Exam Questions FCP_FGT_AD-7.4

FCP - FortiGate 7.4 Administrator

https://www.2passeasy.com/dumps/FCP_FGT_AD-7.4/

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.

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.iSCSI.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

A network administrator is configuring an IPsec VPN tunnel for a sales employee travelling abroad. Which IPsec Wizard template must the administrator apply?

A. Remote Access
B. Site to Site
C. Dial up User
D. iHub-and-Spoke

Answer: A

Explanation:

For configuring an IPsec VPN tunnel for a sales employee traveling abroad, the "Remote Access" template is the most appropriate choice. This template is designed to allow remote users to securely connect to the internal network of an organization from any location using FortiClient or a compatible client. The other options, such as "Site to Site," "Dial up User," and "iHub-and-Spoke," are used for connecting different networks or sites, not individual remote users.

References:

FortiOS 7.4.1 Administration Guide: IPsec Wizard Template Types

NEW QUESTION 4

Refer to the exhibits, which show the firewall policy and an antivirus profile configuration.

Edit Antivirus Profile

Name	default
Comments	Scan files and block viruses. 29/255
AntiVirus scan 🛈	**Block** Monitor
Feature set	**Flow-based** Proxy-based

Inspected Protocols

HTTP 🟢

SMTP 🟢

POP3 🟢

IMAP 🟢

FTP 🟢

CIFS ⚪

APT Protection Options

Treat Windows executables
in email attachments as viruses 🛈 🟢

Send files to FortiSandbox for inspection 🛈 ⚪

Send files to FortiNDR for inspection 🛈 ⚪

Include mobile malware protection 🟢

Quarantine 🛈 ⚪

Virus Outbreak Prevention 🛈

Use FortiGuard outbreak prevention database ⚪

Use external malware block list ⚪

Use EMS threat feed 🛈 ⚪

Why is the user unable to receive a block replacement message when downloading an infected file for the first time?

A. The intrusion prevention security profile must be enabled when using flow-based inspection mode.
B. The option to send files to FortiSandbox for inspection is enabled.
C. The firewall policy performs a full content inspection on the file.

D. Flow-based inspection is used, which resets the last packet to the user.

Answer: D

Explanation:
In flow-based inspection mode, FortiGate sends a reset (RST) packet to the client instead of providing a replacement message, which causes the block message not to be displayed.

NEW QUESTION 5
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 6
Which inspection mode does FortiGate use for application profiles if it is configured as a profile-based next- generation firewall (NGFW)?

A. Full content inspection
B. Proxy-based inspection
C. Certificate inspection
D. Flow-based inspection

Answer: D

Explanation:
When FortiGate is configured in NGFW profile-based mode, it primarily uses flow-based inspection for application profiles. Flow-based inspection provides faster processing and lower latency by inspecting traffic in real-time without buffering, making it suitable for scenarios where performance is a priority.
References:

