.
- E. If the newcli daemon continues to be in the R state, it will need to be manually restarted.

Answer: ABD

NEW QUESTION 10

Exhibit.

```
ike 0: comes 10.0.0.2:500->10.0.0.1:500,ifindex=7.
ike 0: IKEv1 exchange=Aggressive id=a2fbd6bb6394401a/06b89c022d4df682 lem=426
ike 0: Remotesite:3: initiator: aggressive mode get 1st response.
ike 0: Remotesite:3: VID DD AFCAD71368A1F1C96B8696FC77570100
ike 0: Remotesite:3: DPD negotiated FC77570100
ike 0: Remotesite:3: VID FORTIGATE 8299031757A3608
ike 0: Remotesite:3: peer is Fortigate/Fortios, (v2C6A621DE00000000
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EB0 bo)
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: Remotesite:3: received peer identifier FQDNCE88525E7DE7F00D6C2D3C0000000
ike 0: Remotesite:3: negotiation result 'remote'
ike 0: Remotesite:3: proposal id =1:
ike 0: Remotesite:3: protocol id = ISAKMP:
ike 0: Remotesite:3: trans id = KEY IKE.
ike 0: Remotesite:3: encapsulation = IKE/
ike 0: Remotesite:3: type=OAKLEY_ENCI none
ike 0: Remotesite:3: type=OAKLEY_HASH_RYPT_ALG, val=AES CBC, key-len=128
ike 0: Remotesite:3: type=AUTH METHOD, val=ALG, val=SHA.
ike 0: Remotesite:3: type=OAKLEY_GROUP, val=PRESHARED KEY.
ike 0: Remotesite:3: ISAKMP SA lifetime=86400 val=MODP1024.
ike 0: Remotesite:3: NAT-T unavailable
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06b89c022d4df682 key 16:39915120ED73E520787C801DE3678916
ike 0: Remotesite:3: PSK authentication succeeded
ike 0: Remotesite:3: authentication OK
ike 0: Remotesite:3: add INITIAL-CONTACT
ike 0: Remotesite:3: enc A2FBD6BB6394401A06B89C022D4DF6820810040100000000000000500B000018882A07809026CA8B2
ike 0: Remotesite:3: out A2FBD6BB6394401A06B89C022D4DF68208100401000000000000005C64D5CBA90B873F150CB8B5CCZA
ike 0: Remotesite:3: sent IKE msg (agg i2send): 10.0.0.1:500->10.0.0.2:500, len=140, id=a2fbd6bb6394401a/
ike 0: Remotesite:3: established IKE SA a2fbd6bb6394401a/06b89c022d4df682
```

Refer to the exhibit, which contains partial output from an IKE real-time debug. Which two statements about this debug output are correct? (Choose two.)

- A. Perfect Forward Secrecy (PFS) is enabled in the configuration.
- B. The local gateway IP address is 10.0.0.1.
- C. It shows a phase 2 negotiation.
- D. The initiator provided remote as its IPsec peer ID.

Answer: CD

NEW QUESTION 12

Refer to the exhibit, which shows partial outputs from two routing debug commands.

```
FortiGate # get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=100.64.1.254 dev=3 (port1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=10 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=100.64.2.254 dev=6 (port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.1.0.0/24 pref=10.1.0.254 gwy=0.0.0.0 dev=9 (port3)

FortiGate # get router info routing-table all

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.64.1.254, port1
          [10/0] via 100.64.2.254, port2, [10/0]
C       10.1.0.0/24 is directly connected, port3
S       10.1.10.0/24 [10/0] via 10.1.0.1, port3
C       100.64.1.0/24 is directly connected, port1
C       100.64.2.0/24 is directly connected, port2
```

Which change must an administrator make on FortiGate to route web traffic from internal users to the internet, using ECMP?

- A. Set snat-route-change to enable.
- B. Set the priority of the static default route using port2 to 1.
- C. Set preserve-session-route to enable.
- D. Set the priority of the static default route using port1 to 10.

Answer: D

NEW QUESTION 16

Refer to the exhibit, which shows the omitted output of a session table entry.

```
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=14720 confiauth_info=0 chk_client_info=0 vd=0
serial=0002932f tos=ff/ff app_list=2000 app=34050 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=1
rpd_b_link_id=80000000 ngfwid=n/a
npu_state=0x003c94 ips_offload
npu_info: flag=0x81/0x81, offload=8/8, ips_offload=1/1, epid=16/16, ipid=64/88, vlan=0x0000/0x0000
vlifid=64/88, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=0/0
```

Which two statements are true? (Choose two.)

