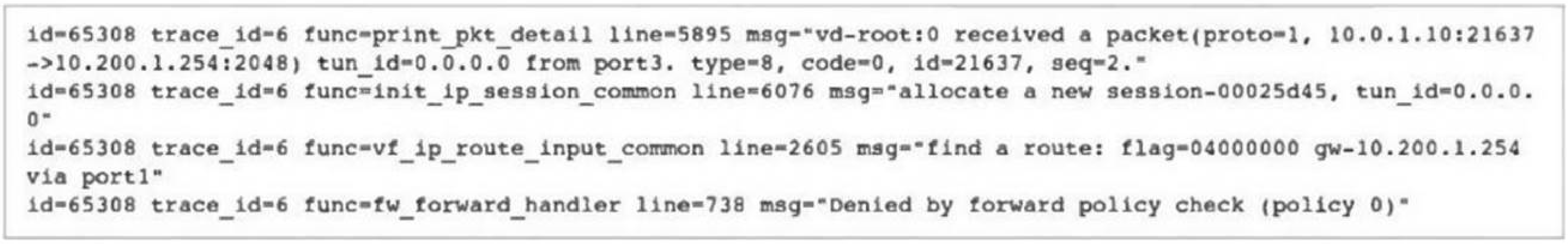
Fortinet

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?

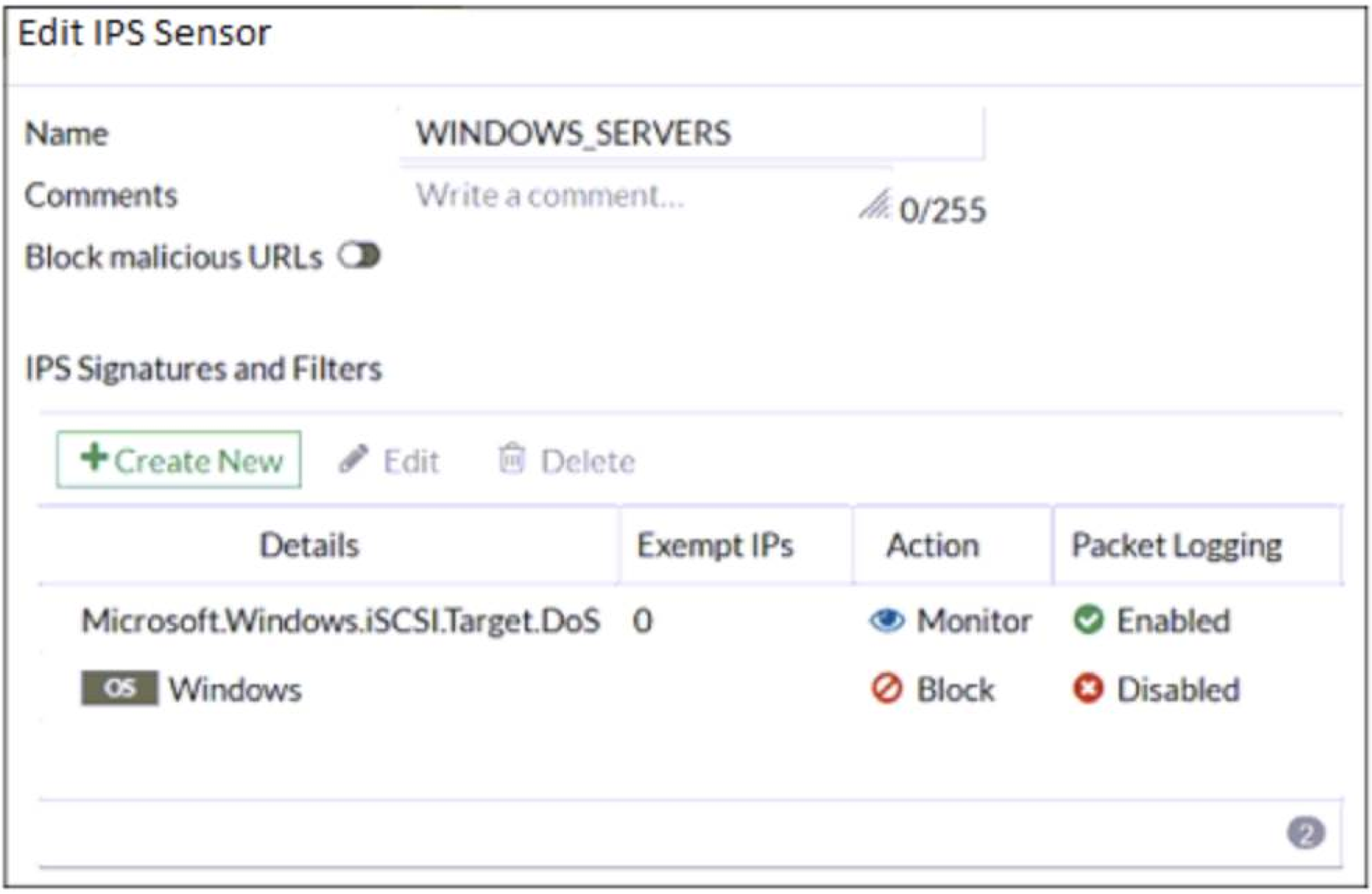
A. It matched an explicitly configured firewall policy with the action DENY
B. It failed the RPF check.
C. The next-hop IP address is unreachable.
D. It matched the default implicit firewall policy

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
Which two statements describe how the RPF check is used? (Choose two.)