» FortiOS 7.4.1 Administration Guide: Inspection Modes

NEW QUESTION 7
Refer to the exhibit.
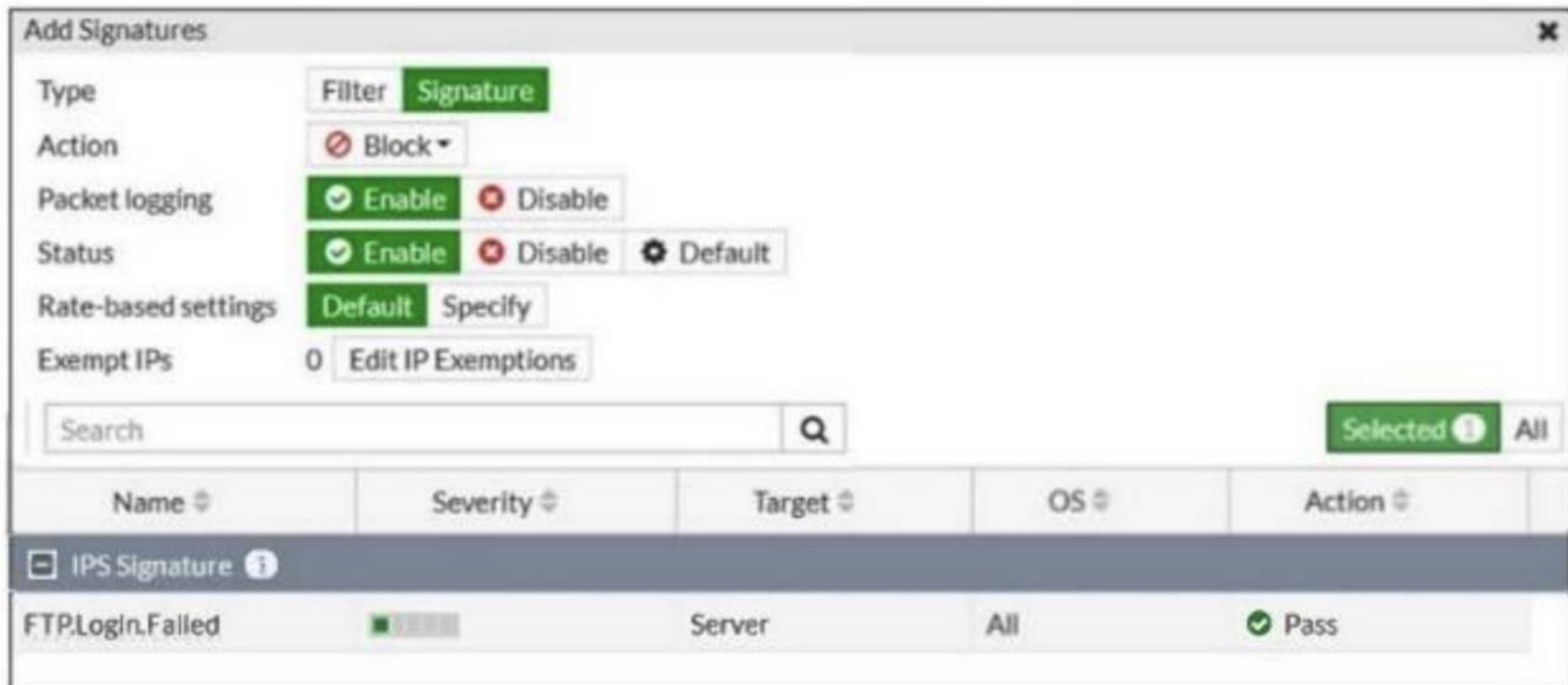
Review the intrusion prevention system (IPS) profile signature settings shown in the exhibit. What do you conclude when adding the FTP.Login.Failed signature to the IPS sensor profile?

A. Traffic matching the signature will be allowed and logged.
B. The signature setting uses a custom rating threshold.
C. The signature setting includes a group of other signatures.
D. Traffic matching the signature will be silently dropped and logged.

Answer: A

Explanation:
The exhibit shows that the "FTP.Login.Failed" IPS signature is set with the action "Pass" and packet logging enabled. This means that any traffic matching this signature will be allowed through the FortiGate, and the traffic details will be logged for monitoring and analysis purposes.
References:

➢   FortiOS 7.4.1 Administration Guide: IPS Signature Actions

NEW QUESTION 8
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 9
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 10
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 10
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 14
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 19
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 22
Refer to the exhibits.

