



Fortinet

Exam Questions FCP_FGT_AD-7.6

FCP - FortiGate 7.6 Administrator

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

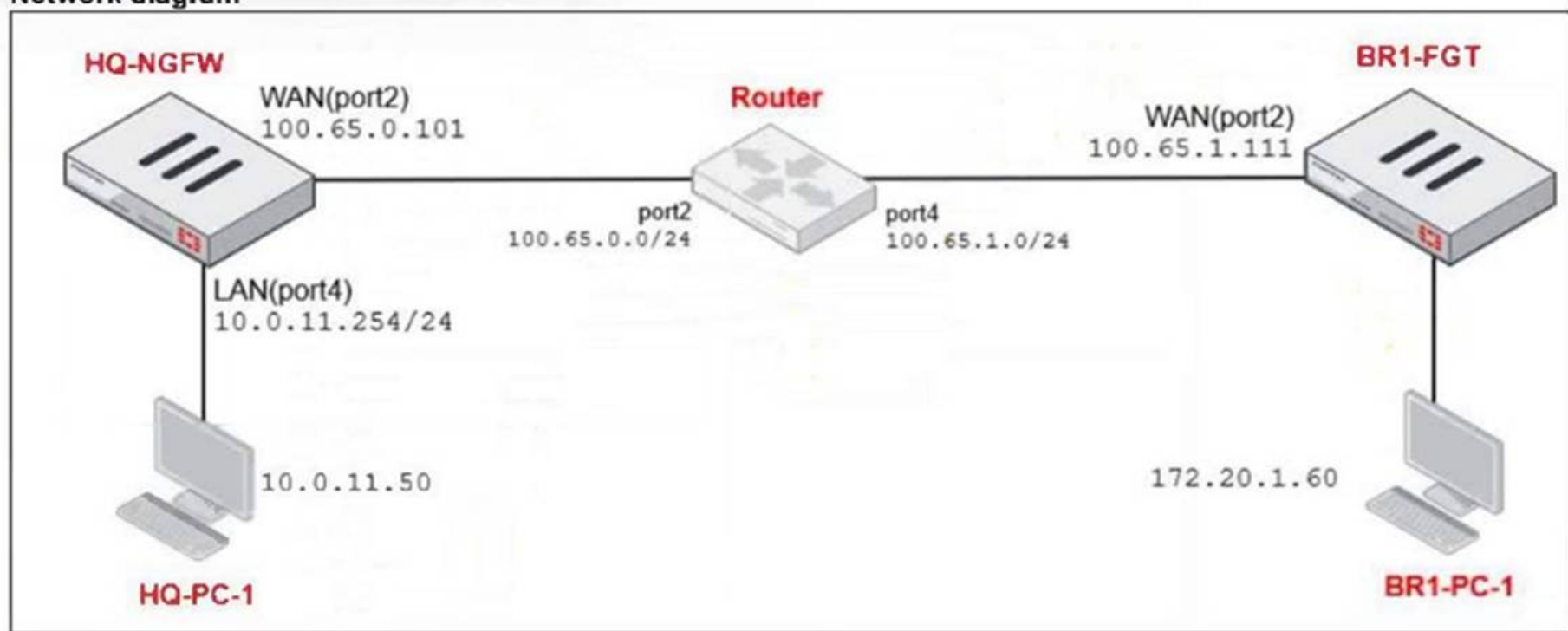
Explanation:

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



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 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 (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 3

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 4

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 5

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.)

