

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

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 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 all its interfaces and port1 will be enabled 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

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 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

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 7

Refer to the exhibit.

Profile Name
Monitoring_Access
NOC_Access
prof_admin
super_admin

The NOC team connects to the FortiGate GUI with the NOC_Access admin 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 admin timeout value under config system accprofile NOC_Access.

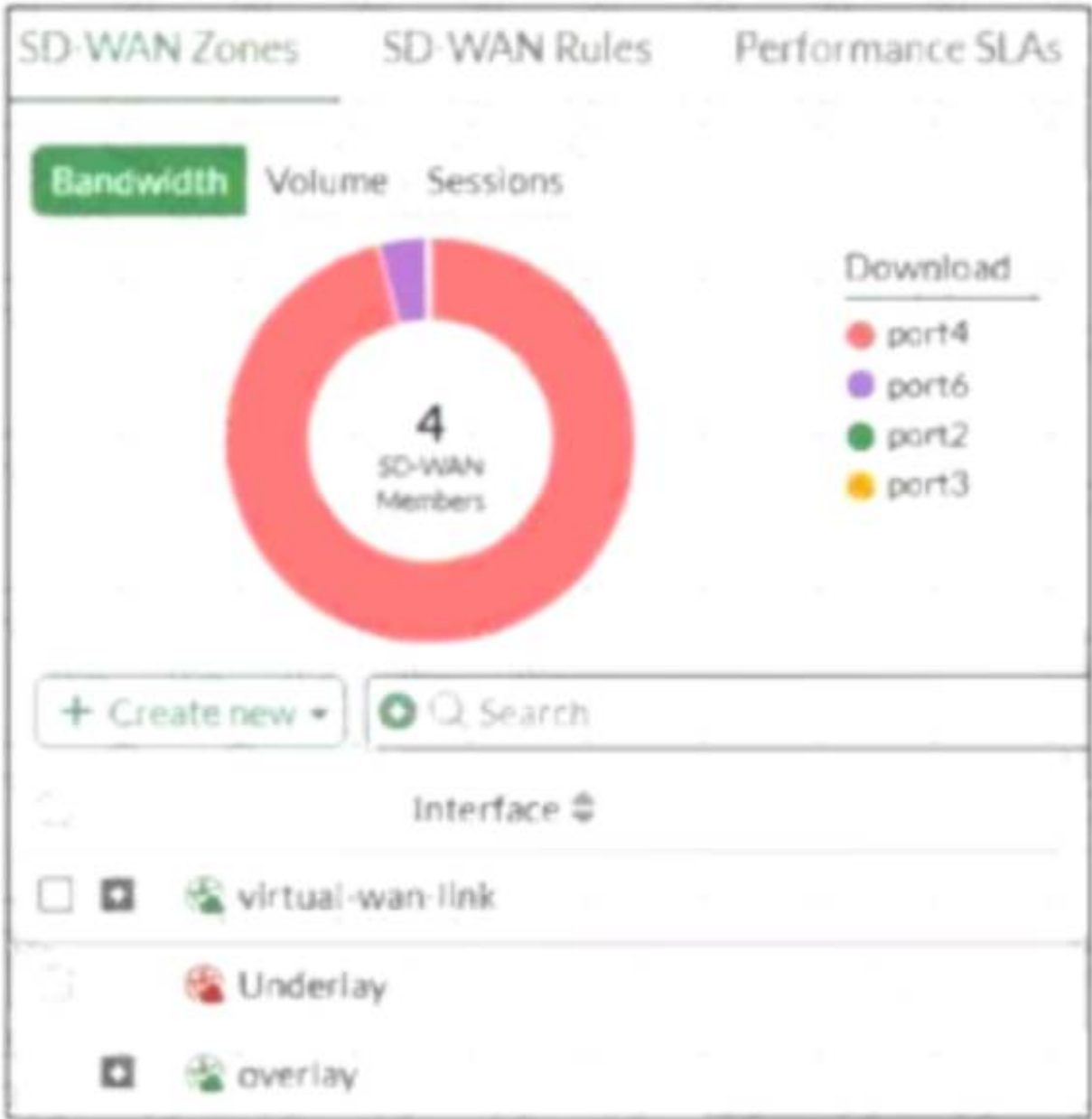
Answer: D

Explanation:

The admin timeout 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 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.

