

# Fortinet

## Exam Questions NSE4\_FGT\_AD-7.6

Fortinet NSE 4 - FortiOS 7.6 Administrator



**NEW QUESTION 1**

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-fffffffa002c9c7

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 answers)

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

**Answer:** AD

**NEW QUESTION 2**

There are multiple dialup IPsec VPNs configured in aggressive mode on the HQ FortiGate. The requirement is to connect dial-up users to their respective department VPN tunnels.

Which phase 1 setting you can configure to match the user to the tunnel?

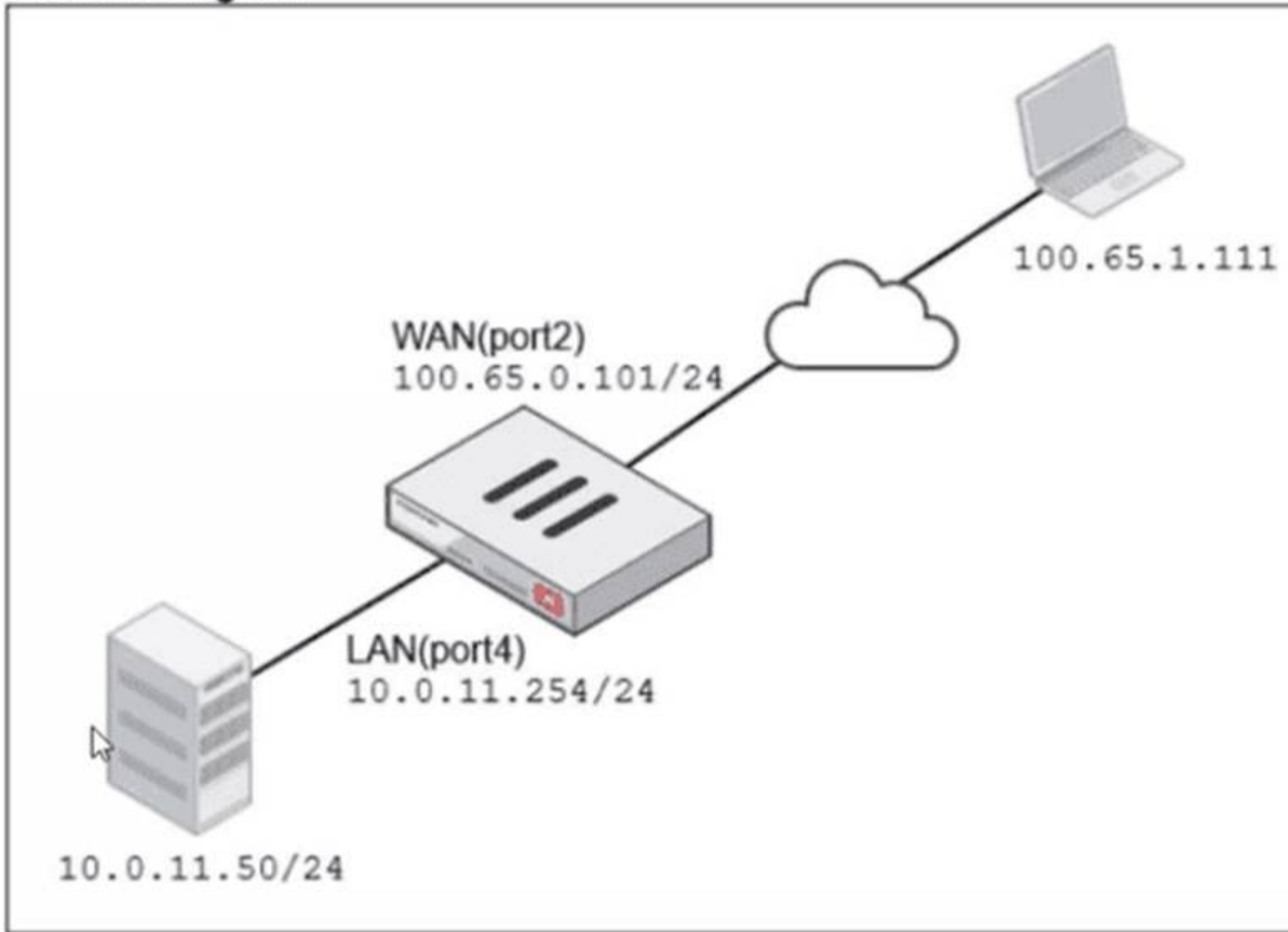
- A. Local Gateway
- B. Dead Peer Detection
- C. Peer ID
- D. IKE Mode Config

**Answer:** C

**NEW QUESTION 3**

Refer to the exhibits.