Network diagram
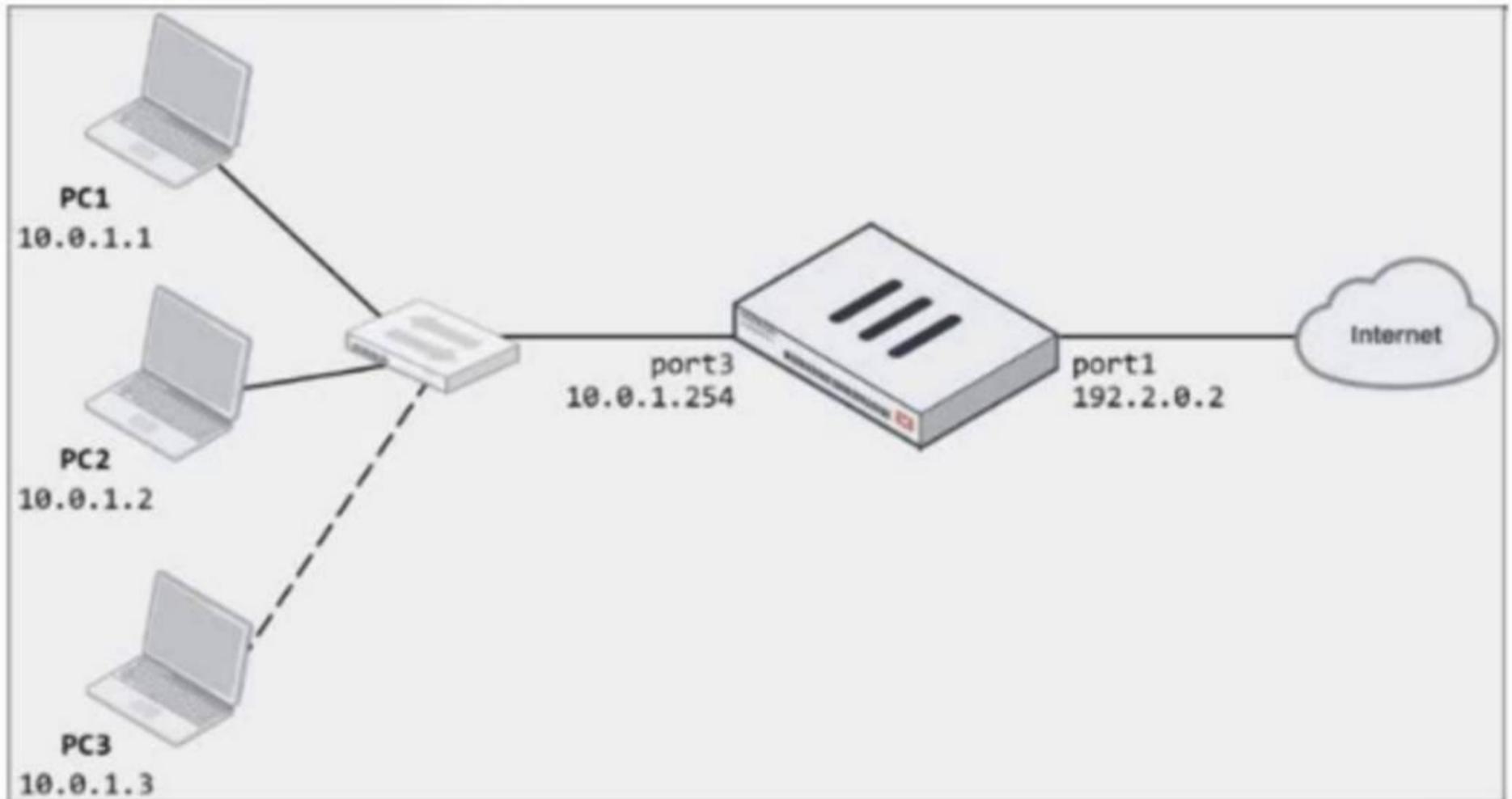
Dynamic IP pool

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 ℹ️	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 26
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 30
Refer to the exhibit to view the firewall policy.

Firewall policy configuration

Edit Policy

Name ℹ️	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 32
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 34
Refer to the exhibit.

FortiGate routing database

```
Local-FortiGate # get router info routing-table database
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
       > - selected route, * - FIB route, p - stale info


Routing table for VRF=0
S       0.0.0.0/0 [20/0] via 10.200.2.254, port2, [1/0]
S     *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
C     *> 10.0.1.0/24 is directly connected, port3
C     *> 10.200.1.0/24 is directly connected, port1
C     *> 10.200.2.0/24 is directly connected, port2
C     *> 172.16.100.0/24 is directly connected, port8
```

Which two statements are true about the routing entries in this database table? (Choose two.)