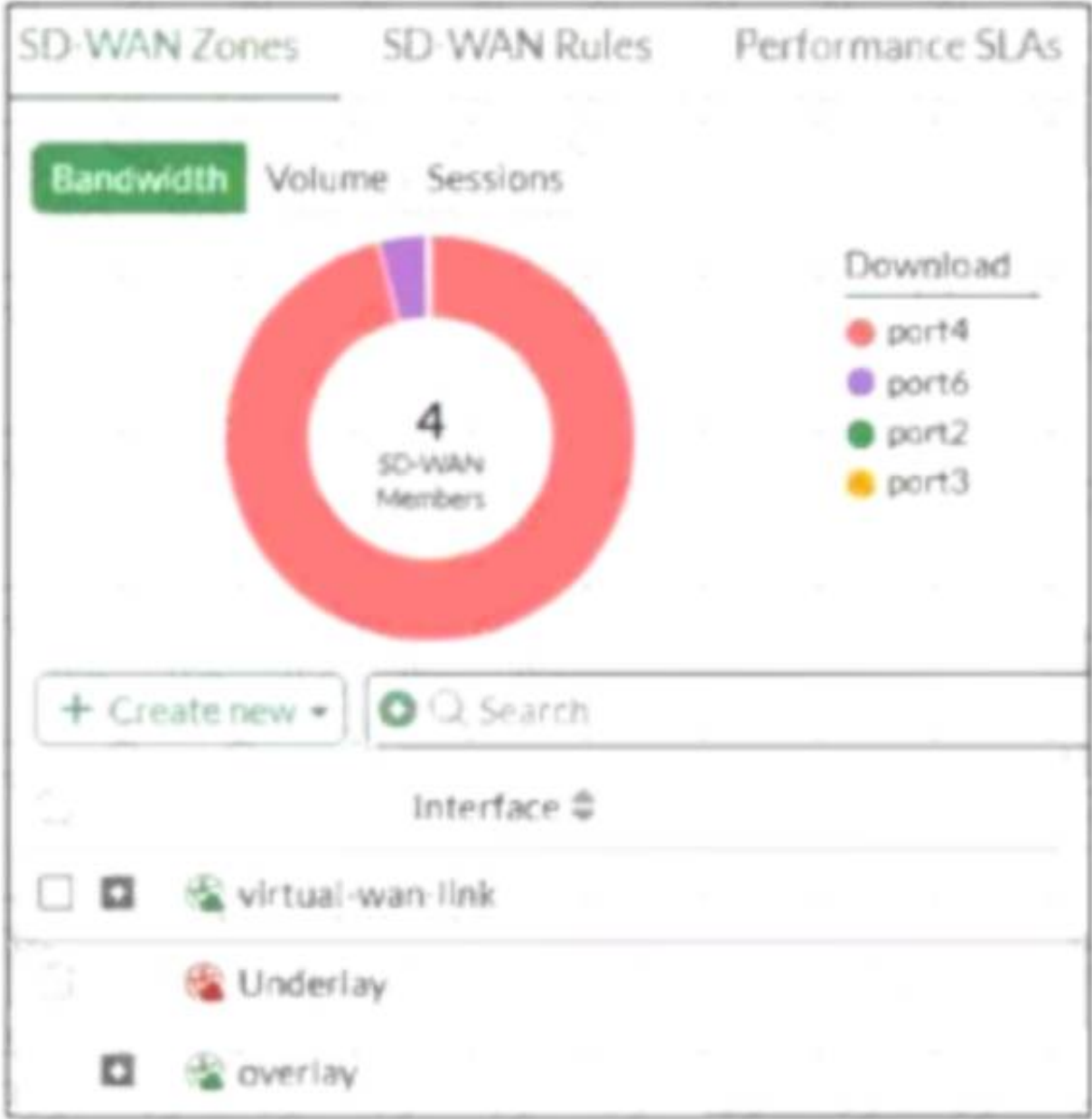
- A. The selected SSL inspection profile has certificate inspection enabled.

- B. The website is exempted from SSL inspection.
- C. The EI 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 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.

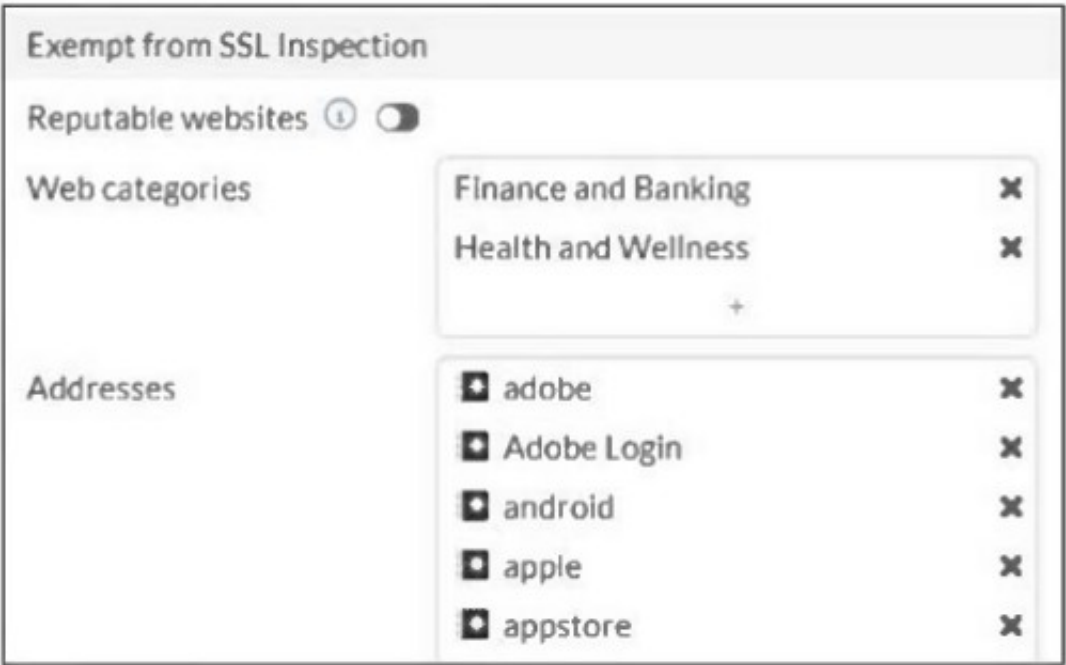
Answer: A

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.



