Fortinet.FCSS_NST_SE-7.6.v2026-07-08.q55

Exam Code:	FCSS_NST_SE-7.6
Exam Name:	FCSS - Network Security 7.6 Support Engineer
Certification Provider:	Fortinet
Free Question Number:	55
Version:	v2026-07-08
# of views:	105
# of Questions views:	600
https://www.freecram.net/torrent/Fortinet.FCSS_NST_SE-7.6.v2026-07-08.q55.html	

NEW QUESTION: 1

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

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

Which statement is true?

A. The total slab size of the sctp_session slab is 0 kB and is associated with the user space.

B. The total slab size of the ip_session slab is 3600 kB and is associated with the user space.

C. The total slab size of the ip6_session slab is 1300 kB and is associated with the kernel.

D. The total slab size of the tcp_session slab is 7500 kB and is associated with the kernel.

Answer: (SHOW ANSWER)

The study guide states:

"The kernel memory slabs are collections of objects with a common purpose. The kernel uses them to store information in memory." It also gives the exact calculation rule:

"Total slab size = available objects x object size"

From the exhibit:

tcp_session 3 5 1500 ...

So:

available objects = 5

object size = 1500

Therefore:

Total slab size = 5 × 1500 = 7500 kB

That makes D correct, and it is associated with the kernel, not user space.

Why the other options are wrong:

A is wrong because sctp_session 0 0 1600 ... gives 0 × 1600 = 0, but slabs are associated with the kernel, not user space.

B is wrong because ip_session 1 3 1200 ... gives 3 × 1200 = 3600, but again slabs are kernel memory, not user space.
C is wrong because ip6_session 0 0 1300 ... gives 0 × 1300 = 0, not 1300.

NEW QUESTION: 2
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: (SHOW ANSWER)
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.
References:
FortiOS VPN Manual: IKEv2 Exchange Process and DoS Protections
IKEv2 RFC 7296: Description of IKE_SA_INIT and DoS Cookie Mechanism

NEW QUESTION: 3
Refer to the exhibit, which shows the modified output of the routing kernel.

Routing information

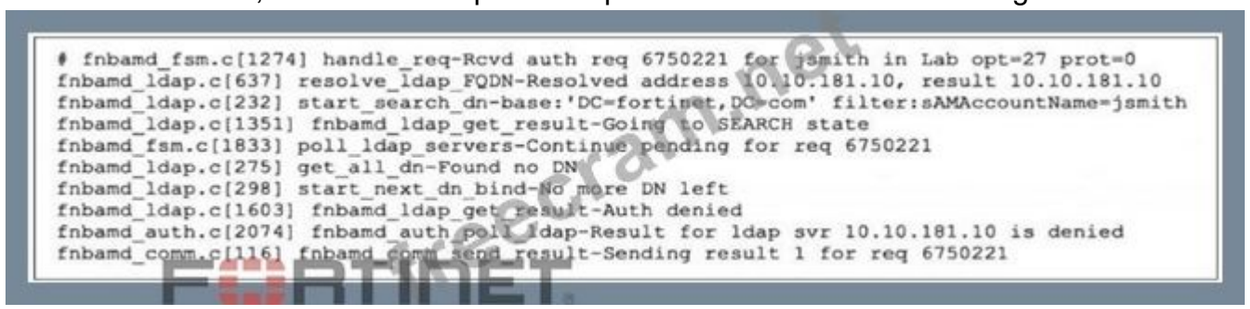
```
# get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS 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, port1, [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, port8 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
O        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, port4
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, port1
C     *> 10.200.2.0/24 is directly connected, port2
```


Which statement is true?
A. The egress interface associated with static route 8.8.8.8/32 is administratively up.
B. The BGP route to 10.0.4.0/24 is not in the forwarding information base.
C. The default static route through port2 is in the forwarding information base.
D. The default static route through 10.200.1.254 is not in the forwarding information base.
Answer: (SHOW ANSWER)

NEW QUESTION: 4

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



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

A. Ensure the user is providing the correct user credentials.

B. Ensure the user is a member of at least one AD group to ensure step 4 of the LDAP authentication process is successful.

C. Ensure the account is active.

D. Ensure the user logs in using 'John Smith' not 'jsmith'.

Answer: (SHOW ANSWER)

NEW QUESTION: 5

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: (SHOW ANSWER)

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 end-users while still supporting granular inspection.

References:

FortiGate 7.6.4 Administration Guide: Certificate Inspection

SSL/SSH Inspection Profile Configuration

NEW QUESTION: 6

Refer to the exhibit.

Diagnose output

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 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=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=1 auth_info=0 chk_client_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: (SHOW ANSWER)

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."

NEW QUESTION: 7
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: (SHOW ANSWER)
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.
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."

NEW QUESTION: 8
Refer to the exhibit, which shows the output of get router info bgp summary.

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: (SHOW ANSWER)

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.

References:

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

NEW QUESTION: 9

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 the same TCP port but run on different UDP ports.

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

Answer: (SHOW ANSWER)

The correct answer is B.

The study guide explicitly states: "IKE version 2 does not interoperate with IKE version 1, but they share enough of the header format that both versions can unambiguously operate over the same UDP port." That directly proves B.

Why the other options are wrong:

A is wrong because the study guide shows authentication methods as Asymmetric for IKEv2 and Symmetric for IKEv1 C is wrong because the study guide does not say they use the same TCP port; instead, it specifically says they can operate over the same UDP port D is wrong because the study guide states: "IKEv2 does not use the concept of phase 1 or phase 2", even though FortiOS CLI/GUI still uses those terms for configuration purposes

NEW QUESTION: 10

Refer to the exhibit.