A. All of the entries in the routing database table are installed in the FortiGate routing table.
B. The port2 interface is marked as inactive.
C. Both default routes have different administrative distances.
D. The default route on porc2 is marked as the standby route.

Answer: CD

Explanation:
The routing table in the exhibit shows two default routes (0.0.0.0/0) with different administrative distances: ❯ The default route through port2 has an

administrative distance of 20.

❯   The default route through port1 has an administrative distance of 10.
Administrative distance determines the priority of the route; a lower value is preferred. Here, the route through port1 with an administrative distance of 10 is the preferred route. The route through port2 with an administrative distance of 20 acts as a standby or backup route. If the primary route (port1) fails or is unavailable, traffic will then be routed through port2.
Regarding the statement that the port2 interface is marked as inactive, there is no indication in the routing table that port2 is inactive. Similarly, all the routes displayed are not necessarily installed in the FortiGate routing table, as the table could include both active and backup routes.
References:

❯   FortiOS 7.4.1 Administration Guide: Default route configuration

❯   FortiOS 7.4.1 Administration Guide: Routing table

NEW QUESTION 39
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 44
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 47
Refer to the exhibits.

FortiGate HA cluster topology
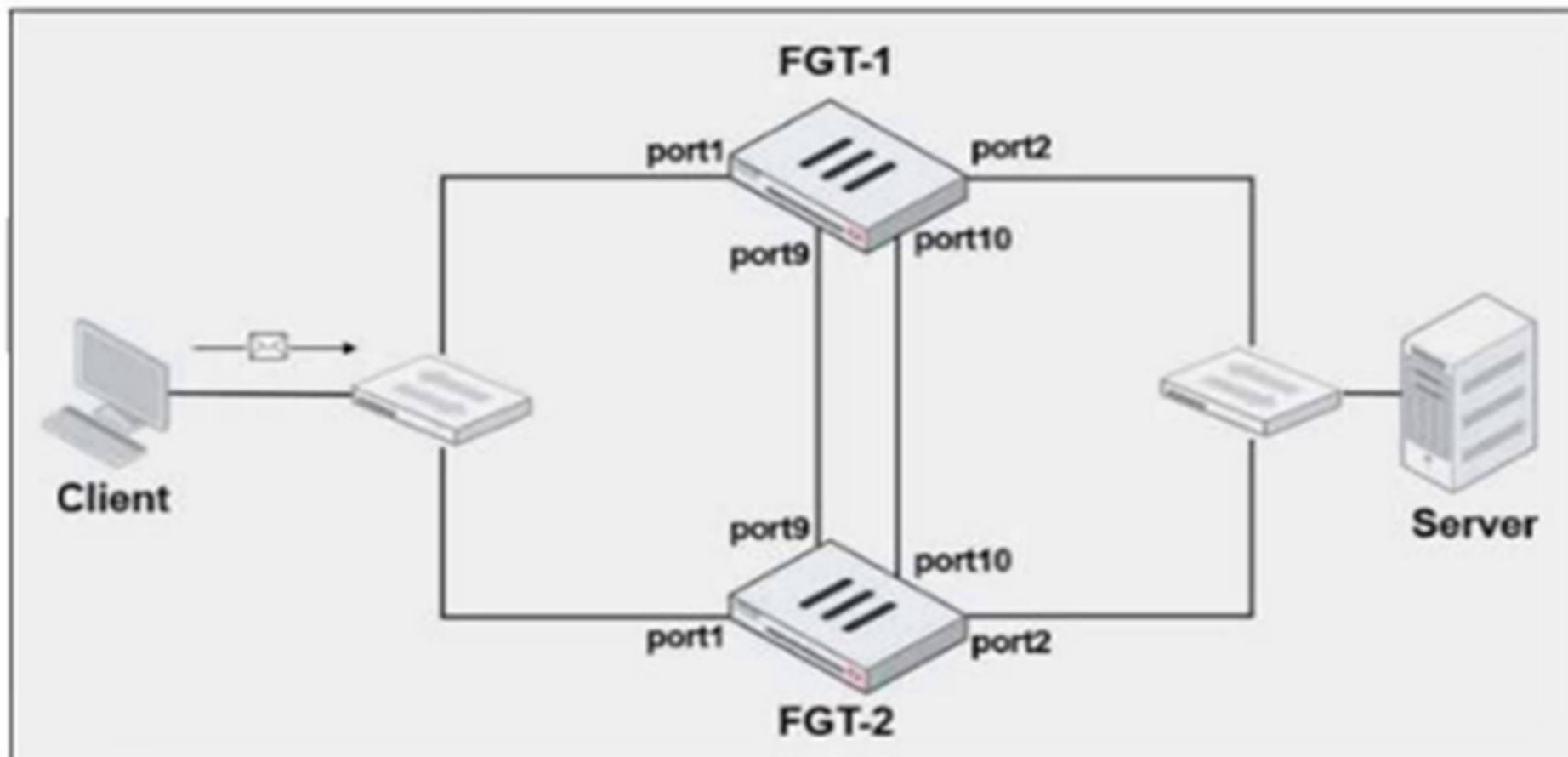
Current HA status

```
# get system ha status
...
Configuration Status:
    FGVM010000064692(updated 4 seconds ago): in-sync
    FGVM010000064692 chksum dump: 13 8b 52 c7 59 2a 9a 5c 5f
    FGVM010000065036(updated 4 seconds ago): in-sync
    FGVM010000065036 chksum dump: 13 8b 52 c7 59 2a 9a 5c 5f
...
Primary     : FGT-1, FGVM010000064692, HA cluster index = 1
Secondary   : FGT-2, FGVM010000065036, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000064692, HA operating index = 0
Secondary: FGVM010000065036, HA operating index = 1
```

