

Question NSE4 : SSL VPN (pg. 57-65)

258. Comment le trafic est-il acheminé vers un tunnel SSL VPN du côté de l'unité FortiGate ?

L'attribution d'une adresse IP au client entraîne l'ajout d'une route hôte à la table de routage du noyau de l'unité FortiGate.

259. Lorsque le proxy SSL n'effectue pas d'interception intermédiaire (man-in-the-middle) du trafic SSL, quel champ de certificat peut être utilisé pour déterminer la notation d'un site Web

Nom commun

260. Concernant l'utilisation du VPN SSL en mode Web uniquement, quelle affirmation est correcte ?

Il nécessite que l'utilisateur dispose d'un navigateur Web prenant en charge la longueur de chiffrement 64 bits

261. Parmi les affirmations suivantes, lesquelles sont vraies concernant l'inspection de contenu SSL Man-in-the-middle ?

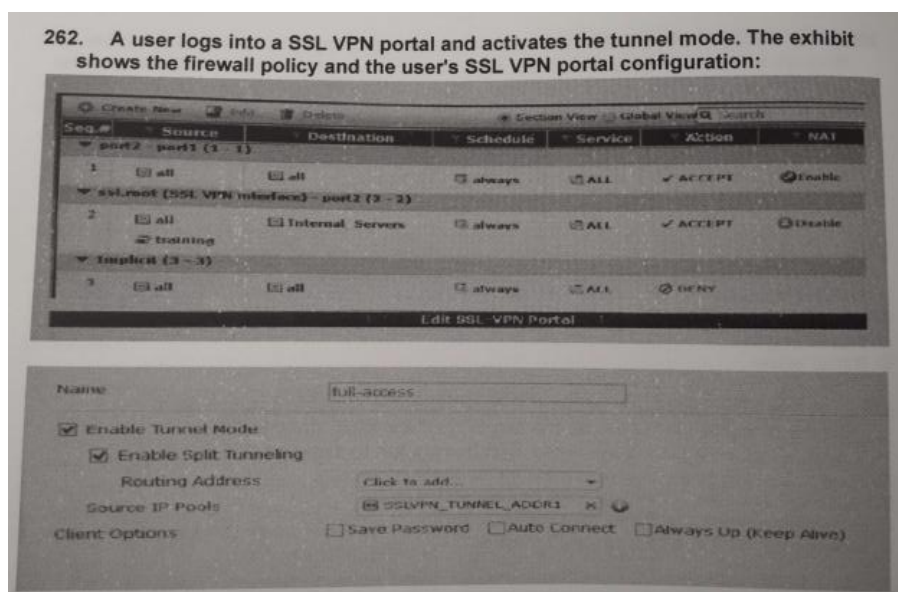
L'appareil FortiGate agit comme une sous-autorité de certification

Le certificat de service local du serveur Web doit être installé dans l'appareil FortiGate

Le certificat SSL Proxy requis doit d'abord être demandé à une autorité de certification publique (CA)

262. Un utilisateur se connecte à un portail VPN SSL et active le mode tunnel.

L'exposition montre la politique de pare-feu et la configuration du portail VPN SSL de l'utilisateur. Quelle route statique est automatiquement ajoutée à la table de routage du client lorsque le mode tunnel est activé ?



Une route vers un sous-réseau de destination correspondant à l'objet d'adresse Internal_Servers.

