



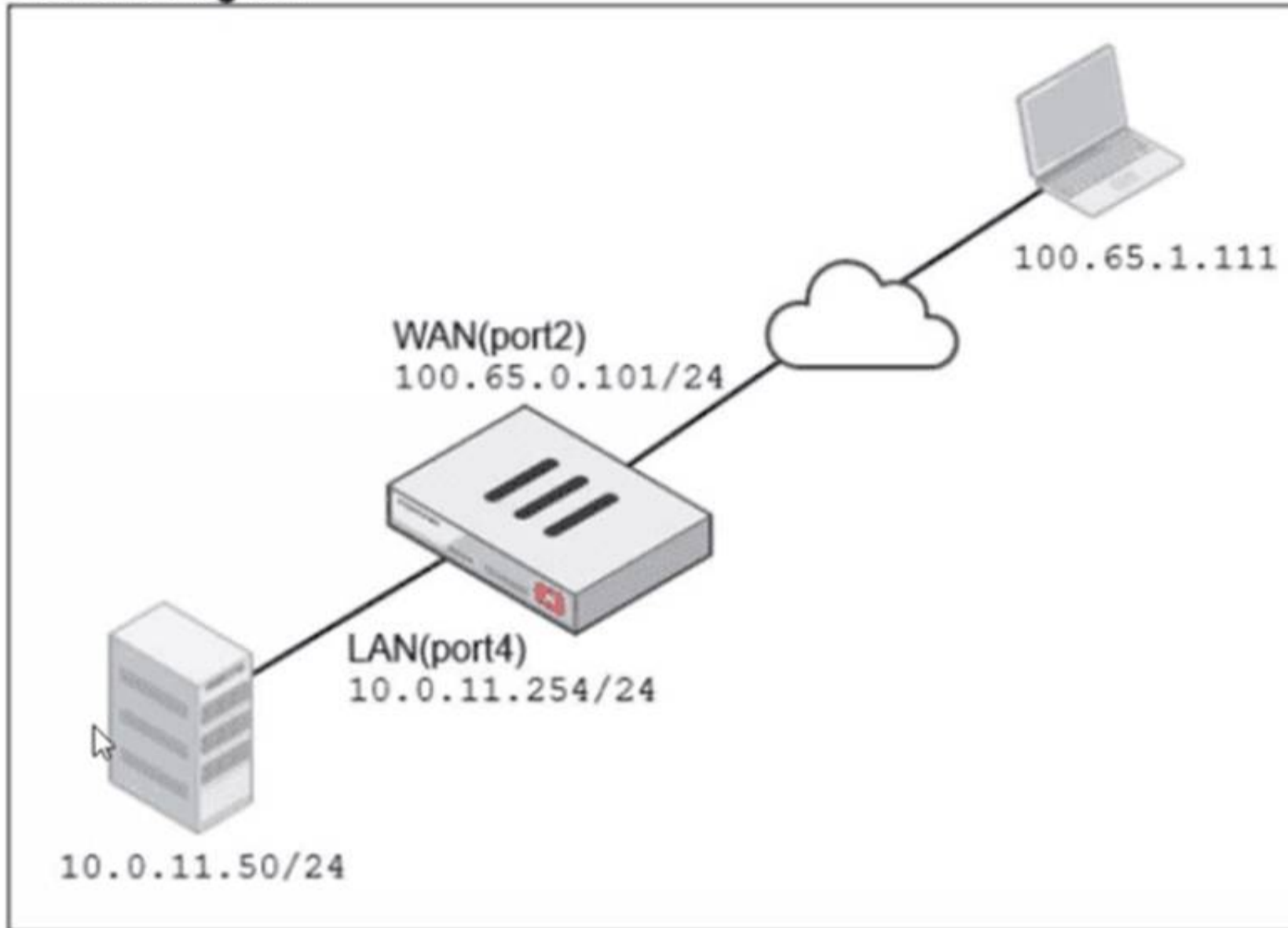
**Fortinet**

**Exam Questions NSE4\_FGT\_AD-7.6**

Fortinet NSE 4 - FortiOS 7.6 Administrator

**NEW QUESTION 1**  
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 2**

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

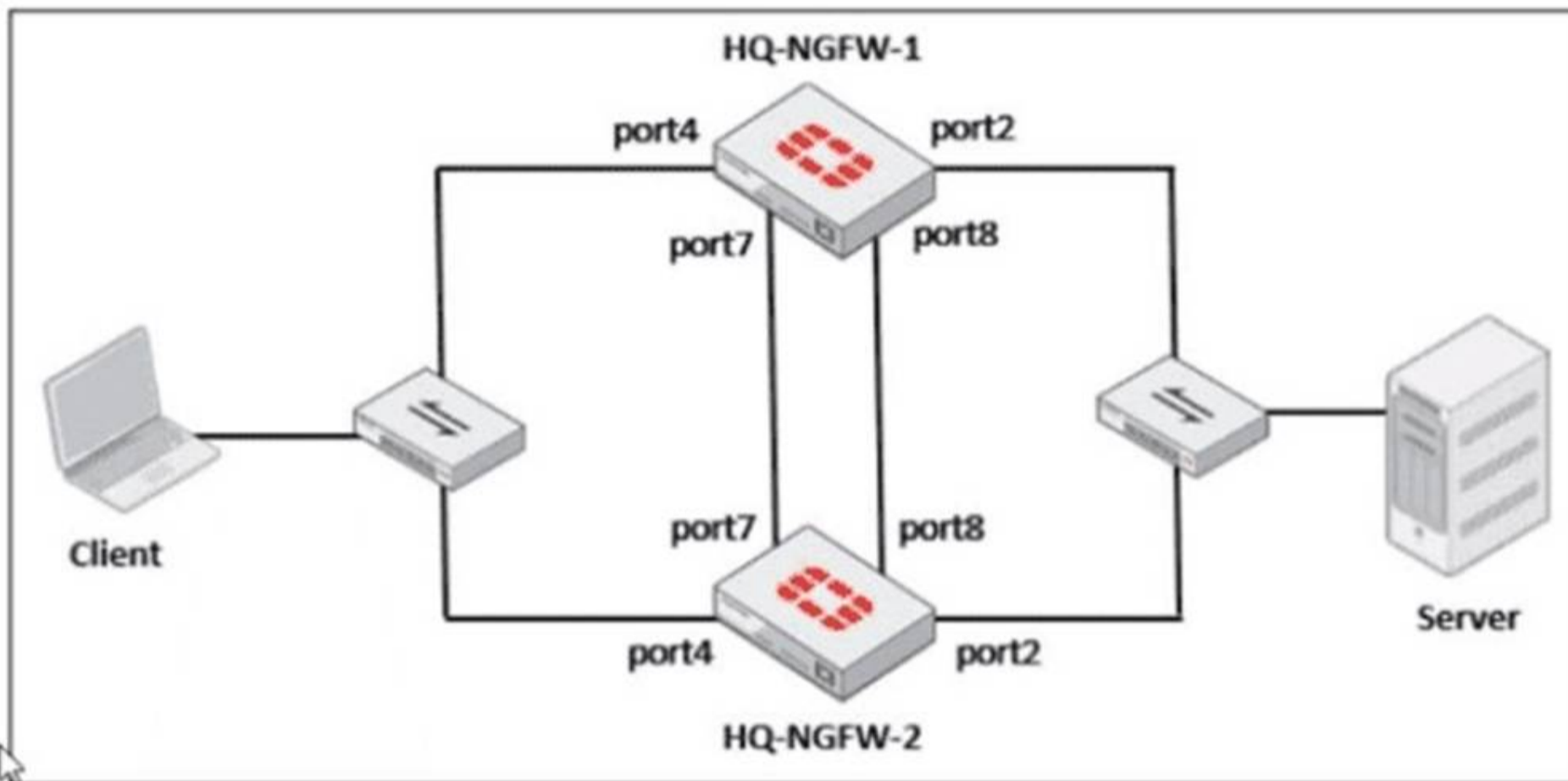
the possible reason of the diagnose output shown in the exhibit?

- 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 3**  
 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 4

Which two components are part of the secure internet access (SIA) agent-based mode on FortiSASE? (Choose two.)

- A. FortiSASE Firewall-as-a-Service (FWaaS)
- B. The proxy auto-configuration (PAC) file
- C. VPN policies
- D. FortiExtender

**Answer:** AC

### NEW QUESTION 5

FortiGate is integrated with FortiAnalyzer and FortiManager.

