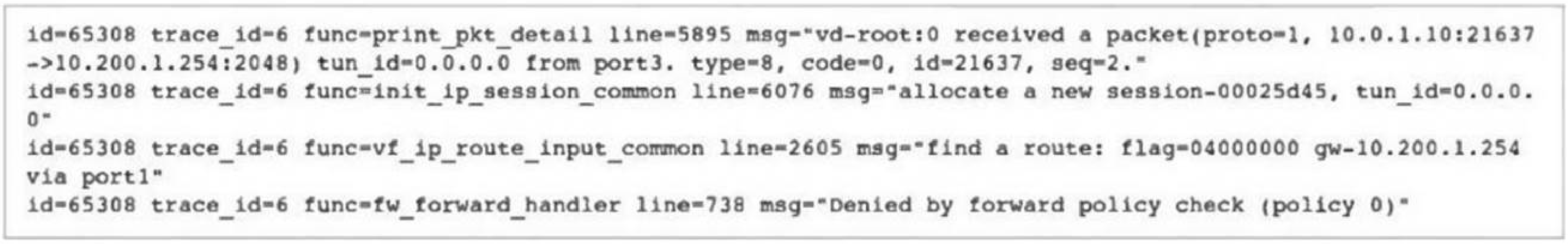
Fortinet

Exam Questions FCP_FGT_AD-7.4

FCP - FortiGate 7.4 Administrator

NEW QUESTION 1
Refer to the exhibit.



```
id=65308 trace_id=6 func=print_pkt_detail line=5895 msg="vd-root:0 received a packet(proto=1, 10.0.1.10:21637
->10.200.1.254:2048) tun_id=0.0.0.0 from port3. type=8, code=0, id=21637, seq=2."
id=65308 trace_id=6 func=init_ip_session_common line=6076 msg="allocate a new session-00025d45, tun_id=0.0.0.
0"
id=65308 trace_id=6 func=vf_ip_route_input_common line=2605 msg="find a route: flag=04000000 gw-10.200.1.254
via port1"
id=65308 trace_id=6 func=fw_forward_handler line=738 msg="Denied by forward policy check (policy 0)"
```

Why did FortiGate drop the packet?

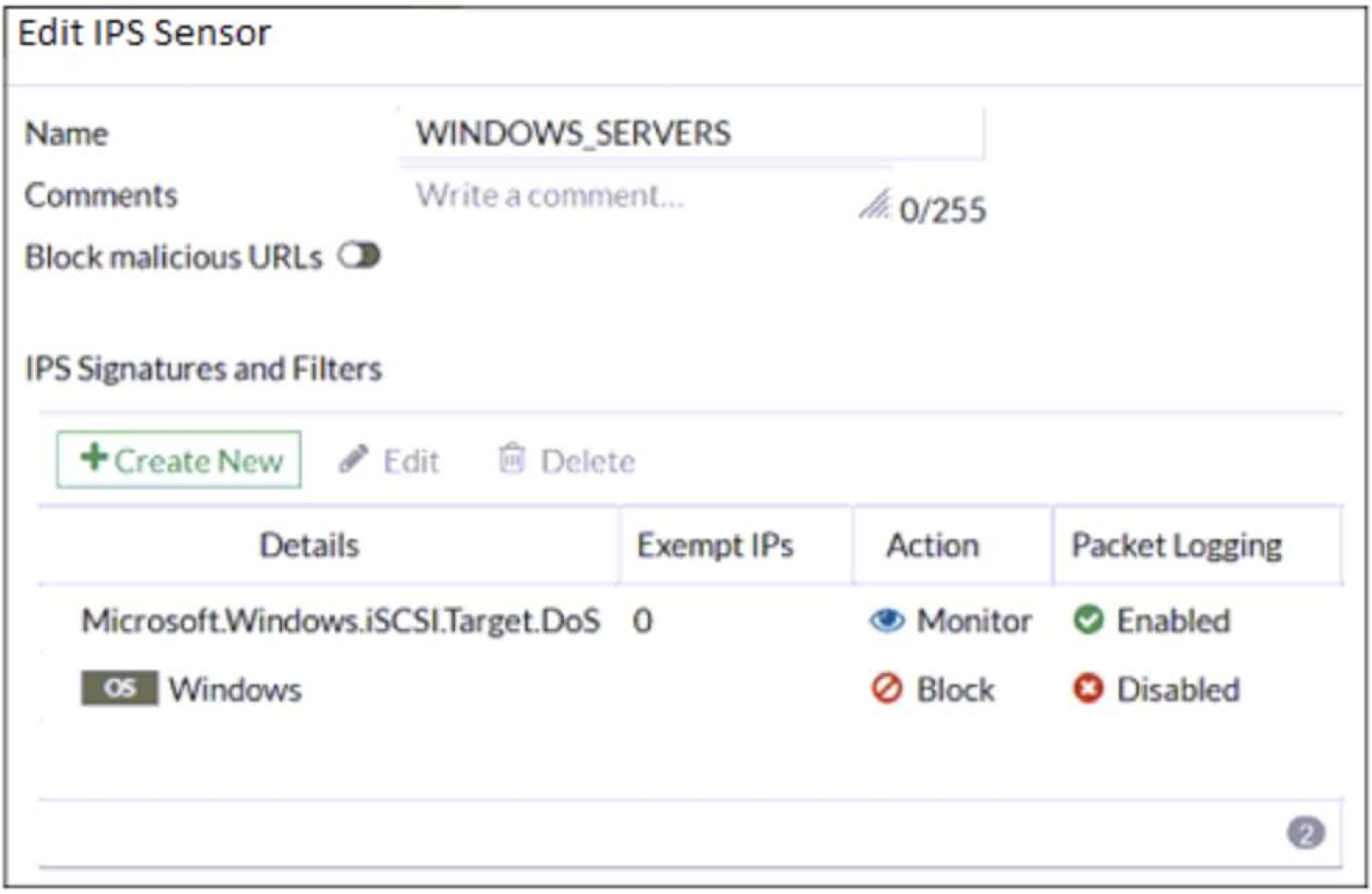
A. It matched an explicitly configured firewall policy with the action DENY
B. It failed the RPF check.
C. The next-hop IP address is unreachable.
D. It matched the default implicit firewall policy

Answer: D

Explanation:
The debug trace output shows that the packet was "Denied by forward policy check (policy 0)." In FortiGate, policy ID 0 corresponds to the default implicit deny policy. This means that if a packet does not match any configured firewall policies, it is denied by the default implicit policy.
References:

- FortiOS 7.4.1 Administration Guide: Firewall Policies

NEW QUESTION 2
Refer to the exhibit, which shows the IPS sensor configuration.



Edit IPS Sensor

Name: WINDOWS_SERVERS
Comments: Write a comment... 0/255
Block malicious URLs

IPS Signatures and Filters

Details	Exempt IPs	Action	Packet Logging
Microsoft.Windows.iSCSI.Target.DoS	0	Monitor	✓ Enabled
OS Windows		Block	✗ Disabled

If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

A. The sensor will gather a packet log for all matched traffic.
B. The sensor will reset all connections that match these signatures.
C. The sensor will allow attackers matching the Microsoft.Windows.iSCSl.Target.DoS signature.
D. The sensor will block all attacks aimed at Windows servers.

Answer: AC

Explanation:
The IPS sensor configuration shows that:

- The Microsoft.Windows.iSCSI.Target.DoS signature is set to "Monitor" with packet logging enabled, meaning that while traffic matching this signature will be allowed, it will also be logged for further analysis.

- The generic Windows filter is set to "Block," meaning that all other attacks matching this filter will be blocked. However, the sensor will not reset connections or log packets unless specified.

Therefore, the sensor will allow attackers matching the specific DoS signature while blocking other attacks against Windows.
References:

- FortiOS 7.4.1 Administration Guide: IPS Configuration

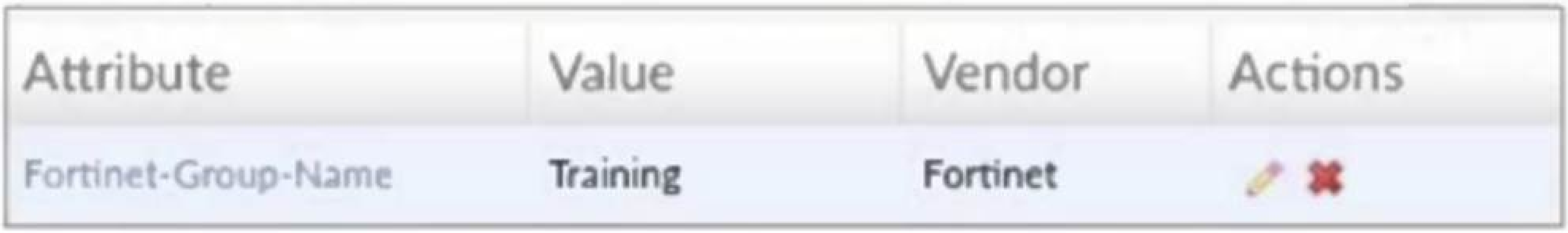
NEW QUESTION 3
What are two features of collector agent advanced mode? (Choose two.)