### Network diagram



Name: VIP-WEB-SERVER

Comments: Write a comment... 0/255

Color: Change

---

**Network**

Interface: WAN (port2)

Type: Static NAT

External IP address/range: 100.65.0.200

Map to:

IPv4 address/range: 10.0.11.50

---

Optional Filters

---

Port Forwarding

Protocol: **TCP** UDP SCTP ICMP

Port Mapping Type: **One to one** Many to many

External service port: 443

Map to IPv4 port: 4443

**Firewall policies**

Policy	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
<input type="checkbox"/> Internet (1)	LAN (port4)	WAN (port2)	all	all	always	ALL	ACCEPT		NAT
<input type="checkbox"/> Web_Server_Access (2)	WAN (port2)	LAN (port4)	all	VIP-WEB-SERVER	always	HTTPS	ACCEPT		Disabled

A diagram of a FortiGate device connected to the network VIP object and firewall policy configurations are shown.

The WAN (port2) interface has the IP address 100.65.0.101/24.

The LAN (port4) interface has the IP address 10.0.11.254/24.

If the host 100.65.1.111 sends a TCP SYN packet on port 443 to 100.65.0.200. what will the source address, destination address, and destination port of the packet be at the time FortiGate forwards the packet to the destination?

- A. 10.0.11.254, 100.65.0.200. and 443, respectively
- B. 10.0.11.254, 10.0.15.50, and 4443. respectively
- C. 100.65.1.111, 10.0.11.50, and 4443. respectively
- D. 100.65.1.111, 10.0.11.50. and 443. respectively

**Answer: C**

**NEW QUESTION 4**

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 5**

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 6**

Refer to the exhibit.

**IPsec tunnel configuration**

The exhibit displays two FortiGate configuration panels for IPsec Phase 2 selectors. On the left, the HQ-NGFW configuration shows a selector named 'ToBR1' with local address 10.0.11.0/255.255.255.0 and remote address 172.20.1.0/255.255.255.0. Its advanced settings include AES128 encryption, SHA1 authentication, and Diffie-Hellman group 5. On the right, the BR1-FGT configuration shows a selector named 'ToHQ' with local address 172.20.1.0/255.255.255.0 and remote address 10.11.0.0/255.255.255.0. Its advanced settings include AES256 encryption, SHA1 authentication, and Diffie-Hellman group 14.

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up, but phase 2 fails to come up.

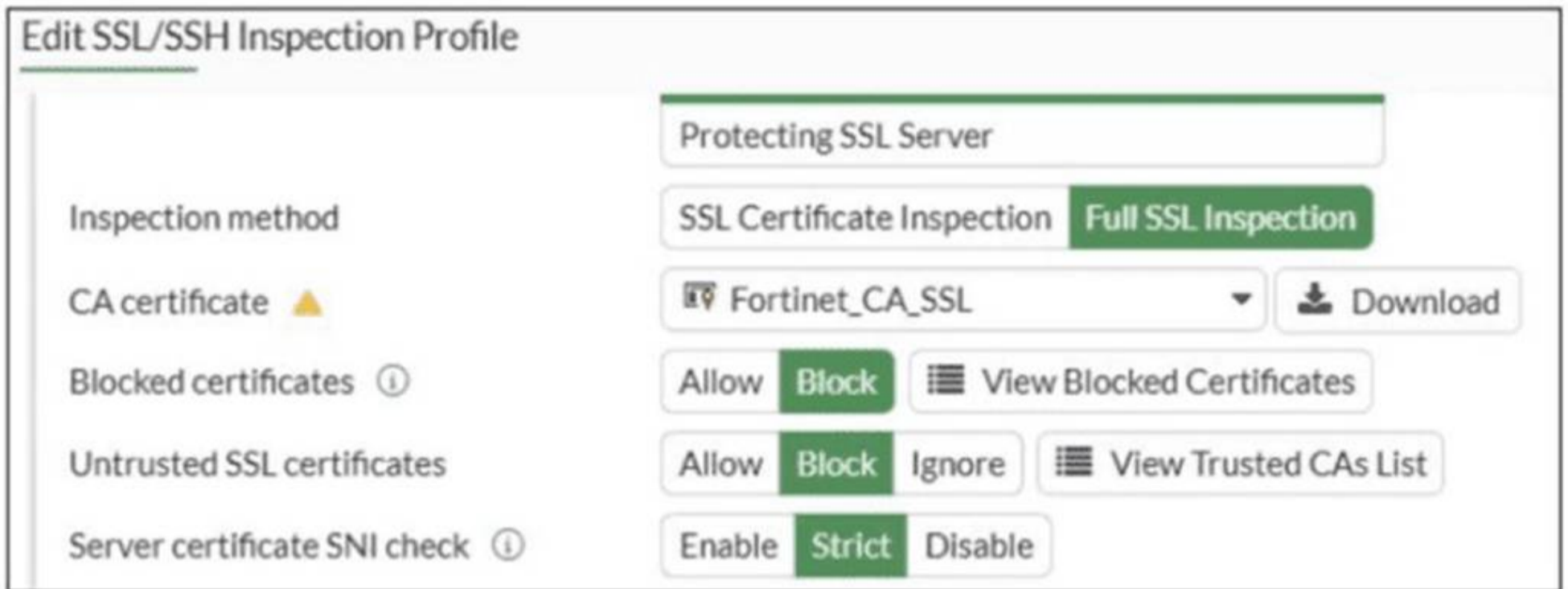
Based on the phase 2 configuration shown in the exhibit, which two configuration changes will bring phase 2 up? (Choose two.)

