Fortinet

Exam Questions FCP_FGT_AD-7.6

FCP - FortiGate 7.6 Administrator

NEW QUESTION 1
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: AC

Explanation:
Disabling IKE fragmentation helps resolve issues caused by intermediate devices blocking large fragmented packets during certificate negotiation.
Using SSL VPN tunnel mode encapsulates traffic over HTTPS, bypassing blocks on ESP and UDP ports commonly used by IPsec.

NEW QUESTION 2
Refer to the exhibit.

Profile Name
Monitoring_Access
NOC_Access
prof_admin
super_admin

The NOC team connects to the FortiGate GUI with theNOC_Accessadmin 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?

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: D

Explanation:
The admintimeout setting in the admin access profile controls the inactivity timeout for GUI sessions. Increasing this value will extend the session duration before automatic disconnection.

NEW QUESTION 3
Refer to the exhibit.

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

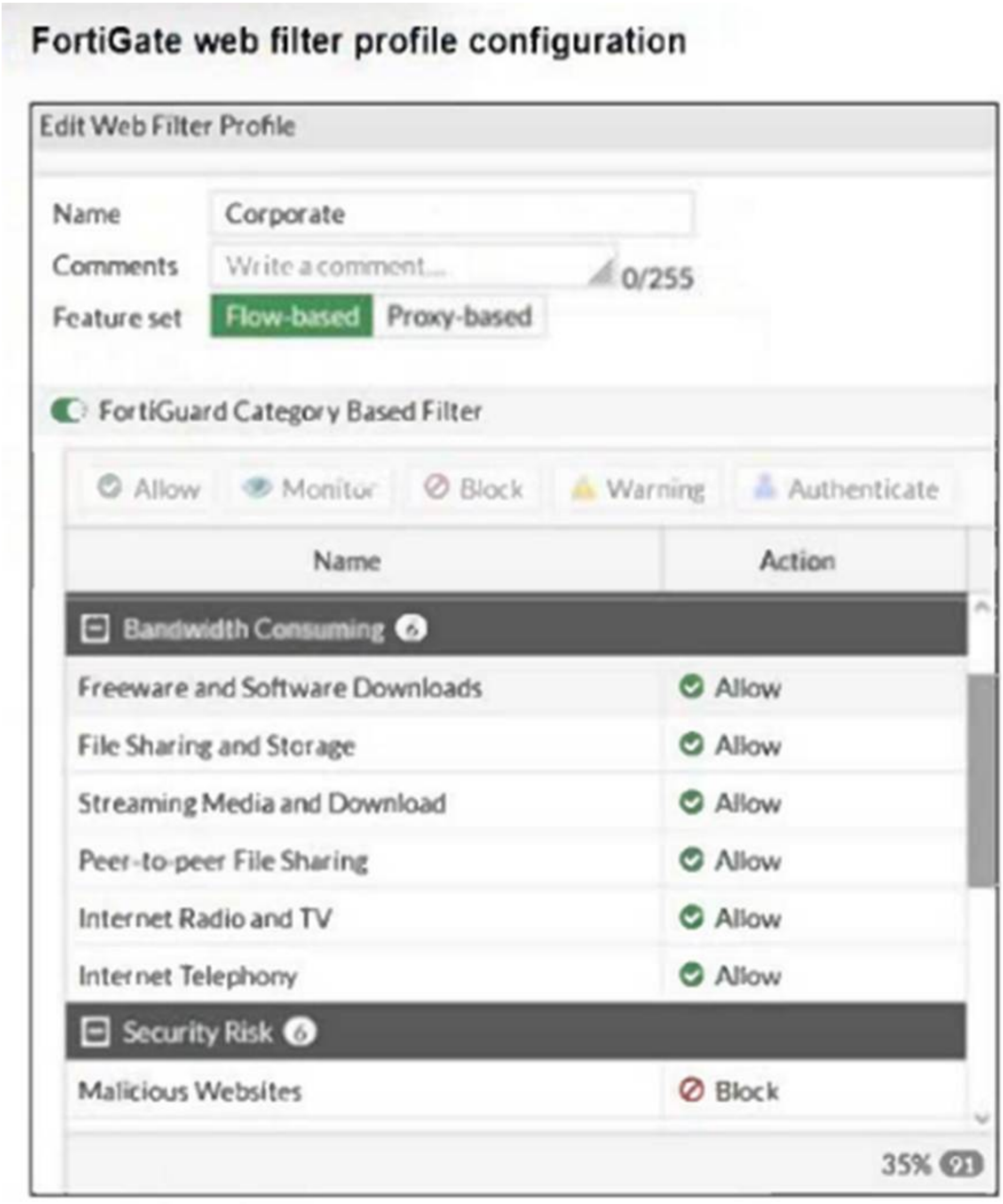
Based on this partial configuration, what are the two possible outcomes when FortiGate enters conserve mode? (Choose two.)