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

Answer: AD

Explanation:
Advanced mode allows for configuration as an LDAP client and supports group filtering directly on the FortiGate, as well as nested or inherited groups.

NEW QUESTION 4
Refer to the exhibit, which shows a partial configuration from the remote authentication server.



Attribute	Value	Vendor	Actions
Fortinet-Group-Name	Training	Fortinet	✎ ✖

Why does the FortiGate administrator need this configuration?

A. To authenticate only the Training user group.
B. To set up a RADIUS server Secret
C. To authenticate and match the Training OU on the RADIUS server.
D. To authenticate Any FortiGate user groups.

Answer: A

NEW QUESTION 5
FortiGate is integrated with FortiAnalyzer and FortiManager.
When a firewall policy is created, which attribute is added to the policy to improve functionality and to support recording logs to FortiAnalyzer or FortiManager?

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

Answer: D

Explanation:
When a firewall policy is created in FortiGate integrated with FortiAnalyzer and FortiManager, a Universally Unique Identifier (UUID) is added to the policy to support logging and management.

NEW QUESTION 6
Which two statements are true regarding FortiGate HA configuration synchronization? (Choose two.)

A. Checksums of devices are compared against each other to ensure configurations are the same.
B. Incremental configuration synchronization can occur only from changes made on the primary FortiGate device.
C. Incremental configuration synchronization can occur from changes made on any FortiGate device within the HA cluster
D. Checksums of devices will be different from each other because some configuration items are not synced to other HA members.

Answer: AB

Explanation:
In FortiGate HA (High Availability) configuration, checksums of device configurations are compared to ensure they are synchronized and identical across the cluster. Incremental synchronization can only happen from changes made on the primary device to ensure consistency and integrity across the cluster members.
Changes made on non-primary devices do not initiate synchronization.
References:

- FortiOS 7.4.1 Administration Guide: HA Configuration Synchronization

NEW QUESTION 7
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.

Answer: BCD

Explanation:
When SSL certificate inspection is enabled on a FortiGate device, the system uses the following three pieces of information to identify the hostname of the SSL server:

- Server Name Indication (SNI) extension in the client hello message (B): The SNI is an extension in the client hello message of the SSL/TLS protocol. It indicates the hostname the client is attempting to connect to. This allows FortiGate to identify the server's hostname during the SSL handshake.
- Subject Alternative Name (SAN) field in the server certificate (C): The SAN field in the server certificate lists additional hostnames or IP addresses that the certificate is valid for. FortiGate inspects this field to confirm the identity of the server.
- Subject field in the server certificate (D): The Subject field contains the primary hostname or domain name for which the certificate was issued. FortiGate uses this information to match and validate the server??s identity during SSL certificate inspection.

The other options are not used in SSL certificate inspection for hostname identification:

- Host field in the HTTP header (A): This is part of the HTTP request, not the SSL handshake, and is not used for SSL certificate inspection.
- Serial number in the server certificate (E): The serial number is used for certificate management and revocation, not for hostname identification.

References

- FortiOS 7.4.1 Administration Guide - SSL/SSH Inspection, page 1802.
- FortiOS 7.4.1 Administration Guide - Configuring SSL/SSH Inspection Profile, page 1799.

NEW QUESTION 8
Which statement is a characteristic of automation stitches?

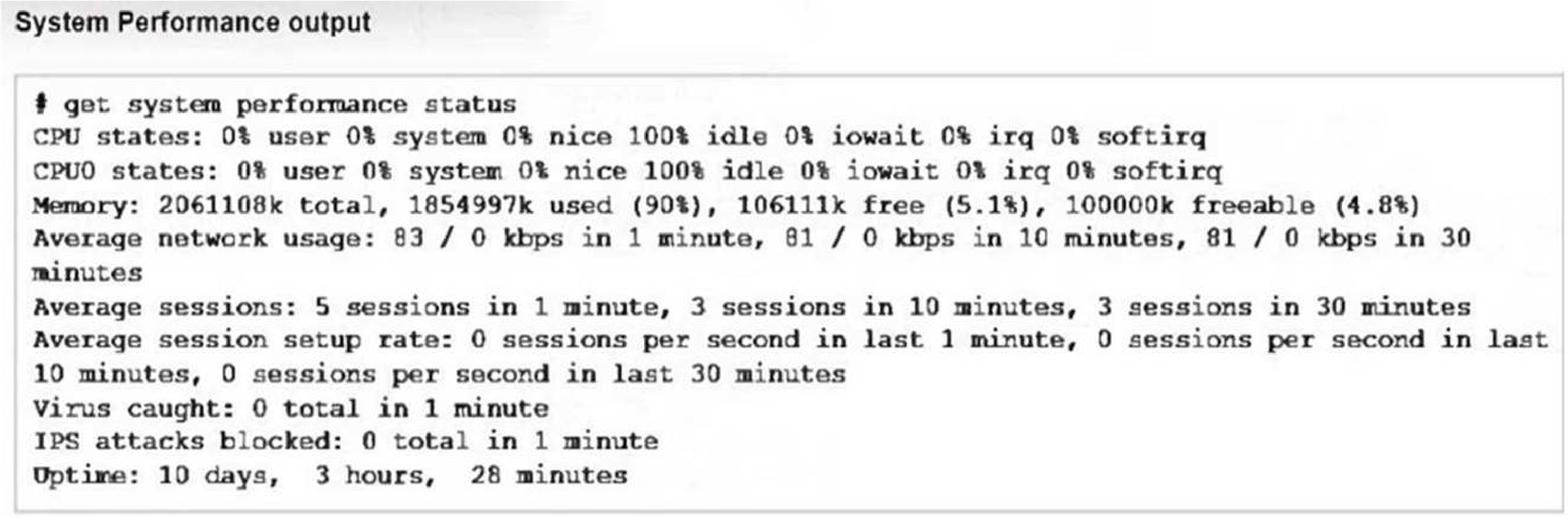
A. They can be run only on devices in the Security Fabric.
B. They can be created only on downstream devices in the fabric.
C. They can have one or more triggers.
D. They can run multiple actions at the same time.

Answer: C

Explanation:
Automation stitches on FortiGate can have one or more triggers, which are conditions or events that activate the automation stitch. The trigger defines when the automation stitch should execute the defined actions. Actions within a stitch can be executed sequentially or in parallel, depending on the configuration.
References:

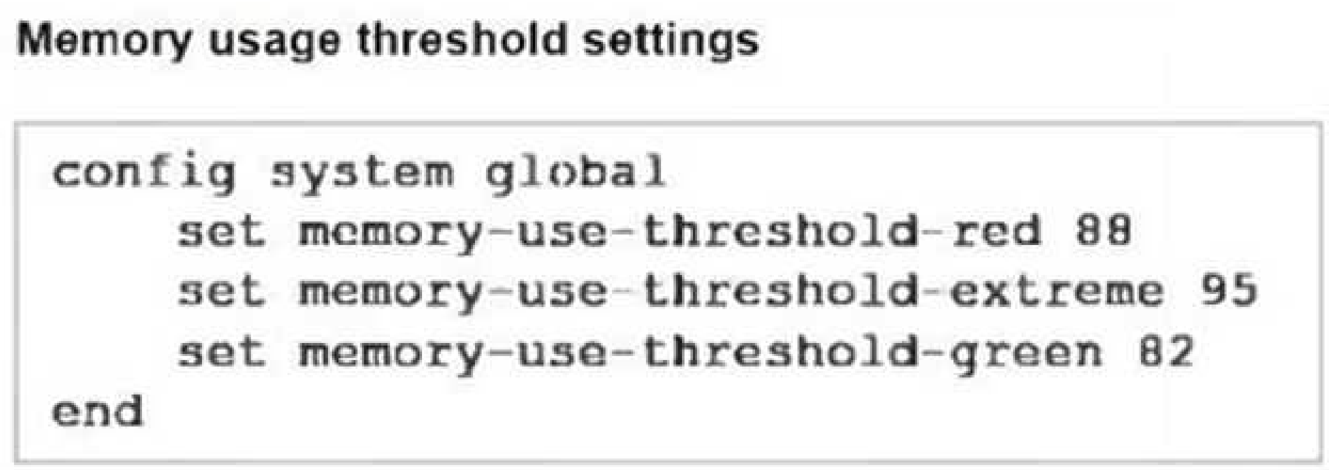
- FortiOS 7.4.1 Administration Guide: Automation Stitches

NEW QUESTION 9
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 onlythrough the console port.

Answer: BC

Explanation:
Based on the system performance output provided, the memory usage on the FortiGate device is at 90%, which is above the green threshold (82%) but below the red threshold (88%). Given this high memory usage, the FortiGate device will enter "conserve mode" to prevent further resource exhaustion. In conserve mode:

- B. FortiGate has entered conserve mode: When the memory usage reaches or exceeds certain thresholds (in this case, the green and red thresholds), the FortiGate enters conserve mode to protect itself from running out of memory entirely. This mode limits some functionalities to reduce memory usage and avoid a potential system crash.
- D. Administrators can access FortiGate only through the console port: During conserve mode, administrative access might be restricted, and administrators may only be able to connect to the device via the console port. This restriction is in place to ensure that the FortiGate can be managed directly, even under low resource conditions.

