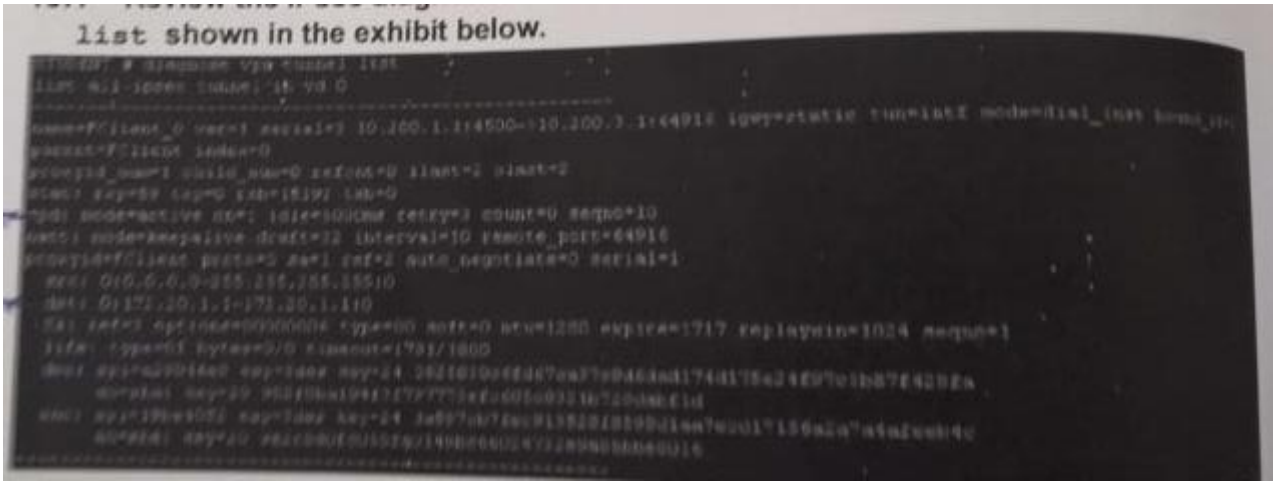
Question NSE4 : VPN IPsec (pg. 38-47)

157. Examinez la sortie de diagnostic IPsec de la commande "*diagnose vpn tunnel list*" illustrée dans l'exposition ci-dessous.

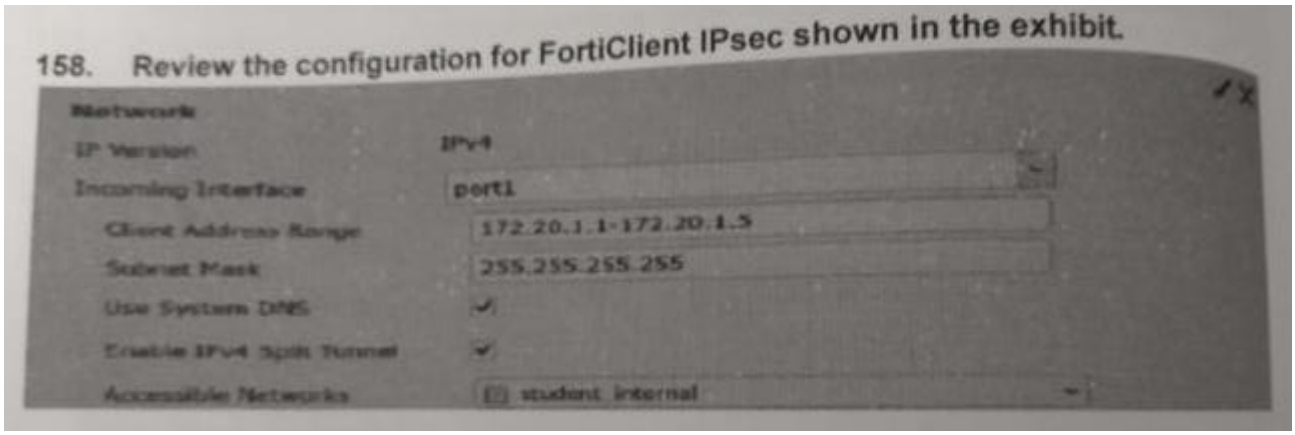


Quelles déclarations sont correctes concernant cette sortie ?