- A. The traffic has been tagged for VLAN 0000.
- B. NP7 is handling offloading of this session.
- C. The traffic matches Policy ID 1.
- D. The session has been offloaded.

Answer: BD

NEW QUESTION 17

Refer to the exhibit, which shows the output of a policy route table entry.

```
id=2113929223 static_route=7 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-0 iif=0 dport=1-65535 path(1) oif=3(port1) gwy=192.2.0.2
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Fortinet-FortiGuard(1245324,0,0,0)
hit_count=0 last_used=2022-02-23 06:39:07
```

Which type of policy route does the output show?

- A. An ISDB route
- B. A regular policy route
- C. A regular policy route, which is associated with an active static route in the FIB
- D. An SD-WAN rule

Answer: A

NEW QUESTION 19

Refer to the exhibit, which shows a session entry.

```
session_info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty none
statistic (bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed (Bps/kbps) : 97/0 rx speed (Bps/kbps) : 97/0
orgin->sink: org pre->post, reply pre->post dev=9->3/3->9 gwy=10.200.1.254/10.1.0.1
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8 (10.200.1.1:60430)
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0 (10.1.10.10:40602)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=0002a5c9 tos=ff/ff app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
```

Which statement about this session is true?

- A. Return traffic to the initiator is sent to 10.1.0.1.
- B. Return traffic to the initiator is sent to 10.200.1.254.
- C. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
- D. It is an ICMP session from 10.1.10.1 to 10.200.5.1.

Answer: D

NEW QUESTION 23

Exhibit.

```
config system fortiguard
  set protocol udp
  set port 8888
  set load-balance-servers1
  set auto-join-forticloud enable
  set update-server-location any
  set sandbox-region ''
  set fortiguard-anycast disable
  set antispam-force-off disable
  set antispam-cache enable
  set antispam-cache-ttl 1800
  set antispam-cache-mpercent2
  set antispam-timeout 7
  set webfilter-force-off enable
  set webfilter-cache enable
  set webfilter-cache-ttl 3600
  set webfilter-timeout 15
  set sdns-server-ip "208.91.112.220"
  set sdns-server-port 53
  unset sdns-options
  set source-ip 0.0.0.0
  set source-id6 ::
  set proxv-server-ip 0.0.0.0
  set proxy-server-port 0
  set proxy-username
  set ddns-server-ip 0.0.0.0
  set dns-server-port 443
end
```

Refer to the exhibit, which shows a FortiGate configuration.

An administrator is troubleshooting a web filter issue on FortiGate. The administrator has configured a web filter profile and applied it to a policy; however the web filter is not inspecting any traffic that is passing through the policy. What must the administrator do to fix the issue?

- A. Disable webfilter-force-off.
- B. Increase webfilter-timeout.
- C. Enable fortiguard-anycast.
- D. Change protocol to TCP.

Answer: A

NEW QUESTION 27

Which two statements about Security Fabric communications are true? (Choose two.)

- A. FortiTelemetry and Neighbor Discovery both operate using TCP.
- B. The default port for Neighbor Discovery can be modified.
- C. FortiTelemetry must be manually enabled on the FortiGate interface.

D. By default, the downstream FortiGate establishes a connection with the upstream FortiGate using TCP port 8013.

Answer: CD

NEW QUESTION 32

What are two reasons you might see iprobe_in_check() check failed, drop when using the debug flow? (Choose two.)

- A. Packet was dropped because of policy route misconfiguration.
- B. Packet was dropped because of traffic shaping.
- C. Trusted host list misconfiguration.
- D. VIP or IP pool misconfiguration.

Answer: CD

NEW QUESTION 33

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCSS_NST_SE-7.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCSS_NST_SE-7.4 Product From:

https://www.2passeasy.com/dumps/FCSS_NST_SE-7.4/

Money Back Guarantee

FCSS_NST_SE-7.4 Practice Exam Features:

- * FCSS_NST_SE-7.4 Questions and Answers Updated Frequently
- * FCSS_NST_SE-7.4 Practice Questions Verified by Expert Senior Certified Staff
- * FCSS_NST_SE-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCSS_NST_SE-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year