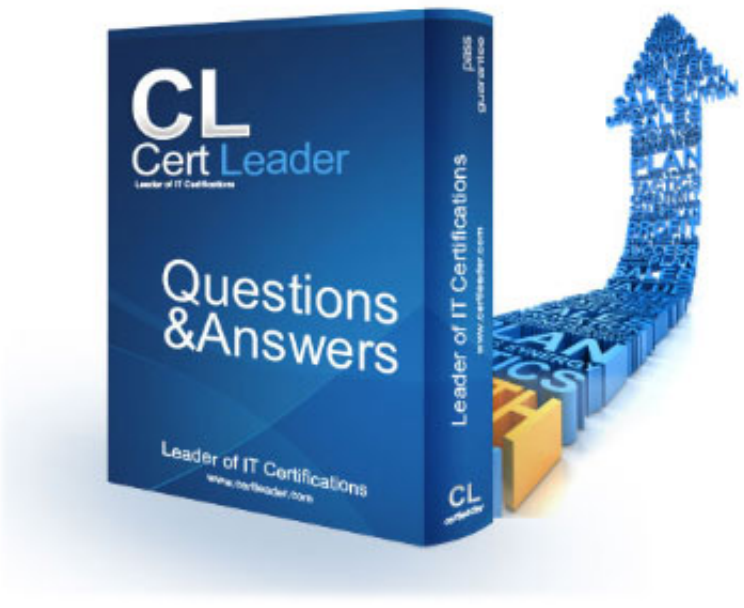
FCP_FGT_AD-7.6 Dumps

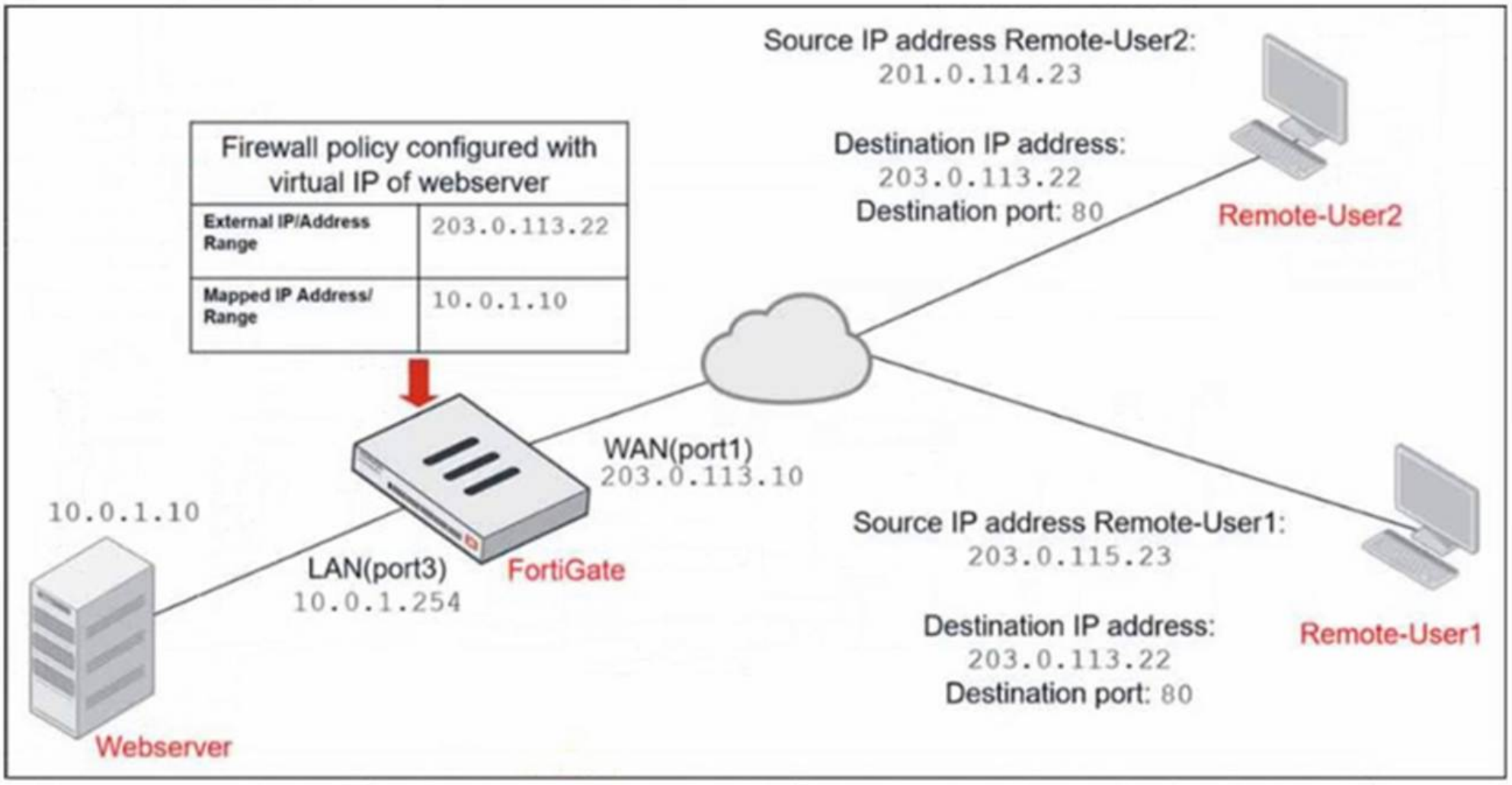
FCP - FortiGate 7.6 Administrator

https://www.certleader.com/FCP_FGT_AD-7.6-dumps.html



NEW QUESTION 1
Refer to the exhibits.

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

The exhibits show a diagram of a FortiGate device connected to the network, and the firewall configuration.
The policy should work such thatRemote-User1must be able to access the Webserver while preventing Remote-User2from accessing theWebserver.
Which additional configuration can the administrator add to a deny firewall policy, beyond the default behavior, to blockRemote-User2from accessing theWebserver?

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 2
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 3
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: B

Explanation:
NetAPI polling mode involves frequent queries to domain controllers, which can cause increased bandwidth usage, especially in large networks with many login events.

