



Fortinet

Exam Questions FCP_FGT_AD-7.6

FCP - FortiGate 7.6 Administrator

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW 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

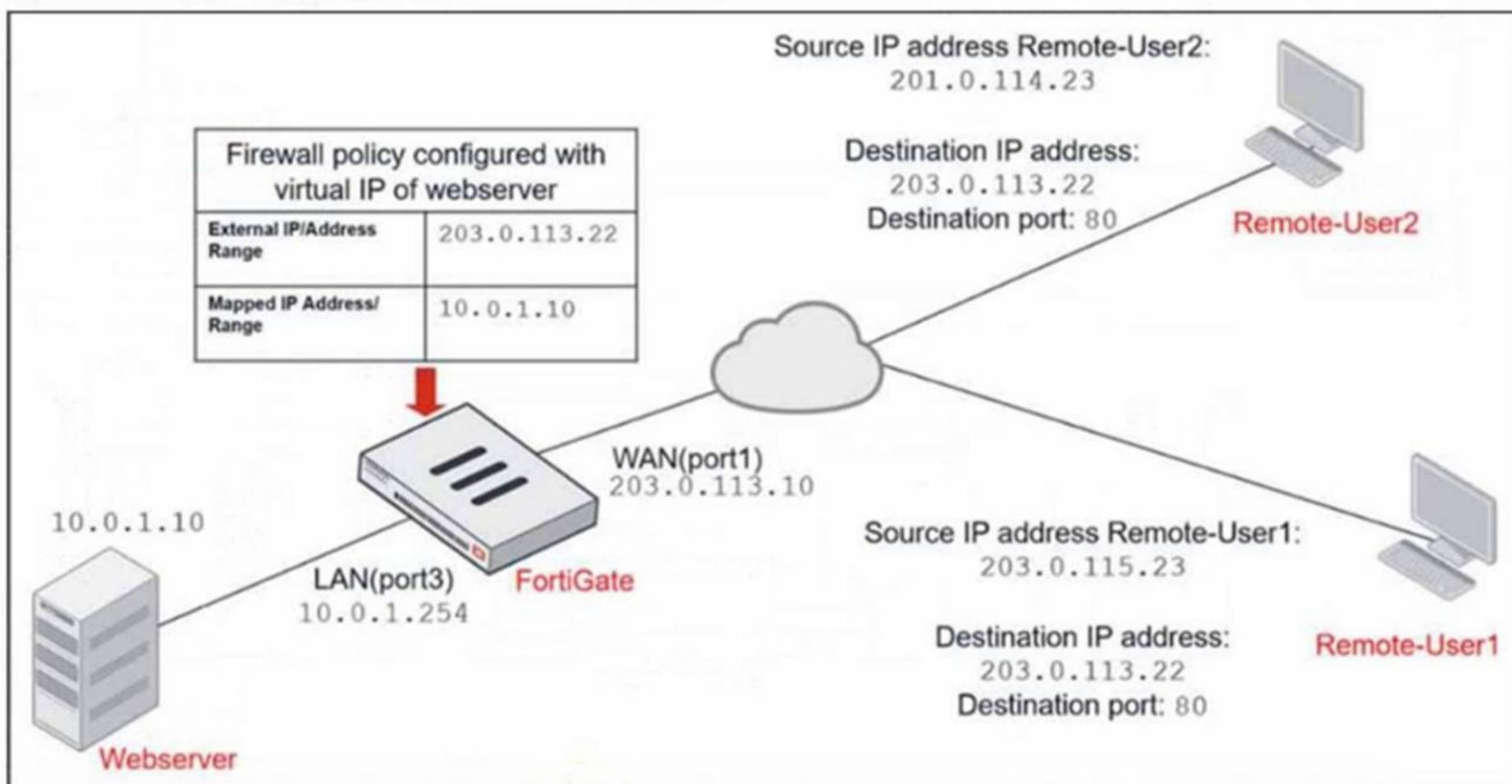
Explanation:

When HA override is enabled, FortiGate uses the following election order: number of connected monitored ports, then device priority, followed by HA uptime, and finally FortiGate serial number as a tiebreaker.

NEW QUESTION 2

Refer to the exhibits.

Network diagram



Firewall address object

Edit Address

Name: Deny_IP

Color: Change

Type: Subnet

IP/Netmask: 201.0.114.23/32

Interface: WAN (port1)

Static route configuration:

Comments: Deny web server access. 23/255

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 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 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

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 5

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 6

Refer to the exhibit.