Le client qui se connecte a reçu l'adresse 172.20.1.1

Dans les paramètres de la phase 1, la détection deadpeer est activée.

158. Passez en revue la configuration de FortiClient IPsec présentée dans l'exposition.



Quelle affirmation est correcte concernant cette configuration ?

Le client VPN qui se connecte installera une route vers une destination correspondant à l'objet « student internal ».

159. Quel mode IPsec inclut les informations d'identification de pair dans le premier paquet ?

Aggressive mode.

160. Vous êtes l'administrateur en charge d'un VPN IPsec point à point entre deux unités FortiGate utilisant le mode route-based. Les utilisateurs de chaque côté doivent pouvoir initier de nouvelles sessions sans aucune restriction. Il n'y a qu'un seul sous-réseau à chaque extrémité et le

FortiGate a déjà une route par défaut. Quelles sont les deux étapes de configuration nécessaires dans chaque FortiGate pour atteindre ces objectifs ?

Créer 2 politiques de pares-feux.

Ajouter une route au sous-réseau distant.

161. Un administrateur souhaite créer un tunnel VPN IPsec entre deux appareils FortiGate. Quelles sont les trois étapes de configuration à effectuer sur les deux unités pour prendre en charge ce scénario ?

Créez des politiques de pare-feu pour autoriser et contrôler le trafic entre les adresses IP source et de destination.

Définir les paramètres de la phase 1 et 2

162. Quelle action une passerelle IPsec effectue-t-elle avec le trafic utilisateur acheminé vers un VPN IPsec lorsqu'il ne correspond à aucun sélecteur de Quick mode de phase 2 ?

Le trafic est abandonné

163. Parmi les méthodes d'authentification suivantes, lesquelles sont prises en charge dans une phase IPsec 1

Signature RSA - Clés pré-partagées

164. Lequel des modes de configuration IPsec suivants peut être utilisé pour implémenter des VPN L2TP sur IPSec ?

Policy-based & route-based VPN

165. Lequel des modes de configuration IPsec suivants peut être utilisé lorsque le FortiGate fonctionne en mode NAT ?

Policy-based & route-based VPN

166. Laquelle des affirmations suivantes est vraie concernant les différences entre les VPN IPsec policy-based & route-based ?

Les politiques de pare-feu pour "policy-based" sont bidirectionnelles. Les politiques de pare-feu pour "route-based" sont unidirectionnelles

Les actions pour les politiques de pare-feu pour les VPN " route-based" peuvent être Accepter ou Refuser, les politiques de pare-feu pour les VPN "policy-based" sont crypté.

167. Quelle partie de la configuration un administrateur spécifie-t-il le type de configuration IPsec (que ça soit policy-based ou route-based) ?

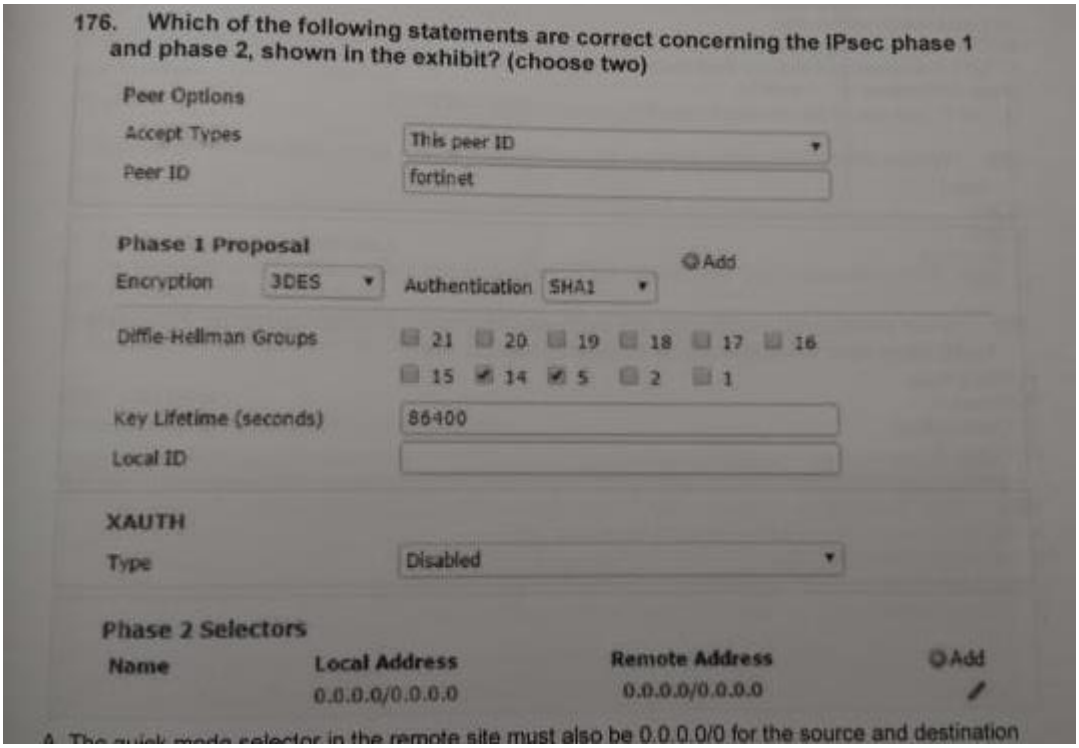
Sous les paramètres globaux du VPN IPsec.

