QUESTION 1
What is the primary FortiGate election process when the HA override setting is enabled?

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

Answer: A
Explanation:
If Override DISABLED then: ports > HA Uptime > Priority > SN.
If Overrrid ENABLED then: ports > Priority > HA Uptime > SN.

QUESTION 2
An administrator wanted to configure an IPS sensor to block traffic that triggers a signature set number of times during a specific time period. How can the administrator achieve the objective?

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

Answer: D
Explanation:
You can also add rate-based signatures to block specific traffic when the threshold is exceeded. On the CLI, If you set the command rate-mode to periodical, FortiGate triggers the action when the threshold is reached during the configured Duration time period.

NEW QUESTION 3
A FortiGate firewall policy is configured with active authentication, however, the user cannot authenticate when accessing a website. Which protocol must FortiGate allow even though the user cannot authenticate?

A. LDAP
B. TACASC+
C. Kerberos
D. DNS

Answer: D
Explanation:
A firewall policy must allow a protocol in order to show the authentication dialog that is used in active authentication (such as HTTP/HTTPS/FTP/Telnet) and DNS.

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

Answer: D
Explanation:
The Fortinet-Group-Name attribute is used to restrict authentication to users who belong specifically to the "Training" user group on the RADIUS server.

NEW QUESTION 5
Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.

Based on the exhibit, which statement is true?

A. The Underlay zone is the zone by default.
B. The Underlay zone contains no member.
C. port2 and port3 are not assigned to a zone.
D. The virtual-wan-link and overlay zones can be deleted.

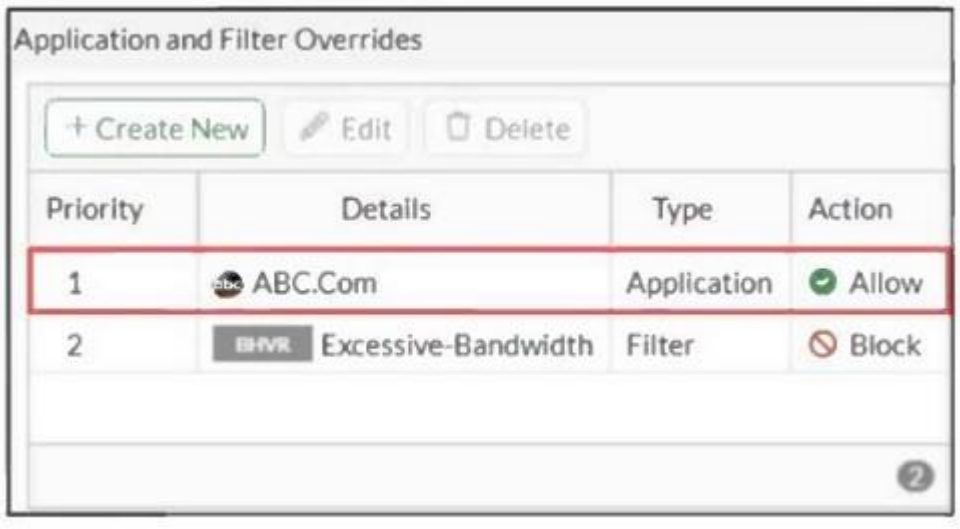
Answer: B
Explanation:
Underlay is not a default zone. It is user defined and not active.

NEW QUESTION 6
Which three statements explain a flow-based antivirus profile? (Choose three.)

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

Answer: ABD
Explanation:
Flow-based antivirus buffers the entire file while simultaneously transmitting data to the client to minimize latency.
Flow-based inspection combines multiple scanning techniques from proxy-based modes for efficient detection.
Flow-based inspection provides better performance by processing traffic on the fly without full proxy overhead.

NEW QUESTION 7
Refer to the exhibit. An administrator has configured an Application Overrides for the ABC.Com application signature and set the Action to Allow. This application control profile is then applied to a firewall policy that is scanning all outbound traffic. Logging is enabled in the firewall policy. To test the configuration, the administrator accessed the ABC.Com web site several times.



Why are there no logs generated under security logs for ABC.Com?

A. The ABC.Com Type is set as Application instead of Filter.
B. The ABC.Com is configured under application profile, which must be configured as a web filter profile.
C. The ABC.Com Action is set to Allow.
D. The ABC.Com is hitting the category Excessive-Bandwidth.

Answer: C
Explanation:
When the action is set to Allow in an application override, traffic matching this override is allowed without generating security logs because it bypasses deeper inspection and blocking.

NEW QUESTION 8
Which two statements describe characteristics of automation stitches? (Choose two.)

A. Actions involve only devices included in the Security Fabric.
B. An automation stitch can have multiple triggers.
C. Multiple actions can run in parallel.
D. Triggers can involve external connectors.

Answer: CD
Explanation:
Automation stitches can execute multiple actions concurrently (in parallel).
Triggers for automation stitches can come from external connectors beyond just Fortinet devices.

NEW QUESTION 9
Which three statements about SD-WAN performance SLAs are true? (Choose three.)

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

Answer: BCE
Explanation:
FortiGate performance SLAs monitor the state of each member—whether it is alive or dead—and measures the member packet loss, latency, and jitter.
When you configure a performance SLA, you can decide whether you want to monitor the link health actively or passively. In active monitoring, the performance SLA checks the health of the member periodically—by default every 500ms— sending probes from the member to one or two servers that act as a beacon. In passive monitoring, the performance SLA determines the health of a member based on the traffic passing through the member.
The SLA target section is optional. It's where you define the performance requirements of alive members (latency, jitter, and packet loss thresholds). The performance SLA uses SLA targets with some SD-WAN rule strategies, like Lowest Cost (SLA), to decide if the link is eligible for traffic steering or not.

NEW QUESTION 10
Which two statements are true about an HA cluster? (Choose two.)

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

Answer: BD
Explanation:
Incremental synchronization also synchronizes other dynamic configuration information such as the DHCP server address lease database, routing table updates, IPsec SAs, MAC address tables, and so on.
HA propagates more than just configuration details. Some runtime data, such as DHCP leases and FIB entries, are also synchronized.

NEW QUESTION 11
Refer to the exhibit. An administrator has created a new firewall address to use as the destination for a static route. Why is the administrator not able to select the new address in the Destination field of the new static route?

A. In the new static route, the administrator must select Named Address.
B. In the new firewall address, the FQDN address must first beresolved.
C. In the new static route, the administrator must first set the interface to port2.
D. In the new firewall address, Routing configuration must be enabled.

Answer: D
Explanation:
To use an FQDN-based address object as a destination in a static route, the "Routing configuration" option must be enabled in the firewall address settings. Without this, the address cannot be selected for routing.

NEW QUESTION 12
FortiGate is operating in NAT mode and has two physical interfaces connected to the LAN and DMZ networks respectively.
Which two statements about the requirements of connected physical interfaces on FortiGate are true? (Choose two.)

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

Answer: BD
Explanation:
In NAT mode, FortiGate routes packets based on layer 3, like a router. Each of its logical network interfaces has an IP address, and FortiGate determines the outgoing or egress interface based on the destination IP address and entries in its routing tables.

