Free Questions for NSE4_FGT-7.2 by braindumpscollection

Shared by Giles on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Which of the following are purposes of NAT traversal in IPsec? (Choose two.)

Options:

A- To detect intermediary NAT devices in the tunnel path.

B- To dynamically change phase 1 negotiation mode aggressive mode.

C- To encapsulation ESP packets in UDP packets using port 4500.

D- To force a new DH exchange with each phase 2 rekey.

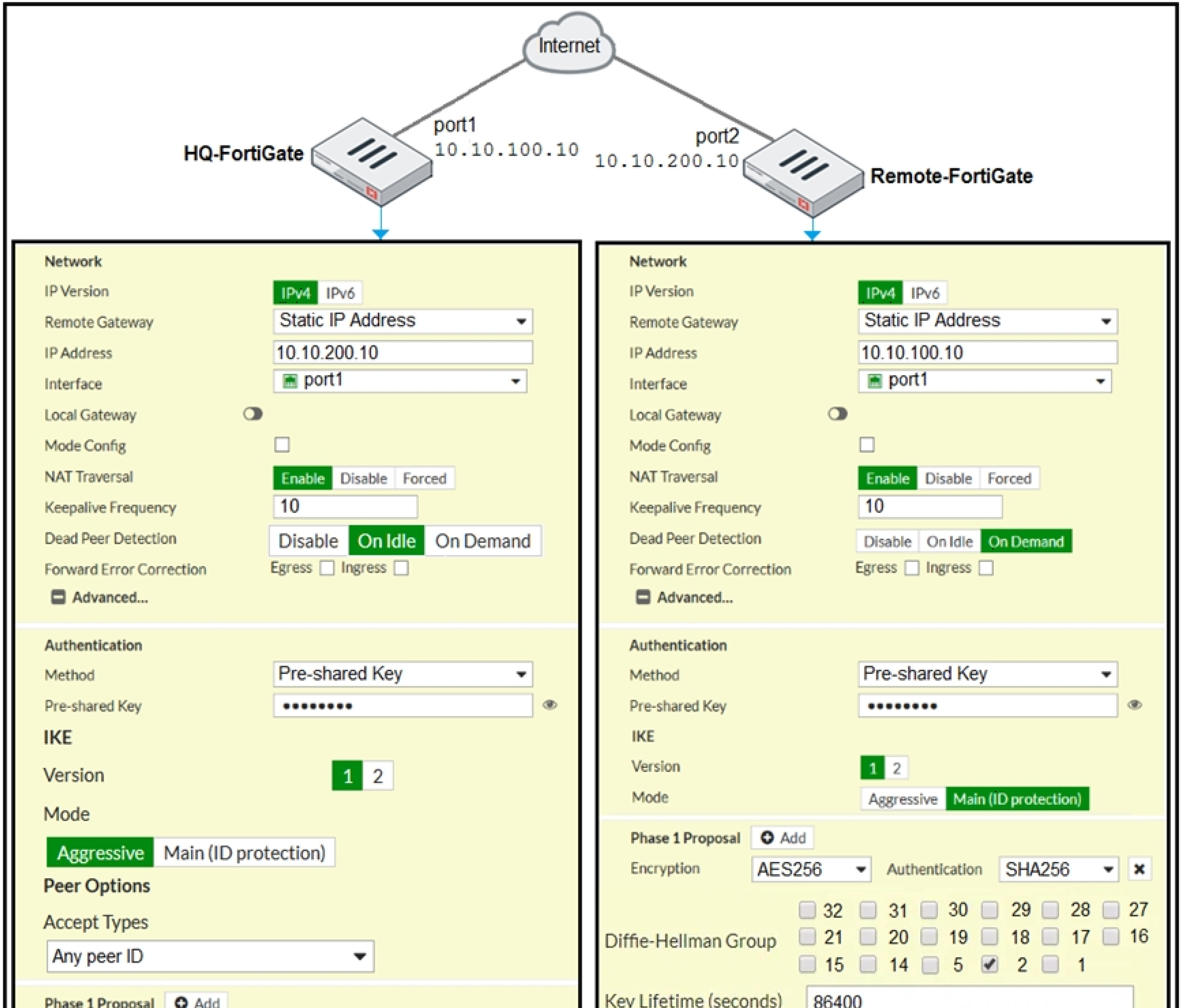
Answer:

A, C

Question 2

Question Type: **MultipleChoice**

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.



Network

IP Version	[✓ IPv4] IPv6
Remote Gateway	Static IP Address ▾
IP Address	10.10.200.10
Interface	port1 ▾
Local Gateway	○
Mode Config	□
NAT Traversal	[✓ Enable] Disable Forced
Keepalive Frequency	10
Dead Peer Detection	Disable [✓ On Idle] On Demand
Forward Error Correction	Egress □ Ingress □

⊟ Advanced...

Authentication

Method	Pre-shared Key ▾
Pre-shared Key	•••••••••

IKE

Version	[✓ 1] 2
Mode	[✓ Aggressive] Main (ID protection)

Peer Options

Accept Types

Any peer ID ▾

Phase 1 Proposal ⊕ Add

Network

IP Version	[✓ IPv4] IPv6
Remote Gateway	Static IP Address ▾
IP Address	10.10.100.10
Interface	port1 ▾
Local Gateway	○
Mode Config	□
NAT Traversal	[✓ Enable] Disable Forced
Keepalive Frequency	10
Dead Peer Detection	Disable On Idle [✓ On Demand]
Forward Error Correction	Egress □ Ingress □

⊟ Advanced...