168. Laquelle des options suivantes définit le mieux ce qu'est Diffie-Hellman ?

Un protocole d'accord clé.

169. Combien de paquets sont échangés entre les deux extrémités IPSec lors de la négociation d'une phase 1 en mode principal ?
6
170. Lequel des modes IKE suivants est celui utilisé lors de la négociation IPsec phase 2 ?
Quick mode
171. Parmi les affirmations suivantes, lesquelles sont vraies concernant le VPN IPsec ?
IPsec augmente la surcharge et la bande passante.
IPsec protège les protocoles de couche supérieure.
IPsec fonctionne au niveau 3 du modèle OSI.
172. Parmi les affirmations suivantes, lesquelles sont correctes concernant les configurations VPN commutées IPsec pour les appareils FortiGate ?
L'ID de pair doit être utilisé lorsqu'il y a plus d'un VPN commuté IPsec en mode agressif sur le même appareil FortiGate.
Le FortiGate ajoutera automatiquement une route statique à l'adresse du sélecteur quick mode source reçue de chaque pair distant
173. Laquelle des combinaisons suivantes de deux configurations d'appareils FortiGate (côtés A et B) peut être utilisée pour établir avec succès un VPN IPsec entre eux ?
Côté A : main mode, passerelle distante avec adresse IP statique, VPN policy-based.
Côté B : main mode, passerelle distante avec adresse IP statique, VPN route-based.
174. Quelle affirmation est correcte concernant un VPN IPsec avec le paramètre de passerelle distante configuré en "DNS dynamique" ?
L'adresse IP de la passerelle distante peut changer dynamiquement.
175. Parmi les affirmations suivantes, lesquelles sont correctes concernant la configuration du mode IKE ?
Il peut attribuer dynamiquement des adresses IP aux clients VPN IPsec
Il peut attribuer dynamiquement des paramètres DNS aux clients VPN IPsec.

176. Parmi les affirmations suivantes, lesquelles sont correctes concernant les phases 1 et 2 d'IPsec, présentées dans l'illustration ?



L'appareil FortiGate ajoutera automatiquement une route statique à l'adresse du sélecteur de mode rapide source reçue de chaque pair VPN distant.

La configuration fonctionnera uniquement pour établir des tunnels FortiClient vers FortiGate. Un tunnel FortiGate nécessite une configuration différente.

177. L’image montre une sortie de "diagnose debug application IKE 255", prise lors de l'établissement d'un VPN. Parmi les affirmations suivantes, lesquelles sont correctes concernant cette sortie ?

La sortie correspond à une négociation phase 2

178. Parmi les protocoles suivants, lequel est défini dans la norme IPsec ?

ESP – AH

179. Quels objets de configuration sont automatiquement ajoutés lors de l'utilisation de l'assistant de configuration FortiClient VPN de FortiGate ?