A. The RPF check is run on the first sent packet of any new session.
B. The RPF check is run on the first reply packet of any new session.
C. The RPF check is run on the first sent and reply packet of any new session.
D. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.

Answer: AD

Explanation:
The Reverse Path Forwarding (RPF) check is run on the first sent packet of any new session to ensure that the packet arrives on a legitimate interface. This check protects the network from IP spoofing attacks by verifying that a return route exists from the receiving interface back to the source IP address. If the route is invalid or not found, the packet is discarded. Options B and C are incorrect because RPF checks are performed on the first sent packet, not the reply packet.
References:

- FortiOS 7.4.1 Administration Guide: Reverse Path Forwarding (RPF) Check

NEW QUESTION 4
Which three methods are used by the collector agent for AD polling? (Choose three.)

A. WinSecLog
B. WMI
C. NetAPI
D. FSSO REST API
E. FortiGate polling

Answer: ABC

Explanation:
The Fortinet Single Sign-On (FSSO) Collector Agent supports three primary methods for Active Directory (AD) polling to collect user information:

- WinSecLog: Monitors Windows Security Event Logs for login events.
- WMI: Uses Windows Management Instrumentation to poll user login sessions.
- NetAPI: Utilizes the Netlogon API to query domain controllers for user session data.

These methods allow the FortiGate to gather user logon information and enforce user-based policies effectively.
References:

- FortiOS 7.4.1 Administration Guide: FSSO Configuration

NEW QUESTION 5
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 6
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 7
A network administrator has configured an SSL/SSH inspection profile defined for full SSL inspection and set with a private CA certificate. The firewall policy that allows the traffic uses this profile for SSL inspection
and performs web filtering. When visiting any HTTPS websites, the browser reports certificate warning errors.
What is the reason for the certificate warning errors?

A. The SSL cipher compliance option is not enabled on the SSL inspection profil
B. This setting is required when the SSL inspection profile is defined with a private CA certificate.
C. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.
D. The browser does not recognize the certificate in use as signed by a trusted CA.
E. With full SSL inspection it is not possible to avoid certificate warning errors at the browser level.

Answer: C

Explanation:
The certificate warning errors occur because the SSL inspection profile is configured to use a private CA certificate that is not recognized by the browser as being signed by a trusted CA. For the browser to trust the FortiGate's re-signed certificates, the CA certificate used by FortiGate for SSL inspection must be installed in the browser's trusted certificate store. Until the browser recognizes the certificate authority (CA) as trusted, it will continue to display warning errors when accessing HTTPS websites.
References:

- FortiOS 7.4.1 Administration Guide: SSL/SSH Inspection Configuration

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
Which method allows management access to the FortiGate CLI without network connectivity?

A. SSH console
B. CLI console widget
C. Serial console
D. Telnet console

Answer: C

Explanation:
The serial console method allows management access to the FortiGate CLI without relying on network connectivity. This method involves directly connecting a computer to the FortiGate device using a serial cable (such as a DB-9 to RJ-45 cable or USB to RJ-45 cable) and using terminal emulation software to interact with the FortiGate CLI. This method is essential for situations where network-based access methods (such as SSH or Telnet) are not available or feasible.
References:

- FortiOS 7.4.1 Administration Guide: Console connection

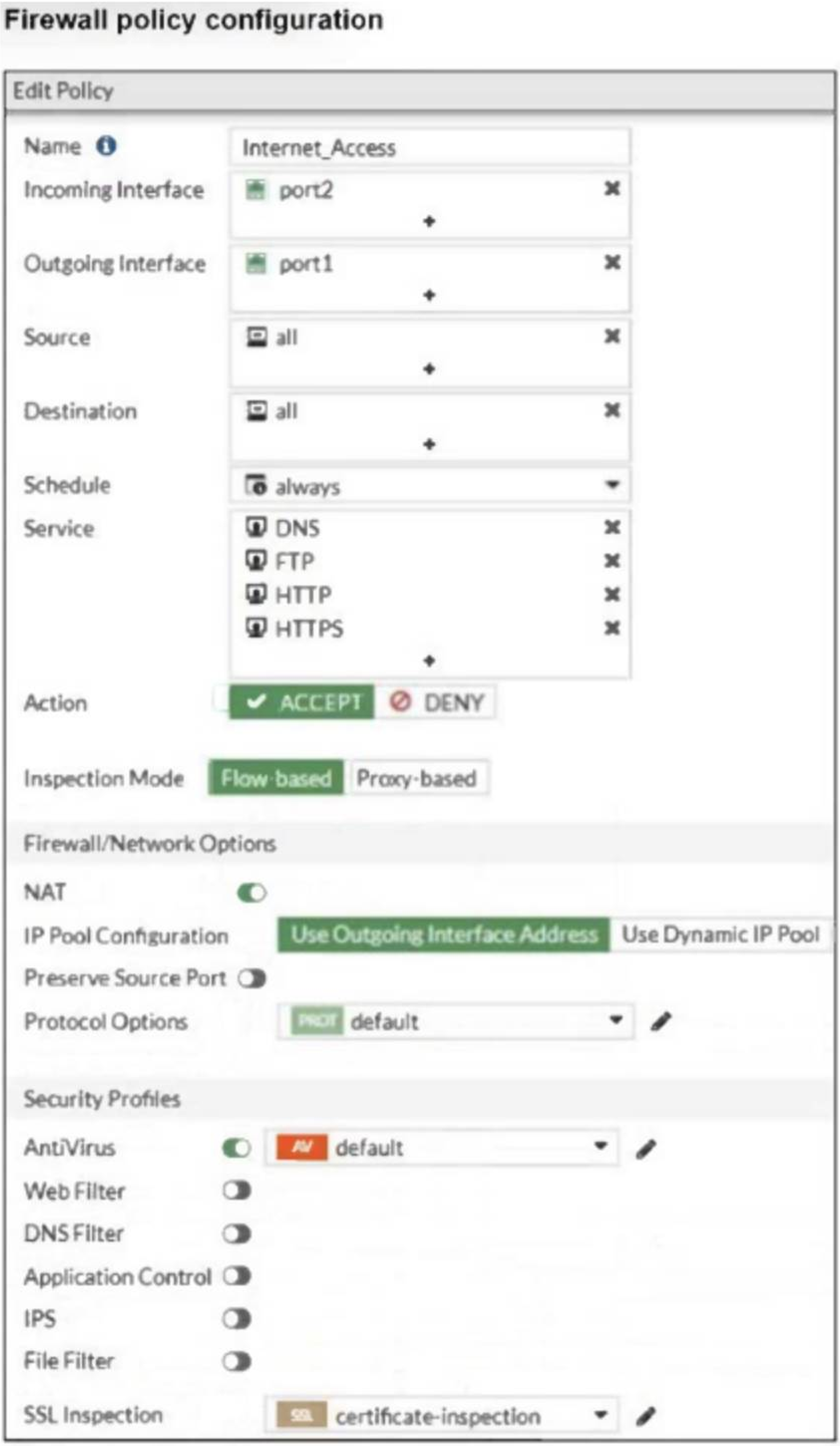
NEW QUESTION 10
An administrator configures FortiGuard servers as DNS servers on FortiGate using default settings. What is true about the DNS connection to a FortiGuard server?

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 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?

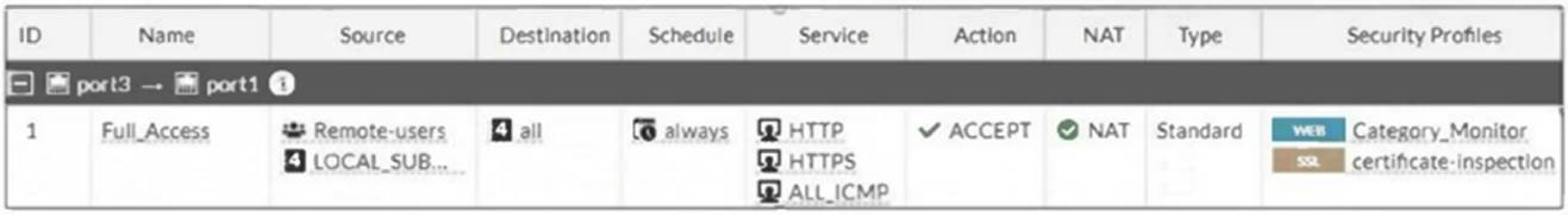
A. The action on the firewall policy is not set to deny.
B. The firewall policy is not configured in proxy-based inspection mode.
C. Web filter is not enabled on the firewall policy to complement the antivirus profile.
D. The firewall policy does not apply deep content inspection.

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 12
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.