- A. On BR1-FGT, set Remote Address to 10.0.11.0/255.255.255.0.
- B. On HQ-NGF
- C. enable Diffie-Hellman Group 2.
- D. On BR1-FG
- E. set Seconds to 43200
- F. On HQ-NGF
- G. set Encryption to AES256.

Answer: AD

**NEW QUESTION 7**

Refer to the exhibit.



What would be the impact of these settings on the Server certificate SNI check configuration on FortiGate?

- A. FortiGate will accept and use the CN in the server certificate for URL filtering if the SNI does not match the CN or SAN fields.
- B. FortiGate will accept the connection with a warning if the SNI does not match the CN or SAN fields.
- C. FortiGate will close the connection if the SNI does not match the CN or SAN fields.
- D. FortiGate will close the connection if the SNI does not match the CN and SAN fields

Answer: C

**NEW QUESTION 8**

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
<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">2</span>			

## 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

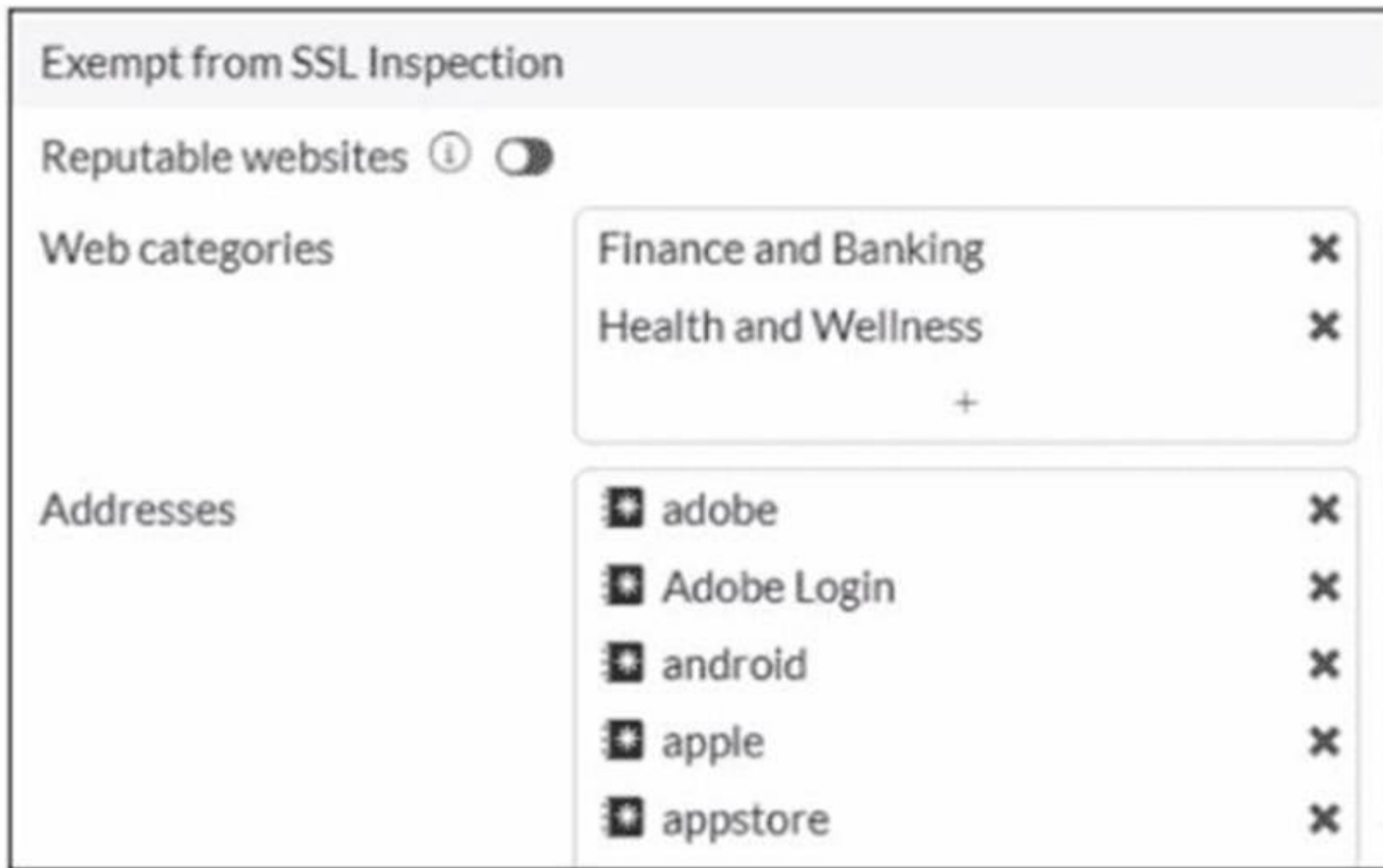
You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits. You cannot access any of the Google applications, but you are able to access www.fortinet.com. Which two actions would you take to resolve the issue? (Choose two.)

