

Exam Questions FCP_FGT_AD-7.6

FCP - FortiGate 7.6 Administrator

https://www.2passeasy.com/dumps/FCP_FGT_AD-7.6/



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

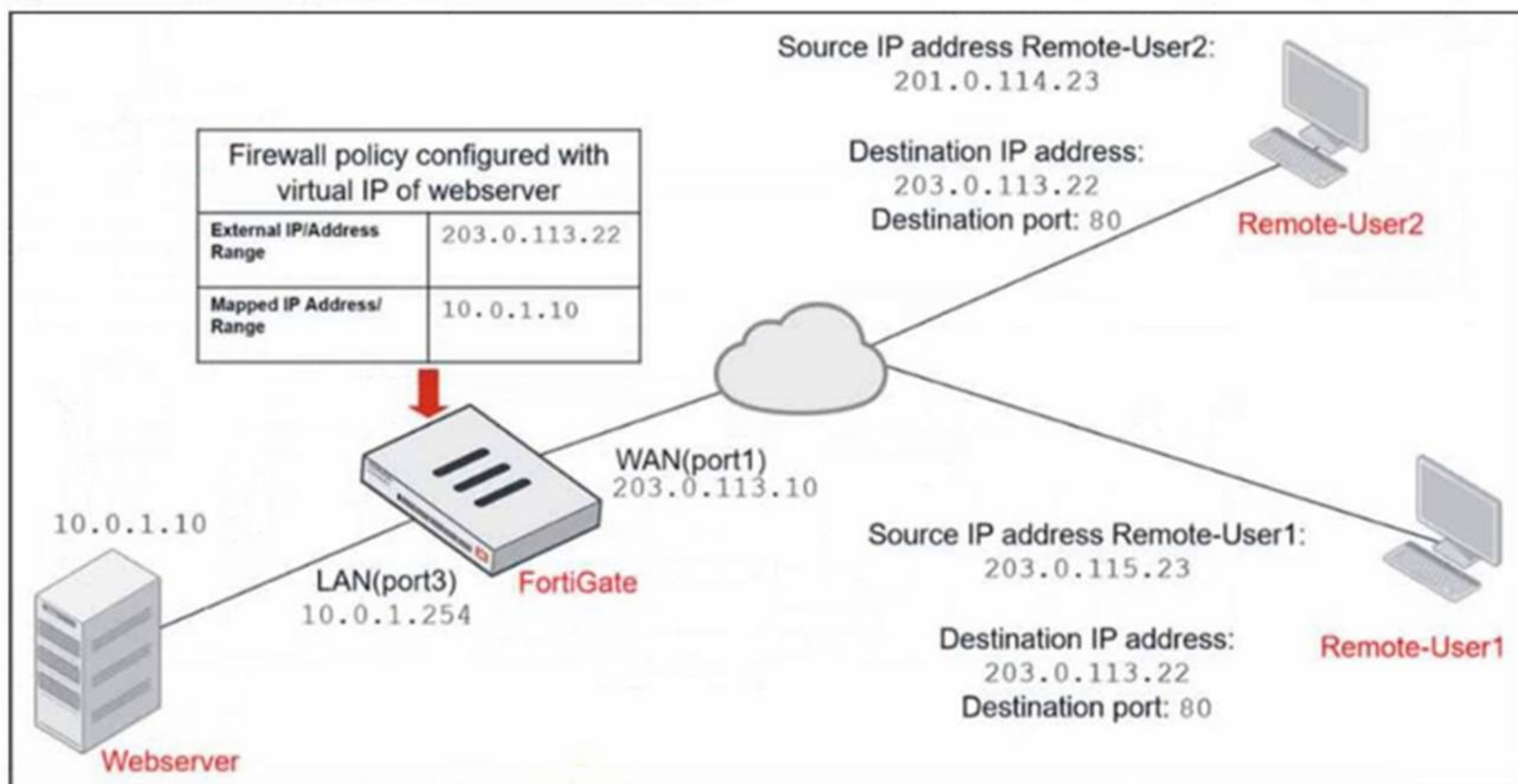
Explanation:

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

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 6

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 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

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 10

Refer to the exhibits.