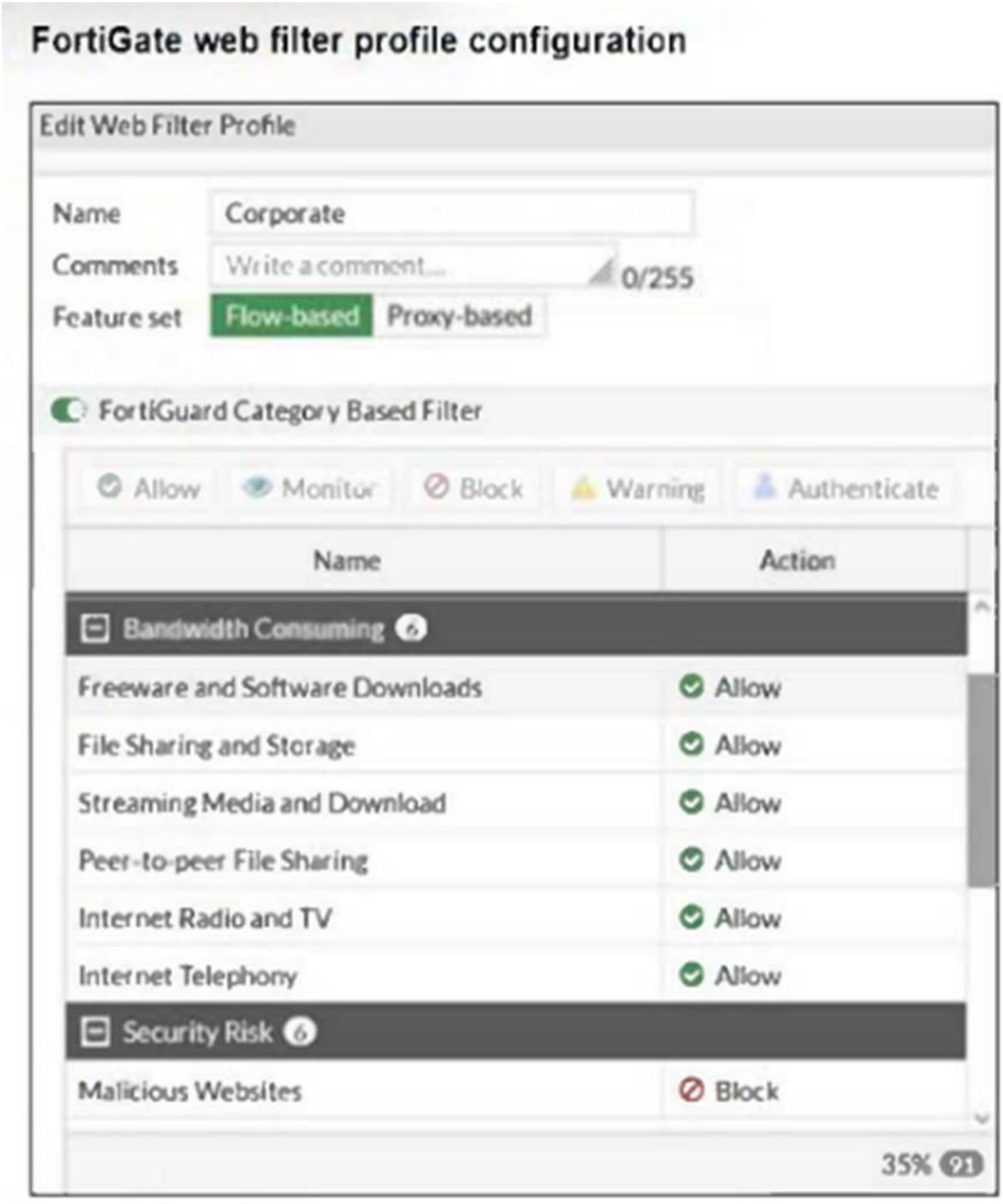
NEW QUESTION 4
Which two statements describe characteristics of automation stitches? (Choose two.)

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 5
Refer to the exhibit.



The exhibit shows theFortiGuard Category Based Filtersection of a corporate web filter profile.
An administrator must block access todownload.com, which belongs to theFreeware and Software Downloadscategory. 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: AC

