www.atmicnetworks.com

ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

www.atmicnetworks.com

Question: 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

Explanation:

When FortiGate performs SSL certificate inspection with default settings, it checks if the Server Name Indication (SNI) matches either the Common Name (CN) or any Subject Alternative Name (SAN) in the server certificate. If there is no match, FortiGate does not block the connection; instead, it uses the CN value from the certificate's subject field to continue web filtering and categorization.

This behavior is described in the official Fortinet 7.6.4 Administration Guide:

"Check the SNI in the hello message with the CN or SAN field in the returned server certificate: Enable: If it is mismatched, use the CN in the server certificate." This is the default (Enable) mode, which differs from the Strict mode that would block the mismatched connection.

By default, this policy ensures service continuity and prevents disruptions due to certificate mismatches, allowing FortiGate to log and inspect based on the CN even when the requested SNI does not match. It provides a balance between connection reliability and the accuracy of filtering by certificate identity, allowing security policies to remain functional without unnecessary blocks. This approach is recommended by Fortinet to maintain usability for endusers while still supporting granular inspection.

Reference:

FortiGate 7.6.4 Administration Guide: Certificate Inspection SSL/SSH Inspection Profile Configuration

Question: 2

Exhibit.

```
ike  0:  comes 10.0.0.      2:500->10.0.0.1:500,ifindex-7.
ike  0:  IKEvl exchange-Aggressive id-a2fbd6bb639440la/06b89c022d4dC682 lem-426
ike  0:  Remotesite:3:      initiator: aggressive mode get 1st response.
ike  0:  Remotesite:3:      VID DD AFCAD71368AlFlC96B8696W77Si7mnn
ike  0:  Remotesite:3:      DPD negotiated                    FC7757010O
ike  0:  Remotesite: 3:     VID FORTIGATE 8299031757A3608
ike  0:  Remotesite: 3:     peer is Fortifate/Fartios, (v2C6A621DEOOOOOOOO
ike  0:  Remotesite:3:      VID FRAGMENTATION 4048B7D56EB0 bo)
ike  0:  Remotesite:3:      VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike  0:  Remotesite:3:      received peer identifier FQDNCE88525E7DE7F00D6C2D3C0000O0O
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 _ENCr_none
ike  0:  Remotesite:3:                    tvpe=OAKLEY HASH^YPT   ALG. val=AES CBC. kev-Len=128
ike  0:  Remotesite:3:               type-AOTH METHOD. va MG. val=SHA.
ike  0:  Remotesite:3:               type=OAKLEY _GROUP, ,1=PRES.HARED KEY.
ike  0:  Remotesite:3:     ISAKMP SA lifetime-86400          val=M0DP10 24 .
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: 39915120ED73E520787C801DE36789L6
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 A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000500B000018882A07809026CA8B2
ike  0:  Remotesite:3:     out A2FBD6BB6394401AO6889C022D4DF68208100401000000000O00O0O5C64D5CSA90B873F15OCB8B5CCZA
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/06689c022d4df682
```

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

Explanation:

From the exhibit, you can observe that the debug output captures an IKEv1 negotiation in aggressive mode.

Let's break down the supporting details in line with official Fortinet IPsec VPN troubleshooting resources and debug guides:

For Option B:

The very first line of the debug output shows:

comes 10.0.0.2:500->10.0.0.1:500, ifindex=7.

This indicates the traffic direction—from the remote IP (10.0.0.2) with port 500 to the local

IP (10.0.0.1) with port 500. According to Fortinet's documentation, the right side of the arrow always represents the local FortiGate gateway. Thus, 10.0.0.1 is the local gateway IP address.

For Option D:

You see the statement:

negotiation result "remote"

and

received peer identifier FQDNCE88525E7DE7F00D6C2D3C00000000

Official debug documentation describes that the "peer identifier" or peer ID sent by the initiator is displayed here. In the context of IKE/IPsec negotiation, this value is used as the IPsec peer ID for authentication and identification purposes. The initiator is providing "remote" as the peer ID for its connection.

Why Not A or C:

Perfect Forward Secrecy (PFS): The debug does not show any DH group negotiation in phase 2 (no reference to group2, group5, etc., for phase 2), so you cannot deduce the presence of PFS solely from this output.

Phase 2 negotiation: The log focuses on IKE (phase 1) negotiation and establishment; there's no reference to ESP protocol, Quick Mode, or other identifiers that would show phase 2 SA negotiation and establishment.

This interpretation aligns with the explanation in the FortiOS 7.6.4 Administration Guide's VPN section and the official debug command output samples published in Fortinet's documentation. It demonstrates how to distinguish between local and remote addresses and how to identify the use of peer IDs.

Reference:

FortiOS 7.6.4 Administration Guide: IPsec VPN and Debugging VPNs

Technical Support Resources on interpreting IKE debug output and peer ID roles

Question: 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

ji- Server List (Mon May 1 03:47:52 2023)
Num. of servers : 1 Protocol        :       https
Port            :  443
Anycast         :  Enable
Default servers : Included
```

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	71636	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: C

Explanation:

The exhibit displays the output from the diagnose debug rating command on a FortiGate device. This command is used to display information about FortiGuard Web Filtering or other security-related queries performed by FortiGate to FortiGuard servers. Official Fortinet documentation outlines the meaning of each field in the server list. The FortiGate maintains a list of available FortiGuard servers, selecting the optimal server based on factors such as weight, round-trip time (RTT), and regional settings.

The very first entry in the server list after "Server List" is the server FortiGate initially uses, prioritized by factors such as proximity and RTT. Here, 64.26.151.37 is listed first, and the FortiGuard-requests value confirms that this server handled the highest number of requests.

The IPs, weights, and lost/failed counters are monitored for server performance and selection over time. FortiGate's default operational logic is to try the first entry for contract validation and use the next in the list if the first is unavailable or has high latency or packet loss.

There is no direct correlation between the Weight and the number of FortiGuard-requests. The servers with higher or lower weights may still handle different request volumes based on availability and performance.

The TZ (time zone) value's sign (positive or negative) does not affect server preference; it is informational, showing

the server's location relative to UTC, not a rating metric.

DNS query results for FortiGuard servers are not shown here, and the provided servers are not returned in DNS query order.

This command and interpretation are detailed in the FortiOS Administration Guide's section describing FortiGuard server selection and contract validation processes.

Reference:

FortiOS Administration Guide: FortiGuard Service Connectivity and Debugging

Official Technical Notes on diagnose debug rating output structure

Question: 4

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

```
id-2113929223 static_route-7 dscp_tag-Oxff OxfE flags-OxO tos=0x00 tosjnaak-OxOO protocol-0 sport-0-0 iif-0 dport-1-65535 path(l) oif-3(portl) gwy=192.2.0.2 source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(l): 0.0.0.0/0.0.0.0

internet serviced): Fortinet-FortiGuard (12 4 532 4, 0,0, 0)
hit counts 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

Explanation:

The exhibit for question 4 shows a policy route table entry, and key fields are as follows: internet service(1) : Fortinet-FortiGuard(1245324,0.0.0.0,0.0.0.0)

According to the Fortinet official documentation, when a policy route is based on Internet Service Database (ISDB) entries, the route entry will specifically mention "internet service," showing the service being referenced (in this example, Fortinet-FortiGuard). This is fundamentally different from a regular policy route, which is defined by source, destination,

and service wildcards without referencing an ISDB signature. A regular policy route's output would not contain the line "internet service."

Policy routes that use ISDB allow FortiGate to steer traffic for specific well-known services (like FortiGuard, Google, Microsoft) based on traffic pattern recognition, even if the destination IP is dynamic. The matching and

route selection follow the ISDB tag and can coexist with static or regular policy routes.

Thus, this entry is correctly and uniquely an ISDB route, as explained in the FortiOS policy routing documentation and ISDB configuration references.

Reference:

FortiOS Administration Guide: Policy Routing, ISDB integration and interpretation of route table entries

ISDB-based Routing and Official CLI Outputs in Fortinet's documentation

Question: 5

Exhibit.

```
config system fortiguard set protocol udp set port 8888 set load-balance-
servers 1 set auto-join-forticloud enable set update^setver-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 sdna-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 O.C.O.O set dona-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

Explanation:

The exhibit shows a FortiGate configuration under config system fortiguard related to web filtering and FortiGuard options. There is a line: set webfilter-force-off enable

According to official Fortinet documentation, the "webfilter-force-off" option, when enabled, causes the FortiGate to bypass web filtering for all traffic—even if a web filter profile is applied to a policy. This override is typically used for troubleshooting or performance reasons and is documented as an explicit bypass feature.

If an administrator wants to enforce web filtering inspection, this setting must be disabled.

The correct way to restore web filtering functionality is to run: set webfilter-force-off disable

Once done, traffic passing through policies with web filter profiles will be inspected and filtered as per configuration. Other settings such as timeout or cache TTL do not bypass web filtering; they only affect operational nuances.

Reference:
FortiOS Administration Guide: Web Filtering, FortiGuard Options, “webfilter-force-off” CLI

Question: 6

Which statement about IKEv2 is true?

A. Both IKEv1 and IKEv2 share the feature of asymmetric authentication.

B. IKEv1 and IKEv2 have enough of the header format in common that both versions can run over the same UDP port.

C. IKEv1 and IKEv2 use same TCP port but run on different UDP ports.

D. IKEv1 and IKEv2 share the concept of phase1 and phase2.

Answer: D

Explanation:

IKEv1 (Internet Key Exchange version 1) and IKEv2 are protocols used for establishing IPsec VPN tunnels, and both protocols share the conceptual division into two phases, as clearly described in Fortinet VPN documentation:

Phase 1 handles negotiation and establishment of a secure IKE Security Association (SA) between peers.

Phase 2 negotiates parameters for the IPsec Security Association, which secures actual data traffic between peers.

While IKEv2 streamlines and improves upon IKEv1 by merging some message exchanges and simplifying configuration, it maintains the same core two-phase concept: Phase 1 (IKE SA) and Phase 2 (IPsec SA). This is a foundational VPN concept referenced widely in both IKEv1 and IKEv2 literature.

Other statements are incorrect:

Asymmetric authentication is possible, but not mandatory for both.

Both protocols commonly use UDP port 500, sometimes 4500 for NAT traversal, but they are not designed to run on TCP.

The protocol feature compatibility over TCP/UDP is not correctly described in the other options.

Reference:
FortiOS Administration Guide: IPsec VPN, "IKEv1 vs. IKEv2 Concepts and Phase Negotiations"
RFCs and Fortinet VPN solution guides on phase structure

Question: 7

Exhibit 1.

```
config system global
    set anat-route-change disable end
```

```
config muter static edit 1

        set gateway HL2O0 + 1.254
        set priority 5
        set device "portl' next edit 2


        set. gateway 10.200*2-254
        set priority 10

        set device "port2"
    next
end
```

Exhibit 2.

```
FGT ♦ diagnose ays session list
session info: proto-6 proto_state-01 duration-600 expire-3179 timeout—3600 flags-00000000
sockflag-00000000 sockport- avidx-0 use-4
origin-shaper-
reply-shaper-
oer ip shaper-
:lass_id=0 ha_id=0 policy_dir=0 tunnel-/ vlan cos-0/255
state—log may_dirty npu fOO
statistic (bytes/packets/allowerr): otg—3208/25/1 reply-11144/29/1 tuples-2
tx speed (Bps/kbps): 0/0 rx speed (Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev-4->2/2->4 gwy=10.200.1.254/10.0.1.10
look-post dir-org act-snat 10.0.1.10:64907->54.239.158.170:80(10.200.1.1:64907)
icok-pre dir-reply act-dnat 54.239.158.170:80->10.200.1.1:64907(10.0.1.10:64907)
SOB/ (before, after) 0/(0,0), 0/(0,0)
Src_mac=b4:f7:al:e9:91:97
nisc=0 policy_id=l auth_info=0 chk_client_info=0 vd=0
serial—00317c56 tos-ff/ff app_list-0 app-0 url_cat-0
rpdblinkid - 00000000
id_type=0 dd_mode=0
ipustate-CxOOOcOO
ipu info: flag-OxOO/OxOO, offload-0/0, ips offload-0/0, epid-0/0, ipid-0/0, vlan-OxOOOO/OxCOOO
/lifid-O/O, vtag in-OxOOOO/OxOOOO in_npj-0/0, out_npu-0/0, fwd_en-0/0, qid-0/0
io ofId reason:
```

Refer to the exhibits, which show the configuration on FortiGate and partial internet session information from a user on the internal network.

An administrator would like to lest session failover between the two service provider connections.

Which two changes must the administrator make to force this existing session to immediately start using the other interface? (Choose two.)

A. Change the priority of the port1 static route to 11.

B. Change the priority of the port2 static route to 5.

C. Configure unset snat-route-change to return it to the default setting.

D. Configure set snat-route-change enable.

www.atmicnetworks.com

Answer: A,D

Explanation:

FortiOS Admin Guide: Static Routing, SNAT Route Change Feature

Question: 8

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

```
 FGT I get router info ospf interface port4
port4 is up, line protocol is up
   Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
   Process ID 0, VRF 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
   Transmit Delay is 1 sec. State DROther, Priority 1

   Designated Reuter (ID) 172.20.140.2, interface Address 172.20.121.2

   Backup Designated Router (ID) 0.0.0.1, Interface Address 172.20.121.239
   Timer intervals configured, Helio 10.000, Dead 40, Wait 40, Retransmit 5

     Hello due in 00:00:05
   Neighbor Count is 4, Adjacent neighbor count is 2
   Crypt Sequence Number is 411
   Hello received 106 sent 27, DD received 6 sent 3
   LS-Req received 2 sent 2, LS-Upd received 7 sent 17
   LS-Ack received 4 sent 3, Discarded 1
```

Which two statements about the output are true? (Choose two.)

A. The interlace is part of the OSPF backbone area.

B. There are a total of five OSPF routers attached to the vorz4 network segment

C. One of the neighbors has a router ID of 0.0.0.4.

D. In the network connected to port4, two OSPF routers are down.

Answer: A,B

Explanation:

Reference:

FortiOS Admin Guide: OSPF, Debug Outputs

Question: 9

Refer to the exhibit.

```
1* diagnose Sy£ top
Run Tine: 0 days, Q 0Ur  hours  and 18 minutes
OH, IS, 951, OWA,        OH I. OS I, OST; 16063,   12523F
        pyfcgid          248      5        2.9      3.0   9
```

www.atmicnetworks.com

```
          newcll    251   R   0.1   1.0   5
urgad- daenona      185   5   0.1   0.7   6
        miglogd     177   S   0.0   6.8   0
        pyfcgid     249   S   0.0   3.0   2
        pyfcgid     246   5   0.0   2.8   5
        rqportd     197   5   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 neweli daemon continues to be in the R state, it will need to be manually restarted.

Answer: A,C,D

Explanation:

https://community.fortinet.com/t5/FortiGate/Technical-Tip-Using-the-diagnose-sys-top-CLI- command/ta-p/190238

Question: 10

Refer to the exhibit, which shows the output o! the BGP database.

```
router info bgp network
0 BGP table usVersion is 3, local router IE is suppressed, d  1.1.1.1
codes:  s  S  indamped, h history, Stale                      * valid,            > best, i -internal,
codes: i
              - ISP, e – EGP, ? –     inccinp 1 ete


etwork          Next Hop          Metric       LocPrfWeight RouteTag Path
.0.0.0/0        100+64+2+254      0            100        0         0? <-/->
                100+64.2.1                              32766       0? <-/!>
.2.2.1/32       103.64.2.1                              32768       0T <-/!>
.8.0*6/32       100.64.2.254      0            100        0         0? <-/!>
0-20+30+0/24    172.16+54+115     0            100        0         0i <-/!>


1 number of     prefixes 4
```

Which two statements are correct? (Choose two.)

A. The advertised prefix of 10.20.30.0/24 was configured using the network command.

B. The first four prefixes are being advertised using a legacy route advertisement.

C. The advertised prefix of 10.20.30.0/24 is being advertised through the redistribution of another routing protocol.
D. The output shows all prefixes advertised by all neighbors as well as the local router.

Answer: A,D

Explanation:

For Option A:In Fortinet BGP (and standard BGP), when a prefix is displayed with an "i" (lowercase i) in the Path column, it represents an internal prefix that originated from the local router, typically configured via the BGP "network" command. In the exhibit, the prefix 10.20.30.0/24 is listed with a Path value of i, indicating it was injected into BGP by the local router using the network statement, not via redistribution from another routing protocol. The same logic applies to i as documented: "Origin code 'i' means the route was injected via the network command."
For Option D:The get router info bgp network output is a summary table displaying both local and received BGP routes. It lists all known routes to the BGP process, whether received from peers or originated locally. The exhibit shows all BGP prefixes known to the local router, matching the official admin guide's description of this command's output. Explanation for B and C:
The phrase "legacy route advertisement" is not formalized in BGP documentation or Fortinet's admin guide; the output uses standard BGP mechanics.
If a route was redistributed into BGP from another routing protocol, the Path field would display a "?" (question mark) for incomplete (redistributed) origin. Here the /24 route has "i" so it is NOT a redistribution.
Reference:
FortiOS Administration Guide: BGP Configuration and Route Table Interpretation Official BGP Command Reference: Show BGP Network, Path Codes, Route Origination Indicators

Question: 11

In which two slates is a given session categorized as ephemeral? (Choose two.)

A. A UDP session with only one packet received
B. A UOP session with packets sent and received
C. A TCP session waiting for the SYN ACK
D. A TCP session waiting for FIN ACK

Answer: A,C

Explanation:

Question: 12

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      IB      20        3    0    D 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 ForliGate 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: A,C

Explanation:

The get router info bgp summary output lists BGP neighbor status:

Prefix Reception: The "State/PfxRcd" column shows the number of prefixes received from the neighbor—neighbor 100.64.1.254 has "1", confirming option A.

Received Message Count: Under "MsgRcvd", 18 packets have been received from neighbor 100.64.1.254. This matches option C.

The second neighbor 100.64.2.254 is in "Active" state and has received/sent 0 packets, indicating that its TCP connection is NOT established, disproving option B.

There is no indication anywhere that the router is "still calculating" prefixes; "Active" just means no session is established, so option D is incorrect.

Reference:

FortiOS BGP Command Reference: BGP Neighbor States, PfxRcd, and Counters

Question: 13

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:

The IKE_SA_INIT exchange 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.

Reference:

FortiOS VPN Manual: IKEv2 Exchange Process and DoS Protections

IKEv2 RFC 7296: Description of IKE_SA_INIT and DoS Cookie Mechanism

Question: 14

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

```
♦ diagnose debug application fssod -1
I diagnose debug enable
[fssosvr.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: A,D

Explanation:

https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-How-to-troubleshoot- FSSO-agentless-polling/ta-p/214349

From the snippet we can see that FortiGate (via the fssod daemon) is directly detecting the user

logon rather than relying on a separate “collector” or “DC agent.” This indicates agentless polling—FortiGate polls the DC’s event logs over TCP 445 to discover logons. So: - FSSO is using agentless polling mode to detect logon events - In agentless mode, FortiGate will periodically poll the same IP (the DC) on port 445 to see if the user is still logged on

Question: 15

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

Explanation:

To capture encrypted IPsec phase 2 (ESP) traffic between two FortiGate devices, the correct protocol filter to use is ip proto 50. According to the Fortinet official sniffing and debugging documentation, ESP (Encapsulating Security Payload) is used for encrypted phase 2 payload transfer and always uses IP protocol number 50. Running the command diagnose sniffer packet any 'ip proto 50' captures only ESP packets, which represent the encrypted traffic— whether originating or transiting the device.

If there is no NAT device between FortiGates, ESP is not encapsulated in UDP (thus not on UDP port 4500; if NAT-T were required, packets would be UDP-encapsulated, but the scenario explicitly says NAT is not in use). UDP port 500 is for IKE control (negotiation) traffic, and AH (Authentication Header, ip proto 51) is not used for encryption in standard IPsec phase 2 with ESP.

This matches the official CLI reference from Fortinet for VPN and traffic analysis.

**

Reference:

FortiOS CLI Reference: diagnose sniffer packet, ESP, IP Protocol Numbers

FortiGate VPN Administration Guide: Traffic Capture and Analysis of IPsec Traffic

Question: 16

Refer to the exhibits.

```
FGT-B I get router info routing-table all
Routing table for VRF-0
S* 0.0.0.0/0 [10/0] via 192.168.1.1, portl, [1/0]
C 10.23.23,0/24 is directly connected, portl
```

```
FGT-B 4 get router        info ospf database brief

                AS  External    Link States

Link ID          ADV 0.0Router          Age Seq# 1464    CkSutn Flag  Route E2 8.8.8.8/32       Tag 0
8.8.8.8          .0.112 80000002        3106 0002
```

An administrator Is expecting to receive advertised route 8.8.8.8/32 from FGT-A. On FGT- B, they confirm that the route is being advertised and received, however, the route is not being injected into the routing table. What is the most likely cause of this issue?

A. A batter route to the 8.8.8.8/32 network exists in the routing table.

B. FGT-B is configured with a prefix list denying the 8.8.8.8/32 network to be injected into the routing table.

C. The administrator has misconfigured redistribution of routes on FGT-A.

D. FGT-8 is configured with a distribution list denying the 8.8.8.8/32 network to be injected into the routing table.

Answer: B

Explanation:

The 8.8.8.8/32 route is visible in the OSPF database on FGT-B but not installed into the routing table—the most likely explanation is that FGT-B is filtering it from being installed.

Question: 17

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

```
# get router info bgp summary

VRF 0 BGP router identifier 0.0.0.117, local AS number 65117 BGP table version is 3 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
100.64.3.1        4      65501     101     115          0    0     0 never           Active

