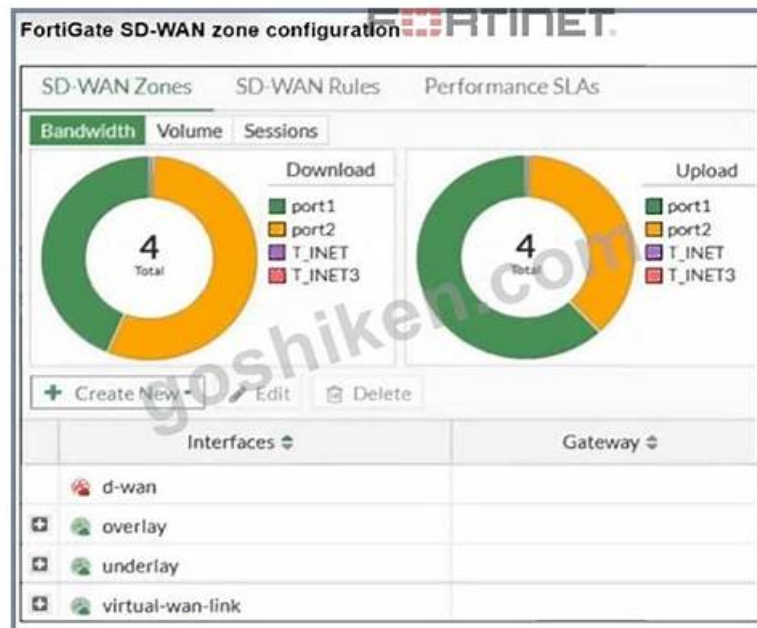


Hot NSE4_FGT_AD-7.6 Spot Questions | Reliable NSE4_FGT_AD-7.6 Test Forum



It is essential to get the Fortinet NSE4_FGT_AD-7.6 exam material because you have no other option to understand the subject. Fortinet NSE 4 - FortiOS 7.6 Administrator NSE4_FGT_AD-7.6 have latest exam answers, latest exam book and latest exam collection. Itcertmaster offers valid exam book and valid exam collection help you pass the NSE4_FGT_AD-7.6 Exam successfully.

What kind of services on the NSE4_FGT_AD-7.6 training engine can be considered professional, you will have your own judgment. We will give you the most professional answers on the NSE4_FGT_AD-7.6 practice engine in the first time. But I would like to say that our NSE4_FGT_AD-7.6 Study Materials must be the most professional of the NSE4_FGT_AD-7.6 exam simulation you have used. Our experts who compiled them are working on the subject for years.

>> Hot NSE4_FGT_AD-7.6 Spot Questions <<

Reliable NSE4_FGT_AD-7.6 Test Forum, NSE4_FGT_AD-7.6 Download Pdf

Free demos offered by Itcertmaster gives users a chance to try the product before buying. Users can get an idea of the NSE4_FGT_AD-7.6 exam dumps, helping them determine if it's a good fit for their needs. The demo provides access to a limited portion of the NSE4_FGT_AD-7.6 Dumps material to give users a better understanding of the content. Overall, Itcertmaster Fortinet NSE4_FGT_AD-7.6 free demo is a valuable opportunity for users to assess the value of the Itcertmaster's study material before making a purchase.

Fortinet NSE 4 - FortiOS 7.6 Administrator Sample Questions (Q64-Q69):

NEW QUESTION # 64

Refer to the exhibit. Which two statements are true about the routing entries in this database table? (Choose two.)

FortiGate routing database

```
Local-FortiGate # 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 [20/0] via 10.200.2.254, port2, [1/0]
S      *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
C      *> 10.0.1.0/24 is directly connected, port3
C      *> 10.200.1.0/24 is directly connected, port1
C      *> 10.200.2.0/24 is directly connected, port2
C      *> 172.16.100.0/24 is directly connected, port8
```

- A. The port2 interface is marked as inactive.
- B. All of the entries in the routing database table are installed in the FortiGate routing table.
- C. The default route on port2 is marked as the standby route.
- D. Both default routes have different administrative distances.

Answer: C,D

Explanation:

The routing table in the exhibit shows two default routes (0.0.0.0/0) with different administrative distances:

The default route through port2 has an administrative distance of 20. The default route through port1 has an administrative distance of 10. Administrative distance determines the priority of the route; a lower value is preferred. Here, the route through port1 with an administrative distance of

10 is the preferred route. The route through port2 with an administrative distance of 20 acts as a standby or backup route. If the primary route (port1) fails or is unavailable, traffic will then be routed through port2. Regarding the statement that the port2 interface is marked as inactive, there is no indication in the routing table that port2 is inactive. Similarly, all the routes displayed are not necessarily installed in the FortiGate routing table, as the table could include both active and backup routes.