NEW QUESTION 13
When configuring a FortiGate in a multi-WAN setup, why would an administrator enable session preservation on an interface?

A. To allow the FortiGate to dynamically change interfaces for all active sessions when a WAN link fails
B. To make sure all sessions without source NAT enabled always use the primary WAN link
C. To improve security by forcing users to authenticate again when the WAN link changes
D. To ensure that existing SSL VPN connections remain on the same interface even if route changes occur

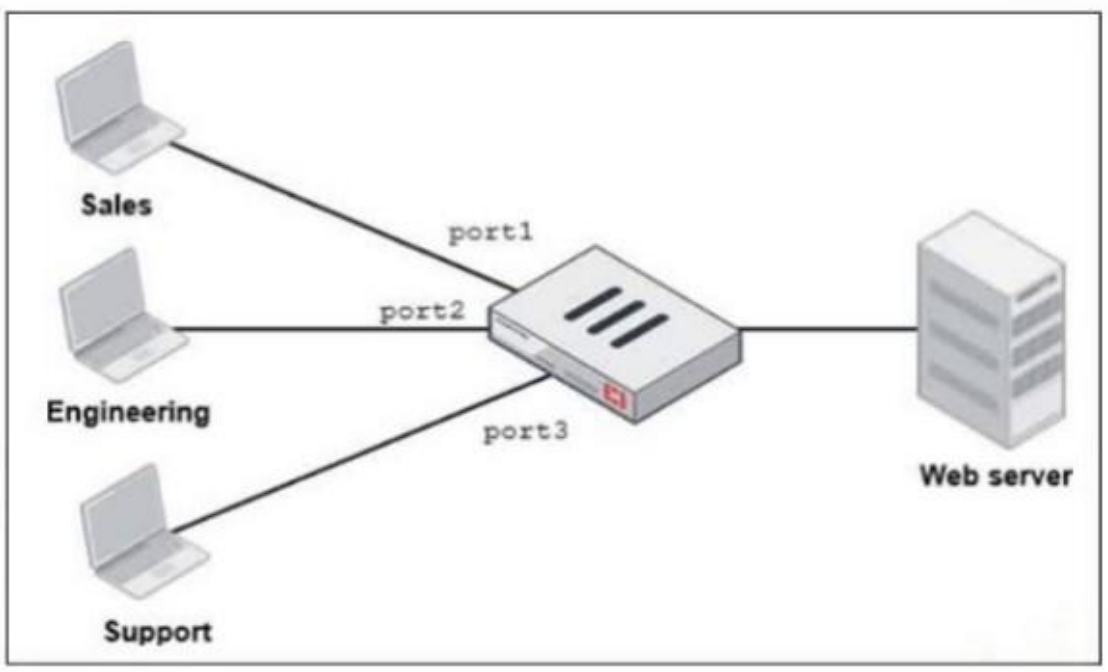
Answer: D
Explanation:
Session preservation keeps active sessions, such as SSL VPNs, tied to the original interface to prevent disruption when WAN routes change.

NEW QUESTION 14
You are analyzing connectivity problems caused by intermediate devices blocking traffic in SSL VPN environment.
In which two ways can you effectively resolve the problem? (Choose two.)

A. You can turn off IKE fragmentation to fix large certificate negotiation problems.
B. You should use IPsec to solve issues with fragment drops and large certificate exchanges.
C. You can use SSL VPN tunnel mode to prevent problems with blocked ESP and UDP ports (500 or 4500).
D. You can configure a hub-and-spoke topology with SSL VPN tunnels to bypass blocked UDP ports.

Answer: CD
Explanation:
The training is basically trying to point out the advantage of FortiGate's SSL VPN over IPSec VPN in situation where issues are caused by an intermediate device.
IPsec uses ESP and UDP 500 and 4500, so where these are blocked, SSL VPN tunnel mode shines because it uses HTTPS (443) and TLS by default (both TCP).
Again where UDP ports are blocked, SSL VPN shines (Tunnel mode Hub and Spoke) because it does not use UDP.

NEW QUESTION 15
Refer to the exhibit. FortiGate has two separate firewall policies for Sales and Engineering to access the same web server with the same security profiles.
Which action must the administrator perform to consolidate the two policies into one?



A. Create an Aggregate interface that includes port1 and port2 to create a single firewall policy.
B. Select port1 and port2 subnets in a single firewall policy.
C. Replace port1 and port2 with the any interface in a single firewall policy.
D. Enable Multiple Interface Policies to select port1 and port2 in the same firewall policy.

Answer: D
Explanation:

Enabling Multiple Interface Policies allows you to select multiple interfaces (like port1 and port2) in a single firewall policy, consolidating access rules for both Sales and Engineering to the web server.

NEW QUESTION 16
You have configured an application control profile, set peer-to-peer traffic to Block under the Categories tab, and applied it to the firewall policy. However, your peer-to-peer traffic on known ports is passing through the FortiGate without being blocked. What FortiGate settings should you check to resolve this issue?

A. FortiGuard category ratings
B. Application and Filter Overrides
C. Network Protocol Enforcement
D. Replacement Messages for UDP-based Applications

Answer: C
Explanation:
Network Protocol Enforcement:
- Ensures that traffic on a specific port matches the expected protocol.
- Enabling it forces FortiGate to examine payloads even on known ports.

NEW QUESTION 17
When configuring firewall policies which of the following is true regarding the policy ID? (Choose two.)

A. It is mandatory to provide a policy ID while creating a firewall policy regardless of GUI or CLI.
B. A firewall policy ID identifies the order of policy execution in firewall policies.
C. You can create a policy in CLI with policy ID 0.
D. A policy ID cannot be modified once a policy is created.

Answer: AD
Explanation:
The policy ID assigned to a firewall policy cannot be modified after creation. When creating a policy via CLI, you can specify policy ID 0, which the system allows. The policy ID does not determine the order of execution; policy sequence in the list determines execution order.

NEW QUESTION 18
Which two statements are correct when FortiGate enters conserve mode? (Choose two.)

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

Answer: BD
Explanation:
It does not accept config changes, because it might increase memory usage even further. It explicitly does NOT run any quarantine actions. You can configure IPS fail-open to control how IPS behaves when the IPS socket buffer is full.

NEW QUESTION 19
A remote user reports slow SSL VPN performance and frequent disconnections. The user is located in an area with poor internet connectivity.
What setting should the administrator adjust to improve the user's experience?

A. Enable split tunneling to reduce VPN traffic.
B. Change the SSL VPN port to a non-standard port.
C. Increase the session timeout for inactive sessions.
D. Configure the DTLS timeout to accommodate high-latency connections.

Answer: D
Explanation:
Adjusting the DTLS timeout helps maintain SSL VPN stability and performance in environments with poor or high-latency internet connectivity by allowing more time for packet retransmissions before dropping the connection.

NEW QUESTION 20
An administrator wants to analyze and manage digital certificates to prevent browser warnings when users connect to the SSL VPN portal.
Which two statements describe how to correctly do this? (Choose two.)