The other options are not correct:

- A. FortiGate will start sending all files to FortiSandbox for inspection: This is unrelated to memory usage and conserve mode.
- C. Administrators cannot change the configuration: While access may be limited, configuration changes can still be made via the console port.

References

- FortiOS 7.4.1 Administration Guide - Monitoring System Resources and Performance, page 325.
- FortiOS 7.4.1 Administration Guide - Conserve Mode, page 330.

NEW QUESTION 10
An administrator configures FortiGuard servers as DNS servers on FortiGate using default settings. What is true about the DNS connection to a FortiGuard server?

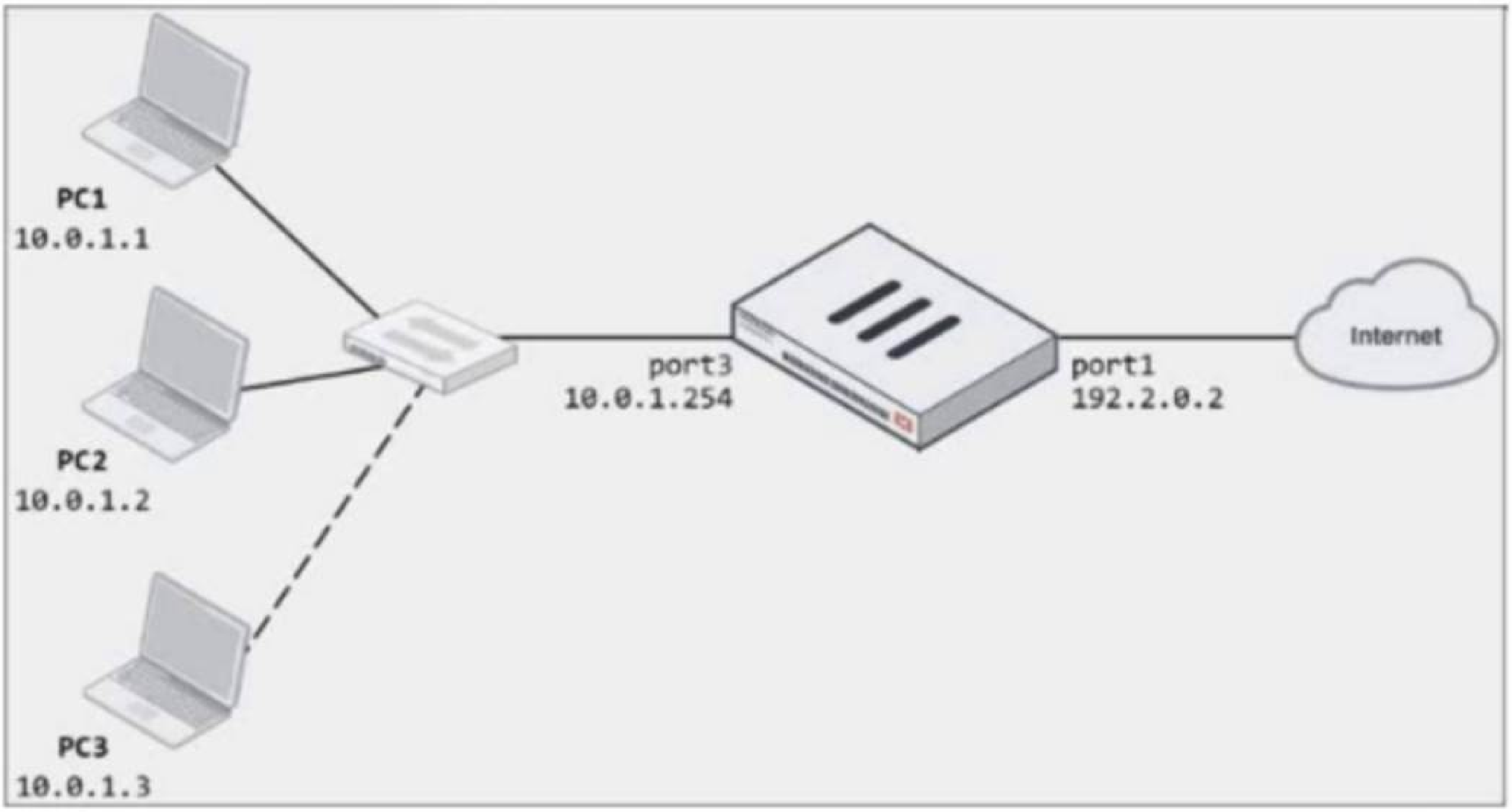
A. It uses UDP 8888.
B. It uses DNS over HTTPS.
C. It uses DNS over TLS.
D. It uses UDP 53.

Answer: D

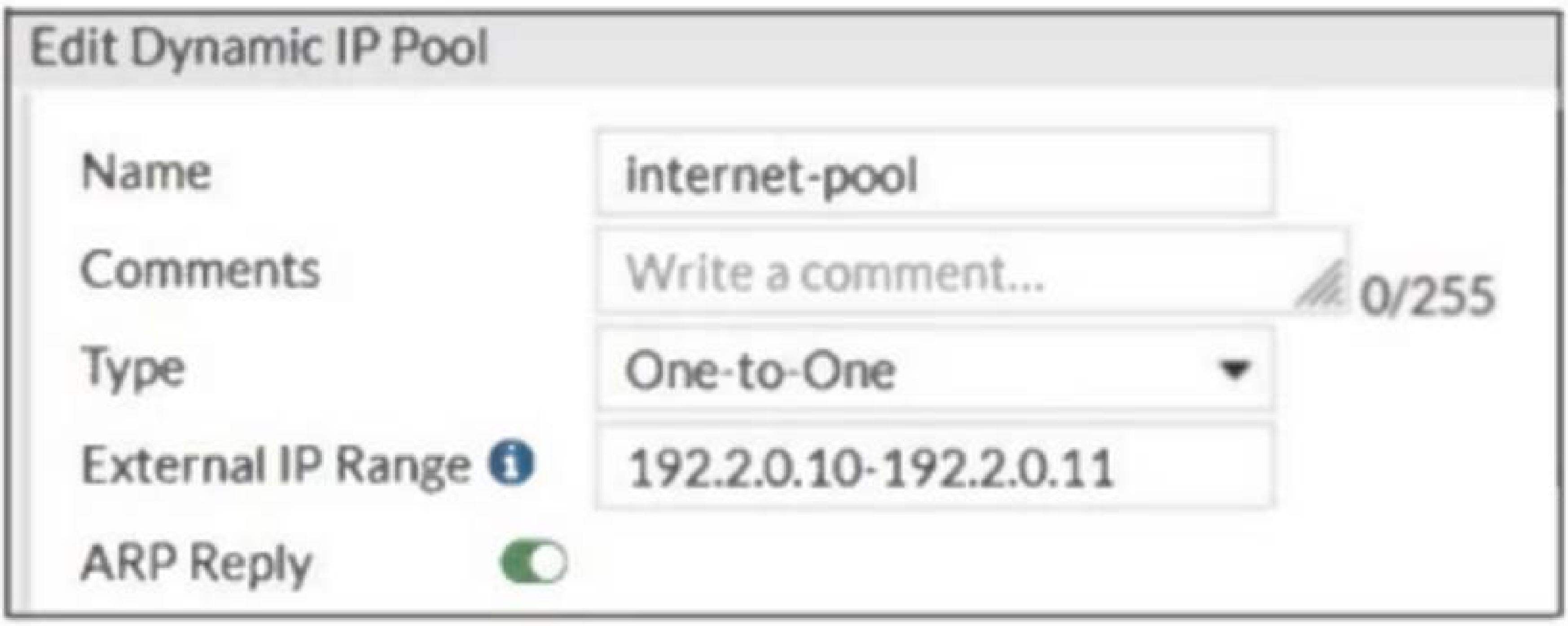
Explanation:
By default, DNS queries to FortiGuard servers use UDP port 53.

NEW QUESTION 10
Refer to the exhibits.