Debug output

```
FGT # diagnose debug application ike -1

FGT # diagnose debug enable

FGT # ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange=Informational id=61bba3725bd738d3/265a0b7a271799b7:9e253b8b len=108 vrf=0
ike 0: in
61BBA3725BD738D3265A0B7A271799B7081005019E253B8B0000006CE3C6FFBD5AD97F5AD027B12CA81C5E5A091209F6D184E10DF2548B9B1FF60F6A13167A172
26398E                851BE86CDACD29234B58E5F48024711F4FA1F216E791CB1B13650F1E4498CE45AE53CE9E627C92E9
ike 0:VPN_0:24266: dec 977A47FB0000002000000000101108D2861BBA3725BD738D3265A0B7A271799B70000014D85DB9684B6CFE9C681AE840B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 0F45C66000000020000000000101108D293C0DB9994E7E8547D50F9D18113B6CA9900000000
ike 0:VPN_0:24319: out AD893C1B9C22FA2E0B17E7FB9574BA4BF1D49AD47DE62294ECA9B9204D090A367D8DDDB20E5812CB470F87CB15504E
ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange=Informational id=30db9994e7e8547d/50f9d18113b6ca99:b1dd9b5f len=108 vrf=0
ike 0: in 82A79C36BC7F9ECDE1062B00FEBC8E239F55E1F3E38196550041EBAAF2034B253855D2A3E253A6480D90
ike 0:VPN_0:24319: dec 8CC06CBDC0000002000000000101108D2830DB9994E7E8547D50F9D18113B6CA9900000001E186A982E682A3E9FBF8F30B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 11AEC31B0000002000000000101108D2830DB9994E7E8547D50F9D18113B6CA9900000001
ike 0:VPN_0:24319: out E83C93D51EF44D937E260373CC9A86A0939BEA3EDDD78FAEC8DE4E1F650DDC2E9E5626F34EF2346DF1807983C12E80D2
ike shrank heap by 335872 bytes
ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0....
ike 0: IKEv1 exchange=Informational id=30db9994e7e8547d/50f9d18113b6ca99:a9040efb len=108 vrf=0
ike 0: in 0710D9A5184A392DC8DB96B354FF46B84EEA79622FC1D44BC7F964986AD85D49AC93BEDE376CB31EA2BD57
ike 0:VPN_0:24319: dec 01A44559000000200000000101108D283C0DB9994E7E8547D50F9D18113B6CA9900000002C0D9F8CEB8B2B7CDD5CACA0B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc E18A83380C0000002000000000101108D293C0DB9994E7E8547D50F9D18113B6CA9900000002
ike 0:VPN_0:24319: out C4906BDDB812D02AE1672BD0E093431344D7BC31E9323A2C56E27DB43B747070805D7954558993B25BC43118695BEA47
ike 0:VPN_0:24266: recv IPsec SA delete, spi count 1
ike 0:VPN_0: deleting IPsec SA with SPI 6161297a
ike 0:VPN_0:vpn2-1: deleted IPsec SA with SPI 6161297a, SA count: 0
ike 0:VPN_0:7220167: del route 172.21.27.56/255.255.255.255 tunnel 73.25.189.174 oif VPN_0(12922) metric 15 priority 1
ike 0:VPN_0: sending SNMP tunnel DOWN trap for vpn2-1
ike 0:VPN_0:vpn2-1: 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. The tunnel drops after the timer expires.

B. The tunnel drops during rekey negotiation.

C. Dead Peer Detection is not receiving its acknowledge packet.

D. Phase 2 drops but Phase 1 is up.

Answer: (SHOW ANSWER)

NEW QUESTION: 11

Refer to the exhibit.

Debug output

```
FGT # diagnose sys session list
session info: proto=6 proto_state=11 duration=35 expire=265 timeout=300 flags=00000000
sockflag=00000000 sockport=0 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=redir local may_dirty 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 gwy=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(192.167.1.100:4954
pos/ (before, after) 0/ (0,0), 0/ (0,0)
src mac=08:5b:0e: 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=0x00/0x00, 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 made

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

D. FortiGate forwarded this session without any inspection.

Answer: (SHOW ANSWER)

The session output includes the flags:

state=redir local may_dirty ...

npu_state=00000000

offload=0/0

The 7.6 study guide explains these flags directly:

local = "Session is to/from local stack"

redir = "Session is being processed by an application layer proxy"

may_dirty = "Session is allowed by a firewall policy"

This makes C correct, because the local flag means the session either originates from FortiGate or terminates on FortiGate. The FortiOS administration guide states the same meaning: "Session is originated from or destined for local stack." This also makes A correct. The redir flag means the session is handled by an application-layer proxy. FortiOS documents explain that proxy-based inspection buffers traffic on the FortiGate and inspects it there, and that proxy-based processing is CPU and memory-intensive Since the session also shows no NPU offload (npu_state=00000000, offload=0/0), this traffic is being handled in software/CPU, not by the NPU.

Why the other options are wrong:

B is wrong because the redir flag proves the session is not passing without inspection; it is being processed by an application-layer proxy D is wrong because there is no authentication flag in this session. In Fortinet examples of captive portal/authentication-related sessions, the session state includes auth or authed flags. The study guide

shows: "Any session for traffic coming from an authenticated user contains the authed flag." This exhibit does not show auth or authed, so there is no basis to conclude the client was redirected to a captive portal for authentication.

NEW QUESTION: 12
Refer to the exhibit, which shows the output o! the BGP database.

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 (LEAVE A REPLY)
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.
References:
FortiOS Administration Guide: BGP Configuration and Route Table Interpretation Official BGP Command Reference: Show BGP Network, Path Codes, Route Origination Indicators

NEW QUESTION: 13
Refer to the exhibit.

The port1 interface configuration on FortiGate and partial session information for ICMP traffic are shown.

Which two things happen to the session information if a routing change occurs that affects this session? (Choose two answers)

A. This session will be unaffected by routing changes. The routing changes will apply only to new sessions.

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

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

D. The session information will not change even when the active route has been removed from the routing table.

Answer: (SHOW ANSWER)

The correct answers are A and C.

The exhibit shows that preserve-session-route is enabled on port1:

config system interface

edit "port1"

set preserve-session-route enable

next

end

The study guide explains the effect of this setting exactly:

"enable: FortiGate marks existing session routing information as persistent, and applies only the modified routes to new sessions" It also states:

"The current route must still be present in the FIB. Otherwise, FortiGate flags the session as dirty and reevaluates it" And the same page further clarifies:

"If you enable this setting, sessions passing through that interface continue to pass without being affected by the routing changes. The routing changes apply only to new sessions. If the route is removed from the FIB, then FortiGate must flag the session as dirty, flush its gateway information, and reevaluate the session." This proves:

A is correct because with preserve-session-route enable, existing sessions are normally preserved and routing changes apply only to new sessions.

C is correct because the session remains unchanged unless the current route is removed from the FIB/routing table, in which case FortiGate dirties and reevaluates the session.

Why the other options are wrong:

B is wrong because when the active route is removed, FortiGate does not simply mark the session dirty and stop there. The study guide says it "flags the session as dirty and reevaluates it", which means route lookup happens again.

D is wrong because the session does change if the active route is removed. FortiGate flushes gateway information and reevaluates the session.

So the verified answers are: A, C.

NEW QUESTION: 14

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: ----------------------------------------------------
OSPF: Header
OSPF:   Version 2
OSPF:   Type 1 (Hello)
OSPF:   Packet Len 48
OSPF:   Router ID 0.0.0.112
OSPF:   Area ID 0.0.0.0
OSPF:   Checksum 0x2f85
OSPF:   AuType 0
OSPF: Hello
OSPF:   NetworkMask 255.255.255.0
OSPF:   HelloInterval 10
OSPF:   Options 0x2 (*|-|-|-|-|-|E|-)
OSPF:   RtrPriority 1
OSPF:   RtrDeadInterval 40
OSPF:   DRouter 192.168.37.114
OSPF:   BDRouter 192.168.37.115
OSPF:   # Neighbors 1
OSPF:     Neighbor 0.0.0.111
OSPF: ----------------------------------------------------
OSPF: RECV[Hello]: From 0.0.0.112 via port2:192.168.37.114: Authentication type 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: (SHOW ANSWER)

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.

NEW QUESTION: 15
Refer to the exhibit, which shows a session entry.