The NOC team connects to the FortiGate GUI with the NOC_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 7

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

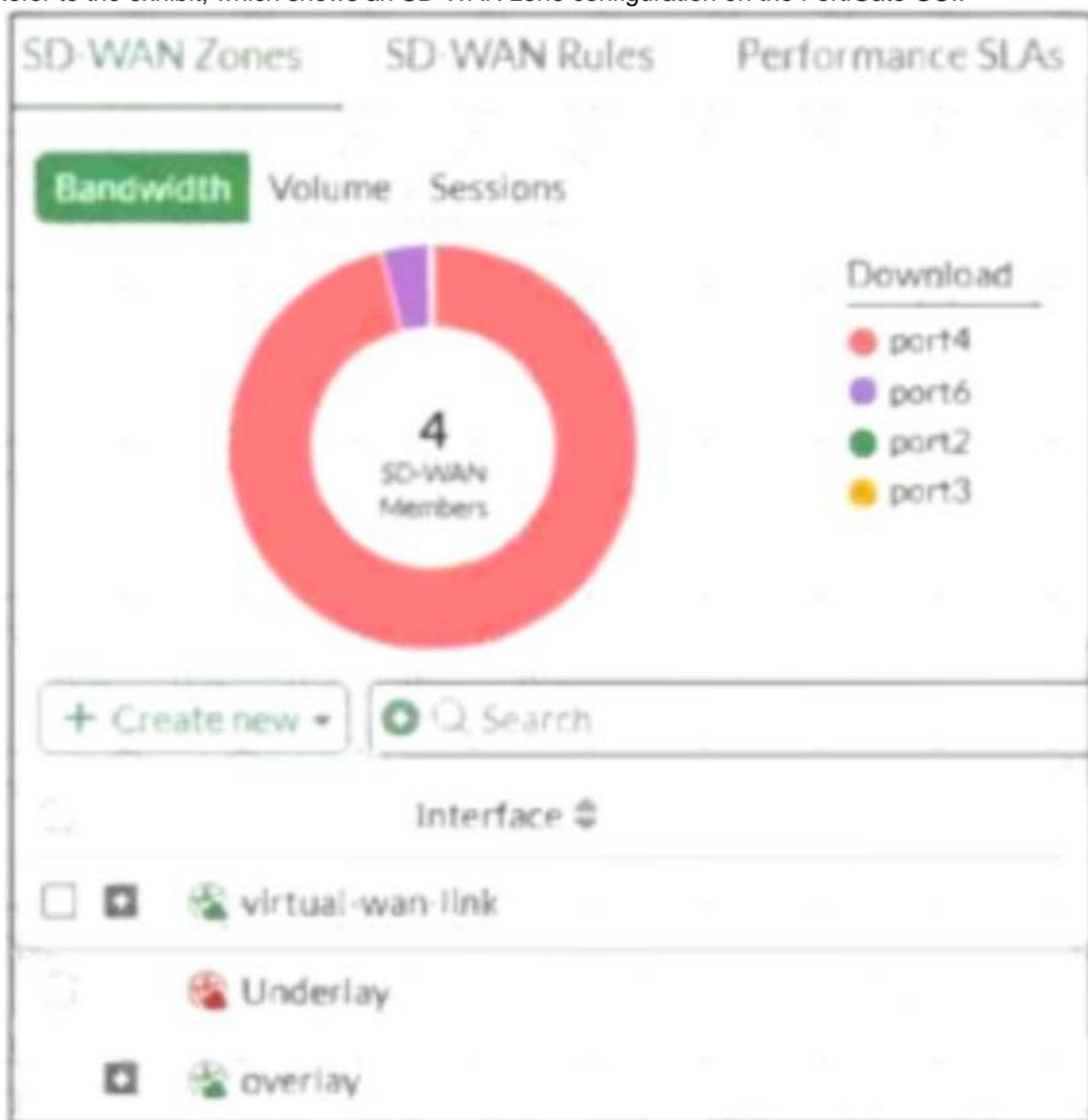
Answer: D

Explanation:

DNS traffic must be allowed so the user can resolve domain names and reach the authentication server or web resources, even if authentication initially fails.

NEW QUESTION 8

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.

