

Fortinet

Exam Questions NSE4_FGT_AD-7.6

Fortinet NSE 4 - FortiOS 7.6 Administrator



NEW QUESTION 1

A network administrator is reviewing firewall policies in both Interface Pair View and By Sequence View. The policies appear in a different order in each view. Why is the policy order different in these two views?

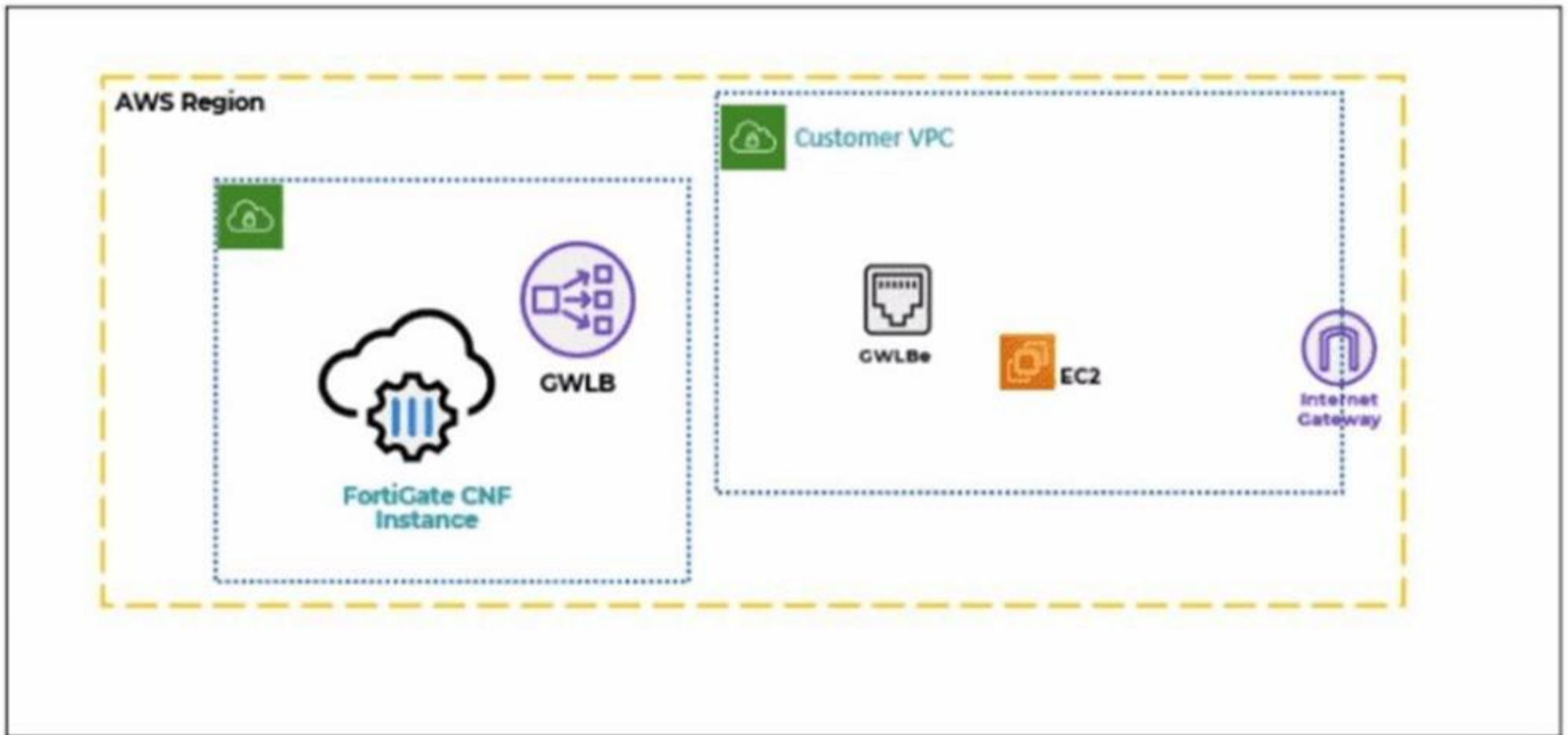
- A. By Sequence View groups policies based on rule priority, while Interface Pair View always follows the order of traffic logs.
- B. The firewall dynamically reorders policies in Interface Pair View based on recent traffic patterns, but By Sequence View remains static.
- C. Interface Pair View sorts policies based on matching interfaces, while By Sequence View shows the actual processing order of rules.
- D. Policies in Interface Pair View are prioritized by security levels, while By Sequence View strictly follows the administrator's manual ordering.