A. The administrator can rely on the default FortiGate self-signed certificate to prevent all security warnings in the browser.
B. The administrator must disable HTTPS administrative access entirely to avoid certificate warnings.
C. The administrator can use a publicly trusted certificate from a known certificate authority (CA) to stop browser warnings.
D. The administrator can import the FortiGate self-signed certificate into each user's browser as a trusted certificate.

Answer: CD
Explanation:
Using a publicly trusted certificate from a known CA prevents browser warnings without additional user action.
Importing the FortiGate self-signed certificate into users' browsers as trusted eliminates warnings caused by untrusted certificates.

NEW QUESTION 21
An administrator suspects that the Collector Agent is not forwarding login events to FortiGate.
What is the most effective troubleshooting step?

A. Verify if DC agent is enabled on the FortiGate.
B. Restart the domain controller to refresh authentication services.

C. Verify if FortiGate is set to use LDAP authentication instead of FSSO.
D. Check if TCP port 8000 is open between the collector agent and FortiGate.

Answer: D
Explanation:
The Collector Agent communicates with FortiGate over TCP port 8000. Ensuring this port is open and reachable is essential for forwarding login events.

NEW QUESTION 22
Refer to the exhibit. A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up, but phase 2 fails to come up.

Based on the phase 2 configuration shown in the exhibit, which two configuration changes will bring phase 2 up? (Choose two.)

A. On BR1-FGT, set Seconds to 43200.
B. On HQ-NGFW, enable Diffie-Hellman Group 2.
C. On BR1-FGT, set Remote Address to 10.0.11.0/255.255.255.0.
D. On HQ-NGFW, set Encryption to AES256.

Answer: CD
Explanation:
Check the IP address
The remote subnet selectors don’t match. Set BR1-FGT’s Remote Address to 10.0.11.0/255.255.255.0 (C).
The phase-2 proposal algorithms don’t match. Change HQ-NGFW Encryption from AES128 to AES256 to match BR1-FGT (D).

NEW QUESTION 23
Refer to the exhibits. An administrator has observed the performance status outputs on an HA cluster for 55 seconds.

HA configuration

```
HQ-NGFW-1 # config system ha

HQ-NGFW-1 (ha) # show
config system ha
    set group-id 5
    set group-name "Training"
    set mode a-p
    set password ENC a4fbyqY4iPexFmAnZgzDY
    set hbdev "port7" 0
    set session-pickup enable
    set override disable
    set priority 200
    set monitor "port1"
    set memory-based-failover enable
    set memory-failover-threshold 70
    set memory-failover-monitor-period 50
    set memory-failover-sample-rate 10
    set memory-failover-flip-timeout 60
end
```

HQ-NGFW-1 System Performance output

```
HQ-NGFW-1 # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87 kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

HQ-NGFW-2 System Performance output