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: BD

Explanation:
In fail-open mode, FortiGate skips quarantine actions to maintain traffic flow despite IPS or antivirus failures. FortiGate drops new sessions that require inspection when in conserve mode and fail-open is enabled, to
protect the network from potentially harmful traffic.

NEW QUESTION 4
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.

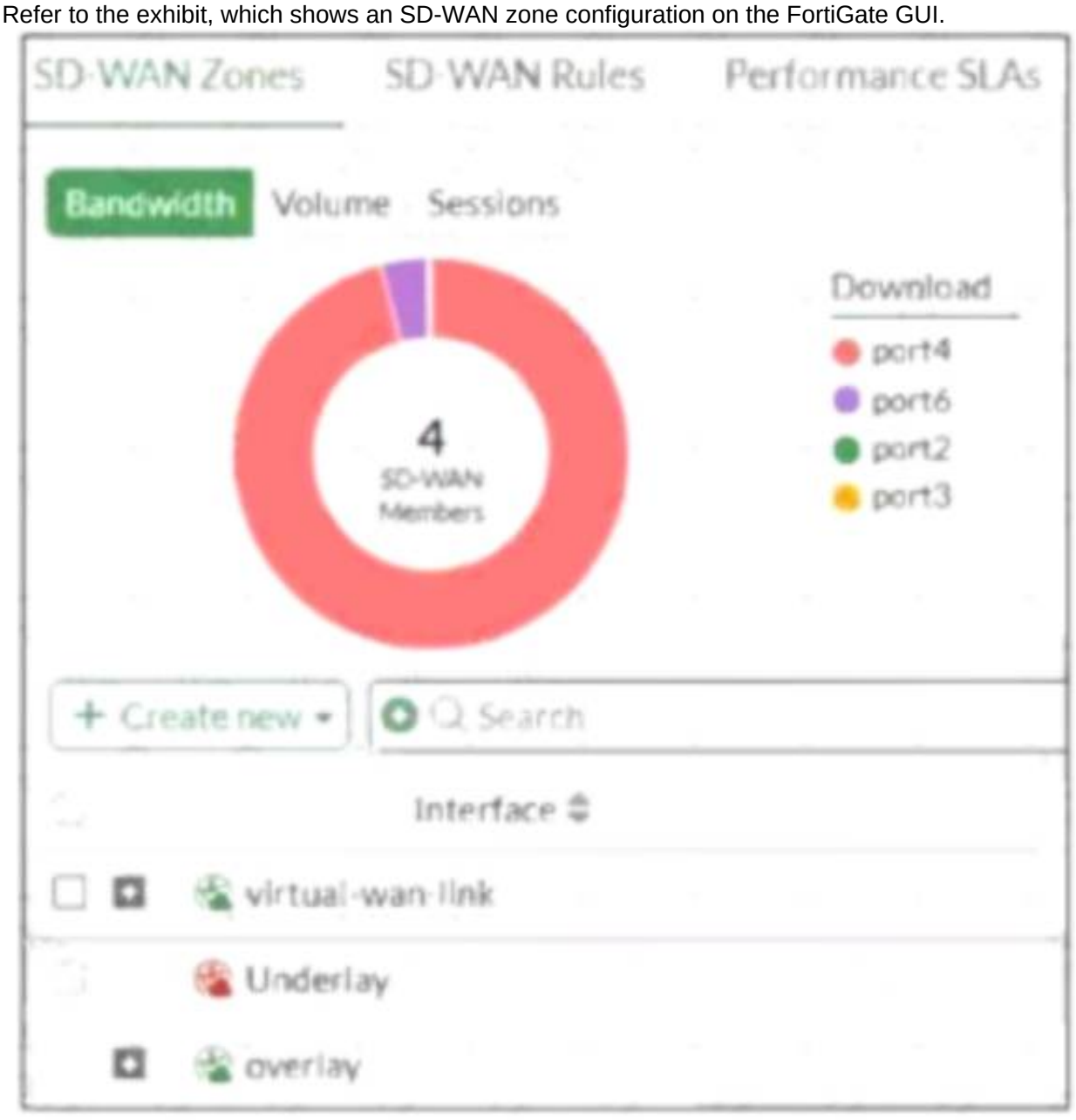
NEW QUESTION 5
You have configured an application control profile, set peer-to-peer traffic to Block under the Categories tab, and applied it to the firewall policy. However, your peer-to-peer traffic on known ports is passing through the FortiGate without being blocked.
What FortiGate settings should 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 settings control how FortiGate inspects and enforces protocols on traffic, including peer-to-peer applications on known ports. If not properly enabled, peer-to-peer traffic may bypass blocking despite the application control profile.