- 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 9

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 10**

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 10**

Refer to the exhibits.

# 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	<span style="background-color: #333; color: white; padding: 2px;">BHVR</span> Excessive-Bandwidth	Filter	<input checked="" type="checkbox"/> Block
2	<span style="background-color: #333; color: white; padding: 2px;">VEND</span> Google	Filter	<input checked="" type="checkbox"/> Monitor
<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">2</span>			

## 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 deep-inspection

Decrypted traffic mirror:

---

#### Logging Options

Log allowed traffic:  Security events All sessions

You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits. Which two factors can you observe from these configurations? (Choose two.)

- A. YouTube access is blocked based on Excessive-Bandwidth Application and Filter override settings.
- B. Facebook access is blocked based on the category filter settings.
- C. Facebook access is allowed but you cannot play Facebook videos based on Video/Audio category filter settings.
- D. YouTube search is allowed based on the Google Application and Filter override settings.

**Answer:** AB

### NEW QUESTION 13

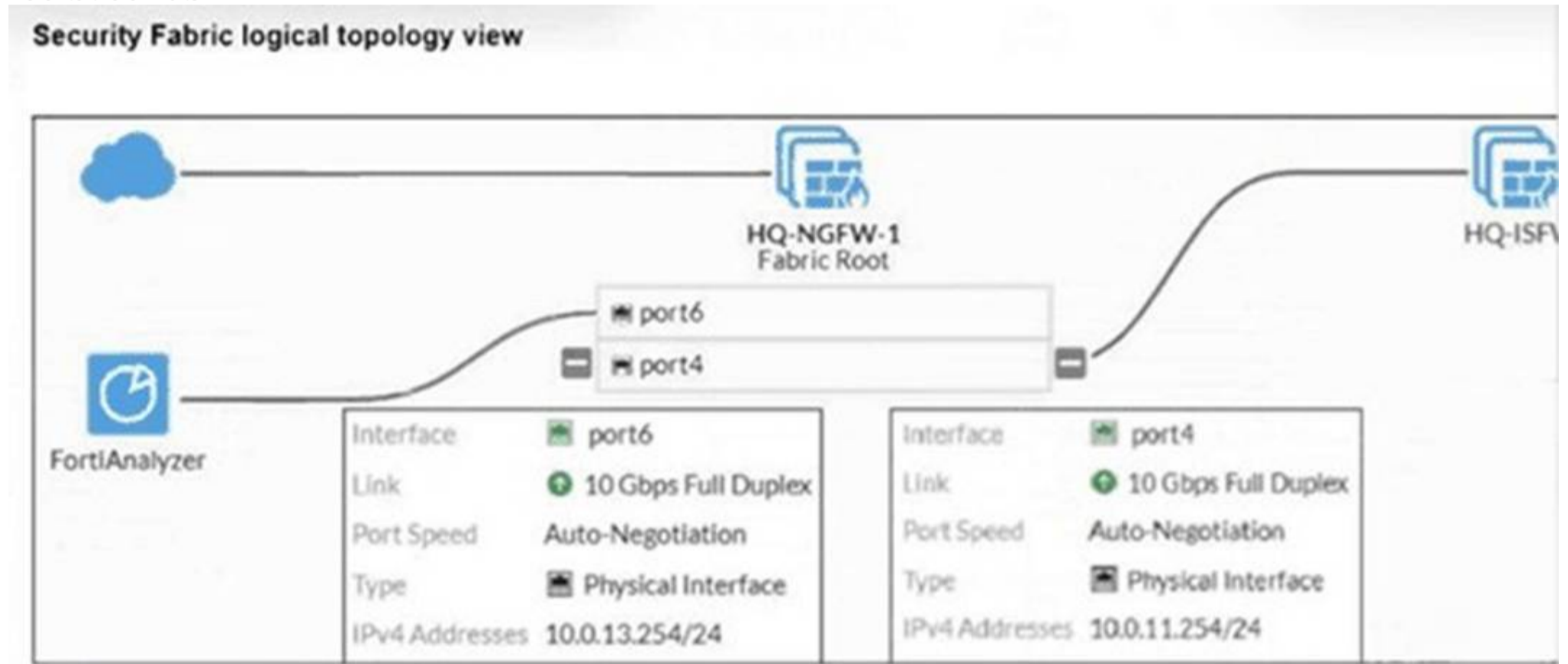
An administrator wants to form an HA cluster using the FGCP protocol. Which two requirements must the administrator ensure both members fulfill? (Choose two.)