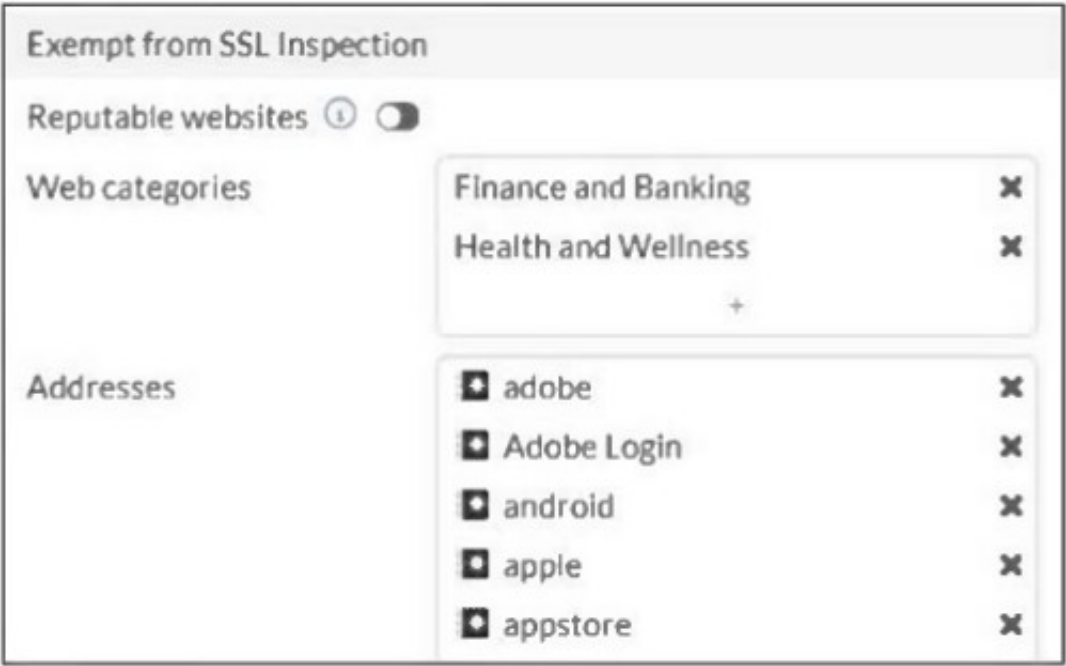
Answer: A

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, 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 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 14

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 18

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 23

A new administrator is configuring FSSO authentication on FortiGate using DC Agent Mode. Which step is NOT part of the expected process?

- A. The DC agent sends login event data directly to FortiGate.
- B. The user logs into the windows domain.
- C. The collector agent forwards login event data to FortiGate.
- D. FortiGate determines user identity based on the IP address in the FSSO list.

Answer: C

Explanation:

In DC Agent Mode, the DC agent sends login event data directly to FortiGate without involving a collector agent.