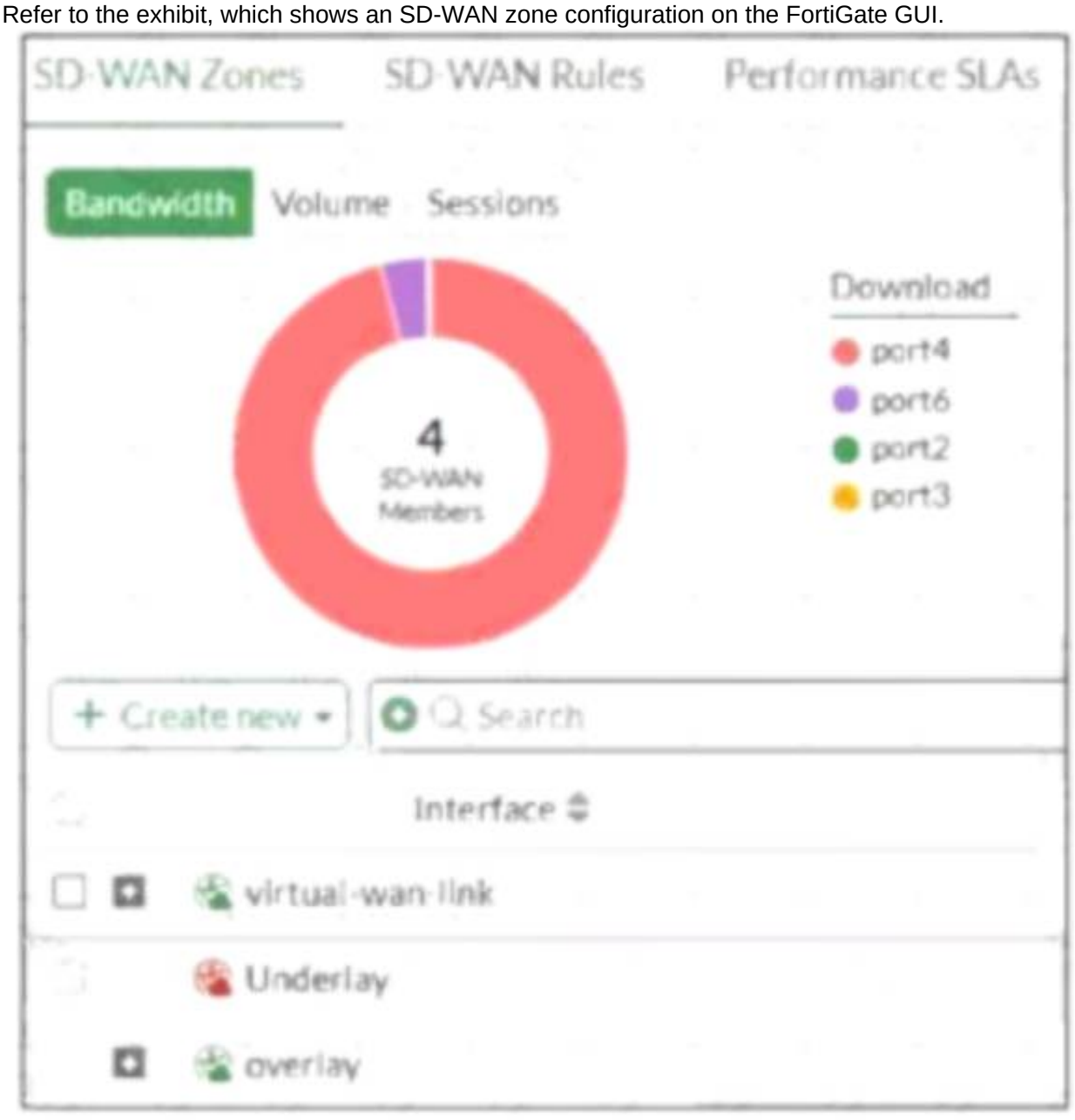
Explanation:
Creating a static URL filter to block download.com specifically allows blocking that site without affecting the entire category.
Using a separate firewall policy with a Deny action for an FQDN address object matching download.com can also block the site while allowing others in the same category.

NEW QUESTION 6
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: BD

NEW QUESTION 7
Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.