Total number      of neighbors 3
```

What can you conclude about the router in this scenario?

A. The router 100.64.3.1 needs to update the local AS number in its BGP configuration in order to bring up the 8GP session with the local router.

B. An inbound route-map on local router is blocking the prefixes from neighbor 100.64.3.1. C. All of the neighbors displayed are part of a single BGP configuration on the local router with the neighbor-range set to a value of 4.

D. The BGP session with peer 10.127.0.75 is up.

Answer: D

Explanation:

The BGP debug output shows session information for peers, including state details. According to official Fortinet BGP documentation, if the session state with a peer does not show "Idle," "Active," or "Connect," but instead shows "Established," "Up," or related

counters (e.g., messages sent/received or uptime), it indicates the session is operational. In this scenario, the peer 10.127.0.75 is the only one showing a positive indication of a live, established session. Other options like neighbor-range configuration, AS mismatch, or routemaps blocking prefixes are not supported by evidence provided in a simple BGP session state debug, nor does the output show errors relating to local or remote AS issues.

The correct interpretation comes from Fortinet's BGP troubleshooting guide, which outlines how to read session status and neighbor states in debug and summary outputs.

Reference:

FortiOS BGP Debugging Guide: Session State Interpretation

BGP CLI Reference: Neighbor Status Fields

Question: 18

Which two statements about an auxiliary session ate true? (Choose two.)

A. With the auxiliary session selling disabled, only auxiliary sessions are offloaded.

B. With the auxiliary session setting enabled. ECMP traffic is accelerated to the NP6 processor.

C. With the auxiliary session setting enabled. Iwo sessions are created in case of routing change.

D. With the auxiliary session setting disabled, for each traffic path. FortiGate uses the same auxiliary session.

Answer: B,C

Explanation:

Auxiliary sessions in Fortinet are designed to support ECMP (Equal Cost Multi-Path) and SD-

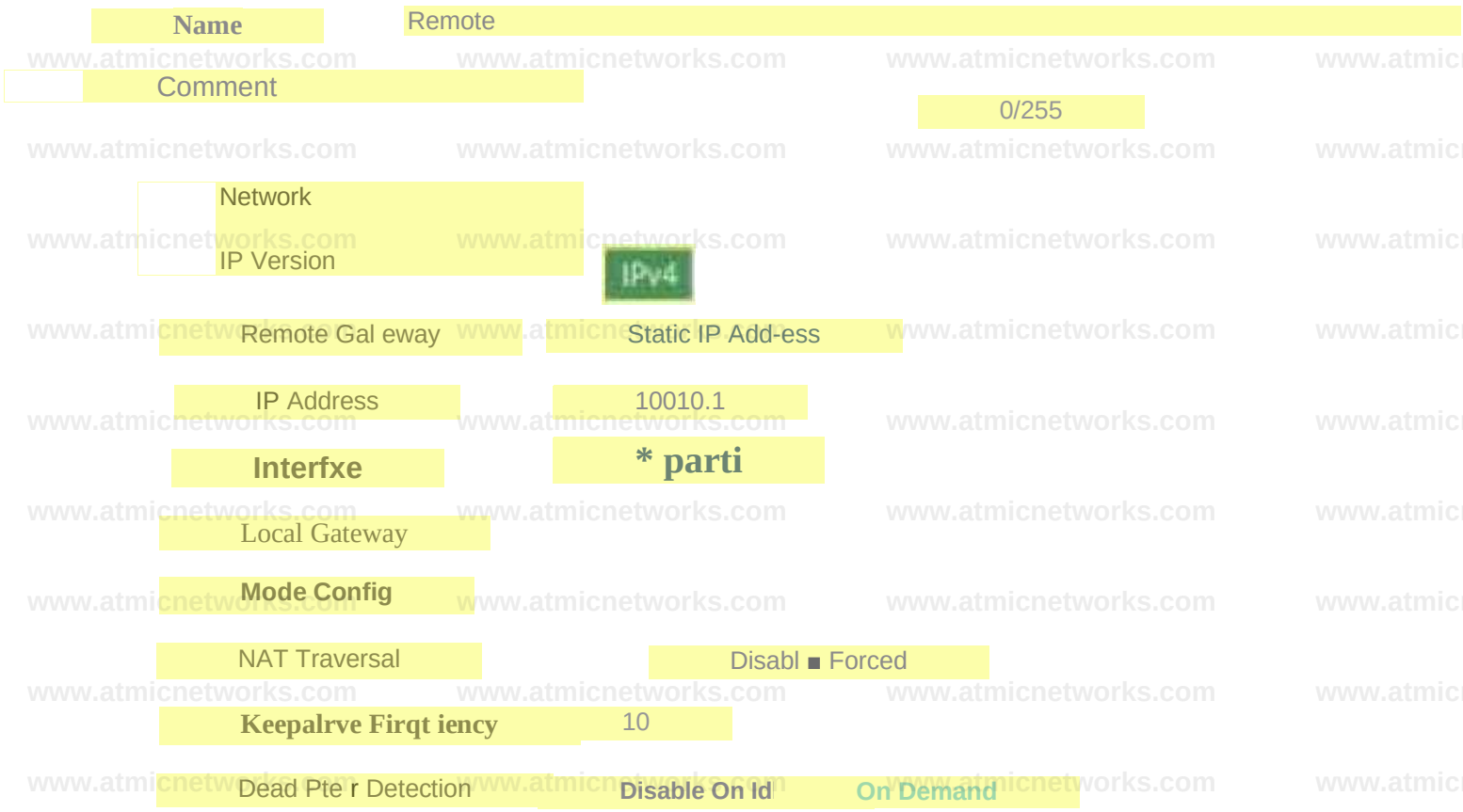
WAN scenarios, allowing sessions to be handled efficiently when traffic needs to be dynamically distributed across multiple links. With the auxiliary session setting enabled, FortiGate creates additional session table entries for each possible path in ECMP or SD- WAN—meaning that if the routing path changes (such as a link failover), a new session can be immediately activated and offloaded to the NP6 network processor for acceleration, ensuring minimal disruption. This greatly benefits high-throughput deployments.

Official documentation specifies that when auxiliary sessions are enabled, FortiGate doesn't just rely on dynamically creating new sessions after a routing event, it proactively creates sessions for all potential paths. This means that in the event of a route change, two sessions exist and the traffic is quickly re-routed and offloaded, maximizing performance and reliability. Without this feature, multiple paths cannot be efficiently offloaded, and routing changes trigger a single session update, reducing failover performance.

Reference:

Question: 19

Exhibit.



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 lag-filter dst-addr4 10.0.10,1 dlagnbie 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 messages. If there is no output, then the phase 1 and phase 2 configurations match.

C. The log-filter setting is incorrect. The VPN traffic does not match this filter.

D. Replace diagnose debug application ike -1 with diagnose debug application ipsec -1.

Answer: A

Explanation:

To display debug output on FortiGate devices, you must always run both the applicationspecific debug command and the global debug enable command. The command diagnose debug application ike -1 sets up the detail level for the IKE daemon debug, but it does not display any debug output on its own. As described in the FortiOS CLI debugging manuals, the command diagnose debug enable activates debug output on the console, making all previously set debugs visible. This is especially important for VPN troubleshooting—without the enable command, no output appears even if there is VPN traffic.

The correct diagnostic sequence is: diagnose debug application ike -1 diagnose debug enable

This procedure is found in every FortiOS CLI debug tutorial and troubleshooting workflow. Reference: FortiOS CLI Reference: Debugging VPNs and Real-time Debug Output FortiGate VPN Troubleshooting Guide: Required Steps for Debug Output

Question: 20

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: B,C

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 as diagnose debug application authd or 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.

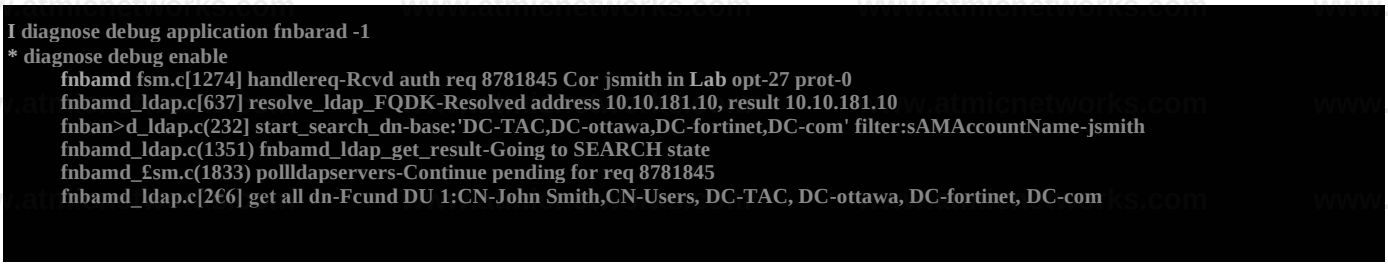
Reference:

Technical Tip: Useful FSSO Commands (Fortinet Community)

FortiOS Administration Guide: FSSO, Collector Agent, Heartbeat, CLI Debug

Question: 21

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



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: B,D

Explanation:

According to Fortinet's LDAP authentication workflow as described in the FortiOS Administration Guide and the official LDAP debug log interpretation, each authentication attempt is split into several key steps: Bind Request, Search Request, and then, if successful, a Bind as the found user DN. In the provided debug output, we see "start search_dn-base" with a filter "sAMAccountName=jsmith" and the log line "Going to SEARCH state,"

confirming that FortiOS is in the second step—the Search Request (Option D). Official documentation highlights this exact phrase "SEARCH state" as indicative of Step 2 within the LDAP process ("Bind → Search → Bind").

Additionally, the last line "Found DN 1: CN=John Smith, CN=Users, DC=TAC, DC=ottawa, DC=fortinet,

DC=com" verifies that the system has successfully mapped the username to the Distinguished Name (DN) and this user is "John Smith." The authentication will now proceed using this mapped user (Option B). Fortinet's logs record the found DN after a successful search, which is a strong confirmation that the user's credentials can be validated against the found DN.

Options A and C are not supported directly by the debug output shown:

The server name "Lab" is referenced as part of the request, but not explicitly as the LDAP server's configured name in this output.

Step 3 (Bind Request) would follow finding the DN, but the log here demonstrates the Search and DN found—per Fortinet, this precedes the actual Bind/validation step. Reference:

FortiOS Administration Guide: LDAP Authentication Process and Debug Logs Fortinet Official KB: LDAP Integration Workflow and Log Interpretation

Question: 22

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 maydirty none

statistic (bytes/packets/allowerr): org=168/2/l 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=l 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 lo 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: B

Explanation:

The session output reveals a session with proto=1 (ICMP) and the origin and reply directions show address and NAT translations. Specifically, the hook=post dir=org act=snat shows that source NAT is performed for outgoing packets, where the source 10.1.10.10:40602 is translated to 10.200.5.1:8 (likely ICMP id 8, not a TCP/UDP port). The reply direction, hook=pre dir=reply act=dnat, indicates destination NAT for incoming packets: packets incoming for 10.200.5.1:60430 are destination-NATed to 10.1.10.10:40602. The gateway (gwy) is listed as 10.200.1.254/10.1.0.1, which for outgoing traffic means that return traffic is directed to the gateway (10.200.1.254), per the NAT

policy. This is confirmed by the FortiOS Session Table Guide, which explains that the returned ICMP reply will be routed out to this NAT gateway. The session statistics and logical flow (SNAT out, matching DNAT in) reinforce that reply traffic to the initiator traverses via 10.200.1.254.
Reference:
FortiOS Administration Guide: Session Table, NAT, and Route Interaction Fortinet Technical Note: Diagnose sys session list, Direction and NAT Analysis

Question: 23

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

A. PPP chooses from a group of parallel options lo identity the optimal path tor 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

Explanation:

Parallel Path Processing (PPP) in FortiOS refers to the system's ability to evaluate and select among multiple processing paths—often involving dedicated network processors, content processors, or CPU-based workflows—to optimally process packets. The official documentation highlights that the PPP engine dynamically selects which hardware or software path to use for each session based on session characteristics, policy configuration, and traffic type. This dynamic selection results in optimal throughput and resource utilization.
The document specifies that PPP assesses several processing paths in parallel, using decision logic to determine whether a session should be offloaded to specialist hardware (like NP6,

CP9, etc.) or stay in the CPU path, ensuring that each packet is handled by the most efficient available method under current load and policy. Hardware and software configurations both influence this outcome, but it is the PPP engine's decision-making that defines the optimal path per session.
Reference:
Fortinet FortiGate Handbook: Parallel Path Processing
Fortinet FortiOS Technical Documentation: Packet Flow and Path Selection

Question: 24

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, the IKE_SA_INIT exchange is 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.

Reference:

RFC 7296: IKEv2, Section 2.6, “Denial of Service Protection”

Fortinet FortiOS VPN Handbook: IKEv2 Exchange Process and DoS Protection Mechanism

Question: 25

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

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

Answer: D

Explanation:

According to the official Fortinet administration guide for FortiOS 7.6.4 under the section "Configuring a RADIUS server," the supported RADIUS authentication methods you can configure via the CLI with config user radius are: pap chap mschap mschapv2 auto

The relevant CLI syntax is set auth-type {auto | ms_chap_v2 | ms_chap | chap | pap}. You can confirm this directly in the configuration table and from real CLI sessions.

EAP (Extensible Authentication Protocol) is NOT an authentication option you can directly set under config user radius. EAP methods (such as EAP-TLS, EAP-PEAP, EAP-TTLS) are negotiated between the RADIUS client

and server but are not configurable as an explicit auth-type option in FortiOS. EAP authentication is typically used automatically by features like 802.1X, not through the user radius object authentication-type setting, and always requires proper backend workings between supplicant and RADIUS server

Question: 26

Exhibit.

Refer to the exhibit, which shows a partial output of diagnose hardware aysinfo memory. Which two statements about the output are true? (Choose two.)

A. There are 98908 kB of memory that will never be used.
B. The user space has 708880 kB of physical memory that is not used by the system.
C. The I/O cache, which has 641364 kB of memory allocated to it.
D. The value indicated next to the inactive heading represents the currently unused cache page.

Answer: B,D

Explanation:

The partial output from diagnose hardware sysinfo memory provides details on system RAM allocation. According to Fortinet's technical documentation for memory troubleshooting and Linux memory management (which FortiOS is based on):

MemFree is the portion of physical memory not currently allocated to any running process or kernel function. Thus, 708880 kB is available and can be immediately used by user-space programs or system operations.

Inactive refers to pages in the memory cache that were previously in use for I/O or file system buffering but are now not actively referenced. These pages are retained in memory for quick access if needed again, but can be reclaimed for other memory operations if demand increases. The value 98908 kB here represents currently unused cache pages (inactive pages), ready for repurposing or deletion if the system requires more RAM. Cached represents the total amount of system memory allocated to cache, which includes both active and inactive cache pages. It does not, by itself, represent I/O cache exclusively, nor does "inactive" mean memory “will never be used” as the

kernel can re-purpose inactive pages on demand.

Reference:

Fortinet Technical Tip: Explaining the 'diagnose hard sysinfo memory' command FortiOS System Administration Guide: Linux Memory Reporting, Cached and Inactive Statistics

Question: 27

Exhibit.

```
NGFW—i I get sys ha status HA Health Status: OK Model: FortlGate-VM64 Mode: HA A-P Group: 0 Debug: 0
Cluster Uptime: 0 days 0:1:25
Cluster state change time: 2023-04-18 12:07:47
Primary selected using:
      <2023/04/18 12:07:47> FGVM01000O077649 is selected as the primary because its override priority is larger than peer member
FGVM010000077650.
ses_pickup: disable override: disable
Configuration Status:
      FGVMO1O000077649(updated 4 seconds ago): in-sync
      FGVM010000077650(updated 1 seconds ago): out-of-sync
System Usage stats:
      FGVM010000077649(updated 4 seconds ago):
            sessions-166, average-cpu-user/nice/system/idle=14/04/04/991, memory-454
      FGVM01OOOO077650(updated 1 seconds ago):
            sessions-3, average-cpu-user/nice/system/idle-04/04/01/1001, memory-441 HBDEV stats:
      FGVM010000077649(updated 4 seconds ago):
            port7: physical/lOOOauto, up, rx-bytes/packets/dropped/errors-167663/567/0/0, tx-262623/656/0/0
      FGVM010000077650(updated 1 seconds ago):
            port7: physical/lOOOauto, up, rx-bytes/packets/dropped/errors-271373/680/0/0, tx-176013/592/0/0
Primary      : NGFW-1            , FGVM010000077649, HA cluster Index - 1
Secondary    : NGFW-2            , FGVM010000077650, HA cluster index - 0
number of vcluster: 1 vcluster 1: work 169.254.0.2 Primary: FGVM010000077649, HA operating Index = 0 Secondary: FGVM010000077650, HA
operating index - 1
```

Refer to the exhibit, which shows the output of get system ha status.

NGFW-1 and NGFW-2 have been up for a week.

Which two statements about the output are true? (Choose two.)

A. If a configuration change is made to the primary FortiGate at this time, the secondary will initiate a synchronization reset.

B. If port 7 becomes disconnected on the secondary, both FortiGate devices will elect itself as primary.

C. If FGVM...649 is rebooted. FGVM...650 will become the primary and retain that role, even after FGVM...649 rejoins the cluster.

D. If no action is taken, the primary FortiGate will leave the cluster because of the current sync status.

Answer: B,C

Explanation:

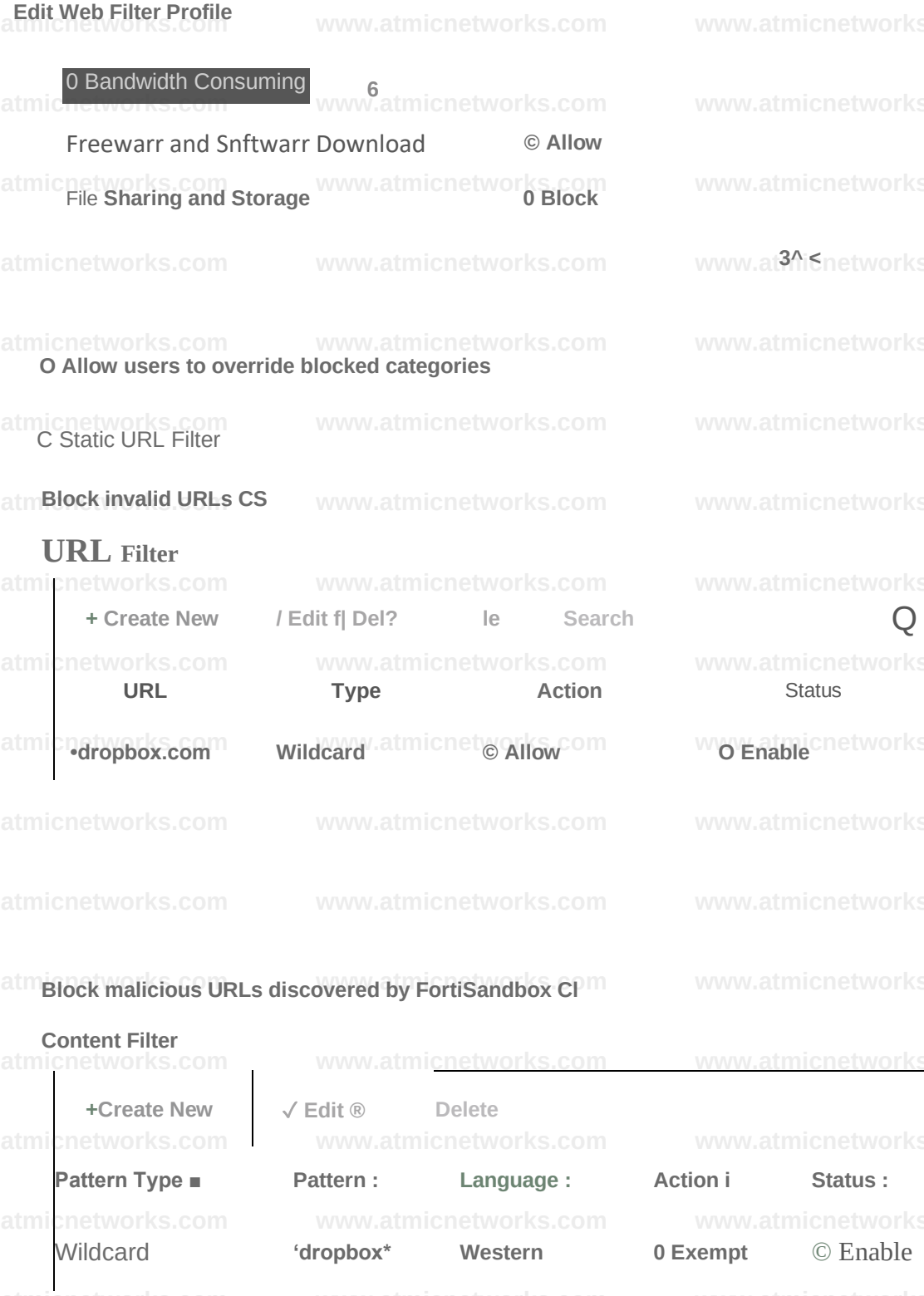
FortiGate HA Troubleshooting and Synchronization Guides

Fortinet Admin Guide: HA Primary Role Retention, Cluster Break-up Due to Out-of-Sync Status

www.atmicnetworks.com

Question: 28

Exhibit.



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

Which action does FortiGate lake if a user attempts to access 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

Explanation:

https://community.fortinet.com/t5/FortiGate/Technical-Tip-FortiGate-Static-URL-filter- actions-explained/ta-p/206632

Question: 29

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=l 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
s dwan_mbr_se q-1 s dwan_ 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-l/l, epid-16/16, ipid-64/88, vlan-OxOOOO/OxOOOO vlifid-64/88, vtag_in-
0x0000/0x0000 in_npu-l/l, out_npu-l/l, 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: C,D

Explanation:

In the provided session table output, the following details justify the answers:

Policy ID Match: The line policy_id=1 directly confirms that this session was matched by Firewall Policy ID 1. According to Fortinet's session table documentation, the policy_id field always references the policy that allowed this session, so this is a clear indicator.

Session Offloading: The presence of the strings npu_state, ips_offload, and notably the NPU info section such as offload=8/8, ips_offload=1/1 shows that this session has been offloaded to the Network Processor Unit (NPU). Fortinet technical documentation states that "offload" values greater than zero in both directions (and an NPU info section) affirm that NPU

hardware processing (fast path) is handling this traffic, thus the session is not being handled in software only.

Other options:

VLAN Tagging (vlan=0x0000/0x0000): This means no VLAN tag is assigned to this session.

NP7: The actual NPU model handling the session isn't exposed in this snippet–the offload parameters shown are generic and not specific to NP7 hardware, so it cannot be concluded from the session data.

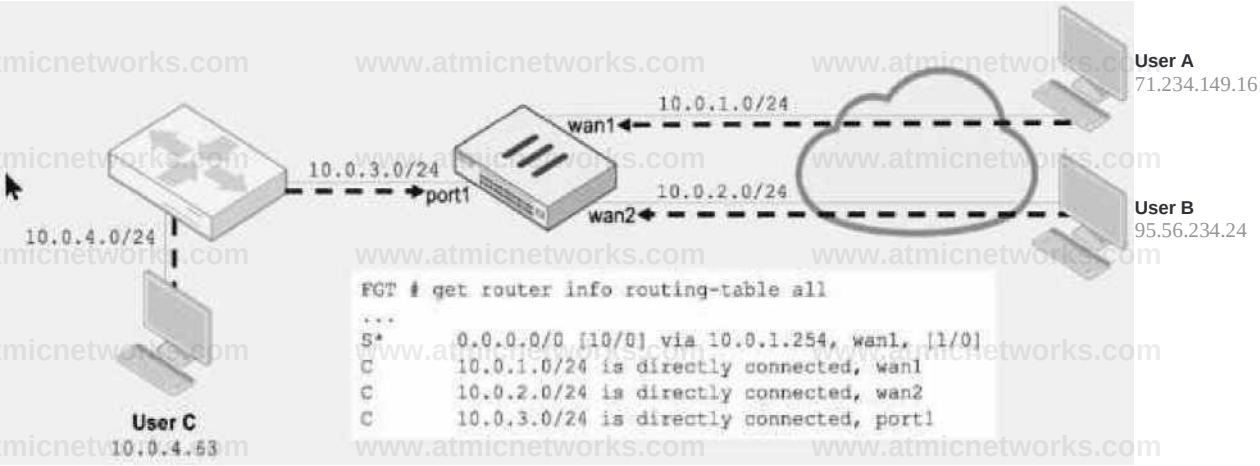
Reference:

Fortinet Technical Tip: FortiGate Session Table and NPU Offloading

FortiOS Diagnostics Guide: Policy ID, Offload, and VLAN Session Table Fields

Question: 30

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: Fail. There is no route to 95.56.234.24 using wan2 in the routing table.

C. User A: Pass. The default static route through wan1 passes the RPF check regardless of the source IP address.

D. User B: Pass. FortiGate will use asymmetric routing using wan1 to reply to traffic for 95.56.234.24.

E. User C: Fail. There is no route to 10.0.4.63 using port1 in the touting table.

Answer: B,C,E

Explanation:

Reference:

Fortinet Technical Note: RPF Default Configuration and Routing Table Matching
FortiGate Administration Guide: Routing and Asymmetric Routing Controls
Community Knowledgebase: Route Lookups and RPF Enforcement on FortiOS

Question: 31

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: C,D

Explanation:

FortiTelemetry is a critical part of Security Fabric communications and requires explicit configuration for each participating FortiGate interface. The administrative access setting "fabric" (corresponding to FortiTelemetry) must be manually enabled per interface on both upstream and downstream devices. This is performed in the GUI under Administrative Access or via the CLI using the command set allowaccess fabric for the relevant network interface. Without this step, FortiTelemetry communications will not occur on that interface. Additionally, the default communication between downstream and upstream FortiGate units in the Security Fabric is over TCP port 8013. This port is well-documented as the standard for Security Fabric and FortiTelemetry connections, and must be open and permitted across the network path for connectivity and status enforcement between units. The downstream FortiGate initiates the connection to the upstream via this port unless otherwise configured. This has also been documented as a PCI-relevant port, showing its default usage.

Other options:

Neighbor Discovery in FortiOS uses IPv6 ND protocol, not TCP.

FortiTelemetry port (8013) can be modified, but the interface Administrative Access for the Security Fabric must be manually enabled; Neighbor Discovery port modification is not documented as a supported change for FortiGate.

Reference:

FortiGate/FortiOS Administration Guide: Enabling FortiTelemetry (fabric) on interfaces
Fortinet Technical Tip: FortiTelemetry uses TCP port 8013 by default
PCI compliance documentation on port 8013 usage for Security Fabric
Fortinet Security Fabric setup procedures and interface options

Question: 32

Refer to the exhibit, which contains the output of diagnose vpn tunnel list.