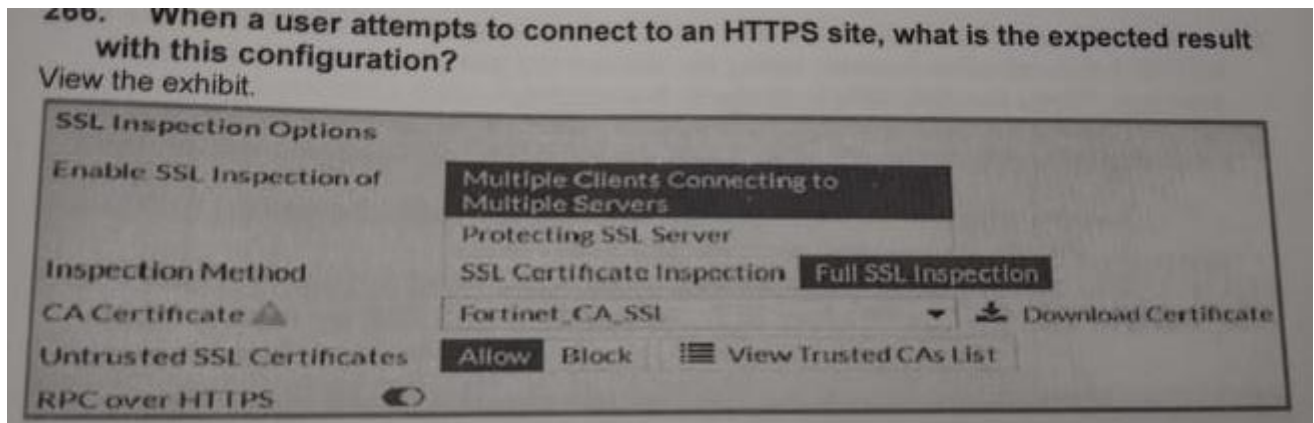
264. Lesquels des agents FSSO suivants sont requis pour une solution en mode agent DC ?

Agent DC - Collecteur DC

265. Quelle étape est requise par un VPN SSL pour accéder à un serveur interne en utilisant le mode de redirection de port ?

Configurer l'application cliente pour transférer le trafic IP vers un proxy d'applet Java

266. Une entreprise doit fournir un accès VPN SSL à deux groupes d'utilisateurs. L'entreprise doit également afficher différents messages de bienvenue sur l'écran de connexion SSL VPN pour les deux groupes d'utilisateurs. Que faut-il dans la configuration SSL VPN pour répondre à ces exigences ?



Différents domaines VPN SSL pour chaque groupe

267. Lorsqu'un utilisateur tente de se connecter à un site HTTPS, quel est le résultat attendu avec cette configuration ?

L'utilisateur reçoit des avertissements de certificat lors de la connexion à des sites qui ont des certificats SSL non approuvés

268. Un administrateur doit inspecter tout le trafic Web (y compris le trafic Web Internet) provenant des utilisateurs se connectant au VPN SSL. Comment cela peut-il être accompli ?

Désactivation du split tunneling

269. Comment un navigateur peut-il faire confiance à un certificat de serveur Web signé par une autorité de certification tierce ?

Le navigateur doit avoir le certificat de l'autorité de certification qui a signé le certificat du serveur Web installé

270. Lorsque vous naviguez vers un serveur Web interne à l'aide d'un signet VPN SSL en mode Web, quelle adresse IP est utilisée comme source de la requête HTTP ?

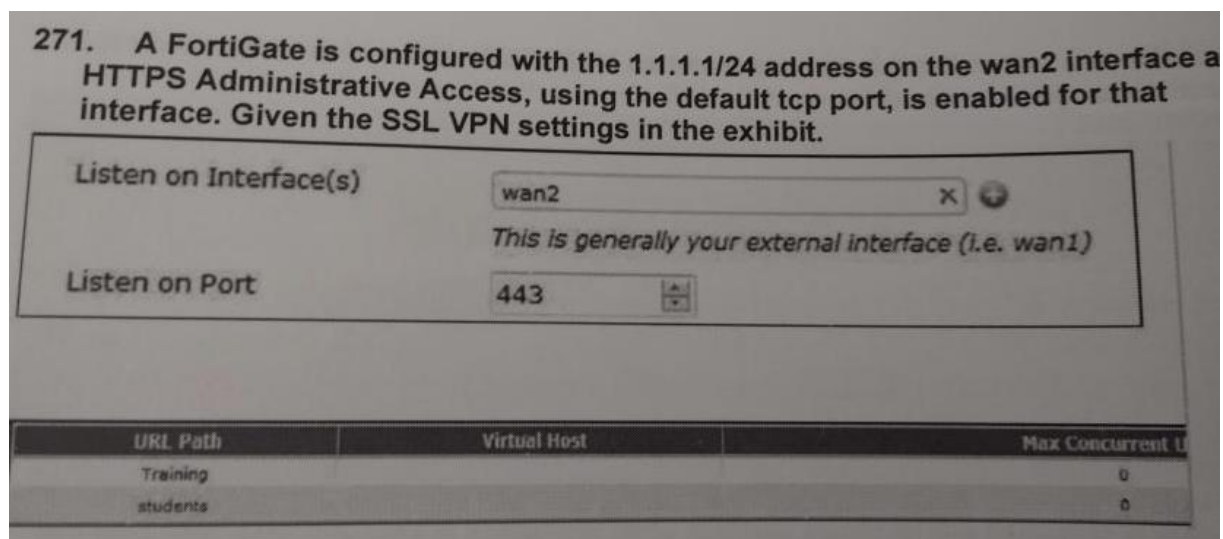
L'adresse IP interne de l'unité FortiGate.