Network diagram



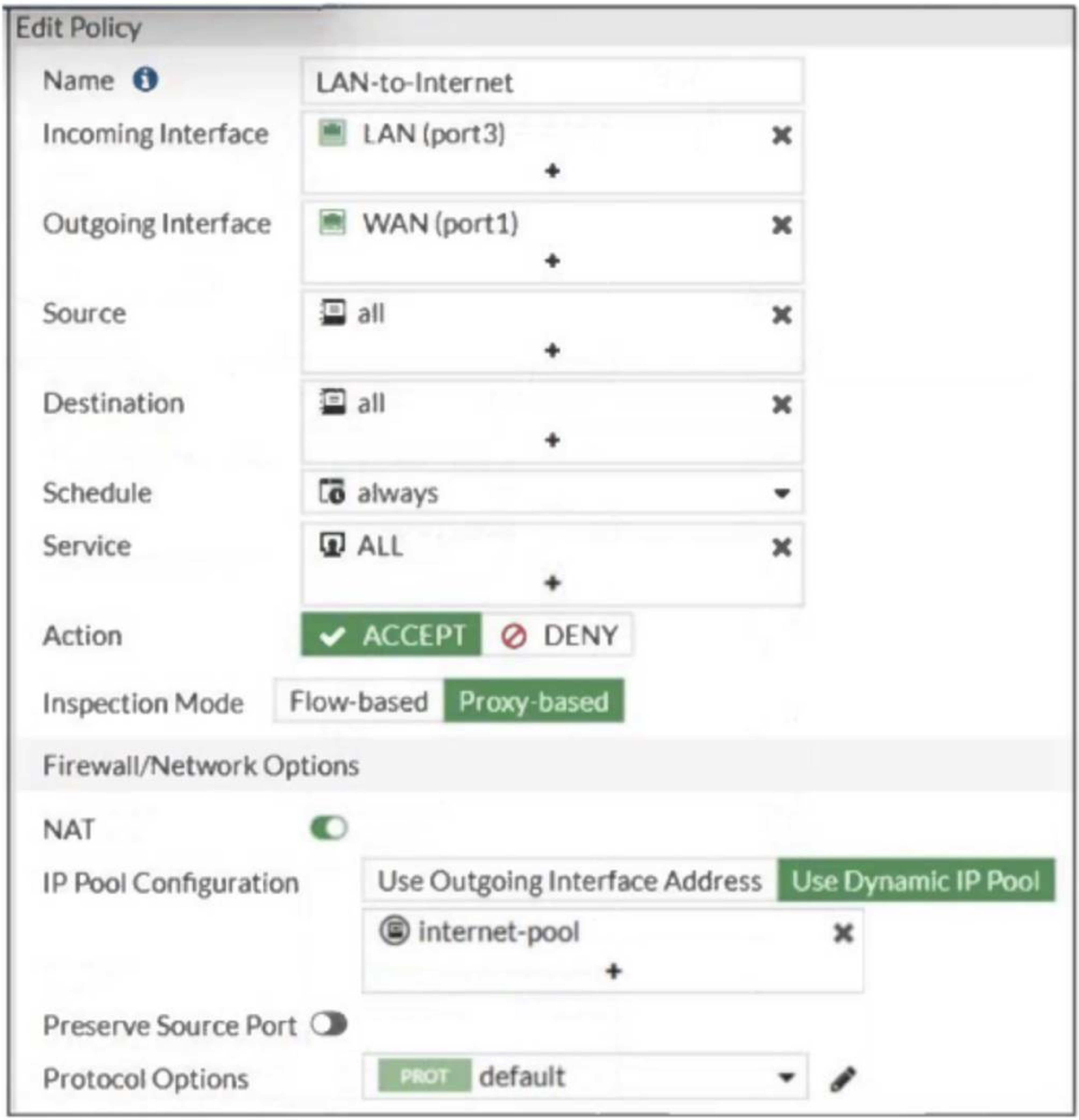
Dynamic IP pool



Edit Dynamic IP Pool

Name	internet-pool
Comments	Write a comment... 0/255
Type	One-to-One
External IP Range	192.2.0.10-192.2.0.11
ARP Reply	●

Firewall policy



Edit Policy

Name	LAN-to-Internet
Incoming Interface	LAN (port3)
Outgoing Interface	WAN (port1)
Source	all
Destination	all
Schedule	always
Service	ALL
Action	[✓ ACCEPT] DENY
Inspection Mode	Flow-based [✓ Proxy-based]

Firewall/Network Options

NAT	●
IP Pool Configuration	Use Outgoing Interface Address [✓ Use Dynamic IP Pool] internet-pool
Preserve Source Port	○
Protocol Options	PROT default

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.
B. 3 as an address object in the source field.
C. In the IP pool configuration, set endig to 192.2.0.12.
D. Configure another firewall policy that matches only the address of PC3 as source, and then place the policy on top of the list.
E. In the IP pool configuration, set cype to overload.

Answer: BD

Explanation:
To resolve the issue of PC3 not being able to access the internet, the administrator needs to adjust the IP pool configuration or the firewall policy. The following two options will fix the connectivity issue:

B. In the IP pool configuration, set the ending IP to 192.2.0.12: The current IP pool range is 192.2.0.10-192.2.0.11, which only provides two IP addresses for network address translation (NAT). To allow PC3 to access the internet, the IP pool should be expanded to include an additional IP address by changing the end of the range to 192.2.0.12.

- D. In the IP pool configuration, set type to overload: Instead of using a one-to-one NAT, changing the type to overload will allow multiple internal addresses (such as PC1, PC2, and PC3) to share a single external IP address. This will solve the issue without needing additional public IP addresses.

The other options are not suitable:

- A. In the firewall policy configuration, add 10.0.1.3 as an address object in the source field: This option is unnecessary since the firewall policy already allows all addresses from the source (LAN port3).
- C. Configure another firewall policy that matches only the address of PC3 as the source, and then place the policy on top of the list: This option is redundant and would not resolve the underlying issue with the IP pool configuration.

References

- FortiOS 7.4.1 Administration Guide - Configuring Firewall Policies, page 512.
- FortiOS 7.4.1 Administration Guide - Configuring NAT with IP Pools, page 518.

NEW QUESTION 14

An administrator configured a FortiGate to act as a collector for agentless polling mode.
What must the administrator add to the FortiGate device to retrieve AD user group information?

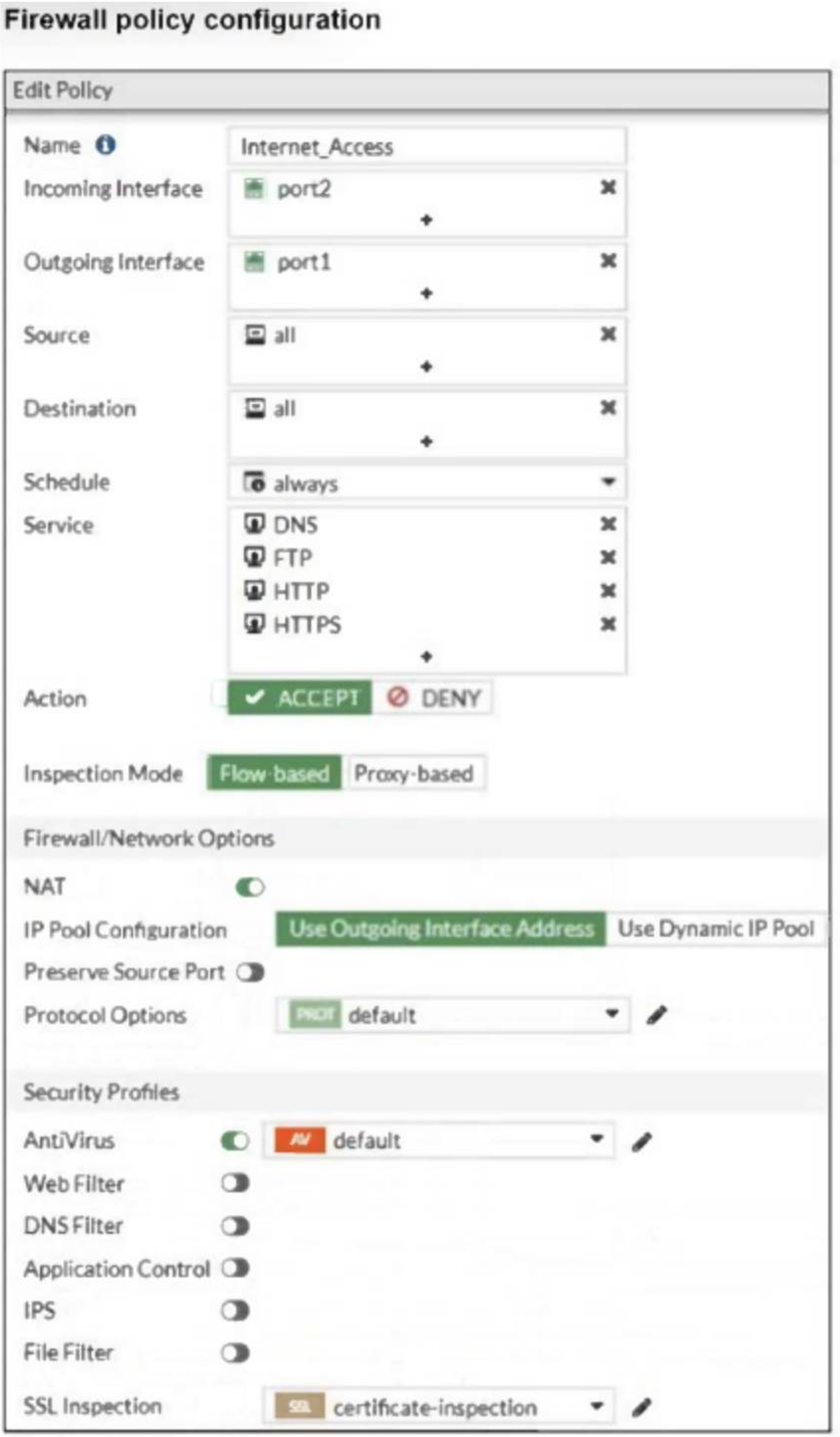
A. LDAP server
B. RADIUS server
C. DHCP server
D. Windows server

Answer: A

Explanation:
To retrieve AD user group information in agentless polling mode, the administrator must add an LDAP server to the FortiGate device.