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: (SHOW ANSWER)
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.
References:

FortiOS Administration Guide: Session Table, NAT, and Route Interaction Fortinet Technical Note: Diagnose sys session list, Direction and NAT Analysis

NEW QUESTION: 16
Refer to the exhibit.

```
# 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: (SHOW ANSWER)
The exhibit shows:
memory conserve mode: on
memory used: 2706 MB 89% of total RAM
memory used threshold red: 2675 MB 88% of total RAM
memory used + freeable threshold extreme: 2887 MB 95% of total RAM
The study guide states that the default thresholds are:
Extreme = 95%
Red = 88%
Green = 82%
So this FortiGate is in conserve mode because memory usage is 89%, which is above the red threshold (88%), but it has not yet reached the extreme threshold (95%).
The study guide then explains exactly what happens during conserve mode:
"For traffic that requires proxy-based inspection (and if memory usage has not exceeded the extreme threshold):
config system global
set av-failopen [off | pass | one-shot]
...
pass (default): All new sessions pass without inspection"
It also says:
"The av-failopen setting also applies to flow-based antivirus inspection." And the same page adds:
"If memory usage exceeds the extreme threshold, all new sessions that require inspection (flow-based or proxy-based) are blocked." Therefore, with default settings and with memory usage below the extreme threshold, FortiGate is allowing new sessions that require inspection, but bypassing inspection. That matches C.
Why the other options are wrong:

A is wrong because the default behavior is not to block proxy-based inspected sessions; the default is pass, meaning they pass without inspection B is wrong because if memory rises another 6%, it reaches 95%, which is the extreme threshold. At that point, the study guide says all new sessions that require inspection are blocked D is wrong because FortiGate blocks all new inspected sessions only when memory usage exceeds the extreme threshold, and the exhibit shows it is currently at 89%, not 95%

NEW QUESTION: 17
Refer to the exhibit.

```
# diagnose sys  session stat
misc info:    session_count=1523 setup_rate=0 exp_count=0 reflect_count=0 clash=113
   memory_tension_drop=0 ephemeral=0/131072 removeable=0 extreme_low_mem=0
   npu_session_count=0
delete=0, flush=1, dev_down=0/0
session walkers: active=0, vf-42, dev-0, saddr-0, npu-0
TCP sessions:
    562 in ESTABLISHED state
    15 in SYN_RECV state
    27 in CLOSE state
```

The partial output of diagnose sys session stat command is shown.
Which statement about the output shown in the exhibit is correct?
A. 113 sessions have been dropped because of memory page exhaustion.
B. There have been 131072 recorded ephemeral sessions but there are no current ones.
C. 562 TCP sessions have their proto_state set to 01 if there is no inspection.
D. 27 sessions have expired but are still in the session table in case any out-of-order packets arrive.
Answer: (SHOW ANSWER)
The correct answer is C.
The exhibit shows:
562 in ESTABLISHED state
27 in CLOSE state
memory_tension_drop=0
ephemeral=0/131072

According to the study guide, for TCP sessions: "The protocol state in the session table is a two-digit number. For TCP, the first number (from left to right) is related to the server-side state and is 0 when the session is not subject to any inspection (flow or proxy)... The second digit is the client-side state." The same page also shows that value 1 = ESTABLISHED So, if a TCP session is in ESTABLISHED state and there is no inspection, its proto_state is 01:
first digit 0 = no inspection
second digit 1 = ESTABLISHED
That makes C correct. This is also consistent with FortiOS examples showing established TCP sessions with proto=6 proto_state=01 Why the other options are wrong:
A is wrong because the field that indicates sessions dropped due to low free memory is memory_tension_drop, and in the exhibit it is 0, not 113. The study guide states: "If there is a lack of free memory, the kernel deletes the oldest sessions. The command shown on this slide displays the number of sessions the kernel deleted because of this mechanism." So 113 is the clash value, not memory-tension drops.
B is wrong because ephemeral=0/131072 does not mean 131072 ephemeral sessions were recorded. The study guide explains that FortiGate "sets a hard limit on the maximum number of ephemeral sessions that can exist at the same time in the session table." Therefore:
0 = current ephemeral sessions
131072 = maximum allowed ephemeral sessions for that model/context
D is wrong because the study guide says the temporary retention for possible out-of-order packets happens in state value 5 (TIME_WAIT): "When a session is closed by both the sender and receiver, FortiGate keeps that session in the session table for a few seconds, to allow for any out-of-order packets that might arrive after the FIN/ACK packet. This is the state value 5." But the exhibit shows 27 in CLOSE state, and the same table shows CLOSE = 6, not TIME_WAIT So the verified answer is C.

NEW QUESTION: 18
Refer to the exhibit.
Partial output of diagnose sys session stat command is shown.

```
# diagnose sys session stat
misc info:       session_count=325683 setup_rate=0 exp_count=0 reflect_count=0
clash=0 memory_tension_drop=4 ephemeral=196608/196608 removeable=0 extreme_low_mem=0
        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.
Answer: (SHOW ANSWER)
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."

NEW QUESTION: 19
Refer to the exhibit, which shows the output of a diagnose command. What can you conclude from the RTT value?

```
FGT # diagnose debug rating
Locale       : english

Service      : Web-filter
Status       : Enable
License      : Contract

Service      : Antispam
Status       : Disable

Service      : Virus Outbreak Prevention
Status       : Disable

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

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

IP                                   Weight    RTT Flags   TZ   FortiGuard-requests  Curr Lost Total Lost           Updated Time
64.26.151.37                             10     45          -5                262432          0        846 Mon May  1 03:47:43 2023
64.26.151.35                             10     46          -5                329072          0       6806 Mon May  1 03:47:43 2023
66.117.56.37                             10     75          -5                 71638          0        275 Mon May  1 03:47:43 2023
65.210.95.240                            20     71          -8                 36875          0         92 Mon May  1 03:47:43 2023
209.22.147.36                            20    103 DI       -8                 34784          0       1070 Mon May  1 03:47:43 2023
208.91.112.194                           20    107 D        -8                 35170          0       1533 Mon May  1 03:47:43 2023
96.45.33.65                              60    144           0                 33728          0        120 Mon May  1 03:47:43 2023
80.85.69.41                              71    226           1                 33797          0        192 Mon May  1 03:47:43 2023
62.209.40.74                            150     97           9                 33754          0        145 Mon May  1 03:47:43 2023
121.111.236.179                          45     44  F        -5                 26410      26226      26227 Mon May  1 03:47:43 2023
```


A. Its value represents the time it takes to receive a response after a rating request is sent to a particular server.
B. Its value is incremented with each packet lost.

C. It determines which FortiGuard server is used for license validation.
D. Its initial value is statically set to 10.
Answer: (SHOW ANSWER)
The correct answer is A.
The study guide explicitly explains the diagnose debug rating table and says that for each server IP, the output shows "The round trip delay" That means the RTT value represents the time it takes for FortiGate to send a request and receive the reply from that FortiGuard server.
The FortiOS administration guide also confirms this by stating:
"Each server is probed for Round Trip Time (RTT) every two minutes."
Why the other options are wrong:
B is wrong because packet loss is shown separately by Curr Lost and Total Lost, while RTT is the round-trip delay C is wrong because license-validation behavior is indicated by flags such as I = Initial, not by the RTT value itself D is wrong because the documents do not say RTT starts at a fixed value of 10; it is measured dynamically as round-trip delay So the verified answer is: A.