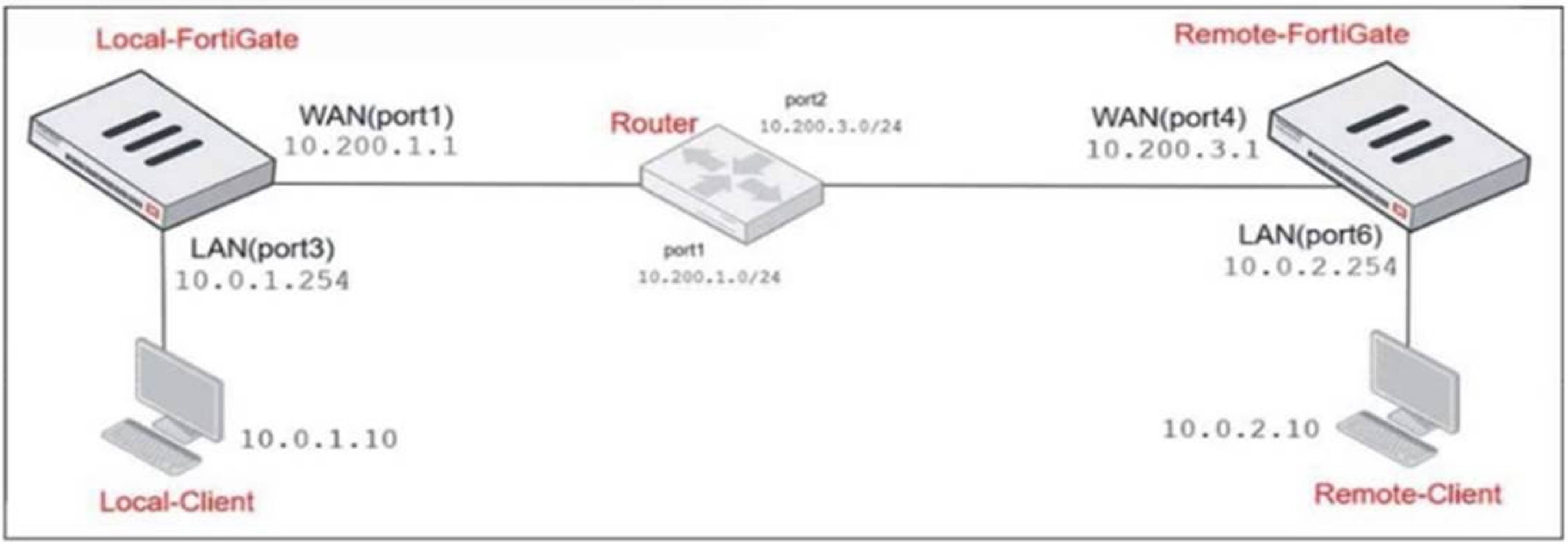
Answer: A

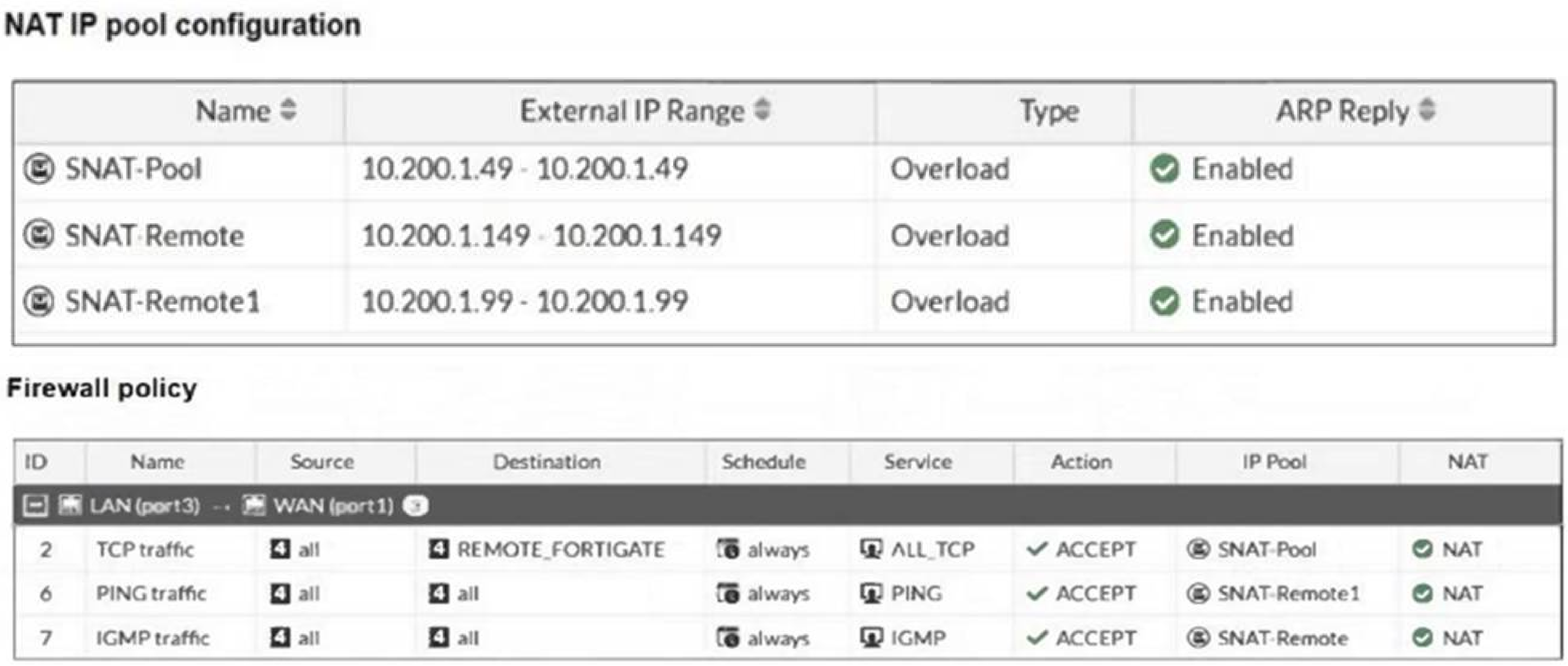
Explanation:
Firewall authentication generally requires the DNS service to be enabled in the firewall policy to correctly resolve hostnames during the authentication process. If DNS is not allowed in the firewall policy, the FortiGate cannot resolve external domains, and as a result, the user may not 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 16
Refer to the exhibits.

