# Fortinet

## Exam Questions NSE4_FGT_AD-7.6

Fortinet NSE 4 - FortiOS 7.6 Administrator

**NEW QUESTION 1**
You have configured the below commands on a FortiGate.

```
config system settings
set strict-src-check enable
end

Config system interface
edit port1
set src-check disable
next
end
```

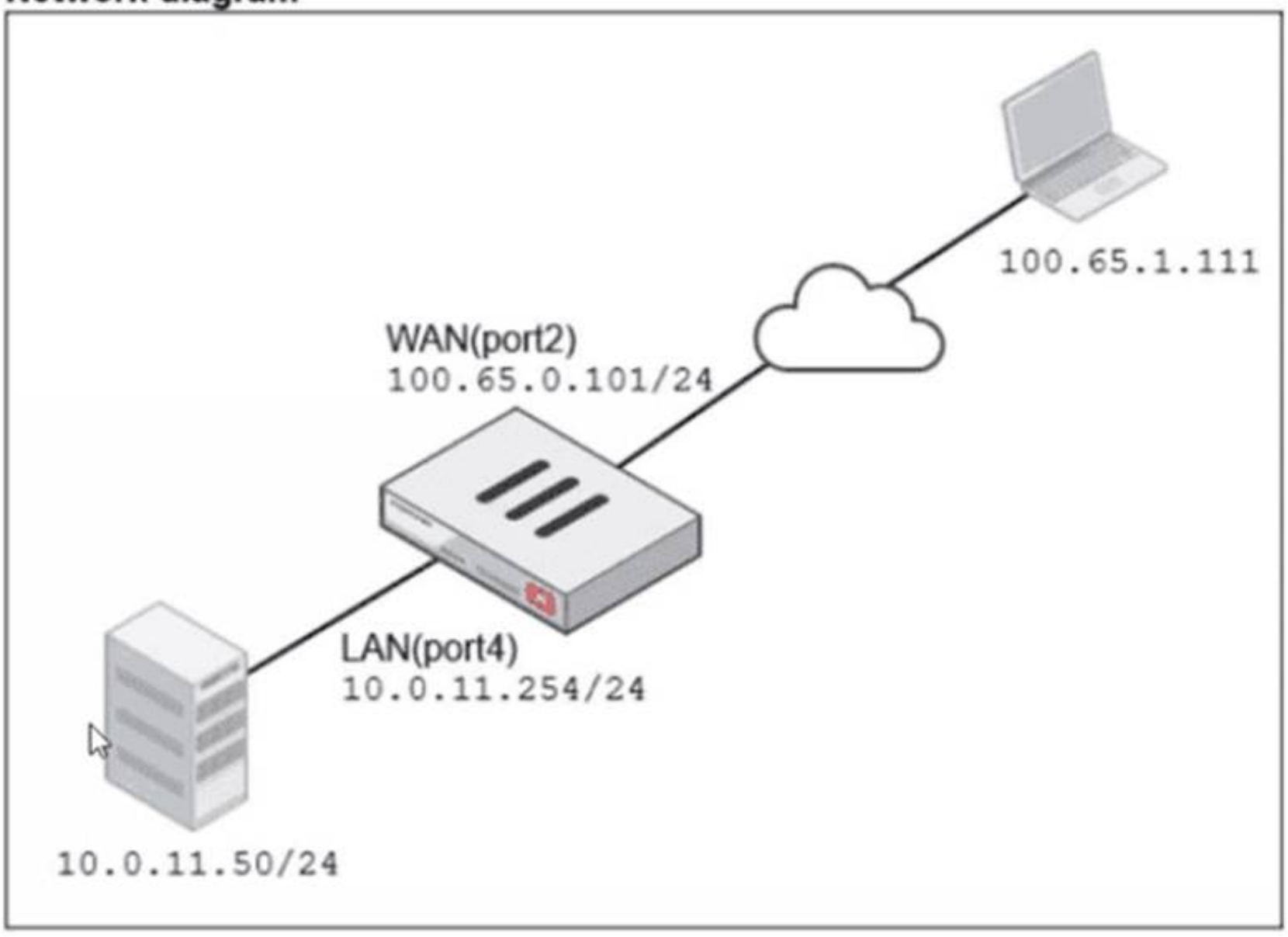
What would be the impact of this configuration on FortiGate?