NEW QUESTION 17

Refer to the exhibit to view the firewall policy.



Firewall policy configuration

Edit Policy

Name	Internet_Access
Incoming Interface	port2
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	DNS FTP HTTP HTTPS
Action	✓ ACCEPT / DENY
Inspection Mode	Flow-based / Proxy-based

Firewall/Network Options

NAT	●
IP Pool Configuration	Use Outgoing Interface Address / Use Dynamic IP Pool
Preserve Source Port	○
Protocol Options	PROT default

Security Profiles

AntiVirus	● AV default
Web Filter	○
DNS Filter	○
Application Control	○
IPS	○
File Filter	○
SSL Inspection	SSL certificate-inspection

Why would the firewall policy not block a well-known virus, for example eicar?

A. The action on the firewall policy is not set to deny.
B. The firewall policy is not configured in proxy-based inspection mode.
C. Web filter is not enabled on the firewall policy to complement the antivirus profile.
D. The firewall policy does not apply deep content inspection.

Answer: B

Explanation:
The firewall policy shown in the exhibit is configured in flow-based inspection mode. In flow-based inspection, certain security features, such as deep content inspection, might not be as effective as in proxy- based mode. Proxy-based inspection is necessary for thorough content inspection, which includes identifying and blocking well-known viruses like EICAR.
References:

- FortiOS 7.4.1 Administration Guide: Inspection Modes

NEW QUESTION 22
A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.
All traffic must be routed through the primary tunnel when both tunnels are up. The secondary tunnel must be used only if the primary tunnel goes down. In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover.
Which two key configuration changes must the administrator make on FortiGate to meet the requirements? (Choose two.)

A. Enable Dead Peer Detection
B. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.
C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
D. Configure a higher distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.

Answer: AC

Explanation:
To configure redundant IPsec VPN tunnels on FortiGate with failover capability, the following two key configuration changes are required:

- A. Enable Dead Peer Detection (DPD): Dead Peer Detection is crucial for detecting if the remote peer is unreachable. By enabling DPD, FortiGate can quickly detect a dead tunnel, ensuring a faster failover to the secondary tunnel when the primary tunnel goes down.
- C. Configure a lower distance on the static route for the primary tunnel and a higher distance on the static route for the secondary tunnel: The static route with the lower distance (higher priority) will be used when both tunnels are operational. If the primary tunnel fails, the higher distance (lower priority) route for the secondary tunnel will take over, ensuring traffic is routed correctly.

The other options are not suitable:

- B. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels:

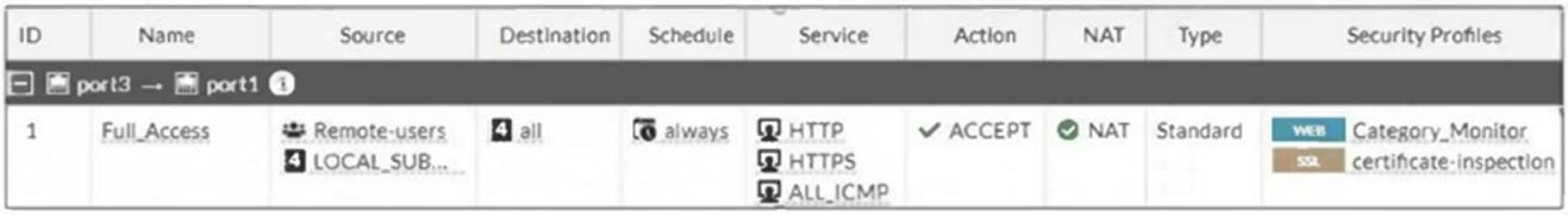
This option is not directly related to the requirements of failover between two IPsec VPN tunnels.

- D. Configure a higher distance on the static route for the primary tunnel and a lower distance on the static route for the secondary tunnel: This would prioritize the secondary tunnel over the primary tunnel, which is opposite to the desired configuration.

References

- FortiOS 7.4.1 Administration Guide - Configuring IPsec VPN, page 1320.
- FortiOS 7.4.1 Administration Guide - Redundant VPN Configuration, page 1335.

NEW QUESTION 27
Refer to the exhibit.



ID	Name	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles
port3 → port1									
1	Full_Access	Remote-users LOCAL_SUB...	all	always	HTTP HTTPS ALL_ICMP	✓ ACCEPT	NAT	Standard	WEB Category_Monitor SSL certificate-inspection

FortiGate is configured for firewall authentication. When attempting to access an external website, the user is not presented with a login prompt.
What is the most likely reason for this situation?

A. The Service DNS is required in the firewall policy.
B. The user is using an incorrect user name.
C. The Remote-users group is not added to the Destination.
D. No matching user account exists for this user.

Answer: A

Explanation:
Firewall authentication generally requires the DNS service to be enabled in the firewall policy to correctly resolve hostnames during the authentication process. If DNS is not allowed in the firewall policy, the FortiGate cannot resolve external domains, and as a result, the user may not be presented with the login prompt when attempting to access an external website.
References:

- FortiOS 7.4.1 Administration Guide: Firewall Authentication Configuration

NEW QUESTION 32
Which two features of IPsec IKEv1 authentication are supported by FortiGate? (Choose two.)

A. Pre-shared key and certificate signature as authentication methods
B. Extended authentication (XAuth)to request the remote peer to provide a username and password
C. Extended authentication (XAuth) for faster authentication because fewer packets are exchanged
D. No certificate is required on the remote peer when you set the certificate signature as the authentication method

Answer: AB

Explanation:
FortiGate supports both pre-shared key and certificate signature methods for IKEv1 authentication. These methods provide flexibility depending on the security requirements of the network. Additionally, FortiGate supports Extended Authentication (XAuth), which requests a username and password from the remote peer, enhancing security by adding an extra layer of authentication. The XAuth method does not necessarily make the authentication faster; it is an additional security measure.
References:

- FortiOS 7.4.1 Administration Guide: IPsec VPN Configuration

NEW QUESTION 35
Which two statements about equal-cost multi-path (ECMP) configuration on FortiGate are true? (Choose two.)

A. If SD-WAN is enabled, you control the load balancing algorithm with the parameter load-balance-mode.
B. If SD-WAN is disabled, you can configure the parameter v4-ecmp-mode to volume-based.
C. If SD-WAN is enabled, you can configure routes with unequal distance and priority values to be part of ECMP
D. If SD-WAN is disabled, you configure the load balancing algorithm in config system settings.

Answer: AD

Explanation:
When SD-WAN is enabled on FortiGate, the load balancing algorithm for Equal-Cost Multi-Path (ECMP) is configured using the load-balance-mode parameter under SD-WAN settings. However, if SD-WAN is disabled, the ECMP load balancing algorithm can be configured under config system settings. This flexibility allows FortiGate to control traffic routing behavior based on the network configuration and requirements.
References:

- FortiOS 7.4.1 Administration Guide: ECMP Configuration

NEW QUESTION 40
What is the primary FortiGate election process when the HA override setting is disabled?

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

Answer: A

Explanation:
When the HA override setting is disabled, FortiGate uses the primary election process based on the following criteria:

- Connected monitored ports: The unit with the most monitored ports up is preferred.
- Priority: The unit with the highest priority is preferred.
- System uptime: The unit with the longest uptime is preferred.
- FortiGate serial number: Used as the final criterion to break any remaining ties.

References:

- FortiOS 7.4.1 Administration Guide: HA election process

NEW QUESTION 41
An employee needs to connect to the office through a high-latency internet connection.
Which SSL VPN setting should the administrator adjust to prevent SSL VPN negotiation failure?

