DUMPSARENA

Fortinet NSE 7 - Enterprise Firewall 6.4

Fortinet NSE7_EFW-6.4

Version Demo

Total Demo Questions: 5

Total Premium Questions: 35

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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

```
# diagnose webfilter fortiguard statistics list

Rating Statistics:
==================
DNS failures                  :    273
DNS lookups                   :    280
Data send failures            :      0
Data read failures            :      0
Wrong package type            :      0
Hash table miss               :      0
Unknown server                :      0
Incorrect CRC                 :      0
Proxy request failures        :      0
Request timeout               :      1
Total requests                :   2409
Request to FortiGuard servers :   1182
Server errored responses      :      0
Relayed rating                :      0
Invalid profile               :      0

Allowed                       :   1021
Blocked                       :   3909
Logged                        :   3927
Blocked Errors                :    565
Allowed Errors                :      0
Monitors                      :      0
Authenticates                 :      0
Warnings:                     :     18
Ovrd request timeout          :      0
Ovrd send failures            :      0
Ovrd read failures            :      0
Ovrd errored responses        :      0

Cache Statistics:
==================
Maximum memory     :
Memory usage       :

Nodes                         :      0
  Leaves                      :      0
    Prefix nodes              :      0
    Exact nodes               :      0

Requests                      :      0
Misses                        :      0
Hits                          :      0
  Prefix hits                 :      0
  Exact hits                  :      0

No cache directives           :      0
Add after prefix              :      0
Invalid DB put                :      0
DB updates                    :      0

Percent full                  :     0%
  Branches                    :     0%
  Leaves                      :     0%
    Prefix nodes              :     0%
    Exact nodes               :     0%

Miss rate                     :     0%
Hit rate                      :     0%
```

Which statement explains why the cache statistics are all zeros?

A. The FortiGuard web filter cache is disabled in the FortiGate configuration.

B. There are no users making web requests.

C. FortiGate is using flow-based inspection, which does not use the cache.

D. The administrator has reallocated the cache memory to a separate process.

ANSWER: A

Explanation:

Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/406127/filtering

Web Filter Cache	Enable/disable web filter cache, and set the amount of time that the FortiGate will store a blocked IP address or URL locally. After the time expires, the FortiGate contacts the FDN to verify the address.
Anti-Spam Cache	Enable/disable email filter cache, and set the amount of time that the FortiGate will store an email address locally.
FortiGuard Filtering Protocol	Select the protocol for contacting the FortiGuard servers.
FortiGuard Filtering Port	Select the port assignments for contacting the FortiGuard servers.
Filtering Service Availability	The status of the filtering service. Click *Check Again* if the filtering service is not available.
Request re-evaluation of a URL's category	Click to re-evaluate a URL category rating on the FortiGuard web filter service.

QUESTION NO: 2

Refer to the exhibits, which show the configuration on FortiGate and partial session information.

```
config system global
    set snat-route-change disable
end
config router static
    edit 1
        set gateway 10.200.1.254
        set priority 5
        set device "port1"
    next
    edit 2
        set gateway 10.200.2.254
        set priority 10
        set device "port2"
    next
end
```

All traffic to the Internet currently egresses from port1. The exhibit shows partial session information for Internet traffic from a user on the internal network.

If the priority on route ID 1 were changes from 5 to 20, what would happen to traffic matching that user session?

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

B. The session would be deleted, and the client would need to start a new session.

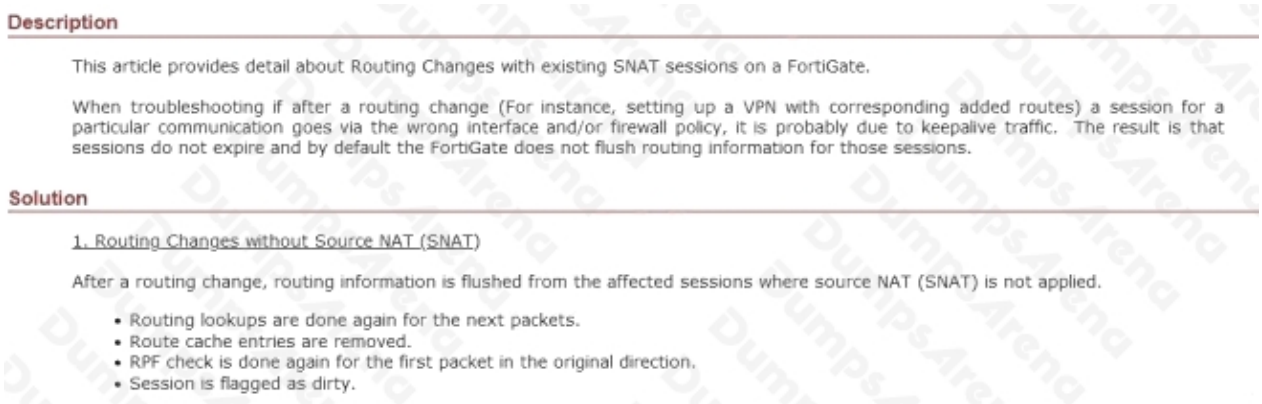
C. The session would remain in the session table, and its traffic would start to egress from port2.