NEW QUESTION 6
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 7
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-NGF
E. set Encryption to AES256

Answer: AC

Explanation:
The key lifetime (Seconds) must match on both sides; BR1-FGT is set to 14400, so setting it to 43200 matches HQ-NGFW.
The remote address on BR1-FGT should match the HQ-NGFW??s local subnet (10.0.11.0/24), but it is currently set incorrectly as 172.20.1.0/24. Changing it to 10.0.11.0/255.255.255.0 will align the Phase 2 selectors.

NEW QUESTION 8
Refer to the exhibit.

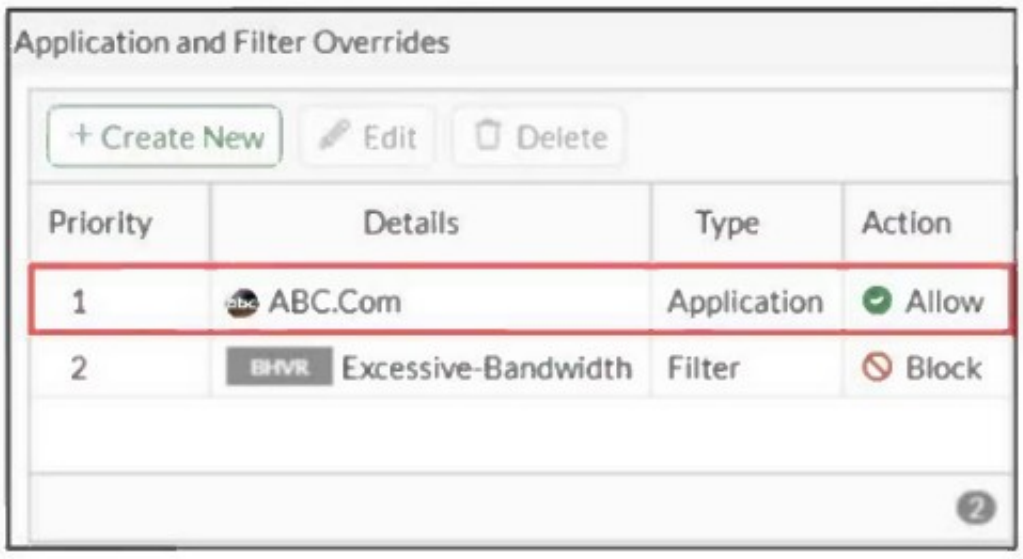
An administrator has created a new firewall address to use as the destination for a static route.
Why is the administrator not able to select the new address in theDestinationfield of the new static route?

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 9
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: A

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 10
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: AD

NEW QUESTION 10
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCP_FGT_AD-7.6 Practice Exam Features:

* FCP_FGT_AD-7.6 Questions and Answers Updated Frequently

* FCP_FGT_AD-7.6 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FGT_AD-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FGT_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The FCP_FGT_AD-7.6 Practice Test Here