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
```

An administrator has observed the performance status outputs on an HA cluster for 55 seconds. 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: D

Explanation:

The HA configuration shows that override is disabled (set override disable), but despite this, HQ-NGFW-1 has the higher priority (200) and is acting as the primary, as indicated by its higher resource usage and uptime.

Override allows the device with higher priority to take over as primary, so HQ-NGFW-1 is the primary device.

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 13

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:

Interfaces must have directly connected routes in the routing table to forward traffic correctly. Interfaces must have IP addresses assigned to communicate within their respective networks.

NEW QUESTION 18

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

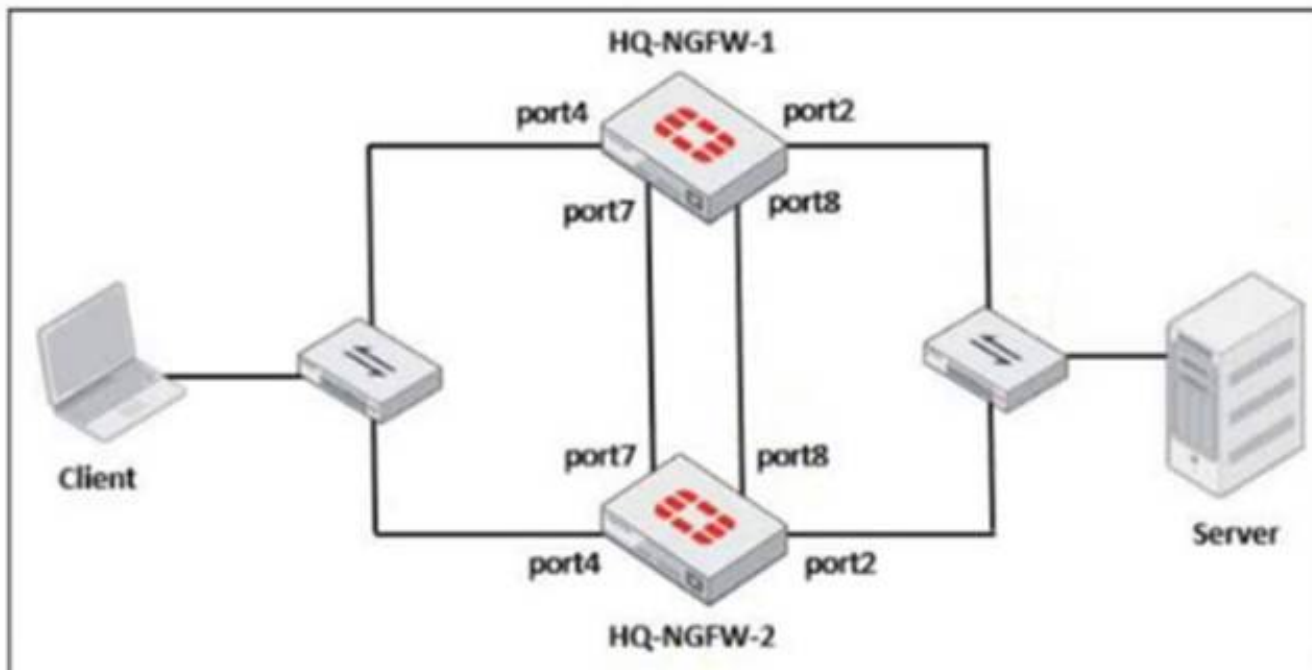
Explanation:

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 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 the override and priority parameters 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 20

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: 0/255

Encapsulation: Tunnel Mode

IP version: IPv4

Named address: ☐

Local address: Subnet Address
10.0.11.0 255.255.255.0

Remote address: Subnet Address
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 ☐ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 27 ☐ 28 ☐ 29 ☐ 30 ☐ 31 ☐ 32

Local port: All Specify

Remote port: All Specify

Protocol: All Specify

Auto-negotiate: ☒ Enable ☐ Disable

Autokey keep alive: ☒ Enable ☐ Disable

Key lifetime: Seconds 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: 0/255

Encapsulation: Tunnel Mode

IP version: IPv4

Named address: ☐

Local address: Subnet Address
172.20.1.0 255.255.255.0

Remote address: Subnet Address
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 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 27 ☐ 28 ☐ 29 ☐ 30 ☐ 31 ☐ 32

Local port: All Specify

Remote port: All Specify

Protocol: All Specify

Auto-negotiate: ☒ Enable ☐ Disable

Autokey keep alive: ☒ Enable ☐ Disable

Key lifetime: Seconds 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-NGFW
- 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 22

Refer to the exhibits.

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
```

The exhibits show the system performance output and default configuration of high memory usage thresholds on a FortiGate device. 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: CD

Explanation:

Since memory usage is at 90%, exceeding the red threshold (88%), FortiGate enters a state where configuration changes are still allowed. In this state, FortiGate drops new sessions to preserve resources and maintain stability.