Network diagram





NAT IP pool configuration

Name	External IP Range	Type	ARP Reply
SNAT-Pool	10.200.1.49 - 10.200.1.49	Overload	✓ Enabled
SNAT-Remote	10.200.1.149 - 10.200.1.149	Overload	✓ Enabled
SNAT-Remote1	10.200.1.99 - 10.200.1.99	Overload	✓ Enabled

Firewall policy

ID	Name	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN (port3) → WAN (port1) 3								
2	TCP traffic	all	REMOTE_FORTIGATE	always	ALL_TCP	✓ ACCEPT	SNAT-Pool	✓ NAT
6	PING traffic	all	all	always	PING	✓ ACCEPT	SNAT-Remote1	✓ NAT
7	IGMP traffic	all	all	always	IGMP	✓ ACCEPT	SNAT-Remote	✓ NAT

The exhibits show a diagram of a FortiGate device connected to the network, as well as the IP pool configuration and firewall policy objects.
The WAN (port1) interface has the IP address 10.200.1.1/24. The LAN (port3) interface has the IPaddress 10.0.1.254/24.
Which IP address will be used to source NAT (SNAT) the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?

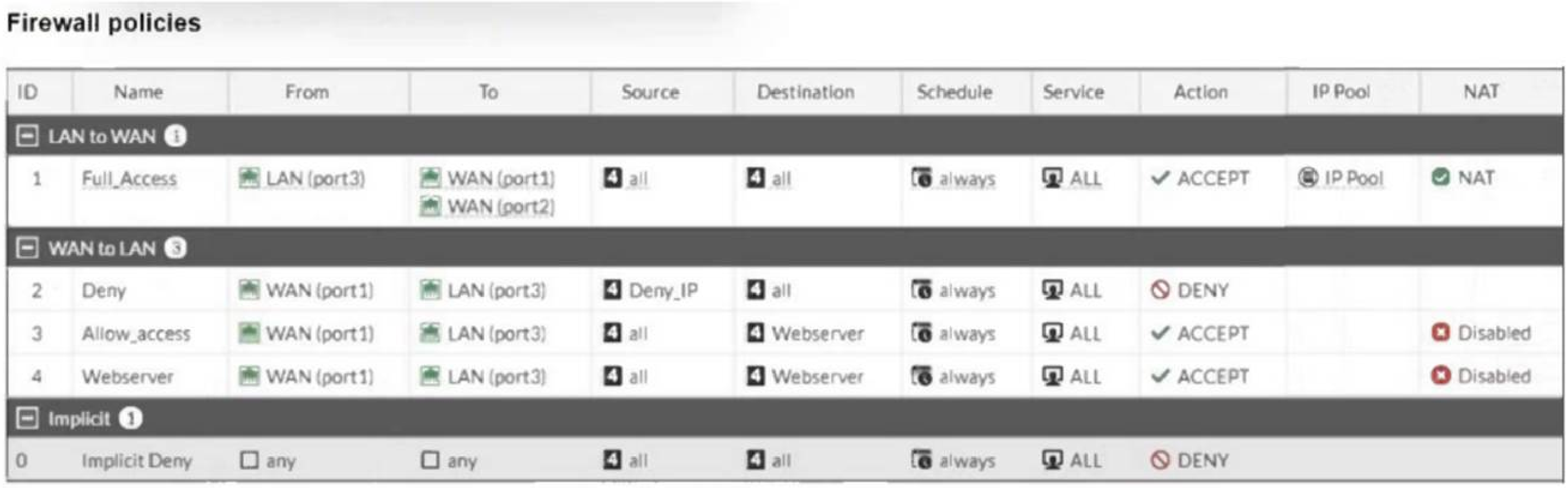
A. 10.200.1.1B.10.200.1.149C.10.200.1.99
B. 10.200.1.49

Answer: C

Explanation:
The traffic from the user on Local-Client (10.0.1.10) pinging the IP address of Remote-FortiGate (10.200.3.1) will match the firewall policy with the service "PING traffic". According to the firewall policy:

- Policy ID 6 is set for PING traffic and uses the NAT IP pool "SNAT-Remote1", which is defined as 10.200.1.99.

NEW QUESTION 18
Refer to the exhibit.



Firewall policies

ID	Name	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN to WAN 1										
1	Full_Access	LAN (port3)	WAN (port1) WAN (port2)	all	all	always	ALL	✓ ACCEPT	IP Pool	✓ NAT
WAN to LAN 3										
2	Deny	WAN (port1)	LAN (port3)	Deny_IP	all	always	ALL	⊘ DENY		
3	Allow_access	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	✓ ACCEPT		✖ Disabled
4	Webserver	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	✓ ACCEPT		✖ Disabled
Implicit 1										
0	Implicit Deny	□ any	□ any	all	all	always	ALL	⊘ DENY		

Which statement about this firewall policy list is true?