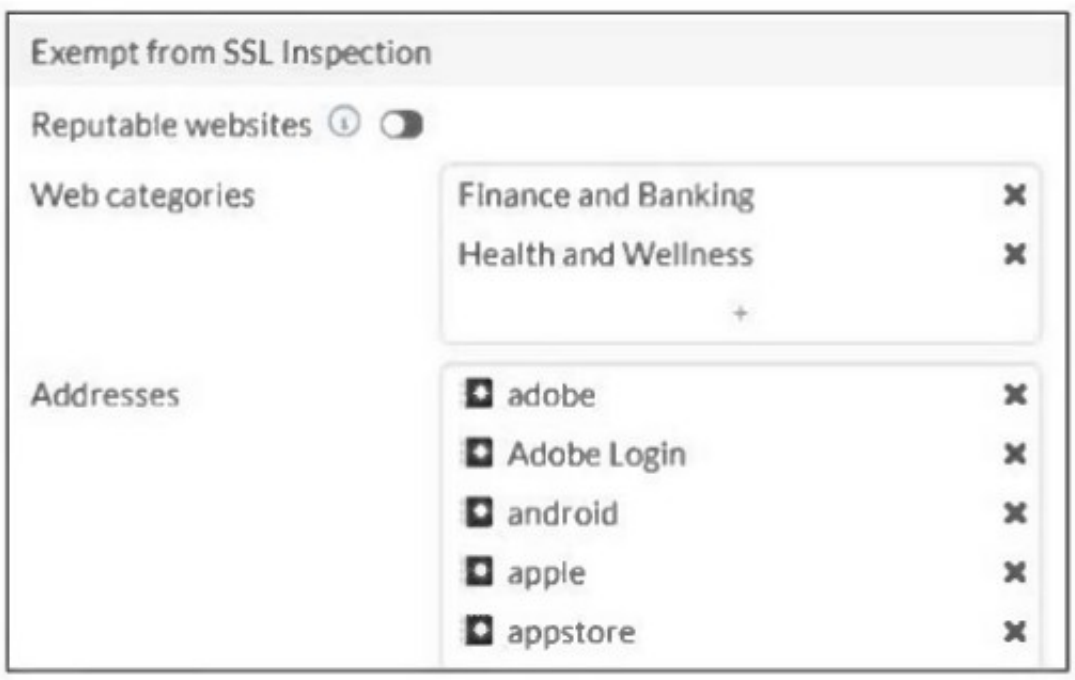
Based on the exhibit, which statement is true?

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: A

Explanation:
The Underlay zone is the default SD-WAN zone, typically representing the physical interfaces in the SD- WAN configuration before overlay or virtual links are added.

NEW QUESTION 8
Refer to the exhibit.



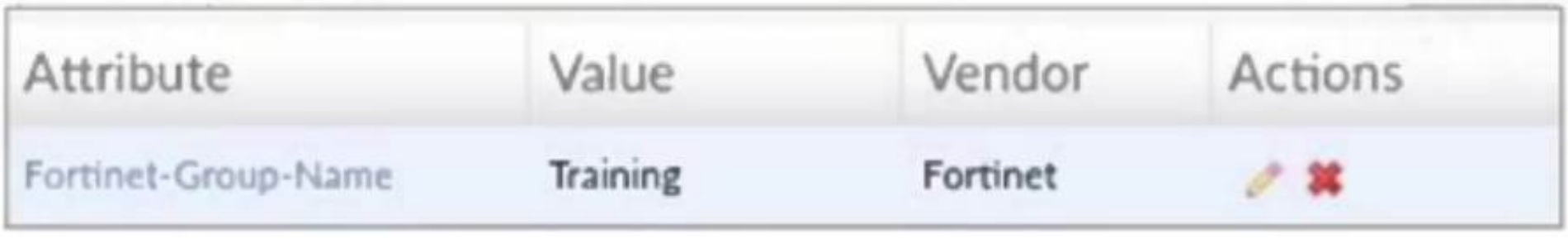
The predefined deep-inspection and custom-deep-inspection profiles exclude some web categories from SSL inspection, as shown in the exhibit.
For which two reasons are these web categories exempted? (Choose two.)

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 9
Refer to the exhibit, which shows a partial configuration from the remote authentication server.



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 10
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 10
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 15
What are three key routing principles in SD-WAN? (Choose three.)