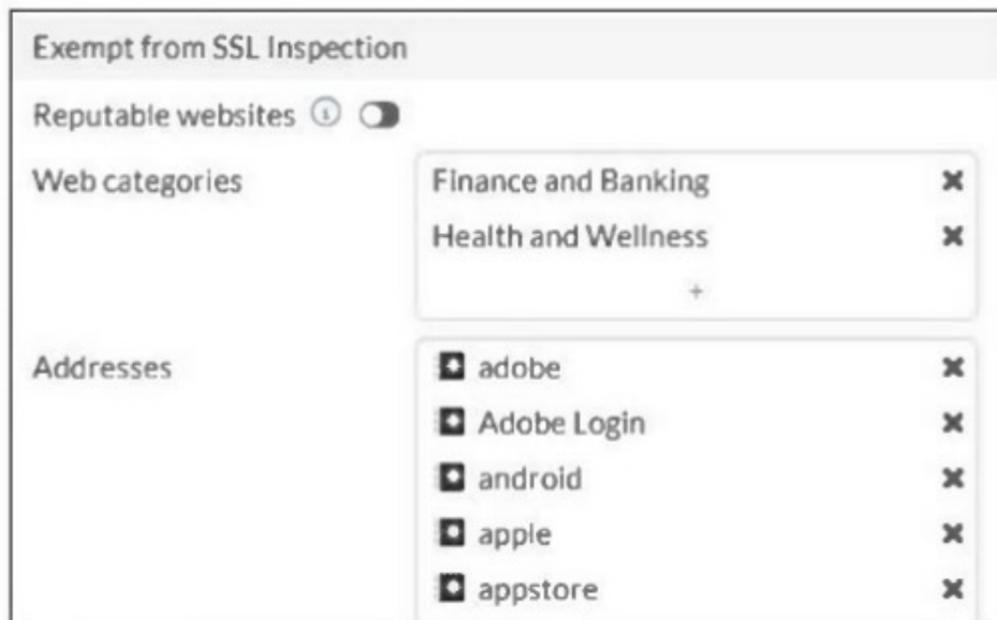
Answer: A

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 9

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 10

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: D

Explanation:

With the Server certificate SNI check set to Strict, FortiGate enforces that the SNI must match either the Common Name (CN) or Subject Alternative Name (SAN) in the server certificate; otherwise, it closes the connection.

NEW QUESTION 10

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

- A. By default
- 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 default
- F. SD-WAN rules are skipped if only one route to the destination is available.
- G. By default
- 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 15

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: B

Explanation:

If user traffic is not matching the appropriate firewall policy that permits SSL VPN, users will be unable to establish connections, making this the first aspect to verify.

NEW QUESTION 19

Refer to the exhibit.



Phase 2 selectors

Name	Local Address	Remote Address	Comments
ToBR1	10.0.11.0/255.255.255.0	172.20.1.0/255.255.255.0	

Edit Phase 2 Selector

Name: ToBR1

Comments: Comments (0/255)

Encapsulation: Tunnel Mode (selected), Transport Mode

IP version: IPv4 (selected), IPv6

Named address:

Local address: Subnet Address (selected), IP Range
 10.0.11.0 255.255.255.0

Remote address: Subnet Address (selected), IP Range
 172.20.1.0 255.255.255.0

Advanced

Encryption - authentication: AES128 - SHA1

Replay detection: Enable Disable

Perfect forward secrecy (PFS): Enable Disable

Diffie-Hellman groups: 1 2 5 16 19 30

Local port: All (selected), Specify

Remote port: All (selected), Specify

Protocol: All (selected), Specify

Auto-negotiate: Enable Disable

Autokey keep alive: Enable Disable

Key lifetime: Seconds (selected), Kilobytes, Both
 43200 second(s)

Phase 2 selectors

Name	Local Address	Remote Address	Comments
ToHQ	172.20.1.0/255.255.255.0	10.11.0.0/255.255.255.0	

Edit Phase 2 Selector

Name: ToHQ

Comments: Comments (0/255)

Encapsulation: Tunnel Mode (selected), Transport Mode

IP version: IPv4 (selected), IPv6

Named address:

Local address: Subnet Address (selected), IP Range
 172.20.1.0 255.255.255.0

Remote address: Subnet Address (selected), IP Range
 10.11.0.0 255.255.255.0

Advanced

Encryption - authentication: AES256 - SHA1

Replay detection: Enable Disable

Perfect forward secrecy (PFS): Enable Disable

Diffie-Hellman groups: 1 2 5 14 15 16 19 30

Local port: All (selected), Specify

Remote port: All (selected), Specify

Protocol: All (selected), Specify

Auto-negotiate: Enable Disable

Autokey keep alive: Enable Disable

Key lifetime: Seconds (selected), Kilobytes, Both
 14400 second(s)