```
HQ-NGFW-2 # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 993836k used (48.7%), 690352k free (33.8%), 357888k freeable (17.5%)
Average network usage: 26/18 kbps in 1 minute, 25/18 kbps in 10 minutes, 24/18 kbps in 30 minutes
Maximal network usage: 91/27 kbps in 1 minute, 92/27 kbps in 10 minutes, 92/32 kbps in 30 minutes
Average sessions: 9 sessions in 1 minute, 9 sessions in 10 minutes, 9 sessions in 30 minutes
Maximal sessions: 11 sessions in 1 minute, 11 sessions in 10 minutes, 13 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 10 hours, 50 minutes
```

Which FortiGate is the primary?

A. HQ-NGFW-2 with the parameter memory-failover-threshold setting
B. HQ-NGFW-2 with the parameter priority setting
C. HQ-NGFW-1 with the parameter memory-failover-flip-timeout setting
D. HQ-NGFW-1 with the parameter override setting

Answer: A
Explanation:
The configured memory failover threshold is 70%, and FW-1 is running at 90%. The monitored period is set to 50 seconds, while the NEW QUESTION states that the admin observed the output for 55 seconds. This means FW-1 has remained above the 70% threshold for more than the configured monitoring period, while the memory usage on FW-2 is below 70%.

NEW QUESTION 24
Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

A. The collector agent uses a Windows API to query DCs for user logins.
B. NetAPI polling can increase bandwidth usage in large networks.
C. The NetSessionEnum function is used to track user logouts.
D. The collector agent must search Windows application event logs.

Answer: C
Explanation:
NetAPI: polls temporary sessions created on the DC when a user logs in or logs out and calls the NetSessionEnum function on Windows. It's faster than the WinSec and WMI methods; however, it can miss some login events if a DC is under heavy system load. This is because sessions can be quickly created and purged from RAM, before the agent has a chance to poll and notify FortiGate.

NEW QUESTION 25
You have configured the FortiGate device for FSSO. A user is successful in log-in to windows, but their access to the internet is denied. What should the administrator check first?

A. Whether the user is assigned to the correct AD group.
B. The FortiGate firewall policy settings for SSL decryption.
C. The FortiGate FSSO active users list for user's IP address.
D. The windows event viewer for failed login attempts.

Answer: C
Explanation:
Checking the active users list verifies if FortiGate correctly associates the user with their IP address, ensuring proper policy enforcement for internet access.

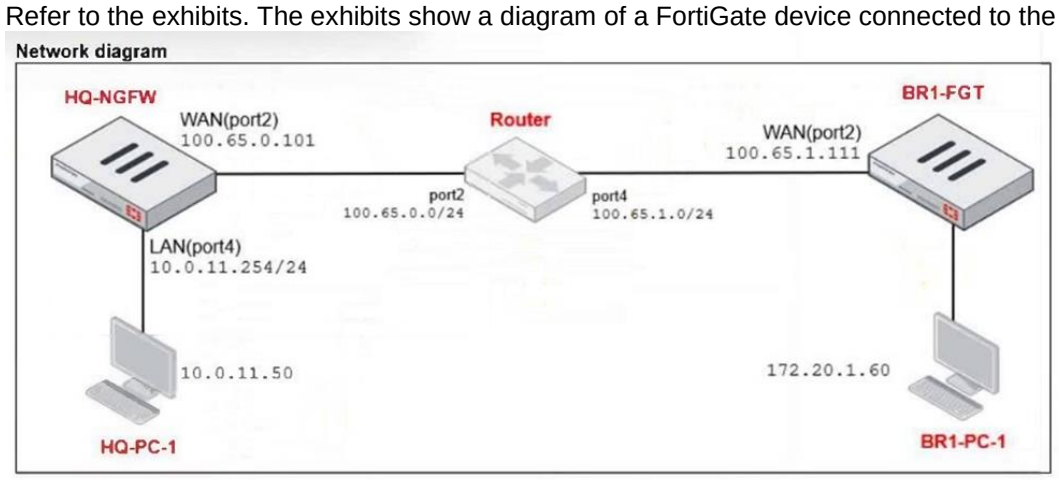
NEW QUESTION 26
What are three key routing principles in SD-WAN? (Choose three.)

A. By default. SD-WAN rules are skipped if the included SD-WAN members do not have a valid route to the destination.
B. SD-WAN rules have precedence over any other type of routes.
C. Regular policy routes have precedence over SD-WAN rules.
D. By default. SD-WAN rules are skipped if only one route to the destination is available.
E. By default. SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.

Answer: ACE
Explanation:
SD-WAN rules are matched only if the best route to the destination points to SD-WAN
SD-WAN member is selected only if it has a route to the destination
https://docs.fortinet.com/document/fortigate/7.0.0/sd-wan-sd-branch-architecture-for-mssps/768108/sd-wan-routing-logic
SDWAN rules are 'policy routes', but regular policy routes have precedence over SD-WAN rules.
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Explaining-the-SD-WAN-rule-matching-process/ta-p/284325

NEW QUESTION 27
Refer to the exhibits. The exhibits show a diagram of a FortiGate device connected to the network, as well as the IP pool configuration and firewall policy objects.

Network diagram



NAT IP pool configuration

Name	External IP Range	Type	ARP Reply
SNAT-Pool	100.65.0.49 - 100.65.0.49	Overload	Enabled
SNAT-Remote	100.65.0.149 - 100.65.0.149	Overload	Enabled
SNAT-Remote1	100.65.0.99 - 100.65.0.99	Overload	Enabled

Firewall policies

Policy	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN (port4) → WAN (port2) 3							
TCP traffic (2)	all	BR1-FGT	always	ALL_TCP	ACCEPT	SNAT-Pool	NAT
PING traffic (3)	all	all	always	PING	ACCEPT	SNAT-Remote1	NAT
IGMP traffic (4)	all	all	always	IGMP	ACCEPT	SNAT-Remote	NAT

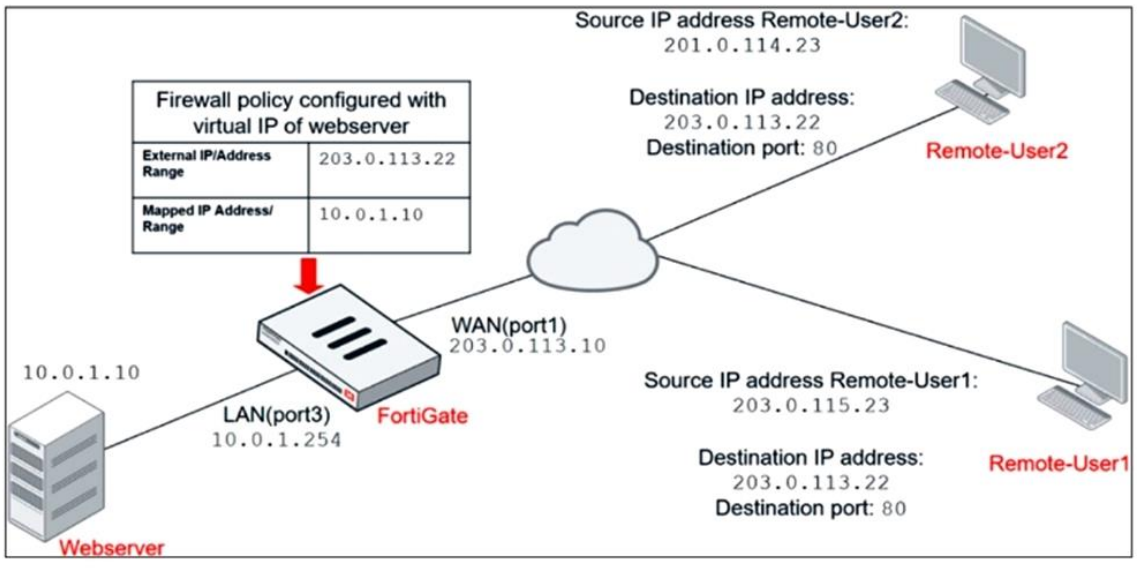
The WAN (port2) interface has the IP address 100.65.0.101/24. The LAN (port4) interface has the IP address 10.0.11.254/24. Which IP address will be used to source NAT (SNAT) the traffic, if the user on HQ-PC-1 (10.0.11.50) pings the IP address of BR-FGT (100.65.1.111)

A. 100.65.0.101
B. 100.65.0.49
C. 100.65.0.99
D. 100.65.0.149

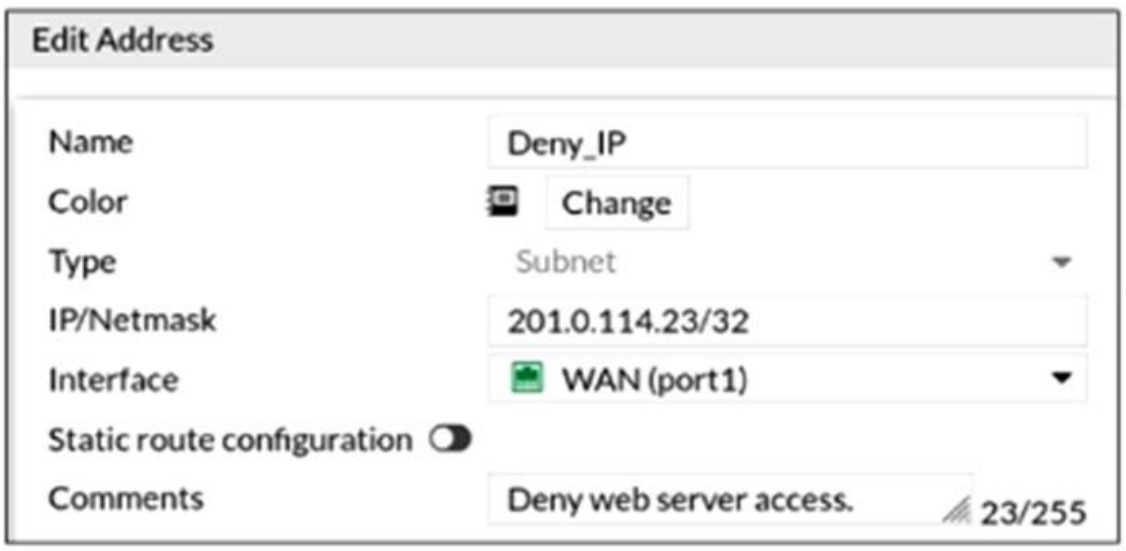
Answer: C
Explanation:
The ping traffic policy uses the IP pool named SNAT-Remote1, which has the external IP range 100.65.0.99. Therefore, traffic matching this policy (ping from HQ-PC-1 to BR1-FGT) will use 100.65.0.99 for source NAT.

NEW QUESTION 28
Refer to the exhibits. The exhibits show a diagram of a FortiGate device connected to the network, and the firewall configuration.

Network diagram



Firewall address object



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

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 additional configuration can the administrator add to a deny firewall policy, beyond the default behavior, to block Remote-User2 from accessing the Webserver?

A. Disable match-vip in the Allow_access policy
B. Configure a One-to-One IP Pool object in a new policy.
C. Set the Destination address as Webserver in the Deny policy.
D. Set the Destination address as Deny_IP in the Allow_access policy.

Answer: C
Explanation:
To block Remote-User2's access to the Webserver, the deny policy must explicitly specify the Webserver as the destination address; otherwise, it denies traffic to all destinations, which is not the desired behavior.

NEW QUESTION 29
Refer to the exhibits. The exhibits show the system performance output and default configuration of high memory usage thresholds on a FortiGate device.

System Performance output

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87 kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

Memory usage threshold settings

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

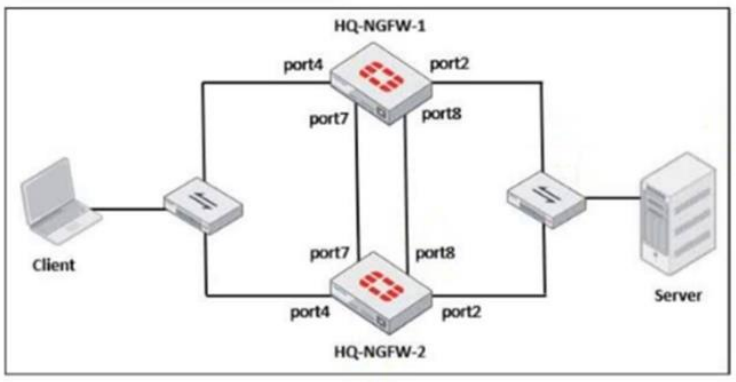
Based on the system performance output, what are the two possible outcomes? (Choose two.)

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

Answer: AD
Explanation:
FG enters conserve mode at 88% by default, at which point you can't make configuration changes. Also, without additional config, FG will drop sessions that require inspection. At 95%, all new sessions are dropped.

NEW QUESTION 30
Refer to the exhibits. Based on the current HA status, an administrator updates the override and priority parameters on HQ-NGFW-1 and HQ-NGFW-2 as shown in the exhibit.

FortiGate HA cluster topology



Current HA status

