Fortinet

Exam Questions FCSS_NST_SE-7.6

FCSS - Network Security 7.6 Support Engineer

NEW QUESTION 1
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 dons-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 2
An administrator wants to capture encrypted phase 2 traffic between two FotiGate 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 'lp proto 50'
C. diagnose sniffer packet any 'udp port 4500'
D. diagnose sniffer packet any 'ah'

Answer: B

NEW QUESTION 3
Refer to the exhibit, which shows a partial output of the real-time LDAP debug.

```
# fnbamd_fsm.c[1274] handle_req-Rcvd auth req 6750221 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=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 6750221
fnbamd_ldap.c[275] get_all_dn-Found no DN
fnbamd_ldap.c[298] start_next_dn_bind-No more DN left
fnbamd_ldap.c[1603] fnbamd_ldap_get_result-Auth denied
fnbamd_auth.c[2074] fnbamd_auth_poll_ldap-Result for ldap svr 10.10.181.10 is denied
fnbamd_comm.c[116] fnbamd_comm_send_result-Sending result 1 for req 6750221
```

What two actions can the administrator take to resolve this issue? (Choose two.)

A. Ensure the user logs in using 'John Smith' not 'jsmith'.
B. Ensure the user is providing the correct user credentials.
C. Ensure the user is a member of at least one AD group to ensure step 4 of the LDAP authentication process is successful.
D. Ensure the account is active.

Answer: BD

NEW QUESTION 4
Refer to the exhibit, which shows one way communication of the downstream FortiGate with the upstream FortiGate within a Security Fabric.

```
# diagnose sniffer packet any "tcp port 8013 or udp port 8014" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[tcp port 8013 or udp port 8014]
47.220358 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
48.215338 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
50.218552 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
54.222117 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
```

What three actions must you take to ensure successful communication? (Choose three.)
A. You must authorize the downstream FortiGate on the root FortiGate.
B. FortiGate must not be in NAT mode.
C. Ensure TCP port 8013 is not blocked along the way.
D. You must enable Security Fabric/Fortitelemetry on the receiving interface of the upstream FortiGate.
E. Ensure the port for Neighbor Discovery has been changed.

A.

Answer: ACD

NEW QUESTION 5
Which exchange lakes care of DoS protection in IKEv2?

A. Create_CHILD_SA
B. IKE_Auth
C. IKE_Req_INIT
D. IKE_SA_NIT

Answer: C

Explanation:
TheIKE_SA_INITexchange in IKEv2 is responsible for DoS protection measures. During IKE_SA_INIT, before authentication and further exchange, the responder can use cookie challenges (per RFC 7296 and Fortinet VPN documentation). If a DoS attack is suspected (many requests from the same source), the responder replies with a cookie. Only after the initiator returns the correct cookie does the exchange proceed, protecting the responder from state exhaustion and certain forms of DoS traffic at the handshake stage.
FortiOS VPN Manual: IKEv2 Exchange Process and DoS Protections
IKEv2 RFC 7296: Description of IKE_SA_INIT and DoS Cookie Mechanism

NEW QUESTION 6
Refer to the exhibit, which shows the output of the command get router info bgp neighbors 100.64.2.254 advertised-routes.

```
# get router info bgp neighbors 100.64.2.254 advertised-routes

VRF 0 BGP table version is 3, local router ID is 172.16.1.254
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network              Next Hop      Metric LocPrf   Weight RouteTag Path

*> 10.20.30.40/24    100.64.2.1           xxx       0        0          100 i <-/->

Total number of prefixes 1
```

What can you conclude from the output?

A. The BGP state of the two BGP participants is OpenConfirm.
B. The router ID of the neighbor is 100.64.2.254.
C. The BGP neighbor is advertising the 10.20.30.40/24 network to the local router.
D. The local router is advertising the 10.20.30.40/24 network to its BGP neighbor.

Answer: D

NEW QUESTION 7
In IKEv2, which exchange establishes the first CHILD_SA?