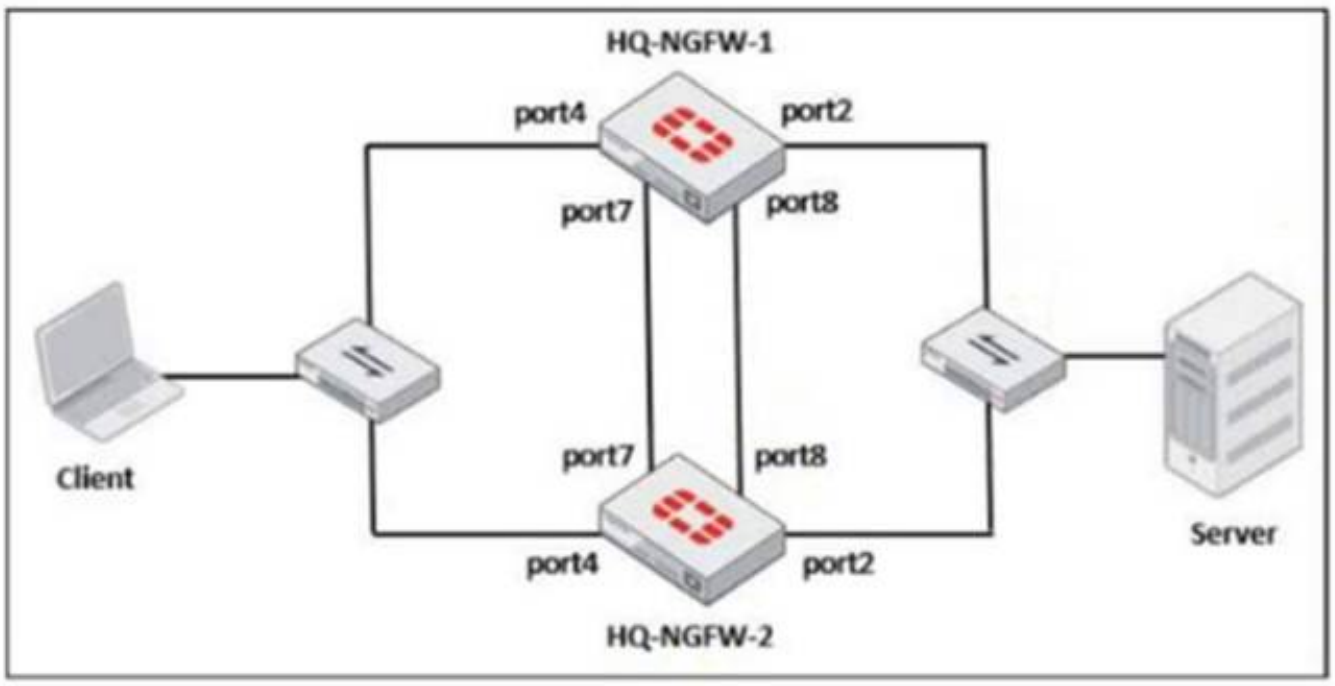
A. By defaul
B. SD-WAN rules are skipped if the included SD-WAN members do not have a valid route to the destination.
C. SD-WAN rules have precedence over any other type of routes.
D. Regular policy routes have precedence over SD-WAN rules.
E. By defaul
F. SD-WAN rules are skipped if only one route to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

Answer: ABE

Explanation:
SD-WAN rules are skipped if none of the SD-WAN members have a valid route to the destination. SD-WAN rules take precedence over other route types.
SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member by default.

NEW QUESTION 19
Refer to the exhibits.

