

Exam : FCSS_NST_SE-7.4

**Title : FCSS - Network Security
7.4 Support Engineer**

Version : DEMO

1. Consider the scenario where the server name indication (SNI) does not match either the common name (CN) or any of the subject alternative names (SAN) in the server certificate.

Which action will FortiGate take when using the default settings for SSL certificate inspection?

- A. FortiGate uses the SNI from the user's web browser.
- B. FortiGate closes the connection because this represents an invalid SSL/TLS configuration.
- C. FortiGate uses the first entry listed in the SAN field in the server certificate.
- D. FortiGate uses the CN information from the Subject field in the server certificate.

Answer: D

2. Exhibit.

```
ike 0: comes 10.0.0.2:500->10.0.0.1:500,ifindex=7.
ike 0: IKEv1 exchange=Aggressive id=a2fbd6bb6394401a/06b89c022d4df682 len=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_HYPT_ALG, val=AES CBC, key-len=128
ike 0: Remotesite:3: type=AUTH METHOD, va ALG, val=SHA.
ike 0: Remotesite:3: type=OAKLEY_GROUP, l1=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 A2FBD6BB6394401A06B89C022D4DF68208100401000000000000005C64D5CBA90B873F150CB8B5CC2A
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: C, D

3. Exhibit.

```

FGT # diagnose debug rating
Locale      : english

Service     : Web-filter
Status      : Enable
License     : Contract

Service     : Antispam
Status      : Disable

Service     : Virus Outbreak Prevention
Status      : Disable

Num. of servers : 1
Protocol     : https
Port        : 443
Anycast     : Enable
Default servers : Included

-- Server List (Mon May 1 03:47:52 2023) --

```

IP	Weight	RTT	Flags	TZ	FortiGuard-requests	Curr	Lost	Total	Lost	Updated	Time
64.26.151.37	10	45		-5	262432	0	846	Mon May 1 03:47:43 2023			
64.26.151.35	10	46		-5	329072	0	6806	Mon May 1 03:47:43 2023			
66.117.56.37	10	75		-5	71638	0	275	Mon May 1 03:47:43 2023			
65.210.95.240	20	71		-8	36875	0	92	Mon May 1 03:47:43 2023			
209.22.147.36	20	103	DI	-8	34784	0	1070	Mon May 1 03:47:43 2023			
208.91.112.194	20	107	D	-8	35170	0	1533	Mon May 1 03:47:43 2023			
				0	33728	0	120	Mon May 1 03:47:43 2023			
				1	33797	0	192	Mon May 1 03:47:43 2023			
				9	33754	0	145	Mon May 1 03:47:43 2023			
				-5	26410	26226	26227	Mon May 1 03:47:43 2023			

Refer to the exhibit, which shows the output of a diagnose command.

What can you conclude about the debug output in this scenario?

- A. The first server provided to FortiGate when it performed a DNS query looking for a list of rating servers, was 121.111.236.179.
- B. There is a natural correlation between the value in the FortiGuard-requests field and the value in the Weight field.
- C. FortiGate used 64.26.151.37 as the initial server to validate its contract.
- D. Servers with a negative TZ value are less preferred for rating requests.

Answer: B

4.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

5.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