

Fortinet

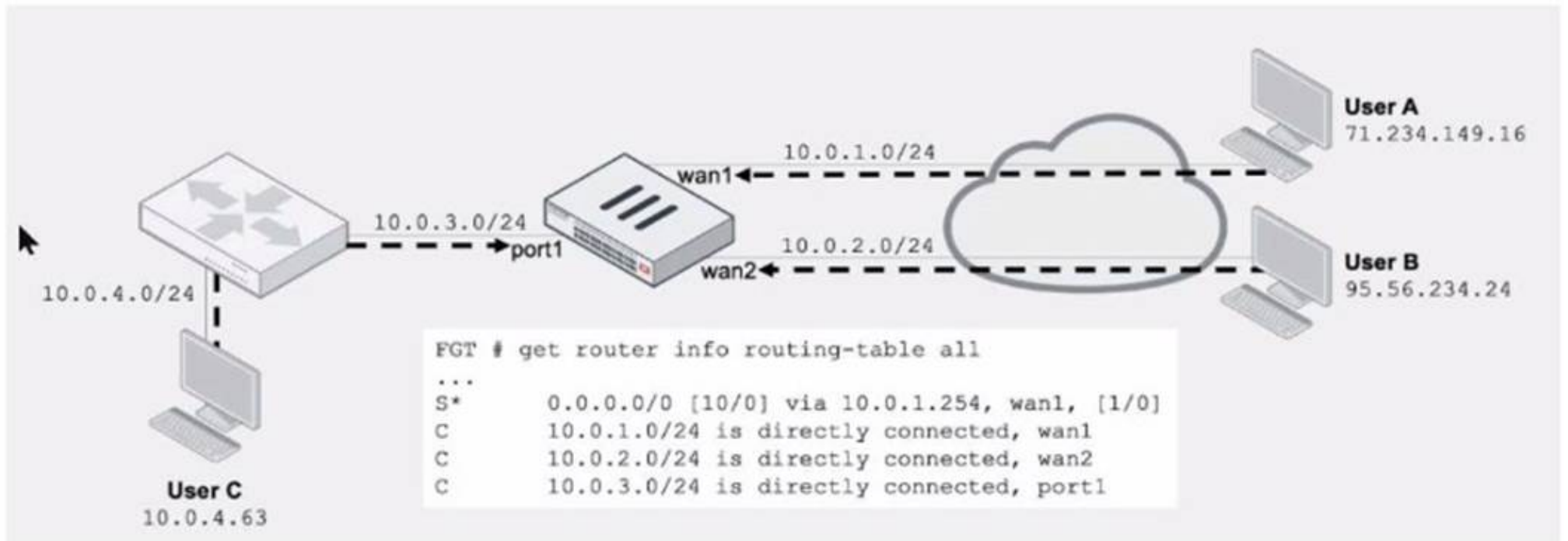
Exam Questions FCSS_NST_SE-7.4

FCSS - Network Security 7.4 Support Engineer



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

Refer to the exhibit, which shows a partial output of the fssod daemon real-time debug command.

```

# diagnose debug application fssod -1
# diagnose debug enable
[fsso_svr.c:save_result:579] event_id=4768, logon=bobby, domain=FSSO workstation=, ip=10.124.2.90 port=49215, time=1372061722
  
```

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

- A. The workstation with IP 10.124.2.90 will be polled frequently using TCP port 445 to see if the user is still logged on.
- B. The logon event can be seen on the collector agent installed on Windows.
- C. FSSO is using DC agent mode to detect logon events.
- D. FSSO is using agentless polling mode to detect logon events.

Answer: AD

NEW QUESTION 3

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 4

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

```
# diagnose debug application fnbamd -1
# 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

Refer to the exhibit, which shows the output of `getrouter info ospf neighbor`.

```
Spoke1 # get router info ospf neighbor

OSPF process 0, VRF 0:
Neighbor ID    Pri   State           Dead Time   Address      Interface
0.0.0.1        1     Full/DR         00:00:39   10.10.2.1    wan1
0.0.0.3        1     Full/DROther    00:00:37   10.10.3.2    wan2
0.0.0.10       cl    Full/-          00:00:36   172.16.1.2   ToHub
```

What can you conclude from the command output?

- A. The network type connecting the local Fortigate and OSPF neighbor 0.0.0.10 is point-to-point.
- B. All neighbors are in area 0.0.0.0.
- C. The local FortiGate is the BDR.
- D. The local FortiGate is not a DROther.

Answer: A

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

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_HASHCRYPT_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 10

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
origin->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 10

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The FCSS_NST_SE-7.4 Practice Test Here](#)