```
HQ-NGFW-1 # get system ha status
...
Configuration Status:
    FGVM02TM24013423(updated 0 seconds ago): in-sync
    FGVM02TM24013423 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
    FGVM02TM24013501(updated 4 seconds ago): in-sync
    FGVM02TM24013501 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
...
number of member: 2
HQ-NGFW-1       , FGVM02TM24013423, HA cluster index = 1
HQ-NGFW-2       , FGVM02TM24013501, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM02TM24013423, HA operating index = 0
Secondary: FGVM02TM24013501, HA operating index = 1
```

New FortiGate HA configuration

```
HQ-NGFW-1
# config system ha
     set group-id 5
     set group-name "Fortinet"
     set mode a-p
     set password *
     set hbdev "port7" 50 "port8" 60
     set session-pick enable
     set override disable
     set priority 90
     set monitor "port3"


HQ-NGFW-2
# config system ha
     set group-id 5
     set group-name "Fortinet"
     set mode a-p
     set password *
     set hbdev "port7" 50 "port8" 60
     set session-pick enable
     set override enable
     set priority 110
     set monitor "port3"
```

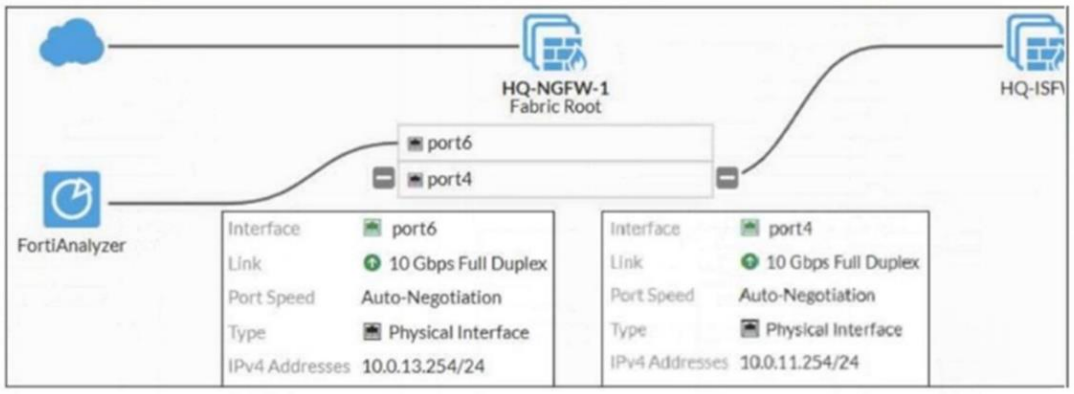
What would be the expected outcome in the HA cluster?

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

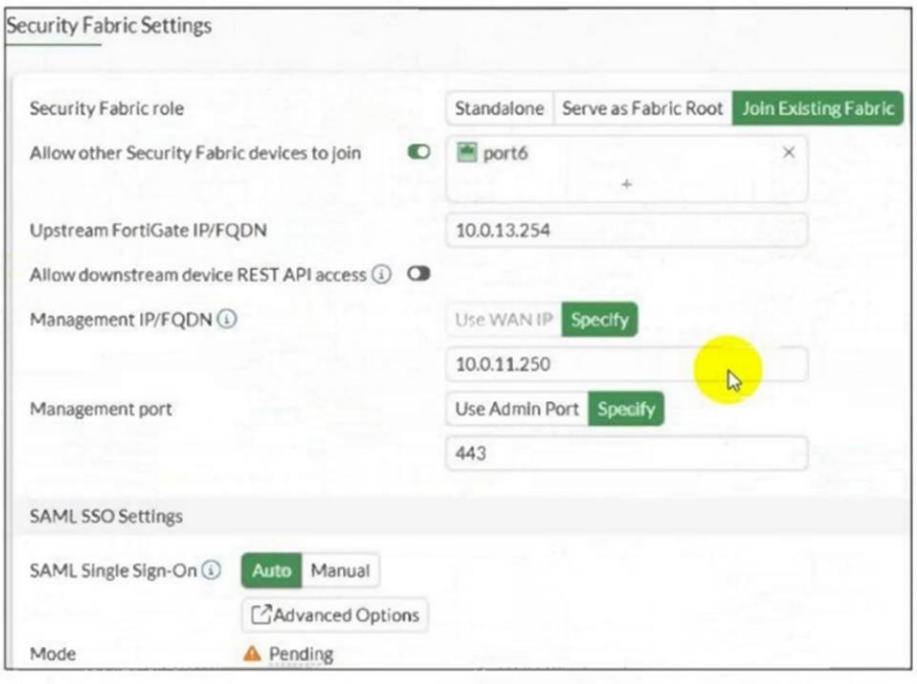
Answer: B
Explanation:
With override enabled on HQ-NGFW-2 and its higher priority (110 vs. 90), HQ-NGFW-2 will become the primary device, preempting HQ-NGFW-1 despite the current primary status.

NEW QUESTION 31
Refer to the exhibits. An administrator wants to add HQ-ISFW-2 in the Security Fabric. HQ-ISFW-2 is in the same subnet as HQ-ISFW. After configuring the Security Fabric settings on HQ-ISFW-2, the status stays Pending.

Security Fabric logical topology view



Security Fabric settings on HQ-ISFW-2



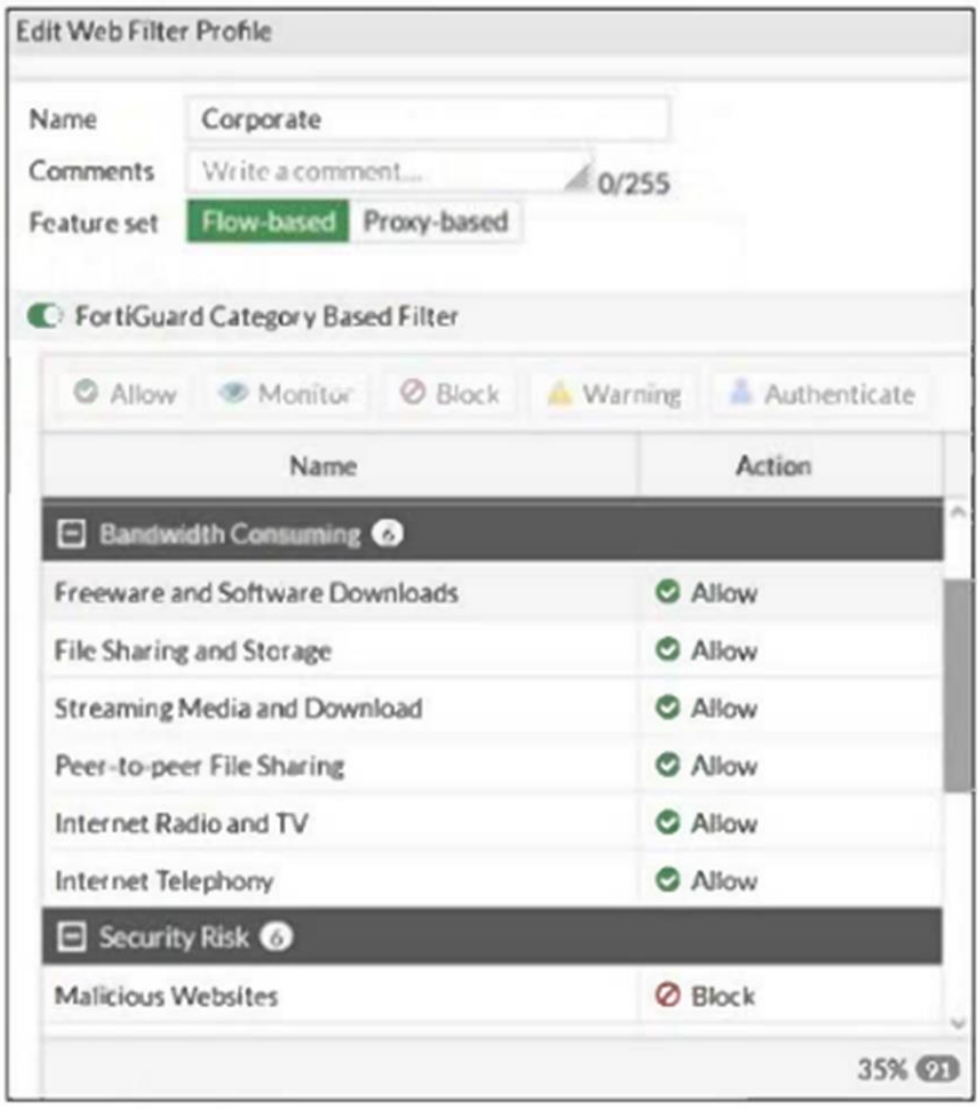
What can be the two possible reasons? (Choose two.)

A. Upstream FortiGate IP must be set to 10.0.11.254.
B. SAML Single Sign-On must be set to Manual.
C. HQ-ISFW-2 must be authorized on HQ-ISFW.
D. Management IP must be set to 10.0.13.254.

Answer: AC
Explanation:
The Upstream FortiGate IP should match the IP address of the Fabric Root interface, which is 10.0.11.254, not 10.0.13.254.
The new device (HQ-ISFW-2) must be authorized on the Fabric Root (HQ-ISFW) before it can join the Security Fabric, otherwise the status remains pending.

NEW QUESTION 32
Refer to the exhibit. The exhibit shows the FortiGuard Category Based Filter section of a corporate web filter profile.

FortiGate web filter profile configuration



An administrator must block access to download.com, which belongs to the Freeware and Software Downloads category. The administrator must also allow other websites in the same category.
What are two solutions for satisfying the requirement? (Choose two.)

A. Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.
B. Configure a web override rating for download.com and select Malicious Websites as the subcategory.
C. Configure a separate firewall policy with action Deny and an FQDN address object for*.download.com as destination address.
D. Set the Freeware and Software Downloads category Action to Warning.

Answer: AB
Explanation:
You can create a web rating override to change the website category to someone that is blocked in the web filter profile
You can enable the URL Filter in the Web Filter Profile and block the website.

NEW QUESTION 33
An administrator wants to configure dead peer detection (DPD) on IPsec VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when there is no inbound traffic.
Which DPD mode on FortiGate meets this requirement?

A. Enabled
B. On Idle
C. Disabled
D. On Demand

Answer: D
Explanation:
Disable: Disable Dead Peer Detection.
On-idle: Trigger Dead Peer Detection when no IPsec traffic is received.
On-demand: Trigger Dead Peer Detection when no IPsec traffic is received AND FortiGate has been sending IPsec traffic. On-demand is the default setting.

NEW QUESTION 34
Which two statements about equal-cost multi-path (ECMP) configuration on FortiGate are true? (Choose two.)

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

Answer: CD
Explanation:

SD-WAN is enabled: v4-ecmp-mode is hide and you control the ECMP algorithm with the load-balance-mode setting.
SD-WAN is disabled: ECMP algorithm is set on the CLI: config system settings.
https://docs.fortinet.com/document/fortigate/7.4.6/administration-guide/25967/equal-cost-multi-path

NEW QUESTION 35
You have created a web filter profile named restrict_media-profile with a daily category usage quota. When you are adding the profile to the firewall policy, the restrict_media-profile is not listed in the available web profile drop down.
What could be the reason?

A. The firewall policy is in no-inspection mode instead of deep-inspection.
B. The inspection mode in the firewall policy is not matching with web filter profile feature set.
C. The web filter profile is already referenced in another firewall policy.
D. The naming convention used in the web filter profile is restricting it in the firewall policy.

Answer: B
Explanation:
Web filter profiles with category usage quotas require the firewall policy to be in proxy-based (deep) inspection mode; if the inspection mode does not match this requirement, the profile will not appear in the drop-down list.

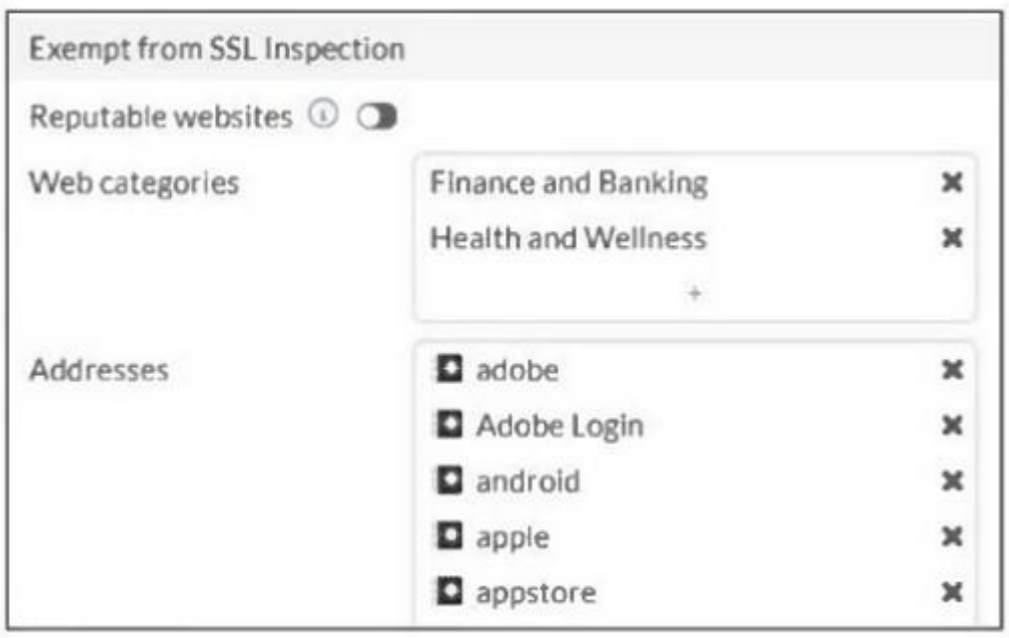
NEW QUESTION 36
Refer to the exhibit. As an administrator you have created an IPS profile, but it is not performing as expected. While testing you got the output as shown in the exhibit.
What could be the possible reason of the diagnose output shown in the exhibit?