NEW QUESTION: 20
Refer to the exhibit.

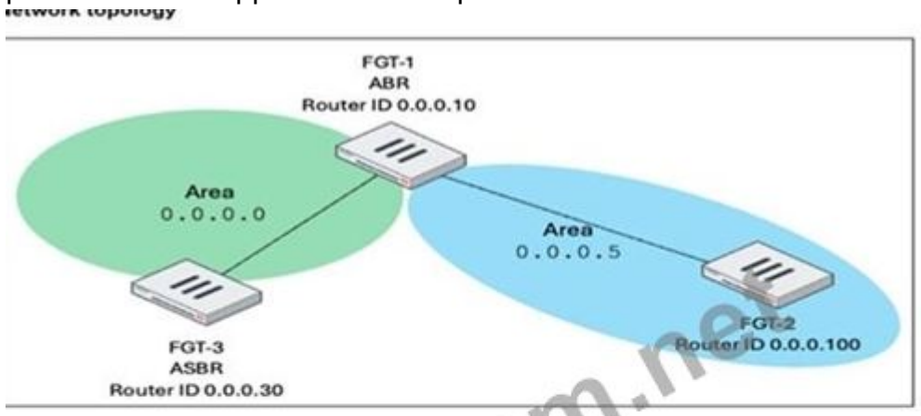
Session entry

```
# diagnose sys session list
session info: proto=6 proto_state=11 duration=1 expire=3599 timeout=3600 refresh_dir=both flags=00000000 socktype=0
origin-shaper=medium prio=3 guarantee 0Bps max 134217728Bps traffic 232868Bps drops 0B
reply-shaper=medium prio=3 guarantee 0Bps max 134217728Bps traffic 232868Bps drops 0B
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty ndr npu f00 app_valid
statistic(bytes/packets/allow_err): org=1720/9/1 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)
misc=0 policy_id=1 pol_uuid_idx=14720 confiauth_info=0 chk_client_info=0 vd=0
serial=0002932f tos=ff/ff app_list=2000 app=34050 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=1
rpdb_link_id=80000000 ngfwid=n/a
npu_state=0x003c94 ips_offload
npu info: flag=0x81/0x81, offload=8/8, ips_offload=1/1, epid=16/16, ipid=64/88, vlan=0x0000/0x0000
vlifid=64/88, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=0/0
```


The exhibit shows a session entry. Which statement about this TCP session is true?
A. The session will expire in one second.
B. It is a TCP session from 10.9.31.117 to 10.1.0.3.
C. The session is offloaded using NPU.
D. Return traffic to the initiator is sent to 10.9.31.117.
Answer: (SHOW ANSWER)
The correct answer is C. The session is offloaded using NPU.
The exact session example in the study guide shows:
proto=6 → this is a TCP session

expire=3599 → the session will expire in 3599 seconds, not in one second 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) npu info: ... offload=8/8 ...
and the slide explicitly states: "Offloaded in both directions using NP6" The study guide also explains this exact point clearly:
"Counters for hardware acceleration-The presence of the npu info field indicates the session has been offloaded to hardware acceleration. In this example, traffic is being offloaded in both directions using network processor (NP) 6, which is represented by the value of 8." Why the other options are wrong:
A is wrong because expire=3599, not 1. The duration=1 field means the session has existed for 1 second, not that it will expire in 1 second.
B is wrong because the original session is from 10.9.31.117 to the remote server 200.8.57.5:443. The IP 10.1.0.3 is the SNAT-translated source address, not the final destination.
D is not the best answer for this single-select question. The reply is indeed DNATed back toward the original client, but the exact validated takeaway highlighted by the study guide for this exhibit is the NPU offload state.

NEW QUESTION: 21
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.



OSPF database

```
FGT-2 # get router info ospf 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         ADV Router      Age  Seq#       CkSum Flag Link count
0.0.0.10        0.0.0.10        302  80000008 13ea   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      Age  Seq#       CkSum Flag
100.64.1.1      0.0.0.10        302  80000001 feaa   0002

                Summary Link States (Area 0.0.0.5 [Stub])

Link ID         ADV Router      Age  Seq#       CkSum Flag Route
0.0.0.0         0.0.0.10        320  80000005 df70   0002 0.0.0.0/0
10.1.0.0        0.0.0.10        315  80000002 fc54   0002 10.1.0.0/24
10.1.10.0       0.0.0.10        [illegible]
```

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: (SHOW ANSWER)

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.
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.
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.
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.

NEW QUESTION: 22
Refer to the exhibit, which shows the output of diagnose sys session stat.

```
NGFM-1 # diagnose sys session stat
misc info:          session_count=591 setup_rate=0 exp_count=0 clash=162
          memory_tension_drop=0 ephemeral=0/65536 removeable=0
delete=0, flush=0, dev_down=0/0 ses_walkers=0
TCP sessions:
              166 in NONE state
              1 in ESTABLISHED state
              3 in SYN SENT state
              2 in TIME WAIT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000006
fadn6_count=00000000
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0
```


Which statement about the output shown in the exhibit is correct?
A. All the sessions in the session table are TCP sessions.
B. 162 sessions have been deleted because of memory page exhaustion.
C. There are 166 TCP sessions waiting to complete the three-way handshake.
D. There are two sessions that have not been removed in case any out-of-order packets arrive.
Answer: (SHOW ANSWER)
The correct answer is D.
The exhibit shows:
session_count=591
clash=162
memory_tension_drop=0

TCP sessions:
166 in NONE state
1 in ESTABLISHED state
3 in SYN_SENT state
2 in TIME_WAIT state
The study guide explains the TCP protocol states and states explicitly:
"When a session is closed by both the sender and receiver, FortiGate keeps that session in the session table for a few seconds, to allow for any out-of-order packets that might arrive after the FIN/ACK packet. This is the state value 5." In diagnose sys session stat, the exhibit shows 2 in TIME_WAIT state. Since TIME_WAIT = state value 5, those are the sessions being kept briefly for possible out-of-order packets. That makes D correct.
Why the other options are wrong:
A is wrong because session_count=591 is the total number of sessions, while the TCP sessions shown add up to only 172 (166 + 1 + 3 + 2). So not all sessions in the table are TCP sessions.
B is wrong because the study guide says the number of sessions deleted because of low free memory is shown by memory_tension_drop, and in the exhibit it is 0, not 162.
C is wrong because the study guide defines ephemeral/open TCP sessions as those not fully established, but the exhibit does not say all 166 in NONE state are specifically "waiting to complete the three-way handshake." The clearest directly supported statement from the displayed states is the 2 TIME_WAIT sessions retained for out-of-order packets.
So the verified answer is: D.