Authentication

Method	Pre-shared Key ▾
Pre-shared Key	•••••••••

IKE

Version	[✓ 1] 2
Mode	Aggressive [✓ Main (ID protection)]

Phase 1 Proposal ⊕ Add

Encryption AES256 ▾ Authentication SHA256 ▾ ✖

Diffie-Hellman Group

□ 32	□ 31	□ 30	□ 29	□ 28	□ 27
□ 21	□ 20	□ 19	□ 18	□ 17	□ 16
□ 15	□ 14	□ 5	☑ 2	□ 1	

Key Lifetime (seconds) 86400

Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes will bring phase 1 up? (Choose two.)

Options:

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.

Answer:

A, D

Explanation:

'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

Question Type: **MultipleChoice**

Which of the following conditions must be met in order for a web browser to trust a web server certificate signed by a third-party CA?

Options:

A- The public key of the web server certificate must be installed on the browser.

B- The web-server certificate must be installed on the browser.

C- The CA certificate that signed the web-server certificate must be installed on the browser.

D- The private key of the CA certificate that signed the browser certificate must be installed on the browser.

Answer:

C

Question 4

Question Type: **MultipleChoice**

An administrator has configured two-factor authentication to strengthen SSL VPN access. Which additional best practice can an administrator implement?

Options:

A- Configure Source IP Pools.

B- Configure split tunneling in tunnel mode.

C- Configure different SSL VPN realms.

D- Configure host check .

Answer:

D

Question 5

Question Type: **MultipleChoice**

Which two statements ate true about the Security Fabric rating? (Choose two.)

Options:

A- It provides executive summaries of the four largest areas of security focus.

B- Many of the security issues can be fixed immediately by clicking Apply where available.

C- The Security Fabric rating must be run on the root FortiGate device in the Security Fabric.

D- The Security Fabric rating is a free service that comes bundled with alt FortiGate devices.

Answer:

B, C

Question 6

Question Type: **MultipleChoice**

Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

Options:

A- The firmware image must be manually uploaded to each FortiGate.

B- Only secondary FortiGate devices are rebooted.

C- Uninterruptable upgrade is enabled by default.

D- Traffic load balancing is temporally disabled while upgrading the firmware.

Answer:

C, D

Question 7

Question Type: **MultipleChoice**

When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

Options:

A- Log ID

B- Universally Unique Identifier

C- Policy ID

D- Sequence ID

Answer:

B

Explanation:

FortiGate Security 7.2 Study Guide (p.67): 'When creating firewall objects or policies, a universally unique identifier (UUID) attribute is added so that logs can record these UUIDs and improve functionality when integrating with FortiManager or FortiAnalyzer.'

Question 8

Question Type: MultipleChoice

Which statement about the IP authentication header (AH) used by IPsec is true?

Options:

A- AH does not provide any data integrity or encryption.

B- AH does not support perfect forward secrecy.

C- AH provides data integrity bur no encryption.

D- AH provides strong data integrity but weak encryption.

Answer:

C

Question 9

Question Type: **MultipleChoice**

If Internet Service is already selected as Source in a firewall policy, which other configuration objects can be added to the Source filed of a firewall policy?

Options:

A- IP address

B- Once Internet Service is selected, no other object can be added

C- User or User Group

D- FQDN address

Answer:

B

Explanation:

https://docs.fortinet.com/document/fortigate/6.2.5/cookbook/179236/using-internet-service-in-policy

Question 10

Question Type: MultipleChoice

The HTTP inspection process in web filtering follows a specific order when multiple features are enabled in the web filter profile. What order must FortiGate use when the web filter profile has features enabled, such as safe search?

Options:

A- DNS-based web filter and proxy-based web filter

B- Static URL filter, FortiGuard category filter, and advanced filters

C- Static domain filter, SSL inspection filter, and external connectors filters

D- FortiGuard category filter and rating filter

Answer:

B

Explanation:

FortiGate Security 7.2 Study Guide (p.285): 'Remember that the web filtering profile has several features. So, if you have enabled many of them, the inspection order flows as follows: 1. The local static URL filter 2. FortiGuard category filtering (to determine a rating) 3. Advanced filters (such as safe search or removing Active X components)'

Question 11

Question Type: MultipleChoice

Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)

Options:

A- hard-timeout

B- auth-on-demand

C- soft-timeout

D- new-session

E- Idle-timeout

Answer:

A, D, E

Explanation:

https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221

Question 12

Question Type: **MultipleChoice**

Which two statements are correct regarding FortiGate HA cluster virtual IP addresses? (Choose two.)

Options:

A- Heartbeat interfaces have virtual IP addresses that are manually assigned.

B- A change in the virtual IP address happens when a FortiGate device joins or leaves the cluster.

C- Virtual IP addresses are used to distinguish between cluster members.

D- The primary device in the cluster is always assigned IP address 169.254.0.1.

Answer:

B, D

20%
DISCOUNT