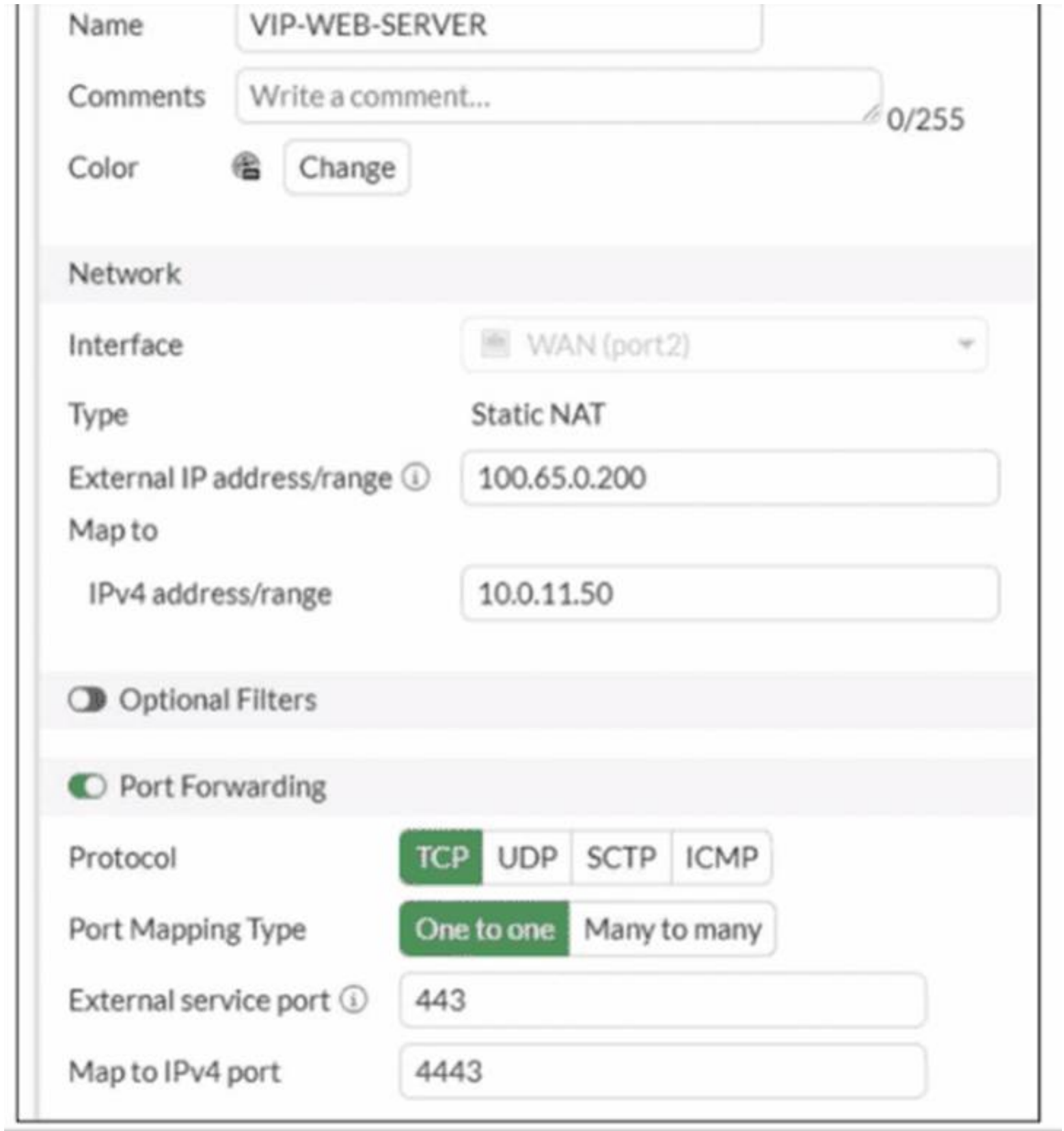
A. FortiGate will enable strict RPF on all its interfaces and porti will be exempted from RPF checks.
B. FortiGate will enable strict RPF on all its interfaces and porti will be enable for asymmetric routing.
C. The global configuration will take precedence and FortiGate will enable strict RPF on all interfaces.
D. Port1 will be enabled with flexible RP
E. and all other interfaces will be enabled for strict RPF

**Answer:** A

**NEW QUESTION 2**
Refer to the exhibits.

**Network diagram**






**Firewall policies**

| | Policy | From | To | Source | Destination | Schedule | Service | Action | IP Pool | NAT |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | Internet (1) | LAN (port4) | WAN (port2) | all | all | always | ALL | ✓ ACCEPT | | NAT |
| ☐ | 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. ill, 10.0.11.50, and 4443. respectively
D. 100.65.1.111, 10.0.11.50. and 443. respectively

**Answer:** C

**NEW QUESTION 3**
Refer to the exhibit.


The NOC team connects to the FortiGate GUI with the NOC_Access admin profile. They request that their GUI sessions do not disconnect too early during inactivity. What must the administrator configure to answer this specific request from the NOC team? (Choose one answer)

A. Move NOC_Access to the top of the list to ensure all profile settings take effect.
B. Increase the offline value of the Override Idle Timeout parameter in the NOC_Access admin profile.
C. Ensure that all NOC_Access users are assigned the super_admin role to guarantee access.
D. Increase the admintimeout value under config system accprofile NOC_Access.