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 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 25

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

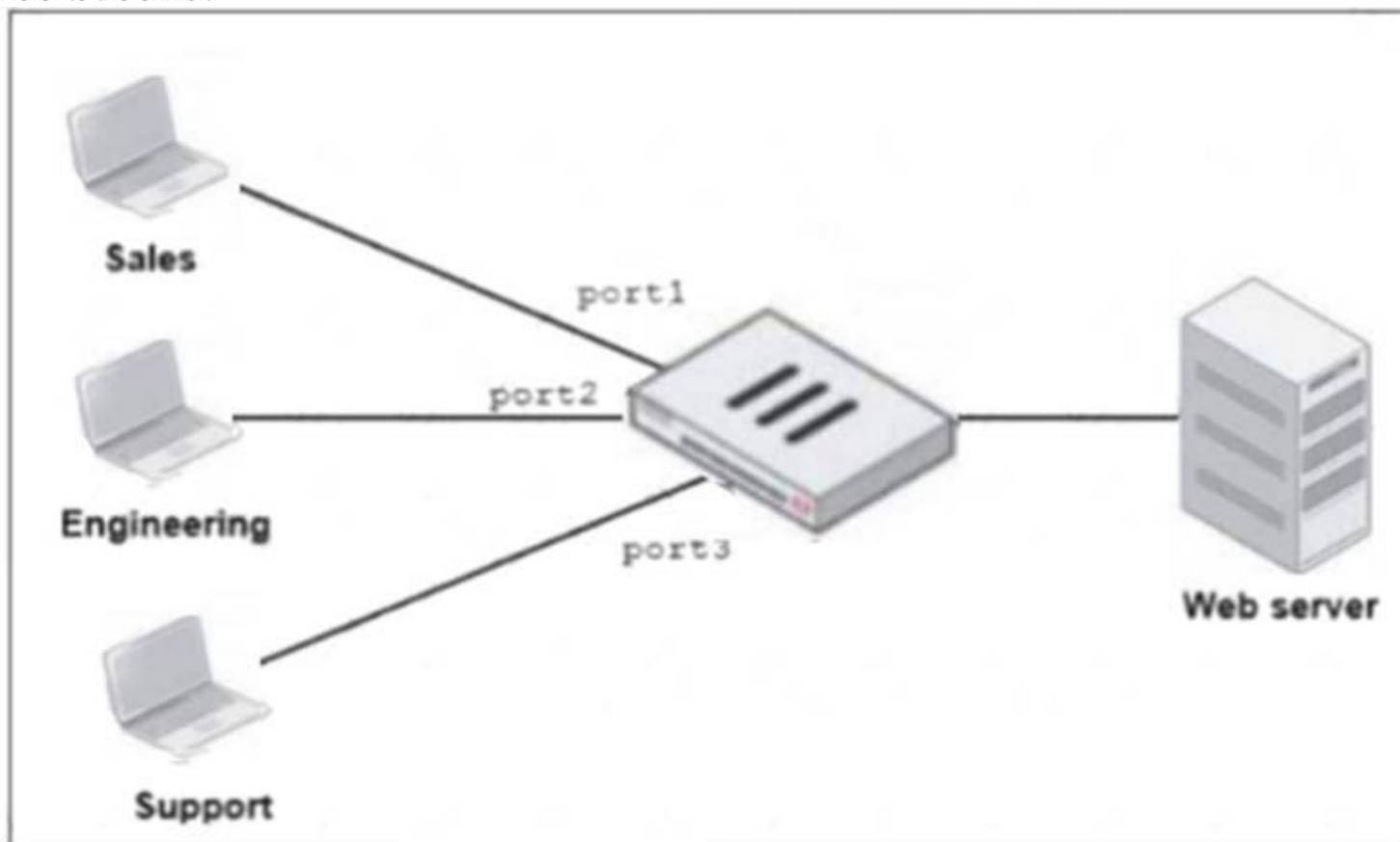
Explanation:

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 33

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 38

.....

Relate Links

100% Pass Your FCP_FGT_AD-7.6 Exam with Exambible Prep Materials

https://www.exambible.com/FCP_FGT_AD-7.6-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>