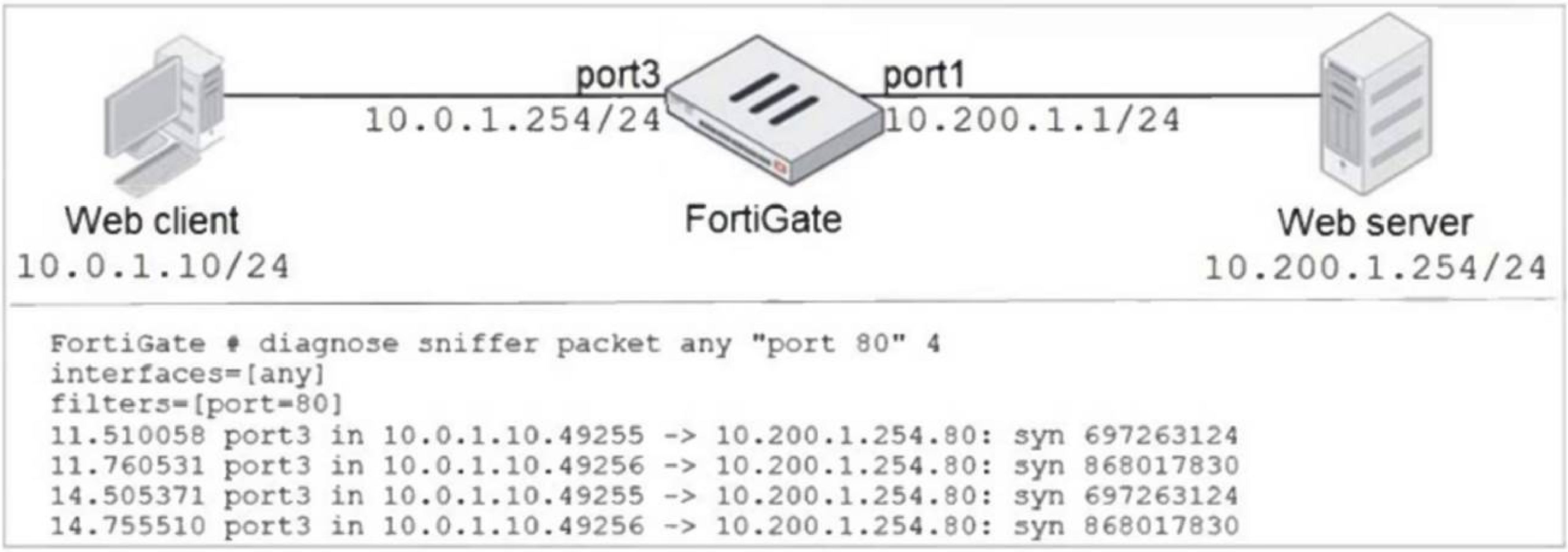
A. The Implicit group can include more than one deny firewall policy.
B. The firewall policies are listed by ID sequence view.
C. The firewall policies are listed by ingress and egress interfaces pairing view.
D. LAN to WA
E. WAN to LA
F. and Implicit are sequence grouping view lists.

Answer: C

Explanation:
The firewall policy list in the exhibit is arranged in the "Interface Pair View," where policies are grouped by their incoming (ingress) and outgoing (egress) interface pairs. Each section (LAN to WAN, WAN to LAN, etc.) groups policies based on these interface pairings. This view helps administrators quickly identify which policies apply to specific traffic flows between network interfaces. Options A and D are incorrect because the Implicit group typically does not include more than one deny policy, and there is no "sequence grouping view" in FortiGate. Option B is incorrect as the list is not displayed strictly by ID sequence.
References:
FortiOS 7.4.1 Administration Guide: Firewall Policy Views

