NSE4_FGT-7.2^{Q&As}

Fortinet NSE 4 - FortiOS 7.2

Pass Fortinet NSE4_FGT-7.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/nse4_fgt-7-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet
Official Exam Center

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

Which two statements are true about the FGCP protocol? (Choose two.)

A. FGCP elects the primary FortiGate device.

B. FGCP is not used when FortiGate is in transparent mode.

C. FGCP runs only over the heartbeat links.

D. FGCP is used to discover FortiGate devices in different HA groups.

Correct Answer: AC

The FGCP (FortiGate Clustering Protocol) is a protocol that is used to manage high availability (HA) clusters of FortiGate devices. It performs several functions, including the following:

FGCP elects the primary FortiGate device: In an HA cluster, FGCP is used to determine which FortiGate device will be the primary device, responsible for handling traffic and making decisions about what to allow or block. FGCP uses a

variety of factors, such as the device\\'s priority, to determine which device should be the primary.

FGCP runs only over the heartbeat links: FGCP communicates between FortiGate devices in the HA cluster using the heartbeat links. These are dedicated links that are used to exchange status and control information between the devices.

FGCP does not run over other types of links, such as data links.

Reference:

https://docs.fortinet.com/document/fortigate/6.4.0/ports-and-protocols/564712/fgcp-fortigate-clustering-protocol

FortiGate Infrastructure 7.2 Study Guide (p.292): "FortiGate HA uses the Fortinet- proprietary FortiGate Clustering Protocol (FGCP) to discover members, elect the primary FortiGate, synchronize data among members, and monitor the health

of members. To discover and monitor members, the members broadcast heartbeat packets over all configured heartbeat interfaces."

QUESTION 2

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 fails to come up. The administrator has also re-entered the pre-shared key on both FortiGate devices to make sure they match.
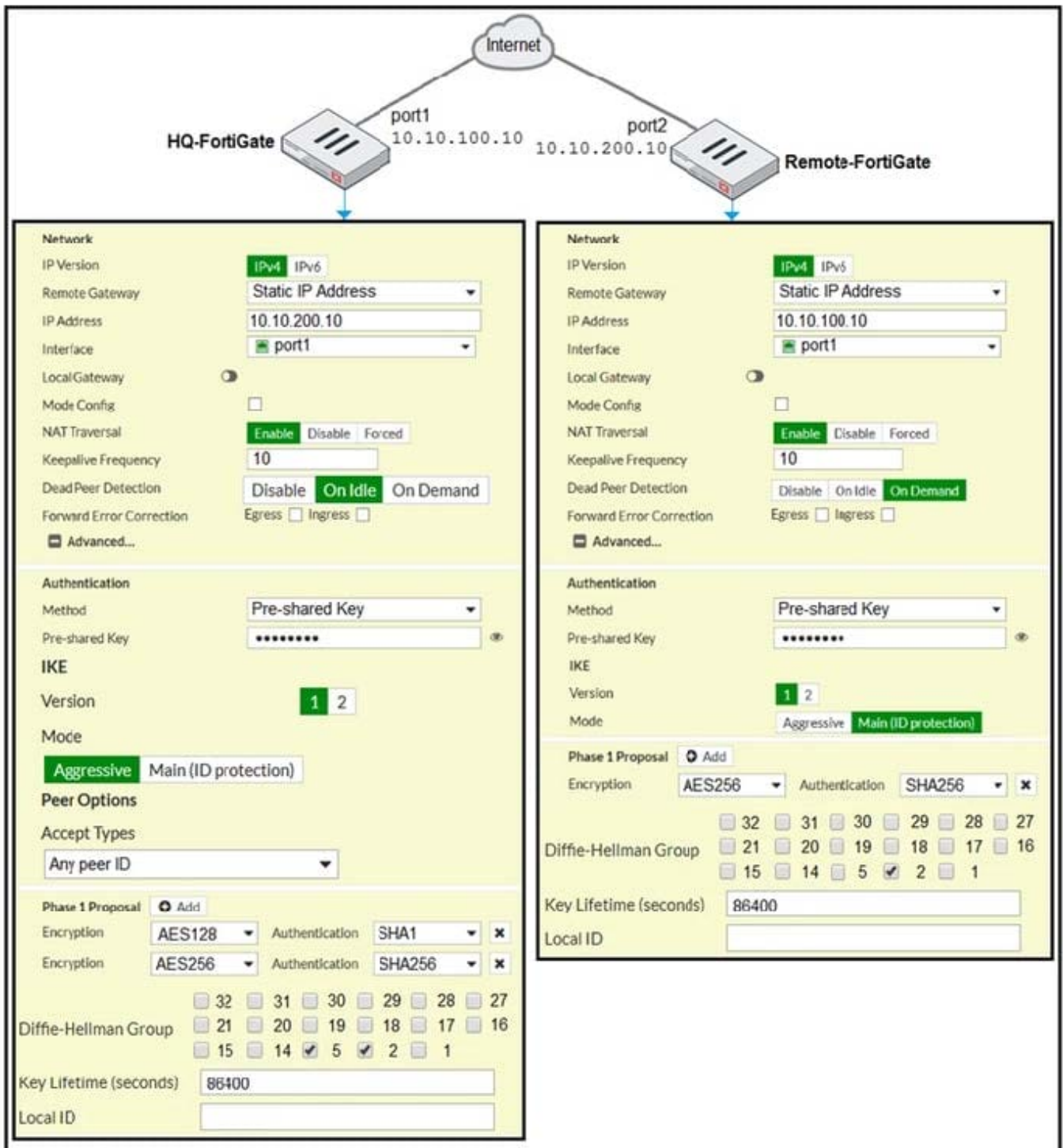
Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes will bring phase 1 up? (Choose two.)