NEW QUESTION 24

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

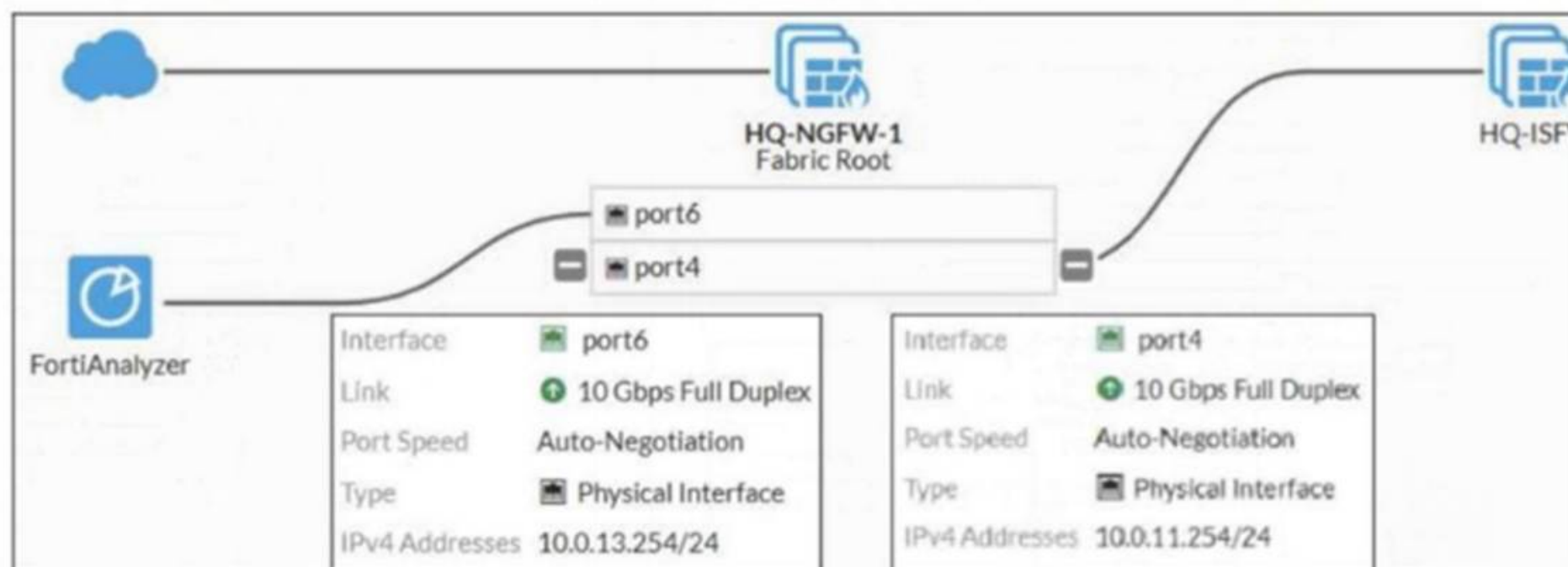
Explanation:

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 25

Refer to the exhibits.

Security Fabric logical topology view



Security Fabric settings on HQ-ISFW-2

Security Fabric Settings

Security Fabric role: Standalone | Serve as Fabric Root | **Join Existing Fabric**

Allow other Security Fabric devices to join: ☒ port6 +

Upstream FortiGate IP/FQDN:

Allow downstream device REST API access: ☒

Management IP/FQDN: Specify

Management port: Specify

SAML SSO Settings

SAML Single Sign-On: **Auto** | Manual

Advanced Options

Mode: Pending

An administrator wants to add HQ-ISFW-2 in the Security Fabric. HQ-ISFW-2 is in the same subnet as HQ-ISFW. After configuring the Security Fabric settings on HQ-ISFW-2, the status stays Pending. What can be the two possible reasons? (Choose two.)

- A. Upstream FortiGate IP must be set to 10.0.11.254.
- B. SAML Single Sign-On must be set to Manual.
- C. HQ-ISFW-2 must be authorized on HQ-ISFW.
- D. Management IP must be set to 10.0.13.254.

Answer: AC

Explanation:

The Upstream FortiGate IP should match the IP address of the Fabric Root interface, which is 10.0.11.254, not 10.0.13.254.

The new device (HQ-ISFW-2) must be authorized on the Fabric Root (HQ-ISFW) before it can join the Security Fabric, otherwise the status remains pending.

NEW QUESTION 29

Which three statements about SD-WAN performance SLAs are true? (Choose three.)

- A. They rely on session loss and jitter.
- B. They can be measured actively or passively.

- C. They are applied in a SD-WAN rule lowest cost strategy.
- D. They monitor the state of the FortiGate device.
- E. All the SLA targets can be configured.

Answer: ABE

Explanation:

SD-WAN SLAs monitor metrics like packet loss and jitter to evaluate link performance. SLA measurements can be performed using active probing or passive monitoring. Administrators can configure all SLA target parameters to define performance criteria.

NEW QUESTION 34

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 39

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 40

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 43

Which three statements explain a flow-based antivirus profile? (Choose three.)

- A. FortiGate buffers the whole file but transmits to the client at the same time.
- B. Flow-based inspection uses a hybrid of the scanning modes available in proxy-based inspection.
- C. If a virus is detected, the last packet is delivered to the client.
- D. Flow-based inspection optimizes performance compared to proxy-based inspection.
- E. The IPS engine handles the process as a standalone.

Answer: ABD

Explanation:

Flow-based antivirus buffers the entire file while simultaneously transmitting data to the client to minimize latency.

Flow-based inspection combines multiple scanning techniques from proxy-based modes for efficient detection. Flow-based inspection provides better performance by processing traffic on the fly without full proxy overhead.

NEW QUESTION 48

.....

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