A. SSL VPN idle-timeout
B. SSL VPN login-timeout
C. SSL VPN dtls-hello-timeout
D. SSL VPN session-ttl

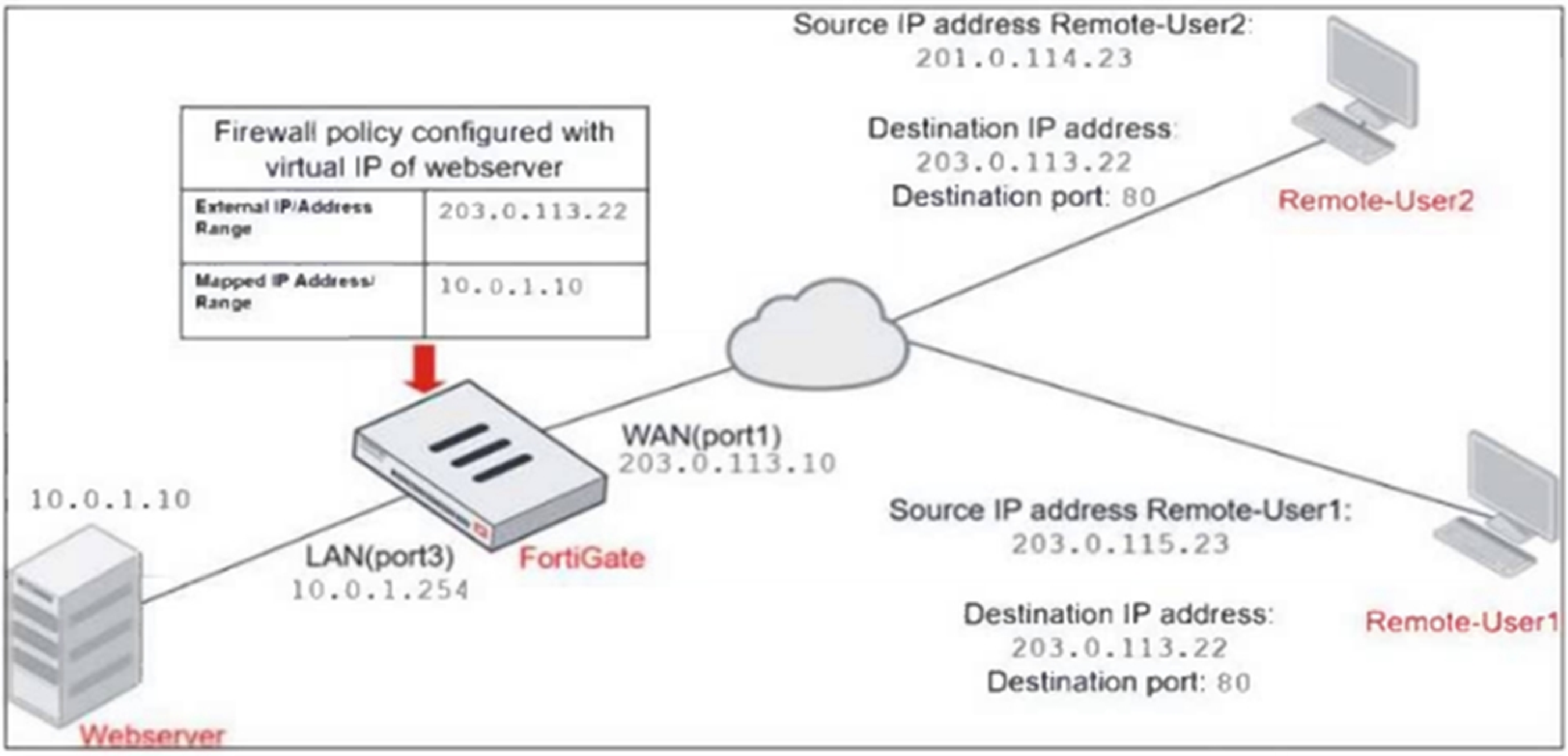
Answer: C

Explanation:
For a high-latency internet connection, the SSL VPN setting that should be adjusted is:
* C. SSL VPN dtls-hello-timeout: This setting determines how long the FortiGate will wait for a DTLS hello message from the client. For high-latency connections, increasing this timeout will prevent SSL VPN negotiation failures caused by delays in receiving the DTLS hello message.
The other options are not suitable:
* A. SSL VPN idle-timeout: This setting controls the idle time allowed before a session is terminated,

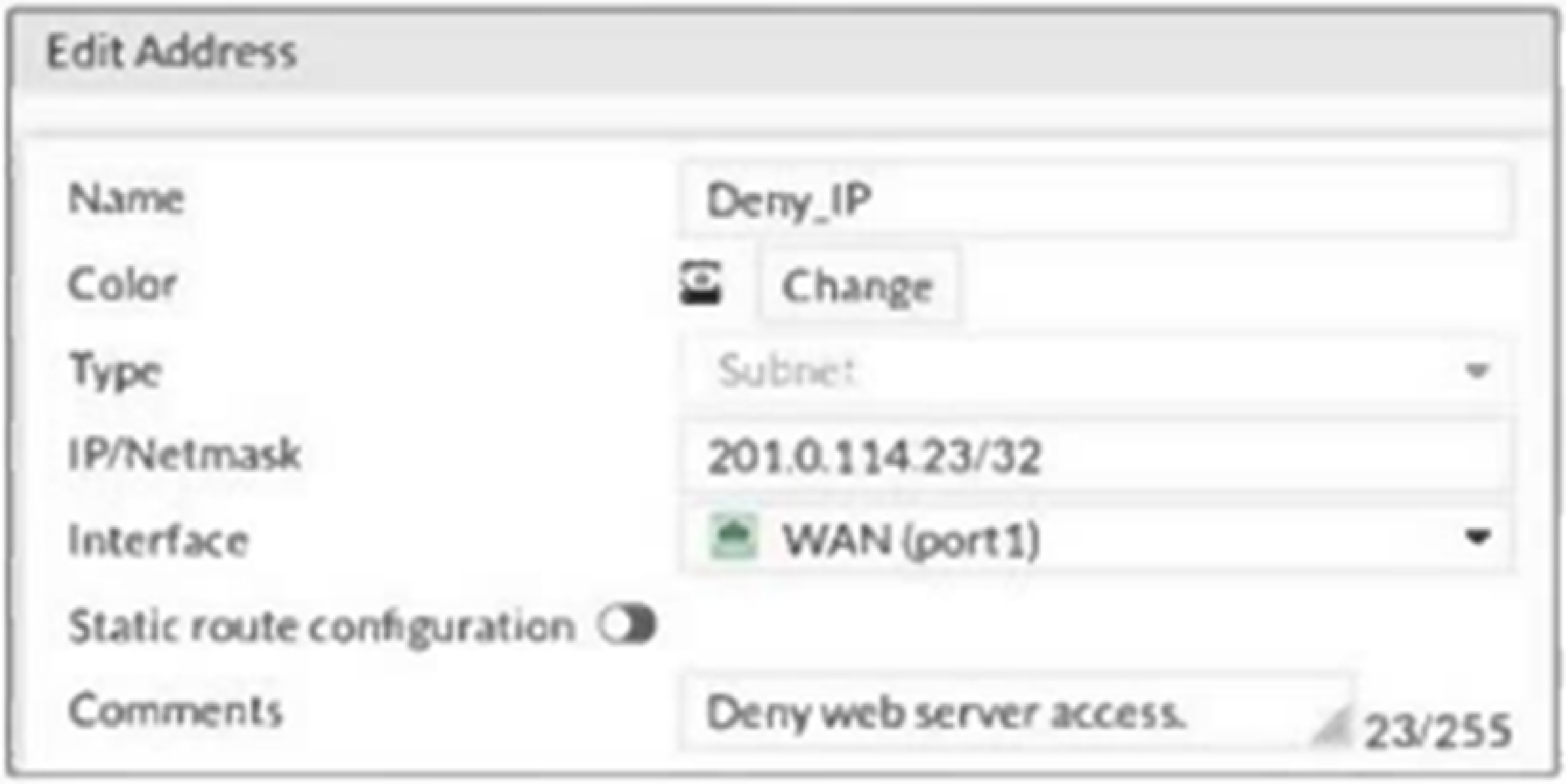
which is not relevant to the initial connection establishment.
* B. SSL VPN login-timeout: This setting controls the maximum time allowed for a user to log in, but does not affect connection negotiation.
* D. SSL VPN session-ttl: This setting controls the total time-to-live for an SSL VPN session but does not directly address issues caused by high latency.
References
FortiOS 7.4.1 Administration Guide - SSL VPN Configuration, page 1415.

NEW QUESTION 42
Refer to the exhibits.

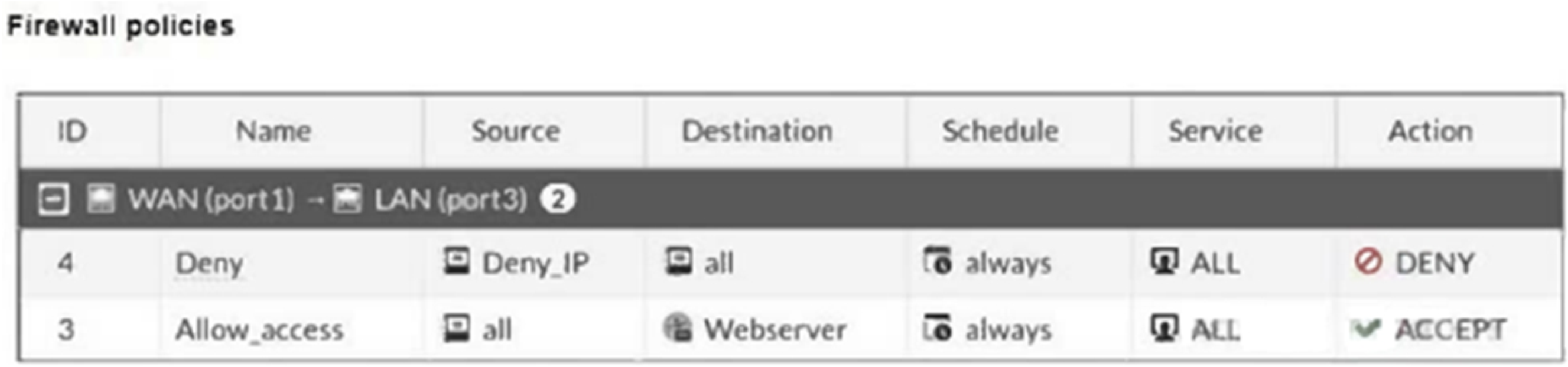
Network diagram



Firewall address object


Edit Address

Name	Deny_IP
Color	Change
Type	Subnet
IP/Netmask	201.0.114.23/32
Interface	WAN (port1)
Static route configuration	○
Comments	Deny web server access. 23/255



Firewall policies

ID	Name	Source	Destination	Schedule	Service	Action
WAN (port1) → LAN (port3) 2						
4	Deny	Deny_IP	all	always	ALL	⊘ DENY
3	Allow_access	all	Webserver	always	ALL	✓ ACCEPT

The exhibits show a diagram of a FortiGate device connected to the network, and the firewall configuration.
An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2.
The policy should work such that Remote-User1 must be able to access the Webserver while preventing Remote-User2 from accessing the Webserver.
Which two configuration changes can the administrator make to the policy to deny Webserver access for Remote-User2? (Choose two.)