NEW QUESTION: 23
Refer to the exhibit.

```
# get router info bgp summary

VRF 0 BGP router identifier 172.16.23.58, local AS number 65100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.23.153   4        100     218     3220        0    0    0 never     Connect

Total number of neighbors 1
```


The output of a BGP debug command is shown.
Why has the local router at 172.16.23.58 been unable to establish adjacency with its only neighbor?
A. The neighbor router has become unreachable, which is evident by the low ratio of messages received to messages sent.
B. The local router has not received an OPEN message from the neighbor.
C. The local router has not received a SYN/ACK packet from the neighbor.
D. There is no active route to the BGP neighbor.
Answer: (SHOW ANSWER)
The correct answer is C.
The exhibit shows the neighbor state as Connect in the State/PfxRcd column. The study guide explains the BGP states exactly as follows:
"Connect: Waiting for a successful three-way TCP connection"
"OpenSent: Waiting for an OPEN message from the peer"

"Established: Peers have successfully exchanged OPEN and keepalive messages" Because the router is still in Connect state, the TCP three-way handshake has not completed yet. In practical terms, the local router has sent the TCP SYN but has not successfully received the SYN/ACK needed to complete the handshake. That is why C is correct.
Why the other options are wrong:
A is wrong because the message counters alone do not prove that the neighbor is unreachable. The study guide says the State/PfxRcd field shows the BGP state when the session is not established, and here that state is specifically Connect B is wrong because waiting for an OPEN message happens in OpenSent, not Connect D is not the best answer for this output. The study guide ties the displayed state directly to the protocol phase: Connect means the device is still waiting for a successful TCP handshake So the verified answer is: C.

NEW QUESTION: 24
Refer to the exhibit, which shows one way communication of the downstream FortiGate with the upstream FortiGate within a Security Fabric.

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

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

NEW QUESTION: 25
Refer to the exhibit, which shows the partial output of command diagnose debug rating.

```
-=- Server List (Mon May  6 03:47:52 2024) -=-
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  6 03:47:43 2024
64.26.151.35                            10     46          -5              329072           0       6606 Mon May  6 03:47:43 2024
66.117.56.37                            10     75          -5               71638           0        275 Mon May  6 03:47:43 2024
65.210.95.240                           20     71          -8               36875           0         92 Mon May  6 03:47:43 2024
209.22.147.36                           20    103 DI       -8               34784           0       1070 Mon May  6 03:47:43 2024
208.91.112.194                          20    107 D        -8               35170           0       1533 Mon May  6 03:47:43 2024
96.45.33.65                             60    144          0                33720           0        120 Mon May  6 03:47:43 2024
80.85.69.41                             71    226          1                33797           0       2152 Mon May  6 03:47:43 2024
62.209.40.74                           150    302          9                33754           0        145 Mon May  6 03:47:43 2024
121.111.236.179                         45     44 F        -5               26410       15906      24227 Mon May  6 03:47:43 2024
```

In this exhibit, which FDS server will the FortiGate algorithm choose?
A. 66.117.56.37
B. 64.26.151.37
C. 209.22.147.36

D. 208.91.112.194
Answer: (SHOW ANSWER)

NEW QUESTION: 26
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 (LEAVE A REPLY)
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 route-maps 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.
References:
FortiOS BGP Debugging Guide: Session State Interpretation
BGP CLI Reference: Neighbor Status Fields

NEW QUESTION: 27
What are two functions of automation stitches? (Choose two.)
A. You can configure automation stitches to run diagnostic commands and attach the results to an email message when CPU or memory usage exceeds specified thresholds.
B. You can configure automation stitches to modify packet headers and payloads if specific traffic triggers an anomaly IPS event.
C. You can configure automation stitches to take parameters from previous actions as input for the next action if the automation stitches are set to execute actions in sequence.
D. You can configure automation stitches to insert a delay between actions if the automation stitches are set to execute actions in parallel.
Answer: (SHOW ANSWER)

NEW QUESTION: 28
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: (SHOW ANSWER)
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.

NEW QUESTION: 29
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 if both peers have an IP address within the same subnet.
B. Check if IP protocol 89 is blocked.
C. Check if TCP port 179 is blocked.
D. Check if there is an active static route to the peer.

Answer: (SHOW ANSWER)
The correct answers are A and B.
The Network Security Support Engineer 7.6 Study Guide states under OSPF Troubleshooting:
"Follow these steps to troubleshoot an OSPF problem between two peers:
Check that the local router can reach the remote peer. IP addresses must be in the same subnet and have the same subnet mask.
Ensure that IP protocol 89 is not blocked.
Hello and dead intervals must match.
The OSPF router ID for each peer must be unique. Duplicate router IDs are not allowed.
Do the MTUs match?
If authentication is enabled, the type and password must match on both sides."** The same page also summarizes the troubleshooting tips as:
"Do peers have an IP address within the same subnet?"
"Is IP protocol 89 blocked?"
This directly confirms:
A is correct
B is correct
Why the other options are wrong:
C is wrong because TCP port 179 is used by BGP, not OSPF. OSPF uses IP protocol 89, as the study guide explicitly notes D is wrong because the study guide's OSPF adjacency troubleshooting checklist does not require an active static route to the peer. OSPF neighbors form adjacency on directly reachable networks, and the guide instead focuses on same subnet, protocol 89, intervals, router ID, MTU, and authentication matching So the verified answers are: A, B.

NEW QUESTION: 30
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: (SHOW ANSWER)
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."

NEW QUESTION: 31
Exhibit.

```
… name_ip_match: failed to connect to workstation: <Workstation Name> (192.168.1.1)
… failed to connect to registry: WORKSTATION02 (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. The user's status shows as "not verified" in the collector agent.
B. Remote registry is not running on the workstation.
C. DNS resolution is unable to resolve the workstation name.
D. A firewall is blocking traffic to port 139 and 445.
E. The FortiGate firmware version is not compatible with that of the collector agent.
Answer: (SHOW ANSWER)

NEW QUESTION: 32
Refer to the exhibit.

Debug output

```
ike 0:624000:98: responder: main mode get 1st message...
ike 0:624000:98: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:624000:98: VID FORTIGATE 8299031757A36082C6A621DE00000000
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_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=MODP2048.
ike 0:624000:98: ISAKMP 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=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 0:624000:98:    protocol id - ISAKMP:
ike 0:624000:98:         trans_id = 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, val=PRESHARED_KEY.
ike 0:624000:98:               type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
```

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: (SHOW ANSWER)

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.

NEW QUESTION: 33
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: (SHOW ANSWER)
References:

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

NEW QUESTION: 34
Refer to the exhibit.

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

Chip	XAUI	Ports	Max Speed	Cross-chip offloading
np6_1	0	port1	1G	No
	0	port5	1G	No
	0	port9	1G	No
	0	port13	1G	No
	0	port17	1G	No
	0	port21	1G	No

-omitted-

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.
```
diagnose npu np6 port-list disable 5 17
```

B.
```
config firewall policy
edit 5
set auto-asic-offload disable
end
next
edit 17
set auto-asic-offload disable
end
```

C.
```
diagnose npu np6 fastpath disable 1
```

D.
```
config system npu
set fastpath disable
end
```

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 35
Refer to the exhibit.

Routing information