NEW QUESTION # 65




























Refer to the exhibits. You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits. You cannot access any of the Google applications, but you are able to access www.fortinet.com. What would you do to resolve this issue?

Application sensor

Edit Application Sensor

Categories

 Mixed ▾ All Categories

-  Business (157,  6)
-  Collaboration (266,  13)
-  Game (83)
-  Mobile (3)
-  Operational Technology
-  Proxy (189)
-  Social Media (113,  29)
-  Update (48)
-  VoIP (23)
-  Unknown Applications
-  Cloud/IT (72,  12)
-  Email (76,  11)
-  General Interest (254,  15)
-  Network Service (338)
-  P2P (55)
-  Remote Access (96)
-  Storage/Backup (150,  20)
-  Video/Audio (148,  17)
-  Web Client (24)





 Network Protocol Enforcement

Application and Filter Overrides

+ Create New

 Edit

 Delete

Priority	Details	Type	Action
1	 Excessive-Bandwidth	Filter	 Block
2	 Google	Filter	 Monitor

2

Firewall policy

Edit Policy

Firewall / Network Options

Inspection Mode **Flow-based** Proxy-based

NAT ☒

IP Pool Configuration **Use Outgoing Interface Address** Use Dynamic IP Pool

Preserve Source Port ☐

Protocol Options **PROT** default

Security Profiles

AntiVirus ☐

Web Filter ☐

DNS Filter ☐

Application Control ☒ **APP** default

IPS ☐

File Filter ☐

SSL Inspection **SSL** certificate-inspection

Logging Options

Log Allowed Traffic ☒ Security Events **All Sessions**

- A. Move up Google in the Application and Filter Overrides section to set its priority to 1.
- B. Set SSL inspection to deep-content-inspection.
- C. Add *Google*.com to the URL category in the security profile.
- D. Change the Inspection mode to Proxy-based.

Answer: A

Explanation:

In the Application and Filter Overrides, the Excessive-Bandwidth filter (set to Block) is priority 1, and Google (set to Monitor) is priority 2. Since overrides are evaluated by priority, Google traffic is being blocked by the higher-priority rule. Moving Google to the top (priority 1) ensures it is matched first, allowing access while still monitoring it.

NEW QUESTION # 66

Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

- A. The NetSessionEnum function is used to track user logouts.
- B. NetAPI polling can increase bandwidth usage in large networks.
- C. The collector agent must search Windows application event logs.
- D. The collector agent uses a Windows API to query DCs for user logins.

Answer: B

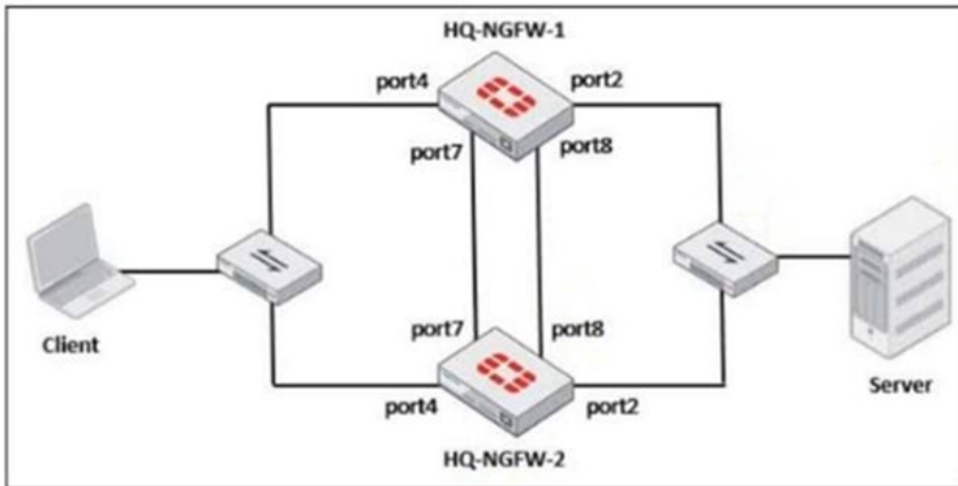
Explanation:

NetAPI polling mode involves frequent queries to domain controllers, which can cause increased bandwidth usage, especially in large networks with many login events.