```
HQ-NGFW-1 # diagnose test application ipsmonitor 1
            pid = 2044, engine count = 0 (+1)
            0 - pid:2074:2074 cfg:1 master:0 run:1
```

A. There is a no firewall policy configured with an IPS security profile.
B. FortiGate entered into IPS fail open state.
C. Administrator entered the command diagnose test application ipsmonitor 5.
D. Administrator entered the command diagnose test application ipsmonitor 99.

Answer: A
Explanation:
The output shows the IPS engine count as 0, indicating no active IPS engines are running. This typically means no firewall policy is referencing the IPS security profile, so the IPS profile is not being applied or triggered.

NEW QUESTION 37
Refer to the exhibit. The predefined deep-inspection and custom-deep-inspection profiles exclude some web categories from SSL inspection, as shown in the exhibit.
For which two reasons are these web categories exempted? (Choose two.)



A. The FortiGate temporary certificate denies the browser's access to websites that use HTTP Strict Transport Security.
B. These websites are in an allowlist of reputable domain names maintained by FortiGuard.
C. The resources utilization is optimized because these websites are in the trusted domain list on FortiGate.
D. The legal regulation aims to prioritize user privacy and protect sensitive information for these websites.

Answer: AD
Explanation:
FortiGate's temporary SSL certificate may cause access denial to sites using HTTP Strict Transport Security (HSTS), so such sites are exempted from deep SSL inspection.
Legal regulations require exemption of certain categories to protect user privacy and sensitive
information, so these web categories are excluded from SSL inspection.

NEW QUESTION 38
Refer to the exhibit. The NOC team connects to the FortiGate GUI with the NOC_Access admin profile. They request that their GUI sessions do not disconnect too early during inactivity. What must the administrator configure to answer this specific request from the NOC team?

Profile Name
Monitoring_Access
NOC_Access
prof_admin
super_admin

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

Answer: B
Explanation:
You can override the idle timeout setting per administartor profile using the Override Idle Timeout setting.
You can configure an administrator profile to increase inactivity timeout and facilitate use of the GUI for central monitoring. Then Override Idel Timeout setting allows the admintimeout value, under the config system accprofile, to be overridden per access profile.

NEW QUESTION 39
Refer to the exhibit. Based on this partial configuration, what are the two possible outcomes when FortiGate enters conserve mode? (Choose two.)

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

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

Answer: AB
Explanation:
System configuration cannot be changed because of the IPS Global configuration "fail-open enabled"
FortiGate skips quarantine actions - again because of the IPS Global configuration "fail-open enabled"

NEW QUESTION 40
A network administrator enabled antivirus and selected an SSL inspection profile on a firewall policy. When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and does not block the file, allowing it to be downloaded.
The administrator confirms that the traffic matches the configured firewall policy. What are two reasons for the failed virus detection by FortiGate? (Choose two.)

A. The selected SSL inspection profile has certificate inspection enabled.
B. The website is exempted from SSL inspection.
C. The El CAR test file exceeds the protocol options oversize limit.
D. The browser does not trust the FortiGate self-signed CA certificate.

Answer: AB
Explanation:
Certificate inspection is not deep ssl inspection hence no inspection of the packet would happen since it is encrypted.
If the https site is in exampted list then yes it is a valid reason.

NEW QUESTION 41
You have configured the below commands on a FortiGate.

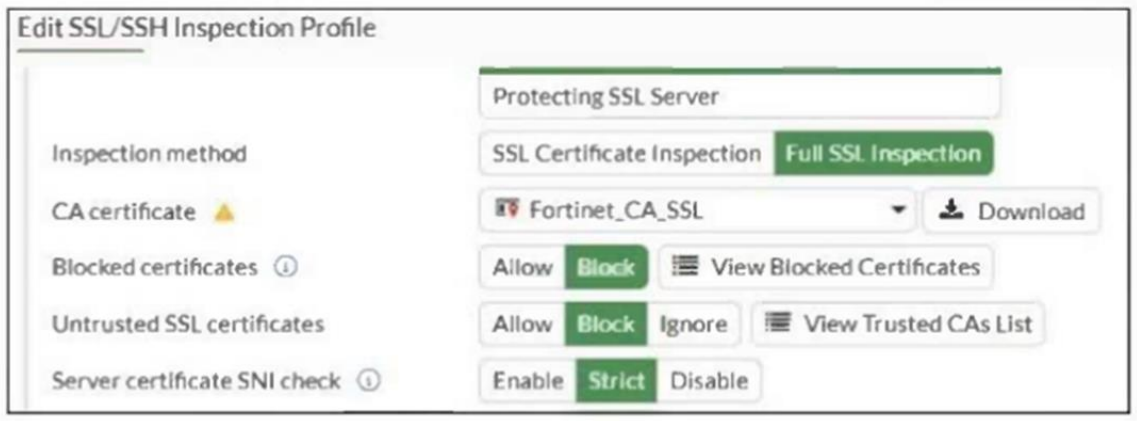
```
config system settings
set strict-src-check enable
end

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

What would be the impact of this configuration on FortiGate?