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 8

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 9

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

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 10

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

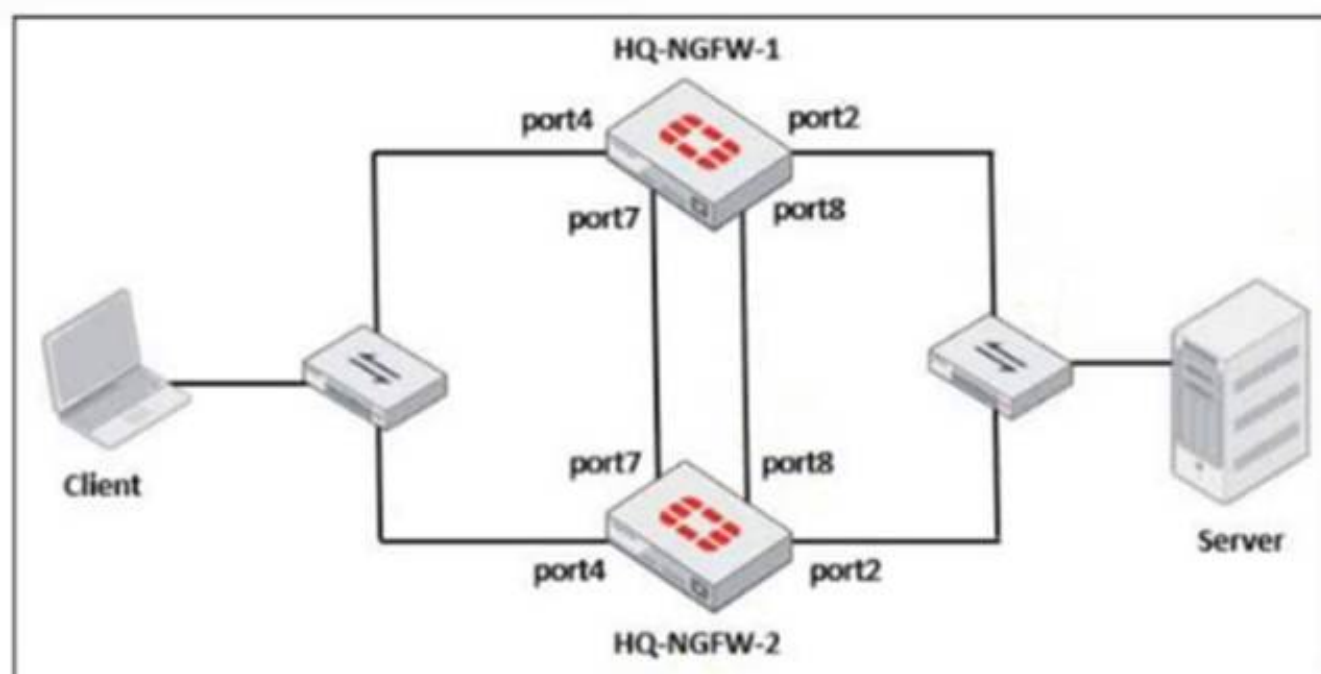
Explanation:

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 14

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 19

Refer to the exhibit.



Phase 2 selectors

+ Create new Edit Delete

Q Search

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 Transport Mode

IP version: IPv4 IPv6

Named address: ☐

Local address: IP Address Subnet Address IP Range
 10.0.11.0 255.255.255.0

Remote address: IP Address Subnet Address 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 ☐ 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

+ Create new Edit Delete

Q Search

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 Transport Mode

IP version: IPv4 IPv6

Named address: ☐

Local address: IP Address Subnet Address IP Range
 172.20.1.0 255.255.255.0

Remote address: IP Address Subnet Address 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 ☐ 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 20

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

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 30

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 32

Refer to the exhibit.

+ Create New Edit Delete			
Priority	Details	Type	Action
1	 ABC.Com	Application	 Allow
2	 Excessive-Bandwidth	Filter	 Block
2			

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 35

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 39

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 40

.....

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](#)