A. IKE_SA_INIT

B. INFORMATIONAL
C. CREATE_CHILD_SA
D. IKE_Auth

Answer: A

Explanation:
According to RFC 7296 (IKEv2) and Fortinet's official documentation, theIKE_SA_INIT exchangeis responsible for negotiating cryptographic parameters, performing the initial Diffie-Hellman exchange, and implementing the cookie challenge mechanism for DoS protection. When the responder suspects a DoS attack (such as mass requests by the same source), it includes a cookie in the IKE_SA_INIT response. The initiator must return the cookie in its next request to prove that it truly exists at the IP address it claims, thereby mitigating resource exhaustion attacks.
This two-step exchange ensures the responder only allocates resources after successful proof of address, aligning with best security practices. Fortinet documentation confirms that this process occurs strictly in the IKE_SA_INIT phase, not in subsequent IKE_Auth or CHILD_SA exchanges.
[References:, RFC 7296: IKEv2, Section 2.6, ??Denial of Service Protection??, Fortinet FortiOS VPN Handbook: IKEv2 Exchange Process and DoS Protection Mechanism, , ,]

NEW QUESTION 8
Which two statements are true regarding heartbeat messages sent from an FSSO collector agent to FortiGate? (Choose two.)

A. The heartbeat messages can be seen using the command diagnose debug authd fsso list.
B. The heartbeat messages can be seen in the collector agent logs.
C. The heartbeat messages can be seen on FortiGate using the real-lime FSSO debug.
D. The heartbeat messages must be manually enabled on FortiGate.

Answer: BC

Explanation:
According to the official Fortinet documentation (Technical Tip: Useful FSSO Commands), heartbeat messages play a crucial role in communication between the FSSO Collector Agent and FortiGate. These messages are regularly sent from the Collector Agent to verify its status, maintain session awareness, and confirm connectivity between the authentication infrastructure and FortiGate appliances.
Option B is confirmed by Fortinet, as the collector agent logs on Windows or its management console will specifically note heartbeat events, connection status, and any issues maintaining contact with FortiGate units.
Option C is validated by both official CLI documentation and the technical tip linked. On FortiGate, heartbeat messages from the collector agent are visible using real-time debug tools such asdiagnose debug application authdor FSSO-specific commands. These enable administrators to monitor live logon states, session status, and connection health directly from the FortiGate CLI. The debug stream shows heartbeats received and their effect on active logons, associating health monitoring with active sessions.
Heartbeat operation is fully automated once FSSO is set up—there is no requirement for manual enablement or configuration, aligning with Fortinet??s philosophy of seamless integration and centralized management across the Security Fabric. This ensures that both FortiGate and the collector agent can quickly and reliably detect any miscommunication or outage, addressing authentication issues proactively.
[References:, Technical Tip: Useful FSSO Commands (Fortinet Community)?, FortiOS Administration Guide: FSSO, Collector Agent, Heartbeat, CLI Debug,]

NEW QUESTION 9
Which authentication option can you not configure under config user radius on FortiOS?

A. mschap
B. pap
C. mschap2
D. eap

Answer: D

NEW QUESTION 10
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
rpdb_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 10
Refer to the exhibit, which shows the partial output of FortiOS kernel slabs.