NEW QUESTION 19

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
14.755510 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
```

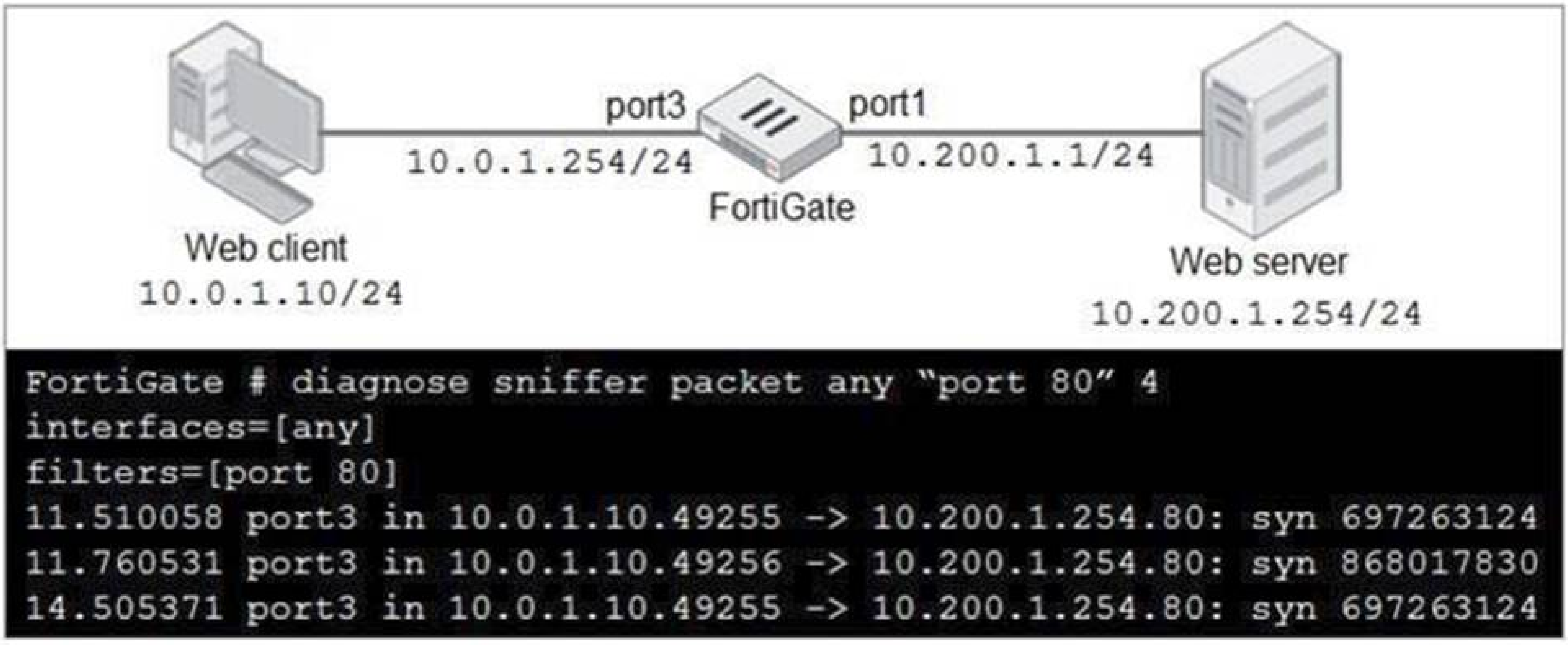
In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output shown in the exhibit.
What should the administrator do next, to troubleshoot the problem?

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

Answer: A

NEW QUESTION 22

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?

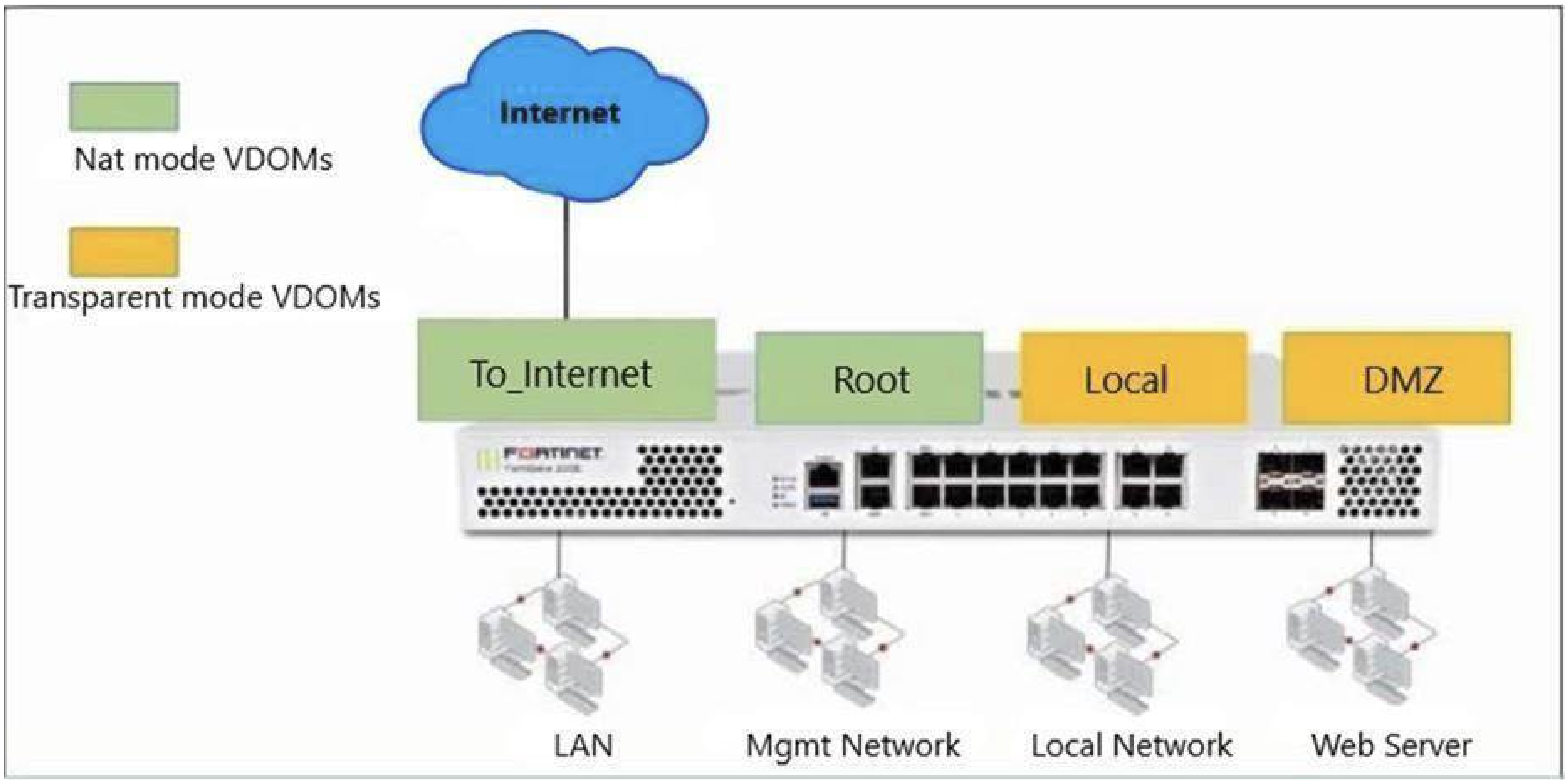
A. Run a sniffer on the web server.
B. Capture the traffic using an external sniffer connected to port1.
C. Execute another sniffer in the FortiGate, this time with the filter ??host 10.0.1.10??
D. Execute a debug flow.

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 25
Refer to the exhibit.



The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.
The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem.
With this configuration, which statement is true?

A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.
B. A default static route is not required on the To_Internet VDOM to allow LAN users to access the internet.
C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.
D. Inter-VDOM links are not required between the Root and To_Internet VDOMs because the Root VDOM is used only as a management VDOM.

Answer: A

Explanation:
In this scenario, multiple Virtual Domains (VDOMs) are used, and each VDOM operates either in NAT mode or transparent mode:
- Root VDOM (management) and To_Internet VDOM are in NAT mode.
- DMZ VDOM and Local VDOM are in transparent mode.

To allow traffic between different VDOMs (e.g., Local and Root), inter-VDOM links must be configured.
Since Local VDOM is in transparent mode, it functions at Layer 2, meaning it requires an inter-VDOM link to pass traffic through the Root VDOM, which operates in NAT mode at Layer 3.
Why the other options are less appropriate:
- B. A default static route is not required on the To_Internet VDOM:

A default route is required on the To_Internet VDOM to send traffic from LAN users to the internet.
- C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs:

Both Local and DMZ are in transparent mode and operate at Layer 2, so direct communication would require inter-VDOM links if passing through another VDOM.
- D. Inter-VDOM links are not required between the Root and To_Internet VDOMs:

Even if the Root VDOM is only used for management, it still requires inter-VDOM links to communicate with other VDOMs (like To_Internet) in the Security Fabric.

NEW QUESTION 29
Consider the topology:
Application on a Windows machine <--{SSL VPN} -->FGT--> Telnet to Linux server.
An administrator is investigating a problem where an application establishes a Telnet session to a Linux server over the SSL VPN through FortiGate and the idle session times out after about 90 minutes. The administrator would like to increase or disable this timeout.
The administrator has already verified that the issue is not caused by the application or Linux server.
This issue does not happen when the application establishes a Telnet connection to the Linux server directly on the LAN.
What two changes can the administrator make to resolve the issue without affecting services running through FortiGate? (Choose two.)

A. Set the maximum session TTL value for the TELNET service object.