- A. They must have the same hard drive configuration.
- B. They must have the same number of configured VDOMs.
- C. They must have the heartbeat interfaces in the same subnet
- D. They must have the same HA group ID.

**Answer:** BD

**NEW QUESTION 16**

Refer to the exhibits.



**Security Fabric settings on HQ-ISFW-2**

**Security Fabric Settings**

Security Fabric role: Standalone | Serve as Fabric Root | **Join Existing Fabric**

Allow other Security Fabric devices to join:  port6

Upstream FortiGate IP/FQDN: 10.0.13.254

Allow downstream device REST API access:

Management IP/FQDN: Use WAN IP **Specify** 10.0.11.250

Management port: Use Admin Port **Specify** 443

SAML SSO Settings

SAML Single Sign-On: **Auto** | Manual

Advanced Options

Mode: ⚠ Pending

An administrator wants to add HQ-ISFW-2 in the Security Fabric. HQ-ISFW-2 is in the same subnet as HQ-ISFW. After configuring the Security Fabric settings on HQ-ISFW-2, the status stays Pending. What can be the two possible reasons? (Choose two answers)

- A. Upstream FortiGate IP must be set to 10.0.11.254.
- B. SAML Single Sign-On must be set to Manual.
- C. HQ-ISFW-2 must be authorized on HQ-ISFW.
- D. Management IP must be set to 10.0.13.254.

**Answer:** AC

**NEW QUESTION 17**

What are two features of collector agent advanced mode? (Choose two.)

- A. In advanced mode, security profiles can be applied only to user groups, not individual users.
- B. In advanced mod
- C. FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
- D. Advanced mode uses the Windows convention—NetBios: Domain\Username.
- E. Advanced mode supports nested or inherited groups.

**Answer:** BD

**NEW QUESTION 22**

An administrator has configured a dialup IPsec VPN on FortiGate with add-route enabled. However, the static route is not showing in the routing table. Which two statements about this scenario are correct? (Choose two.)

- A. The administrator must use a policy route instead of a static route for add-route to work properly.
- B. The administrator must ensure phase 2 is successfully established
- C. The administrator must define the remote network correctly in the phase 2 selectors.
- D. The administrator must enable a dynamic routing protocol on the dialup interface.

**Answer:** BC

**NEW QUESTION 25**

When configuring firewall policies which of the following is true regarding the policy ID? (Choose two.)

- A. A firewall policy ID identifies the order of policy execution in firewall policies.
- B. A policy ID cannot be modified once a policy is created.
- C. You can create a policy in CLI with policy ID 0
- D. It is mandatory to provide a policy ID while creating a firewall policy regardless of GUI or CLI.

**Answer:** BC

**NEW QUESTION 28**

.....

## **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](#)**