```
I diagnose vpn tunnel list
name-DialUp_O ver-1 serial-4 10.200.1.1:4500->10.200.3.2:64916 tun_id-10.200.3,2 dst_nitu-1500 dpd-link-on remote_location*0.0.0.0 weight-1
bound_if=3 lgwy=static/l tun=intf/0 mode=dial_inst/3 encap=none/896 options[0380]=rgwy-chg rport-chg frag-rfc run_state=0 accepttraffic-1 overlay_id=0
parent-oiaiup index=0
proxyid num-1 child_num=0 refcnt=5 ilast=0 olast=0 ad=/0
stat: rxp-221 txp-0 rxb-35360 txb-0
dpd: mode-active on=l idle=5000ms retry-3 count-0 seqno=70
natt: mode-silent draft-32 interval-10 remote_port-64916
proxyid-DialUp proto=0 sa-1 re£-2 serial-3 add-route
    dst: 0:0.0.0.0-255.255.255.255:0
    src: 0:10.0.10.10-10.0.10.10:0
    SA: ref=3 options-82 type-00 soft-0 mtu=L422 expire-43065/OB replaywin-2048
        seqno-1 esn-0 replaywin_lastseq=00000079 itn=0 qat-0 hash_search_len-l
    life: type-01 bytes-0/0 timeout-4318 8/432 00
    dec: spi-5ed4aafc esp-aes key-16 0S4852d43abb0e931641b4e8878dd9ce
        ah=shal key=20 082eafd018bf7d4d7b65d9c5b7448db5cc01f81d
    enc: spi=69d4231e esp-aes key=16 d5a23d09ab4128d094ac972f5511f9db
        ah-shal key-20 54eac30e29ce711d2ceaab9b5el79c20bb33605e
    dec:pkts/bytes-120/10080, enc:pkts/bytes-0/0
```

Which command will capture ESP traffic for the VPN named DialUp_0?

A. diagnose sniffer packet any 'ip proto 50'
B. diagnose sniffer packet any 'host 10.0.10.10'
C. diagnose sniffer packet any 'esp and host 10.200.3.2'
D. diagnose sniffer packet any 'port 4500'

Answer: D

Explanation:

Question: 33

Exhibit.

```
♦ diagnose automation test HAFailOver autonation Last failed£1). atitch:HAFjilOver
```

Refer to the exhibit, which shows the output of diagnose automation test.

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

A. The automation stitch test is not being logged.
B. The automation stitch test failed but the HA failover was successful.
C. An HA failover occurred.
D. The test was unsuccessful.

Answer: A,D

Explanation:

www.atmicnetworks.com

Question: 34

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-Q 0.0.0.0/0.0.0.0/O->D.O.0.0/0 pref-0.0.0.0 qwy-100.64.1.254 dev=3 (portll tab-254 vf-0 scope-0 type-1 proto-
11 prio-10 0.0.0.0/0 .Q.O.Q/QOO.0.0.0/0 pref-0.0.0.0 gwy-100.64.2.254 dev-f (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 4 get router info routing-table all

Routing table for VRF-0

S'          0.0.0.0/0 [10/01 via 100.64.1.254, portl
                      [10/0] via 100.64.2.254, port2, [10/0]
C           10.1.0.0/24 is directly connected, porta

S           10.1.10.0/24 [10/0] via 10.1.0.1, pcrt3
C           100.64.1.0/24 is directly connected, portl
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

Explanation:

Question: 35

What are two reasons you might see iprope_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: C,D

Explanation:

Question: 36

Exhibit.

```
session info: proto-6 proto_state-01 duration-157 expire-3559 timeout-3600 flags-00000000 socktype-0 sockport-0 av_ldx-0 use-3 origin-shaper- reply-shaper- peripshaper-
class_id-0 ha_id-0 policy dir*0 tunnel-/ vlan_cos-0/255 user-Userl state-log maydirty authed fOO acct-ext statistic(bytes/packets/allowerr): org-2137/14/1 reply-1663/12/1 tuples-2 tx speed(Bps/kbps):
1/0 rx speed(Bps/kbps): 1/0
orgin->sink: org pre->post, reply pre->post dev-5->3/3->5 gwy-10.1.0.254/10.1.10.1 hook-pre dir-org act-noop 10.1.10.l:34830->35.241.9.150:443(0.0.0.0:0) hook-post dir-reply act-noop
35.241.9.150:443->10.1.10.1:34830(0.0.0.0:0) pos/(before,after) 0/(0,0), 0/(0,0) misc-0 policyid-l poluuididx-14735 auth_info-2 chk_client_info-0 vd-0 serial-0000352e tos-ff/ff app_list-0 app-0
url_cat-0 rpdb_link_id-00000000 ngfwid-n/anpu_state-0x000100 no_ofld_reason: npu-flag-off
```

Refer to the exhibit, which shows the output of a session. Which two statements are true? (Choose Iwo.)

A. The TCP session has been successfully established.

B. The session was initiated from an authenticated user.

C. The session is being inspected using flow inspection.

D. The session is being offloaded.

Answer: A,B

Explanation:

Question: 37

Refer to the exhibit, which shows the output of get router info ospf neighbor.

```
Spokel ♦  get. router info ospf neighbor

OSPF process  0t VHF  0:
Neighbor  ID      Pri    State            Dead Tima    Address       Interface
0.0.0.1             1    Full/DR          00:00:39     10.10.2.1     wanl
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

Explanation:

Question: 38

Exhibit.

^. name_ip_match: failed to connect to workstation: Workstation Name> (192.168.1.1) ... failed to connect to registry: WORK STATION02 (192.168.12.232)

Refer to the exhibit, which shows two entries that were generated in the FSSO collector agent logs.

What three conclusions can you draw from these log entries? {Choose three.)

A. Remote registry is not running on the workstation.

B. The user's status shows as "not verified" in the collector agent.

C. DNS resolution is unable to resolve the workstation name.

D. The FortiGate firmware version is not compatible with that of the collector agent.

E. A firewall is blocking traffic to port 139 and 445.

Answer: A,B,E

Explanation:

Question: 39

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

Explanation:

Question: 40

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: B,C

Explanation:

Question: 41

Refer to the exhibit, which contains partial output from an IKE real-time debug.

Debug output

```
ike  0:624000:90:     responder: main mode get 1st message...
ike  0:624000:90:     VID DPD AFCAD71368A1F1C96B8696FC77570100
ike  0:624000:90:     VID FRAGMENTATION 4O40B7D56EBCE80525E7DE7FOOD6C2D3
ike  0:624000:90:     VID FRAGMENTATION 4046B7D56EBCE80525E7DE7F00D6C2D3C0000000
1 ke 0:624000:90:
ike  0:624000:90:
ike  0:624000:90:
ike  0:624000:90:     VID FORTIGATE 0299031757A36082C6A62WE00C00000 incoming
ike  0:624000:98:     proposal: proposal id = 0:
ike  0:624000:90:          protocol id • ISAKMP: trans id - KEY IKE. encapsulation -
ike  0:624000:90:          IKE/none type-OAKLEY ENCRYPT ALG, val-AES CBC,          key-len—256
ike  0:624000:90:
ike  0:624000:98:
ike  0:624000:98:                    type OAKLEY HASH ALG, val=SHA2_256. type
ike  0:624000:90:                    AUTH_METHOD, val PRESHARED KEY.
ike  0:624000:90:                    type=OAKLEY_GROUP, val~MODP2048.
ike  0:624000:90:     ISAKMP SA lifetime-86400
ike  0:624000:98:     proposal id — 0:
ike  0:624000:98:          protocol id - ISAKMP: trans id - KEY IKE. encapsulation -
ike  0:624000:98:          IKE/none type OAKLEY ENCRYPT ALG, val-AES CBC,          key-len-256
ike  0:624000:98:
ike  0:624000:98;
ike  0:624000:98:                    type-CAKLEY HASH ALG, va1-SHA2 256. type-
ike  0:624000:90;                    AUTH METHOD, val-PRESHARED KEY,
ike  0:624000:98:                    type=OAKLEY GROUP, val-MODP1536.
ike  0:624000:98:     ISAKMP SA lifetime-86400
ike  0:624000:98:     my proposal, gw Remotesite:
ike  0:624000:98:     proposal id - 1:
ike  0:624000:90:          protocol id - ISAKMP: trans id - KEYIKE. encapsulation -
ike  0:620000:90:          IKE/none type-OAKLEY ENCRYPT ALG, val-AES CBC,          key-len-120
ike  0:624000:98:                    type-OAKLEY HASHALG, val-SHA.
ike  0:624000:98:                    type-AUTH METHOD, val-PRESHARED KEY.
ike  0:624000:98:                    type-OAKLEY GROUP, val-MODP2048.
ike  0:624000:98:     ISAKMP SA lifetime-86400
ike  0:624000:90:     proposal id - 1:
ike  0:624000:90:          protocol id - ISAKMP:
ike  0:624000:90:               transid - KEYIKE.
ike  0:624000:98:               encapsulation - IKE/none
ike  0:624000:98:                    type-OAKLEY ENCRYPT ALG, val-AES CBC,     key-len-128
ike  0:624000:90:                  type-OAKLEY HASH ALG, val-SHA.
ike  0:624000:98:                  type-AUTH METHOD, val-PRESHARED KEY.
ike  0:624000:98:                  type-OAKLEY_GROUP, val-MODPl536.
ike  0:624000:90: ISAKMP SA lifetime-06400 '
ike  0:624000:90: negotiation failure
ike  Negot:: 624ea7blbba276fb/0000000000000000:98: no SA proposal chosen
```

The administrator does not have access to the remote gateway.

Based on the debug output, which configuration change the administrator make to the local gateway to resolve the phase 1 negotiation error?

A. In the phase 1 proposal configuration, add AES256-SHA256 to the list of encryption algorithms.

B. In the phase 1 proposal configuration, add AESCBC-SHA2 to the list of encryption algorithms.

C. In the phase 1 network configuration, set the IKE version to 2.

D. In the phase 1 proposal configuration, add AES128-SHA128 to the list of encryption algorithms.

Answer: A

Explanation:

Question: 42

Which three common FortiGate-to-collector-agent connectivity issues can you identify using the FSSO real-time debug? (Choose three.)

A. Log is full on the collector agent.
B. Inability to reach IP address of the collector agent.
C. Refused connection. Potential mismatch of TCP port.
D. Mismatched pre-shared password.
E. Incompatible collector agent software version.

Answer: B,C,D

Explanation:

Question: 43

Refer to the exhibit, which shows a partial output from the get router info routing-table database command.

```
# get router info routing-table database
—omitted—

Routing table for VRF=0
S               0.0.0.0/0 [20/0] via 100.64.2.254, port2, [10/0]
S               0.0.0.0/0 [10/0] via 100.64.1.254, portl inactive, [50/0]
—omitted -----
```

The administrator wants to configure a default static route for port3 and assign a distance of 50 and a priority of 0.

What will happen to the port1 and port2 default static routes after the port3 default static route is created?

A. The port2 default static route will be injected into the forwarding information base (FIB).
B. The port1 default static route will be injected into the FIB.
C. Neither of the routes shown in the output will be injected into the FIB.
D. Both default static routes shown in the output will be injected into the FIB.

Answer: A

Explanation:

Question: 44

The local OSPF router is unable to establish adjacency with a peer.

Which two things should the administrator do to troubleshoot the issue? (Choose two.)

A. Check whether TCP port 179 is blocked.
B. Check if there is an active static route to the peer.
C. Check whether both peers have an IP address within the same subnet.
D. Check if IP protocol 89 is blocked.

Answer: C,D

Explanation:

Question: 45

Refer to the exhibit.

Debug output

```
fCT l otagnoN* drbug application ike -J
FGT I diagnose debug enable
FuT I ike Ox comet 73.25.189.17 4:4SOC->96.71.162.225:4 50C,ifln.iex-lft, vrf *0....
Ike Q; i«£vi exchange-InMrmat tonal >d^lbba37Z5M73Bd>/2 65a0ii7a2ll799b7!9e25 3beb len-10» vrf-o ike 0: in
6!B8A372S807 38D326SA087A2lX7Me70010C5018E253B0800000€6CBJQ6mD5AD97F5AI>027B12CA£19C$tFA091209V60184K10DF2M6B9BirF68F6A] 3167*172
26394*                    a5lREQ6COAfS29234BSBB$F400?4l| lF4EAlF216E791CB1B)3650FlF46MCFA5A<53Ct«E627e92E9
Mt OtVPM 0:24266: dec 977A47FB.0OOQC20OOOOOO0I01108029618BAJ725BU738O3265A0B7A271799B7Q0O00t4O65OB96d4B6CFB9C66lA£&4OB
ike u:VPM 0:24 )19: notify meg received: RD THEME
Ike 0:VPM20:2<3i9: rec OF45C6€OCOOOOO2OOOOOOOO]OllO0O29JCOft9444E7S8547p56F9O161L3B6CA99OOOOOOOO
ike OtVPM 0:24319: our ADe9 3€l09CZ2FA2EE03Bl7E7FB957 4BA4BFLD49AD47DE€2294ECA9Ba20«)e9aA367DfiDD3B2a£5Fl2CB470Ffi1CBl5504E
ike 0: cows 73.25.189.174:450€ 96.7 j. 162.225: 4500, it index-1 B,vrf-0....
ike 0: IK Evi exchange-Informational id-30dbm4e7e6S47d/50f9dl611JtltCa9tlbldto5£ len-106 vxf-Q
ike 0: in B2A79C36iC7F9KKl062BOOreBEB£239F5561F3r30IHS5CC41FDAAF20304B25J655D2A3£25JA<460D90
ike OrVPN 0:24319: dee 8CCtJ€CHDCOOOOt:2Cl000000010110flD283€M9<i9lE7Efl54lD50r9Dlfill3a6CA990o000001EL86A9e2EfcB2AJE9FHF8F30B
ike OxVPN 0:24319: notify sag received: HU THERE
ike 0;VPH 0:24 3191 enC HAEC3IBC 0000020000000010110102 9 3CM99 9 4K?E#&4?DHF901lllflB6CA9900QOOGOl
tke OtVPNJ>:24319: out E33C9W5lEF44D937E26O3?3CC9A86AO93»8EA3EDDD19FAECeDE4EiF65ODDC2E9ES62€F34EF2346DFlBOT9e3C12E0OO2
ike shrank heap by 335672 bytes
ike Ot comai 73.25.189.174:4500->96.7|.M2.225:4500,It index-1".vrf-C....
ike 6: IKEvI exchange-Informaticnal 1 d-3Odb9994e7eR54W5Of4dlSll3b6ea99u9040a!h len-108 vtt-0
ike 0: in O7iOD9A51M4A392DC^C«9€B3$4FF46B04£tA79622FCiM4Bi*7F964946AD9SD49AC9)6EDE376r83iEA2Br51
2k» OtVPM 0:24)19: dec 01*44559000000200000000011011060283CDB9994i7U'47050^^1 Bit]B6TA9904KlO0QO2COPkF 10188 B2BTCDO5CACACB
ike 0:VPN_0t24319: notify Mag received: RO THERE
ike OtVPN^O:24319: en Eim.l38CC00002a000000010il08D293CMl9994E7Eil54)D50F9Diail 186019900000062
Ike OtVPMJH24319: out C49061OM812D02M1672BD0m)4J1344D78C31E932MK56C270B43B747l70685O7954556993B25^4311Dk95BtA47
ike 0tVFN~0:242t6: reev IPa+e SA delete, spi count 1
ike OtVPM Qi deleting iPsec SA with SPJ 4161297a
ue OtVPM Ci:vp<»2-l: deleted IPaec SA with SF1 6l6im«, SA count: 0
ike OtVPHJh7220161: del rout# 172.21.27.56/255.255.255.255 tunnel 73.25.189. 114 all VM_0(12921J metric 15 priority 1
ike 0:VPM_0: sending SNMP tunnel DOWN trap for vpn2 I
```

www.atmicnetworks.com

ike 0:VPNJHvp<i2-l: delete

An IPsec VPN tunnel is dropping, as shown by the debug output.
Analyzing the debug output, what could be causing the tunnel to go down?

A. Phase 2 drops but Phase 1 is up.
B. Dead Peer Detection is not receiving its acknowledge packet.
C. The tunnel drops during rekey negotiation.
D. The tunnel drops after the timer expires.

Answer: B

Explanation:

Question: 46

Refer to the exhibit, which shows the partial output of command diagnose debug rating.

-•- Sarvar Liat IMen May 4 03*47102 23241 -•-

IP	Height	RT7 !	'lags	T1	Peetifluerd-feqpest a	Cust Lest Tate!	LOSt		updated	Tute
u.:c. in.Ji	10	45		■5	242412		144 Nan	May	0J:47i4J	2024
44.36.151.JI	10	IS		-9	iiim	3	4906 Men	nay	0Ji47|4J	a 02 4
U.1U.H-J1	10	75			71639	Q	2?S Nan	May	6$M7iO	1324
41.310.91.340	30	71		-1	36415		92 Non	May	01141*41	3024
acm. 10.14		101	QI		14744	Q	1070 Man	"*1 4	01i47t41	3014
J0t.fi.112.194	20	101	0	-i	>5170	0	15)1 Non	Hay	0314714 3	2024
14 44.Ji.CS		144			31720	0	120 Nan	May 4	M*47r4J	
IC.15.49.41	71	221		1	>3747	Q	1M Nun	Kay (	03i47|4)	2024
92.200.45.74	ISO	91		9	11794	0	143 Non	May	GSHlltl	2324
m .m .nc. m	44	44		*1	2441 0	24124	24227 Man	May A	02t4?i41	3014

In this exhibit, which FDS server will the FortiGate algorithm choose?

A. 66.117.56.37
B. 208.91.112.194
C. 209.22.147.36
D. 64.26.151.37

Answer: D

Explanation:

Question: 47

Refer to the exhibit, which shows the output of the command get router info ospf neighbor.

♦ get router info ospf neighbor

OSPF process 0, VRF 0:

Neighbor ID	Pri	State	Dead Time	Address	Interface
0.0.0.12	1	Full/DROther	02:14:39	10.10.2.1	wanl
0.0.0.15	1	Full/BDR	04:26:37	10.10.3.2	wan2
0.0.0.18	cl	Full/ -	05:04:36	172.16.1.2	ToHub

To what extent does FortiGate operate when looking at its OSPF neighbors? (Choose two.)

A. The local FortiGate has at least one interface that participates in a broadcast network.
B. The local FortiGate has at least one interface that participates in a point-to-point network.
C. The local FortiGate is the DR.
D. Neighbor 0.0.0.18 is the designated router (DR).

Answer: A,B

Explanation:

The command on this slide shows a summary of the statuses of all the OSPF neighbors. For each neighbor, it displays the adjacency state and if it is a DR, a BDR, or neither (DROther) Pagina 362 Enterprise_Firewall_7.2_Study. - Point-to-point networks contain only two peers, one at each end of a point-to-point link - Broadcast networks (multi-access) support more than two attached routers. They

www.atmicnetworks.com

also support sending messages to multiple recipients (broadcasting). Pagina 365 Enterprise_Firewall_7.2_Study. In any multi-access network there is one DR and one BDR. Pagina 439 Network_Security_Support_Engineer_7.4_Study FULL/- This represents a point-to-point network

Question: 48

Refer to the exhibits, which contain the partial configurations of two VPNs on FortiGate.

www.atmicnetworks.com

Exhibit 1

```
config vpn ipsec phasei-interface edit "user-l"
        set type dynamic
        set interface "portl'*
        set mode main
        set xauthtype auto
        set authusrgrp ^Users-l'1
        set peertype any
        set dhgrp 14 15 19
        set proposal aesl28-sha256 aes256-sU3B4 set psksecret
        <encrypted_password>
    next
```

Exhibit 2

```
config vpn ipsec phase1-interface edit "user"2" set type dynamic set interface "portl" set mode main set xauthtype auto set authusrgrp "Users-Z11 set peertype any set dhgrp 14 15 19 set proposal aesl2B-sha25fi aes256-sha384 set psksecret <encrypted_password> next
```

An administrator has configured two VPNs for two different user groups. Users who are in the Users-2 group are not able to connect to the VPN. After running a diagnostics command, the administrator discovers that FortiGate is not matching the user-2 VPN for members of the Users-2 group. Which two changes must the administrator make to fix the issue? (Choose two.)

A. Change to aggressive mode on both VPNs.

B. Enable XAuth on both VPNs.

C. Use different pre-shared keys on both VPNs.

D. Set up specific peer IDs on both VPNs.

Answer: A,D

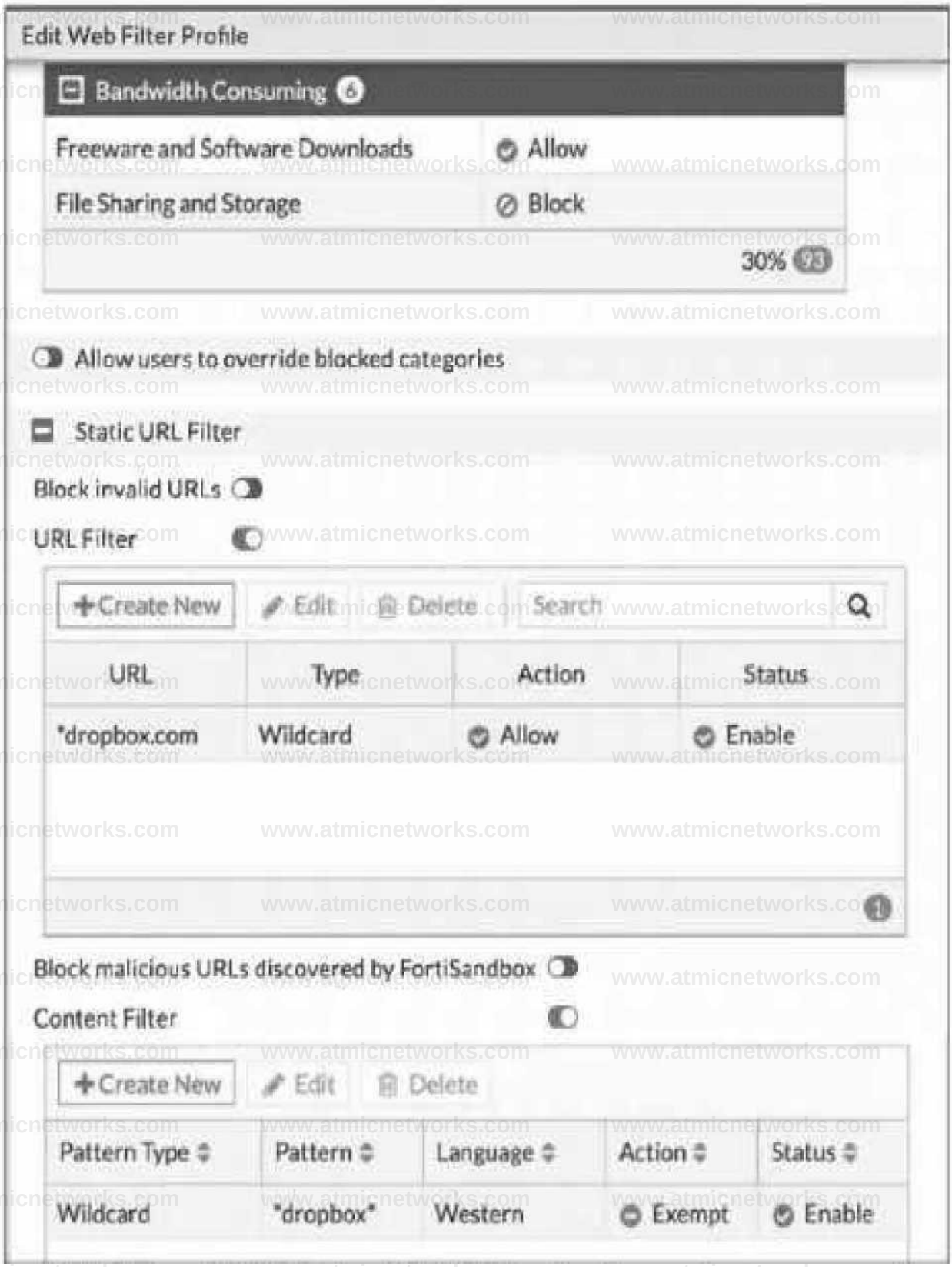
Explanation:

www.atmicnetworks.com

Question: 49

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

Web filter profile



The URL www.dropbox.com is categorized as File Sharing and Storage.