A. Enable match-vip in the Deny policy.
B. Set the Destination address as Webserver in the Deny policy.
C. Disable match-vip in the Deny policy.
D. Set the Destination address as Deny_IP in the Allow_access policy.

Answer: AB

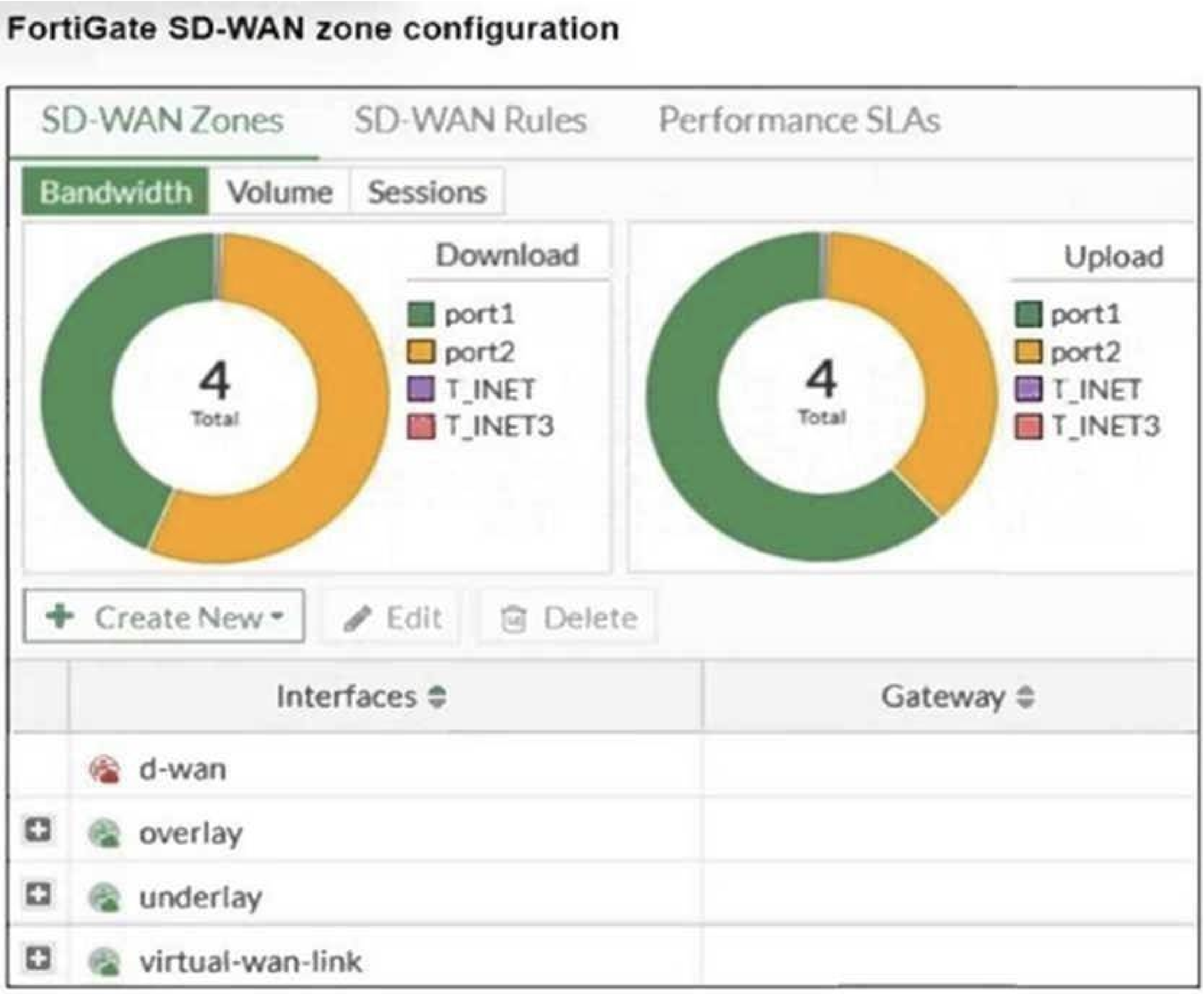
NEW QUESTION 44
Which two IP pool types are useful for carrier-grade NAT deployments? (Choose two.)

A. Port block allocation
B. Fixed port range
C. One-to-one
D. Overload

Answer: AB

Explanation:
In carrier-grade NAT (CGNAT) deployments, specific IP pool types are used to manage large-scale NAT translations efficiently. The correct IP pool types for CGNAT are:
• A. Port block allocation: This type of IP pool allocates a block of ports from a single public IP to multiple clients. It allows efficient use of a limited number of public IPs by distributing port ranges among users, which is crucial for carrier-grade NAT environments where a large number of users need access to the internet.
• B. Fixed port range: In this type, each client is assigned a fixed range of ports, ensuring that the same public IP and port range are used consistently. This helps in reducing the complexity and overhead of managing dynamic port assignments, which is particularly useful in large-scale CGNAT setups.
Why the other options are less appropriate:
• C. One-to-one: One-to-one NAT is used for mapping a single private IP address to a single public IP address. This is not efficient for carrier-grade NAT because CGNAT is designed to allow multiple clients to share a smaller number of public IPs.
• D. Overload: Overload, also known as PAT (Port Address Translation), maps multiple private IPs to a single public IP by differentiating connections based on port numbers. While commonly used in regular NAT setups, CGNAT benefits more from port block allocation and fixed port range due to th

NEW QUESTION 49
Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.



FortiGate SD-WAN zone configuration

	Interfaces ⇕	Gateway ⇕
	d-wan	
⊞	overlay	
⊞	underlay	
⊞	virtual-wan-link	

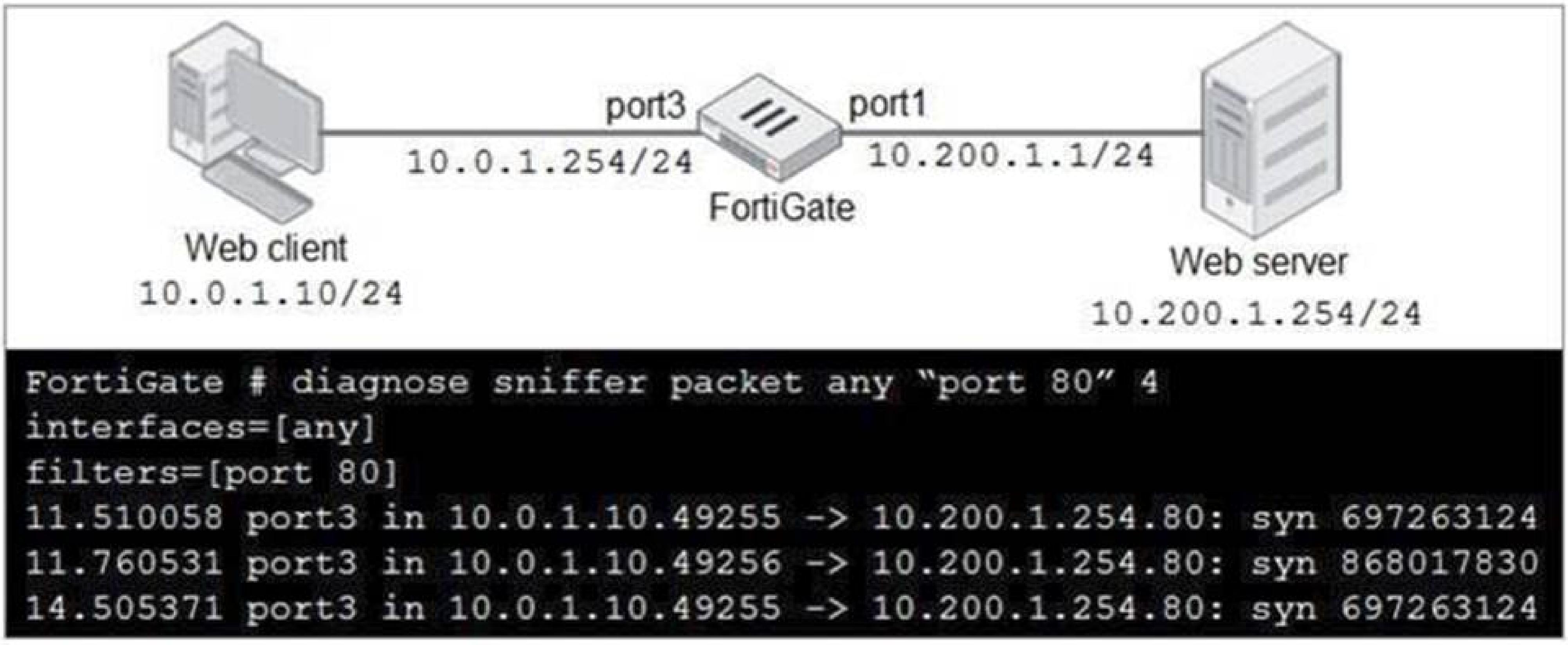
Based on the exhibit, which statement is true?