A. FortiGate will enable strict RPF on ail its interfaces and port1 will be enable for asymmetric routing.
B. FortiGate will enable strict RPF on all its interfaces and port1 will be exempted from RPF checks.
C. Port1 will be enabled with flexible RPF, and all other interfaces will be enabled for strict RPF
D. The global configuration will take precedence and FortiGate will enable strict RPF on all interfaces.

Answer: B
Explanation:
The global setting enables strict source checking (RPF) on all interfaces by default. The per-interface setting disables the source check on port1, exempting it from strict RPF enforcement.

NEW QUESTION 42
Refer to the exhibit. What would be the impact of these settings on the Server certificate SNI check configuration on FortiGate?



A. FortiGate will accept and use the CN in the server certificate for URL filtering if the SNI does not match the CN or SAN fields.
B. FortiGate will accept the connection with a warning if the SNI does not match the CN or SAN fields.
C. FortiGate will close the connection if the SNI does not match the CN or SAN fields.
D. FortiGate will close the connection if the SNI does not match the CN and SAN fields

Answer: C
Explanation:
SNI-server-cert-check
Enable: Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.
Strict: Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.
Disable: Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.

NEW QUESTION 43
A new administrator is configuring FSSO authentication on FortiGate using DC Agent Mode.
Which step is NOT part of the expected process?

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

Answer: A
Explanation:
In DC Agent mode, the DC agent installed on the Domain Controller captures the logon events (e.g., Event ID 4624) in real-time. It then pushes this information to the Collector Agent. The Collector Agent, which runs as a service on a dedicated machine, is responsible for consolidating this information and then forwarding it to the FortiGate firewall. The FortiGate receives this data and uses the user's IP address to apply appropriate security policies.

NEW QUESTION 44
A network administrator is reviewing firewall policies in both Interface Pair View and By Sequence View. The policies appear in a different order in each view.
Why is the policy order different in these two views?

A. Policies in Interface Pair View are prioritized by security levels, while By Sequence View strictly follows the administrator's manual ordering.
B. By Sequence View groups policies based on rule priority, while Interface Pair View always follows the order of traffic logs.
C. The firewall dynamically reorders policies in Interface Pair View based on recent traffic patterns, but By Sequence View remains static.
D. Interface Pair View sorts policies based on matching interfaces, while By Sequence View shows the actual processing order of rules.

Answer: D
Explanation:
Interface Pair View organizes policies grouped by source and destination interfaces, whereas By Sequence View displays policies in the exact order they are processed by the firewall.

NEW QUESTION 45
An administrator notices that some users are unable to establish SSL VPN connections, while others can connect without any issues.
What should the administrator check first?

A. Ensure that the affected users are using the correct port number.
B. Ensure that user traffic is hitting the firewall policy.
C. Ensure that forced tunneling is enabled to reroute all traffic through the SSL VPN
D. Ensure that the HTTPS service is enabled on SSL VPN tunnel interface

Answer: A
Explanation:
The key part of the NEW QUESTION is some users can connect and some cannot, which strongly suggests a client-side connection issue rather than a firewall-policy issue (policy only applies after the tunnel is established).

For SSL-VPN, the first thing to check when users fail to connect is whether they are using the correct connection settings (especially the port).

NEW QUESTION 46
Refer to the exhibit. Why did FortiGate drop the packet?

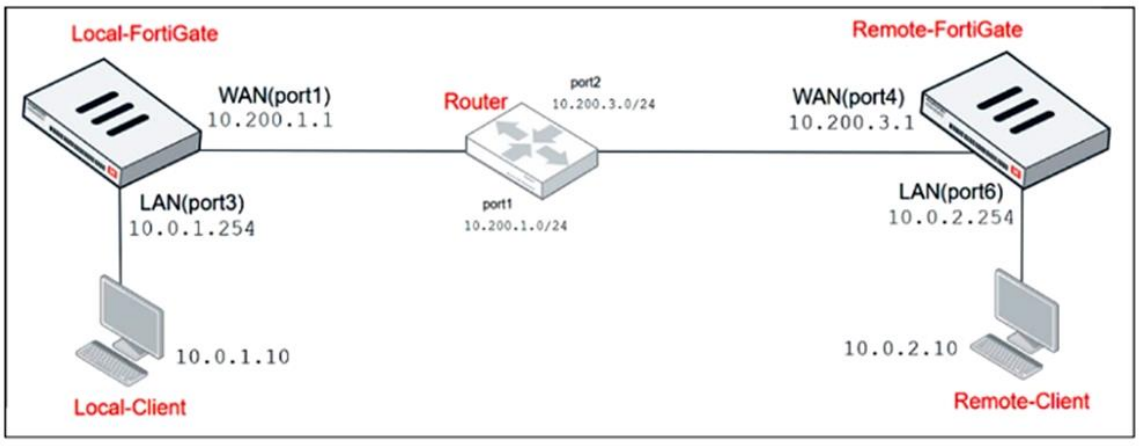
```
id=65308 trace_id=6 func=print_pkt_detail line=5895 msg="vd-root:0 received a packet(proto=1, 10.0.1.10:21637
->10.200.1.254:2048) tun_id=0.0.0.0 from port3. type=8, code=0, id=21637, seq=2."
id=65308 trace_id=6 func=init_ip_session_common line=6076 msg="allocate a new session-00025d45, tun_id=0.0.0.
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)"
```

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.

NEW QUESTION 47
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 IP address `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. 10.200.1.1
B. 10.200.1.149
C. 10.200.1.99
D. 10.200.1.49

Answer: C
Explanation:
All_TCP doesn't include ICMP. So you would match rule ID 2, in which uses IP Poop remote 1.

NEW QUESTION 48
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 profile. This setting is required when the SSL inspection profile is defined with a private CA certificate.
B. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.
C. The browser does not recognize the certificate in use as signed by a trusted CA.
D. 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.

NEW QUESTION 49
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: AB
Explanation:
Also, advanced mode supports nested or inherited groups; that is, users can be members of subgroups that belong to monitored parent groups.
In advanced mode, you can configure FortiGate as an LDAP client and configure the group filters on FortiGate. You can also configure group filters on the collector agent.

NEW QUESTION 50
You are encountering connectivity problems caused by intermediate devices blocking IPsec traffic.
In which two ways can you effectively resolve the problem? (Choose two.)

A. You can use SSL VPN tunnel mode to prevent problems with blocked ESP and UDP ports (500 or 4500).
B. You can configure a hub-and-spoke topology with SSL VPN tunnels to bypass blocked UDP ports.
C. You can turn on fragmentation to fix large certificate negotiation problems.
D. You should use the protocol IKEv2.

Answer: AB
Explanation:
The training is basically trying to point out the advantage of FortiGate's SSL VPN over IPSec VPN in situation where issues are caused by an intermediate device.
IPsec uses ESP and UDP 500 and 4500, so where these are blocked, SSL VPN tunnel mode shines because it uses HTTPS (443) and TLS by default (both TCP).
Again where UDP ports are blocked, SSL VPN shines (Tunnel mode Hub and Spoke) because it does not use UDP.
……