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

ANSWER: A

Explanation:

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD40943



Description

This article provides detail about Routing Changes with existing SNAT sessions on a FortiGate.

When troubleshooting if after a routing change (For instance, setting up a VPN with corresponding added routes) a session for a particular communication goes via the wrong interface and/or firewall policy, it is probably due to keepalive traffic. The result is that sessions do not expire and by default the FortiGate does not flush routing information for those sessions.

Solution

1. Routing Changes without Source NAT (SNAT)

After a routing change, routing information is flushed from the affected sessions where source NAT (SNAT) is not applied.

- Routing lookups are done again for the next packets.
- Route cache entries are removed.
- RPF check is done again for the first packet in the original direction.
- Session is flagged as dirty.

QUESTION NO: 3

Which three conditions are required for two FortiGate devices to form an OSPF adjacency? (Choose three.)

A. OSPF peer IDs match

B. IP addresses are in the same subnet

C. Hello and dead intervals match

D. OSPF IP MTUs match

E. OSPF costs match

ANSWER: B C D

Explanation:

Reference: https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-advanced-routing-54/Routing_OSPF/OSPF_Background_Concepts.htm#Adjacenc

For two OSPF routers to become neighbors, the following conditions must be met.

- The subnet mask used on both routers must be the same subnet.
- The subnet number derived using the subnet mask and each router's interface IP address must match.
- The Hello interval & The Dead interval must match.
- The routers must have the same OSPF area ID. If they are in different areas, they are not neighbors.
- If authentication is used, they must pass authentication checks.

If any of these parameters are different between the two routers, the routers do not become OSPF neighbors and cannot be adjacent. If the routers become neighbors, they are adjacent.

QUESTION NO: 4

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

```
FGT # get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
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
```

Which statement about the exhibit is true?

A. The local router has not established a TCP session with 100.64.3.1

B. The local router BGP state is OpenConfirm with the 10.127.0.75 peer.

C. Since the counters were last reset, the 100.64.3.1 peer has never been down.

D. The local router has received a total of three BGP prefixes from all peers.

ANSWER: A

Explanation:

Active means it is actively trying to establish a TCP connection using port 179, but has not yet actually established one.

QUESTION NO: 5

Which two conditions must be met for a static route to be active in the routing table? (Choose two.)

A. The link health monitor (if configured) is up.

B. The next-hop IP address is up.

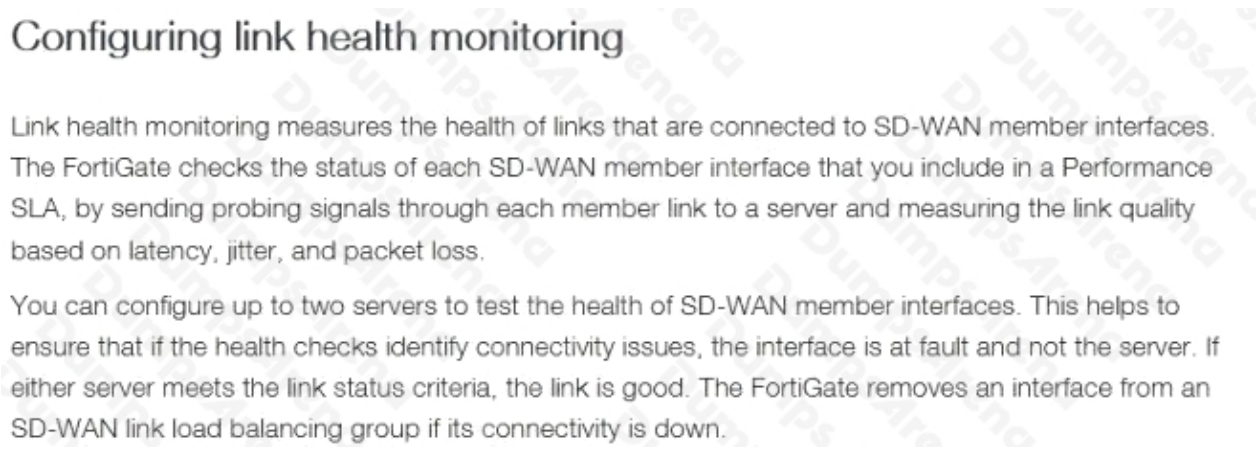
C. The outgoing interface is up.

D. There is no other route to the same destination, with a higher distance.

ANSWER: A C

Explanation:

Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/370572/configuring-link-health-monitoring



Configuring link health monitoring

Link health monitoring measures the health of links that are connected to SD-WAN member interfaces. The FortiGate checks the status of each SD-WAN member interface that you include in a Performance SLA, by sending probing signals through each member link to a server and measuring the link quality based on latency, jitter, and packet loss.

You can configure up to two servers to test the health of SD-WAN member interfaces. This helps to ensure that if the health checks identify connectivity issues, the interface is at fault and not the server. If either server meets the link status criteria, the link is good. The FortiGate removes an interface from an SD-WAN link load balancing group if its connectivity is down.