```
# get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - 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, port1, [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, port8 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
O        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, port4
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, port1
C     *> 10.200.2.0/24 is directly connected, port2
```

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: (SHOW ANSWER)
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."

NEW QUESTION: 36
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: (SHOW ANSWER)
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.
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."

NEW QUESTION: 37
Refer to the exhibit.

Partial output of the fssod daemon real-time debug command is shown. Which two conclusions can you draw from the output? (Choose two answers)

A. FSSO cannot verify if the user is still logged in.

B. Fortinet Single Sign-On (FSSO) is using DC Agent mode to detect logon events.

C. FortiGate is frequently polling the workstation in case the user has logged out.

D. FSSO is using agentless polling mode to detect logon events.

E. FortiGate polled this event through TCP port 8000.

Answer: (SHOW ANSWER)

The correct answers are C and D.

The key clue is the command itself:

diagnose debug application fssod -1

The study guide explicitly states: "There is a specific FortiGate daemon that handles the polling mode. It is the fssod daemon. To enable agentless polling mode real-time debug use the command: diagnose debug application fssod -1." That directly proves D. FSSO is using agentless polling mode to detect logon events.

The study guide also states: "In agentless polling mode, FortiGate frequently polls all workstations (as a standalone collector agent does) to check which users are still logged in. You can sniffer this traffic on port 445." That directly proves C. FortiGate is frequently polling the workstation in case the user has logged out.

Why the other options are wrong:

A is wrong because the "cannot verify if the user is still logged in" / Not Verified condition is described for the collector agent workstation status, not as a conclusion from this FortiGate fssod debug line. The study guide says: "A user goes to not verified status when they log out, or when there is a problem in the polling done by the collector agent to the workstation." B is wrong because DC Agent mode is part of agent-based FSSO, where DC agents send events to a collector agent. This output is from the fssod daemon, which the study guide ties to agentless polling mode, not DC Agent mode.

E is wrong because TCP port 8000 is used for communication between the collector agent and FortiGate, while in agentless polling mode FortiGate polls workstations and that traffic can be sniffed on TCP port 445.

So the verified answers are: C, D.

NEW QUESTION: 38

Exhibit.

```
config system fortiguard
    set protocol udp
    set port 8888
    set load-balance-servers1
    set auto-join-forticloud enable
    set update-server-location any
    set sandbox-region ''
    set fortiguard-anycast disable
    set antispam-force-off disable
    set antispam-cache enable
    set antispam-cache-ttl 1800
    set antispam-cache-mpercent 2
    set antispam-timeout 7
    set webfilter-force-off enable
    set webfilter-cache enable
    set webfilter-cache-ttl 3600
    set webfilter-timeout 15
    set sdns-server-ip "208.91.112.220"
    set sdns-server-port 53
    unset sdns-options
    set source-ip 0.0.0.0
    set source-iD6 ::
    set proxv-server-ip 0.0.0.0
    set proxy-server-port 0
    set proxy-username
    set ddns-server-ip 0.0.0.0
    set dons-server-port 443
end
```


Refer to the exhibit, which shows a FortiGate configuration.

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

What must the administrator do to fix the issue?

A. Disable webfilter-force-off.

B. Increase webfilter-timeout.

C. Enable fortiguard-anycast.

D. Change protocol to TCP.

Answer: (SHOW ANSWER)

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

NEW QUESTION: 39

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

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: (SHOW ANSWER)

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.

References:

Fortinet Technical Tip: FortiGate Session Table and NPU Offloading

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

NEW QUESTION: 40

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: (SHOW ANSWER)

The study guide states:

"FortiGate categorizes an entry in the session table as an ephemeral session when it is a TCP session that is not fully established (three-way handshake not completed), or when it is a UDP session with only one packet received." This directly proves:

A is correct because a UDP session with only one packet received is ephemeral.

C is correct because a TCP session waiting for the SYN/ACK is not fully established, so it is ephemeral. The study guide's TCP state table shows that the handshake is only completed when the session reaches ESTABLISHED Why the other options are wrong:

B is wrong because once UDP traffic has been seen in both directions, it is no longer the "single packet received" condition described for ephemeral sessions. The study guide says for UDP: 00 = one way, 01 = both ways D is wrong because a TCP session waiting for FIN/ACK is already in the closing stage after establishment, not in the "not fully established" stage. The study guide explains that after both sides close the session, FortiGate can keep it briefly in the table in state value 5 for out-of-order packets after FIN/ACK

NEW QUESTION: 41
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: (SHOW ANSWER)
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.
References:
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

NEW QUESTION: 42
Which three conditions are required for two FortiGate devices to form an OSPF adjacency? (Choose three answers)
A. OSPF link costs match.
B. OSPF interface priority settings are unique.
C. OSPF interface network types match.
D. Authentication settings match.
E. OSPF router IDs are unique.
Answer: (SHOW ANSWER)
The same study-guide slide also states other requirements such as:
peers' primary IPs must be in the same subnet with the same mask
hello and dead intervals must match
OSPF MTUs must match
Why the other options are wrong:

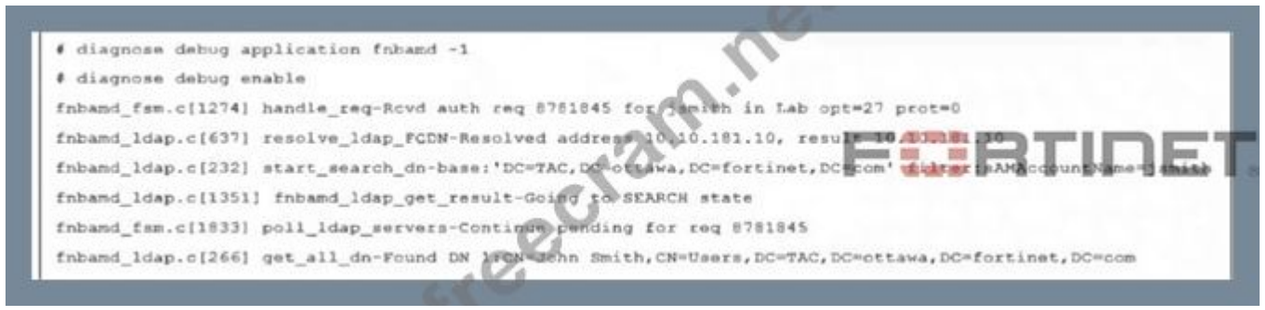
A is wrong because link cost matching is not listed as an adjacency requirement. OSPF cost affects path selection, not whether adjacency can form.
B is wrong because interface priority does not need to be unique. Priority is used for DR/BDR election, where the highest priority wins, and ties are broken by router ID.
So the verified answers are: C, D, E.
Explanation:
The correct answers are C, D, and E.
The study guide lists the exact OSPF adjacency requirements:
"Interfaces of peers are the same type and in the same OSPF area"
"Each peer has a unique router ID"
"OSPF authentication, if enabled, is successful"
These map directly to:

NEW QUESTION: 43
Refer to the exhibit.

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

NEW QUESTION: 44
Which two statements about conserve mode are true? (Choose two.)
A. FortiGate exits conserve mode when the system memory goes below the configured green threshold.
B. FortiGate enters conserve mode when the system memory reaches the configured extreme threshold.
C. FortiGate starts taking the configured action for new sessions requiring content inspection when the system memory reaches the configured red threshold.
D. FortiGate starts dropping all new sessions when the system memory reaches the configured red threshold.
Answer: (SHOW ANSWER)

NEW QUESTION: 45
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: (SHOW ANSWER)

The exhibit includes these key debug lines:

start_search_dn-base:'DC=TAC,DC=ottawa,DC=fortinet,DC=com' filter:sAMAccountName=jsmith get_all_dn-Found DN 1:CN=John Smith,CN=Users,DC=TAC,DC=ottawa,DC=fortinet,DC=com The study guide explains that in regular bind, LDAP authentication has four steps, and that during step 2, FortiGate searches the LDAP tree to find the user's DN:

"During the second step, FortiGate does a search query in the LDAP database to find the user's location-in other words, the user's DN. If the user is found, the server replies with the user's DN." It also states for the real-time debug of step 2:

"An fnbamd_ldap_build_dn_search_req-base message indicates that FortiGate is performing step two: searching for the user in the LDAP tree. This message includes the base branch (distinguished name setting) and the name of the attribute used to locate the user... If the LDAP server finds the user, the output shows the user's full DN." That directly proves:

D is correct because the debug is showing step 2: Search Request

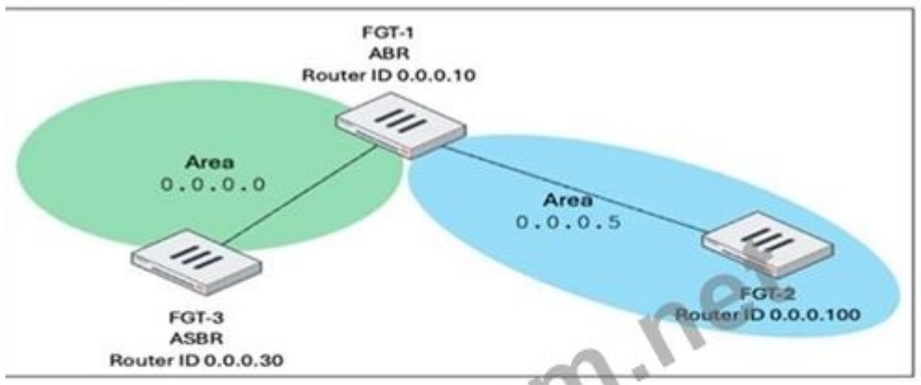
A is correct because the base DN and found DN are under DC=TAC,DC=ottawa,DC=fortinet,DC=com, which corresponds to the LDAP domain/tree root TAC.ottawa.fortinet.com Why the other options are wrong:

B is wrong because binding with the user's credentials is step 3, not the step shown here. The study guide says: "Step 3 - Bind user credentials" and shows that this happens later with fnbamd_ldap_build_userbind_req / __ldap_build_bind_req-Binding to 'CN=John Smith...' C is wrong because collecting user group information is step 4, not the step shown in the exhibit. The study guide says: "The last step is to get the user group information" and shows step 4 with Attr query / memberOf search

NEW QUESTION: 46

Refer to the exhibits.

Network topology



OSPF database