Answer: C

NEW QUESTION 2

Refer to the exhibit.

A partial cloud topology is shown.



You deployed a FortiGate Cloud-Native Firewall (CNF) in AWS. During the deployment, which components must the FortiGate CNF create to handle traffic from the EC2 instance?

- A. The customer VPC and GWLB
- B. The gateway load balancer endpoint (GWLBe) in the customer virtual private cloud (VPC)
- C. The CNF VP
- D. customer VP
- E. and GWLB
- F. The GWL
- G. GWLBe, and the internet gateway (IGW) in the customer VPC

Answer: B

NEW QUESTION 3

Refer to the exhibit.

```
FortiGate # diagnose debug rating
Locale      : english

Service     : Web-filter
Status      : Enable
License     : Contract
\
Num. of servers : 1
Protocol    : https
Port        : 8888
Anycast     : Disable
Default servers : Not included

--- Server List (Wed Sep 20 09:22:42 2023) ---
IP          Weight  RTT  Flags  TZ  FortiGuard-requests  Curr Lost  Total Lost  Updated Time
10.0.1.241  -244   2 I    0    122                 0          0  Wed Sep 20 09:21:55 2023
```

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

- A. The weight increases as the number of failed packets rises
- B. You can configure unreliable protocols to communicate with FortiGuard Server.

- C. FortiGate identified the FortiGuard Server using DNS lookup.
- D. FortiGate is using the default port for FortiGuard communication.

Answer: AD

NEW QUESTION 4

An administrator wants to configure dead peer detection (DPD) on IPsec VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when there is no inbound traffic.
Which DPD mode on FortiGate meets this requirement?

- A. On Demand
- B. Enabled
- C. On Idle
- D. Usabled

Answer: A

NEW QUESTION 5

An administrator manages a FortiGate model that supports NTurbo How does NTurbo acceleration enhance antivirus performance?

- A. For flow-based inspectio
- B. NTurbo establishes a dedicated data path to redirect traffic between the IPS engine and FortiGate ingress and egress interfaces.
- C. For flow-based inspectio
- D. NTurbo creates two inspection sessions on the FortiGate device.
- E. For proxy-based inspectio
- F. NTurbo offloads traffic to the content processor.
- G. For proxy-based inspectio
- H. NTurbo buffers the whole file and then sends it to the antivirus engine.

Answer: A

NEW QUESTION 6

Which two statements describe characteristics of automation stitches? (Choose two answers)

- A. Actions involve only devices included in the Security Fabric.
- B. An automation stitch can have multiple triggers.
- C. Multiple actions can run in parallel.
- D. Triggers can involve external connectors.

Answer: CD

NEW QUESTION 7

Refer to the exhibit.

```
HQ-NGFW-1 # diagnose test application ipsmonitor 1
pid = 2044, engine count = 0 (+1)
0 - pid:2074:2074 cfg:1 master:0 run:1
```

As an administrator you have created an IPS profile, but it is not performing as expected. While testing you got the output as shown in the exhibit What could be the possible reason of the diagnose output shown in the exhibit?