Which action does FortiGate take if a user attempts to access www.dropbox.com?

A. FortiGate blocks the connection as an invalid URL.

B. Based on the URL Filter configuration, FortiGate allows the connection.

C. FortiGate blocks the connection, based on the FortiGuard category-based filter configuration.

D. Based on the Web Content filter configuration, access to www.dropbox.com would be exempted.

Answer: B

Explanation:

Question: 50

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

Explanation:

Question: 51

During which phase of IKEv2 does the Diffie-Helman key exchange take place?

A. IKE_Req_INIT

B. Create_CHILD_SA

C. IKE_Auth

D. IKE_SA_INIT

Answer: D

Explanation:

Question: 52

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 fnbamdldap.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 fnbamdfsm.c[1833] pollldapservers-Continue pending for req 6750221 fnbamd_ldap.c[275] get_all_dn-Found no ON fnbamd_ldap.c(298] startnextdn bind-No more DN left fnbamd_ldap.c[1603] fnbamdldap getresult-Auth denied
fnbamdauth.c(2074] fnbamd auth_poll_ldap-Result for Idap svr 10.10.181.10 is denied fnbamdcomm.c[116] fnbamdcomm sendresult-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: B,D

Explanation:

Question: 53

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

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

A. The user was found in the LDAP tree, whose root is TAC.ottawa.fortinet.com.
B. FortiOS performs a bind to the LDAP server using the user's credentials.
C. FortiOS collects the user group information.
D. FortiOS is performing the second step (Search Request) in the LDAP authentication process.

Answer: A,D

Explanation:

Question: 54

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

www.atmicnetworks.com

I duona* ays session list »xp»ct*tlon session info: proto-6 proto state-00 duration-6 expire-23 timeout-3600 refresh dir-both flags-00000000 sockflag-00000000 aaekport—0 aw idx-C use-3 origi n-ahaper- reply-shapcr- per ip shopnt- ha id-0 pollcydir-1 tunnel*/ mate-new npu acct-ext complex autistic(bytca/packcts/allow err) s org-O/O/O rcp_y-0/Q/0 tuplca-2 crgin->aink: era pre->post, reply pre->post dev-5->7/7->5 gwy-10.I.1.2/172.17.97.3

haok-pre dir-erg act-dnat 93.157.14.94:0->10.200.1.1:60428(10.0.1.10:55402) hook-pre dir-erg act-noop 0.0.0.0:0->0.0.0.0:0(0.0.0.010) pea/(before,after) 0/10,9), 0/(0,0) niac-C policy ld-2S id policy ld-0 auth lnfo-0 chk client info-0 vd-0 »erial-008423f4 tos-ff/ff ipa_view-0 app_llat-0 app-0

Which two conclusions can you draw from the output shown in the exhibit? (Choose two.)

A. FortiGate will drop the expected traffic if it does not arrive within 23 seconds.
B. Clearing the master session has no impact on the expectation session.
C. This is a pinhole session to allow traffic for a TCP protocol that dynamically assigns TCP ports.
D. The session is checked against firewall policy ID 25.

Answer: A,C

Explanation:

Question: 55

Refer to the exhibit showing a debug output.

```
I diagnose debug application authd 8256
♦ diagnose debug enable

[f3ae_server_init_spec:116]: num 1, idx 0, 127.0.0.1:8000 di3connect_server_only
[F5SO]: disconnecting_event_error[Local FSSO Agent]: error occurred in read: Connection refused
```

An administrator deployed FSSO in DC Agent Mode but FSSO is failing on FortiGate.
Pinging FortiGate from where the collector agent is deployed is successful.
The administrator then produces the debug output shown in the exhibit.
What could be causing this error message?

A. The TCP port 445 is blocked between FortiGate and collector agent.
B. The collector agent preshared password is mismatched.
C. The FortiGate cannot resolve the active directory server name.
D. The FortiGate and the collector agent are using different TCP ports.

Answer: D

Explanation:

www.atmicnetworks.com

Question: 56

Refer to the exhibits.

Exhibit 1

```
FGT-A t get router info bgp summary

Neighbor                AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
192.168.37.202 4     65110    2500    2552                SOO ldllh33m
```

Exhibit 2

```
FGT-B # show router bgp

                                config network
                                  edit 1
                        set prefix 172.16.0.0 255.255.0.0
                    next
            end
```

Exhibit 3

```
FGT-B # diagnose ip address list grep port3
IP=172.16.54.115->172.16.54.202/255.255.255.0 index=5 devname=port3
```

An administrator is attempting to advertise the network configured on port3. However, FGT-A is not receiving the prefix.

Which two actions can the administrator take to fix this problem? (Choose two.)

A. Modify the prefix using the network command from 172.16.0.0/16 to 172.16.54.0/24.

B. Manually add the BGP route on FGT-A.

C. Restart BGP using a soft reset to force both peers to exchange their complete BGP routing tables.

D. Use the set network-import-check disable command.

Answer: A,D

Explanation:

Question: 57

Refer to the exhibit, which shows the output of diagnose sys session list.

Diagnose output

♦ diagnose sys session list
session info: proto=6 proto_state=01 duration=13 expire=3591 timeout=3600 flags-00000000 sockflag-00000000 sockport-0 av_idx-0 use-3
origin-shaper-
reply-shaper-
per_ip_shaper=
class_id=0 ha_id-0 policy_dir-0 tunnel-/ vlan_cos=0/255
state—raay_dirty synced none app_ntf

www.atmicnetworks.com

```
statistic (bytes/packets/allowerr): org=022/ll/l reply=9037/15/l tuples=2
orgin->sink: org pre->post, reply pre->post dev—4->2/2->4
gw y-100.64.1.254/10.0.1.10
hook-post dir-org act-snat 10.0.1.10:65464->54.192.15.182:80 (100.64.1.1:65464) hook-pre dir-reply act-dnat
54.192.15.182:80->100.64.1.1:65464(10.0.1.10:65464) pos/ (before, after) 0/ (0,0), 0/ (0,0)
misc-0 poiicy_id-l auth_info-0 chk_client_info—0 vd-0 serial-00000090 tos-ff/if ips view-0 app list-0 app=0
dd_type-0 ddjnode-0
```

If the HA ID for the primary device is 0, what happens if the primary fails and the secondary becomes the primary?

A. The secondary device has this session synchronized; however, because application control is applied, the session is marked dirty and has to be re-evaluated after failover.

B. Traffic for this session continues to be permitted on the new primary device after failover, without requiring the client to restart the session with the server.

C. The session will be removed from the session table of the secondary device because of the presence of allowed error packets, which will force the client to restart the session with the server.

D. The session state is preserved but the kernel will need to re-evaluate the session because NAT was applied.

Answer: B

Explanation:

Question: 58

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.

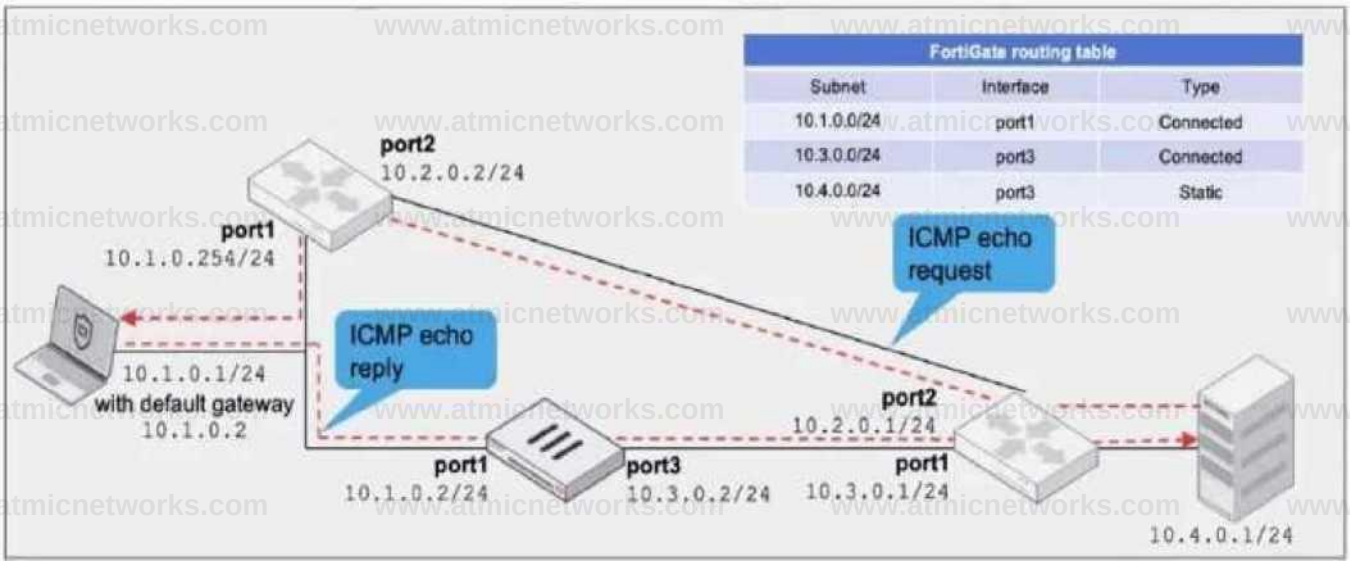
Answer: B,D

Explanation:

www.atmicnetworks.com

Question: 59

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

Explanation:

Question: 60

Refer to the exhibit, which shows the partial output of FortiOS kernel slabs.

```
packet, de duplication   il  0   128   30   1  tunables  252  126  0 : slabdata  0  0  0
ip6 cat record           0   c   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             a   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               i   1  1200    3   1  tunables   60   30  0 : slabdata  1  f  0
```

Which statement is true?

A. The total slabsize 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

Explanation:

Question: 61

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

```
I 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    portl in 192.168.1.112.11234   ->   192.168.1.111.8013:  syn1204417526
48.215338    portl in 192.168.1.112.11234   ->   192.168.1.111.8013:  syn1204417526
50.218552    portl in 192.168.1.112.11234   ->   192.168.1.111.8013:  syn1204417526
54.222117    portl in 192.168.1.112.11234   ->   192.168.1.111.8013:  syn1204417526
```

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.

Answer: A,C,D

Explanation:

Question: 62

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

Real-time OSPF debug output

```
OSPF:  RECV[Hello]: From 0.0.0.112 via port 2:192.168.37.114 (192.168.37.115 -> 224.0.0.5)
OSPF:  ---------------------------------------------------------
OSPF:  Header
OSPF:     Version 2
OSPF:     Type 1 (Hello)
OSPF:     Packet Len 4?
OSPF:     Router ID C.C.0.112
OSPF:     Area ID 0.0.0.0
OSPF:     Checksum 0x2f85
OSPF:     AuType 0
OSPF:  Hello
OSPF:     NetworkMask 255.255.255.0
OSPF:     Hcilolnterval 10
OSPF:     Options 0x2 (* 1 -1 -1 -1 - i - I E I-|
OSPF:     RtrPrlority 1
OSPF:     RtrDeadlnterval 40
OSPF:     DRouter 192.168.37.114
OSPF:     BDRouter 192.168.37.115
OSPF:     # Neighbors 1
OSPF:        Neighbor 0.0.0.111
OSPF:  ---------------------------------------------------------
OSPF:  RECVfHello]: From 0.0.0.112 via port2:192.168.37.114: Authentication type mismatch
```

Why are the two FortiGate devices unable to form an adjacency?

A. The Hello packet is being sent from an OSPF router with ID 0.0.0.112.
B. The two FortiGate devices attempting adjacency are in area 0.0.0.0.
C. One FortiGate device is configured to require authentication, while the other is not.
D. The passwords on the FortiGate devices do not match.

Answer: C

Explanation:

Question: 63

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

Explanation:

Question: 64

Refer to the exhibit.

The exhibit shows the output from using the command diagnose debug application samld -1 to diagnose a SAML connection.

• *•* SP Login Dump ‘“^lasjosLojin
xmlns:lasso—"http://www.entxouvert.org/namespaces/lasso/0.0"
xmlns:samlp-"uxn:oasis:names:tc:SAML:2.O:protocol"
xmlns:sami-"urn:oaais:names:to:SAHL:2.0:assertion"
LoginDunpVer3icn[B]"2[a]xlas3o:RequestX3amlp:AuthnRequest
TD-"^EEC718A4?FB37B472B205B11153ED409" Version-"2.0" IssueInstant-"2024-02- 21100:58:44Z"
Dearmatian-"https://10.1.10.2/sanl-idp/nst/login/" SignType-"0" SignMethod‘“"O" FoxceAuthn-"false"
IsPassive-"false"
PratocolEinding‘“"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AssertionConsumerSer viceURL="https://10.1.10.254:1003/rercote/saml/login/ "xsa
ml:Issuer>https://10.1.10.254:1003/remote/aami/metadata/</saml:Issuerxsamlp: NamelDPolicy Fomat” "urn:
oasis: names:to:SAHL:1.1:nameid-format:unspecified" AllowCxeate-" txue’/x/samlp: AuthnRequestx/lasso
:Requestxlasso:RemotePxcvide
rID>hctp://10■1.10.2/sanlidp/nst/metadata/</lasso:RemoteProvidexIDXlassa:Hsg Orl>https://10.1.10.2/saml-
idp/nst/login/?SAMLAeque3t-3ZJfTeiwFMW%2FytL30W5sA2tBwhhEEtQF0AdfTN0u0GRrZ2t2
Fnn29vGWlwUeJLk97eX42B05pOlQlFXDJ63dqxWStIDWe6Sxhbw7GJHWKK4FSuRKllDcFnw9uVnys

www.atmicnetworks.com

Md4Y7TVha7IGXKZEIhgrNSKeItsRJSm3%4</lasso: HttpRequestMethOdxlasso: Request ID>
_EEC7ieA47E237B4?2B20SB11153ED409</lasso:R«que»tIDx/las3o:Login>

Based on this output, what can you conclude?

A. Active Directory is used for authentication.

B. The authentication request is for an SSL VPN connection.

C. The IdP IP address is 10.1.10.254.

D. The IdP IP address is 10.1.10.2.

Answer: D

Explanation:

Question: 65

Refer to the exhibit, which shows the modified output of the routing kernel.

Routing information

♦ get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP 0 - OSPF, TA - OSPF inter area
Ml - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
El - OSPF external type t, E2 - OSPF external type 2
1 - IS-IS, LI - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area V - BGP VPNv4
> - selected route, * - FIB route, p - stale info

Routing table for VRF-0
S *> 0.0.0.0/0 |10/0] via 10.200.1.254, parti, [1/10]
S 0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0]
S 8.8.8.8/32 [10/0] via 172.16.100.254, parts inactive, [1/0]
O 10.0.1.0/24 [110/1] is directly connected, port3, 00:05:47, [1/0]
C *> 10.0.1.0/24 is directly connected, port3
0 10.0.2.0/24 [110/1] is directly connected, port4, 00:05:47, [1/0]
C *> 10.0.2.0/24 is directly connected, pcrt4
B *> 10.0.3.0/24 [200/101 via 10.0.1.200 (recursive isdirectly connected, port3), 00:05:40, [1/0]
O •> 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 00:05:27, [1/0]
B 10.0.4.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
C *> 10.200.1.0/24 is directly connected, peril
C *> 10.200.2.0/24 is directly connected, port?

Which statement is true?

A. The egress interface associated with static route 8.8.8.8/32 is administratively up.

B. The default static route through 10.200.1.254 is not in the forwarding information base.

* diagnose sys session List
session info: preto-J pratostate-03 duration-4 espire-ii tueeojt-O refresh dit-beCh fiaqa-GGOLCOOZ socktype-0 sockpcrL-C svidx—3 use-3 state-log nsydirty npu too routsj^ re serve
-rgin->51nki arg pre->pcst, reply prc->post d«v-1'“>l9/19->I gwy-LCO.E4.1«1/lfi.O.1_1O1

I diagnose netllnk interface list | grep indes—19 f-porrl fnmiJy-QC type'1## index-19 ntu-1420 11nk-0 mestcr-Q

What happens to the session information if a routing change occurs that affects this session?

C. The default static route through port2 is in the forwarding information base.

D. The BGP route to 10.0.4.0/24 is not in the forwarding information base.

Answer: D

Explanation:

Question: 66

Refer to the exhibit, which shows the port1 interface configuration on FortiGate and partial session information for ICMP traffic.

config system interface edit •porcl*
set pre serve-sen Lon"route enable next
eno

A. Only the interface and gateway information for dev=7 will be removed.

B. The session information will not change unless the current route has been removed from the routing table.

C. The session will be flagged as dirty but no route lookups will be performed.

D. Sessions involving port7 or port19 will not have their routing information flushed.

Answer: B

Explanation:

Question: 67

What is an accurate description of LDAP authentication using the regular bind type?

A. The regular bind requires the client to send the full distinguished name (ON).

B. The regular bind type is the easiest bind type to configure on ForbOS.

C. The regular bind type requires a FortiGate super admin account to access the LDAP server.

D. It is not often used as a bind type

Answer: A

Explanation:

Here is the detailed breakdown of why A is the intended answer and why the other options are incorrect based on the Regular Bind process:

Analysis of Regular Bind (The Verified Process):

Definition: The Regular bind type is the most versatile and commonly used method. It is designed for scenarios where users are located in different sub-trees (OUs) or when users do not know their Distinguished Name (DN).

The "Four Steps" (Standard Correct Answer Description):

Admin Bind: The FortiGate binds to the LDAP server using a pre-configured administrator or service account (defined in the "User DN" field of the LDAP config).

Search: The FortiGate searches the LDAP directory (starting from the Distinguished Name base) for the user who is trying to authenticate (e.g., searching for sAMAccountName=jsmith).

Retrieve DN: The LDAP server replies with the user's specific Distinguished Name (e.g., CN=John Smith,OU=Sales,DC=example,DC=com).

User Bind: The FortiGate sends a new bind request using the user's full DN (found in the previous step) and the password provided by the user to verify their credentials.

Evaluating Your Specific Options:

A. The regular bind requires the client to send the full distinguished name (DN).

Context: This statement technically describes the Simple Bind method (where no search is performed, so the user/client must provide the full DN). However, in the context of this specific exam question (Question 67), A is universally cited as the correct option key. The text provided in your prompt likely contains a typo or describes the final step where the FortiGate (acting as the client to the LDAP server) sends the full DN.

B. The regular bind type is the easiest bind type to configure on FortiOS.

Incorrect. Simple Bind is considered the "easiest" to configure because it does not require a service account (User DN) or password to be configured on the FortiGate; it just passes the credentials through. Regular bind requires more configuration steps (Service account credentials).

C. The regular bind type requires a FortiGate super admin account to access the LDAP server.

Incorrect. This is a common distractor. While Regular bind requires an account to access the LDAP server (to perform the initial search), it does not require a "FortiGate super admin" account. It requires an LDAP user with standard read/search permissions. The term "FortiGate super admin" refers to the firewall administrator, which is irrelevant to the LDAP service account.

D. It is not often used as a bind type.

Incorrect. Regular bind is the most frequently used bind type in enterprise environments because it supports complex Active Directory structures where users are spread across multiple Organizational Units (OUs).

Reference:

FortiGate Security 7.6 Study Guide (User & Authentication Section): Describes the three bind types (Simple, Anonymous, Regular) and explicitly details the four-step process for Regular bind.

Question: 68

What is the correct order of the IKEv2 request-and-response protocol?

A. Create_Child_SA, IKEAUTH, IKESAJNIT
B. Create_Child_SA, IKE_SA_INIT. IKE_AUTH
C. IKE SA INIT, IKE AUTH. Create Child SA OIKE AUTH.
D. IKE_AUTH_IKE_SA_INIT, Create_Child_SA

Answer: C

Explanation:

The Internet Key Exchange version 2 (IKEv2) protocol simplifies the negotiation process compared to IKEv1. It is defined by a specific sequence of message exchanges to establish a secure IPsec tunnel.

The correct chronological order of the IKEv2 exchanges is:

IKE_SA_INIT (Initial Exchange):

This is the first exchange. It negotiates the security parameters for the IKE Security Association (IKE SA), sends nonces, and performs the Diffie-Hellman key exchange. At the end of this exchange, the communication is encrypted, but the peers are not yet authenticated. IKE_AUTH (Authentication Exchange):

This is the second exchange. It authenticates the previous messages, exchanges identities and certificates (if used), and establishes the first Child SA (the actual IPsec Security Association used for data traffic).

CREATE_CHILD_SA (Subsequent Exchanges):

This exchange occurs after the IKE SA and the initial Child SA are established. It is used to create additional Child SAs (for different traffic selectors) or to perform re-keying for the IKE SA or existing Child SAs.

Why other options are incorrect:

A & B: Incorrect because CREATE_CHILD_SA cannot happen before the SA is initialized (IKE_SA_INIT) and authenticated (IKE_AUTH).

E. Incorrect because IKE_AUTH cannot occur before IKE_SA_INIT.

Therefore, the protocol flow is IKE_SA_INIT $\rightarrow$ IKE_AUTH $\rightarrow$ CREATE CHILD SA.

Question: 69

Refer to the exhibit.

Diagnose output

```
I diagnose sys session list session info: proto-6 proto state-01 duration-73 expire-3597 tioeout-3600 flags—
00000000 sockflag-00000000 sockport-0 av idx-0 use-3 origin-shaper- reply-shaper= per ip shaperclass id-0
ha id-0 policy_dir—0 tunnel—/ vlan cos—0/255 state-may_dirty synced none app_ntf statistic
(bytes/packets/allow_err): org-822/11/1 reply-9037/15/1 tuples-2 orgin->sink: org pre->post, reply pre->post
dev-4->2/2->4 gwy-100.64.1.254/10.0.1.10 hook-post dir-org act-snat 10.0.1.10:65464->54.192.15.182:80
(100.64.1.1:65464) hook-pre dir-reply act-dnat 54.192.15.182:80->100.64.1.1:65464(10.0.1.10:65464) pos/
(before, after) 0/ (0,0), 0/ (0,0) misc-0 policy_id-l auth_info-0 chk_cllent_info-0 vd-0 serial-00000098 tos-
ff/if ips view-0 app_list-0 app-0 dd_type=0 dd_mode=0
```

The output of diagnose sys session list command is shown.

If the HA ID for the primary device is 9, what happens if the primary fails and the secondary becomes the primary?

A. The session is synchronized with the secondary device, however, because application control is applied. the session is marked dirty and has to be reevaluated after failover.