271. Quelle affirmation décrit le mieux ce qu'est SSL.root ?

Le nom d'une interface virtuelle dans le VDOM racine d'où provient tout le trafic utilisateur du VPN SSL

272. Un FortiGate est configuré avec l'adresse 1.1.1.1/24 sur l'interface wan2 et l'accès administratif HTTPS, utilisant le port TCP par défaut, est activé pour cette interface. Compte tenu des paramètres VPN SSL dans l'exposition. Lequel si les URL de portail de connexion VPN SSL suivantes sont valides ?

271. A FortiGate is configured with the 1.1.1.1/24 address on the wan2 interface and HTTPS Administrative Access, using the default tcp port, is enabled for that interface. Given the SSL VPN settings in the exhibit.



URL Path	Virtual Host	Max Concurrent U
Training		0
students		0

<https://1.1.1.1:443/>

<https://1.1.1.1:443/STUDENTS>

273. Parmi les affirmations suivantes, lesquelles sont correctes concernant le mode SSL VPN Web uniquement ?

L'accès aux ressources du réseau interne est possible depuis le portail SSL VPN.

Le client VPN SSL FortiClient autonome NE PEUT PAS être utilisé pour établir un VPN SSL Web uniquement.

274. Laquelle des méthodes d'authentification suivantes peut être utilisée pour l'authentification VPN SSL ?

Authentification par mot de passe à distance (RADIUS, LDAP)

Authentification à deux facteurs

FSSO

275. Quelle affirmation décrit le mieux ce que fait le contrôle d'intégrité du client VPN SSL ?

Détecte les applications de sécurité du client Windows exécutées sur les PC du client SSL VPN

276. Quelle affirmation est incorrecte concernant le mode SSL VPN Tunnel ?

Un nombre limité d'applications IP est pris en charge

277. 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.

278. 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.

279. Parmi les affirmations suivantes, lesquelles sont vraies concernant le certificat proxy SSL qui doit être utilisé pour l'inspection du contenu SSL ?

Il doit avoir soit le champ "CA=true" soit le champ "Key Usage = KeyCertSign"

Il doit être installé dans l'appareil FortiGate

280. Parmi les affirmations suivantes, lesquelles sont vraies concernant les utilisateurs PKI créés dans un appareil FortiGate ?

Peut être utilisé pour l'authentification par jeton.

Peut être utilisé pour l'authentification à deux facteurs.

281. Lequel des énoncés suivants décrit le mieux ce qu'est une requête de signature de certificat (CSR) ?

Une demande soumise à une autorité de certification (CA) pour demander un certificat d'autorité de certification racine.

282. Laquelle des actions suivantes peut être utilisée pour sauvegarder les clés et les certificats numériques dans un appareil FortiGate ?