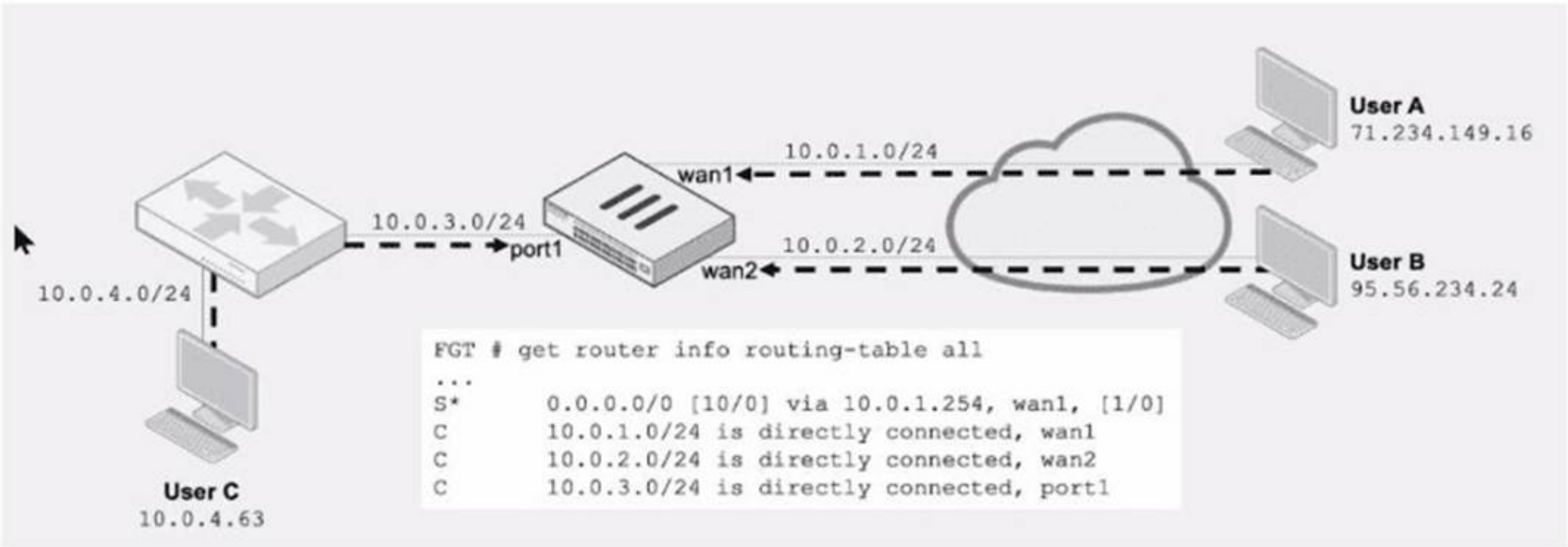
```
...
packet_de_duplication    0    0    128    30    1 : tunables  252  126    0 : slabdata    0    0    0
ip6_nat_record           0    0    128    30    1 : tunables  252  126    0 : slabdata    0    0    0
tcp6_session             0    0   1536     5    2 : tunables   60   30    0 : slabdata    0    0    0
ip6_session              0    0   1300     3    1 : tunables   60   30    0 : slabdata    0    0    0
ip_nat_record            0    0     64    59    1 : tunables  252  126    0 : slabdata    0    0    0
sctp_session             0    0   1600     5    2 : tunables   60   30    0 : slabdata    0    0    0
tcp_session              3    5   1500     5    2 : tunables   60   30    0 : slabdata    1    1    0
ip_session               1    3   1200     3    1 : tunables   60   30    0 : slabdata    1    1    0
...
```

Which statement is true?

A. The total slab size of the sctp_session slab is 0 kB and is associated with the user space.
B. The total slab size of the ip_session slab is 3600 kB and is associated with the user space.
C. The total slab size of the ip6_session slab is 1300 kB and is associated with the kernel.
D. The total slab size of the tcp_session slab is 7500 kB and is associated with the kernel.

Answer: D

NEW QUESTION 12
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 touting table.

Answer: BDE

NEW QUESTION 17
In the SAML negotiation process, which section does the Identity Provider (IdP) provide the SAML attributes utilized in the authentication process to the Service Provider (SP)?