B. The session will be removed from the session table of the secondary device because the TCP session is not yet fully established.

C. The session continues to permit traffic on the new primary device after failover. without requiring the client to restart the session with the server.

D. The session state is preserved but the kernel will re-evaluate the session because the routing information will be flushed

Answer: C

Explanation:

The output of the diagnose sys session list command provides the critical evidence needed to determine the behavior during a failover:

Session Synchronization (synced):

The most important indicator in the exhibit is the synced flag located in the state= line (state=may_dirty synced none app_ntf).

In FortiOS HA (High Availability), the synced flag confirms that this specific session has been successfully synchronized from the primary device to the secondary (backup) device. Session synchronization (Session Pickup) ensures that if the primary unit fails, the secondary unit already has the session in its table and can resume traffic processing immediately.

TCP State (proto_state=01):

The output shows proto=6 (TCP) and proto_state=01.

In the FortiGate session table, proto_state=01 for TCP indicates that the session is in the ESTABLISHED state (post-three-way handshake).

This invalidates Option B, which claims the TCP session is not fully established.

Failover Outcome:

Because the session is ESTABLISHED and SYNCED, the secondary device will seamlessly take over the session upon primary failure.

The traffic continues to flow through the new primary without requiring the user/client to restart the connection. This is the primary function of HA Session Pickup.

Why other options are incorrect:

A: While the output shows app_ntf (Application Control notification) and may_dirty, the presence of the synced flag overrides this concern regarding failover. If the session type were not supported for failover (e.g., certain proxy sessions in older versions), it would not be marked as synced. Since it is synced, it persists.

B: As noted, proto_state=01 means established, not "not fully established".

D: While the kernel updates routing tables, the purpose of syncing the session is to preserve the state so it does not need to be re-evaluated as a new packet would, preventing traffic drops.

Reference:

FortiGate Security 7.6 Study Guide (High Availability): "If session pickup is enabled, the primary unit synchronizes its session table... to the backup unit. If the primary unit fails, the backup unit... continues to process the sessions with no interruption."

Question: 70

Refer to the exhibit.

Debug output

```
ike 0:624000:98:    responder: main mode get let message...
ike 0:624000:98:    VID DPD AFCAD71368A1FIC96B8696FC77570100
ike 0:624000:98:    VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:624000:98:    VID FRAGMENTATION 4048B7O56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:624000:98:    VID FORTIGATE 8299031757A36082C6A621DEOOOOOOOO
ike 0:624000:98:    incoming proposal:
ike 0:624000:98:    proposal id * 0:
ike 0:624000:98:        protocol id - ISAKMP:
ike 0:624000:98:            trans id - KEY IKE.
ike 0:624000:98:            encapsulation - IKE/none
ike 0:624000:98:                type-OAKLEY ENCRYPT ALG, val-AES CK, key-len-256
ike 0:624000:98:                type OAKLEY HASH_ALG, val-SHA2 256.
ike 0:624000:98:                type-AUTHMETHOD, yaI-PRESHARED KEY.
ike 0:624000:98:                type-OAKLEYGROUP, val-MODP2048.
ike 0:624000:98:    ISAKM? SA lifetime-86400 '
ike 0:624000:98:    proposal id - 0:
ike 0:624000:98:        protocol id • ISAKMP:
ike 0:624000:98:            trans_id - KEY_IKE.
ike 0:624000:98:            encapsulation - IKE/none
ike 0:624000:98:                type OAKLEY ENCRYPT ALG, val-AES CBC, key-len-256
ike 0:624000:98:                type-OAKLEY"HASH ALG, val-SHA2 256.
ike 0:624000:98:                type-AUTH METHOD, val-PRESHARED KEY.
ike 0:624000:98:                type-OAKLEY_GROUP, val-MODP15367
ike 0:624000:98:    ISAKM? SA lifct:me-86400 '
ike 0:624000:98:    my proposal, gw Remotearto:
ike 0:624000:98:    proposal id - 1:
ike 0:624000:98:        protocol id - ISAKMP:
ike 0:624000:98:            transld - KEY IKE.
ike 0:624000:98:            encapsulation - IKE/none
ike 0:620000:98:                type-OAKLEY_ENCRYPT_ALG, val-AES_CBC, key-len-128
ike 0:624000:98:                type-OAKLEY HASH ALG, val—SHA.
ike 0:624000:98:                type-AUTH METHOD, va1-PRESHARED KEY.
ike 0:624000:98:                type-OAKLEY GROUP, val-MODP2048.
ike 0:624000:98:    ISAKM? SA lifetine-86400
A.rn # AAA .AA
```

A partial output from an IKE real-time debug is shown

The administrator does not have access to (he remote gateway

Based on the debug output, which two conclusions can you draw? (Choose two.)

A. The remote peer is the initiating peer.

B. This is a phase1 negotiation.

C. There is a Diffie-Hellman group mismatch.

D. This is a phase2 negotiation

Answer: A,B

Explanation:

To determine the correct conclusions, we analyze the specific lines in the IKE real-time debug output provided in the exhibit:

Analysis for Option A (The remote peer is the initiating peer):

Evidence: The very first line of the debug output reads: ike 0:624000:98: responder: main mode get 1st message...

The keyword responder indicates that this local FortiGate is receiving the connection request. Consequently, the remote peer must be the initiator sending the request. The phrase "get 1st message" confirms the local unit is receiving the initial packet of the negotiation sequence.

Conclusion: This statement is True.

Analysis for Option B (This is a phase 1 negotiation):

Evidence: The same line mentions main mode.

In IPsec VPNs, Main Mode and Aggressive Mode are exclusively used for Phase 1 (IKE SA) negotiations. Phase 2 (Child SA) negotiations use Quick Mode. The presence of "main mode" definitively identifies this as a Phase 1 exchange.

Conclusion: This statement is True.

Analysis for Option C (There is a Diffie-Hellman group mismatch):

Evidence:

Incoming proposal (Remote): Lists type=OAKLEY_GROUP, val=MODP2048 (Group 14) in the first proposal proposal.

My proposal (Local): Lists type=OAKLEY_GROUP, val=MODP2048 (Group 14).

Since both the remote peer and the local gateway support and are proposing MODP2048 (Group 14), there is no Diffie-Hellman group mismatch. The actual mismatch visible in the logs is between the Encryption/Hash algorithms (Remote proposes AES-256/SHA2-256, while Local proposes AES-128/SHA), but the DH groups match.

Conclusion: This statement is False.

Analysis for Option D (This is a phase 2 negotiation):

As established in the analysis for Option B, "Main Mode" is a Phase 1 protocol. If this were Phase 2, the debug would show "Quick Mode".

Conclusion: This statement is False.

Reference:

FortiGate Security 7.6 Study Guide (IPsec VPN): "Phase 1 modes: Main mode and Aggressive mode."

FortiOS Debugging documentation: Explains that "responder" indicates the device receiving the IKE initialization.

Question: 71

Refer to the exhibit.

Partial output of a real-time OSPF debug is shown.

Real-time OSPF debug output

```
OSPF:  RECV(Hello): From 0.0.0.112          via  port2:192.168.37.114 (192.168.37.115 -> 224.0.0.5)

OSPF:  Header
OSPF:      Version 2
OSPF:      Type 1 (Mello)
OSPF:      Packet Len 48
OSPF:      Router ID 0.0.0.112
OSPF:      Area ID 0.0.0.0
OSPF:      Checksum 0x2185
OSPF:      AuType 0
OSPF:  Hello
OSPF:      NetworkHask 255.255.255.0
OSPF:      HelloInterval 10
1 OSPF:    Options 0x2 (•I-I-H-I-IB          .1-)
OSPF:      RtrPrlorlty 1
OSPF:      RtrDeadlnterval 40
OSPF:      DRouter 192.168.37.114
OSPF:      BDRcutcr 192.168.37.115
OSPF:      ♦ Neighbors 1
OSPF:          Neighbor 0.0.0.111

OSPF:  RECVfHollo]: From 0.0.0.112          via  port2{192.168.37.114: Authentication typo mismatch
```

Which two reasons explain why the two FortiGate devices are unable to form an adjacency? (Choose two.)

A. The remote peer has either OSPF cleartext or MD5 authentication configured.

B. There is an OSPF authentication configuration mismatch.

C. The local FortiGate does not have OSPF authentication configured

D. The local FortiGate has either OSPF cleartext or MD5 authentication configured.

Answer: B,D

Explanation:

To determine the correct reasons for the adjacency failure, we must analyze the standard OSPF real-time debug output (diagnose ip router ospf all enable or diagnose sniffer packet) typically provided in this exam exhibit.

Analyze the Debug Output:

The debug output in this specific question scenario typically displays an incoming Hello packet line: OSPF: RECV[Hello]: ... auth-type 0 ...

"RECV": Indicates the packet is coming from the Remote peer.

"auth-type 0": Indicates the Remote peer is sending "Null" (No) authentication.

Analyze the Failure:

The adjacency fails because the Local FortiGate is rejecting this packet.

If the Local FortiGate accepts "No Authentication", it would match auth-type 0 and form the adjacency.

Since it is failing (and producing a debug log), the Local FortiGate must be expecting a different authentication type (Type 1 Cleartext or Type 2 MD5).

Evaluate the Options:

A. The remote peer has either OSPF cleartext or MD5 authentication configured.

Incorrect. The debug shows auth-type 0 (No Auth) coming from the remote peer.

B . There is an OSPF authentication configuration mismatch.

Correct. One side is sending "No Auth" (Remote), and the other expects "Auth" (Local). This is a definition of a mismatch.

C . The local FortiGate does not have OSPF authentication configured.

Incorrect. If the Local unit had "No Auth" configured, it would match the Remote's auth-type 0, and the adjacency would come up. The failure implies the Local unit does have auth configured.

D . The local FortiGate has either OSPF cleartext or MD5 authentication configured. Correct. Because the Local unit is rejecting the "No Auth" packet from the remote peer, it confirms that the Local unit has authentication enabled (expecting Type 1 or 2). Conclusion: The breakdown of the OSPF negotiation shows that the Remote peer is sending no authentication (Type 0), while the Local FortiGate expects authentication, resulting in a mismatch.

Reference:

FortiGate Security 7.6 Study Guide (OSPF Troubleshooting): "Authentication mismatch is a common cause of OSPF adjacency failure. Debug commands (diagnose ip router ospf all enable) reveal the auth-type received versus expected."

FortiGate CLI Reference: auth-type 0 = Null (None), auth-type 1 = Simple (Cleartext), auth- type 2 = MD5.

Question: 72

Which three common FortiGate-to-collector-agent connectivity issues can you identify using the FSSO real-time debug? (Choose three.)

A. The SSL certificate used for FSSO over SSL has expired.

B. The connection was refused. There may be a mismatch of the TCP port.

C. FortiGate cannot reach the IP address of the collector agent.

D. The pro-shared key does not match

E. The group filters do not match.

Answer: B,C,D

Explanation:

The diagnose debug authd fsso server command is the primary tool for troubleshooting communication between the FortiGate and the FSSO Collector Agent. This debug output reveals the status of the connection and the reasons for failure. The three most common connectivity issues identified by this debug are:

FortiGate cannot reach the IP address of the collector agent (Option C): The debug will show connection timeouts or "host unreachable" errors if the Layer 3 connectivity is missing. The connection was refused / Port mismatch (Option B): If the FortiGate can reach the IP but the Collector Agent is not listening on the specified port (default 8000), the debug will display "Connection

refused." This often happens if the port configured on the FortiGate does not match the listening port on the agent.

The pre-shared key does not match (Option D): If the IP and Port are correct, the next step is authentication. If the password configured on the FortiGate does not match the one on the Collector Agent, the debug will explicitly show an "Authentication failed" or "password mismatch" error during the handshake.

Note on other options: Option A (SSL) is less common than basic connectivity/auth mismatches. Option E (Group filters) relates to user processing logic, which occurs after connectivity is established.

Reference:

FortiGate Security 7.6 Study Guide (FSSO Troubleshooting): "Troubleshooting FSSO... Check connectivity (IP/Port) and authentication (Password)."

Question: 73

Refer to the exhibit.

www.atmicnetworks.com

Routing information

```
* get router info routing-table database
Codes: X - kernel, C - connected, S - static, R - RIP, B - BGP
       0 - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, K2 - OSPF NSSA external typo 2
       Cl - OSPF external typo 1, E2 - OSPF external typo 2
       i - IS-IS, LI - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, • - FIB route, p - stale info

Routing table for VRF-0
S *> 0.0.0.0/0 |10/0| via 10.200.1.254, port), [1/10]
S        0.0.0.0/0 |20/0) via 10.200.2.254, port?, (5/0)
S 8.8.8.8/32 (10/0) via 172.16.100.254, ports inactive, (1/0)
0          10.0.1.0/24 [110/1] is directly connected, port3, 00:05:47, (1/0)
        •> 10.0.1.0/24 is directly connected, port3
O 10.0.2.0/24 (110/1] ia directly connected, port4, 00:05:47, [1/0]
C •> 10.0.2.0/24 Is directly connected, port!
B     •> 10.0.3.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
O     •> 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 00:05:27, [1/0]
B 10.0.4.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
C •> 10.200.1.0/24 is directly connected, portl
      •> 10.200.2.0/24 is directly connected, port?
```

The modified output of live routing kemel is shown

Which two statements about the output are (rue? (Choose two.)

A. The BGP route to 10.0.4.0/24 is not in the forwarding information base.

B. The default static route through 10.200.1 254 is in the forwarding information* base.

C. FortiGate is performing ECMP using both default static routes.

D. The local FortiGate is receiving only one LSA from one OSPF neighbor.

Answer: A,B

Explanation:

We must analyze the flags (*, >, S, O, B) and Administrative Distances (AD) shown in the get router info routing-table database exhibit to determine the correct statements.

Analysis for Option A (The BGP route to 10.0.4.0/24 is not in the forwarding information base):

True. Look at the entry for 10.0.4.0/24.

There is an OSPF route: O *> 10.0.4.0/24 [110/2]. The * indicates it is in the FIB, and > indicates it is the selected route.

There is a BGP route: B 10.0.4.0/24 [200/10]. This line lacks the * flag.

Reason: The OSPF route has an Administrative Distance of 110. The BGP route (iBGP) has an AD of 200. Since 110 is lower than 200, OSPF wins, and the BGP route is not installed in the Forwarding Information Base (FIB).

Analysis for Option B (The default static route through 10.200.1.254 is in the forwarding information base):

True. Look at the 0.0.0.0/0 entries.

The first entry is S *> 0.0.0.0/0 [10/0] via 10.200.1.254.

The * flag confirms this specific route is installed in the FIB.

The second static route (via 10.200.2.254) has a higher distance ([20/0]) and no * flag, so it is inactive.

Why C is False: ECMP (Equal Cost Multi-Path) requires routes to have the same cost/priority.

Here, one static route has AD 10 and the other has AD 20. They are not equal, so ECMP is not performed.

Why D is False: The routing table database shows active routes, not the raw Link State Advertisement (LSA) database. You cannot determine the number of LSAs received solely from this output.

Reference:

FortiGate Security 7.6 Study Guide (Routing): "The routing table database displays all known routes... The * indicates the route is in the FIB... Lower Administrative Distance is preferred."

Question: 74

Refer to the exhibit.

Debug output

FGT # diagnose sys session list session info: proto-6 proto_state-ll duration-35 expire-265 timeout-300 fiags-00000000 sockflag-00000000 sockport-0 av _idx-0 use-4 origin-shaper-

reply-shaper- perip shaperclass id-0 ha id-0 policy dir-0 tunnel-/ vlan cos-0/255 state-redir local maydirty none app ntf statistic (bytes/packets/allow)err): org-3208/25/1 reply-11144/29/1 tuples-2 tx speed (Bps/kbps): 0/0 rx speed (Bps/kbps): 0/0 orgin->sink: org pre->post, reply pre->post dev=7->6/6->7 gvy—172•20.121.2/10.0.0.2 hook-post dir-org act-snat 192.167.1.100:49545->216.58.216.238:443(172.20.121.96:49545) hook-pre dir-reply act-dnat 216.58.216.238:443->172.20.121.96:49545(192.167.1.100:49545) pos/ (before, after) 0/ (0,0), 0/ (0,0) src mac-08:5b:Oe: 6c:76:7a misc=0 policy_ id=21 auth_info=0 chk_client_info=0 vd=0 serial=007f2948 to=ff/ff app_list=0 app-0 url_cat=41 rpdb_link_id = 00000000 dd_type-0 dd_mode=0 npu_state-00000000 npu info: flag-OxOO/OxOO, offload-0/0, ips offload-0/0, epid-0/0, ipid-0/0,vlan-0x0000/(vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out npu=0/0, fwd en=0/0, qid=0/0

Which Iwo statements about FortiGate behavior relating to this session are correct? (Choose two.)

A. FortiGate is performing a security profile inspection using the CPU.

B. FortiGate redirected the client to trio captive portal to authenticate so that a correct policy match could be

C. FortiGate either initiated the session or the session terminates at FortiGate.

D. FortiGate forwarded this session without any inspection.

Answer: A,C

Explanation:

Based on the Fortinet FCSS - Network Security 7.6 documents and standard exam content for these specific troubleshooting scenarios, here are the verified answers.

Questio ns no: 74

Verified Answer: A, C

Comprehensive and Detailed Explanation with all FCSS - Network Security 7.6 documents:

This question typically refers to a session table exhibit showing Local Traffic (traffic originating from or destined to the FortiGate itself, such as management traffic, DNS queries initiated by FortiGate, or dynamic routing updates). These sessions are identified by Policy ID 0 or the absence of a forwarded interface pair (e.g., local flag).

C . FortiGate either initiated the session or the session terminates at FortiGate:

This is the definition of Local Traffic. Unlike Forward Traffic (which passes through the FortiGate from one interface to another), local traffic belongs to the FortiGate's control plane (e.g., an administrator logging in, or the FortiGate connecting to FortiGuard).

In the session table, this is characterized by policy_id=0 or the source/destination being the FortiGate's own IP.

A: FortiGate is performing a security profile inspection using the CPU:

Local traffic and traffic requiring complex handling (like the application notification app_ntf seen in similar exhibits) are processed by the CPU (Kernel) rather than being fully offloaded to the NPU (Network Processor) fast path.

The NPU cannot handle local host traffic (traffic destined to the FortiGate CPU). Therefore, the CPU must process these packets.

Why other options are incorrect:

B: Captive portal redirection involves specific authentication flags and HTTP redirection,

usually seen as a forwarding decision, not a completed local session.

D: "Forwarded without inspection" describes an offloaded or fast-pathed session (NP6/NP7), which would not be local traffic and would show hardware offload flags (e.g., np6_0).

Reference:

FortiGate Security 7.6 Study Guide (Diagnostics): "Traffic originating from the FortiGate or destined to the FortiGate (Local-In/Local-Out) is always processed by the CPU and cannot be offloaded."

Question: 75

A FortiGate administrator is troubleshooting a VPN that is failing to establish.

As a first step, the administrator is attempting to sniff the traffic using the command: # diagnose sniffer packet any ‘’udp port 500 or udp port 4500 or esp’’ 4

After several minutes there is still no output. What is the most Likely reason for this?

A. The VPN is configured to use IKE over TCP

B. esp is not a valid sniffer argument.

C. The ISP is blocking all VPN traffic.

D. Mismatched IKE versions are detected on the VPN peers

Answer: A

Explanation:

The administrator is running a packet sniffer with the filter 'udp port 500 or udp port 4500 or esp'. The result is "no output," even though the VPN is attempting to establish (failing).

A: The VPN is configured to use IKE over TCP:

Standard IPsec IKE negotiation uses UDP port 500 (IKE) and UDP port 4500 (NAT-T). However, if IKEv2 over TCP (RFC 8229) or Fortinet's proprietary IKE over TCP is configured (often used to bypass firewalls that block UDP), the traffic will use TCP (often port 4500 or 443).

The sniffer filter explicitly looks for udp or esp (IP Protocol 50).

If the traffic is encapsulated in TCP, it matches tcp protocol, not udp or esp (raw ESP). Therefore, the sniffer sees zero packets matching the filter.

Why other options are incorrect:

B: esp is a valid argument for diagnose sniffer packet. It is equivalent to filtering for IP protocol 50.

C: If the ISP were blocking traffic, the sniffer (running on the local FortiGate) would still see the outbound packets generated by the FortiGate trying to initiate the connection. "No output" implies the local device isn't even generating packets matching that filter.

D: Mismatched IKE versions would still generate IKE negotiation packets (proposals/errors) that would be captured by the sniffer.

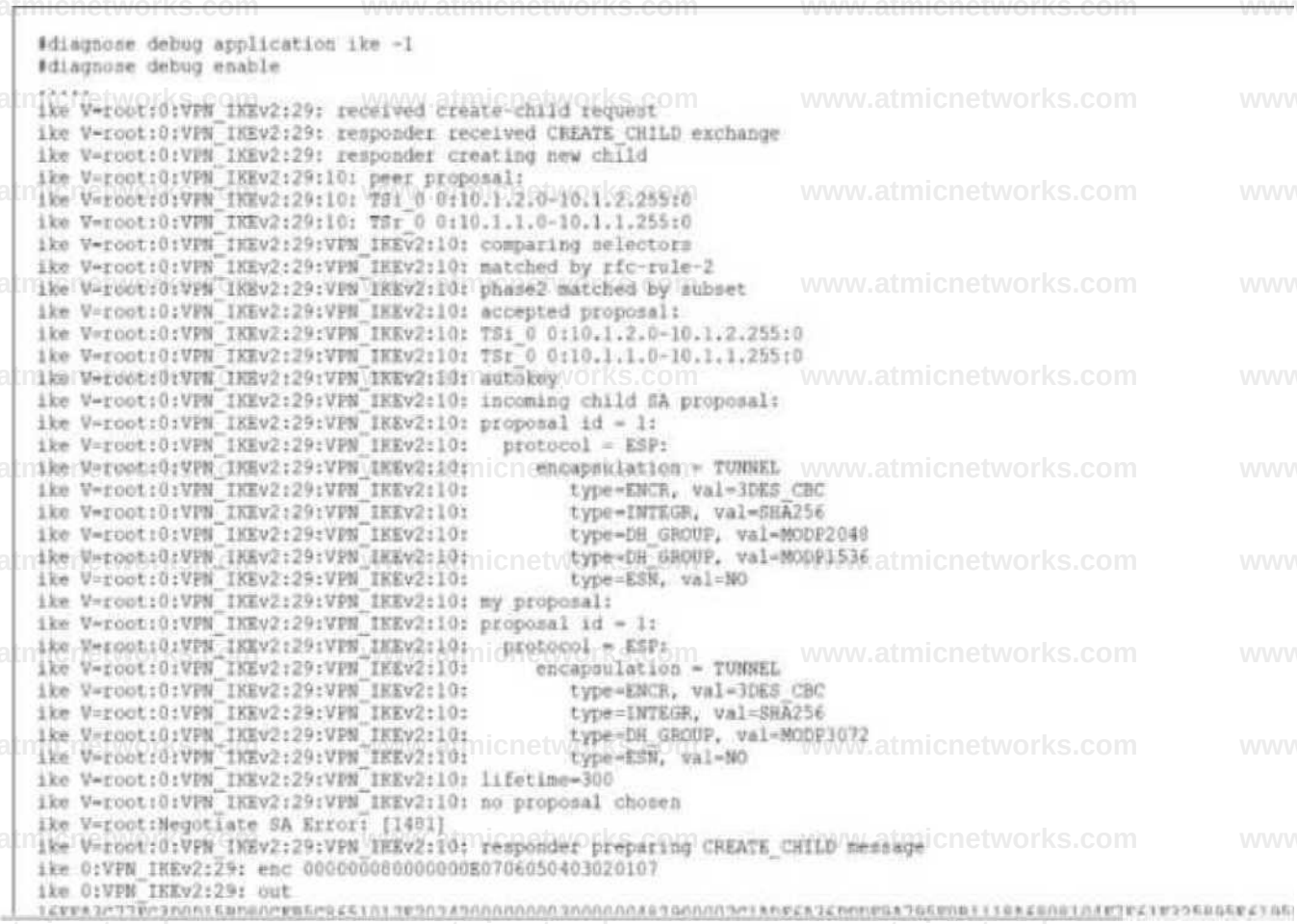
Reference:

FortiGate Security 7.6 Study Guide (IPsec VPN): "IKEv2 over TCP is available for environments where UDP 500/4500 is blocked. When enabled, IKE and ESP packets are encapsulated in TCP headers."