Effectuer une sauvegarde complète de la configuration FortiGate

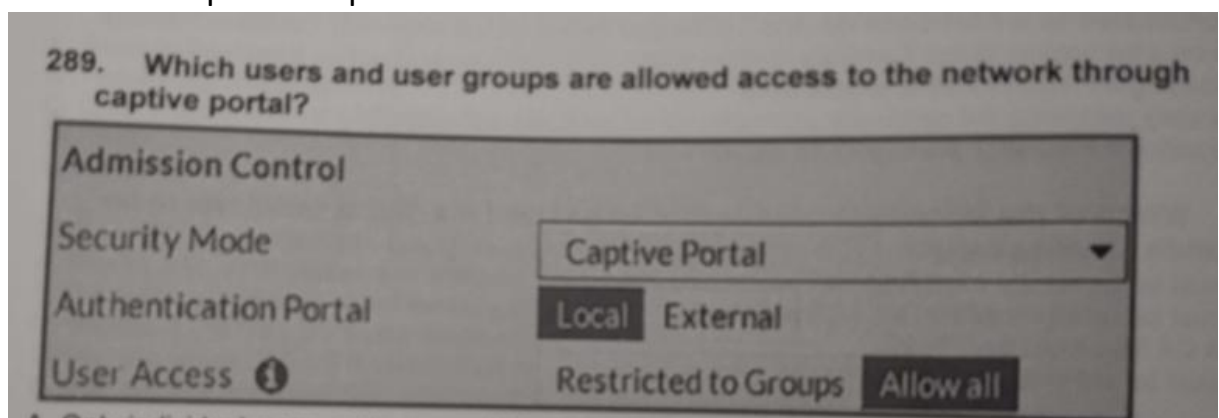
Téléchargement d'un fichier PKCS#12 sur un serveur TFTP

283. 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

284. Quelle affirmation est vraie concernant les minuteurs VPN SSL ?
- Permettre d'atténuer les attaques DoS (Deny of Service) à partir de requêtes HTTP partielles.
 - Empêcher les utilisateurs SSL VPN d'être déconnectés en raison d'une latence élevée du réseau.
285. Laquelle des conditions suivantes doit être remplie pour qu'un navigateur Web fasse confiance à un certificat de serveur Web signé par une autorité de certification tierce ?
- Le certificat CA qui a signé le certificat du serveur Web doit être installé sur le navigateur
286. L'épinglage de clé publique HTTP (HPKP) peut être un obstacle à la mise en œuvre d'une inspection SSL complète. Quelles solutions pourraient résoudre ce problème ?
- Remplacez les navigateurs Web par un autre qui ne prend pas en charge HPKP.
 - Exempte les sites Web qui utilisent HPKP de l'inspection SSL.
287. Laquelle des affirmations suivantes est vraie concernant les paramètres VPN SSL pour un portail VPN SSL ?
- Par défaut, le portail VPN SSL nécessite l'installation d'un certificat client
288. Quelle est la description correcte d'un résultat de hachage en ce qui concerne les certificats numériques ?
- Une valeur unique utilisée pour vérifier les données d'entrée.
289. Un administrateur doit créer une connexion SSL-VPN pour accéder à un serveur interne à l'aide du signet Port Forward. Quelle étape est requise pour cette configuration ? Configurer l'application cliente pour transférer le trafic IP vers un proxy d'applet Java
290. Quels utilisateurs et groupes d'utilisateurs sont autorisés à accéder au réseau via le portail captif ?



Utilisateurs et groupes définis dans la politique de pare-feu

291. Quelles sont les deux affirmations vraies concernant les VPN IPsec et les VPN SSL ?

Le VPN SSL crée une connexion HTTPS, pas IPsec.

Un VPN SSL ou un VPN IPsec peut être établi entre un poste de travail d'utilisateur final et un appareil FortiGate.

292. Concernant le VPN SSL en mode tunnel, quelles sont les trois affirmations correctes ?

Le split tunneling est pris en charge.

Il nécessite l'installation d'un client VPN.

Une adresse IP VPN SSL est attribuée dynamiquement au client par le boîtier FortiGate.

293. Quelles tâches relèvent de la responsabilité du proxy SSL dans une connexion HTTPS typique ?

La poignée de main (handshake) SSL du client Web.

La poignée de main (handshake) SSL du serveur Web.

294. Un client peut créer une connexion sécurisée à un appareil FortiGate en utilisant SSL VPN en mode Web uniquement. Laquelle des affirmations suivantes est correcte concernant l'utilisation du VPN SSL en mode Web uniquement ?

Le mode Web uniquement nécessite que l'utilisateur dispose d'un navigateur Web prenant en charge la longueur de chiffrement 64 bits.

295. Un client peut établir une connexion sécurisée à un réseau d'entreprise en utilisant SSL VPN en mode tunnel. Parmi les affirmations suivantes, lesquelles sont correctes concernant l'utilisation du VPN SSL en mode tunnel ?

Le split tunneling peut être activé lors de l'utilisation du VPN SSL en mode tunnel.