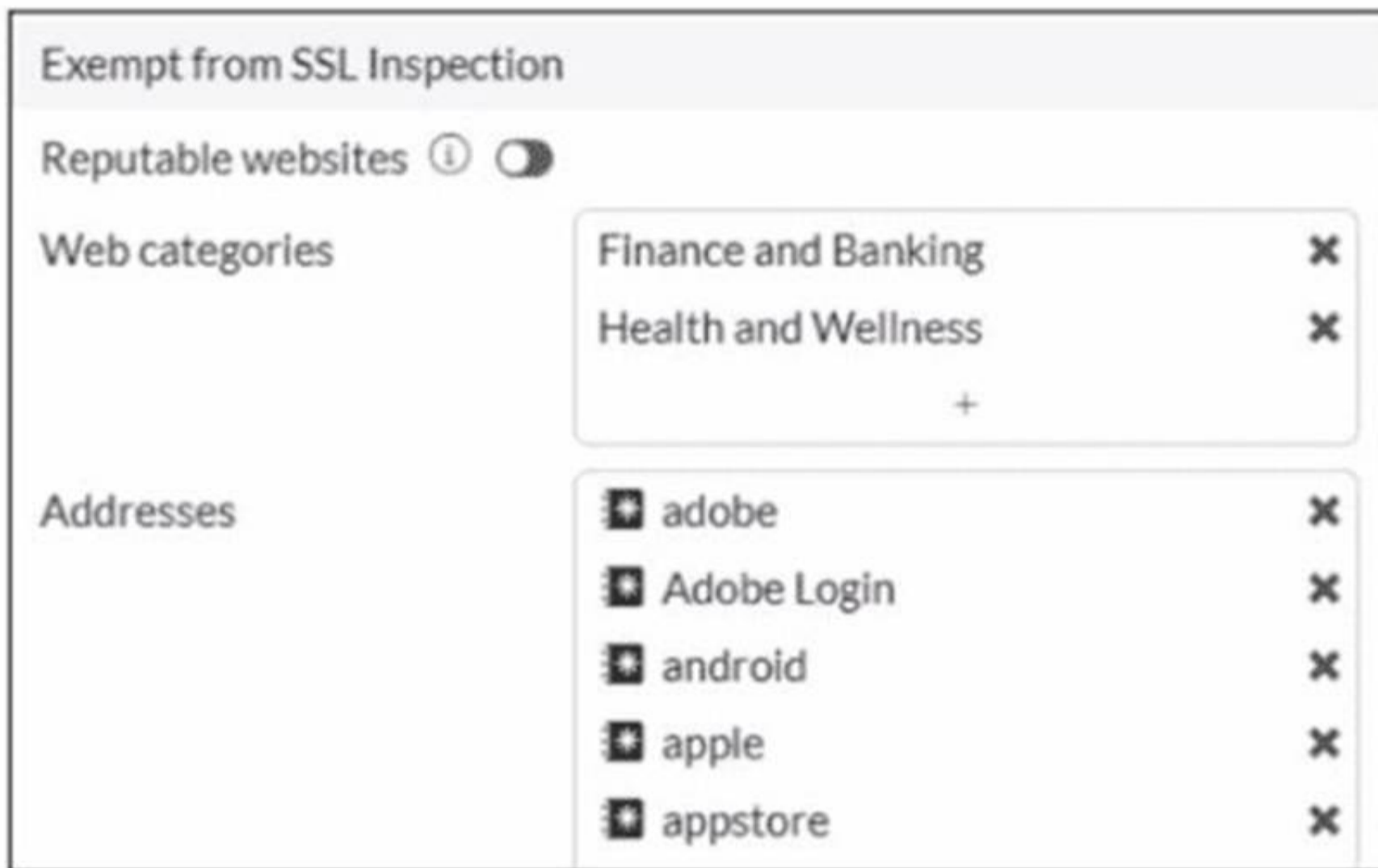
When creating a firewall policy, which attribute must an administrator include to enhance functionality and enable log recording on FortiAnalyzer and FortiManager?

- A. Universally Unique Identifier
- B. Policy ID
- C. Sequence ID
- D. Log ID

**Answer:** A

**NEW QUESTION 6**

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 7**

Which three statements explain a flow-based antivirus profile? (Choose three answers)

- A. FortiGate buffers the whole file but transmits to the client at the same time.
- B. Flow-based inspection uses a hybrid of the scanning modes available in proxy-based inspection.
- C. If a virus is detected, the last packet is delivered to the client.
- D. Flow-based inspection optimizes performance compared to proxy-based inspection.
- E. The IPS engine handles the process as a standalone.