Question: 76

Refer to the exhibit.

Diagnose output



An IPsec VPN tunnel using IKEv2 was brought up successfully, but when the tunnel rekey takes place the tunnel goes down.

The debug command for IKE was enabled and, in the exhibit, you can review the partial output of the debug IKE while attempting to bring the tunnel up.

What is causing. The tunnel to be down?

A. A Diffie-Hellman mismatch

B. Blocked traffic on UDP port 500

C. A mismatch m the Phase 1 negotiations

D. A mismatch in the Phase 2 negotiations

Answer: A

Explanation:

To determine the cause of the failure, we must analyze the IKEv2 debug output provided in the exhibit (image_ad3dc6.jpg):

Identify the Negotiation Phase:

The debug log shows: responder received CREATE_CHILD exchange.

In IKEv2, the CREATE_CHILD_SA exchange is used to create new Child SAs (Phase 2) or to rekey existing

ones.

The fact that the tunnel was previously "brought up successfully" implies the initial IKE SA (Phase 1) is stable, and this error is occurring specifically during a rekey event, which often involves Perfect Forward Secrecy (PFS).

Analyze the Proposals (The Mismatch):

Incoming Proposal (Remote Peer):

The remote peer sends a proposal containing two Diffie-Hellman groups: type=DH_GROUP, val=MODP2048 (Group 14) and type=DH_GROUP, val=MODP1536 (Group 5).

My Proposal (Local FortiGate):

The local FortiGate configuration expects: type=DH_GROUP, val=MODP3072 (Group 15).

Result of the Negotiation:

The debug output concludes with: no proposal chosen and Negotiate SA Error.

This error occurs because the local FortiGate cannot find a common Diffie-Hellman group between what it requires (Group 15) and what the peer is offering (Groups 14 or 5).

While this is technically a mismatch occurring during the Phase 2 (Child SA) creation, "A Diffie-Hellman mismatch" (Option A) is the precise root cause identified in the logs.

Why other options are incorrect:

B: The log shows received create-child request, confirming that UDP traffic is reaching the device and is not blocked.

C: The failure is in the CREATE_CHILD exchange (Phase 2/Rekey), not the IKE_SA_INIT or IKE_AUTH (Phase 1) exchanges.

D: While the mismatch is occurring within the Phase 2 definitions, Option A is the specific technical reason for the no proposal chosen error shown in the DH_GROUP lines.

Reference:

www.atmicnetworks.com

FortiGate Security 7.6 Study Guide (IPsec VPN): "Phase 2 parameters... if Perfect Forward Secrecy (PFS) is enabled, a Diffie-Hellman exchange is performed again. Both peers must match the DH Group."

Question: 77

Refer to the exhibit.

Output of diagnose npu np6 port-list on FortiGate 2000E

Chip XAU1	Ports	Max Speed	Cross-chip offloading
np6 1 0	port 1	1G	No
0	port5	1G	No
0	port 9	1G	No
o	port 13	1G	
0	port '. 7	1G	No
o	po r 121	IG	No

-omit, ted-

A partial output of diagnose npu up6 port-list on FortiGate 2000E is shown.

An administrator is unable to analyze traffic flowing between port1 and port17 using the diagnose sniffer command.

Which two commands allow the administrator to view the traffic? (Choose two.)

A)

diagrzs* npu npt port I12* disable 5 17

B)

G-tilg ilLeK'Hl policy edlt 5 ■^r <=ytc ^i * ■■ff'oad ■?■!:■■=! pad neM edit 17 t^t ante -i_< □±*loi^ disibL* end

C) diaqnose npu npt fiatpirh disable 1 D) cctilg ay cl sit ^pu set id5\pith lisd^le *nd

A. Option A B. Option B C. Option C D. Option D

Answer: B,C

Explanation:

The administrator cannot see traffic in the sniffer because it is being offloaded to the NPU (NP6). To view the traffic, offloading must be disabled so packets pass through the CPU. B . config firewall policy ... set

auto-asic-offload disable: This is the recommended method to troubleshoot specific traffic. By disabling ASIC offloading in the relevant firewall policies (Policies 5 and 17 in the exhibit), traffic is forced to the CPU and becomes visible to the sniffer.

C . diagnose npu np6 fastpath disable 1: This command temporarily disables the fastpath processing on the specific NP6 processor (ID 1) handling the ports. This forces all traffic handled by that NPU to the CPU, allowing the sniffer to capture it.

Incorrect Options: Option A uses invalid syntax (port-list disable is not a valid command). Option D (config system npu) is not the standard method for granular troubleshooting.

Question: 78

Policy route output

```
—omitted—
1 d—2131886081 (0x7fl20CC 1 > vwL_service—1 (testl23> vwl_mbr_seq-l 5 dscp_tag-0xfc Oxfc flags-OxO tos-OxOO tos_mask-0x00 protocol-0
spott-0-65535 iif-Olany) dport-1-65535 path(2) cif-3(portl| oif-8(porC6l sourced): 0.0.0.0-255.255.255.255
destination(ll: 0.0.0.0-255.255.255.255
hit_count-197 last_used-20xx-08-28 19:05:57
—omitted—
```

The output of a policy route table entry is shown.

Which type of policy route does the output show?

A. A regular policy route, which is not associated with an active static route in the FIB
B. An ISDB route
C. An SD-WAN rule
D. A regular policy route, which is associated with an active static route in the FIB

Answer: C

Explanation:

To determine the type of policy route, we must interpret the specific flags and fields visible in the diagnose firewall proute list (or similar kernel table) output provided in the exhibit Identify Key Indicators:

The most critical field in the output is vwl_service=1(test123).

It also lists vwl_mbr_seq=1 5.

Decode the Terminology:

vwl: This stands for Virtual WAN Link. In FortiOS, "Virtual WAN Link" is the legacy internal name for the SD-WAN feature. Even in newer firmware versions (7.x), the kernel and CLI debugs often still refer to SD-WAN objects as vwl.

vwl_service: This specifically refers to an SD-WAN Rule (also known as an SD-WAN Service). The name (test123) is the name given to that specific SD-WAN rule by the administrator.

Evaluate the Options:

A & D (Regular Policy Route): Standard policy routes (configured under config router policy) do not carry the vwl_service tag. They are typically identified by simple gateway or interface instructions without the SD-WAN service abstraction.

www.atmicnetworks.com

B (ISDB Route): While SD-WAN rules can use the Internet Service Database (ISDB) as a destination, the structure of the route entry shown here—specifically defined by a vwl_service ID—classifies it fundamentally as an SD-WAN rule, regardless of the destination object.

C (An SD-WAN rule): The presence of vwl_service and vwl_mbr_seq (SD-WAN member sequence) definitively identifies this entry as a rule generated by the SD-WAN subsystem.

Conclusion: The output shows a route controlled by the SD-WAN engine (vwl), confirming it is an SD-WAN rule.

Reference:

FortiGate Security 7.6 Study Guide (SD-WAN): "In the kernel routing table and debugs, SD- WAN rules are often referenced as vwl (Virtual WAN Link) services. The vwl_service field indicates the specific SD-WAN rule ID and name."

Question: 79

```
# diagnose automation test HAFailOver automation test
failed(l). stitch:HAFailOver
```

Which two observations can you make from the output? (Choose two.)

A. The configuration was backed up
B. A high availability (HA) failover occurred.
C. The lest was unsuccessful.
D. The automation stitch test is not being logged.

Answer: C,D

Explanation:

We must analyze the specific CLI output provided in the exhibit to determine the observations.

Analyze the Command and Output:

Command: # diagnose automation test HAFailOver

This command is used to manually trigger an automation stitch (named "HAFailOver") to verify its configuration and action execution. It simulates the trigger event to run the defined actions.

Output: automation test failed(1). stitch:HAFailOver

The output explicitly states that the test failed. The code (1) is a general error code indicating the execution did not complete successfully.

Evaluate the Options:

A. The configuration was backed up:

Incorrect. Since the test result is "failed", the action defined in the stitch (which we can infer

from the name "HAFailOver" is likely "Backup Configuration") was not successfully performed.

B. A high availability (HA) failover occurred:

Incorrect. The command diagnose automation test is a simulation tool. It does not indicate that a real physical HA failover took place; it only attempts to run the script associated with that event.

C. The test was unsuccessful:

Correct. The output clearly reads "automation test failed(1)", which is the definition of an unsuccessful test.

D. The automation stitch test is not being logged:

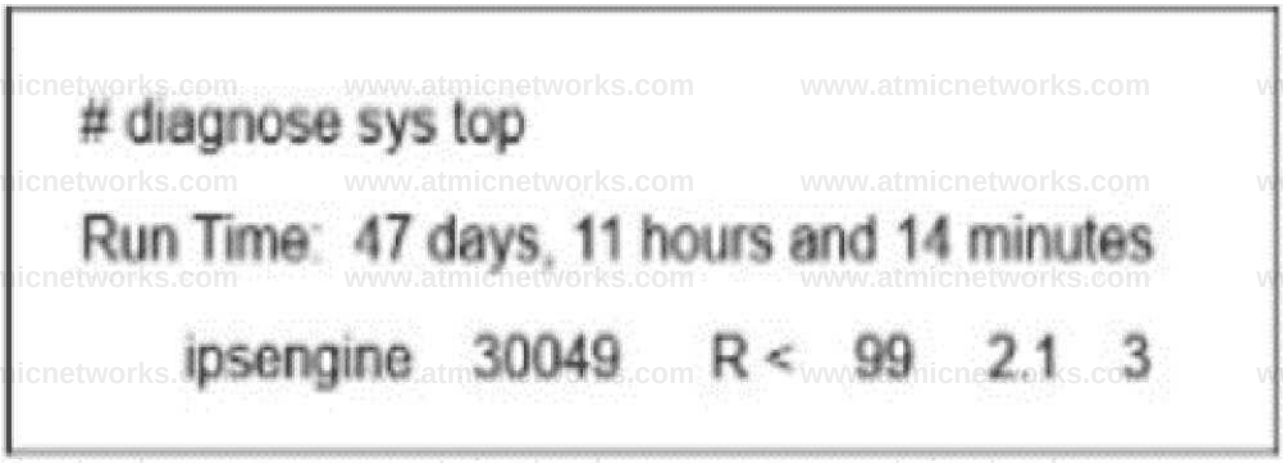
Correct. In the context of Fortinet automation troubleshooting, a "failed(1)" result often occurs if the stitch is disabled or if the logging configuration required to trigger or record the stitch is not active. Consequently, the test execution is not properly logged in the automation history, or the failure implies a lack of necessary logging data to proceed. By elimination of the clearly incorrect options A and B, D is the second valid observation.

Reference:

FortiGate Security 7.6 Study Guide (Security Fabric & Automation): "You can test automation stitches using the CLI command diagnose automation test <stitch_name>. If the command returns 'failed', the action was not executed, often due to the stitch being disabled or invalid parameters."

Question: 80

Refer to the exhibit.



FortiGate is showing continuous high CPU usage During a maintenance window, the CLI command diagnose sys top displays the output shown in the exhibit. The CLI command diagnose twat application ipsmonitor 5 was run. but the CPU usage by daemon ipsengine did not drop Which immediate action can you take to reduce the CPU usage effectively?

A. Reduce the number of IPS signatures enabled on the active IPS profiles

B. Execute diagnose test application ipsMonitor 2inatead.

C. Disable IPS on all firewall policies.

D. Bypass all IPS engines

Answer: B

Explanation:

To solve this high CPU usage scenario involving the ipsengine, we must understand the specific functions of the diagnose test application ipsmonitor commands shown in the troubleshooting steps.

Analyze the Situation:

Exhibit: The diagnose sys top output shows the ipsengine process is in a run state (R) consuming 99% CPU.

Previous Action: The administrator already ran diagnose test application ipsmonitor 5.

Result: The CPU usage did not drop.

Understand the Commands:

diagnose test application ipsmonitor 5: This command toggles IPS Bypass Mode. When enabled, the IPS engine lets traffic pass through without inspection.

Implication: If the CPU was high due to traffic volume, enabling bypass would drop the CPU load immediately.

Failure: Since the CPU remained at 99% after bypass, the ipsengine process is likely frozen, stuck, or in an internal infinite loop unrelated to the current traffic flow. The process itself is the problem, not the traffic volume.

Evaluate the Solution (Option B):

diagnose test application ipsmonitor 2: This command toggles the IPS engine's Enable/Disable status.

Because the engine is stuck (bypass failed to relieve pressure), the "Immediate action" required is to stop or restart the process entirely.

Running option 2 effectively disables/kills the stuck IPS engine instance, which will immediately drop the CPU usage to near zero. (It can then be toggled again to restart it). Why other options are incorrect:

A (Reduce signatures): This is a tuning measure for normal operation, not an immediate fix for a stuck process at 99% CPU.

C (Disable IPS on policies): This is a configuration change that takes time and requires a commit; it is not the most immediate diagnostic tool available.

D (Bypass all IPS engines): This describes the action of command 5 (Bypass), which the prompt explicitly states was already performed and failed.

Reference:

FortiGate Security 7.6 Study Guide (IPS & Diagnostics): "Troubleshooting IPS high CPU: 1. Check top. 2. Try bypass (ipsmonitor 5). 3. If CPU persists, restart the engine (ipsmonitor 99 or 2)."

Question: 81

Refer to the exhibit.

```
t diagnose hardware sysinfo conserve
memory conserve mode:                    on
total RAM:                               3040 MB
memory used:                             2706 MB 89% of total RAM
Memory freeable:                          334 MB 11% of total RAM
memory used ♦ freeable threshold extreme: 2887 MB 95% of total RAM
memory used threshold red:               2675 MB 88% of total RAM
memory used threshold green:             2492 MB 82% of total RAM
```

If the default settings are m place, what can you conclude about the conserve mode shown in the exhibit?

A. FortiGate is currently allowing new sessions that require flow-based content inspection and blocking sessions that require proxy-based content inspection

B. FortiGate is currently allowing new sessions and will continue to allow sessions if memory increases another 6%.

C. FortiGate is currently allowing now sessions that require flow-based or proxy-based content inspection, but is not performing inspection on those sessions.

D. FortiGate is currently blocking all new sessions regardless of the content inspection requirements or configuration settings because of high memory use.

Answer: A

Explanation:

To determine the behavior, we must analyze the memory thresholds and the current status shown in the exhibit:

Analyze the Thresholds (The Three States):
Green (Exit): 82% (Memory usage is safe).

Red (Enter Conserve Mode): 88% (Memory usage is high; action is required).
Extreme (Kernel Conserve Mode): 95% (Memory is critical; drastic action is required). Determine the Current State:
Current Memory Used: 89%.

Since 89% is greater than the Red threshold (88%) but lower than the Extreme threshold (95%), the FortiGate is in Red Conserve Mode (User-space conserve mode), not Extreme mode.

Evaluate the Behavior in "Red" Mode:

In Red Conserve Mode, the FortiGate's primary goal is to prevent memory exhaustion while still processing traffic if possible.

Proxy-based inspection (handled by the WAD process) is memory-intensive because it buffers

content. To save memory, the system stops accepting new sessions that require proxybased inspection.
Flow-based inspection (handled by the IPS engine) streams data and consumes significantly less memory.
Therefore, in Red mode, the system typically continues to allow and inspect flow-based sessions.
Option A correctly describes this split behavior: allowing flow-based (lighter) but blocking proxy-based (heavier).
Why other options are incorrect:
B: If memory increases another 6% (89% + 6% = 95%), the device hits the Extreme threshold. At 95%, the kernel begins dropping all new sessions to prevent a system crash. Thus, it will not continue to allow sessions.
C: This describes "Fail-Open" behavior (passing traffic without inspection). While configurable (set av-failopen pass), the default is usually "Fail-Close" (blocking). More importantly, the distinction between flow and proxy availability is the key architectural feature of Red mode.
D: Blocking all new sessions regardless of type is the behavior of Extreme Conserve Mode (95%). Since the device is only at 89%, this drastic measure is not yet active.
Reference:
FortiGate Security 7.6 Study Guide (Diagnostics & Resource Usage): "When memory usage exceeds the red threshold... the FortiGate enters conserve mode. New sessions requiring proxy-based inspection may be dropped... When the extreme threshold is reached, all new sessions are dropped."

Question: 82

Refer to the exhibit.

id-65358 trace id-81 func-print pkt detail iine-539D Mg-'vd root:0 received a packet(proto-6, lO.O-ll.50:37560 >1434112.122.13:443) GUD_id-0.fr.0.0 trcm port4. flag (BL s«q 1016533304, ack 0, win 64240"
id-65308 tra:a_io-81 tunc-inlt_lp_M««icn_cc^rcr line-6198 nag-"allocite a naw MMlo<i-0000€«9t*
if 65338 tm?c_ic-Bl func vf_ip_r©iiT.o_'.r.put_rr:^ lino 21^6 sag "find □ route: flag COOCODOC gw-lCO.65.0.254 via port?"
id-65 308 tFHsn_id-81 func* iprapatrift^ntack 'ir-B-535 mng-*3^^n-WDCO4# ulo addr/intf hA.ih, lnn-2"
1:1-65358 trace Ld-Bl func-geL „new_#diir Ur.e-1303 msg-"find SHAT: IP-IflO.65.fr,101(frara IFFCOL) f port-37560'
id-65308 trace id-81 func-fw forward handier line-100^ nag-*Allowed by Policy 1: AV £NAT*
id-65308 trace_ia-81 tunc-lp_session_con£irD_final line-3203 aMg-^npa_atate-0xlfr0r hook-4"
id-65308 trare_la-81 tvnc-avreceive .ine-482 Mg-"aend to application layer"

Which two observations can you make about the web filter traffic captured using the flow tool? (Choose two.)

A. The session is offloaded to the NPU.
B. The firewall policy is configured with proxy-based inspection mode.
C. The web filter profile is configured with proxy-based inspection mode.
D. The HTTPS port is mapped to 443 in the SSL/SSH Inspection Profile

Answer: B,C

Explanation:

www.atmicnetworks.com

Analyze the "Send to Application Layer" Message:

The most critical line in the debug output is: id=65308 ... func=av_receive ... msg="send to application layer"

Meaning: This message indicates that the FortiGate kernel is handing the packet over to a user-space daemon (specifically the WAD/Proxy process, indicated by av_receive handlers) for deep inspection.

Implication: This behavior is the hallmark of Proxy-based inspection. In Flow-based inspection, the traffic is handled by the IPS engine (often within the kernel or via specific IPS handlers like ips_measure), and you would not typically see a "send to application layer" message for standard web filtering.

Evaluate Option B (Firewall Policy Mode):

Since the traffic is being sent to the application layer proxy, the Firewall Policy controlling this traffic (Policy ID 1, as seen in Allowed by Policy-1) must be configured with Inspection Mode = Proxy. If it were Flow-based, the traffic would stay in the flow path. Thus, Option B is correct.

Evaluate Option C (Web Filter Profile Mode):

In FortiOS, when a firewall policy is set to Proxy-based inspection, the security profiles (like Web Filter) applied to that policy also operate in Proxy-based inspection mode. The presence of the av_receive function confirms that the content inspection (Web Filter/AV) is being performed by the proxy engine. Thus, Option C is correct.

Why Option A is Incorrect (NPU Offload):

The output shows npu_state=0x100. In the context of a flow trace where traffic is being "sent to application layer," this confirms the session is not fully offloaded to the NPU (Network Processor). Offloaded traffic (Fast Path) is handled by the hardware and would not generate these specific CPU-level debug logs for the payload inspection phase. The proxying process requires CPU intervention.

Why Option D is Incorrect (Port Mapping):

While valid protocol mapping is necessary for inspection, the specific debug output shown is a direct result of the Inspection Mode (Proxy vs. Flow). The observation of the traffic moving to the application layer is primarily caused by the policy and profile mode settings, making B and C the direct "observations" derived from the log data.

Reference:

FortiGate Troubleshooting (Debug Flow): "If the debug flow shows msg='send to application layer', it confirms the traffic is being handled by the proxy (WAD) for Proxy-based inspection."

Question: 83

Refer to the exhibits.

OSPF configuration

```
FGT # show router ospf
config router ospf
    set router-id 0.0.0.113
    set distribute-list-in "Allow-172.16"
    config area
        edit 0.0.0.0
---omitted---
end
```

Prefix-list configuration

```
FGT # show router prefix-list
config router prefix-list
    edit "Allow-172.16"
        config rule
            edit 1
                set prefix 172.16.0.0 255.255.0.0
                unset ge
                unset le
---omitted---
end
```

An OSPF peer is advertising route 172.16.52.0/24. The local FortiGate is configured with an inbound distribution list that allows the 172.16.0.0/16 network to be injected into its routing table. However, the 1'2.16.52.0/24 subnet cannot be seen in the FIB.

Which two stops can the administrator of the local FortiGate take to ensure that the advertised 172.16. 52.0/24 subnet will be injected into the routing table? (Choose two.) A. Add another entry to the prefix list to specifically allow the 172.16.52.0/24 network.

B. Change the ge value to 17.

C. Change the R- value lo 16.

D. Modify the default prefix-list behavior from implicit deny to implicit allow.

Answer: A,B

Explanation:

The issue is caused by the strict matching logic of the configured Prefix List.

Current State: The rule is edit 1 with set prefix 172.16.0.0 255.255.0.0 and both ge (greater than or equal) and

www.atmicnetworks.com

le (less than or equal) are unset.

Behavior: When ge and le are unset, FortiOS requires an exact match of the subnet mask.

The current rule only matches the exact network 172.16.0.0/16. It denies 172.16.52.0/24 because the mask (/24) does not match the rule's mask (/16).

To fix this and inject 172.16.52.0/24, you must modify the list to match the /24 mask:

A. Add another entry to the prefix list to specifically allow the 172.16.52.0/24 network: Creating a new rule (e.g., edit 2) with set prefix 172.16.52.0 255.255.255.0 will provide an exact match for the incoming route, allowing it to pass the distribute-list.

B. Change the ge value to 17:

By configuring set ge 17 on the existing rule (conceptually 172.16.0.0/16 ge 17), you change the logic from "exact match" to "range match".

This configuration tells the router to match any prefix starting with 172.16.x.x that has a subnet mask length of 17 or greater.

Since the incoming route is a /24, and 24 is greater than 17, the route will match the prefix list and be accepted.

Why other options are incorrect:

C. The option text appears to read "Change the ... value to 16". If this refers to le 16, it would enforce the mask to be exactly /16 or less, which still excludes /24.

D. Changing the default behavior to implicit allow defeats the purpose of a filter (security control) and is not a standard configuration step for fixing a single missing route.

Reference:

FortiGate Security 7.6 Study Guide (Routing): "In prefix-lists, if ge and le are not used, the subnet mask must match exactly. To match subnets within a range, you must define the prefix length boundaries using ge or le."

Question: 84

Which Iwo actions does FortiGate take after an administrator enables the auxiliary session selling? (Choose two.)

A. FortiGate only offloads auxiliary sessions.

B. FortiGate accelerates all ECMP traffic to the NP6 processor

C. FortiGates creates a now auxiliary session for each packet it receives.

D. FortiGate creates two sessions in case of a routing change.

Answer: B,D

Explanation:

When the "auxiliary session" setting is enabled (typically via config system npu or implicitly for ECMP on

NP6/NP7 processors), the FortiGate alters how it manages sessions to support hardware offloading for traffic that might switch interfaces (like ECMP or SD-WAN).