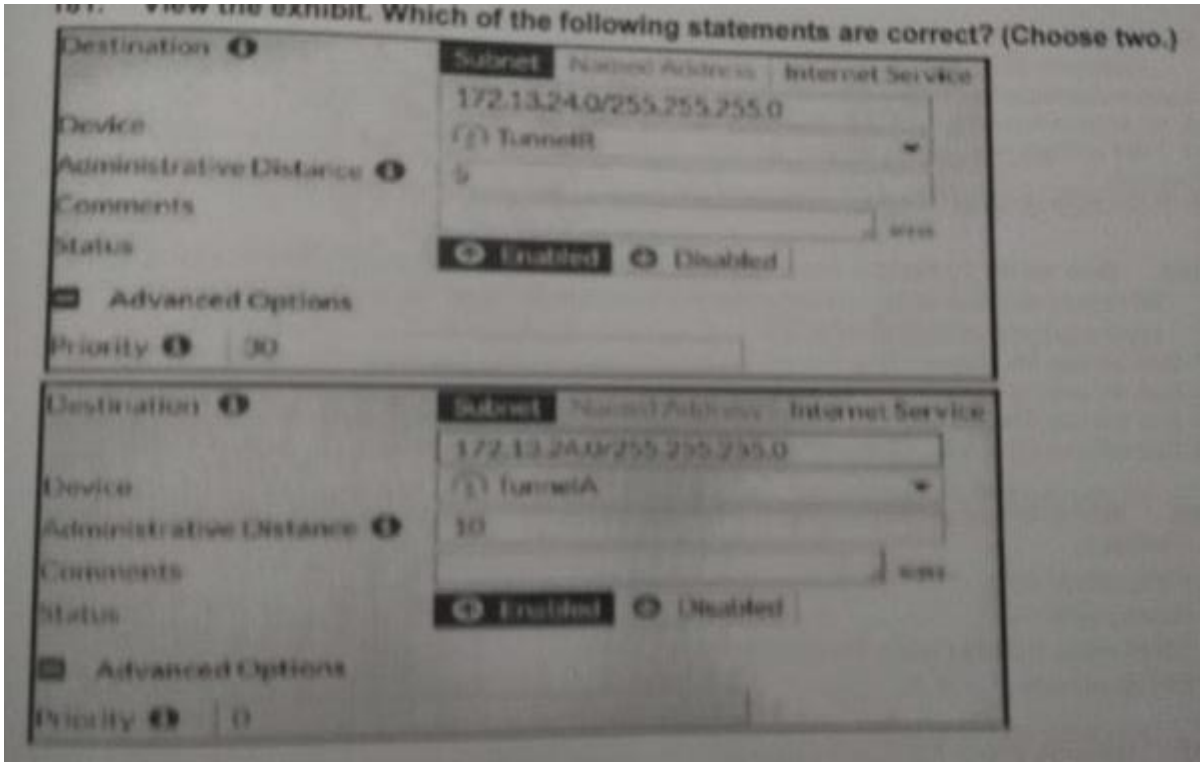
Phase 1 et 2

180. A quoi sert la traversée NAT dans IPsec ?

Pour détecter les périphériques NAT intermédiaires dans le chemin du tunnel.

Pour encapsuler des paquets ESP dans des paquets UDP à l'aide du port 4500.

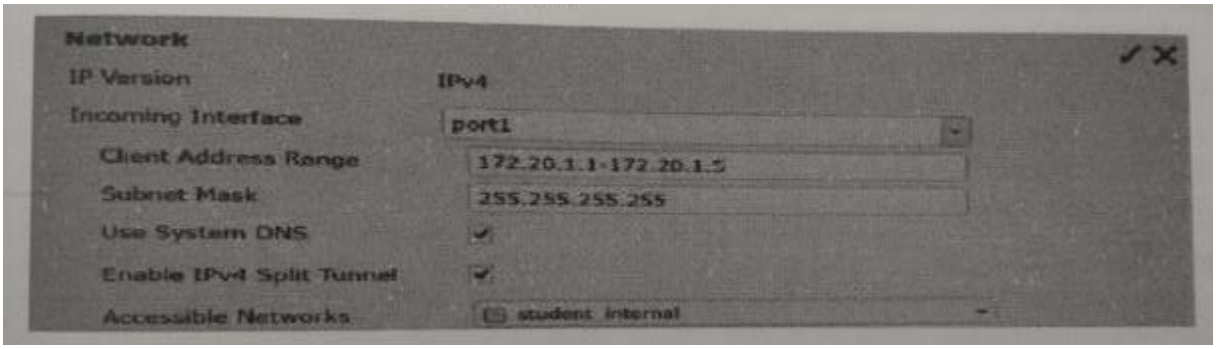
181. Parmi les affirmations suivantes, lesquelles sont correctes ?