New FortiGate HA configuration

```
FGT-1
#config system ha
    set group-id 3
    set group-name "Fortinet"
    set mode a-p
    set password *
    set hbdev "port9" 50 "port10" 50
    set session-pickup enable
    set override disable
    set priority 90
    set monitor port3

FGT-2
#config system ha
    set group-id 3
    set group-name "Fortinet"
    set mode a-p
    set password *
    set hbdev "port9" 50 "port10" 50
    set session-pickup enable
    set override enable
    set priority 110
    set monitor port3
```

FGT-1 and FGT-2 are updated with HA configuration commands shown in the exhibit.
What would be the expected outcome in the HA cluster?

A. FGT-1 will remain the primary because FGT-2 has lower priority.
B. FGT-2 will take over as the primary because it has the override enable setting and higher priority than FGT-1.
C. FGT-1 will synchronize the override disable setting with FGT-2.
D. The HA cluster will become out of sync because the override setting must match on all HA members.

Answer: B

NEW QUESTION 48
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
Which of the following methods can be used to configure FortiGate to perform source NAT (SNAT) for outgoing traffic?

A. Configure a static route pointing to the external interface.
B. Enable the "Use Outgoing Interface Address" option in a firewall policy.
C. Create a virtual server with an external IP address.
D. Deploy an IPsec VPN tunnel with NAT enabled.

Answer: B

Explanation:
To configure source NAT (SNAT) for outgoing traffic on FortiGate, one of the most common methods is to enable the "Use Outgoing Interface Address" option in a firewall policy. This option ensures that the source IP address of packets leaving the FortiGate device is replaced by the IP address of the outgoing interface. This is typically done when traffic is exiting a private network to access the internet, requiring source NAT to translate the private IP addresses to a public IP.
Why the other options are less appropriate:
* A. Configure a static route pointing to the external interface: A static route is used to direct traffic, but it does not configure SNAT. It determines where packets are sent but does not modify the source IP.
• C. Create a virtual server with an external IP address: Virtual servers are used to provide destination NAT (DNAT) for incoming traffic, not SNAT for outgoing traffic.
• D. Deploy an IPsec VPN tunnel with NAT enabled: While IPsec VPN tunnels can be configured with NAT traversal, this is not the typical method for configuring SNAT for general outgoing internet traffic.