**Answer:** ABD

**NEW QUESTION 8**

An administrator wanted to configure an IPS sensor to block traffic that triggers the signature set number of times during a specific time period. How can the administrator achieve the objective?

- A. Use IPS group signatures, set rate-mode 60.
- B. Use IPS packet logging option with periodical filter option.
- C. Use IPS signatures, rate-mode periodical option.
- D. Use IPS filter, rate-mode periodical option.

**Answer:** D

**NEW QUESTION 9**

What is the primary FortiGate election process when the HA override setting is enabled? (Choose one answer)

- A. Connected monitored ports > Priority > HA uptime > FortiGate serial number
- B. Connected monitored ports > Priority > System uptime > FortiGate serial number
- C. Connected monitored ports > HA uptime > Priority > FortiGate serial number
- D. Connected monitored ports > System uptime > Priority > FortiGate serial number

**Answer:** A

**NEW QUESTION 10**

FortiGate is operating in NAT mode and has two physical interfaces connected to the LAN and DMZ networks respectively. Which two statements about the requirements of connected physical interfaces on FortiGate are true? (Choose two.)

- A. Both interfaces must have DHCP enabled and interfaces set to LAN and DMZ roles assigned.
- B. Both interfaces must have the interface role assigned.
- C. Both interfaces must have directly connected routes on the routing table.
- D. Both interfaces must have IP addresses assigned.

**Answer:** CD

**NEW QUESTION 10**

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 11**

Which two statements are correct when the FortiGate device enters conserve mode? (Choose two.)

- A. FortiGate refuses to accept configuration changes.
- B. FortiGate halts complete system operation and requires a reboot to regain available resources.
- C. FortiGate continues to transmit packets without IPS inspection when the fail-open global setting in IPS is enabled.
- D. FortiGate continues to run critical security actions, such as quarantine.

**Answer:** AC

**NEW QUESTION 13**

Refer to the exhibit.

```
config system global
    set av-failopen one-shot
end
config ips global
    set fail-open enable
end
```

Based on this partial configuration, what are the two possible outcomes when FortiGate enters conserve mode? (Choose two.)

- A. FortiGate drops new sessions requiring inspection.
- B. Administrators must restart FortiGate to allow new sessions.
- C. Administrators cannot change the configuration.
- D. FortiGate skips quarantine actions.

**Answer:** CD

**NEW QUESTION 14**

Refer to the exhibits.

## Web filter profile configuration

Edit Web Filter Profile

Feature set **Flow-based** Proxy-based

FortiGuard Category Based Filter

Allow
  Monitor
  Block
  Warning
  Authenticate

Name	Action
Job Search	<input checked="" type="radio"/> Allow
Medicine	<input checked="" type="radio"/> Allow
News and Media	<input checked="" type="radio"/> Allow
Social Networking	<input checked="" type="radio"/> Allow
Political Organizations	<input checked="" type="radio"/> Allow
Reference	<input checked="" type="radio"/> Allow
Global Religion	<input checked="" type="radio"/> Allow
Shopping	<input checked="" type="radio"/> Allow
Society and Lifestyles	<input checked="" type="radio"/> Allow

58% **95**

Allow users to override blocked categories

Search Engines

Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex

Static URL Filter

Block invalid URLs

URL Filter

URL	Type	Action	Status
www.facebook.com	Simple	<input type="radio"/> Monitor	<input checked="" type="radio"/> Enable

## Firewall policy configuration

**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:  WEB default

Video filter:

DNS filter:

Application control:

IPS:

File filter:

SSL inspection:  SSL certificate-inspection

**FortiGuard block page**



A web filter profile configuration and firewall policy configuration are shown. You are trying to access www.facebook.com, but you are redirected to a FortiGuard web filtering block page. Based on the exhibits, what is the possible cause of the issue?

- A. The web rating override configuration is incorrect.
- B. The web filter profile feature set is configured incorrectly.
- C. The firewall policy inspection mode is incorrect.
- D. For ww
- E. faceboo
- F. co
- G. the URL filter action is incorrect.

**Answer: C**

**NEW QUESTION 19**

.....

## 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](#)