Un logiciel client est requis pour pouvoir utiliser un VPN SSL en mode tunnel

Les utilisateurs tentant de créer une connexion SSL VPN en mode tunnel doivent être authentifiés par au moins une politique SSL VPN.

L'adresse IP source utilisée par le client pour le VPN SSL en mode tunnel est attribuée par l'unité FortiGate.

296. Un problème peut éventuellement survenir lorsque vous cliquez sur Connecter pour démarrer le VPN SSL en mode tunnel. Le tunnel démarrera pendant quelques secondes, puis s'arrêtera. Parmi les affirmations suivantes, laquelle décrit le mieux comment résoudre ce problème ?

Cette unité FortiGate peut avoir plusieurs connexions Internet. Pour éviter ce problème, utilisez la commande CLI appropriée pour lier la connexion VPN SSL à l'interface entrante d'origine.

297. Une unité FortiGate peut créer une connexion sécurisée avec un client en utilisant SSL VPN en mode tunnel. Parmi les affirmations suivantes, lesquelles sont correctes concernant l'utilisation du VPN SSL en mode tunnel ?

Le split tunneling peut être activé lors de l'utilisation du VPN SSL en mode tunnel.

Le logiciel doit être téléchargé sur le client Web pour pouvoir utiliser un VPN SSL en mode tunnel.

Les utilisateurs tentant de créer une connexion VPN SSL en mode tunnel doivent être membres d'un groupe d'utilisateurs configuré sur l'unité FortiGate.

Le VPN SSL en mode tunnel nécessite l'installation du logiciel FortiClient sur l'ordinateur de l'utilisateur.

L'adresse IP source utilisée par le client pour le VPN SSL en mode tunnel est attribuée par l'unité FortiGate.

298. Un utilisateur final se connecte au portail SSL VPN et sélectionne l'option Tunnel Mode en cliquant sur le bouton "connecter". L'administrateur n'a pas activé le split tunneling et l'utilisateur final doit donc accéder à Internet via le tunnel VPN SSL. Quelles politiques de pare-feu sont nécessaires pour permettre à l'utilisateur final non seulement d'accéder au réseau interne mais aussi d'accéder à Internet ?

the internal network but also reach the internet

A.

	Status	ID	Source	Destination	Schedule	Service	Action
ssl.root -> internal (1)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2	all	all	always	ANY
ssl.root -> wan1 (1)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3	all	all	always	ANY
wan1 -> internal (1)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	all	all	always	ANY
Implicit (1)							

B.

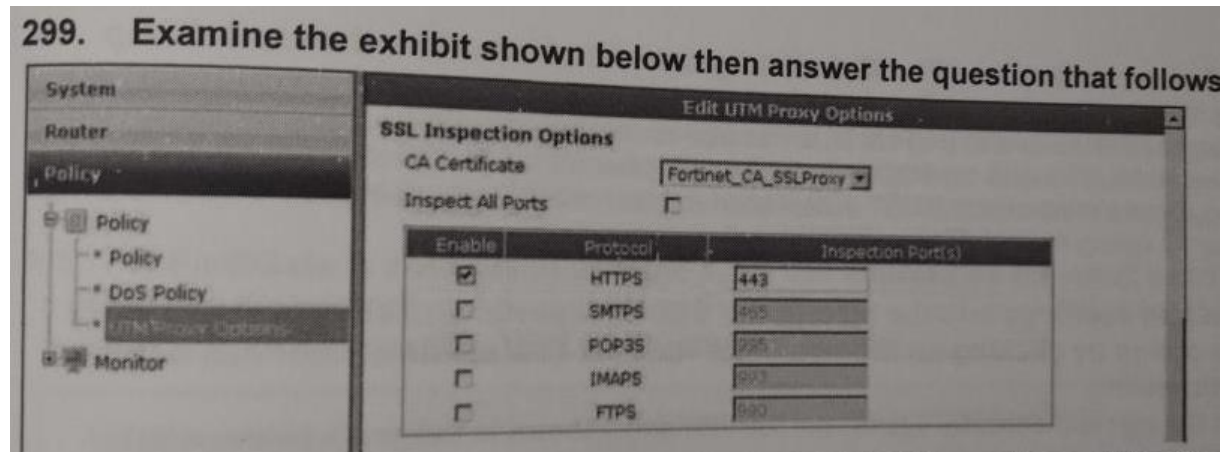
	Status	ID	Source	Destination	Schedule	Service	Action
ssl.root -> internal (1)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2	all	all	always	ANY
ssl.root -> wan1 (1)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3	all	all	always	ANY
wan1 -> internal (1)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	all	all	always	ANY
Implicit (1)							

C.