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"
```

Based on the current HA status, an administrator updates theoverrideandpriorityparameters on HQ-NGFW-1 and HQ-NGFW-2 as shown in the exhibit.
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 24
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.

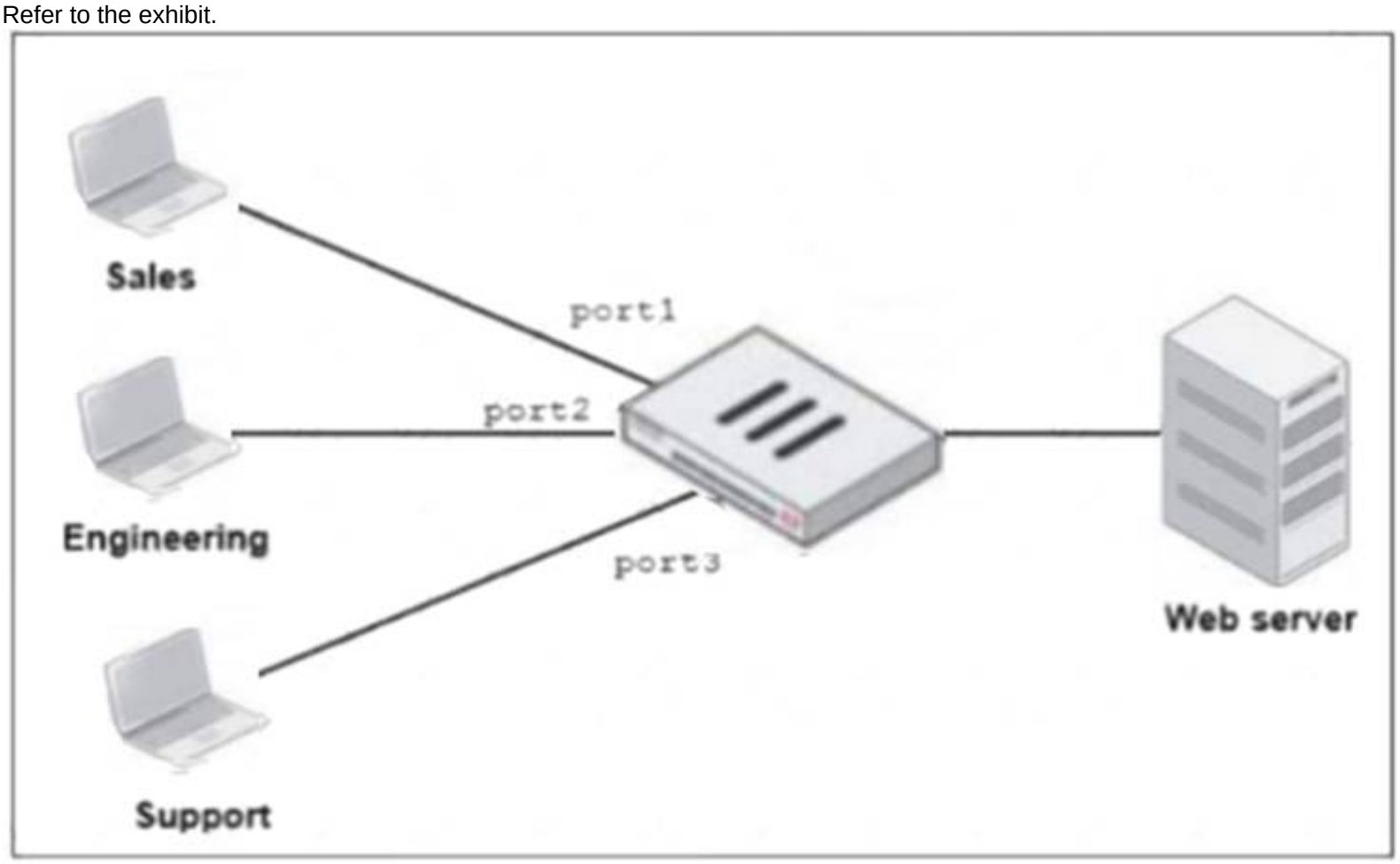
NEW QUESTION 27
Which two statements are correct when FortiGate enters conserve mode? (Choose two.)

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:
In conserve mode, FortiGate restricts configuration changes to preserve system stability.
When IPS fail-open is enabled, FortiGate continues forwarding traffic without IPS inspection during resource constraints (conserve mode).

NEW QUESTION 28
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 30
Refer to 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
```

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?

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 35
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCP_FGT_AD-7.6 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCP_FGT_AD-7.6-dumps.html