NEW QUESTION 54
Refer to the exhibit.
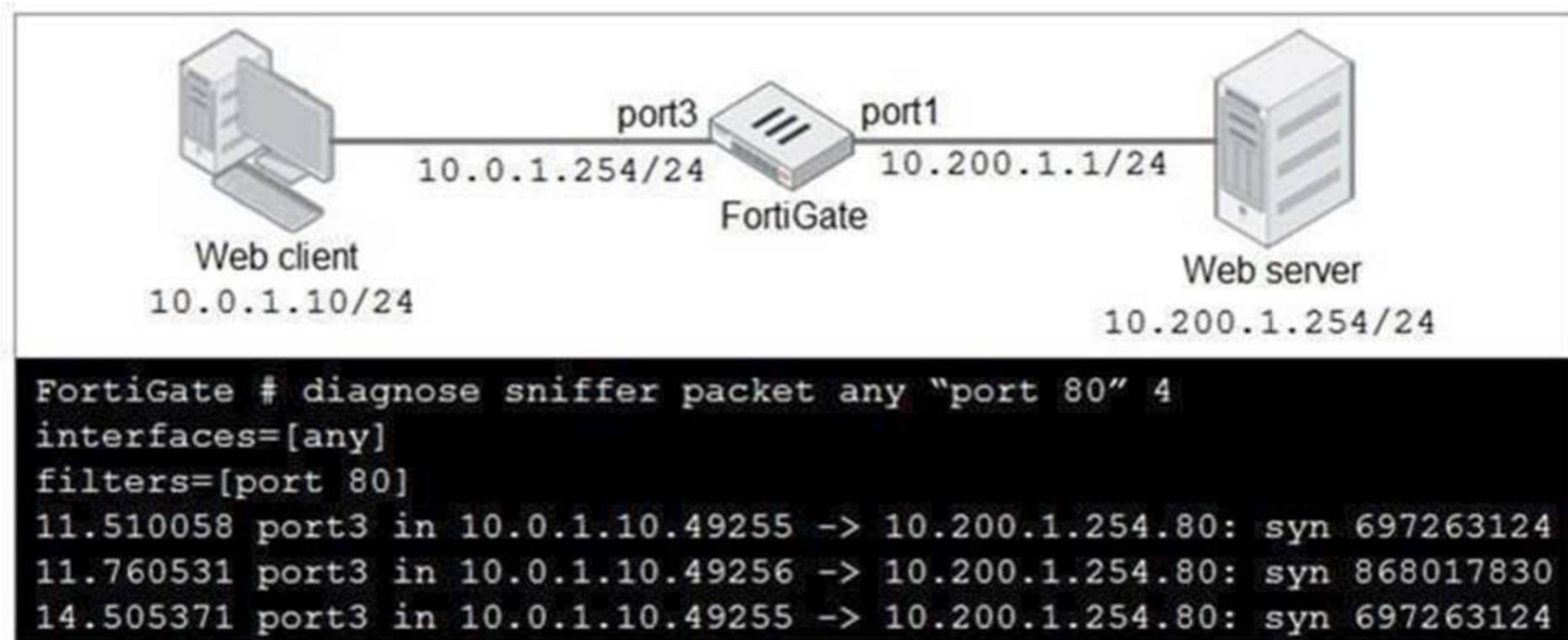
In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output as shown in the exhibit.
What should the administrator do next to troubleshoot the problem?

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 59
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 63
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 64
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCP_FGT_AD-7.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCP_FGT_AD-7.4 Product From:

https://www.2passeasy.com/dumps/FCP_FGT_AD-7.4/

Money Back Guarantee

FCP_FGT_AD-7.4 Practice Exam Features:

* FCP_FGT_AD-7.4 Questions and Answers Updated Frequently

* FCP_FGT_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FGT_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FGT_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year