NEW QUESTION 26

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

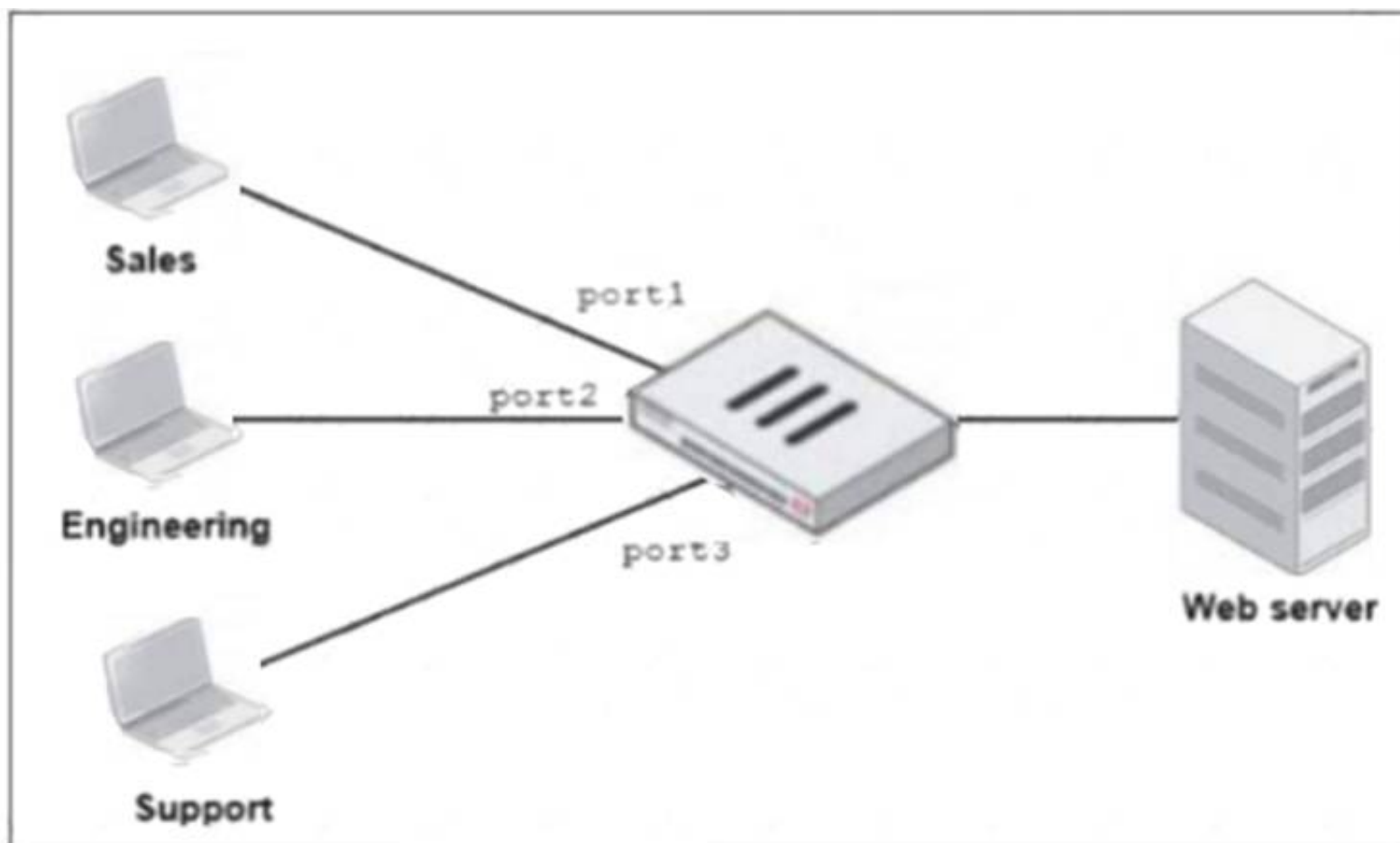
Explanation:

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 27

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 32

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: A

Explanation:

The "On Idle" DPD mode configures FortiGate to send DPD probes only when no inbound traffic is detected, meeting the requirement to send probes only when the tunnel is idle.

NEW QUESTION 37

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 40

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 41

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCP_FGT_AD-7.6 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCP_FGT_AD-7.6 Product From:

https://www.2passeasy.com/dumps/FCP_FGT_AD-7.6/

Money Back Guarantee

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