	Status	ID	Source	Destination	Schedule	Service	Action
wan1 -> internal (1)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	all	all	always	ANY
wan1 -> wan1 (1)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2	all	all	always	ANY
Implicit (1)							

	Status	ID	Source	Destination	Schedule	Service	Action
wan1 -> internal (1)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	all	all	always	ANY
wan1 -> wan1 (1)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2	all	all	always	ANY
Implicit (1)							

299. L'inspection du contenu SSL est activée sur l'unité FortiGate. Laquelle des étapes suivantes est nécessaire pour empêcher qu'un utilisateur ne reçoive un avertissement de navigateur Web lorsqu'il accède à un site Web crypté SSL ?



Le certificat root du proxy FortiGate SSL doit être importé dans le magasin de certificats local sur le poste de travail de l'utilisateur.

300. Examinez l'image ci-dessous, puis répondez à la question qui la suit. Avec les options de proxy UTM, le certificat CA Fortinet_CA_SSLProxy définit lequel des éléments suivants :

Certificat de signature de l'unité FortiGate utilisé par le proxy SSL.

301. Parmi les affirmations suivantes, lesquelles sont correctes concernant la configuration d'un boîtier FortiGate en tant que passerelle VPN SSL ?

Pour appliquer un portail à un utilisateur, cet utilisateur doit appartenir à un groupe d'utilisateurs SSL VPN.

Les paramètres du portail spécifient si la connexion fonctionnera en mode Web uniquement ou en mode tunnel.

302. Lorsque le proxy SSL inspecte le certificat du serveur pour le filtrage Web uniquement en mode SSL Handshake, quel champ de certificat est utilisé pour déterminer l'évaluation du site ?

Nom commun

303. Dans le widget Tunnel Mode du portail Web, l'administrateur a configuré un pool d'adresses IP et activé le split tunneling. Laquelle des affirmations suivantes est vraie concernant l'adresse IP utilisée par le client VPN SSL ?

Le pool d'adresses IP spécifié dans les options du widget de mode tunnel SSL-VPN remplacera la plage d'adresses IP définie dans les paramètres SSL-VPN.

304. La fonction Host Check peut être activée sur l'unité FortiGate pour les connexions VPN SSL. Lorsque cette fonctionnalité est activée, l'unité FortiGate sonde l'ordinateur hôte distant pour vérifier qu'il est "sûr" avant que l'accès ne soit accordé. Lequel des éléments suivants n'est PAS une option dans le cadre de la fonction de vérification de l'hôte ?

Logiciel de pare-feu Microsoft Windows

305. Que faut-il dans une configuration FortiGate pour avoir plus d'un VPN IPsec commuté en mode agressif ?

Chaque numérotation en mode agressif DOIT accepter les connexions de différents ID de pair.

306. Un utilisateur final se connecte au portail VPN SSL à accès complet et sélectionne l'option Mode Tunnel en cliquant sur le bouton « Se connecter ». L'administrateur a activé le split tunneling. Étant donné que l'utilisateur s'authentifie par rapport à la politique VPN SSL illustrée dans l'image ci-dessous, la déclaration ci-dessous identifie la route qui est ajoutée à la table de routage du client.

statement below identifies the route that is added to the client's routing table.

Seq.#	Source	Destination	Schedule	Service	Authentication	Action	UTM Profile	Log	NA
▼ port3 - port1 (1 - 1)									
1	all	all	always	ALL		✓ ACCEPT			
▼ port1 - port3 (2 - 2)									
2	all	WIN2K3				SSL-VPN			
▼ ssl.root (sslvpn tunnel interface) - port3 (3 - 3)									
3	all	all	always	ALL		✓ ACCEPT			
▼ Implicit (4 - 4)									
4	any	any	always	ALL		DENY			

Une route vers la destination correspondant à l'objet d'adresse "WIN2K3".