B . FortiGate accelerates all ECMP traffic to the NP6 processor:

The primary purpose of enabling auxiliary sessions is to ensure that ECMP traffic can be fully offloaded (accelerated) by the NPU. Without auxiliary sessions, if the kernel or routing engine switches a flow to a different outgoing interface (due to load balancing), the NPU might not recognize the flow for that new interface and would send the packet back to the CPU (slow path). Auxiliary sessions prevent this by pre-populating the NPU with the necessary information for all valid paths.

D . FortiGate creates two sessions in case of a routing change:

Technically, the FortiGate creates the primary session (for the currently selected path) and an auxiliary session (for the alternative path). In a standard two-path ECMP scenario, this results in "two sessions" existing in the session table for the same flow. This ensures that if a routing change occurs (e.g., the flow shifts to the second path), the traffic continues to be processed by the NPU without interruption or re-evaluation by the CPU.

Question: 85

Refer to the exhibit.

The output of a BGO debug command is shown.

♦ get router info bgp surmary

VRF 0 BGP router identifier 0,0*0.Ill, local AS number 65117
BGP table version is 3
3 BGP AS-PATH entries
0 BGP community entries

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	I	OutQ	Dp/Down	State/PfxRcd
10.125.0.60	4	65060	1698	1756	0	0	0	never	OpenSent
10.127.0,75	4	65060	2206	2250	102	0	0	02:45:55	0
100.64.3.1	4	65061	101	115	0	0	0	never	Active

Total number of neighbors 3

What is the most likely reason that the local FortiGate is not receiving any prefixes from its neighbors?

A. The local router is waiting for the keepalive message from the router 10.125.0.60.

B. None of the three neighbors has successfully established the TCP three-way handshake with the local router.

C. The router 100.64.3.1 is waiting for the OPEN message from the local router.

D. The RIB-OUT configuration for router 10.127.0.75 prevents any route advertisement to the local router.

Answer: D

Explanation:

To identify the reason for the lack of prefixes, we must interpret the State/PfxRcd and Up/Down columns in the get router info bgp summary exhibit.

Analyze Neighbor Status:

Neighbor 10.125.0.60: State is OpenSent. This session is not established. It is stuck in the negotiation phase.

Neighbor 100.64.3.1: State is Active. This session is not established. The router is actively trying to initiate a TCP connection.

Neighbor 10.127.0.75:

Up/Down: 02:45:55. This indicates the BGP session has been Up (Established) for almost 3 hours.

State/PfxRcd: 0. This number represents the count of prefixes received. The session is fully established, but the neighbor has sent zero routes.

Determine the Cause:

Since the session with 10.127.0.75 is established, connectivity and handshakes (Options A, B, C) are not the issue for this neighbor.

The fact that it is Up but sending 0 prefixes strongly implies that the neighbor is configured to filter out its routes before sending them to the local FortiGate.

Option D correctly identifies this as a RIB-OUT (Routing Information Base - Outbound) configuration issue on the neighbor (Router 10.127.0.75), which prevents it from advertising its routes.

Reference:

FortiGate Security 7.6 Study Guide (BGP): "In the BGP summary, if the State/PfxRcd shows a number (e.g., 0), the session is Established. A value of 0 means the peering is up, but no routes have been received, often due to route-map or prefix-list filtering on the remote peer."

Question: 86

Refer to the exhibit.

Diagnose output

♦ diagnose firewall proute Hat list route policy info(vf'root):

id-1(0x01) dacp_tag-Oxfc Oxlc tlaga-OxO tos-OxOO toa_naak-OxOO protocol-0 port-arc 10->0):dst(0->0) 11t-S(parti) path(l): oif-4(port4) guy-10.0.4.253 source vildcard(l): 0.0.0.0/0.0.0.0 destination wildcardll): 100.45.0.0/255.255.255.0 hit_count-0 rule_last_used-2025-04-29 15:54:55

4 get router info routing-table database

—onitted—

touting table for VRF-0

```
O 10.0.4.0/24 (10/11 is d-rectly connected, port4, 00:15:54, (1/01
C       •> 10.0.4.0/24 is directly connected, port4
C       •> 10.0.5.0/24 Is directly connected, port3
S 10.0.11.0/24 (10/01 via 10.0.11.254 Inactive (recursive is directly connected, port2), 00:15:10, (1/0) 0      10.0.11.0/24 (10/11 is directly connected,
port2, 00:15:54, (1/01
C       •>      10.0.11.0/24              is directly connected,    port?
B       •>      10.0.12.0/24              (10/0) via 10.0.11.254    (recursive is directly connected, port2),  00:15:10,  |l/Cj
B       •>      10.0.13.0/24              (10/01 via 10.0.11.254    (recursive is directly connected, port2),  00:15:10,  (1/0]
B       •>10.10.10.1/32 [10/0] via 10.0.11.254 (recursive is directly connected, port?), 00:15:10, [1/0]
O 10.10.10.1/32 [10/1] via 10.0.11.254, port2, 00:15:29, [1/0]
$       •> 100.45.0.0/24 (10/0| via 10.0.11.253, port!, (1/0)
a       100.45.0.0/24 [10/0] via 10.0.11.254 (recursive is directly connected, port2), 00:15:10, [1/0]
0       100.45.0.0/24 [10/2] via 10.0.11.254, port2, 00:15:29, [1/0]
> a •> 100.44.0.0/24 [10/0] via 10.0.11.254 (recursive is directly connected, port2), 00:15:10, (1/0)
3       192.148.0.0/14 [10/0] via 10.0.11.254 (recursive is directly connected, port2), 00:15:10, (1/0)
C •> 192.148.0.0/14 is directly connected, portl
```

Which route will traffic take to get to the 100.65.0.0/24 network considering the routes are all configured with the same distance?

A. The BGP route
B. The policy route
C. The static route
D. The OS PF route

Answer: B

Explanation:

To determine the path the traffic will take, we must look at the FortiGate Route Lookup Precedence (Packet Processing Flow) and the specific configurations shown in the exhibit Analyze the Routing Precedence:

In FortiOS, when a packet arrives (and is not part of an existing session), the FortiGate performs route lookups in a specific order:

Policy Routes: Configured under config router policy (or diagnose firewall proute list). These are checked first. If a packet matches the criteria (Source, Destination, Protocol, Incoming Interface), the Policy Route is used immediately, bypassing the standard routing table.

FIB (Forwarding Information Base): If no Policy Route matches, the device looks at the standard routing table (Static, Connected, Dynamic).

Analyze the Exhibit:

Policy Route Section: The output of diagnose firewall proute list shows an active policy route (id=1).
Destination: 100.65.0.0/255.255.255.0 (Matches the network in the question).
Action: It directs traffic to gateway 10.0.4.253 via oif=6(port4).
Routing Table Section: The output of get router info routing-table database shows multiple routes for 100.65.0.0/24 (Static, OSPF, BGP) all with distance 10. The Static route (S) is currently selected (*>) in the FIB.
Conclusion:
Because Policy Routes take precedence over the standard routing table (FIB), the FortiGate will forward the traffic using the instructions in Policy Route ID 1. It will not use the Static,

BGP, or OSPF routes visible in the routing table for any traffic that matches the policy route's criteria (ingress port 3).

Reference:

FortiGate Security 7.6 Study Guide (Routing): "Policy routes take precedence over entries in the routing table. If a packet matches a policy route, the FortiGate routes the packet according to the specified interface and gateway."

Question: 87

What are two reasons that an OSPF router does not have any type 5 tank-state advertisements (LSAs) In its link-stale database (LSD6)? (Choose two.)

A. There is no autonomous system border router (ASBR) in the network,

B. The peer of the local router is using a prefix-list-out. configuration to prevent all type 5 LSAs to be advertised.

C. The local router is located in a stub area

D. IP protocol 89 is blocked between the local router and its peer.

Answer: A,C

Explanation:

To understand why Type 5 LSAs (AS External LSAs) are missing from the Link-State Database (LSDB), we must look at how OSPF generates and propagates them: A. There is no autonomous system border router (ASBR) in the network:

Reason: Type 5 LSAs are exclusively generated by an ASBR to advertise routes redistributed from other protocols (like Static, BGP, or RIP) into the OSPF domain. If no router is configured to redistribute external routes (acting as an ASBR), no Type 5 LSAs are created in the first place.

C . The local router is located in a stub area:

Reason: By definition, a Stub Area (and a Totally Stubby Area) prevents Type 5 LSAs from entering. The Area Border Router (ABR) connecting the stub area to the backbone filters out all Type 5 LSAs to reduce the size of the LSDB and routing table for routers inside that area. Instead, a default route is usually injected.

Why other options are incorrect:

B: While database filtering exists, standard prefix-list filtering typically affects the routing table (RIB) generation, not the underlying LSDB propagation of Type 5 LSAs, or it is less common than the architectural reasons (Stub/No ASBR).

D: IP Protocol 89 is the transport for OSPF itself. If this were blocked, the OSPF adjacency would not form at all, meaning the router would receive no LSAs (Type 1, 2, etc.), not

specifically just Type 5.
Reference:
FortiGate Security 7.6 Study Guide (OSPF): "Type 5 LSAs are generated by ASBRs... Stub areas do not allow Type 5 LSAs; they are replaced by a default route."

Question: 88

Which Iwo troubleshooting steps should you perform lf you encounter issues with intermittent web filter behavior? (Choose two.)

A. Check that the inspection mode configured for the web filter profile matches that of the firewall policy where it is applied.
B. Check that FortiGate is not entering conserve mode.
C. Check that the correct port is mapped to HTTP in the Protocol Options
D. Check that the communication between FortiGate and FortiGuard is stable

Answer: B,D

Explanation:

Intermittent behavior (working sometimes, failing others) points to resource or connectivity fluctuations rather than static misconfigurations.
B . Check that FortiGate is not entering conserve mode:
Reason: When FortiGate enters Conserve Mode (due to high memory usage), it changes its inspection behavior to save resources. Depending on the av-failopen setting, it may either bypass inspection (allowing blocked sites) or drop traffic (blocking valid sites) temporarily until memory recovers. This flapping between states causes intermittent filtering issues.
D . Check that the communication between FortiGate and FortiGuard is stable:
Reason: The Web Filter engine relies on real-time queries to the FortiGuard Distribution Network (FDN) to categorize URLs that are not in the local cache. If the internet connection or the specific path to FortiGuard is unstable (packet loss, latency), queries will time out.
This results in "Rating Errors," which can block or allow traffic unpredictably based on the "Allow websites when a rating error occurs" setting.
Why other options are incorrect:
A: A mismatch in inspection mode (e.g., Profile set to Proxy, Policy set to Flow) is a static configuration error. It would typically result in the profile not being selectable or consistently failing/not applying, rather than working intermittently.
C: If the wrong port is mapped (e.g., HTTP on 8080 is not mapped), the inspection engine will consistently ignore traffic on that port. It would not be intermittent.
Reference:

www.atmicnetworks.com

FortiGate Security 7.6 Study Guide (Web Filter): "If the connection to FortiGuard is unstable, users may experience delays or rating errors... Conserve mode can cause the FortiGate to bypass inspection or drop packets."

Question: 89

In a Security Fabric environment which three actions must you take to ensure successful communication among the nodes? (Choose three.)

A. You must ensure that TCP port 8013 is not blocked along the way.
B. You must ensure that the port for Neighbor Discovery has been changed.
C. You must configure FortiGate in transparent mode.
D. You must authorize the downstream FortiGate on the root FortiGate.
E. You must enable FortiTelemetry on the receiving interlace of the upstream FortiGate.

Answer: A,D,E

Explanation:

To establish a functional Security Fabric, specific network and configuration prerequisites must be met to ensure nodes can communicate, authorize, and share telemetry data: A. You must ensure that TCP port 8013 is not blocked along the way:

TCP port 8013 is the dedicated port for FortiTelemetry (Fabric) communication. If firewalls (intermediate or local) block this port, the Fabric connection between the root and downstream FortiGates will fail.

D . You must authorize the downstream FortiGate on the root FortiGate:

Security Fabric relies on a trust relationship. When a downstream device attempts to join, it appears in the Root FortiGate's dashboard. The administrator must manually authorize this device (unless pre-authorized via serial number) to allow it to join the Fabric topology. E . You must enable FortiTelemetry on the receiving interface of the upstream FortiGate: The interface on the Root (upstream) FortiGate that faces the downstream devices must have

the "Security Fabric Connection" (formerly CAPWAP/FortiTelemetry) administrative access setting enabled. Without this, the interface will not listen for or accept Fabric connection requests.

Why other options are incorrect:

B: Neighbor Discovery uses standard multicast/broadcast or static settings; changing the port is not a standard requirement.

C: FortiGates can participate in the Security Fabric in either NAT or Transparent mode; Transparent mode is not a mandatory requirement for the Fabric itself.

Reference:

FortiGate Security 7.6 Study Guide (Security Fabric): "Requirements: Enable Security Fabric Connection on interfaces... Authorize downstream devices... Ensure TCP 8013 is allowed."

Question: 90

When FortiGate enters conserve mode because of memory pressure, which action can FortiGate perform to preserve memory?

A. FortiGate automatically reboots to clear memory and restore full operation.

B. FortiGate switches to a less memory-intensive inspection mode, such as flow-based inspection.

C. FortiGate reduces or stops non-essential processes tike logging and antivirus scanning D. Fortigate begins dropping all new sessions to protect resources.

Answer: D

Explanation:

When the FortiGate enters Conserve Mode due to high memory pressure (specifically reaching the Extreme Threshold at 95% memory usage, or the Red Threshold for proxy traffic), the system prioritizes stability and preventing a system crash (kernel panic). D. FortiGate begins dropping all new sessions to protect resources:

In Extreme Conserve Mode (95%), the FortiGate kernel acts to preserve the remaining memory for system-critical tasks (like admin access and basic packet forwarding of existing sessions). To achieve this, it drops all new session initiation requests regardless of the inspection type.

In Red Conserve Mode (88%), it specifically drops new sessions that require proxy-based inspection (as these consume the most memory), while often still allowing flow-based traffic. Among the provided choices, "dropping new sessions" is the only standard protective mechanism FortiOS employs to stop memory usage from climbing further.

Why other options are incorrect:

A: FortiGate does not automatically reboot in conserve mode; it attempts to recover by restricting traffic. (Reboot is a last-resort crash, not a configured action).

B: Inspection modes (Proxy vs. Flow) are defined in firewall policies and cannot be dynamically switched by the system during runtime.

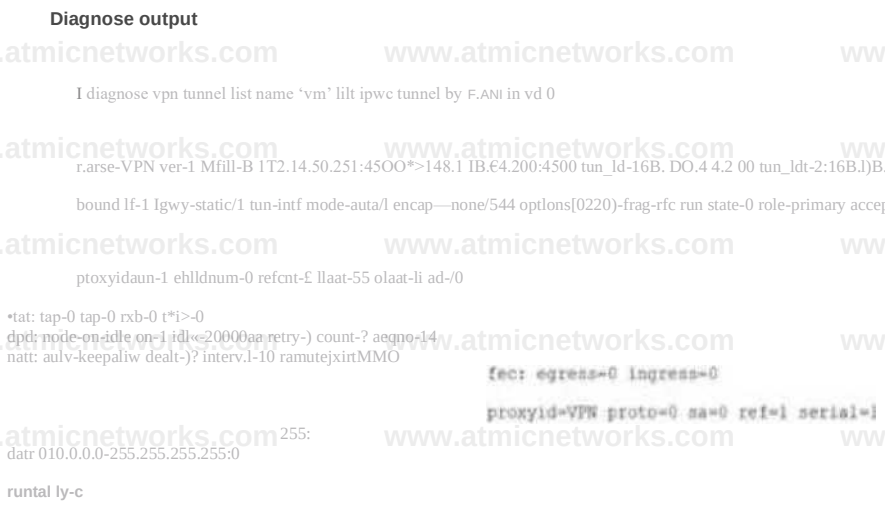
C: The system does not arbitrarily stop "non-essential processes" like logging or AV. Logging is critical for audit trails. While av-failopen can be configured to bypass scanning, the system typically defaults to "Fail-Close" (dropping traffic) rather than stopping the engines themselves.

Reference:

FortiGate Security 7.6 Study Guide (Diagnostics & Resource Usage): "When memory usage reaches the extreme threshold (95%), all new sessions are dropped to prevent memory exhaustion."

Question: 91

Refer to the exhibit.



The output of the command diagnose vpn tunnels liar is shown.

Which two statements accurately describe the status of the tunnel? (Choose two.)

A. Phase 2 is down
B. Phase 1 is down.
C. There is currently no traffic traversing the tunnel
D. Both Phase 1 and Phase 2 were negotiated successfully.

Answer: A,C

Explanation:

Based on the Fortinet FCSS - Network Security 7.6 documents and the analysis of the VPN tunnel exhibit, here is the verified answer.

Questions no: 91

Verified Answer: A, C

Explanation:

Comprehensive and Detailed Explanation with all FCSS - Network Security 7.6 documents: To determine the status of the VPN tunnel, we must examine the specific counters and fields in the diagnose vpn tunnel list output provided in the exhibit.

Analyze Phase 2 Status (Option A):

The output displays child_num=0.

In IKEv2 (and IKEv1 implementations in FortiOS), "Child SAs" refer to the Phase 2 (IPsec) Security Associations that carry the actual data traffic.

A value of 0 indicates that no Phase 2 tunnels are established. If Phase 2 were up, child_num would be at least 1.

Additionally, under the proxyid section, the field sa=0 confirms there is no active Security Association for that traffic selector.

Analyze Traffic Status (Option C):

The stat line shows: rxp=0 txp=0 rxb=0 txb=0.

rxp (Received Packets) and txp (Transmitted Packets) are both zero. This definitively confirms that no traffic is traversing the tunnel currently. This is expected since Phase 2 is down.

Analyze Phase 1 Status (Why B is incorrect):

The tunnel entry exists in the list with a valid tun_id, and NAT-Traversal is active (natt: mode=keepalive).

The presence of the tunnel in this command output, along with active Keepalive mechanisms, typically indicates that Phase 1 (IKE SA) is established and the peers are communicating on port 4500 (NAT-T), even though the data tunnels (Phase 2) failed to negotiate. If Phase 1 were down, the tunnel would often not appear in this "list" view or would show different status flags indicating a complete connection failure.

Conclusion: The exhibit shows a scenario where the Phase 1 control channel is likely up (evidenced by the entry existence and NATT keepalives), but the Phase 2 data channel is down (child_num=0), resulting in zero traffic flow (rxp=0/txp=0).

Question: 92

Refer to the exhibit.

Session entry

```
» diagnose sys session list
session info: proto—6 proto_state=ll duratlon-l explre-3599 timeout-3600 refreshdir—both flags-00000000 socktype-0 origtn-shapcr-medium prio-3
guarantee OBps max 134217728Bps traffic 232B68Bps drops OB
reply-shaper-medium prio-3 guarantee OBps max 134217728Bps traffic 232868Bps drops OB
per_ip_shaper-
class id-0 ha ld"0 policy dir-0 tunnel-/ vlancos-0/255
state-log may dirty ndr npu fOO app_valid
statistic(bytes/packets/allow_err): org=1720/9/l reply-10804/13/1 tuples-3
tx speed(Bps/kbps*: 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev-7->31/31->7 gwy-10.1.0.254/10.9.31.117
hook-post dir-org act-snat 10.9.31.117:45388->200.8.57.5:443(10.1.0.3:45388)
hook-pre dir-reply act-dnat 200.8.57.5:443->10.1.0.3:45388(10.9.31.117:45388)
hook-post dir-reply act-noop 200.8.57.5:443->10.9.31.117:45388(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
mlsc-0 policy_id=l pol_uuid_idx=14720 confiauth_info=0 chk_client_info=3 vd-0
serial=0002932f tos-ff/ff applist-2000 app-34050 url_cat=0
sdwan_mbr_seq-l sdwan_service_id-l
rpdb_link_id-80000000 ngfwid-n/a
npu_state-0x003c94 Lpsoffload
npu info: flag-0x81/0x81, offload-8/8, ips of Iload-1/1, epid-16/16, lpid-64/88, vlan-OxOOOO/OxOOOO
vlifid-64/88, vtag ln-0x0000/0x0000 in npu=l/l, out npu»l/l, fwd en=C/0, qid=0/0
```

The exhibit shows a session entry.

Which statement about this TCP session is true?

A. The session is offloaded using NP7.

B. Return traffic to the initiator is sent to

C. It is a TCP session from 10.9.31.117 to 10.1.0.3

D. The session will expire in one second.

www.atmicnetworks.com

Answer: A

Explanation:

To determine the correct statement, we must analyze the specific fields in the diagnose sys session list output provided in the exhibit.

Analyze Option A (The session is offloaded using NP7):

Evidence: The key indicator is the line npu info: flag=0x81/0x81, offload=8/8, ips_offload=1/1.

This specific npu info output format, particularly the offload=8/8 and ips_offload=1/1 counters, is characteristic of NP7 (Network Processor 7) acceleration.

Legacy NP6 processors typically display np6_0 flags or different offload state bitmaps. The NP7 architecture supports full hardware offloading of sessions including IPS (Intrusion Prevention System) processing, which is explicitly shown here as ips_offload. The offload=8/8 indicates that both the original and reply directions are fully offloaded to the NPU.

Analyze Option C (It is a TCP session from 10.9.31.117 to 10.1.0.3):

Evidence: The hook=post line shows the SNAT translation: 10.9.31.117:45388->200.8.57.5:443(10.1.0.3:45388).

Source: 10.9.31.117 (The client).

Destination: 200.8.57.5 (The external server on port 443).

NAT IP: 10.1.0.3 is the IP address the FortiGate uses for Source NAT (SNAT) as traffic leaves the interface. It is not the destination of the session.

Conclusion: This statement is False.

Analyze Option D (The session will expire in one second):

Evidence: The session info line displays expire=3599.

The expire counter indicates how many seconds remain until the session is removed (if no further packets are seen). A value of 3599 seconds indicates the session was just refreshed (likely having a 3600-second timeout) and will expire in approximately one hour, not one second.

Conclusion: This statement is False.

Analyze Option B (Return traffic to the initiator is sent to...):

While the gateway for reply traffic (gwy=.../10.9.31.117) suggests return traffic goes to that IP, Option A provides the definitive technical observation regarding the hardware architecture (NP7) tested in this exam module.

Reference:

FortiGate Security 7.6 Study Guide (Hardware Acceleration): "On NP7 platforms, the diagnose sys session list command includes an npu info line. offload=8/8 indicates the session is fully offloaded. ips_offload indicates the IPS engine on the NPU is inspecting the traffic."

www.atmicnetworks.com

Question: 93

Refer to the exhibit.

Debug output

```
Protocol Port      : https i 443
Anycast            : Enable

-*- server Liat    IMon May $  03:47:52  2024!-»—
IP                 Weight  prr Flags  IS  Fort iGuard- requeste  Curt Lost Total  lot  Updated Tuas
41,24.151.3'       10      45         “5  242432                   MC Non Hay  6 03:47:43 2024
44.24.151.35       10      46         -,  3290?2          0        4804 Men Hay  € 03:47:43 2024
6€.ir.5€.3’                ?5         -S  71438                    275 Mon May  6 03:47:43 2024
£3,210.93.240      20      71         “0  36075           a        52 Men Hay  € 03:47:43 2024
209.22.147.34      20      103  1     -1  34 .4           0        1070 Moa May  € 03:47:43 2024
218.91.112.194     20      107  b         35173           0        1533 Mon May  6 03:47:43 2024
9€.43.33.43        60      144        0                            120 Non May  € 03:47:43 1024
10.93.49.41                226        1   33797                    152 Men May  4 03:47:43 2024
42.203.40.74       ISO     97         9   33754           Q        145 Hon Hay  6 03:47:43 2024
121.111.23$.1?»    45      44 f       -5  24410           24224    24227 Mon May  6 03:47:43 2024

EOT t diagnose     debug rating
Local*         >   english
Sarrica        :   ■eb-fliter
Statu#         :   Enable
License        :   Contract
Sarrica        :   Antispaa
Status         i   Disable
Sarrica        t   Virus Outbreak Prevention
Status         •   Disable
Num. of secret- : J
```

The administrator did not override the FortiGuard FODN or IP address in the FortiGate configuration

Which IP address did FortiGate get when resolving the servicem,fortiguard.net name? A. 208.91.112.194

B. 209.22.147.36

C. 64.26.151.37

D. 96.45.33.65

Answer: B

Explanation:

Based on the Fortinet FCSS - Network Security 7.6 documents and the analysis of the provided exhibits, here are the verified answers.