**Answer:** D

**NEW QUESTION 4**
Refer to the exhibits.

**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
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87  kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions  in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions  in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

**Memory usage threshold settings**

```
config system global
    set memory-use-threshold-extreme 89
    set memory-use-threshold-green 82
    set memory-use-threshold-red 88
end
```

The system performance output and default configuration of high memory usage thresholds on a FortiGate device are shown.
Based on the system performance output, what are the two possible outcomes? (Choose two.)

A. Administrators can access FortiGate only through the console port.
B. FortiGate has entered conserve mode.
C. FortiGate drops new sessions.
D. Administrators can change the configuration.

**Answer:** BD

**NEW QUESTION 5**
A new administrator is configuring FSSO authentication on FortiGate using DC Agent Mode. Which step is not part of the expected process?

A. The DC agent sends login event data directly to FortiGate.
B. FortiGate determines user identity based on the IP address in the FSSO list.
C. The collector agent forwards login event data to FortiGate.
D. The user logs into the windows domain.

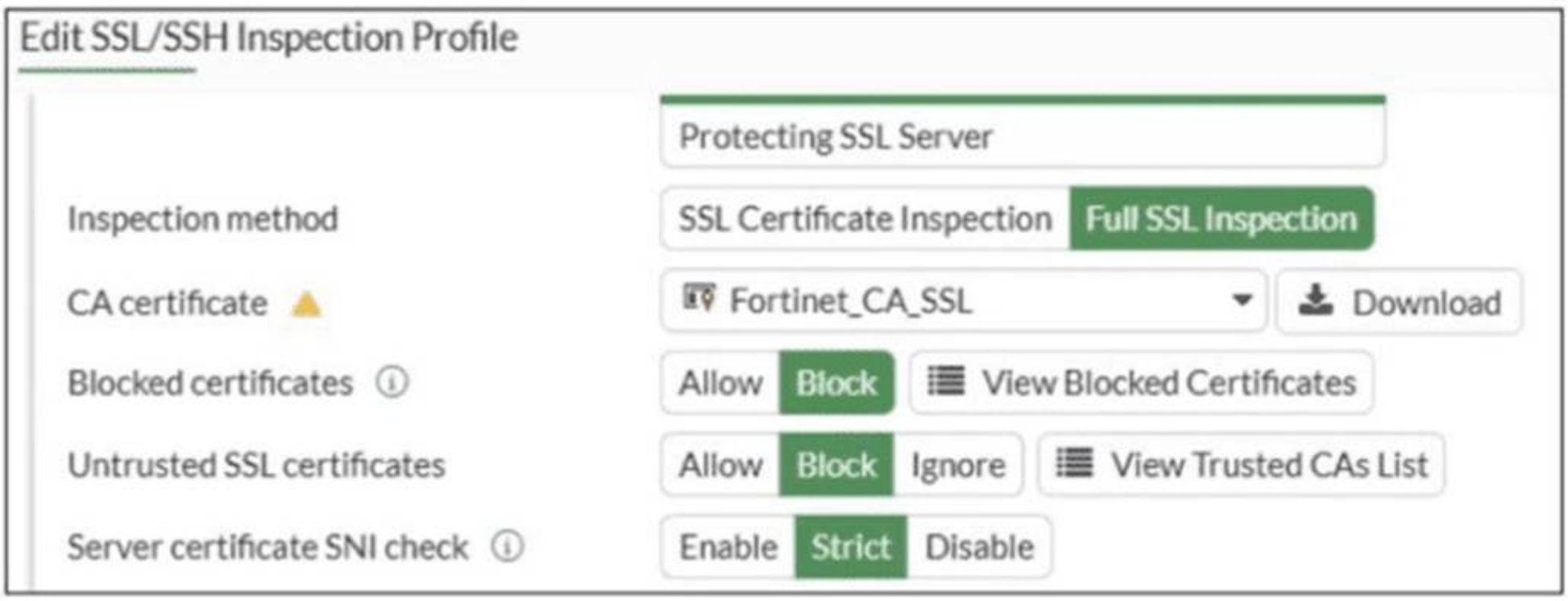
**Answer:** A

**NEW QUESTION 6**
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 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**
Which two statements are correct when FortiGate enters conserve mode? (Choose two answers)