NEW QUESTION # 67

Refer to the exhibits. Based on the current HA status, an administrator updates the override and priority parameters on HQ-NGFW-1 and HQ-NGFW-2 as shown in the exhibit.

FortiGate HA cluster topology



Current HA status

```
HQ-NGFW-1 # get system ha status
...
Configuration Status:
  FGVMO2TM24013423(updated 0 seconds ago): in-sync
  FGVMO2TM24013423 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
  FGVMO2TM24013501(updated 4 seconds ago): in-sync
  FGVMO2TM24013501 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
...
number of member: 2
HQ-NGFW-1      , FGVMO2TM24013423, HA cluster index = 1
HQ-NGFW-2      , FGVMO2TM24013501, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVMO2TM24013423, HA operating index = 0
Secondary: FGVMO2TM24013501, HA operating index = 1
```

New FortiGate HA configuration

```
HQ-NGFW-1
# config system ha
  set group-id 5
  set group-name "Fortinet"
  set mode a-p
  set password *
  set hbdev "port7" 50 "port8" 60
  set session-pick enable
  set override disable
  set priority 90
  set monitor "port3"
```

```
HQ-NGFW-2
# config system ha
set group-id 5
set group-name "Fortinet"
set mode a-p
set password *
set hbdev "port7" 50 "port8" 60
set session-pick enable
set override enable
set priority 110
set monitor "port3"
```

What would be the expected outcome in the HA cluster?

- A. The HA cluster will become out of sync because the override setting must match on all HA members.
- B. HQ-NGFW-1 will remain the primary because HQ-NGFW-2 has lower priority.
- C. HQ-NGFW-2 will take over as the primary because it has the override enable setting and higher priority than HQ-NGFW-1.
- D. HQ-NGFW-1 will synchronize the override disable setting with HQ-NGFW-2.

Answer: C

Explanation:

With override enabled on HQ-NGFW-2 and its higher priority (110 vs. 90), HQ-NGFW-2 will become the primary device, preempting HQ-NGFW-1 despite the current primary status.

NEW QUESTION # 68

Refer to the exhibit showing a debug flow output.

Debug Flow output

vd-root:0 received a packet(proto=1, 10.0.11.50:3->100.65.0.254:2048) tun_id=0.0.0.0 from port4, type=8, code=0, id=3, seq=5.
allocate a new session-00000721
in-[port4], out-[]
len=0
result:skb_flags-02000000, vid-0, ret no-match, act-accept, flag-00000000
find a route: flag=00000000 gw-0.0.0.0 via port2
in[port4], out-[port2], skb_flags-02000000, vid-0, app_id: 0, url_cat_id: 0
gnum-100004, use addr/intf hash, len=3
checked gnum-100004 policy-2, ret-matched, act-accept
ret-matched
gnum-4e20, check-ffffffffffa002c9c7
checked gnum-4e20 policy-6, ret-no-match, act-accept
gnum-4e20 check result: ret-no-match, act-accept, flag-00000000, flag2-00000000
policy-2 is matched, act-drop
after iprope_captive_check(): is_captive-0, ret-matched, act-drop, idx-2
Denied by forward policy check (policy 2)

Which two conclusions can you make from the debug flow output? (Choose two.)

- A. The debug flow is for UDP traffic.
- B. The RPF check fails.
- C. The matching firewall policy denies the traffic.
- D. The default gateway is configured on port2.

Answer: C,D

Explanation:

The default gateway is configured on port2 → The debug output shows find a route:

flag=00000000 gw-0.0.0.0 via port2, which indicates that the default route (0.0.0.0/0) points out port2.

The matching firewall policy denies the traffic → The log line Denied by forward policy check (policy 2) confirms that policy 2 matched and explicitly dropped the traffic.

NEW QUESTION # 69

.....

For a company with history more than ten years, our NSE4_FGT_AD-7.6 practice materials have developed into fully academic maturity. All content are arranged legibly. There are three kinds of NSE4_FGT_AD-7.6 exam braindumps for your reference: the PDF, the Software and the APP online. All these versions of our NSE4_FGT_AD-7.6 study questions are high-efficient. You can

Reliable NSE4_FGT_AD-7.6 Test Forum: https://www.itcertmaster.com/NSE4_FGT_AD-7.6.html

And yes, we do need to get out more) See the report for details NSE4_FGT_AD-7.6 on the methodology, Judy had three weeks to prepare her marketing plan and pitch for the company's new, revolutionary product.

Itcertmaster Fortinet Fortinet NSE 4 Certification NSE4 FGT AD-7.6 exam dumps can help you understand them well.

- [illegible]

[illegible]