Il s'agit d'une configuration IPsec redondante.

La route Tunnel B est la principale pour rechercher le site distant. La route du tunnel A est utilisée uniquement si le VPN du tunnel B est en panne.

182. Parmi les affirmations suivantes, laquelle est correcte ?



Le client VPN qui se connecte installera une route vers une destination correspondant à l'objet « student internal ».

183. Lequel des énoncés suivants décrit certaines des différences entre la cryptographie symétrique et asymétrique ?

La cryptographie symétrique utilise une clé pré-partagée. La cryptographie asymétrique utilise une paire ou des clés.

Des clés asymétriques peuvent être envoyées au pair distant via des certificats numériques. Les clés symétriques ne peuvent pas.

184. A Lequel des énoncés suivants décrit le mieux ce qu'est une autorité de certification publique ?

Un service qui valide les certificats numériques à des fins d'authentification basée sur des certificats.

185. Bob souhaite envoyer à Alice un fichier chiffré à l'aide de la cryptographie à clé publique. Laquelle des affirmations suivantes est correcte concernant l'utilisation de la cryptographie à clé publique dans ce scénario ?

Bob va utiliser la clé publique d'Alice pour chiffrer le fichier et Alice va utiliser sa clé privée pour déchiffrer le fichier.

186. Quel mode de configuration IPsec peut être utilisé pour implémenter des VPN GRE-over-IPsec ?

Route-based

187. Qu'est-ce qu'un IPS Perfect Forwarding Secrecy (PFS) ?

Un paramétrage de phase 2 qui autorise le recalcul d'une nouvelle clé secrète commune à chaque expiration de la clé de session.

188. Un administrateur a configuré un VPN IPsec site-à-site en mode route-based. Quelle affirmation est correcte à propos de la configuration du VPN IPsec ?

Une interface virtuel IPsec a automatiquement été créé une fois la configuration de la phase 1 terminée.

189. Dans une configuration passerelle à passerelle IPsec, deux unités FortiGate créent un tunnel VPN entre deux réseaux privés distincts. Laquelle des étapes de configuration suivantes doit être effectuée sur les deux unités FortiGate pour prendre en charge cette configuration ?
Créez des politiques de pare-feu pour contrôler le trafic entre les adresses IP source et de destination.
Définir les paramètres de phase 2 dont l'unité FortiGate a besoin pour créer un tunnel VPN avec le pair distant.
Définir les paramètres de Phase 1 dont l'unité FortiGate a besoin pour authentifier les pairs distants.

190. Vous êtes l'administrateur responsable d'une unité FortiGate qui agit comme une passerelle VPN. Vous avez choisi d'utiliser le mode Interface lors de la configuration du tunnel VPN et vous souhaitez que les utilisateurs de chaque côté puissent initier de nouvelles sessions. Il n'y a qu'un seul sous-réseau à chaque extrémité et l'unité FortiGate a déjà une route par défaut. Parmi les étapes de configuration suivantes, lesquelles sont nécessaires pour atteindre ces objectifs ?
Créer 2 règles de pare-feu.
Ajouter une route pour le sous-réseau distant.
Créer une définition de phase 1 et 2.

191. Laquelle des affirmations suivantes doit être vraie pour qu'un certificat numérique soit valide ?
Il doit être signé par une autorité de certification "de confiance"
Il doit être encore dans sa période de validité.

192. Pourquoi devez-vous utiliser le mode agressif lorsqu'une passerelle FortiGate IPSec locale accède à plusieurs tunnels commutés ?
En mode agressif, les pairs distants peuvent fournir leurs identifiants de pairs dans le premier message.

193. Lesquelles des conditions suivantes sont requises pour établir un VPN IPsec entre deux appareils FortiGate ?

Si XAuth est activé en tant que serveur dans un pair, il doit être activé en tant que client dans l'autre pair.