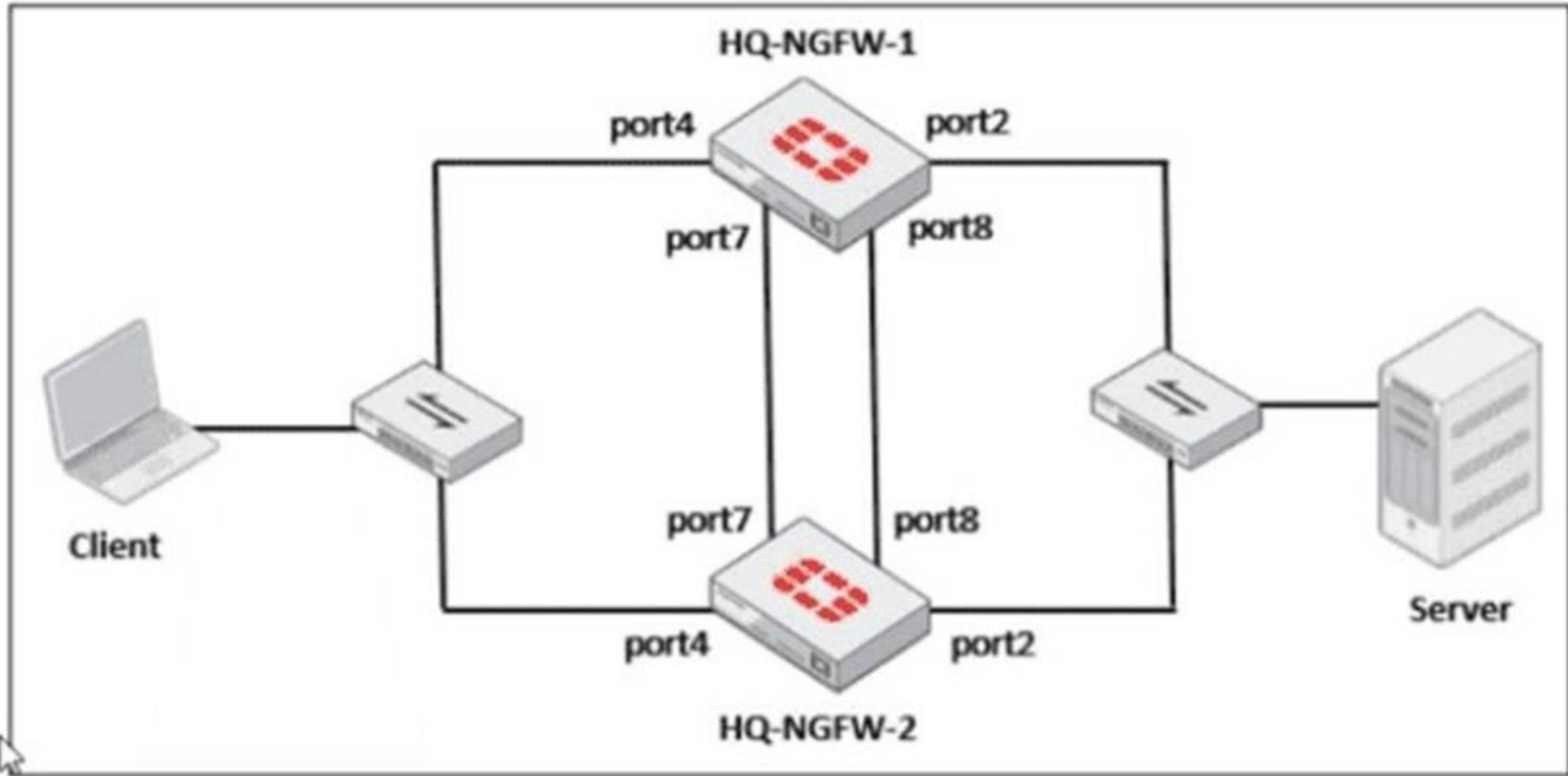
- A. There is a no firewall policy configured with an IPS security profile.
- B. Administrator entered the command diagnose test application ipsmonitor 5.
- C. FortiGate entered into IPS fail open state.
- D. Administrator entered the command diagnose test application ipsmonitor 99.

Answer: A

NEW QUESTION 8

Refer to the exhibits.

FortiGate HA cluster topology



Current HA status

```
HQ-NGFW-1 # get system ha status
...
Configuration Status:
  FGVM02TM24013423(updated 0 seconds ago): in-sync
  FGVM02TM24013423 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
  FGVM02TM24013501(updated 4 seconds ago): in-sync
  FGVM02TM24013501 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      , FGVM02TM24013423, HA cluster index = 1
HQ-NGFW-2      , FGVM02TM24013501, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM02TM24013423, HA operating index = 0
Secondary: FGVM02TM24013501, 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"
```

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 exhibits. What would be the expected outcome in the HA cluster?

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

Answer: A

NEW QUESTION 9

Refer to the exhibit.