A. The underlay zone contains port1 and
B. The d-wan zone contains no member.
C. The d-wan zone cannot be deleted.
D. The virtual-wan-link zone contains no member.

Answer: C

Explanation:
In FortiGate's SD-WAN configuration, the d-wan zone is a system default SD-WAN zone that is automatically created and cannot be deleted. This zone is used to manage dynamic WAN links for SD-WAN
traffic balancing and routing. It ensures that multiple WAN interfaces can be grouped and managed
effectively for WAN link optimization.
Why the other options are less appropriate:
• A. The underlay zone contains port1 and: There is no mention in the exhibit about an "underlay zone" containing port1.
• B. The d-wan zone contains no member: This statement is irrelevant since the focus is on the zone's deletion, not its members.
• D. The virtual-wan-link zone contains no member: This is unrelated to the core fact that the d-wan zone cannot be deleted.
Reference:
FortiOS 7.4.1 Administration Guide: SD-WAN Zone Configuration

NEW QUESTION 54
Refer to the exhibit.



```
FortiGate # diagnose sniffer packet any "port 80" 4
interfaces=[any]
filters=[port 80]
11.510058 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
11.760531 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
14.505371 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
```

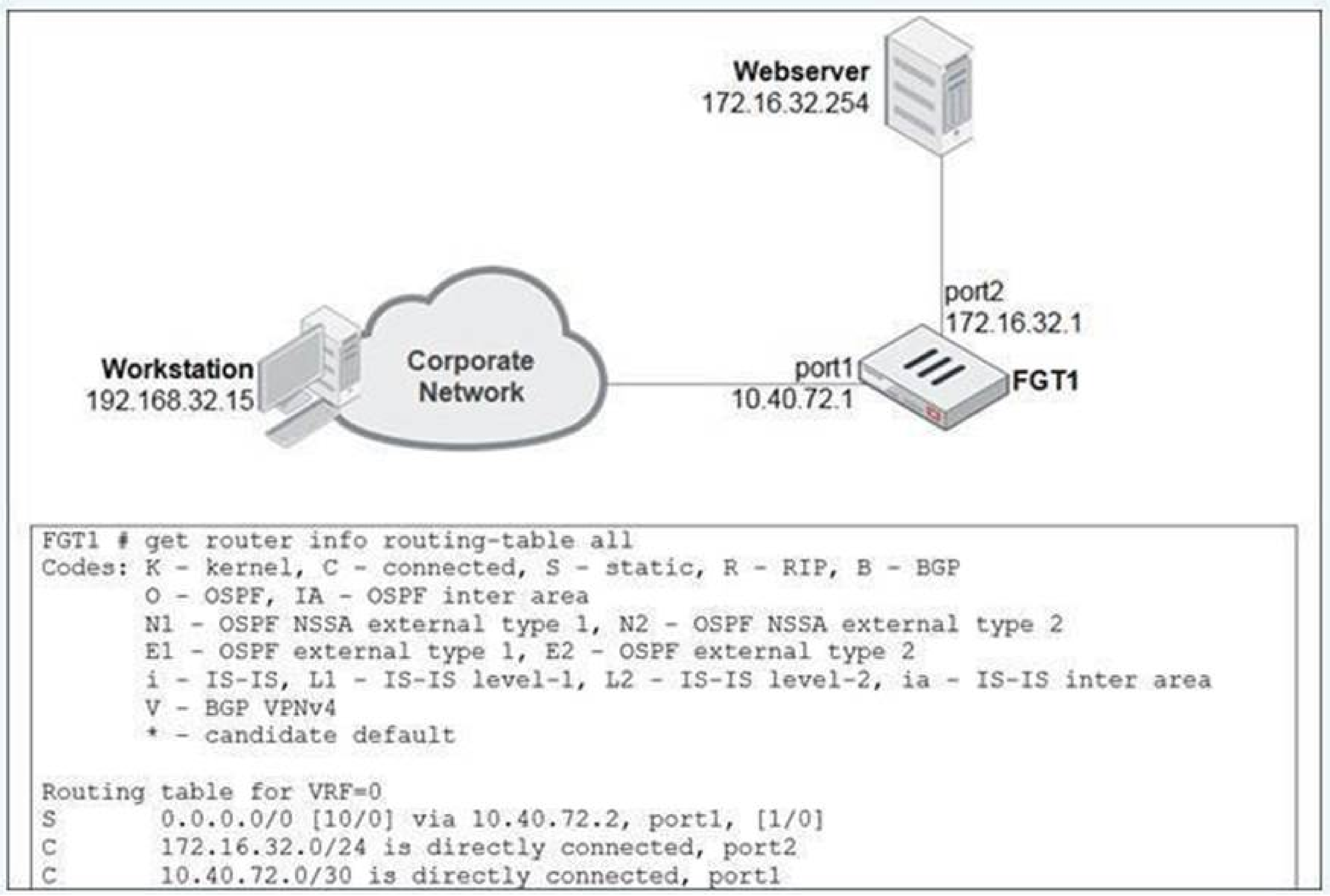
In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output as shown in the exhibit.
What should the administrator do next to troubleshoot the problem?

A. Run a sniffer on the web server.
B. Capture the traffic using an external sniffer connected to port1.
C. Execute another sniffer in the FortiGate, this time with the filter ??host 10.0.1.10??
D. Execute a debug flow.

Answer: D

Explanation:
The next step for troubleshooting the problem would be to execute a debug flow on the FortiGate. The debug flow command provides detailed insights into how FortiGate handles the traffic, including whether the traffic is being dropped, allowed, or forwarded to the correct interface. It helps in identifying issues like firewall policy misconfigurations, routing issues, or NAT problems.
• A. Run a sniffer on the web server: While this might help diagnose server-side issues, the initial focus should be on the FortiGate, as the problem might lie in the firewall configuration or traffic handling.
• B. Capture the traffic using an external sniffer connected to port1: This may provide packetlevel information, but it's more useful to first analyze FortiGate's internal decision-making process with a debug flow.
• C. Execute another sniffer in the FortiGate, this time with the filter ??host 10.0.1.10??: Running a sniffer on the specific host might give more packet details, but the debug flow provides more comprehensive information on how the firewall processes the packets.
Thus, using the debug flow will offer a more direct understanding of how the traffic is being processed or
blocked within FortiGate.

NEW QUESTION 55
View the exhibit.
A user at 192.168.32.15 is trying to access the web server at 172.16.32.254.



```
FGT1 # get router info routing-table all
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
       * - candidate default

Routing table for VRF=0
S       0.0.0.0/0 [10/0] via 10.40.72.2, port1, [1/0]
C       172.16.32.0/24 is directly connected, port2
C       10.40.72.0/30 is directly connected, port1
```

Which two statements best describe how the FortiGate will perform reverse path forwarding (RPF) checks on this traffic? (Choose two.)

A. Strict RPF check will deny the traffic.
B. Loose RPF check will allow the traffic.
C. Strict RPF check will allow the traffic.
D. Loose RPF check will deny the traffic.

Answer: BC

Explanation:
When FortiGate performs reverse path forwarding (RPF) checks, it can operate in two modes: Strict RPF and Loose RPF. Here??s how these two checks work:
In strict RPF, FortiGate checks whether the best route back to the source IP of the packet (in this case, 192.168.32.15) goes through the same interface on which the packet was received. If the best return path uses a different interface, the packet is denied. Based on the scenario:
o C. Strict RPF check will allow the traffic:
If the return path for 192.168.32.15 matches the interface where the traffic was received, the strict RPF check will allow the traffic.
• Loose RPF Check:
In loose RPF, FortiGate only checks if there is any route back to the source IP of the packet, regardless of the interface. This is a more permissive check, and if a route exists, the packet will be allowed.
o B. Loose RPF check will allow the traffic:
Since loose RPF requires only that a valid route to the source exists, the traffic is allowed.
Why the other options are less appropriate:
• A. Strict RPF check will deny the traffic:
This would only happen if the return route didn??t match the incoming interface, which is not indicated here.
• D. Loose RPF check will deny the traffic:
Loose RPF is more permissive, so it will not deny the traffic as long as a valid route to the source IP exists.

NEW QUESTION 60
......