A. SP Login dump
B. Authentication Response
C. Authentication Request
D. Assertion dump

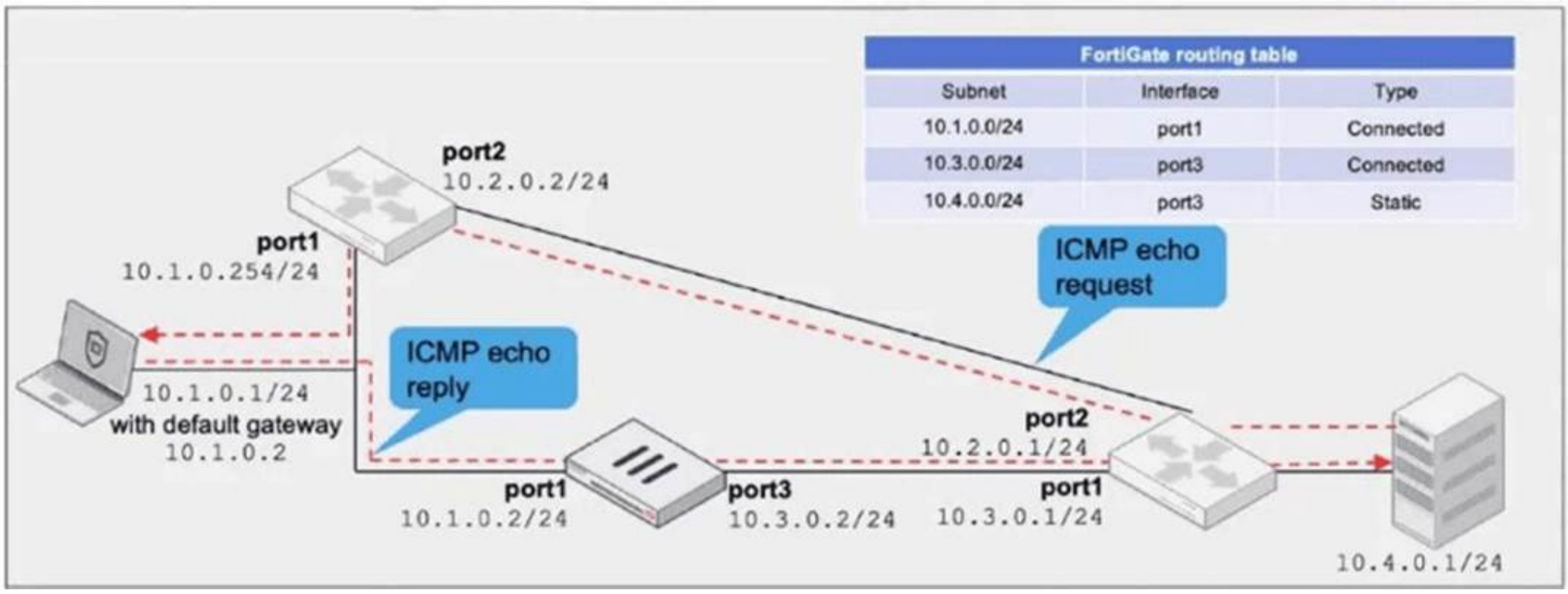
Answer: D

NEW QUESTION 21
What are two functions of automation stitches? (Choose two.)

A. You can configure automation stitches on any FortiGate device in a Security Fabric environment.
B. You can configure automation stitches to execute actions sequentially by taking parameters from previous actions as input for the current action.
C. You can set an automation stitch configured to execute actions in parallel to insert a specific delay between actions.
D. You can create automation stitches to run diagnostic commands and attach the results to an email message when CPU or memory usage exceeds specified thresholds.

Answer: BD

NEW QUESTION 26
Refer to the exhibit, which a network topology and a partial routing table.



FortiGate has already been configured with a firewall policy that allows all ICMP traffic to flow from port1 to port3.
Which changes must the administrator perform to ensure the server at 10.4.0.1/24 receives the echo reply from the laptop at 10.1.0.1/24?

A. Enable asymmetric routing under config system settings.
B. Change the configuration from strict RPF check mode to feasible RPF check mode.
C. A firewall policy that allows all ICMP traffic from port3 to port1.
D. Modify the default gateway on the laptop from 10.1.0.2 to 10.2.0.2.

Answer: A

NEW QUESTION 27
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

FCSS_NST_SE-7.6 Practice Exam Features:

* FCSS_NST_SE-7.6 Questions and Answers Updated Frequently

* FCSS_NST_SE-7.6 Practice Questions Verified by Expert Senior Certified Staff

* FCSS_NST_SE-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCSS_NST_SE-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year