Destination ⇅	Gateway IP ⇅	Interface ⇅	Status ⇅
0.0.0.0/0	100.65.0.254	 port2	 Enabled
10.10.10.0/24	100.66.0.254	 port3	 Enabled
10.0.13.0/24	10.0.13.125	 port6	 Enabled

Based on the routing table shown in the exhibit, which two statements are true? (Choose two.)

- A. A packet with the source IP address 10.0.13.10 arriving on port2 is allowed if strict RPF is disabled.
- B. A packet with the source IP address 10.100.110.10 arriving on port2 is allowed if strict RPF is enabled.
- C. A packet with the source IP address 10.100.110.10 arriving on port3 is allowed if strict RPF is disabled.
- D. A packet with the source IP address 10.10.10.10 arriving on port2 is allowed if strict RPF is enabled.

Answer: AC

NEW QUESTION 10

Refer to the exhibits.

Application sensor

Edit Application Sensor

Categories

Mixed ▾
All Categories

Business (157, 6)

Cloud/IT (72, 12)

Collaboration (266, 13)

Email (76, 11)

Game (83)

General Interest (254, 15)

Mobile (3)

Network Service (338)

Operational Technology

P2P (55)

Proxy (189)

Remote Access (96)

Social Media (113, 29)

Storage/Backup (150, 20)

Update (48)

Video/Audio (148, 17)

VoIP (23)

Web Client (24)

Unknown Applications

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:

Video filter:

DNS filter:

Application control: APP default

IPS:

File filter:

SSL inspection: SSL certificate-inspection

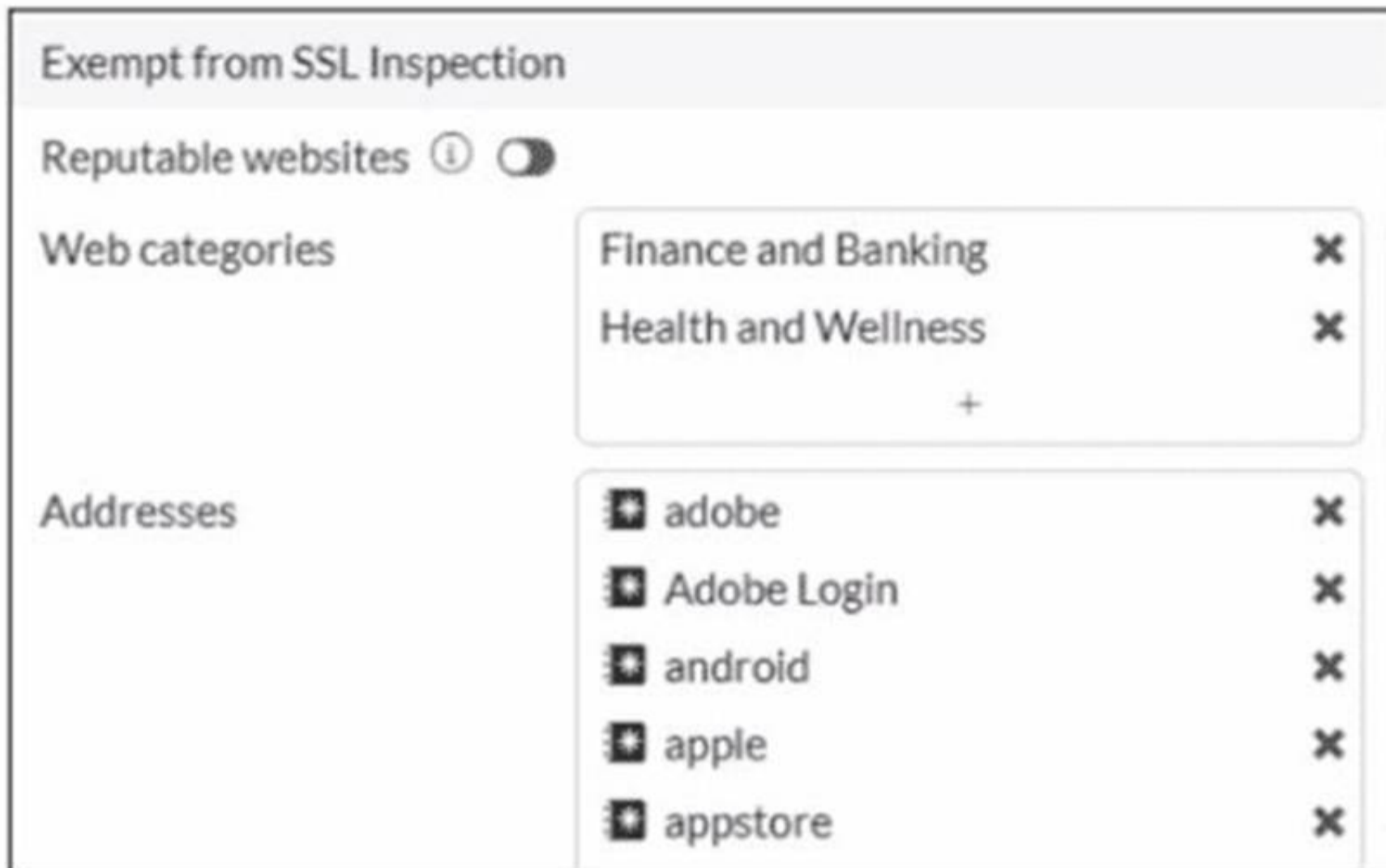
You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits. You cannot access any of the Google applications, but you are able to access www.fortinet.com. Which two actions would you take to resolve the issue? (Choose two.)