Si le VPN est configuré en tant qu'utilisateur d'accès à distance dans un pair, il doit être configuré en tant qu'adresse IP statique ou DNS dynamique dans l'autre pair.

194. Au cours du processus de vérification numérique, la comparaison des résultats de hachage originaux satisfait à quelle exigence de sécurité ?

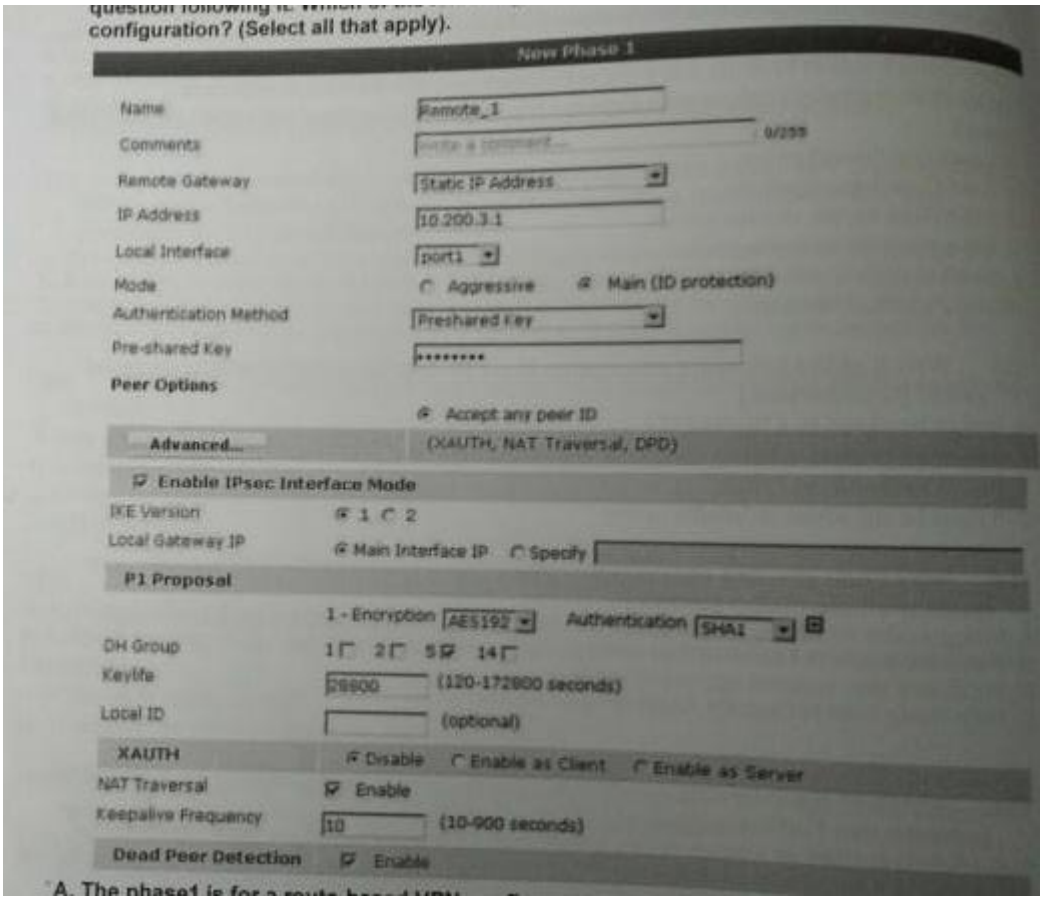
Intégrité des données

195. Parmi les affirmations suivantes concernant les tunnels IPsec basés sur des règles (policy-based), lesquelles sont correctes ?

Ils peuvent être configurés en modes de fonctionnement NAT/route et transparent.

Ils supportent L2TP-over-IPsec.

196. Examine l'image ci-dessous ; Laquelle des affirmations suivantes est vraie à propos de cette configuration ?



La phase 1 est pour une configuration VPN route-based.