B. Set the session TTL on the SSLVPN policy to maximum, so the idle session timeout will not happenafter 90 minutes.
C. Create a new service object for TELNET and set the maximum session TTL.
D. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy.

Answer: CD

Explanation:
The issue with the idle session timing out after 90 minutes can be resolved by adjusting the session Time-To-Live (TTL) for the TELNET service used over the SSL VPN connection. Here's how the administrator can address the problem:

• C. Create a new service object for TELNET and set the maximum session TTL:
By creating a new service object specifically for TELNET and setting a custom maximum session TTL, the administrator can ensure that the TELNET session does not time out prematurely. This way, the session will last longer or indefinitely, depending on the configured TTL.
• D. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy:
Creating a dedicated firewall policy for SSL VPN traffic and placing it above the existing one allows the administrator to apply the new TELNET service object with a longer session TTL. This will ensure the new policy with the adjusted settings takes precedence for TELNET traffic.
Why the other options are less appropriate:
• A. Set the maximum session TTL value for the TELNET service object:
This would work if you were adjusting an existing TELNET service object. However, creating a new service object for TELNET and applying it in the firewall policy (as described in options C and D) is more granular and won't affect other services using the same TELNET object.
• B. Set the session TTL on the SSLVPN policy to maximum:
While this would extend the session timeout for the entire SSL VPN traffic, it could affect other services running through the SSL VPN, which may not be desirable. This option would lack the necessary specificity for only the TELNET traffic.

NEW QUESTION 34
Which three criteria can FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)

A. Services defined in the firewall policy
B. Highest to lowest priority defined in the firewall policy
C. Destination defined as Internet Services in the firewall policy
D. Lowest to highest policy ID number
E. Source defined as Internet Services in the firewall policy

Answer: ACE

Explanation:
• A. Services defined in the firewall policy: FortiGate uses the service specified in the firewall policy to match traffic. Services define the types of traffic (like HTTP, FTP) that the policy will apply to.
• C. Destination defined as Internet Services in the firewall policy: Policies can be matched based on the destination being categorized as Internet Services, allowing specific handling of such traffic.
• E. Source defined as Internet Services in the firewall policy: Similarly, traffic from sources categorized as Internet Services can be matched and processed according to the policy configuration.
Why the other options are less relevant:
• B. Highest to lowest priority defined in the firewall policy: Policies are processed from top to bottom, not by priority. The highest priority policy is processed first, but this is about the order of policy processing rather than criteria for matching traffic.
• D. Lowest to highest policy ID number: Policies are processed from the top of the list (the lowest policy ID) to the bottom (the highest policy ID), which is about the processing order rather than matching criteria.

NEW QUESTION 36
......