- A. Set SSL inspection to deep-content inspection.
- B. Move up Google in the Application and Filter Overrides section to set its priority lot
- C. Add "Google".com to the URL category in the security profile.
- D. Change the Inspection mode to Flow-based
- E. Set the action for Google in the Application and Filter Overrides section to Allow

Answer: BE

NEW QUESTION 10

Refer to the exhibit.



The predefined deep-inspection and custom-deep-inspection profiles exclude some web categories from SSL inspection, as shown in the exhibit For which two reasons are these web categories exempted? (Choose two.)

- A. The resources utilization is optimized because these websites are in the trusted domain list on FortiGate.
- B. The legal regulation aims to prioritize user privacy and protect sensitive information for these websites.
- C. These websites are in an allowlist of reputable domain names maintained by FortiGuard.
- D. The FortiGate temporary certificate denies the browser's access to websites that use HTTP Strict Transport Security.

Answer: BC

NEW QUESTION 12

Which three statements about SD-WAN performance SLAs are true? (Choose three.)

- A. They rely on session loss and jitter.
- B. They monitor the state of the FortiGate device.
- C. All the SLA targets can be configured.
- D. They are applied in a SD-WAN rule lowest cost strategy.
- E. They can be measured actively or passively.

Answer: CDE

NEW QUESTION 17

You have created a web filter profile named restrictmedia-profile with a daily category usage quota. When you are adding the profile to the firewall policy, the restrict_media-profile is not listed in the available web profile drop down. What could be the reason?

- A. The web filter profile is already referenced in another firewall policy.
- B. The firewall policy is in no-inspection mode instead of deep-inspection.
- C. The naming convention used in the web filter profile is restricting it in the firewall policy.
- D. The inspection mode in the firewall policy is not matching with web filter profile feature set.

Answer: D

NEW QUESTION 22

Refer to the exhibit.

SD-WAN traffic log

Application Name	Result	Policy ID	Destination Interface	SD-WAN Quality	SD-WAN Rule Name
YouTube	✓ Accept (8.08 kB / 27...	1 (DIA)	port2		
YouTube	✓ Accept (UTM Allowed)	1 (DIA)	port2		
Facebook	✓ Accept (UTM Allowed)	1 (DIA)	port1		
Facebook	✓ Accept (UTM Allowed)	1 (DIA)	port1		
Facebook	✓ Accept (3.33 kB / 10...	1 (DIA)	port1		
YouTube	✓ Accept (44.63 kB / 3...	1 (DIA)	port2		
CNN	✓ Accept (UTM Allowed)	1 (DIA)	port1		
CNN	✓ Accept (UTM Allowed)	1 (DIA)	port2		
CNN	✓ Accept (UTM Allowed)	1 (DIA)	port2		

The administrator configured SD-WAN rules and set the FortiGate traffic log page to display SD-WAN-specific columns: SD-WAN Quality and SD-WAN Rule Name. FortiGate allows the traffic according to policy ID 1 placed at the top. This is the policy that allows SD-WAN traffic. Despite these settings, the traffic logs do not show the name of the SD-WAN rule used to steer those traffic flows. What could be the reason?

