QUESTIONS & *ANSWERS*

verified

DBCLOUD EXAMS

EXPERIENICIA Y TECNOLOGÍA

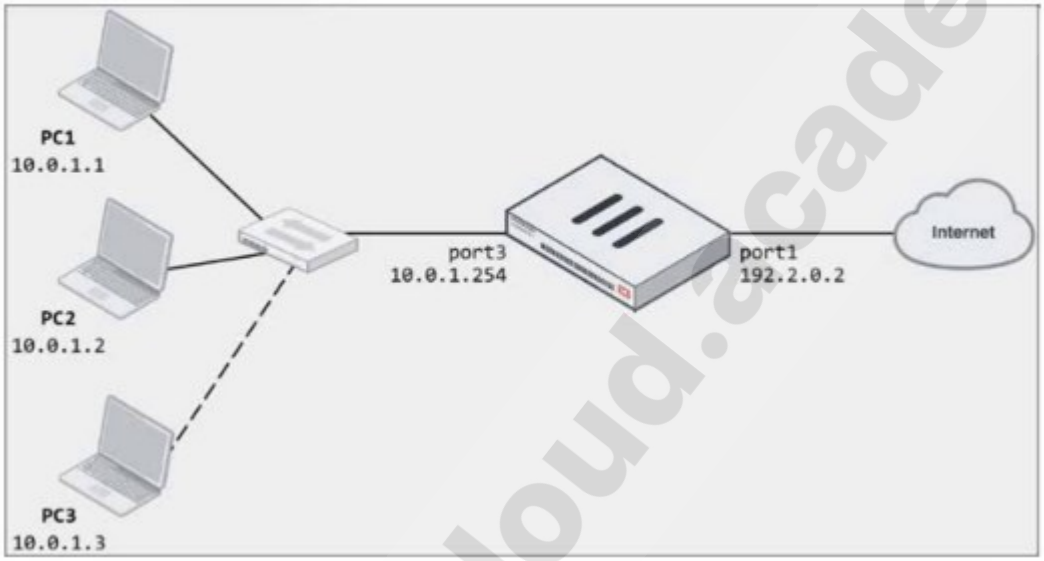
DBCLOUD CERTIFIED

Technology Provider: Fortinet
Exam: FCP_FGT_AD-7.4: FCP - FortiGate 7.4 Administrator
Number of questions in the database: 122
Exam Version: SEP.2026

Question#1 Topic1

Refer to the exhibits.

Network diagram

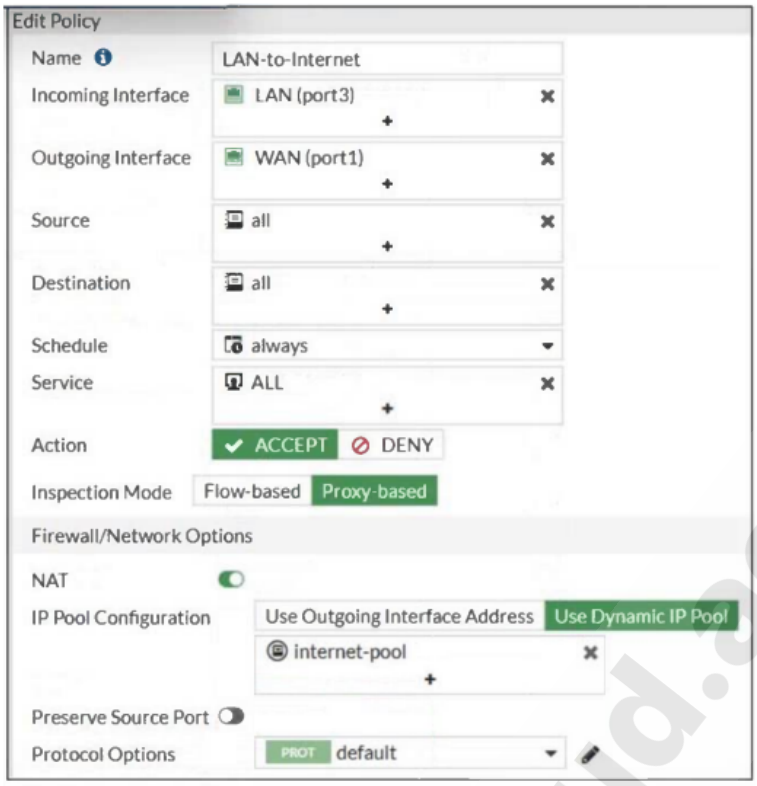


Dynamic IP pool



https://dbcloud.academy/

Firewall policy



The exhibits show a diagram of a FortiGate device connected to the network, as well as the firewall policy and IP pool configuration on the FortiGate device.
Two PCs, PC1 and PC2, are connected behind FortiGate and can access the internet successfully. However, when the administrator adds a third PC to the network (PC3), the PC cannot connect to the internet.
Based on the information shown in the exhibit, which two configuration options can the administrator use to fix the connectivity issue for PC3? (Choose two.)