```
FGT-2 # get router info ospf 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         ADV Router      Age  Seq#       CkSum Flag Link count
0.0.0.10        0.0.0.10        302  80000008 13ea  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      Age  Seq#       CkSum Flag
100.64.1.1      0.0.0.10        302  80000001 feaa  0002

                Summary Link States (Area 0.0.0.5 [Stub])

Link ID         ADV Router      Age  Seq#       CkSum Flag Route
0.0.0.0         0.0.0.10        320  80000005 df70  0002 0.0.0.0/0
10.1.0.0        0.0.0.10        315  80000002 fc54  0002 10.1.0.0/24
10.1.10.0       0.0.0.10        311  80000001 9a1c  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: (SHOW ANSWER)

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 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).

NEW QUESTION: 47
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: (SHOW ANSWER)
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."

NEW QUESTION: 48
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=73 expire=3597 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=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=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/if ips view=0 app_list=0 app=0
dd_type=0 dd_mode=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. 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.

C. 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.

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

Answer: (SHOW ANSWER)

NEW QUESTION: 49

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

```
FortiGate # get router info routing-table database

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, port1

FortiGate # get router info routing-table all

Routing table for VRF=0
S*          0.0.0.0/0 [10/0] via 100.64.1.254, port1
```

Why is the port2 default route not in the second command output?

A. The port2 interface is disabled in the FortiGate configuration.

B. The port1 default route has a higher priority value than the default route using port2.

C. The port1 default route has a lower priority value than the default route using port2.

D. The port1 default route has a lower distance than the default route using port2.

Answer: (SHOW ANSWER)

The correct answer is D.

In the exhibit, get router info routing-table database shows both static default routes:

0.0.0.0/0 [20/0] via 100.64.2.254, port2

0.0.0.0/0 [10/0] via 100.64.1.254, port1

But get router info routing-table all shows only:
0.0.0.0/0 [10/0] via 100.64.1.254, port1
The study guide explains that get router info routing-table all displays the routes that make it to the FIB - the best active routes. It also says that this command doesn't show standby or inactive routes, which can remain only in the routing table database. It gives the exact rule: "when two static routes to the same destination subnet have different distances, the one with the lower distance is installed in the routing table, and the one with the higher distance is installed in the routing table database." The study guide also shows the route selection process:
Most specific route
Lowest distance
Lowest metric (dynamic routes)
Lowest priority (static routes)
ECMP
So the port2 default route is absent from the second output because its distance is 20, while the port1 default route has distance 10. The lower-distance route is installed in the active routing table/FIB.
Why the other options are wrong:
A is wrong because the exhibit does not indicate port2 is down or disabled.
B and C are wrong because priority is checked only after distance for static routes. Here, the routes already differ by distance, so priority is not the deciding factor.
So the verified answer is: D.

NEW QUESTION: 50
Refer to the exhibits.

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-B is configured with a distribution list denying the 8.8.8.8/32 network to be injected into the routing table.
Answer: B (LEAVE A REPLY)
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.

NEW QUESTION: 51
Refer to the exhibit, which shows partial outputs from two routing debug commands.

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 (LEAVE A REPLY)

The 7.6 study guide explains the route selection order:

"Route Selection Process

Most specific route

Lowest distance

Lowest metric (dynamic routes)

Lowest priority (static routes)

ECMP (static, BGP, and OSPF routes)"**

It then states:

"If there are multiple routes with the same netmask, distance, metric, and priority, FortiGate shares the traffic among all of them. This is called equal-cost multi-path (ECMP)."