- A. SD-WAN rule names do not appear immediately.
- B. The administrator must refresh the page.
- C. There is no application control profile applied to the firewall policy.
- D. Destinations in the SD-WAN rules are configured for each application, but feature visibility is not enabled.
- E. FortiGate load balanced the traffic according to the implicit SD-WAN rule.

Answer: D

NEW QUESTION 25

What are two characteristics of HA cluster heartbeat IP addresses in a FortiGate device? (Choose two.)

- A. Heartbeat IP addresses are used to distinguish between cluster members.
- B. The heartbeat interface of the primary device in the cluster is always assigned IP address 169.254.0.1.
- C. A change in the heartbeat IP address happens when a FortiGate device joins or leaves the cluster.
- D. Heartbeat interfaces have virtual IP addresses that are manually assigned.

Answer: AC

NEW QUESTION 29

Refer to the exhibit.

```
date=2025-09-03 time=09:09:57 id=7545895911432388608 itime="2025-09-03 09:10:02" euid=3 epid=3 dsteuid=3 dstepid=101
logflag=0 logver=706003401 type="utm" subtype="app-ctrl" level="warning" action="block" sessionid=510 policyid=1 srcip=
10.0.11.50 dstip=54.146.230.62 srcport=53398 dstport=80 proto=6 logid=1059028705 service="HTTP" eventtime=
1756915797391471958 incidentserialno=116391982 direction="outgoing" apprisk="elevated" appid=30220 srcintfrole="undefined"
dstintfrole="undefined" applist="default" appcat="Video/Audio" app="ABC.Com" hostname="abc.go.com" url="/favicon.ico"
eventtype="signature" srcintf="port4" dstintf="port2" msg="Video/Audio: ABC.Com" tz="-0700" policytype="policy"
srccountry="Reserved" dstcountry="United States" poluid="b11ac58c-791b-51e7-4600-12f829a689d9" agent="Mozilla/5.0 (X11;
Ubuntu; Linux x86_64; rv:142.0) Gecko/20100101 Firefox/142.0" httpmethod="GET" referralurl="http://abc.go.com/"
devid="FGVM02TM24013423" vd="root" dtime="2025-09-03 09:09:57" itime_t=1756915802 devname="HQ-NGFW-1"
```

Which two ways can you view the log messages shown in the exhibit? (Choose two.)

- A. By right clicking the implicit deny policy
- B. Using the FortiGate CLI command diagnose log test
- C. By filtering by policy universally unique identifier (UUID) and application name in the log entry
- D. In the Forward Traffic section

Answer: CD

NEW QUESTION 32

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

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

Answer: B

NEW QUESTION 33

Refer to the exhibit.
 A routing table is shown

Network	Gateway IP	Interfaces	Distance	Metric	Priority	Type
10.0.11.0/24	0.0.0.0	port4	0	0	0	Connected
10.0.12.0/24	0.0.0.0	port5	0	0	0	Connected
10.0.13.0/24	0.0.0.0	port6	0	0	0	Connected
100.65.0.0/24	0.0.0.0	port2	0	0	0	Connected
100.66.0.0/24	0.0.0.0	port3	0	0	0	Connected
172.20.1.0/24	100.66.0.254	port3	9	0	2	Static
192.168.0.0/16	0.0.0.0	port1	0	0	0	Connected

An administrator wants to create a new static route so the traffic to the subnet 172.20.1.0/24 is routed through port2 only. What are the two criteria that the administrator can use to achieve this objective? (Choose two.)

- A. The new static route must have the priority set to 3.
- B. The new static route must have the metric set to 1.
- C. The existing static route through port3 must have the distance set to 11.
- D. The new static route must have the distance set to 9

Answer: CD

NEW QUESTION 35

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE4_FGT_AD-7.6 Practice Exam Features:

- * NSE4_FGT_AD-7.6 Questions and Answers Updated Frequently
- * NSE4_FGT_AD-7.6 Practice Questions Verified by Expert Senior Certified Staff
- * NSE4_FGT_AD-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE4_FGT_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE4_FGT_AD-7.6 Practice Test Here](#)