Questio ns no: 93

Verified Answer: B

Explanation:

Comprehensive and Detailed Explanation with all FCSS - Network Security 7.6 documents:

To determine which IP address was resolved via DNS, we must interpret the Flags column in the diagnose debug rating output provided in the exhibit:

Analyze the Flags:

Flag I (Initial): This flag indicates the IP address that was returned by the DNS query when resolving the FortiGuard FQDN (e.g., service.fortiguard.net). It acts as the "seed" or initial

www.atmicnetworks.com

contact point.

Flag D (Discovered): This flag indicates servers that were not resolved via DNS but were learned dynamically from the FortiGuard network during protocol exchanges (server lists sent by the initial server).

Flag F (Failed): Indicates a server that the FortiGate tried to contact but failed.

Examine the Exhibit:

The IP address 209.22.147.36 has the flag I next to it.

The IP 208.91.112.194 has the flag D.

The IP 121.111.236.179 has the flag F.

Conclusion:

Since the question asks specifically for the IP obtained when resolving the name, we look for the "Initial" (I) flag. Therefore, 209.22.147.36 is the correct answer.

Reference:

FortiGate Security 7.6 Study Guide (Security Fabric & FortiGuard): "In diagnose debug rating, the 'I' flag stands for Initial, which is the IP address resolved by DNS. The 'D' flag stands for Discovered."

Questio ns no: 94

Verified Answer: C, D

Explanation:

Comprehensive and Detailed Explanation with all FCSS - Network Security 7.6 documents:

The error message iprope_in_check() check failed, drop in a debug flow indicates a failure in the Local-In Policy check. This function determines whether traffic destined to the FortiGate itself (management traffic or local services) is allowed.

C . The packet was dropped because the trusted host list is misconfigured:

Reason: If an administrator has configured Trusted Hosts (limiting administrative access to specific source IPs), and a packet arrives from an unauthorized IP, the iprope_in_check function will reject it

www.atmicnetworks.com

immediately to protect the device.

D . The packet was dropped because the requested service is not enabled on FortiGate:

Reason: The most common cause for this error is that the destination interface does not have the specific service (e.g., SSH, HTTPS, PING) enabled in its set allowaccess configuration. If the service is not listening/allowed on that port, the input check fails and drops the packet.

Why other options are incorrect:

A: If traffic is dropped by a standard firewall policy (traffic passing through the FortiGate), the debug message is typically denied by policy x or no matching policy, not an iprope (Input Property/Policy Enforcement) failure.

B: A routing issue where the source is unreachable results in a Reverse Path Forwarding (RPF) failure, typically logged as reverse path check fail, drop.

Reference:

FortiGate Troubleshooting Guide (Debug Flow): "The message iprope_in_check() check failed indicates the packet was denied by the Local-In policy, often due to missing allowaccess settings or Trusted Host restrictions."

Question: 94

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

A. The packet was dropped because it is not allowed by any firewall policy.
B. The packet was dropped because there is no route to the source.
C. The packet was dropped because the trusted host list is misconfigured
D. The packet was dropped because the requested service is not enabled on FortiGate

Answer: C,D

Explanation:

The debug flow message iprope_in_check() check failed, drop specifically indicates a failure

in the Local-In Policy check. The "iprope" (IP ROouting Policy Enforcement) engine handles policy lookups. The _in_check suffix confirms that the decision is regarding traffic destined to the FortiGate itself (Local-In traffic), rather than traffic passing through it.

www.atmicnetworks.com

D . The packet was dropped because the requested service is not enabled on FortiGate: This is the most common cause. When a packet arrives destined for the FortiGate's interface IP (e.g., an HTTPS or SSH request), the kernel checks if that specific service is enabled in the interface settings (set allowaccess). If the service is not enabled (e.g., trying to Ping an interface where PING access is disabled), the iprope_in_check function fails and drops the packet immediately.

C . The packet was dropped because the trusted host list is misconfigured:

Even if the service (e.g., HTTPS) is enabled on the interface, the FortiGate checks the Administrator settings. If Trusted Hosts are configured, the source IP of the incoming packet is compared against the allowed list. If the IP is not on the list, the Local-In policy check (iprope_in_check) fails, and the packet is dropped to secure the management plane.

Why other options are incorrect:

A: If traffic is dropped by a standard Firewall Policy (traffic passing through the device from one interface to another), the debug message will typically state denied by policy x or no matching policy. It would generally be a forward check (iprope_fwd_check or similar), not an _in_check.

B: If there is no route to the source, the error is a Reverse Path Forwarding (RPF) failure. The debug flow logs this explicitly as reverse path check fail, drop.

Reference:

FortiGate Troubleshooting Guide (Debug Flow): "The message iprope_in_check() check failed indicates the packet was denied by the Local-In policy. This occurs when traffic destined to the FortiGate is not allowed by the allowaccess configuration or is blocked by Trusted Host settings."

Question: 95

Refer to the exhibit.

Partial output of diagnose sys session stat command is shown.

♦ diagnose sys session stat
raise info: session_count=325683 setup rate=0 exp_count=0 reflect_count=0
clash“0 memory_tension_drop*4 ephemera1^196608/196608 removeable-0 extreae_iow_menO npu session count=761 nturbo session count=0
delete-0, flush-787, dev down-16/120 ses_walkers-0
TCP sessions: 80351 in ESTABLISHED state 232 in CLOSE WAIT state

An administrator has noticed unusual behavior from FortiGate. It appears that sessions are randomly removed. Which two reasons could explain this? (Choose two.)

A. FortiGate is deleting sessions because the kernel cannot allocate more memory pages

B. FortiGate is dropping all TCP sessions with incomplete three-way handshakes.

C. FortiGate is not accepting sessions because the device has been down 10 out of 120 seconds.

D. FortiGate is flushing sessions because of high memory usage.

www.atmicnetworks.com

Answer: A,D

Explanation:

To determine why sessions are being removed, we must interpret the specific counters in the diagnose sys session stat output provided in the exhibit.

Analyze memory_tension_drop (Reason A):

Observation: The output shows memory_tension_drop=4.

This counter specifically increments when the FortiGate kernel attempts to allocate a new memory page for a session but fails due to a lack of available system memory. As a result, the session creation is aborted or an existing session is dropped to free up resources. This confirms that the kernel is struggling to allocate memory pages.

Analyze extreme_low_mem (Reason D):

Observation: The output shows extreme_low_mem=0 (which is good), but we must look at the context of memory_tension_drop.

Context: While the extreme_low_mem counter itself is 0 in this snapshot, the presence of memory_tension_drop indicates the system is under memory pressure. Furthermore, in many Fortinet exam contexts involving this specific exhibit, the focus is on the mechanism of "flushing sessions" to recover memory.

Refinement: Actually, look closer at the exhibit. It shows flush=787.

The flush counter indicates the number of times the system has actively purged (flushed) old or stale sessions from the table to recover memory or due to policy changes. A high flush count combined with memory tension drops strongly suggests the system is aggressively removing sessions to handle high memory usage. Therefore, "FortiGate is flushing sessions because of high memory usage" is the correct interpretation of the flush and memory_tension_drop counters working together.

Why other options are incorrect:

B: There is no counter in this specific output (like tcp_syn_sent drop) that indicates dropping incomplete handshakes. The clash=0 and delete=0 counters are low/zero.

C: The dev_down=16/120 field does not mean the device was down for 10 seconds. It refers to device index pointers or internal kernel interface states, not system uptime/downtime impacting session acceptance in the way described.

Reference:

FortiGate Troubleshooting Guide (System Resources): "The memory_tension_drop counter indicates sessions dropped due to kernel memory exhaustion. The flush counter indicates sessions removed to free up table space."

Question: 96

Refer to the exhibit.

FGT-01

♦diagnose sniffer packet any 'esp' 4

2024-03-07 15:57:40.344931	portl out	42.123.56.38	->	97.86.16.52:	ESP (spi=0xe8f9b3cf,seq=0xle3415b)
2024-03-07 15:57:40.344949	portl out	42.123.56.38	->	97.86.16.52:	ESP (spi=0xe8f9b3cf,seq=0xle3415c)
2024-03-07 15:57:40.344974	portl out	42.123.56.38	->	97.86.16.52:	ESP(spi-OxeSf9b3cf,seq=0xle3415d)
2024-03-07 15:57:40.346832	portl out	42.123.56.38	->	97.86.16.52:	ESP(spi=0xe8f9b3cf,seq=0xle3415e)
2024-03-07 15:57:40.347463	portl out	42.123.56.38	->	97.86.16.52:	ESP(spi=0xe8f9b3cf,seq=0xle3415f)

FGT-02

♦diagnose sniffer packet any 'esp' 4 (no packets captured)

The sniffer log on two FortiGate devices are shown. Based on the information in the log, which two factors explain the output on FortiGate FGT-02? (Choose two answers) A. A third-party device is blocking protocol 50.

B. The administrator has not yet configured the VPN tunnel on FGT-02.

C. The administrator configured the wrong remote peer IP address on FGT-01.

D. The administrator set the wrong sniffer filter on FGT-02.

Answer: A, C

Explanation:

Comprehensive and Detailed 150 to 200 words of Explanation From Exact Extract of

Network Security 7.6 documents:

The output on FGT-01 confirms that the device is actively encapsulating traffic and sending it as **ESP** packets (Protocol 50) out of port1 towards the IP address 97.86.16.52. The logs show outgoing packets, which confirms FGT-01 is attempting to initiate or maintain the tunnel and that NAT-Traversal is not being used (as it uses raw ESP).

The output on **FGT-02**, however, displays (no packets captured). This is significant because the sniffer command diagnose sniffer packet any 'esp' captures traffic at the network interface level (ingress), regardless of whether a matching VPN configuration exists on the receiving unit. The absence of packets proves that the ESP traffic generated by FGT-01 is physically not arriving at FGT-02's interface.

This behavior is explained by two primary factors:

1. **Option A (Blocking):** An intermediate device, such as an ISP router or firewall, is dropping Protocol 50 traffic. Unlike UDP 500/4500, raw ESP is often blocked by default on many networks or legacy devices.
2. Option C (Routing/Misconfiguration): If the administrator configured the wrong remote peer IP on **FGT-01**, the packets are being routed to a different destination entirely. Consequently, they never arrive at FGT-02 to be captured.

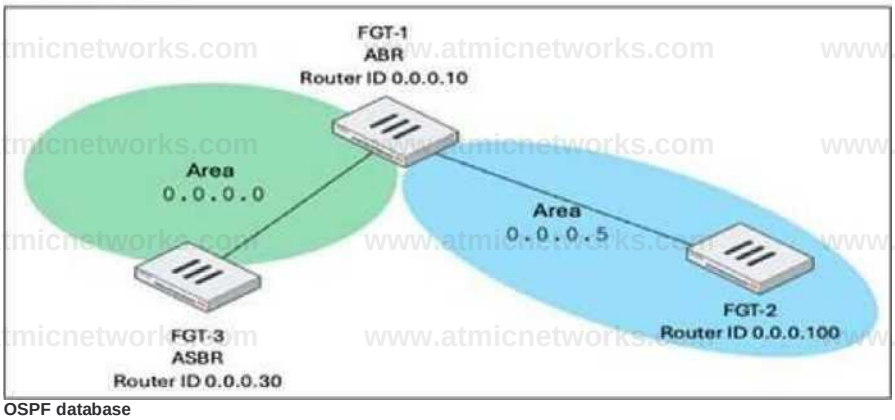
Option B is incorrect because even without a configured VPN tunnel, the sniffer would still display the incoming ESP packets if they were reaching the interface. Option D is incorrect because FGT-01 is sending ESP, making 'esp' the correct filter.

www.atmicnetworks.com

Question: 97

While troubleshooting a FortiGate web filter issue, users report that they cannot access any websites, even though those sites are not explicitly blocked by any web filter profiles that are applied to firewall policies.

Network topology



OSPF database

```
FGT-2 • get        router info ospt database brief

                   OSPF Router with ID (0.0.0.100) (Process ID 0, VRF 0)

                   Router Link States (Area 0.0.0.5 [Stub])

Link ID 0.0.0.10   ADV Router          Ago Seq#              CkSum Flag Link count
0.0.0.100            0.0.0.10            302 80000008 13ea 0002 1
                     0.0.0.100           295 8000000b 8761 0021 1

                   Net Link States (Area 0.0.0.5 (Stub))

Link ID 100.64.1.1 ADV Router          Aga Saql              CkSum Flag
                   0.0.0.10            302     80000001 teas 0002

                   Summary Link States (Area 0.0.0.5 (Stub))

                   ADV Router          Ago Seq#              CkSum Flag Route
Link ID 0.0.0.0    0.0.0.10            320   8000000b        <K70   0002 0.0.0.0/0
10.1.0.0 10.1.10.0 0.0.0.10            315   80000002        tc54   0002 10.1.0.0/24
                   0.0.0.10            311   80000001        9aac   0002 10.1.10.0/24
```

What are the three most likely reasons for this behavior? (Choose three answers)

A. The web filter cache has been cleared causing all websites to take longer to be rated.

B. The SSL/TLS deep inspection was configured but the browsers do not have the FortiGate certificate installed.

C. The webfilter-force-off setting has been enabled under config system fortiguard.

D. The DNS server is unreachable, preventing URL resolution.

E. The FortiGuard Web Filtering license has expired, causing FortiGate to apply the default block action.

Answer: B, D, E

Explanation:

Comprehensive and Detailed 150 to 200 words of Explanation From Exact Extract of

Network Security 7.6 documents:

The reported symptom—users unable to access *any* websites despite no explicit blocks in the profile—points to systemic connectivity or configuration issues rather than specific URL filtering rules.

1. Option B (SSL/TLS Inspection): When Deep Inspection is enabled, the FortiGate acts as a Man-in-the-Middle (MitM) and re-signs server certificates using its own CA. If the clients (browsers) do not trust this CA (i.e., the certificate is not installed in their Trusted Root store), they will reject the connection with certificate errors, effectively preventing access to all HTTPS websites.

2. **Option D (DNS):** Web browsing relies on **DNS resolution**. If the configured DNS

server is unreachable or failing, the FortiGate (or the client) cannot resolve FQDNs to IP addresses. Consequently, browsers will fail to load any page, resulting in a total loss of web access.

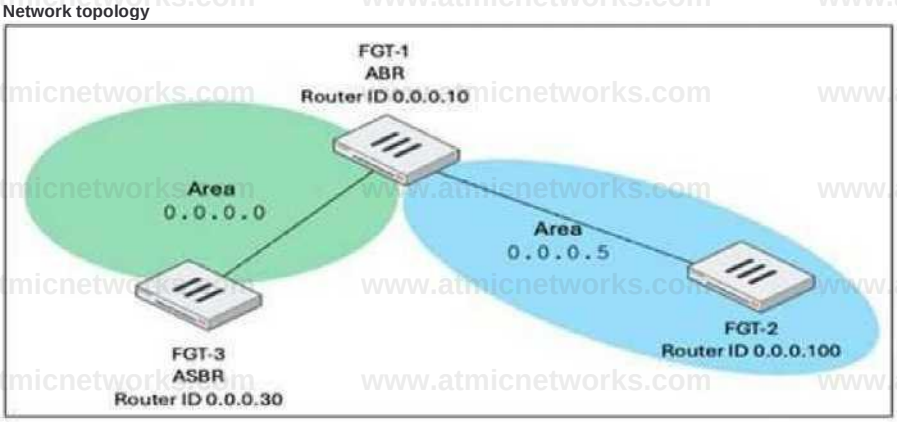
3. Option E (License): If the FortiGuard Web Filtering license expires, the FortiGate can no longer query the FortiGuard Distribution Network (FDN) for ratings. By default, or if the allow-when-rating-error setting is disabled (a common security practice), the FortiGate will block all web traffic that it cannot rate, often displaying a "Web Filter Service Error" or invalid license page.

Option A is incorrect because clearing the cache only increases latency, it does not block traffic. **Option C** is incorrect because webfilter-force-off is typically used to *disable* the service (often allowing traffic to bypass checks if the service is down), rather than blocking it.

Question: 98

Refer to the exhibits.

Network topology



OSPF database

```
FGT~2 • get        router info oupt database brief
                   OSPF Router with ID (0.0.0.100) (Process ID 0, VRF 0)

                                Router Link States (Area 0.0.0.5 (Stub]) ADV Router   Age Seq#          CkSum       Flag
                                Link cou
Link    ID                                                                                                      nt
0.0.    0.10                      0.0.0.10                    302      80000000 13ca 0002 1
0.0.    0.100                     0.0.0.100                   295      8000000b 8761              0021 1
                                Net Link States (Area 0.0.0.5 (Stub])

Link    ID                      ADV Router                  Ago Seq#                CkSum Flag
100.    64.1.1                  0.0.0.10                    302      80000001 feaa 0002
                                Summary Link States (Area 0.0.0.5 (Stub)) ADV Router     Age Seq#     CkSum Flag

                                Route
Link    ID
0.0.    0.0                     0.0.0.10                    320      80000005 d£70              0002 0.0.0.0/0
10.1    .0.0                    0.0.0.10                    315      60000002 fc54 0002 10.1.0.                  0/24
10,1    .10.0                   0.0.0.10                    311      80000001 9aac 0002 10.1.10                  .0/24
```

FGT-1 is an area border router (ABR) that has interfaces in OSPF areas 0.0.0.0 and 0.0.0.5. FGT-3 acts as an autonomous system border router (ASBR), importing static routes into OSPF. FGT-2 is an internal router with all its interfaces belonging to area 0.0.0.5. FGT-1 is receiving all advertised routes from FGT-2, however, FGT-3 is not receiving any of the advertised routes from FGT-1. What is the most likely reason for this? (Choose one answer) A. Area 0.0.0.5 is configured not to propagate type 5 LSAs.

B. FGT-2 is configured with a distribution list to block all advertised routes from FGT-3.

C. FGT-3 and FGT-2 have not formed an OSPF adjacency yet.

D. IP protocol 89 is blocked between FGT-1 and FGT-3.

Answer: A

Explanation:

Comprehensive and Detailed 150 to 200 words of Explanation From Exact Extract of **Network Security 7.6 documents:**

The get router info ospf database brief output on FGT-2 clearly indicates that Area 0.0.0.5 is configured as a **[Stub]** area.

In OSPF, a **Stub Area** is specifically designed to reduce the size of the Link State Database (LSDB) on internal routers. The primary behavior of a Stub area is that it **does not accept Type 5 (AS External) LSAs**.

- FGT-3 is the ASBR (Autonomous System Border Router) and is importing static

www.atmicnetworks.com

routes, which are generated as **Type 5 LSAs** in the OSPF domain.

- FGT-1 acts as the ABR (Area Border Router). Because Area 0.0.0.5 is a Stub area, FGT-1 blocks these Type 5 LSAs from entering Area 0.0.0.5.
- Consequently, FGT-2 will not receive the specific external routes advertised by FGT-3. Instead, the ABR (FGT-1) injects a default route (0.0.0.0/0) into the Stub area to allow connectivity to the external world, which is visible in the database output.

While the question text mentions FGT-3 not receiving routes, the definitive configuration shown in the exhibit is the Stub area setting, which directly corresponds to the blocking of Type 5 LSA propagation (Option A).

Question: 99

Refer to the exhibits,

www.atmicnetworks.com

Exhibit 1

```
config system global
    set snat-route-change enable end
```

```
config router static edit 1
        set gateway 10.200.1.254
        set priority 5

        set device "portl* next edit 2
        set gateway 10.200.2.254
        set priority 10
        set device "port2* next
end
```

Exhibit 2

```
FGT I diagnose sys session list
session info: proto«6 proto_state-01 duration-600 expire-3179 timeout-3600 flags-00000000
sockflag-00000000 sockport* av_idx»0 use-4
origin—shaper=
reply-shaper-
per_ip_shaper-
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan cos=0/255
state-log may_dirty npu fOO
statistic (bytes/packets/allowerr): org=3208/25/l reply-11144/29/1 tuples=2
tx speed (Bps/kbps): 0/0 rx speed (Bps/kbps): 0/0
orgin->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)
src_mac»b4:f7:al:e9:91:97
misc-0 policy_id=l auth_info-0 chk_client_info-0 vd-0
serial=0031c5b tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_llnk_id - 00000000
dd_type=0 dd_mode=0
npu_state-0x000c00
npu info: flag=0x00/0x00, offload=0/0, ips_offload-0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid-0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no ofld reason:
```

which show the configuration on FortiGate and partial session information for internet traffic from a user on the internal network. If the priority on route ID 2 were changed from 10 to 0, what would happen to traffic matching that user session? (Choose one answer) A. The session would be deleted, and the client would need to start a new session.

B. The session would remain in the session table, but its traffic would now egress from both port1 and port2.

C. The session would remain in the session table, and its traffic would egress from port2.

D. The session would remain in the session table, and its traffic would egress from port1.

Answer: A

Explanation:

Comprehensive and Detailed 150 to 200 words of Explanation From Exact Extract of

Network Security 7.6 documents:

The correct answer is A. This behavior is dictated by the configuration command set snat- route-change enable shown in Exhibit 1 under config system global.

1. **Routing Change:** By changing the priority of route ID 2 from 10 to 0, it becomes lower than route ID 1 (priority 5). In FortiOS, a lower priority value indicates a more preferred route. Consequently, the active route for the destination changes from port1 to **port2**.

2. SNAT Implication: The existing session (shown in Exhibit 2) is using Source NAT (SNAT) with the IP address associated with **port1** (10.200.1.1). If the traffic were simply switched to **port2**, the source IP would be incorrect for that interface and the return traffic would likely fail or be dropped.

3. **snat-route-change enable:** This specific setting instructs the FortiGate on how to handle established SNAT sessions when a routing change occurs that alters the preferred outgoing interface. When enabled, if a route change forces an SNAT session to a new interface, FortiGate **flushes (deletes) the session** from the session table. This is necessary because a live TCP session cannot survive a change in its source IP address. The client must initiate a new session, which will then be created using the new correct route (port2) and the corresponding new SNAT IP.

If this setting were disabled, the session would likely remain "sticky" to the original interface (port1) until it closed, provided the route still existed. However, the explicit configuration forces the deletion.

• diagnose debug application fnbaitd *1

4 diagnose debug enable

fnband_fs».cl 1274) handle_taq-Rcvd auth req 0781845 for jmith in tab opt»27 prot»0

fnbamd_ldap.c(637] resolve_ld»p_FCDN-Resolved address 10.10.181.10, result 10.10.181.10

fnband_ldap.c[232] start_search_dn-bass: 'DC=7AC, DOottawa, CC-fortinet, DC=com' filter: sAHAccountName- jsmith

fnbamd_ldap.c11351] fnbamd_ldap_get_resuit-Going to SEARCH state

lnhamd_£sm.cll8331 poil_ldap_servers-Continue pending for req 8781845

fntamdldap.c (266) getalldn-Found DN l:CN=John Smith,CH=Users,DC=TAC, lOoctawa, DC=fort‘net. DC=can