A. On HQ-FortiGate, set IKE mode to Main (ID protection).

B. On both FortiGate devices, set Dead Peer Detection to On Demand.

C. On HQ-FortiGate, disable Diffie-Helman group 2.

D. On Remote-FortiGate, set port2 as Interface.

Correct Answer: AD

"In IKEv1, there are two possible modes in which the IKE SA negotiation can take place:

main, and aggressive mode. Settings on both ends must agree; otherwise, phase 1 negotiation fails and both IPsec peers are not able to establish a secure channel."

QUESTION 3

An administrator does not want to report the logon events of service accounts to FortiGate. What setting on the collector agent is required to achieve this?

A. Add the support of NTLM authentication.

B. Add user accounts to Active Directory (AD).

C. Add user accounts to the FortiGate group fitter.

D. Add user accounts to the Ignore User List.

Correct Answer: D

Reference: https://community.fortinet.com/t5/Support-Forum/Collector-Agent-and-problem-getting-login-info/m-p/95481

QUESTION 4

You have enabled logging on a FortiGate device for event logs and all security logs, and you have set up logging to use the FortiGate local disk. What is the default behavior when the local disk is full?

A. No new log is recorded after the warning is issued when log disk use reaches the threshold of 95%.

B. No new log is recorded until you manually clear logs from the local disk.

C. Logs are overwritten and the first warning is issued when log disk use reaches the threshold of 75%.

D. Logs are overwritten and the only warning is issued when log disk use reaches the threshold of 95%.

Correct Answer: C

config log disk setting

set diskfull [overwrite | nolog]

Action to take when disk is full. The system can overwrite the oldest log messages or stop logging when the disk is full. (default --> overwrite)

config log memory global-setting

set full-first-warning-threshold {integer}

Log full first warning threshold as a percent. (default --> 75) Reference:

https://docs.fortinet.com/document/fortigate/7.2.5/cli-reference/421620/config-log-disk- setting

https://docs.fortinet.com/document/fortigate/7.2.5/cli-reference/418620/config-log-memory- global-setting

Logs are overwritten and the first warning is issued when log disk use reaches the threshold of 75%.

This is true because this is the default behavior of FortiGate when logging to the local disk. The local disk is the internal storage of FortiGate that can be used to store event logs and security logs. When the local disk is full, FortiGate will

overwrite the oldest logs with the newest ones, and issue warnings at different thresholds of disk usage. The first warning is issued when log disk use reaches 75%, the second warning is issued when log disk use reaches 85%, and the final

warning is issued when log disk use reaches 95%. The administrator can configure these thresholds and the action to take when the disk is full using the CLI command config log disk setting1

QUESTION 5

Which feature in the Security Fabric takes one or more actions based on event triggers?

A. Fabric Connectors

B. Automation Stitches

C. Security Rating

D. Logical Topology

Correct Answer: B

Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/286973/fortinet-security-fabric