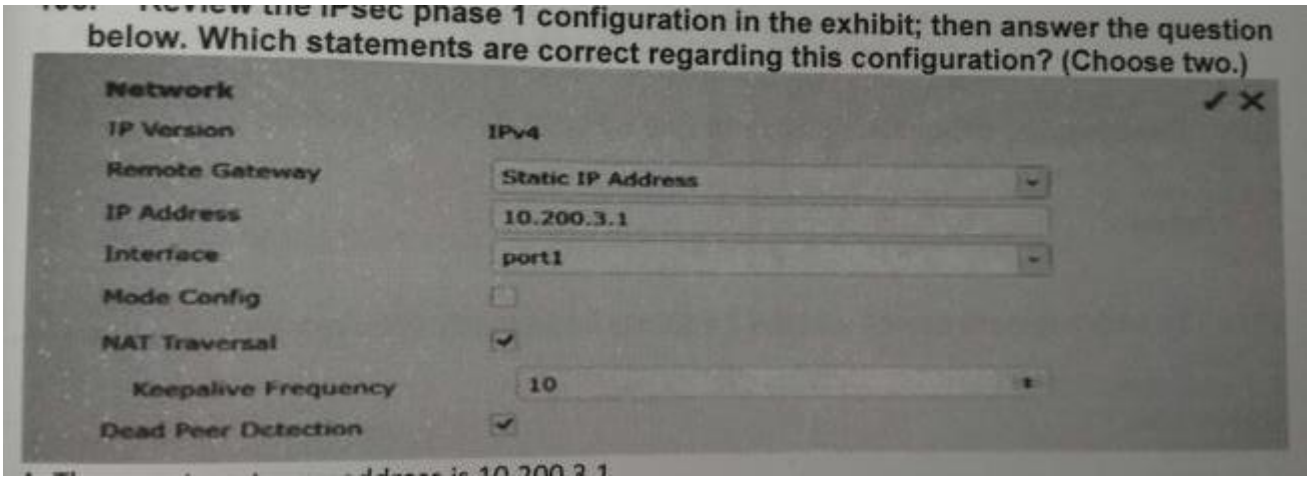
L'IP de la passerelle locale correspond aux adresses attribuées au port 1.

197. Passez en revue la configuration de route statique pour IPsec présentée dans l'image au-dessus ; puis répondez à la question ci-dessous. Quelles affirmations sont correctes concernant cette configuration ?

L'interface distante est une interface IPsec.

Une adresse de passerelle n'est pas nécessaire car l'interface est une connexion point à point.

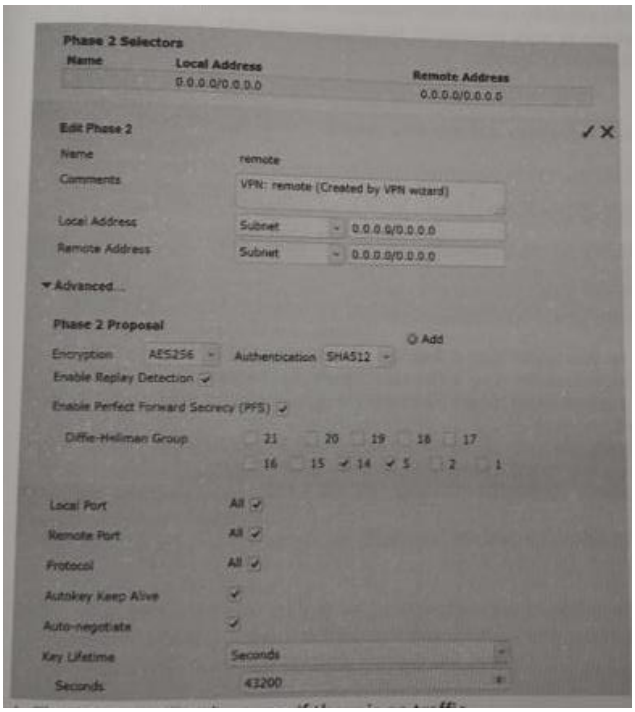
198. Passez en revue la configuration IPsec phase 1 dans l'image. Quelles déclarations sont correctes concernant cette configuration ?



La passerelle distante est 10.200.3.1

L'IP de la passerelle locale est l'adresse attribuée au port 1.

199. Quelles affirmations sont correctes concernant cette configuration ?



La phase va échanger des clés ? (re-key) même s'il n'y a pas de trafic.

Il y aura un échange DH pour chaque re-key.