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

**Answer:** BD

**NEW QUESTION 9**
Which two statements are true about an HA cluster? (Choose two answers)

A. An HA cluster cannot have both in-band and out-of-band management interfaces at the same time.
B. Link failover triggers a failover if the administrator sets the interface down on the primary device.
C. When sniffing the heartbeat interface, the administrator must see the IP address 169.254.0.2.
D. HA incremental synchronization includes FIB entries and IPsec SAs.

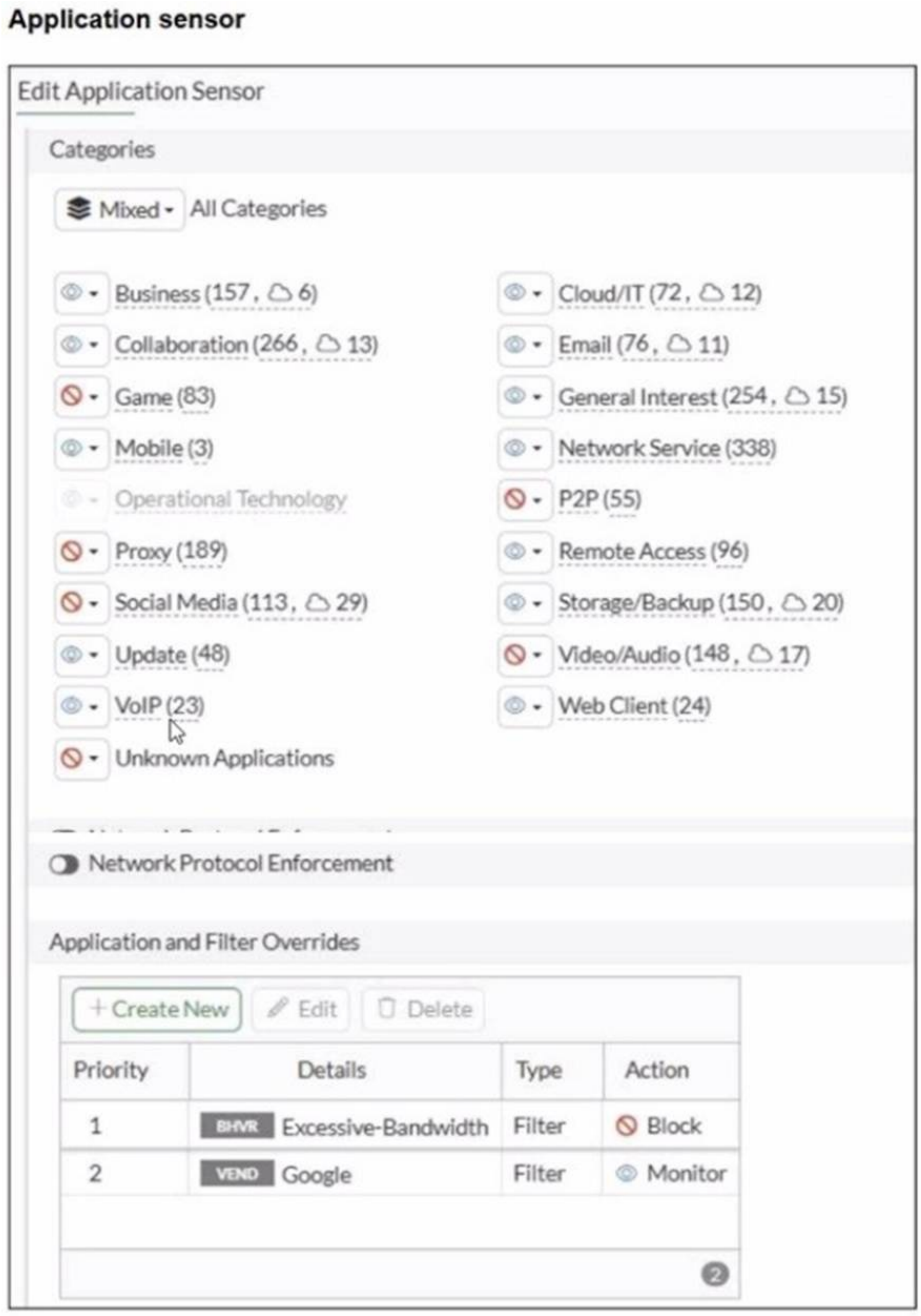
**Answer:** BD

**NEW QUESTION 10**
Which three statements about SD-WAN performance SLAs are true? (Choose three.)

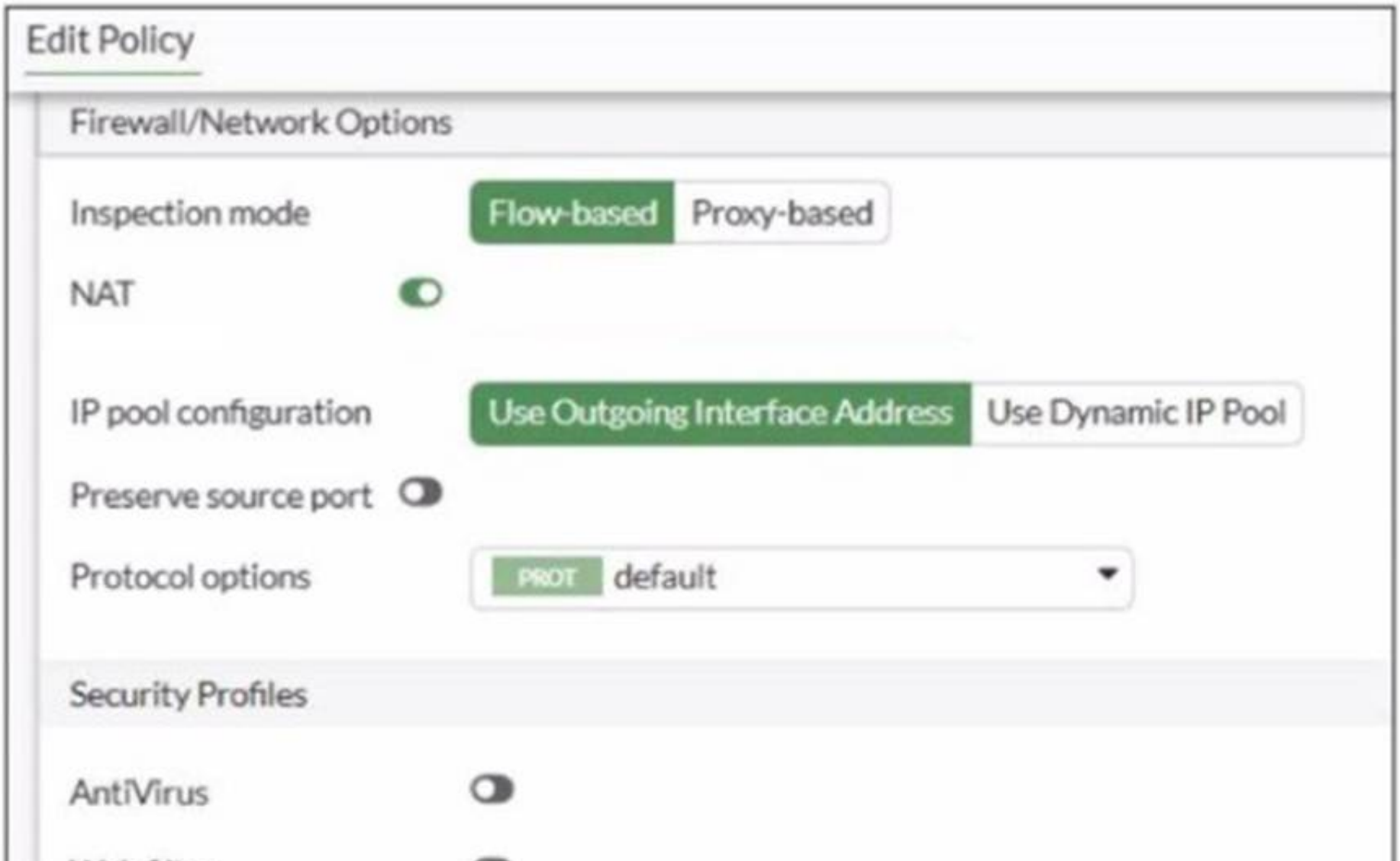
A. They rely on session loss and jitter.
B. They monitor the state of the FortiGate device.
C. All the SLA targets can be configured.
D. They are applied in a SD-WAN rule lowest cost strategy.
E. They can be measured actively or passively.

**Answer:** CDE

**NEW QUESTION 10**
Refer to the exhibits.



**Firewall policy**




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 15**
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 19**
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 23**
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 25**
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 26**
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 28**
.....

# Thank You for Trying Our Product

## We offer two products:

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

2nd - Questons 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