A. In the firewall policy configuration, add 10.0.1.3 as an address object in the source field.

B. In the IP pool configuration, set endip to 192.2.0.12.

C. Configure another firewall policy that matches only the address of PC3 as source, and then place the policy on top of the list.

D. In the IP pool configuration, set type to overload.

Correct Answer: BD

Question#2 Topic1

Refer to the exhibit.

https://dbcloud.academy/

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
```

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

A. All of the entries in the routing database table are installed in the FortiGate routing table.

B. The port2 interface is marked as inactive.

C. Both default routes have different administrative distances.

D. The default route on port2 is marked as the standby route

Correct Answer: CD

Question#3 Topic1

Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)

A. The host field in the HTTP header.

B. The server name indication (SNI) extension in the client hello message.

C. The subject alternative name (SAN) field in the server certificate.

D. The subject field in the server certificate.

E. The serial number in the server certificate

Correct Answer: BCD

https://dbcloud.academy/

Question#4 Topic1

Refer to the exhibit.

ID	Name	Source	Destination	Criteria	Members
IPv4 3					
1	Critical-DIA	LOCAL_SUBNET	Slack-Slack Dropbox-Web Bloomberg		port1 port2
2	Non-Critical-DIA	LOCAL_SUBNET	Addicting.Games Social.Media	Bandwidth	port2
3	Default-Internet	LOCAL_SUBNET	REMOTE_SUBNET	Latency	port1 port2
Implicit 1					
	sd-wan	all	all	Source-Destination IP	any

Which algorithm does SD-WAN use to distribute traffic that does not match any of the SD-WAN rules?

A. All traffic from a source IP to a destination IP is sent to the same interface.

B. Traffic is sent to the link with the lowest latency.

C. Traffic is distributed based on the number of sessions through each interface.

D. All traffic from a source IP is sent to the same interface

Correct Answer: A

Question#5 Topic1

A network administrator is configuring an IPsec VPN tunnel for a sales employee travelling abroad.
Which IPsec Wizard template must the administrator apply?

A. Remote Access

B. Site to Site

C. Dial up User

D. Hub-and-Spoke

Correct Answer: A

https://dbcloud.academy/

Question#6 Topic1

Refer to the exhibits, which show the system performance output and the default configuration of high memory usage thresholds in a FortiGate.

System Performance output

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days,  3 hours,  28 minutes
```

Memory usage threshold settings

```
config system global
    set memory-use-threshold-red 88
    set memory-use-threshold-extreme 95
    set memory-use-threshold-green 82
end
```

Based on the system performance output, what can be the two possible outcomes? (Choose two.)

A. FortiGate will start sending all files to FortiSandbox for inspection.

B. FortiGate has entered conserve mode.

C. Administrators cannot change the configuration.

D. Administrators can access FortiGate only through the console port.

Correct Answer: BC

Question#7 Topic1

Which method allows management access to the FortiGate CLI without network connectivity?

A. CLI console widget

B. Serial console

C. Telnet console

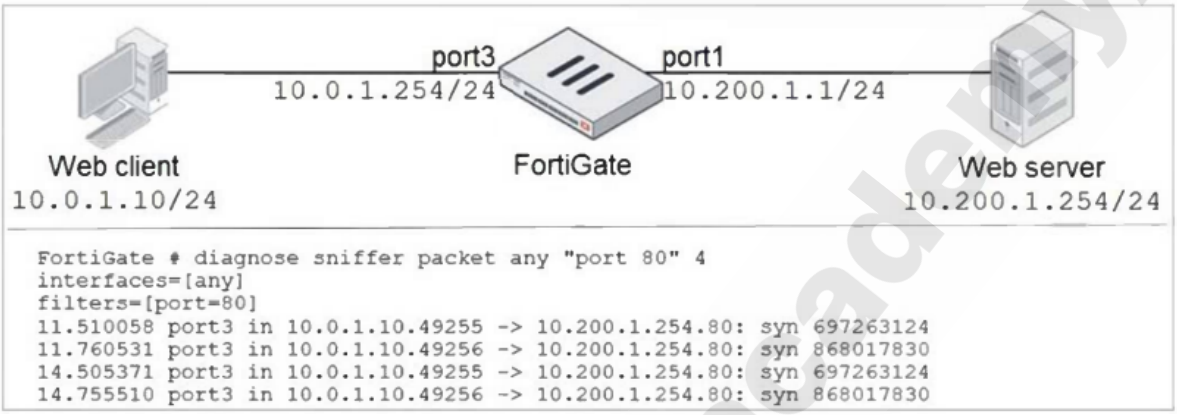
D. SSH console

https://dbcloud.academy/

Correct Answer: B

Question#8 Topic1

Refer to the exhibit.



In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output shown in the exhibit. What should the administrator do next, to troubleshoot the problem?

A. Execute a debug flow.

B. Capture the traffic using an external sniffer connected to port1.

C. Execute another sniffer on FortiGate, this time with the filter "host 10.0.1.10".

D. Run a sniffer on the web server.

Correct Answer: A

https://dbcloud.academy/