The FortiOS administration guide confirms the ECMP prerequisite:

"Routes must have the same destination and costs. In the case of static routes costs include distance and priority." In the exhibit, the kernel/FIB output shows the two default routes as:

gwy=100.64.1.254 dev=3 (port1) prio=0

gwy=100.64.2.254 dev=6 (port2) prio=10

So although both are default routes, their priorities are different. Since FortiGate uses the FIB/kernel for forwarding traffic, ECMP will not happen until the static-route priorities are the same. The study guide also notes that the FIB is the table used to perform standard routing Therefore, to make the two default routes eligible for ECMP, the administrator must make the priorities equal. Since port2 is already 10, the needed change is to set the port1 default route priority to 10.

Why the other options are wrong:

A is wrong because snat-route-change affects how existing SNAT sessions react to routing changes, not whether static routes qualify for ECMP B is wrong because changing port2 to priority 1 still would not match port1 at 0, so the routes still would not have equal cost for ECMP C is wrong because preserve-session-route affects existing-session route persistence after routing changes, not ECMP qualification

NEW QUESTION: 52

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

Which two statements are true? (Choose two answers)

A. The RADIUS server queried for authentication is located at IP address 172.25.188.164.

B. Authentication was unsuccessful.

C. The authentication scheme used was pop3.

D. Authentication was successful.

E. Two-factor authentication was required.

Answer: (SHOW ANSWER)

The correct answers are A and D.

The debug output shows:

Sent RADIUS req to server 'RadiusServer': IP=172.25.188.164 ... user="student" using CHAP Result for radius svr 'RadiusServer' 172.25.188.164(0) is 0 Sending result 0 for req 2 The study guide explains that in RADIUS real-time debug, FortiGate shows the IP address of the RADIUS server it is querying. In the example, it says FortiGate "creates an access request to the RADIUS server at IP address 10.0.13.130" and shows the line Sent radius req to server ... IP=10.0.13.130 So in your exhibit, the queried server is clearly 172.25.188.164, which makes A correct.

The study guide also states:

"The message fnbamd_comm_send_result-Sending result 0 indicates that the authentication was successful and that FortiGate received the Access-Accept message." Since your exhibit also ends with Sending result 0, that makes D correct.

Why the other options are wrong:

B is wrong because result 0 means authentication successful, not failed C is wrong because the debug explicitly shows using CHAP, and the study guide lists supported RADIUS schemes as CHAP, PAP, MS-CHAP, and MS-CHAPv2 E is wrong because the study guide says two-factor authentication would involve an Access-Challenge response: "If two-factor authentication is enabled on the server, the response is an Access-Challenge message" Your exhibit shows successful result 0 / Access-Accept, not a challenge.

So the verified answers are: A, D.

NEW QUESTION: 53

Refer to the exhibit.

VPN tunnel details

```
Hub # get vpn ipsec tunnel details
gateway
    name: 'Hub2Spoke1'
    type: route-based
    local-gatewav: 10.10.1.1:0 (static)
    remote-gateway: 10.10.2.2:0 (static)
    mode: ike-v1
    interface: 'wan2' (6)
    rx packets: 1025 bytes: 524402 errors: 0
    tx packets: 641 bytes: 93 errors: 0
    dpd: on-demand/negotiated idle: 20000ms retry: 3 count: 0
    selectors
      name: 'Hub2Spoke1'
      auto-negotiate: disable
      mode: tunnel
      src: 0:192.168.1.0/0.0.0.0:0
      dst:0:10.10.20.0/0.0.0.0:0
      SA
        lifetime/rekey: 43200/32137
        mtu: 1438
        tx-esp-seq: 2ce
        replay: enabled
        inbound
          spi: 01e54b14
          enc: aes-cb 914dc5d092667ed436ea7f6efb867976
          auth:  shal a81b019d4cdfda32ce51e6b01d0blea42a74adce
      outbound
        spi: 3dd3545f
        enc:  aes-cb 017b8ff6c4ba21eac99b22380b7de74d
        auth: shal   edd8141f4956140eef703d9042621d3dbf5cd961
      NPU acceleration: encryption (outbound) decryption (inbound)
```


Partial output of the get vpn ipsec tunnel details command is shown. Based on the output, which two statements are correct? (Choose two.)

A. The npu_flag for this tunnel is 02.

B. Different SPI values are a result of auto-negotiation being disabled for phase2 selectors.

C. The npu_flag for this tunnel is 03.

D. Anti-replay is enabled.

Answer: (SHOW ANSWER)

The correct answers are C and D.

The study guide's get vpn ipsec tunnel details example shows:

replay: enabled

inbound and outbound sections with separate SPIs

NPU acceleration: encryption(outbound) decryption(inbound)

and it labels these as "Phase 2 SAs for each direction" and "Hardware acceleration" This directly proves D. Anti-replay is enabled, because the output explicitly says replay: enabled For the NPU status, the study guide explains the exact npu_flag meanings:

npu_flag=00 = both IPsec SAs loaded to the kernel

npu_flag=01 = outbound IPsec SA copied to NPU

npu_flag=02 = inbound IPsec SA copied to NPU
npu_flag=03 = both outbound and inbound IPsec SAs copied to NPU
Because the exhibit shows hardware acceleration in both directions - encryption(outbound) and decryption(inbound) - the matching npu_flag is 03, not 02. That makes C correct and A incorrect.
Why B is wrong:
The same study guide output labels the tunnel as having Phase 2 SAs for each direction, so different inbound and outbound SPIs are normal for the two SAs. Also, the FortiOS administration guide explains that auto-negotiate controls whether phase 2 SA negotiation is initiated automatically, not whether inbound and outbound SPIs are different: "By default the phase 2 security association (SA) is not negotiated until a peer attempts to send data... Auto-negotiate initiates the phase 2 SA negotiation automatically..." So the verified answers are: C, D.

NEW QUESTION: 54
Which Iwo troubleshooting steps should you perform If 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: (SHOW ANSWER)
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:
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."

NEW QUESTION: 55
During the SAML negotiation process, in which section does the Identity Provider (IdP) provide the SAML attributes used in the authentication process to the Service Provider (SP)?
A. Bindings HTTP post
B. Assertion dump
C. Authentication request
D. Authentication response

Answer: (SHOW ANSWER)

The correct answer is B. Assertion dump.

The study guide states: "SAML attributes are pieces of information about a user that are exchanged between IdPs and SPs during the SAML authentication process. These attributes are included in the SAML assertion, which is built by the IdP as part of the authentication process." The same study guide page for real-time SAML troubleshooting shows the section labeled **** Assertion Dump ****, and inside that assertion it displays the actual user attributes, such as:

<saml:Attribute Name="username">

<saml:Attribute Name="groups">

It also explicitly marks this part as "Attributes sent by IdP"

Why the other options are wrong:

A . Bindings HTTP post is incorrect because bindings define how SAML messages are transported, not the section that contains the attributes. The study guide says: "Bindings: Define how SAML protocol messages are transmitted over different communication channels." C . Authentication request is incorrect because that is built by the SP and sent toward the IdP, not where the IdP's user attributes are shown. The study guide's flow says the SP "Builds auth request" and the IdP later "Builds auth response." D . Authentication response is broader than the exact section being asked. The exact section in the study guide where the IdP-provided attributes are shown is the Assertion dump.

So the verified answer is: B.